CloudStack Administration Documentation

Version 4.8.0

Apache Software Foundation

08 February 2017

Table des matières

Ce guide est destiné aux administrateurs d'un cloud basé sur CloudStack. Pour les notes de versions, l'installation et l'introduction générale à CloudStack, veuillez vous référer aux guides suivants :

- Accueil de la documentation
- Guide d'installation
- Notes de versions

CHAPITRE 1

Interface utilisateur

1.1 Interface utilisateur

1.1.1 Se connecter à l'interface utilisateur

CloudStack fournit une console web destinée à la fois aux administrateurs et aux utilisateurs finaux. La version appropriée de cette interface est affichée en fonction des identifiants utilisés à la connexion. L'interface est disponible depuis les navigateurs internet les plus populaires, incluant IE7, IE8, IE9, Firefox 3.5+, Firefox 4, Safari 4 et Safari 5. L'URL est : (remplacer par l'adresse IP de votre serveur de gestion)

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

Sur une nouvelle installation d'un serveur de gestion, un assistant de configuration apparaît. Lors des futures visites, vous verrez un écran de connexion dans lequel vous spécifierez ce qui suit pour accéder au tableau de bord :

Utilisateur -> L'identifiant utilisateur de votre compte. L'utilisateur par défaut est admin.

Mot de passe -> Le mot de passe associé à l'identifiant utilisateur. Le mot de passe pour l'utilisateur par défaut est password.

Domaine -> Si vous êtes un utilisateur root, laissez ce champ vide.

Si vous êtes un utilisateur d'un des sous-domaines, renseigner le chemin complet du domaine, en excluant le domaine racine.

Par exemple, en supposant que plusieurs niveaux aient été créés sous le domaine racine, comme par exemple Comp1/rh. Les utilisateurs du domaine Comp1 doivent renseigner Comp1 dans le champ Domaine, tandis que les utilisateurs du domaine Comp1/ventes doivent saisir Comp1/ventes.

Pour plus de conseils à propos des choix qui apparaissent lors de la connexion à cette interface, voir Se connecter en tant qu'Administrateur.

Vue d'ensemble de l'interface pour les utilisateurs

L'interface de CloudStack aide les utilisateurs de l'infrastructure cloud à visualiser et utiliser leurs ressources cloud, incluant les machines virtuelles, les modèles et les ISOs, les volumes de données et les instantanés, les réseaux invités et les adresses IP. Si l'utilisateur est un membre ou administrateur d'un ou plusieurs projets CloudStack, l'interface fournit une vue orientée projet.

Vue d'ensemble de l'interface pour les administrateurs

L'interface de CloudStack aide l'administrateur CloudStack à provisionner, voir et gérer l'infrastructure cloud, les domaines, les comptes utilisateurs, les projets et les paramètres de configuration. La première fois que vous démarrez l'interface utilisateur d'une nouvelle installation du serveur de gestion, vous pouvez choisir de suivre l'assistant de démarrage pour provisionner votre infrastructure cloud. Lors des connexions ultérieures, le tableau de bord de l'utilisateur connecté apparaît. Les différents liens de cet écran et de la barre de navigation sur la gauche fournissent un accès à une variété de fonctions administratives. L'administrateur peut également utiliser l'interface pour effectuer l'ensemble des tâches qui sont proposées à un utilisateur final.

Se connecter en tant qu'Administrateur

Après l'installation et le démarrage du logiciel de gestion, vous pouvez utiliser l'interface utilisateur de CloudStack. Cette interface est là pour vous aider à provisionner, voir et gérer votre infrastructure cloud.

1. Ouvrir votre navigateur web favori et aller à cette URL. Remplacer par l'adresse IP de votre serveur de gestion :

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

   Après s'être connecté sur une nouvelle installation d'un serveur de gestion, un assistant de configuration apparaît. Lors des futures visites, vous serez directement redirigé vers le tableau de bord :

2. Si vous voyez l'écran de premier démarrage, choisissez une des options suivantes :
   — **Continuer avec la configuration basique.** Choisissez cette option si vous êtes juste en train d'essayer CloudStack et si vous voulez un guide pour vous aider dans la configuration la plus simple possible afin de vous permettre de démarrer rapidement. Nous vous aiderons à configurer un cloud avec les fonctionnalités suivantes : une machine unique qui fait fonctionner le logiciel CloudStack et qui utilise le service NFS comme stockage ; une machine unique faisant fonctionner des machines virtuelles sous les hyperviseurs XenServer ou KVM ; et un réseau public partagé.
   Les indications de cette visite guidée devraient vous fournir toutes les informations dont vous avez besoin, mais si vous désirez un peu plus de détails, vous pouvez suivre le Guide d'Installation.
   — **J'ai déjà utilisé CloudStack.** Choisissez cette option si vous avez déjà effectué une phase de design et planifié un déploiement plus sophistiqué ou si vous êtes prêts à démarrer la configuration d'un cloud d'essais que vous auriez configuré plus tôt avec les écrans de configuration basiques. Dans l'interface d'administration, vous pouvez commencer à utiliser les plus puissantes fonctionnalités de CloudStack, comme les réseaux avancés à base de VLAN, la haute disponibilité, les éléments réseaux additionnels comme les répartiteurs de charge et les pare-feu et le support de multiples hyperviseurs incluant Citrix XenServer, KVM et VMware vSphere.
   Le tableau de bord de l'administrateur apparaît.

3. Vous devriez fournir un nouveau mot de passe pour l'administrateur. Si vous choisissez la configuration basique, un nouveau mot de passe vous sera demandé juste après. Si vous choisissez Utilisateur expérimenté, suivre la procédure *Changer le mot de passe Root*.

Avertissement : Vous êtes connectés en tant qu'administrateur. Ce compte gère le déploiement de CloudStack, incluant l'infrastructure physique. L'administrateur peut modifier les paramètres de configuration pour changer les fonctionnalités de base, créer ou supprimer des comptes utilisateurs et effectuer des actions qui ne peuvent l'être que par une personne autorisée. Pensez à changer le mot de passe par défaut pour un nouveau.

Changer le mot de passe Root

Durant l'installation et tout au long de l'administration du cloud, vous devrez vous connecter à l'interface en tant qu'administrateur. Le compte administrateur gère le déploiement de CloudStack, incluant l'infrastructure physique. L'administrateur peut modifier les paramètres par défaut pour changer les fonctionnalités de base, créer ou supprimer des comptes utilisateurs et effectuer des actions qui ne peuvent l'être que par une personne autorisée. Lorsque vous installez CloudStack pour la première fois, pensez à changer le mot de passe par défaut pour un nouveau.

1. Ouvrir votre navigateur web favori et aller à cette URL. Remplacer par l'adresse IP de votre serveur de gestion :

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

2. Se connecter à l'interface en utilisant le compte root et son mot de passe. Les valeurs par défaut sont admin, password.
3. Cliquer sur Comptes.
4. Cliquer sur le nom du compte administrateur.
5. Cliquer sur Voir les utilisateurs.
6. Cliquer sur le nom de l'administrateur.
7. Cliquer sur le bouton Changer le mot de passe. 
8. Saisir le nouveau mot de passe et cliquer sur OK.

CHAPITRE 2

Gérer les comptes, les utilisateurs et les domaines

2.1 Gérer les rôles, les comptes, les utilisateurs et les domaines

2.1.1 Rôles, Comptes, Utilisateurs et Domaines

Rôles

Un rôle représente un ensemble de fonctions autorisées. Tous les comptes CloudStack ont un rôle qui leur est attaché et qui applique des règles qui lui autorisent ou qui lui refusent une requête d'API. Typiquement, il existe 4 rôles par défaut : admin root, admin de ressources, admin de domaine et utilisateur.

Comptes

Un compte représente généralement un client du fournisseur de service ou un département dans une grande organisation. Plusieurs utilisateurs peuvent exister dans un compte.

Domaines

Les comptes sont regroupés par domaines. Les domaines contiennent généralement plusieurs comptes qui ont une certaine relation logique entre eux et un ensemble d'administrateurs délégués avec une certaine autorité sur le domaine et ses sous-domaines. Par exemple, un fournisseur de services avec plusieurs revendeurs pourrait créer un domaine pour chaque revendeur.

Pour chaque compte créé, le Cloud crée trois types de comptes différents : administrateur root, administrateur de domaine et utilisateur.

Utilisateurs

Les utilisateurs sont comme des alias dans le compte. Les utilisateurs qui sont dans le même compte ne sont pas isolés les uns des autres mais sont isolés des utilisateurs des autres comptes. La plupart des installations n'ont aucune notion des utilisateurs ; elles ont seulement un utilisateur par compte. Un même utilisateur ne peut pas appartenir à plusieurs comptes.

Le nom d'utilisateur est unique dans un domaine. Le même nom d'utilisateur peut exister dans d'autres domaines ou sous-domaines. Un nom de domaine peut être réutilisé seulement si le chemin complet est unique. Par exemple, vous pouvez créer root/d1, ainsi que root/exemple/d1 et root/ventes/d1.

Les administrateurs sont des comptes disposants de droits spéciaux dans le système. Il peut y avoir plusieurs administrateurs dans le système. Les administrateurs peuvent créer ou supprimer d'autres administrateurs et changer le mot de passe de n'importe quel utilisateur du système.

Administrateurs de domaine

Les administrateurs de domaine peuvent exécuter des opérations administratives pour les utilisateurs appartenant à leur domaine. Les administrateurs de domaine n'ont pas de visibilité sur les serveurs physiques ou sur les autres domaines.

Administrateur root

Les administrateurs racines ont un accès complet au système, incluant la gestion des modèles, les offres de service, les administrateurs de clientèles et les domaines.

Propriétaire d'une ressource

Les ressources appartiennent à un compte, elles n'appartiennent pas à un utilisateur individuel de ce compte. Par exemple, la facturation, les limites de ressources, etc. sont calculées pour un compte, elles ne le sont pas par utilisateurs. Un utilisateur peut opérer sur n'importe quelle ressource de son compte pour peu que le compte fournissant l'utilisateur dispose des privilèges pour cette opération. Les privilèges sont déterminés par le rôle. Un administrateur peut changer le propriétaire de n'importe quelle machine virtuelle d'un compte vers un autre compte en utilisant l'API assignVirtualMachine. Un administrateur de domaine ou de sous-domaine peut faire de même pour les machines virtuelles de son domaine d'un compte à un autre compte de son domaine ou de n'importe lequel de ses sous-domaines.

2.1.2 Utiliser les rôles dynamiques

En complément des quatre rôles par défaut, la fonctionnalité de vérification d'API basée sur les rôles dynamiques autorise les administrateurs à créer de nouveaux rôles avec des permissions personnalisées. Les règles d'autorisations/refus peuvent être configurées dynamiquement durant le fonctionnement sans devoir redémarrer le(s) serveur(s) de gestion.

Pour une compatibilité ascendante, tous les rôles sont rattachés à un des quatre types de rôle : admin, admin de ressource, admin de domaine, et utilisateur. Un nouveau rôle peut être créé en utilisant les onglets rôles dans l'interface en spécifiant un nom, un type de rôle et optionnellement une description.

Les règles spécifiques d'un rôle peuvent être configurés par l'onglet règles dans la page de détails d'un rôle spécifique. Une règle est soit un nom d'API ou un chaîne de caractères jockers qui sont une autorisation ou un refus et optionnellement une description.

Quand un utilisateur effectue une requête d'API, le backend vérifie si l'API demandée apparaît dans les règles configurées (dans l'ordre dont les règles ont été configurées) pour le rôle du compte utilisateur appelant. Il va parcourir toutes les règles et autorisera la requête d'API si l'API correspond à une règle d'autorisation, ou la refusera si elle correspond à une règle de refus. Ensuite, si la requête d'API échoue dans la correspondance avec une règle configurée, il l'autorisera si l'API par défaut autorise ce type de rôle utilisateur et finalement refusera la requête d'API s'il échoue à l'autoriser/refuser explicitement par les règles de permissions des rôles ou par l'autorisation par défaut de l'API. Note : pour éviter à l'administrateur d'être verrouillé par le système, tous les comptes d'administrateur racine sont autorisés pour toutes les APIs.

La fonctionnalité de rôles dynamiques est activée par défaut seulement pour les nouvelles installations de CloudStack depuis la version 4.9.x.

Après une montée de version, les déploiements déjà existant peuvent être migrés pour mettre en oeuvre cette fonctionnalité en lançant l'outil de migration en tant qu'administrateur CloudStack. L'outil de migration se situe sous `/usr/share/cloudstack-common/scripts/util/migrate-dynamicroles.py`.

Durant la migration, cet outil active un drapeau interne dans la base de données, copie les règles statiques basées sur les rôles depuis le fichier commands.properties fournit (typiquement sous `/etc/cloudstack/management/commands.properties`) vers la base de données et renomme le fichier commands.properties (typiquement sous /etc/cloudstack/management/commands.properties.deprecated). Le processus de migration ne nécessite pas un redémarrage du ou des serveurs de gestion.

Utilisation : `migrate-dynamicroles.py` [options] [-h pour l'aide]

Options :

-b DB	Le nom de la base de données, par défaut : cloud
-u USER	Nom d'utilisateur : un utilisateur MySQL avec les privilèges sur la base de données cloud, par défaut : cloud
-p PASSWORD	Mot du passe de l'utilisateur MySQL disposant des privilèges sur la base de données cloud
-H HOST	Nom d'hôte ou adresse IP du serveur Mysql
-P PORT	Port du serveur Mysql, par défaut : 3306
-f FILE	Le fichier commands.properties, par défaut : /etc/cloudstack/management/commands.properties
-d	Cet outil va effectuer des tests et des opérations de debuggage.

Exemple :

sudo python /usr/share/cloudstack-common/scripts/util/migrate-dynamicroles.py -u cloud -p cloud -h localhost -p 3006 -f /etc/cloudstack/management/commands.properties

Si vous avez plusieurs serveurs de gestion, supprimer ou renommer le fichier commands.properties sur tous les serveurs de gestion, typiquement sous /etc/cloudstack/management, après avoir lancé l'outil de migration sur le premier serveur de gestion.

2.1.3 Dédier des ressources à des comptes et des domaines

L'administrateur root peut dédier des ressources à un domaine spécifique ou à un compte qui nécessite une infrastructure privée pour plus de sécurité ou des garanties de performances. Une zone, un pod, un cluster ou un hôte peut être réservé par l'administrateur root pour un domaine ou un compte spécifique. Seuls les utilisateurs dans ce domaine ou ses sous-domaines peut utiliser cette infrastructure. Par exemple, seuls les utilisateurs dans un domaine donné peut créer des invités dans la zone dédiées à ce domaine.

Ils existes de nombreux types d'attribution possibles :

- Attribution explicite. Une zone, un pod, un cluster ou un hôte sont dédiés à un compte ou un domaine par l'administrateur racine durant le déploiement initial et la configuration.
- Attribution stricte implicite. Un hôte ne sera pas partagé pour différents comptes. Par exemple, une attribution stricte implicite est utile pour le déploiement de certains types d'applications, comme les applications de bureaux, où aucun hôte ne peut être partagé entre des comptes différents sans violer les termes de licences du logiciel de bureau.
- Attribution implicite préférée. La VM sera déployée si possible dans l'infrastructure dédiée. Sinon, la VM peut être déployée dans l'infrastructure partagée.

2.1.4 Comment dédier une zone, un cluster, un pod ou un hôte à un compte ou à un domaine

Pour l'attribution explicite : lors du déploiement d'une nouvelle zone, d'un pod, d'un cluster ou d'un hôte, l'administrateur root peut cliquer sur la case à cocher Dedié, et choisir alors un domaine ou un compte propriétaire de la ressource.

Pour explicitement dédié une zone, un pod, un cluster ou un hôte déjà existant : se connecter en tant qu'administrateur root, trouver la ressource dans l'interface et cliquer sur le bouton Dédier. 

Pour l'attribution implicite : L'administrateur créer une offre de service !compute ! et dans le champ Planification de déploiement, choisit ImplicitDedicationPlanner. Alors, ans le mode Plannification, l'administraeur spécifie soit Strict, soit Préféré, en fonction de s'il est possible d'autoriser l'utilisation de ressources partagées lorsque les ressources dédiées ne sont pas disponibles. Même si un utilisateur créé une VM basée sur cette offre de service, elle est allouée sur un de ses hôtes dédiés.

Comment utiliser les Hôtes Dédiés

Pour utiliser un hôte dédié explicitement, utiliser le type de groupe d'affinité Explicitement-dédié (voir "Groupes d'affinité"). Par exemple, lorsque une nouvelle VM est créée, un utilisateur final peut choisir de la placer dans son infrastructure dédiée. Cette opération fonctionnera seulement si une partie de son infrastructure a déjà été assignée comme dédiée au compte de l'utilisateur ou au domaine.

Comportement des hôtes, clusters, pods et zones dédiés

L'administrateur peut migrer à chaud des machines virtuelles depuis ses hôtes dédiés, s'il le désire, même si la destination est un hôte réservé pour un compte/domaine différent ou si un hôte est partagé (non dédié à un compte ou un domaine particulier). CloudStack va générer une alerte, mais l'opération sera permise.

Les hôtes dédiés peuvent être utilisés en conjonction avec les tags d'hôtes. Si à la fois un tag d'hôtes et une réservation sont demandées, la machine virtuelle sera placée seulement sur un hôte qui réponds aux deux requêtes. S'il n'y a pas de ressources dédiées disponible pour cet utilisateur qui n'aurait également le tag d'hôte demandé par l'utilisateur, alors la machine ne sera pas déployée.

Si vous supprimez un compte ou un domaine, tous les hôtes, les clusters, les pods, et les zones qui lui ont été dédiées sont libérées. Ils seront dorénavant disponibles pour être partagés par n'importe quel compte ou domaine, ou l'administrateur peut choisir de les dédier à nouveau à un autre compte ou un autre domaine.

Les machines virtuelles systèmes et les routeurs virtuels affecte le comportement de la réservation d'hôte. Les machines virtuelles et les routeurs virtuels appartiennent au compte système CloudStack et peuvent être déployé sur n'importe quel hôte. Ils ne respecte pas les réservations explicites. La présence de VM systèmes et de routeurs virtuels sur un hôte rendent la réservation explicite stricte inappropriée. L'hôte ne peut pas servir pour la réservation implicite puisque l'hôte a déjà des VMs d'un compte spécifique (le compte système par défaut). Toutefois, un hôte avec des VMs systèmes ou des routeurs virtuels peut être utilisé pour la réservation implicite préférée.

2.1.5 Utiliser un serveur LDAP pour l'authentification des utilisateurs

Vous pouvez utiliser un serveur LDAP externe comme Microsoft Active Directory ou ApacheDS pour authentifier les utilisateurs CloudStack. CloudStack cherchera dans l'arbre de l'annuaire LDAP externe depuis un répertoire de base spécifié et obtiendra les informations de l'utilisateur comme son nom, son prénom, son email et son nom d'utilisateur.

Pour l'authentification, le nom d'utilisateur et le mot de passe saisis par l'utilisateur sont utilisés. CloudStack effectue une recherche pour un utilisateur avec le nom fourni. S'il existe, il effectue une requête d'authentification avec le DN et le mot de passe.

Pour paramétrer l'authentification LDAP dans CloudStack, appeler la commande d'API CloudStack ‘‘addLdapConfiguration‘‘et fournir un nom de machine ou une adresse IP et le port d'écoute du serveur LDAP. Vous pouvez bien entendu configurer plusieurs serveurs. Ces derniers sont considérés comme des réplicats. Si un serveur tombe en panne, le suivant sera utilisé.

Les options de configuration globale suivantes devraient également être configurée (les valeurs par défaut s'applique à openldap)

- `ldap.basedn` : Positionne le basedn pour LDAP. Ex : **OU=APAC,DC=company,DC=com**
- `ldap.bind.principal`, `ldap.bind.password` : DN et mot de passe pour l'utilisateur qui dispose des droits pour lister tous les utilisateurs dans la basedn fournie ci-dessus. Ex : **CN=Administrator, OU=APAC, DC=company, DC=com**
- `ldap.user.object` : type d'objet définissant les utilisateurs au sein de LDAP. La valeur par défaut est **user** pour AD et **inetorgperson** pour openldap.
- `ldap.email.attribute` : attributs email au sein de LDAP pour un utilisateur. La valeur par défaut pour AD et pour openldap est **mail**.
- `ldap.firstname.attribute` : attribut prénom au sein de LDAP pour un utilisateur. La valeur par défaut pour AD et openldap est **givenname**.
- `ldap.lastname.attribute` : attribut nom de famille au sein de LDAP pour un utilisateur. La valeur par défaut pour AD et openldap est **sn**.
- `ldap.username.attribute` : attribut nom d'utilisateur pour un utilisateur au sein de LDAP. La valeur par défaut est **SAMAccountName** pour AD et **uid** pour openldap.

Restreindre les utilisateurs LDAP à un groupe :

- `ldap.search.group.principle` : ceci est optionnel et si positionné seuls les utilisateurs de ce groupe sont listés.

LDAP SSL :

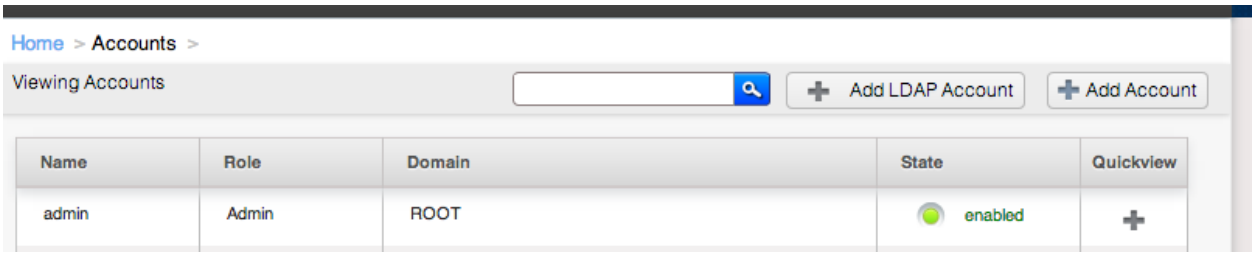
Si le serveur LDAP nécessite SSL, vous devez activer les configurations ci-dessous. Avant d'activer SSL pour LDAP, vous devez obtenir le certificat utilisé par le serveur LDAP et l'ajouter à votre magasin de confiance. Vous devez connaître le chemin d'accès au magasin et le mot de passe.

- `ldap.truststore` : chemin d'accès au magasin de clefs
- `ldap.truststore.password` : mot de passe du magasin de clefs

Groupes LDAP :

- `ldap.group.object` : type d'objet pour un groupe au sein de LDAP. La valeur par défaut pour AD est **group** pour AD et **groupOfUniqueNames** pour openldap.
- `ldap.group.user.uniquemember` : attributs pour les membres d'un groupe. La valeur par défaut est **member** pour AD et **uniquemember** pour openldap.

Une fois configuré, sur la page Ajout de compte, vous verrez un bouton "Ajouter un compte LDAP" qui ouvre une boîte de dialogue et les utilisateurs sélectionnés peuvent être importés.



Vous pouvez également utiliser les commandes d'API : `listLdapUsers`, `ldapCreateAccount` et `importLdapUsers`.

Une fois que LDAP est activé, les utilisateurs ne seront plus autorisés à changer leurs mots de passe directement depuis depuis CloudStack.

2.1.6 Utiliser un fournisseur d'identité SAML 2.0 pour l'authentification des utilisateurs

Vous pouvez utiliser un fournisseur d'identité SAML 2.0 avec CloudStack pour l'authentification utilisateur. Cela nécessitera d'activer le plugin du fournisseur de service SAML 2.0. Pour cela, activer le plugin SAML en configuration `saml2.enabled` à `true` et redémarrer le serveur de gestion.

Depuis la version 4.5.2, le plugin SAML utilise un workflow d'autorisation dans lequel les utilisateurs devrait être autorisés par un administrateur à utiliser l'API `authorizeSamlSso`. Auparavant, ces utilisateurs pouvaient utiliser le Single Sign On via un IdP spécifique. Ceci peut être fait en cochant la case d'activation SAML Single Sign On et en sélectionnant un IdP lors de l'ajout ou de l'importation d'utilisateurs. Pour un utilisateur existant, les administrateurs peuvent aller à la page de l'utilisateur et cliquer sur l'option activation/désactivation de l'option SAML SSO pour un utilisateur et sélectionner un fournisseur d'identité. Un utilisateur peut être autorisé pour s'autentifier via un seul IdP.

La méta-donnée de CloudStack du fournisseur de service est accessible en utilisant la commande d'API `getSPMetadata` ou depuis l'URL http://acs-server:8080/client/api?command=getSPMetadata où acs est le nom de domaine ou l'adresse IP du serveur de gestion. L'administrateur de l'IdP peut obtenir la métadonnée du SP depuis CloudStack et l'ajouter à son serveur IdP.

Pour commencer une authentification Single Sign-On SAML 2.0, les utilisateurs, depuis la page de connexion, doivent sélectionner le fournisseur d'identité ou l'institution/département avec lequel ils peuvent s'authentifier et cliquer sur le bouton Connexion. Cette action appelle la commande d'API `samlsso` qui va rediriger l'utiliser à la page de connexion du fournisseur d'identité. Après une authentification réussie, l'IdP va rediriger l'utilisateur vers CloudStack. Dans le cas ou un utilisateur dispose de plusieurs comptes avec le même nom d'utilisateur (sur plusieurs domaines) pour le même IdP autorisé, cet utilisateur devra spécifier le chemin du domaine après avoir sélectionner son serveur IdP depuis la liste de choix. Par défaut, les utilisateurs n'ont pas besoin de spécifier un chemin de domaine. Après qu'un utilisateur soit authentifié avec succès par un serveur IdP, le plugin d'authentification SAML trouve les comptes utilisateurs dont le nom d'utilisateur correspond à l'attribut nom d'utilisateur retourné par la réponse d'authentification SAML ; ceci échoue seulement lorsqu'il trouve qu'il existe plusieurs comptes utilisateurs avec le même nom d'utilisateur pour cet IdP spécifiquement et dans les autres cas le compte utilisateur unique est autorisé, et l'utilisateur est connecté à son compte.

Limitations :

- Le plugin utilise l'attribut utilisateur retourné par le serveur IDP dans la réponse SAML pour trouver et associer l'utilisateur autorisé dans CloudStack. L'attribut par défaut est *uid*.
- Le plugin d'authentification SAML support les authentifications HTTP-Redirect et HTTP-Post.
- Testé avec Shibboleth 2.4, SSOCircle, Microsoft ADFS, OneLogin, Feide OpenIDP, PingIdentity.

La configuration globale suivante doit être effectuée :

- `saml2.enabled` : Indique si le plugin SAML SSO est activé ou non. La valeur par défaut est **false**
- `saml2.sp.id` : chaîne de l'identifiant du fournisseur de service SAML2
- `saml2.idp.metadata.url` : URL du fichier de méta-données du fournisseur d'identité SAML2 ou nom de fichier . Si une URL est fournie, il cherchera un fichier dans le répertoire de configuration /etc/cloudstack/management
- `saml2.default.idpid` : L'ID par défaut du fournisseur d'identité (IdP) à utiliser seulement dans le cas de multiples fournisseurs d'identités.
- `saml2.sigalg` : L'algorithme à utiliser lors de la signature de requêtes SAML. Par défault l'algorithme est SHA1, les algorithmes autorisés sont : SHA1, SHA256, SHA384, SHA512.
- `saml2.redirect.url` : L'URL de l'interface CloudStack vers lequel le SSO doit rediriger après un succès. L'URL par défaut est **http ://localhost :8080/client**
- `saml2.sp.org.name` : Nom de l'organisme du fournisseur de service SAML2
- `saml2.sp.org.url` : URL de l'organisme du fournisseur de service SAML2
- `saml2.sp.contact.email` : Adresse email de contact du fournisseur de service SAML2

— `saml2.sp.contact.person` : Nom du contact du fournisseur de service SAML2
— `saml2.sp.slo.url` : URL de déconnexion du fournisseur de service SAML2
— `saml2.sp.sso.url` : URL Single Sign On du fournisseur de service SAML2 CloudStack
— `saml2.user.attribute` : Nom de l'attribut à rechercher dans la réponse SAML qui contient le nom d'utilisateur. La valeur par défaut est **uid**
— `saml2.timeout` : Interval de temps de rafraîchissement en secondes des méta-données du fournisseur d'identité SAML2, la valeur minimale est fixée à 300. La valeur par défaut est 1800.

CHAPITRE 3

Utiliser les projets pour organiser les ressources des utilisateurs

3.1 Utiliser les projets pour organiser les utilisateurs et les ressources

3.1.1 Vue d'ensemble des projets

Les projets sont utilisés pour organiser les personnes et les ressources. Les utilisateurs CloudStack, dans les limites d'un seul domaine peuvent se regrouper eux-mêmes dans des équipes de projets et ainsi collaborer et partager des ressources virtuelles, comme des VMs, des instantanés, des modèles, des disques de données et des adresses IP. CloudStack surveille l'utilisation des ressources par projet comme par utilisateur, si bien que l'utilisation des ressources peut être facturé aussi bien à un compte utilisateur qu'à un projet. Par exemple, un cloud privé dans une compagnie de logiciel peut avoir tous les membres du département QA affecté à un projet, la compagnie peut ainsi surveiller les ressources employées durant les tests pendant que les membres du projet peuvent plus facilement isoler leurs efforts des autres utilisateurs du même cloud.

Vous pouvez configurer CloudStack pour autoriser n'importe quel utilisateur à créer un nouveau projet, ou restreindre cette possibilité aux administrateurs CloudStack. Une fois que vous avez créé un projet, vous devenez l'administrateur de ce projet et pouvez ajouter d'autres utilisateurs de votre domaine dans le projet. CloudStack peut être configuré de telle manière que vous puissiez directement ajouter des utilisateurs dans un projet, ou que vous deviez envoyer une invitation qui doit être acceptée. Les membres du projet peuvent voir et gérer toutes les ressources virtuelles créés par n'importe qui dans le projet (par exemple partager des VMs). Un utilisateur peut être membre d'autant de projets que nécessaire et peut changer de vues dans l'interface CloudStack pour n'afficher seulement que les informations relatives à un projet, comme les VMs d'un projet, les membres du projet, les alertes du projet, etc.

L'administrateur du projet peut transmettre ce rôle à un autre membre du projet. L'administrateur du projet peut également ajouter plus de membres, en supprimer depuis le projet, fixer de nouvelles limites de ressources (aussi longtemps qu'elles sont inférieures aux valeurs globales par défaut fixée par l'administrateur CloudStack), et supprimer le projet. Quand un administrateur supprime un membre du projet, les ressources crées par cet utilisateur, comme les instances de VMs demeurent dans le projet. Ceci nous amène au sujet des propriétaires des ressources et quelles ressources peuvent être utilisées par un projet.

Les ressources créés au sein d'un projet appartiennent au projet, pas à un compte particulier de CloudStack, et elles ne peuvent être utilisées qu'au sein du projet. Un utilisateur qui appartient à un ou plusieurs projet peut toujours créer des ressources en dehors de ces projets, et ces ressources appartiennent au compte de l'utilisateur ; elles ne seront pas comptabilisée dans le taux d'utilisations du projet ou dans ses limites de ressources. Vous pouvez créer un réseau du niveau projet pour isoler le trafic au sein d'un projet et fournir des services réseaux comme le transfert de port, la répartition de charge, le VPN et le NATage statique. Un projet peut également faire l'usage de certains types de ressources depuis l'extérieur du projet, si ces ressources sont partagées. Par exemple, un réseau partagé ou un modèle public est accessible à n'importe quel projet dans le domaine. Un projet peut obtenir l'accès à un modèle privé si le propriétaire du modèle l'autorise. Un projet peut utiliser n'importe quelle offre de service ou offre de disque

disponible dans son domaine, cependant vous ne pouvez pas créer des services privés et des offres de disques au niveau d'un projet.

3.1.2 Configurer les projets

Avant que les utilisateurs CloudStack puissent commencer à utiliser les projets, l'administrateur CloudStack doit configurer différentes parties du système, incluant les invitations des membres, les limites sur les ressources de projet, et contrôler qui peut créer des projets.

Configurer les invitations

CloudStack peut être configuré de telle sorte que soit les administrateurs de projet peuvent ajouter des personnes directement à un projet ou si cela est nécessaire devoir leur envoyer une invitation qui doit être acceptée. L'invitation peut être envoyé par email ou via le compte utilisateur CloudStack. Si vous voulez que les administrateurs utilisent une invitation pour ajouter des membres à des projets, activer et configurer la fonctionnalité d'invitations dans CloudStack.

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation à gauche, cliquer sur Paramètres globaux.
3. Dans la zone de recherche, taper project et cliquer sur le bouton de recherche. 
4. Dans les résultats de recherche, vous pouvez voir un petit nombre d'autres paramètres que vous devez fixer pour contrôler comment les invitations se comportent. Le tableau ci-dessous montre les paramètres de configuration globale en relation avec les invitations de projet. Cliquer sur le bouton Editer pour fixer chaque paramètre.

Paramètres de configuration	Description
project.invite.required	Positionner à true pour activer la fonctionnalité d'invitations.
project.email.sender	L'adresse email à afficher dans le champ From des emails d'invitation.
project.invite.timeout	Durée laissée à un nouveau membre pour répondre à une invitation.
project.smtp.host	Nom de l'hôte qui agit comme serveur de messagerie pour gérer les invitations.
project.smtp.password	(Optionnel) Mot de passe requis par le serveur SMTP. Vous devez également positionner le champ project.smtp.username et project.smtp.useAuth à true.
project.smtp.port	Port d'écoute du serveur SMTP
project.smtp.useAuth	Positionner à true si le serveur SMTP nécessite un utilisateur et un mot de passe.
project.smtp.username	(Optionnel) Ne nom d'utilisateur requis par le serveur SMTP pour l'authentification.

5. Redémarrer le serveur de gestion :

```
service cloudstack-management restart
```

Configurer les limitations de ressources pour les projets

L'administrateur de CloudStack peut fixer les limites par défaut globales pour contrôler la quantité de ressources qui peuvent appartenir à chaque projet dans le cloud. Cela permet de prévenir d'un usage incontrôlé des ressources comme les instantanés, les adresses IP et les instances de machines virtuelles. Les administrateurs de domaine peuvent passer outre ces limites de ressources pour des projets individuels de leurs domaines, tant que ces limites sont sous les valeurs globales par défaut fixée par l'administrateur racine de CloudStack. L'administrateur racine peut aussi fixer des limites inférieures pour n'importe quel projet dans le cloud.

Configurer les limitations de ressources par projet

L'administrateur racine CloudStack ou l'administrateur de domaine du domaine dans lequel le projet demeure peut fixer de nouvelles limites de ressources pour un projet individuel. Le propriétaire du projet peut fixer les limites de ressources seulement si le propriétaire est aussi un administrateur de domaine ou racine.

Les nouvelles limites doivent être inférieure des limites globales par défaut fixées par l'administrateur de CloudStack (comme décrit dans *"Configurer les limites de ressources pour les Projets"*). Si le projet détient déjà plus que le nouveau maximum d'un type de ressource donné, les ressources ne sont pas affecté ; toutefois, le projet ne peut plus ajouter de ressources de ce type tant que le total ne repasse pas sous la nouvelle limite.

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans la liste de choix de vue, choisir Projets.
4. Cliquer sur le nom du projet avec lequel vous voulez travailler.
5. Cliquer sur l'onglet Ressources. Ce tableau liste les valeurs maximales courantes que le projet est autorisé à posséder pour chaque type de ressource.
6. Saisir les nouvelles valeurs pour une ou plusieurs ressources.
7. Cliquer sur Appliquer.

Configurer les limites de ressources globales des projets

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation à gauche, cliquer sur Paramètres globaux.
3. Dans la boîte de recherche, saisir max.projects et cliquer sur le bouton de recherche.
4. Dans les résultats de la recherche, vous verrez les paramètres que vous pouvez utiliser pour fixer les montants maximum de ressources par projet qui s'appliqueront à tous les projets du cloud. Aucun projet ne peut avoir plus de ressources, mais un projet individuel peut avoir des limites inférieures. Cliquer sur le bouton Editer pour fixer chaque paramètre. 

max.project.publicips	Le nombre maximum d'adresses IP publiques qui peuvent être possédées par un projet du cloud. Voir A propos des adresses IP publiques.
max.project.snapshots	Nombre maximum d'instantanés qui peuvent être possédés par un projet du cloud. Voir Travailler avec des instantanés.
max.project.templates	Nombre maximum de modèles qui peuvent être possédés par un projet dans le cloud. Voir Travailler avec des modèles.
max.project.user.vms	Nombre maximum de machines virtuelles invitées qui peuvent être possédées par un projet du cloud. Voir Travailler avec des machines virtuelles.
max.project.volumes	Nombre maximum de volumes de données qui peuvent être possédés par un projet du cloud. Voir Travailler avec des volumes.

5. Redémarrez votre serveur de gestion.

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

Configurer les permissions de créateur de projet

Vous pouvez configurer CloudStack pour autoriser n'importe quel utilisateur à créer un nouveau projet, ou vous pouvez restreindre cette possibilité aux seuls administrateurs de CloudStack.

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation à gauche, cliquer sur Paramètres globaux.

3. Dans la boîte de recherche, saisir allow.user.create.projects.
4. Cliquer sur le bouton d'édition pour changer le paramètre . 
   `allow.user.create.projects`
   Fixer à true pour autoriser les utilisateurs finaux à créer des projets. Fixer à false si vous voulez que seul l'administrateur racine de cloudstack et les administrateurs de domaine puisse le faire.
5. Redémarrez votre serveur de gestion.

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

3.1.3 Créer un nouveau projet

Les administrateurs CloudStack et les administrateurs de domaine peuvent créer des projets. Si le paramètre de configuration global allow.user.create.projects est fixé à true, les utilisateurs finaux peuvent également créer des projets.

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans le sélecteur de vue, cliquer sur Projets.
4. Cliquer sur Nouveau projet.
5. Donner au projet un nom et une description pour l'affichage aux utilisateurs, et cliquer sur Créer un projet.
6. Un écran apparaît dans lequel vous pouvez immédiatement ajouter plus de membres au projet. Ceci est optionnel. Cliquer sur Suivant quand vous êtes prêts à y aller.
7. Cliquer sur Sauvegarder.

3.1.4 Ajouter des membres à un projet

Les nouveaux membres peuvent être ajoutés à un projet par l'administrateur du projet, l'administrateur de domaine du domaine dans lequel réside le projet ou un de ses domaines parents, ou l'administrateur racine de CloudStack. Il y a deux façons d'ajouter des membres dans CloudStack, mais une seule peut être activée à la fois :

— Si les invitations ont été activées, vous pouvez envoyer des invitions aux nouveaux membres.
— Si les invitations n'ont pas été activées, vous pouvez ajouter des membres directement via l'interface de gestion.

Envoyer des invitations d'adhésion au projet

Utiliser ces étapes pour ajouter un nouveau membre à un projet si la fonctionnalités d'invitations est activée dans le cloud comme décrit dans *"Configurer les invitations"*. Si la fonctionnalité d'invitations n'est pas activée, utiliser la procédure Ajouter des membres à un projet depuis l'interface.

1. Se connecter à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans la liste de choix de vue, choisir Projets.
4. Cliquer sur le nom du projet avec lequel vous voulez travailler.
5. Cliquer sur l'onglet Invitations.
6. Dans Ajouter par, sélectionner un des choix suivants :
   (a) Compte - L'invitation va apparaître dans l'onglet Invitationsde l'utilisateur dans la vue Projet. Voir Utiliser la vue projet.
   (b) Email - L'invitation sera envoyée à l'adresse email de l'utilisateur. Chaque invitation envoyée inclue un code unique appelé un jeton que le destinataire fournira en retour dans CloudStack lorsqu'il acceptera l'invitation. Les invitations par email fonctionneront seulement si les paramètres globaux en relation avec le serveur SMTP ont été positionnés. Voir *"Configurer les invitations"*.

7. Saisir le nom de l'utilisateur ou l'adresse email du nouveau membre que vous voulez ajouter et cliquer sur Inviter. Saisir le nom de l'utilisateur si vous avez choisi Compte à l'étape précédente. Si vous aviez choisi Email, saisir l'adresse email. Vous pouvez seulement inviter des personnes qui ont un compte dans ce cloud au sein du même domaine que le projet. Toutefois, vous pouvez envoyer l'invitation à n'importe quelle adresse email.
8. Pour voir et gérer les invitations que vous avez envoyés, retourner dans cet onglet. Quand une invitation est acceptée, les nouveaux membres vont apparaître dans l'onglet Comptes du projet.

Ajouter des membres à un projet depuis l'interface

Les étapes ci-dessous explique comment ajouter un nouveau membre à un projet si la fonctionnalité d'invitations n'est pas activée dans le cloud. Si les invitations sont activées, comme décris dans *"Configurer les invitations"*, utiliser la procédure *"Envoyer des invitations aux membres d'un projet"*.

1. Se connecter à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans la liste de choix de vue, choisir Projets.
4. Cliquer sur le nom du projet avec lequel vous voulez travailler.
5. Cliquer sur l'onglet Comptes. Les membres actuels du projet sont listés.
6. Saisir le nom de compte du nouveau membre que vous voulez ajouter et cliquer sur Ajouter le compte. Vous pouvez ajouter seulement les personnes qui ont un compte dans ce cloud et qui sont dans le même domaine que le projet.

3.1.5 Accepter une invitation d'appartenance.

Si vous avez reçu une invitation à joindre un projet CloudStack, et que vous voulez accepter l'invitation, suivre les étapes suivantes :

1. Se connecter à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans la zone de sélection, choisir Invitations.
4. Si vous voyez l'invitation listée à l'écran, cliquer sur le bouton Accepter.
   Les listes d'invitations dans l'écran vous ont été envoyées en utilisant votre nom de compte CloudStack.
5. Si vous avez reçu un email d'invitation, cliquer sur le bouton Saisir le jeton, et fournir l'ID du projet et le code d'identification unique de l'email.

3.1.6 Suspendre ou effacer un projet

Quand un projet est suspendu, il conserve les ressources qu'il possède, mais elle ne peuvent plus être utilisées. Aucune nouvelle ressource ou aucun membre ne peut être ajouté à un projet suspendu.

Quand un projet est supprimé, ses ressources sont détruites, et les comptes des membres sont supprimés du projet. Le status du projet est affiché comme Désactiver durant la suppression finale.

Un projet peut être suspendu ou supprimé par l'administrateur du projet, l'administrateur du domaine du domaine auquel appartient le projet ou d'un de ses domaines parents, ou par l'administrateur root de CloudStack.

1. Se connecter à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Projets.
3. Dans la liste de choix de vue, choisir Projets.
4. Cliquer sur le nom du projet.

5. Cliquer sur un des boutons :
   Pour supprimer, utiliser **|Supprimer un projet|**
   Pour suspendre, utiliser 

3.1.7 Utiliser la vue Projet

Si vous êtes membre d'un projet, vous pouvez utiliser la vue Projet de CloudStack pour voir les membres du projet, les ressources consommées, etc. La vue projet n'affiche que les informations en relation avec le projet. C'est une façon pratique pour filtrer les autres informations ainsi vous pouvez vous concentrer sur le statut du projet et ses ressources.

1. Se connecter à l'interface CloudStack.
2. Cliquer sur la vue Projet.
3. La tableau de bord du projet apparaît, affichant les VMs, les volumes, les utilisateurs, les évènements, les configurations réseaux, etc. du projet. Depuis le tableau de bord, vous pouvez :
   — Cliquer sur l'onglet Comptes pour voir et gérer les membres du projet. Si vous êtes l'administrateur du projet, vous pouvez ajouter des nouveaux membres, retirer des membres, ou changer le rôle d'un membre depuis utilisateur jusqu'à administrateur. Seulement un membre à la fois peut avoir le rôle d'administrateur, ainsi si vous modifier le rôle d'un autre utilisateur pour administrateur, votre rôle va devenir utilisateur standard.
   — (Si les invitations sont activées) Cliquer l'onglet Invitations pour voir et gérer les invitations qui ont été envoyées aux nouveaux membres du projet mais qui ne les ont pas encore acceptés. Les invitations en attentes resteront dans cette liste jusqu'à ce que soit les nouveaux membres les acceptent, soit le délais imparti est atteint, ou si vous annulez l'invitation.

CHAPITRE 4

Offres de services

4.1 Offres de service

En complément à l'infrastructure physique et logique de votre cloud et des serveurs et logiciels CloudStack, vous avez également besoin d'une couche de services utilisateurs pour que les utilisateurs puissent faire un usage du cloud. Cela ne signifie pas seulement une interface utilisateur, mais un ensemble d'options et de ressources parmi lesquels les utilisateurs peuvent se servir, comme les modèles pour créer des machines virtuelles, des disques de stockage, etc. Si vous gérer un service commercial, vous conserverez un suivi de quels services et quelles ressources les utilisateurs ont fait l'usage et leur facturerez. Même si vous ne facturez rien aux personnes qui utilisent votre cloud, en d'autres mots si les utilisateurs sont strictement internes à votre organisation, ou juste des amis qui partagent votre cloud, vous pouvez continuer à suivre quels services ils utilisent et combien le font.

4.1.1 Offres de service, offres de disque, offres de réseau et modèles

Un utilisateur qui créé une nouvelle instance peut faire de nombreux choix à propos de ses caractéristiques et ses capacités. CloudStack fournit plusieurs façons de présenter aux utilisateurs les choix lorsqu'ils créent une nouvelle instance :

- Les offres de services, définies par l'administrateur CloudStack, fournissent un choix de vitesse CPU, de nombre de CPUs, de taille de RAM, d'étiquettes sur les disques racines, et d'autres choix. Voir Créer une nouvelle offre de calcul.
- Les offres de services, définies par l'administrateur CloudStack, fourni un choix de taille de disque et de IOPS (qualité de service) pour le stockage primaire des données. Voir créer une nouvelle offre de disque.
- Les offres de réseaux, définies par l'administrateur CloudStack, décrivent les fonctionnalitées qui sont disponibles aux utilisateurs finaux depuis le routeur virtuel ou un élément de réseau externe sur un réseau d'invité défini. Voir offres de réseaux.
- Les modèles, définis par l'administrateur CloudStack ou par n'importe quel utilisateur, sont des images d'OS de base que les utilisateurs peuvent choisir lorsqu'ils créent une nouvelle instance. Par exemple, CloudStack inclue CentOS comme modèle. Voir Travailler avec les modèles.

En plus de ces choix qui sont proposés aux utilisateurs, il y a un autre type d'offre de service qui n'est disponible qu'à l'administrateur racine de CloudStack et qui est utilisé pour configurer les ressources d'infrastructures virtuelles. Pour plus d'information, voir Mettre à jour un Routeur Virtuel avec les Offres de service système.

4.1.2 Offres de service de disque et de calcul

Une offre de service est un ensemble de fonctionnalités matérielles virtuelles comme un nombre de coeur CPU et de vitesse, de mémoire et de taille disque. L'administrateur CloudStack peut configurer différentes offres que les utilisateurs finaux peuvent choisir depuis les offres disponibles lorsqu'ils créent leur nouvelle VM. Selon l'offre choisie par l'utilisateur, CloudStack émet un enregistrement d'utilisation qui peut être intégré avec le système de paiement.

Certaines caractéristiques d'offres de service doivent être définies par l'administrateur CloudStack et les autres peuvent être laissées indéfinies de façon à ce que les utilisateurs finaux puissent saisir les valeurs qu'ils souhaitent. C'est utile pour réduire le nombre d'offres que l'administrateur doit définir. Au lieu de définir une offre de calcul pour chaque combinaison imaginable de valeurs que l'utilisateur peut désirer, l'administrateur peut définir les offres qui fournissent un peu de flexibilité aux utilisateurs et peuvent servir de base pour de nombres configurations différentes de VM.

Une offre de service inclue les éléments suivants :

- Les ressources CPU, mémoire et réseau garanties
- Comment les ressources sont mesurées
- Comment l'utilisation de la ressources est chargé
- Combien de fois les frais sont générés

Par exemple, une offre de service peut autoriser les utilisateurs à créer une instance de machine virtuelle qui est équivalente à 1 CPU Intel® Core™ 2 à 1 GHz, avec 1 Go de mémoire à 0.20€ de l'heure, avec un trafic réseau mesurée à 0.10€ par Go.

CloudStack sépare les offres de service en offres de calcul et offres de disque. L'offre de service de calcul spécifie :

- Le CPU de l'invité (optionnel). Si non défini par l'administrateur CloudStack, les utilisateurs peuvent choisir les attributs du CPU.
- La RAM de l'invité (optionnel). Si non défini par l'administrateur CloudStack, les utilisateurs peuvent choisir la RAM.
- Le type de réseau invités (virtuel ou direct)
- Les étiquettes sur le disque racine

L'offre de disque spécifie :

- La taille du disque (optionnel). Si non défini par l'administrateur CloudStack, les utilisateurs peuvent choisir la taille du disque.
- Les étiquettes sur le disque de données

Offre de calcul personnalisé

CloudStack vous fournis la flexibilité de spécifier les valeurs désirées pour le nombre de CPU, la vitesse CPU, la mémoire lorsque vous déployez une VM. En tant qu'administrateur, vous créez une offre de calcul en la marquant comme personnalisée et les utilisateurs pourront personnaliser dynamiquement les offres de calcule en spécifiant la mémoire, le CPU au moment de la création ou de la mise à jour de VM. Une offre de calcul personnalisée est la même chose qu'une offre de calcul normale à l'exception que les valeurs des paramètres dynamiques seront fixées à zéro dans les ensembles de modèles donnés. Utiliser cette offre pour déployer une VM en spécifiant des valeurs personnalisées pour les paramètres dynamiques. La mémoire, CPU et nombres de CPU sont considérés comme des paramètres dynamiques.

Les offres de calcul dynamiques peuvent être utilisées dans les cas suivants : déployer une VM, changer l'offre de calcul d'une VM stoppée et augmenter l'offre de VMs en cours de fonctionnement. Pour supporter cette fonctionnalité, un nouveau champs, Personnalisé, a été ajouté à la page Créer une offre de calcul. Si le champs personnalisé est coché, l'utilisateur sera capable de créer une offre de calcul personnalisé en remplissant les valeurs désirées du nombre de CPU, de vitesse CPU et de mémoire. Voir ? pour plus d'informations.

Enregistrer les évènements d'utilisation pour les ressources assignées dynamiquement.

Pour supporter cette fonctionnalité, les évènements d'utilisation ont été améliorées pour enregistrer les évènements des ressources assignée dynamiquement. Les évènements d'utilisation sont enregistrés lorsque la VM est créée depuis une offre de calcul personnalisée et lors des changements d'offre de calcul d'une VM stoppée ou en fonctionnement. Les valeurs de ces paramètres, comme le CPU, la vitesse, la RAM sont enregistrés.

Créer une nouvelle offre de calcul

Pour créer une nouvelle offre de calcul :

1. Se connecter avec les privilèges administrateur dans l'interface de CloudStack.

2. Dans la barre de navigation de gauche, cliquer sur Offres de service.
3. Dans Choisir une offre, choisir Offre de calcul.
4. Cliquer sur Ajouter une offre de calcul.
5. Dans la boîte de dialogue, faire les choix suivants :
   - **Nom** : N'importe quel nom souhaité pour l'offre de service.
   - **Description** : Une description courte pour l'offre qui peut être affichée aux utilisateurs
   - **Type de stockage** : Le type de disque qui doit être alloué. Les allocations locales depuis les stockages directement attachés à l'hôte sur lequel la VM est en fonctionnement. Les allocations partagées depuis un stockage accessible via NFS.
   - **Personnalisée** : Offres de calcul personnalisée peuvent être utilisée dans les cas suivants : déployer une VM, changer l'offre de calcul pour des VM stoppées ou en fonctionnement.
     Si le champ Personnalisé est validée, l'utilisateur final doit remplir les valeurs désirées pour le nombre de CPU, la vitesse CPU et la mémoire RAM lors du choix d'une offre de calcul personnalisée. Lorsque vous cochez la case, ces trois champs de saisie sont masquées dans la boîte de dialogue.
   - **# de coeurs CPU** : le nombre de coeurs qui devraient être allouée à une VM système avec cette offre. Si Personnalisé est coché, ce champ n'apparaît pas.
   - **CPU (en MHz)** : La vitesse CPU des coeurs qui sont alloués à cette VM système. Par exemple, "2000" fournira une fréquence d'horloge de 2GHz. Si Personnalisé est coché, ce champ n'apparaît pas.
   - **Mémoire (en MB)** : La quantité de mémoire en mégabytes que la VM système aura d'alloué. Par exemple, "2048" devrait fournir une allocation de 2GB de RAM. Si Personnalisé est validé, ce champ n'apparaît pas.
   - **Vitesse Réseau** : vitesse de transfert de données autorisée par seconde.
   - **Taux de lecture disque** : taux de lecture disque autorisé en bits par seconde.
   - **Taux d'écriture disque** : taux d'écriture disque autorisé en bits par seconde.
   - **Taux de lecture disque** : taux de lecture disque autorisé en IOPS (opération d'entrées/sorties par seconde).
   - **Taux d'écriture disque** : taux d'écriture disque autorisé en IOPS (opérations d'entrées/sorties par seconde).
   - **Offre HA** : Si oui, l'administrateur peut choisir d'avoir la VM système de monitorée et d'être aussi hautement disponible que possible.
   - **Type de QoS** : Trois options : Vide (pas de qualité de service), hyperviseur (taux de limitation forcé du côté hyperviseur) et stockage (IOPS minimum et maximum garantis forcé du côté stockage). Si vous tirez parti de la QoS, soyez sur que le système de l'hyperviseur ou du stockage supporte cette fonctionnalité.
   - **IOPS personnalisé** : si coché, l'utilisateur peut fixer ses propres IOPS. Si non coché, l'administrateur racine peut définir les valeurs. Si l'admin racine ne fixe pas les valeurs lors de l'utilisation de la QoS du stockage, les valeurs par défaut sont utilisés (les valeurs par défaut peuvent être changée si les paramètres par défaut sont passés à CloudStack lors de la création du stockage primaire en question).
   - **IOPS min** : apparaît seulement si la QoS du stockage doit être utilisée. Fixer un nombre de IOPS garanties forcé du côté du stockage.
   - **IOPS Max** : Apparaît seulement si la QoS doit être utilisée. Fixer un nombre de IOPS maximum a forcer du côté stockage (le système peut aller au delà de ces limites dans certaines circonstances pour des intervalles courts).
   - **Réserve d'instantanés sur l'Hyperviseur** : Pour les stockages gérés seulement. C'est une valeur qui est un pourcentage de la taille du disque racine. Si le disque racine est de 20GB et que la réserve d'instantanée sur l'hyperviseur est de 200%, le volume de stockage qui est réservé sur le dépôt de stockage (XenServer) ou sur le datastore (VMware) en question est taillée à 60GB (20 GB + (20 GB * 2)). Ceci valide de l'espace pour les instantanés en complément du disque virtuel qui représente le disque racine. Ceci ne s'applique pas à KVM.
   - **Étiquettes de stockage** : Les étiquettes qui devraient être associées avec le stockage primaire utilisé par la VM système.
   - **Étiquettes d'hôte** : (Optionnel) Toutes étiquettes que vous utilisez pour organiser vos hôtes
   - **CPU cap** : Pour limiter le taux d'utilisation du CPU ou si les réserves de capacités sont disponibles.
   - **Public** : Indique si l'offre de service doit être disponible pour tous les domaines ou seulement pour certains domaines. Choisir Oui pour rendre disponible à tous les domaines. Choisir No pour limiter la portée à un sous-domaine ; CloudStack va alors demander le nom du sous-domaine.

— **Est volatile** : Si coché, la VM crée depuis cette offre de service aura ces disques racines réinitialisés à chaque redémarrage. C'est utilise pour sécuriser des environnements qui ont besoin d'un démarrage neuf à chaque démarrage et pour les bureaux qui ne doivent pas retenir les états.
— **Planning de déploiement** : Choisir la technique que vous voulez que Cloudstack utilise lorsqu'il déploie la VM basée sur cette offre de service.
First Fit place les nouvelles VMs sur le premier hôte qu'il trouve disposant de suffisamment de capacité pour supporter les besoins de la VM.
User Dispersing fait le maximum d'efforts pour distribuer équitablement les VMs appartenant au même compte sur des clusters ou des pods différents.
User Concentrated préfère déployer les VMs appartenant au même compte sur un pod unique.
L'attribution implicite va déployer les VMs sur une infrastructure privée qui est dédiée à un domaine spécifique ou un compte. Si vous choisissez cette planification, alors vous devez aussi choisir une valeur pour le Mode de planification. Voir "Dédier des ressources à des comptes et des domaines".
Bare Metal est utilisé avec les hôtes bare metal. Voir Installation Bare Metal dans le guide d'installation.
— **Mode de planification** : Utilisé quand ImplicitDedicationPlanner est sélectionné dans le champ précédent.
Le mode de planification détermine comment les VMs vont être déployée sur une infrastructure privée qui est dédiée à un seul domaine ou à un compte.
Strict : Un hôte ne sera pas partagé par plusieurs comptes. Par exemple, la attribution implicite stricte est utile pour le déploiement de certains types d'applications, comme les Bureaux, où aucune hôte ne peut être partagé entre différents comptes sans violer les termes de licence du logiciel de bureau.
Préférée : La VM sera déployée dans une infrastructure dédiée si possible. Sinon, la VM peut être déployée dans une infrastructure partagée.
— **GPU Assigne un GPU physique (GPU-passthrough) ou un portion d'un GPU physique** Carte GPU (vGPU) à la VM invitée. Cela permet à des applications graphique de fonctionner sur la VM. Sélectionner la carte depuis la liste des cartes supportées.
Les options proposées sont NVIDIA GRID K1 et NVIDIA GRID K2. Ces cartes vGPU sont capables d'autoriser plusieurs vGPUs sur un seul GPU physique. Si vous voulez utiliser une carte plutôt que celles-ci, suivre les instructions dans la page **"Support GPU et vGPU pour les VMs invitées CloudStack"** dans le document de conception CloudStack Version 4.4 que vous trouverez dans le wiki CloudStack.
— **Type vGPU** : Représente le type de GPU virtuel à assigner à la VM invitée. Dans ce cas, seulement une partie de la carte physique GPU (vGPU) est attribuée à la VM invitée.
En complément, le type **passthrough vGPU** est défini pour représenter un périphérique GPU physique. Un **passthrough vGPU** peu être directement assigné à une seule VM invitée. Dans ce cas, un périphérique physique GPU est exclusivement alloué à une seule VM invitée.

6. Cliquer sur Ajouter.

Créer une Nouvelle offre de disque.

Pour créer une nouvelle offre de disque :

1. Se connecter avec les privilèges administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Offres de service.
3. Dans Sélectionner une offre, choisir Offre de disque.
4. Cliquer sur Ajouter une offre de disque.
5. Dans la boîte de dialogue, faire les choix suivants :
   — **Nom** : N'importe quel nom souhaité pour l'offre de disque.
   — **Description** : Une description courte pour l'offre qui peut être affichée aux utilisateurs
   — **Taille de disque personnalisée** : Si cochée, l'utilisateur peut fixer sa propre taille de disque. Si non cochée, l'administrateur racine doit définir une taille de disque.
   — **Taille de disque** : Apparaît seulement si la taille de disque personnalisée n'est pas sélectionnée. Définir une taille de volume en GB (2^30 1GB = 1,073,741,824 Bytes).

- **Type de QoS** : Trois options : Vide (pas de qualité de service), hyperviseur (taux de limitation forcé du côté hyperviseur) et stockage (IOPS minimum et maximum garantis forcé du côté stockage). Si vous tirez parti de la QoS, soyez sur que le système de l'hyperviseur ou du stockage supporte cette fonctionnalité.
- **IOPS personnalisé** : si coché, l'utilisateur peut fixer ses propres IOPS. Si non coché, l'administrateur racine peut définir les valeurs. Si l'admin racine ne fixe pas les valeurs lors de l'utilisation de la QoS du stockage, les valeurs par défaut sont utilisés (les valeurs par défaut peuvent être changée si les paramètres par défaut sont passés à CloudStack lors de la création du stockage primaire en question).
- **IOPS min** : apparaît seulement si la QoS du stockage doit être utilisée. Fixer un nombre de IOPS garanties forcé du côté du stockage.
- **IOPS Max** : Apparaît seulement si la QoS doit être utilisée. Fixer un nombre de IOPS maximum a forcer du côté stockage (le système peut aller au delà de ces limites dans certaines circonstances pour des intervalles courts).
- **Rétention d'instantanés de l'hyperviseur** : pour le stockage de gestion seulement. C'est une valeur qui est un pourcentage de la taille du disque de données. Par exemple, si le disque de données fait 20GB et que la rétention d'instantanés de l'hyperviseur est de 200%, alors le stockage de volume qui soutient le stockage de données (XenServer) ou le datastore (VMware) en question est taillé à 60 GB (20 GB + (20 GB *2)). Cela active de l'espace pour les instantannés de l'hyperviseur en complétement au disque virtuel qui représente les données du disque. Cela ne s'applique pas à KVM.
- **(Optionnel) Etiquettes de stockage** : Les étiquettes qui devraient être associées avec le stockage primaire pour ce disque. Les étiquettes sont des listes d'attributs du stockage séparés par des virgules. Par exemple "ssd,bleu". Les étiquettes sont aussi ajoutées sur le stockage primaire. CloudStack fait correspondre les étiquettes de l'offre de disque aux étiquettes sur le stockage. Si une étiquette est présente sur une offre de disque cette ou ces étiquettes doivent aussi être présente sur le stockage primaire pour que le volume soit provisionné. S'il n'existe pas un tel stockage primaire, l'attribution depuis l'offre de disque va échouer.
- **Public** : Indique si l'offre de service doit être disponible pour tous les domaines ou seulement pour certains domaines. Choisir Oui pour rendre disponible à tous les domaines. Choisir No pour limiter la portée à un sous-domaine ; CloudStack va alors demander le nom du sous-domaine.

6. Cliquer sur Ajouter.

Modifier ou détruire une offre de service

Les offres de service ne peuvent pas être changée une fois crée. Ceci s'applique à la fois aux offres de calcul et aux offres de disque.

Une offre de service peut être supprimée. Si elle n'est plus utilisée, elle est détruite immédiatement et de façon permanente. Si l'offre de service est toujours utlisée, elle restera en base de données jusqu'à ce que toutes les machines virtuelles la référençant ont été supprimées. Après la suppression par l'administrateur, l'offre de service ne sera plus disponible pour les utilisateurs finaux qui créent de nouvelles instances.

4.1.3 Offres de service système

Les offres de service système fournissent un choix de vitesse CPU, un nombre de CPUs, étiquettes et taille de RAM, comme d'autres offres de services le font. Mais plutôt qu'être utilisée pour les instances de machine virtuelle et être exposée aux utilisateurs, les offres de service système sont utilisée pour changer les propriétées par défaut des routeurs virtuels, des proxys console, et d'autres VMs systèmes. Les offres de service système sont visibles seulement par l'administrateur racine CloudStack. CloudStack fournit par défaut les offres de service système par défaut. L'administrateur racine de CloudStack peut créer des offres de services systèmes additionnelles.

Quand CloudStack crée un routeur virtuel pour un réseau invité, il utilise les paramètres par défaut qui sont définis dans l'offre de service associée avec l'offre réseau. Vous pouvez mettre à jour les capacités du routeur virtuel en appliquant une nouvelle offre qui contient une offre de service différente. Tous les routeurs virtuels dans ce réseau vont démarrer en utilisant les configurations de la nouvelle offre de service.

Créer une Nouvelle offre de service système

Pour créer une offre de service système :

1. Se connecter avec les privilèges administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Offres de service.
3. Dans Choisir l'offre, choisir Offre système.
4. Cliquer sur Ajouter une offre de service système.
5. Dans la boîte de dialogue, faire les choix suivants :
   — Nom. N'importe quel nom pour l'offre système.
   — Description. Une description courte pour l'offre qui peut être affichée aux utilisateurs.
   — Type de VM système. Sélectionner le type de machine virtuelle système que cette offre est destinée à supporter.
   — Type de stockage. Le type de disque qui peut être alloué. L'allocation locale depuis un stockage attaché directement à l'hôte où la VM système fonctionne. Les partagées allouent depuis un stockage accessible via NFS.
   — # de coeurs CPU : le nombre de coeurs qui devraient être alloués à la VM système avec cette offre.
   — CPU (en MHz). La vitesse CPU des coeurs alloués à la VM système. Par exemple, "2000" devrait fournir une vitesse d'horloge de 2Ghz.
   — Mémoire (en MB). La quantité de mémoire en mégabytes qui devrait être allouée à la VM système. Par exemple, "2048" devrait fournir une allocation de 2 GB de RAM.
   — Vitesse réseau. Vitesse de transfert de données autorisé en MB par seconde.
   — Offre HA. Si oui, l'administrateur peut choisir d'avoir la VM système de monitorée et d'être aussi hautement disponible que possible.
   — Etiquettes de stockage. Les étiquettes qui sont associées avec le stockage primaire utilisé par la VM système.
   — Etiquettes d'hôtes. (Optionnel) N'importe quelle étiquette que vous utilisez pour organiser vos hôtes.
   — CPU cap. Pour limiter le taux d'utilisation du CPU si la capacité de réserve est disponible.
   — Public. Indique si l'offre de service devrait être disponible dans tous les domaines ou seulement certains domaines. Choisir Oui pour le rendre disponible à tous les domaines. Choisir No pour limiter la portée à un sous-domaine ; CloudStack va alors demander le nom du sous-domaine.
6. Cliquer sur Ajouter.

4.1.4 Régulation du réseau

La régulation du réseau est le processus de contrôle de l'accès au réseau et de l'utilisation de la bande passante selon certaines règles. CloudStack contrôle ce comportement des réseaux invités dans le cloud en utilisant un paramètre de vitesse du réseau. Ce paramètre est défini comme la vitesse de transfert par défaut des données en Mbps (Megabits par secondes) autorisée sur un réseau invité. Il défini les limites supérieures de l'utilisation du réseau. Si l'utilisation courante est inférieure aux limites hautes autorisées, alors l'accès est autorisé, sinon il sera refusé.

Vous pouvez réguler la bande passante du réseau soit pour contrôler l'utilisation au delà de certaines limites pour certains comptes, ou pour contrôler la congestion du réseau dans un grand environnement cloud. La vitesse du réseau de votre cloud peut être configuré selon ce qui suit :
— Offre réseau
— Offre de service
— Paramètre Global
Si le taux du réseau est fixé à NULL dans l'offre de service, la valeur fournie par le paramètre global vm.network.throttling.rate est appliquée. Si la valeur est fixée à NULL pour l'offre réseau, la valeur fournie par le paramètre global network.throttling.rate est pris en considération.

Pour les réseaux public par défaut, stockage et de gestion, la vitesse du réseau est fixé à 0. Cela implique que les réseaux public par défaut, stockage et de gestion auront une bande passante illimitée par défaut. Pour le réseau invité

par défaut, la vitesse du réseau est fixée à NULL. Dans ce cas, la vitesse du réseau est fixée par défaut à la valeur du paramètre global.

Le tableau suivant donne une vue d'ensemble de comment la vitesse du réseau est appliquée sur différents types de réseaux dans CloudStack.

Réseaux	La vitesse du réseau est fournie par
Réseau invité d'un Routeur Virtuel	Offre de réseau invité
Réseau public du Routeur Virtuel	Offre de réseau invité
Réseau de stockage d'une VM de Stockage Secondaire	Offre de réseau système
Réseau de gestion d'une VM de Stockage Secondaire	Offre de réseau système
Réseau de stockage d'une VM Console Proxy	Offre de réseau système
Réseau de gestion d'une VM Console Proxy	Offre de réseau système
Réseau de stockage du Routeur Virtuel	Offre de réseau système
Réseau de gestion du Routeur Virtuel	Offre de réseau système
Réseau public d'une VM de Stockage Secondaire	Offre de réseau système
Réseau public d'une VM Console Proxy	Offre de réseau système
Réseau par défaut d'une VM invitée	Offre de calcul
Réseaux additionnels pour une VM invitée	Offres de réseau correspondant

Une VM invitée doit avoir un réseau par défaut, et peu aussi avoir plusieurs réseaux additionnels. En fonction de nombreux paramètres, comme l'hôte ou le commutateur virtuel utilisé, vous pouvez observer une différence de vitesse du réseau dans votre cloud. Par example, sur un hôte VMware la vitesse réseau actuelle varie en fonction de l'endroit où elle est configurée (offre de calcul, offre réseau, ou les deux) ; le type de réseau (partagé ou isolé) ; et la direction du trafic (entrant ou sortant).

La vitesse réseau fixée pour une offre de réseau utilisée par un réseau particulier dans CloudStack est utilisé pour la stratégie de mise en forme du trafic pour un groupe de port, par exemple : groupe de port A, pour ce réseau : un sous-réseau particulier ou un VLAN sur le réseau actuel. Les routeurs virtuel pour ce réseau connecte au groupe de port A, et par défaut les instances dans ce réseau se connectent à ce groupe de port. Toutefois, si une instance est déployée avec une offre de service avec une vitesse du réseau de fixée, et si cette vitesse est utilisée pour la stratégie de contrôle du trafic d'un autre groupe de port pour le réseau, par exemple le groupe de port B, alors les instances utilisant l'offre de calcule sont connectée sur le groupe de port B, au lieu de se connecter au groupe de port A.

La politique de gestion du trafic sur les groupes de ports standards dans VMware s'applique seulement sur le trafic sortant et les effets sur le réseau dépendent du type de trafic réseau utilisé dans CloudStack. Dans les réseaux partagés, le trafic entrant est illimité pour CloudStack et le trafic sortant est limité à la vitesse qui s'applique au groupe de port utilisé par l'instance au besoin. Si l'offre de calcul a une vitesse de réseau configurée, cette vitesse s'applique au trafic sortant, sinon c'est la vitesse du réseau fixée par l'offre réseau qui s'applique. Pour les réseaux isolés, la vitesse du réseau fixée pour l'offre de réseau, si elle existe, est effectivement appliquée au trafic entrant. Cela est dû en grande partie à la vitesse du réseau fixée pour l'offre de service qui s'applique au trafic sortant depuis le routeur virtuel de cette instance. Le trafic sortant est limité par la vitesse qui s'applique au groupe de port utilisé par l'instance, similairement aux réseaux partagés.

Par exemple :

Vitesse de réseau pour l'offre réseau = 10 Mbps

Vitesse de réseau pour l'offre de calcul = 200 Mbps

Dans les réseaux partagés, le trafic entrant ne sera pas limité pour CloudStack, tandis que le trafic sortant sera limité à 200 Mbps. Dans un réseau isolé, le trafic entrant sera limité à 10 Mbps et le trafic sortant à 200 Mbps.

4.1.5 Changer l'Offre Système par Défaut pour les VMs Systèmes

Vous pouvez changer manuellement l'offre système pour une VM système particulière. En complément, en tant qu'administrateur CloudStack, vous pouvez aussi changer l'offre système par défaut utilisée par les VMs Système.

1. Créer une nouvelle offre système.
   Pour plus d'information, voir Créer une nouvelle offre de service système.
2. Sauvegarder la base de données :

```
mysqldump -u root -p cloud | bzip2 > cloud_backup.sql.bz2
```

3. Ouvrir un invite MySQL :

```
mysql -u cloud -p cloud
```

4. Lancer les requêtes suivantes dans la base de données du cloud.
   (a) Dans la table disk_offering, identifier l'offre par défaut originale et la nouvelle offre que vous voulez utiliser par défaut.
   Noter l'ID de la nouvelle offre.

```
select id,name,unique_name,type from disk_offering;
```

   (b) Pour l'offre par défaut originale, fixer la valeur de unique_name à NULL.

```
# update disk_offering set unique_name = NULL where id = 10;
```

   S'assurer que vous utilisez la valeur correcte pour l'ID.
   (c) Pour la nouvelle offre que vous voulez utiliser par défaut, fixer la valeur de unique_name comme ceci :
   Pour l'offre par défaut de la VM Console Proxy (CPVM), fixer unique_name à 'Cloud.com-ConsoleProxy'. Pour l'offre par défaut de la VM de Stockage Secondaire (SSVM), fixer unique_name à 'Cloud.com-SecondaryStorage'. Par exemple :

```
update disk_offering set unique_name = 'Cloud.com-ConsoleProxy' where id = 16;
```

5. Redémarrer le serveur de gestion de CloudStack. Le redémarrage est requis parce que les offres par défaut sont stockées en mémoire au démarrage.

```
service cloudstack-management restart
```

6. Détruire les CPVM et SSVM existantes et attendre qu'elles soient recréées. Les nouvelles CPVM et SSVM sont configurées avec les nouvelles offres.

CHAPITRE 5

Configurer le réseau pour les utilisateurs

5.1 Configurer le réseau pour les utilisateurs

5.1.1 Tour d'horizon de la configuration du réseau pour les Utilisateurs

Les personnes qui utilisent une infrastructure cloud ont une variété de besoins et préférences quand ils font appel aux services réseaux fournis par le cloud. En tant qu'administrateur CloudStack, vous pouvez faire les choses suivantes pour configurer le réseau pour vos utilisateurs :

- Configurer les réseaux physiques dans les zones
- Configurer plusieurs fournisseurs différents pour le même servicesur un seul réseau physique (par exemple à la fois des parefeus Cisco et Juniper)
- Regrouper différents types de services réseaux dans des offres réseaux, afin que les utilisateurs puissent choisir les services réseaux désirés pour n'importe quelle machine virtuelle.
- Ajouter de nouvelles offres réseaux au fil de l'eau afin que les utilisateurs finaux puissent évoluer vers de meilleurs classe de service sur leur réseau
- Fournir à un utilisateur plusieurs façons d'accéder à un réseau, par exemple via un projet auquel l'utilisateur est un membre

5.1.2 A propos des réseaux virtuels

Un réseau virtuel est une construction logique qui active plusieurs allocations sur un seul réseau physique. Dans CloudStack un réseau virtuel peut être partagé ou isolé.

Réseaux isolés

Un réseau isolé peut être accédé seulement par les machines virtuelles d'un seul compte. Les réseaux isolés ont les propriétés suivantes.

- Les ressources comme les VLAN sont alloués et recyclés dynamiquement
- Il y a une offre réseau pour le réseau entier
- L'offre réseau peut être amélioré ou rétrogradé mais pour le réseau entier

Pour plus d'information, voir "Configurer le Trafic Invité dans une Zone Avancée".

Réseaux partagés

Un réseau partagé peut être accédé par les machines virtuelles qui appartiennent à pleins de comptes différents. L'isolation du réseau dans les réseaux partagés est obtenue en utilisant des techniques comme les groupes de sécurité, qui sont supportés seulement dans les zones Basiques dans CloudStack 3.0.3 et versions ultérieures.

— Les Réseaux Partagés sont créés par l'administrateur
— Les Réseaux Partagés peuvent être désignés pour un domaine particulier
— Les ressources d'un Réseau Partagé comme les VLAN et le réseau physique qui lui est attaché sont désignés par l'administrateur
— Les Réseaux Partagés peuvent être isolés par les groupes de sécurité
— Le Réseau Public est un réseau partagé qui n'est pas affiché aux utilisateurs finaux.
— Le NAT source par zone n'est pas supporté dans un Réseau Partagé quand le fournisseur de service est un routeur virtuel. Toutefois, le NAT source par compte est supporté. Pour plus d'information, voir "Configurer un Réseau Partagé Invité".

L'allocation à chaud de Ressources de Réseau Virtuel

Quand vous définissez un nouveau réseau virtuel, tous vos paramètres pour ce réseau sont stockés dans CloudStack. Les ressources du réseau actuel sont activées seulement lorsque la première machine virtuelle dans le réseau démarre. Quand toutes les machines virtuelles ont quittés le réseau virtuel, les ressources du réseau sont récupérés et recyclée afin de pouvoir être à nouveau allouée. Cela aide à conserver les ressources réseaux.

5.1.3 Fournisseurs de service réseau

Note : Pour la liste la plus à jour des fournisseurs de services réseaux supportés, voir l'interface CloudStack ou appeler *listNetworkServiceProviders*.

Un fournisseur de service (aussi appelé un élément réseau) est un matériel ou une appliance virtuelle qui rend le service réseau possible ; par exemple, une appliance de parefeu peut être installé dans le cloud pour fournir un service de parefeu. Sur un seul réseau, plusieurs fournisseurs peuvent fournir le même service réseau. Par exemple, un service de parefeu peut être fourni par des périphériques Cisco ou Juniper dans le même réseau physique.

Vous pouvez avoir plusieurs instances du même fournisseur de service dans un réseau (comprendre plus d'un périphérique Juniper SRX).

Si différents fournisseurs sont configurés pour fournir le même service sur le réseau, les administrateurs peuvent créer des offres réseaux afin que les utilisateurs peuvent spécifier quel fournisseur de service réseau ils préfèrent (en même temps que les autres choix offerts dans les offres réseaux). Autrement, CloudStack va choisir quel fournisseur utiliser chaque fois que le service est appelé.

Fournisseurs de service réseau supportés

CloudStack est livré avec une liste interne des fournisseurs de services supportés, et vous pouvez choisir depuis cette liste lorsque vous créez une offre réseau.

	Routeur virtuel	Citrix NetScaler	Juniper SRX	F5 BigIP	Basé sur l'hôte (KVM/Xen)
Accès distant VPN	Oui	Non	Non	Non	Non
DNS/DHCP/Données utilisateur	Oui	Non	Non	Non	Non
Pare-feu	Oui	Non	Oui	Non	Non
Répartition de charge	Oui	Oui	Non	Oui	Non
Elastic IP	Non	Oui	Non	Non	Non
Elastic LB	Non	Oui	Non	Non	Non
Source NAT	Oui	Non	Oui	Non	Non
Static NAT	Oui	Oui	Oui	Non	Non
Port Forwarding	Oui	Non	Oui	Non	Non

5.1.4 Offres réseau

Note : Pour la liste la plus à jour des services réseaux supportés, voir l'interface CloudStack ou appeler *listNetworkServices*.

Une offre réseau est un nommage pour un ensemble de services réseau, comme :

- DHCP
- DNS
- Source NAT
- Static NAT
- Port Forwarding
- Répartition de charge
- Pare-feu
- VPN
- (Optionel) Nommer un des nombreux fournisseurs disponibles à utiliser pour un service donné, comme Juniper pour le parefeu.
- (Optionnel) Etiquette réseau pour spécifier quel réseau physique utiliser

Lorsqu'il crée une nouvelle VM, l'utilisateur choisi une des offres réseaux disponibles, et cela détermine quels services réseaux la VM peut utiliser.

L'administrateur CloudStack peut créer autant d'offres réseaux personnalisées en complément des offres réseaux par défaut fournies par CloudStack. En créant plusieurs offres de réseaux personnalisées, vous pouvez configurer votre cloud pour fournir différentes classes de service sur un seul réseau physique. Par exemple, alors que le câblage physique sous-jacent peut être le même pour les deux parties, la partie A peut seulement nécessiter une simple protection par pare-feu de son site, alors que la partie B peut lancer une ferme de serveurs web et nécessiter une solution de pare-feu évolutive, une solution de répartition de charge, et des réseaux alternatifs pour accéder au backend de base de données.

Note : Si vous créez des règles de répartition de charge lors de votre utilisation d'une offre de service réseau qui inclue un périphérique externe de répartition de charge comme un NetScaler, et plus tard changer l'offre de service réseau pour une qui utilise un routeur virtuel CloudStack, vous devrez créer une règle de pare-feu sur le routeur virtuel pour chacune de vos règles de répartition de charge afin qu'il puisse continuer de fonctionner.

Lorsque vous créez un nouveau réseau virtuel, l'administrateur CloudStack choisit quelle offre de réseau activer pour chaque réseau. Chaque réseau virtuel est associé avec une offre de service. Un routeur virtuel peut être amélioré ou rétrogradé en changeant son offre de réseau associé. Si vous faîtes cela, soyez certains de reprogrammer le réseau physique pour correspondre.

CloudStack a aussi des offres de réseaux internes pour les besoins des VMs systèmes CloudStack. Ces offres de réseaux ne sont pas visibles des utilisateurs mais peuvent être modifiées par les administrateurs.

Créer une nouvelle offre de service Réseau

Pour créer une offre de réseau :

1. Se connecter avec les droits d'administrateur à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur les Offres de Service.
3. Dans Sélectionner une offre, choisir une offre réseau.
4. Cliquer sur Ajouter une offre de réseau.
5. Dans la boîte de dialogue, faire les choix suivants :
   - **Nom** : N'importe quel nom souhaité pour l'offre de réseau.

— **Description** : Une description courte pour l'offre qui peut être affichée aux utilisateurs.
— **Vitesse Réseau** : Vitesse de transfert de données autorisée en MB par seconde.
— **Type d'invité**. Choisir si le réseau invité est isolé ou partagé.
Pour une description de ces termes, voir *"A propos des Réseaux Virtuels"*.
— **Persistent**. Indique si le réseau invité est persistent ou pas. Le réseau que vous pouvez provisionner sans avoir à déployer une VM sur celui-ci est appelé réseau persistant. Pour plus d'informations, voir "Réseaux Persistants".
— **Spécifier un VLAN**. (Réseaux invités isolés seulement) Indique si un VLAN peut être spécifié quand cette offre est utilisée. Si vous sélectionnez cette option et plus tard utilisez cette offre réseau lors de la création d'un VPC ou un réseau isolé, vous pourrez spécifier un ID de VLAN pour le réseau que vous créez.
— **VPC**. Cette option indique si le réseau invité est activable pour un Cloud Virtuel Privé. Un Cloud Virtuel Privé (VPC) est une partie de CloudStack privée, isolée. Un VPC peut avoir sa propre topologie réseau virtuelle qui ressemble a un réseau privé traditionnel. Pour plus d'informations sur les VPC, voir "A propos des Clouds Privés Virtuels".
— **Services supportés**. Sélectionner un ou plusieurs des services réseaux possibles. Pour certains services, vous devez aussi choisir le fournisseur de service ; par exemple, si vous sélectionnez un Répartiteur de Charge, vous pouvez choisir le routeur virtuel CloudStack ou n'importe quels autres répartiteurs qui ont été configurés dans la cloud. En fonction du service que vous avez choisi, des champs additionnels peuvent apparaître dans le reste de la boîte de dialogue.
En fonction du type de réseau invité sélectionné, vous pouvez voir les services supportés suivants :

Services supportés	Description	Isolé	Partagé
DHCP	Pour plus d'informations, voir "DNS et DHCP".	Supporté	Supporté
DNS	Pour plus d'informations, voir "DNS et DHCP".	Supporté	Supporté
Répartition de charge	Si vous choisissez Répartiteur de Charge, vous pouvez choisir le routeur virtuel CloudStack ou n'importe quel répartiteur de charge qui a été configuré dans le cloud.	Supporté	Supporté
Pare-feu	Pour plus d'informations, voir le Guide d'Administration.	Supporté	Supporté
Source NAT	Si vous sélectionnez Source NAT, vous pouvez choisir le routeur virtuel CloudStack ou n'importe quel autre fournisseur de Source NAT qui a été configuré dans le cloud.	Supporté	Supporté
Static NAT	Si vous sélectionnez NAT Statique, vous pouvez choisir le routeur virtuel CloudStack ou n'importe quel autre fournisseur de NAT Statique qui a été configuré dans le cloud.	Supporté	Supporté
Port Forwarding	Si vous sélectionnez Transmission de Port, vous pouvez choisir le routeur virtuel CloudStack ou n'importe quel fournisseur de Transmission de Port qui a été configuré dans le cloud.	Supporté	Non supporté
VPN	Pour plus d'informations, voir "Accès distant VPN".	Supporté	Non supporté
Donnée utilisateur	Pour plus d'informations, voir "Données et Méta-données utilisateur".	Non supporté	Supporté
ACL réseau	Pour plus d'informations, voir "Configurer les Listes de Contrôles d'Accès Réseau".	Supporté	Non supporté
Groupes de sécurité	Pour plus d'informations, voir "Ajouter un groupe de sécurité".	Non supporté	Supporté

— **Offre système**. Si le fournisseur de service pour n'importe lequel des services sélectionnés dans les Services Supportés est un routeur virtuel, le champ Offre Système apparaît. Choisir l'offre de service système que vous voulez que les routeurs virtuels utilisent dans ce réseau. Par exemple, si vous avez sélectionné Répartiteur de Charge dans les Services Supportés et sélectionné un routeur virtuel pour fournir la répartition de charge, le champ Offre Système apparaît afin que vous puissiez choisir entre l'offre de service système par défaut de CloudStack ou n'importe quelle offre de service système personnalisée qui a été définie par l'administrateur CloudStack.
Pour plus d'informations, voir "Offres de service système".
— **LB Isolation** : Spécifie quel type d'isolation par répartiteur de charge vous voulez pour le réseau : Partagé ou Dédié.
Dédié : Si vous sélectionnez une isolation par LB dédié, un périphérique répartiteur de charge dédié est assignée pour le réseau depuis la réserve de périphériques de répartition de charge dédiés provisionnés dans la zone. Si aucun périphérique de répartition de charge dédié n'est disponible dans la zone, la création du réseau échoue. Un périphérique dédié est un bon choix pour les réseaux à fort trafic qui font un usage complet des ressources du périphérique.
Partagé : Si vous sélectionnez une isolation par LB partagé, un périphérique de répartition de charge partagé est assigné pour le réseau depuis la réserve des périphériques de répartiteurs de charge partagés provisionnés dans la zone. Lors du provisionnement, CloudStack choisit le périphérique de répartition de charge partagé qui est utilisé par le plus petit nombre de comptes. Une fois que le périphérique a atteint le maximum de ses capacités, le périphérique ne sera plus attribué à de nouveaux comptes.
— **Mode** : Vous pouvez sélectionner soit le mode En ligne ou le mode Côte à Côte.
Mode en ligne : Supporté seulement par les pare-feu Juniper SRX et les périphériques de répartition de charge BigF5. Dans le mode en ligne, un périphérique parefeu est placé devant un périphérique de répartition de charge. Le parefeu agit comme une passerelle pour tout le trafic entrant qui redirige tout le trafic à répartir au répartiteur de charge derrière lui. Le répartiteur de charge dans ce cas n'aura pas laccès directement au réseau public.
Côte à côte : Dans le mode côte à côte, un périphérique de parefeu est déployé en parallèle du périphérique de répartition de charge. Le trafic vers l'adresse IP publique du répartiteur de charge n'est pas routé via le parefeu, et par conséquent il est exposé au réseau public.
— **IP publique associée** : Sélectionnez cette option si vous voulez assigner une adresse IP publique aux VMs déployées dans le réseau invité. Cette option est disponible seulement si
  — Le réseau invité est partagé.
  — Le NAT-age statique est activé.
  — Elastic IP est activé.
  Pour des informations sur Elastic IP, voir "A propos d'Elastic IP".
— **Capacité de routeur redondant** : disponible seulement quand le Routeur Virtuel est sélectionné comme fournisseur de Source NAT. Sélectionner cette option si vous voulez utiliser 2 routeurs virtuels dans le réseau pour des connexion ininterrompues : un opère comme routeur virtuel maître et l'autre comme secours. Le routeur virtuel maître reçoit les requêtes des VMs utilisateurs et leur envoi les réponses. Le routeur virtuel de secours est activé seulement quand le maître est indisponible. Après la panne, le secours devient le routeur virtuel maître. CloudStack déploie les routeurs sur des hôtes différents pour assurer la fiabilité si un des hôtes est indisponible.
— **Mode conservation** : Indique si le mode conservation est utilisé. Dans ce mode, les ressources réseaux sont allouée seulement lorsque la première machine virtuelle démarre dans le réseau. Quand le mode de conservation est arrêté, l'IP publique peut seulement être utilisée pour un seul périphérique. Par exemple, une IP publique utilisée pour une règle de transmission de port ne peut pas être utilisée pour définir d'autres services, comme le StaticNAT ou la répartition de charge. Quand le mode de conservation est activé, vous pouvez définir plus d'un service avec la même IP publique.

Note : Si le StaticNAT est activé, quelque soit le statut du mode conservé, aucune transmission de port ou règle de répartition de charge he peut être crée pour l'IP. Toutefois, vous pouvez ajouter les règles de pare-feu en utilisant la commande createFirewallRule.

— **Etiquettes** : Etiquette réseau pour spécifier quel réseau physique utiliser.

— **Politique de sortie par défaut** : Configurer la politique par défaut pour les règles sortantes par défaut. Les options sont Autoriser ou Refuser. La valeur par défaut est Autoriser si aucune règle sortante n'est spécifiée, ce qui indique que tout le trafic sortant est accepté lorsque le réseau invité est crée depuis cette offre.
Pour bloquer le trafic sortant pour un réseau invité, sélectionner Refuser. Dans ce cas, lorsque vous configurez des règles sortantes pour un réseau invité isolé, les règles sont ajoutées pour autoriser le trafic spécifié.

6. Cliquer sur Ajouter.

CHAPITRE 6

Travailler avec des machines virtuelles

6.1 Travailler avec les Machines Virtuelles

6.1.1 A propos du travail avec les Machines Virtuelles

CloudStack fournit aux administrateurs un contrôle complet du cycle de vie de toutes les VM invitées exécutées dans le cloud. CloudStack fournit différentes opérations de gestion des invités aux utilisateurs finaux et aux administrateurs. Les VMs peuvent être stoppées, démarrées, redémarrées et détruites.

Les VM invitées ont un nom et un groupe. Les noms des VM et les groupes sont opaques pour CloudStack et sont utiles aux utilisateurs finaux pour organiser leurs VM. Chaque VM peut avoir trois noms différents pour utiliser dans différents contextes. Seulement deux de ces noms sont contrôlés par l'utilisateur :

- Nom de l'instance - un ID unique et non modifiable qui est généré par CloudStack et ne peut pas être modifié par l'utilisateur. Ce nom est conforme aux exigences de la RFC 1123 de l'IETF.
- Nom affiché - le nom affiché dans l'interface web CloudStack. Peut être fixé par l'utilisateur. Prend par défaut le nom de l'instance.
- Nom - nom de machine que le serveur DHCP assigne à la VM. Peut être fixé par l'utilisateur. Prend par défaut le nom de l'instance.

Note : Vous pouvez ajouter le nom affiché d'une VM invitée à son nom interne. Pour plus d'informations, voir *"Ajouter un Nom d'Affichage au Nom Interne d'une VM invités."*.

Les VM invités peuvent être configuré pour être Hautement Disponible (HA). Une VM dont la HA est activée est supervisée par le système. Si le système détecte que la VM est à l'arrêt, il va tenter de redémarrer la VM, si possible sur un hôte différent. Pour plus d'information, voir Activer la HA sur les Machines Virtuelles.

Chaque nouvelle VM se voit attribué une adresse IP Publique. Quand la VM est démarrée, CloudStack crée automatiquement un NAT static entre cette adresse IP public et l'adresse IP privée de la VM.

If elastic IP is in use (with the NetScaler load balancer), the IP address initially allocated to the new VM is not marked as elastic. The user must replace the automatically configured IP with a specifically acquired elastic IP, and set up the static NAT mapping between this new IP and the guest VM's private IP. The VM's original IP address is then released and returned to the pool of available public IPs. Optionally, you can also decide not to allocate a public IP to a VM in an EIP-enabled Basic zone. For more information on Elastic IP, see "About Elastic IP".

CloudStack cannot distinguish a guest VM that was shut down by the user (such as with the "shutdown" command in Linux) from a VM that shut down unexpectedly. If an HA-enabled VM is shut down from inside the VM, CloudStack will restart it. To shut down an HA-enabled VM, you must go through the CloudStack UI or API.

6.1.2 Meilleurs pratiques pour les machines virtuels

For VMs to work as expected and provide excellent service, follow these guidelines.

Surveiller la capacité maximale de VM

The CloudStack administrator should monitor the total number of VM instances in each cluster, and disable allocation to the cluster if the total is approaching the maximum that the hypervisor can handle. Be sure to leave a safety margin to allow for the possibility of one or more hosts failing, which would increase the VM load on the other hosts as the VMs are automatically redeployed. Consult the documentation for your chosen hypervisor to find the maximum permitted number of VMs per host, then use CloudStack global configuration settings to set this as the default limit. Monitor the VM activity in each cluster at all times. Keep the total number of VMs below a safe level that allows for the occasional host failure. For example, if there are N hosts in the cluster, and you want to allow for one host in the cluster to be down at any given time, the total number of VM instances you can permit in the cluster is at most (N-1) * (per-host-limit). Once a cluster reaches this number of VMs, use the CloudStack UI to disable allocation of more VMs to the cluster.

Installez les outils et les pilotes requis

Be sure the following are installed on each VM :

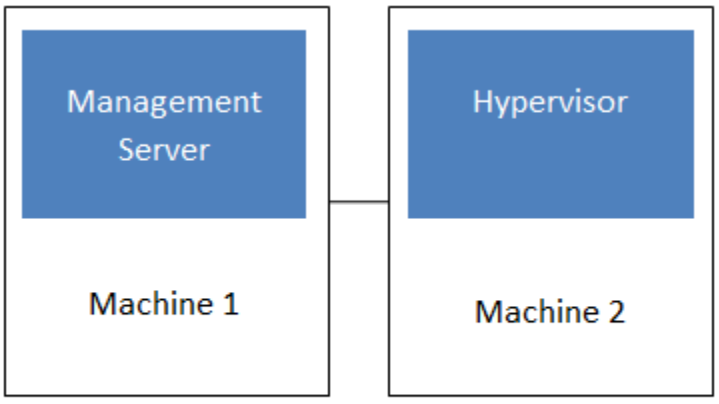
- For XenServer, install PV drivers and Xen tools on each VM. This will enable live migration and clean guest shutdown. Xen tools are required in order for dynamic CPU and RAM scaling to work.
- For vSphere, install VMware Tools on each VM. This will enable console view to work properly. VMware Tools are required in order for dynamic CPU and RAM scaling to work.

To be sure that Xen tools or VMware Tools is installed, use one of the following techniques :

- Create each VM from a template that already has the tools installed ; or,
- When registering a new template, the administrator or user can indicate whether tools are installed on the template. This can be done through the UI or using the updateTemplate API ; or,
- If a user deploys a virtual machine with a template that does not have Xen tools or VMware Tools, and later installs the tools on the VM, then the user can inform CloudStack using the updateVirtualMachine API. After installing the tools and updating the virtual machine, stop and start the VM.

6.1.3 Cycle de vie d'une VM

Les machines virtuelles peuvent se trouver dans les états suivants :



Simplified view of a basic deployment

Once a virtual machine is destroyed, it cannot be recovered. All the resources used by the virtual machine will be reclaimed by the system. This includes the virtual machine's IP address.

A stop will attempt to gracefully shut down the operating system, which typically involves terminating all the running applications. If the operation system cannot be stopped, it will be forcefully terminated. This has the same effect as pulling the power cord to a physical machine.

Un redémarrage est un arrêt suivi d'un démarrage.

CloudStack preserves the state of the virtual machine hard disk until the machine is destroyed.

A running virtual machine may fail because of hardware or network issues. A failed virtual machine is in the down state.

The system places the virtual machine into the down state if it does not receive the heartbeat from the hypervisor for three minutes.

The user can manually restart the virtual machine from the down state.

The system will start the virtual machine from the down state automatically if the virtual machine is marked as HA-enabled.

6.1.4 Creating VMs

Virtual machines are usually created from a template. Users can also create blank virtual machines. A blank virtual machine is a virtual machine without an OS template. Users can attach an ISO file and install the OS from the CD/DVD-ROM.

Note : You can create a VM without starting it. You can determine whether the VM needs to be started as part of the VM deployment. A request parameter, startVM, in the deployVm API provides this feature. For more information, see the Developer's Guide.

To create a VM from a template :

1. Log in to the CloudStack UI as an administrator or user.
2. In the left navigation bar, click Instances.
3. Cliquer sur Ajouter une instance.
4. Sélectionner une zone.
5. Select a template, then follow the steps in the wizard. For more information about how the templates came to be in this list, see *Working with Templates*.
6. Be sure that the hardware you have allows starting the selected service offering.
7. Click Submit and your VM will be created and started.

   Note : For security reason, the internal name of the VM is visible only to the root admin.

To create a VM from an ISO :

Note : (XenServer) Windows VMs running on XenServer require PV drivers, which may be provided in the template or added after the VM is created. The PV drivers are necessary for essential management functions such as mounting additional volumes and ISO images, live migration, and graceful shutdown.

---

1. Log in to the CloudStack UI as an administrator or user.
2. In the left navigation bar, click Instances.

3. Cliquer sur Ajouter une instance.
4. Sélectionner une zone.
5. Select ISO Boot, and follow the steps in the wizard.
6. Click Submit and your VM will be created and started.

6.1.5 Accéder aux VMs.

Tous les utilisateur peuvent accéder à leur propore machines virtuelles. L'administrateur peut accéder à toute les VMs qui fonctionnent dans le cloud.

To access a VM through the CloudStack UI :

1. Log in to the CloudStack UI as a user or admin.
2. Cliquez sur Instances, puis choisissez le nom de la VM en cours d'éxécution.
3. Click the View Console button  .

Pour accéder à une VM directement à travers le réseau :

1. The VM must have some port open to incoming traffic. For example, in a basic zone, a new VM might be assigned to a security group which allows incoming traffic. This depends on what security group you picked when creating the VM. In other cases, you can open a port by setting up a port forwarding policy. See "IP Forwarding and Firewalling".
2. If a port is open but you can not access the VM using ssh, it's possible that ssh is not already enabled on the VM. This will depend on whether ssh is enabled in the template you picked when creating the VM. Access the VM through the CloudStack UI and enable ssh on the machine using the commands for the VM's operating system.
3. If the network has an external firewall device, you will need to create a firewall rule to allow access. See "IP Forwarding and Firewalling".

6.1.6 Stopping and Starting VMs

Once a VM instance is created, you can stop, restart, or delete it as needed. In the CloudStack UI, click Instances, select the VM, and use the Stop, Start, Reboot, and Destroy buttons.

6.1.7 Assigning VMs to Hosts

At any point in time, each virtual machine instance is running on a single host. How does CloudStack determine which host to place a VM on ? There are several ways :

— Automatic default host allocation. CloudStack can automatically pick the most appropriate host to run each virtual machine.
— Instance type preferences. CloudStack administrators can specify that certain hosts should have a preference for particular types of guest instances. For example, an administrator could state that a host should have a preference to run Windows guests. The default host allocator will attempt to place guests of that OS type on such hosts first. If no such host is available, the allocator will place the instance wherever there is sufficient physical capacity.
— Vertical and horizontal allocation. Vertical allocation consumes all the resources of a given host before allocating any guests on a second host. This reduces power consumption in the cloud. Horizontal allocation places a guest on each host in a round-robin fashion. This may yield better performance to the guests in some cases.
— End user preferences. Users can not control exactly which host will run a given VM instance, but they can specify a zone for the VM. CloudStack is then restricted to allocating the VM only to one of the hosts in that zone.

— Host tags. The administrator can assign tags to hosts. These tags can be used to specify which host a VM should use. The CloudStack administrator decides whether to define host tags, then create a service offering using those tags and offer it to the user.
— Affinity groups. By defining affinity groups and assigning VMs to them, the user or administrator can influence (but not dictate) which VMs should run on separate hosts. This feature is to let users specify that certain VMs won't be on the same host.
— CloudStack also provides a pluggable interface for adding new allocators. These custom allocators can provide any policy the administrator desires.

Affinity Groups

By defining affinity groups and assigning VMs to them, the user or administrator can influence (but not dictate) which VMs should run on separate hosts. This feature is to let users specify that VMs with the same "host anti-affinity" type won't be on the same host. This serves to increase fault tolerance. If a host fails, another VM offering the same service (for example, hosting the user's website) is still up and running on another host.

The scope of an affinity group is per user account.

Creating a New Affinity Group

To add an affinity group :

1. Log in to the CloudStack UI as an administrator or user.
2. In the left navigation bar, click Affinity Groups.
3. Click Add affinity group. In the dialog box, fill in the following fields :
   — Name. Give the group a name.
   — Description. Any desired text to tell more about the purpose of the group.
   — Type. The only supported type shipped with CloudStack is Host Anti-Affinity. This indicates that the VMs in this group should avoid being placed on the same host with each other. If you see other types in this list, it means that your installation of CloudStack has been extended with customized affinity group plugins.

Assign a New VM to an Affinity Group

To assign a new VM to an affinity group :

— Create the VM as usual, as described in "Creating VMs". In the Add Instance wizard, there is a new Affinity tab where you can select the affinity group.

Change Affinity Group for an Existing VM

To assign an existing VM to an affinity group :

1. Log in to the CloudStack UI as an administrator or user.
2. In the left navigation bar, click Instances.
3. Click the name of the VM you want to work with.
4. Stop the VM by clicking the Stop button.
5. Click the Change Affinity button. 

View Members of an Affinity Group

To see which VMs are currently assigned to a particular affinity group :

1. In the left navigation bar, click Affinity Groups.
2. Click the name of the group you are interested in.
3. Click View Instances. The members of the group are listed.
   From here, you can click the name of any VM in the list to access all its details and controls.

Delete an Affinity Group

To delete an affinity group :

1. In the left navigation bar, click Affinity Groups.
2. Click the name of the group you are interested in.
3. Click Delete.
   Any VM that is a member of the affinity group will be disassociated from the group. The former group members will continue to run normally on the current hosts, but if the VM is restarted, it will no longer follow the host allocation rules from its former affinity group.

6.1.8 Virtual Machine Snapshots

(Supported on VMware and XenServer)

In addition to the existing CloudStack ability to snapshot individual VM volumes, you can take a VM snapshot to preserve all the VM's data volumes as well as (optionally) its CPU/memory state. This is useful for quick restore of a VM. For example, you can snapshot a VM, then make changes such as software upgrades. If anything goes wrong, simply restore the VM to its previous state using the previously saved VM snapshot.

The snapshot is created using the hypervisor's native snapshot facility. The VM snapshot includes not only the data volumes, but optionally also whether the VM is running or turned off (CPU state) and the memory contents. The snapshot is stored in CloudStack's primary storage.

VM snapshots can have a parent/child relationship. Each successive snapshot of the same VM is the child of the snapshot that came before it. Each time you take an additional snapshot of the same VM, it saves only the differences between the current state of the VM and the state stored in the most recent previous snapshot. The previous snapshot becomes a parent, and the new snapshot is its child. It is possible to create a long chain of these parent/child snapshots, which amount to a "redo" record leading from the current state of the VM back to the original.

If you need more information about VM snapshots on VMware, check out the VMware documentation and the VMware Knowledge Base, especially Understanding virtual machine snapshots.

Limitations on VM Snapshots

— If a VM has some stored snapshots, you can't attach new volume to the VM or delete any existing volumes. If you change the volumes on the VM, it would become impossible to restore the VM snapshot which was created with the previous volume structure. If you want to attach a volume to such a VM, first delete its snapshots.
— VM snapshots which include both data volumes and memory can't be kept if you change the VM's service offering. Any existing VM snapshots of this type will be discarded.
— You can't make a VM snapshot at the same time as you are taking a volume snapshot.
— You should use only CloudStack to create VM snapshots on hosts managed by CloudStack. Any snapshots that you make directly on the hypervisor will not be tracked in CloudStack.

Configuring VM Snapshots

The cloud administrator can use global configuration variables to control the behavior of VM snapshots. To set these variables, go through the Global Settings area of the CloudStack UI.

Configuration Setting Name

Description

vmsnapshots.max

The maximum number of VM snapshots that can be saved for any given virtual machine in the cloud. The total possible number of VM snapshots in the cloud is (number of VMs) * vmsnapshots.max. If the number of snapshots for any VM ever hits the maximum, the older ones are removed by the snapshot expunge job.

vmsnapshot.create.wait

Number of seconds to wait for a snapshot job to succeed before declaring failure and issuing an error.

Using VM Snapshots

To create a VM snapshot using the CloudStack UI :

1. Log in to the CloudStack UI as a user or administrator.
2. Click Instances.
3. Click the name of the VM you want to snapshot.
4. Click the Take VM Snapshot button. 

   Note : If a snapshot is already in progress, then clicking this button will have no effect.

5. Provide a name and description. These will be displayed in the VM Snapshots list.
6. (For running VMs only) If you want to include the VM's memory in the snapshot, click the Memory checkbox. This saves the CPU and memory state of the virtual machine. If you don't check this box, then only the current state of the VM disk is saved. Checking this box makes the snapshot take longer.
7. Quiesce VM : check this box if you want to quiesce the file system on the VM before taking the snapshot. Not supported on XenServer when used with CloudStack-provided primary storage.

   When this option is used with CloudStack-provided primary storage, the quiesce operation is performed by the underlying hypervisor (VMware is supported). When used with another primary storage vendor's plugin, the quiesce operation is provided according to the vendor's implementation.
8. Cliquez sur OK.

To delete a snapshot or restore a VM to the state saved in a particular snapshot :

1. Navigate to the VM as described in the earlier steps.
2. Click View VM Snapshots.
3. In the list of snapshots, click the name of the snapshot you want to work with.
4. Depending on what you want to do :

   To delete the snapshot, click the Delete button. 

   To revert to the snapshot, click the Revert button. 

Note : VM snapshots are deleted automatically when a VM is destroyed. You don't have to manually delete the snapshots in this case.

6.1.9 Changing the VM Name, OS, or Group

After a VM is created, you can modify the display name, operating system, and the group it belongs to.

To access a VM through the CloudStack UI :

1. Log in to the CloudStack UI as a user or admin.
2. Sur la gauche, cliquez sur Instances
3. Select the VM that you want to modify.
4. Click the Stop button to stop the VM. 
5. Click Edit. 
6. Make the desired changes to the following :
7. **Display name** : Enter a new display name if you want to change the name of the VM.
8. **OS Type** : Select the desired operating system.
9. **Group** : Enter the group name for the VM.
10. Click Apply.

6.1.10 Appending a Display Name to the Guest VM's Internal Name

Every guest VM has an internal name. The host uses the internal name to identify the guest VMs. CloudStack gives you an option to provide a guest VM with a display name. You can set this display name as the internal name so that the vCenter can use it to identify the guest VM. A new global parameter, vm.instancename.flag, has now been added to achieve this functionality.

The default format of the internal name is i-<user_id>-<vm_id>-<instance.name>, where instance.name is a global parameter. However, If vm.instancename.flag is set to true, and if a display name is provided during the creation of a guest VM, the display name is appended to the internal name of the guest VM on the host. This makes the internal name format as i-<user_id>-<vm_id>-<displayName>. The default value of vm.instancename.flag is set to false. This feature is intended to make the correlation between instance names and internal names easier in large data center deployments.

The following table explains how a VM name is displayed in different scenarios.

User-Provided Display Name	vm.instancename.flag	Hostname on the VM	Name on vCenter	Internal Name
Oui	True	Display name	i-<user_id>-<vm_id>-displayName	i-<user_id>-<vm_id>-displayName
Non	True	UUID	i-<user_id>-<vm_id>-<instance.name>	i-<user_id>-<vm_id>-<instance.name>
Oui	False	Display name	i-<user_id>-<vm_id>-<instance.name>	i-<user_id>-<vm_id>-<instance.name>
Non	False	UUID	i-<user_id>-<vm_id>-<instance.name>	i-<user_id>-<vm_id>-<instance.name>

6.1.11 Changing the Service Offering for a VM

To upgrade or downgrade the level of compute resources available to a virtual machine, you can change the VM's compute offering.

1. Log in to the CloudStack UI as a user or admin.
2. Sur la gauche, cliquez sur Instances

3. Choose the VM that you want to work with.
4. (Skip this step if you have enabled dynamic VM scaling ; see *CPU and Memory Scaling for Running VMs*.)

   Click the Stop button to stop the VM. 
5. Click the Change Service button. 

   The Change service dialog box is displayed.
6. Select the offering you want to apply to the selected VM.
7. Cliquez sur OK.

CPU and Memory Scaling for Running VMs

(Supported on VMware and XenServer)

It is not always possible to accurately predict the CPU and RAM requirements when you first deploy a VM. You might need to increase these resources at any time during the life of a VM. You can dynamically modify CPU and RAM levels to scale up these resources for a running VM without incurring any downtime.

Dynamic CPU and RAM scaling can be used in the following cases :

— User VMs on hosts running VMware and XenServer.
— System VMs on VMware.
— VMware Tools or XenServer Tools must be installed on the virtual machine.
— The new requested CPU and RAM values must be within the constraints allowed by the hypervisor and the VM operating system.
— New VMs that are created after the installation of CloudStack 4.2 can use the dynamic scaling feature. If you are upgrading from a previous version of CloudStack, your existing VMs created with previous versions will not have the dynamic scaling capability unless you update them using the following procedure.

Updating Existing VMs

If you are upgrading from a previous version of CloudStack, and you want your existing VMs created with previous versions to have the dynamic scaling capability, update the VMs using the following steps :

1. Make sure the zone-level setting enable.dynamic.scale.vm is set to true. In the left navigation bar of the CloudStack UI, click Infrastructure, then click Zones, click the zone you want, and click the Settings tab.
2. Install Xen tools (for XenServer hosts) or VMware Tools (for VMware hosts) on each VM if they are not already installed.
3. Stop the VM.
4. Click the Edit button.
5. Click the Dynamically Scalable checkbox.
6. Click Apply.
7. Restart the VM.

Configuring Dynamic CPU and RAM Scaling

To configure this feature, use the following new global configuration variables :

— enable.dynamic.scale.vm : Set to True to enable the feature. By default, the feature is turned off.
— scale.retry : How many times to attempt the scaling operation. Default = 2.

How to Dynamically Scale CPU and RAM

To modify the CPU and/or RAM capacity of a virtual machine, you need to change the compute offering of the VM to a new compute offering that has the desired CPU and RAM values. You can use the same steps described above in *"Changing the Service Offering for a VM"*, but skip the step where you stop the virtual machine. Of course, you might have to create a new compute offering first.

When you submit a dynamic scaling request, the resources will be scaled up on the current host if possible. If the host does not have enough resources, the VM will be live migrated to another host in the same cluster. If there is no host in the cluster that can fulfill the requested level of CPU and RAM, the scaling operation will fail. The VM will continue to run as it was before.

Limitations

- You can not do dynamic scaling for system VMs on XenServer.
- CloudStack will not check to be sure that the new CPU and RAM levels are compatible with the OS running on the VM.
- When scaling memory or CPU for a Linux VM on VMware, you might need to run scripts in addition to the other steps mentioned above. For more information, see Hot adding memory in Linux (1012764) in the VMware Knowledge Base.
- (VMware) If resources are not available on the current host, scaling up will fail on VMware because of a known issue where CloudStack and vCenter calculate the available capacity differently. For more information, see https://issues.apache.org/jira/browse/CLOUDSTACK-1809.
- On VMs running Linux 64-bit and Windows 7 32-bit operating systems, if the VM is initially assigned a RAM of less than 3 GB, it can be dynamically scaled up to 3 GB, but not more. This is due to a known issue with these operating systems, which will freeze if an attempt is made to dynamically scale from less than 3 GB to more than 3 GB.

6.1.12 Resetting the Virtual Machine Root Volume on Reboot

For secure environments, and to ensure that VM state is not persisted across reboots, you can reset the root disk. For more information, see "Reset VM to New Root Disk on Reboot".

6.1.13 Moving VMs Between Hosts (Manual Live Migration)

The CloudStack administrator can move a running VM from one host to another without interrupting service to users or going into maintenance mode. This is called manual live migration, and can be done under the following conditions :

- The root administrator is logged in. Domain admins and users can not perform manual live migration of VMs.
- The VM is running. Stopped VMs can not be live migrated.
- The destination host must have enough available capacity. If not, the VM will remain in the "migrating" state until memory becomes available.
- (KVM) The VM must not be using local disk storage. (On XenServer and VMware, VM live migration with local disk is enabled by CloudStack support for XenMotion and vMotion.)
- (KVM) The destination host must be in the same cluster as the original host. (On XenServer and VMware, VM live migration from one cluster to another is enabled by CloudStack support for XenMotion and vMotion.)

To manually live migrate a virtual machine

1. Log in to the CloudStack UI as a user or admin.
2. Sur la gauche, cliquez sur Instances
3. Choose the VM that you want to migrate.
4. Click the Migrate Instance button. 

5. From the list of suitable hosts, choose the one to which you want to move the VM.

   Note : If the VM's storage has to be migrated along with the VM, this will be noted in the host list. CloudStack will take care of the storage migration for you.

6. Cliquez sur OK.

6.1.14 Suppression des VM

Les utilisateurs peuvent supprimer leurs machines virtuelles. Une VM en cours d'utilisation sera arrêtée brutalement avant suppression. Les administrateurs peuvent supprimer n'importe quelle VM.

Pour supprimer une machine virtuelle :

1. Log in to the CloudStack UI as a user or admin.
2. Sur la gauche, cliquez sur Instances
3. Choisissez la VM que vous voulez supprimer.
4. Click the Destroy Instance button. 

6.1.15 Working with ISOs

CloudStack supports ISOs and their attachment to guest VMs. An ISO is a read-only file that has an ISO/CD-ROM style file system. Users can upload their own ISOs and mount them on their guest VMs.

ISOs are uploaded based on a URL. HTTP is the supported protocol. Once the ISO is available via HTTP specify an upload URL such as http://my.web.server/filename.iso.

ISOs may be public or private, like templates.ISOs are not hypervisor-specific. That is, a guest on vSphere can mount the exact same image that a guest on KVM can mount.

ISO images may be stored in the system and made available with a privacy level similar to templates. ISO images are classified as either bootable or not bootable. A bootable ISO image is one that contains an OS image. CloudStack allows a user to boot a guest VM off of an ISO image. Users can also attach ISO images to guest VMs. For example, this enables installing PV drivers into Windows. ISO images are not hypervisor-specific.

Adding an ISO

To make additional operating system or other software available for use with guest VMs, you can add an ISO. The ISO is typically thought of as an operating system image, but you can also add ISOs for other types of software, such as desktop applications that you want to be installed as part of a template.

1. Log in to the CloudStack UI as an administrator or end user.
2. In the left navigation bar, click Templates.
3. In Select View, choose ISOs.
4. Click Add ISO.
5. In the Add ISO screen, provide the following :
   — **Name** : Short name for the ISO image. For example, CentOS 6.2 64-bit.
   — **Description** : Display test for the ISO image. For example, CentOS 6.2 64-bit.
   — **URL** : The URL that hosts the ISO image. The Management Server must be able to access this location via HTTP. If needed you can place the ISO image directly on the Management Server
   — **Zone** : Choose the zone where you want the ISO to be available, or All Zones to make it available throughout CloudStack.

- **Bootable** : Whether or not a guest could boot off this ISO image. For example, a CentOS ISO is bootable, a Microsoft Office ISO is not bootable.
- **OS Type** : This helps CloudStack and the hypervisor perform certain operations and make assumptions that improve the performance of the guest. Select one of the following.
  - If the operating system of your desired ISO image is listed, choose it.
  - If the OS Type of the ISO is not listed or if the ISO is not bootable, choose Other.
  - (XenServer only) If you want to boot from this ISO in PV mode, choose Other PV (32-bit) or Other PV (64-bit)
  - (KVM only) If you choose an OS that is PV-enabled, the VMs created from this ISO will have a SCSI (virtio) root disk. If the OS is not PV-enabled, the VMs will have an IDE root disk. The PV-enabled types are :
    - Fedora 13
    - Fedora 12
    - Fedora 11
    - Fedora 10
    - Fedora 9
    - Other PV
    - Debian GNU/Linux
    - CentOS 5.3
    - CentOS 5.4
    - CentOS 5.5
    - Red Hat Enterprise Linux 5.3
    - Red Hat Enterprise Linux 5.4
    - Red Hat Enterprise Linux 5.5
    - Red Hat Enterprise Linux 6

  Note : It is not recommended to choose an older version of the OS than the version in the image. For example, choosing CentOS 5.4 to support a CentOS 6.2 image will usually not work. In these cases, choose Other.

- **Extractable** : Choose Yes if the ISO should be available for extraction.
- **Public** : Choose Yes if this ISO should be available to other users.
- **Featured** : Choose Yes if you would like this ISO to be more prominent for users to select. The ISO will appear in the Featured ISOs list. Only an administrator can make an ISO Featured.

6. Cliquez sur OK.

   The Management Server will download the ISO. Depending on the size of the ISO, this may take a long time. The ISO status column will display Ready once it has been successfully downloaded into secondary storage. Clicking Refresh updates the download percentage.

7. **Important** : Wait for the ISO to finish downloading. If you move on to the next task and try to use the ISO right away, it will appear to fail. The entire ISO must be available before CloudStack can work with it.

Attacher une ISO à une VM

1. Sur la gauche, cliquez sur Instances
2. Choisissez la machine virtuelle avec laquelle vous souhaitez travailler.
3. Click the Attach ISO button. 
4. Dans la boîte de dialogue Attacher une ISO, sélectionnez l'ISO voulue.
5. Cliquez sur OK.

Changing a VM's Base Image

Every VM is created from a base image, which is a template or ISO which has been created and stored in CloudStack. Both cloud administrators and end users can create and modify templates, ISOs, and VMs.

In CloudStack, you can change an existing VM's base image from one template to another, or from one ISO to another. (You can not change from an ISO to a template, or from a template to an ISO).

For example, suppose there is a template based on a particular operating system, and the OS vendor releases a software patch. The administrator or user naturally wants to apply the patch and then make sure existing VMs start using it. Whether a software update is involved or not, it's also possible to simply switch a VM from its current template to any other desired template.

To change a VM's base image, call the restoreVirtualMachine API command and pass in the virtual machine ID and a new template ID. The template ID parameter may refer to either a template or an ISO, depending on which type of base image the VM was already using (it must match the previous type of image). When this call occurs, the VM's root disk is first destroyed, then a new root disk is created from the source designated in the template ID parameter. The new root disk is attached to the VM, and now the VM is based on the new template.

You can also omit the template ID parameter from the restoreVirtualMachine call. In this case, the VM's root disk is destroyed and recreated, but from the same template or ISO that was already in use by the VM.

6.1.16 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.

Creating an Instance Template that Supports SSH Keys

Create an 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 Script to the instance you have created.

```
wget http://downloads.sourceforge.net/project/cloudstack/SSH%20Key%20Gen%20Script/cloud-set-gue
```

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.

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 :

Note : 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&
```

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
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.

Creating an Instance

After you save the SSH keypair file, you must create an instance by using the template that you created at *Section 5.2.1, " Creating an Instance Template that Supports SSH Keys"*. Ensure that you use the same SSH key name that you created at *Section 5.2.2, "Creating the SSH Keypair"*.

Note : 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\&serviceOfferi
```

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

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 example, 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.

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.

6.1.17 Données utilisateur et méta-données

CloudStack fournit un accès à une API pour attacher plus de 2KB de données après encodage en base64 à une VM déployée. En utilisant une requête POST HTTP (via POST body), vous pouvez envoyer jusqu'à 32K de données après encodage en base64. Les VM déployées ont ainsi accès aux méta-données d'instance via le routeur virtuel.

Créer une machine virtuelle via l'API : deployVirtualMachine en utilisant le paramètre `userdata=` pour inclure les données utilisateurs formatées en base64.

Accéder aux données utilisateur depuis la VM. Une ois que l'adresse IP du routeur virtuel est connue, utiliser les étapes suivantes pour récupérer les méta-données :

1. Lancer la commande suivante pour trouver le routeur virtuel.

```
# cat /var/lib/dhclient/dhclient-eth0.leases | grep dhcp-server-identifier | tail -1
```

2. Accéder aux données utilisateurs en lancer la commande suivante utilisant le résultat de la commande précédente

```
# curl http://10.1.1.1/latest/user-data
```

Les méta-données peuvent être accédées de manière similaire, utilisant une URL de la forme `http://10.1.1.1/latest/meta-data/{metadata type}`. (Pour des raisons de compatibilités ascendantes, les anciennes URL `http://10.1.1.1/latest/{metadata type}` sont aussi supportées.) Pour le type de méta-données, utiliser au choix :

— `service-offering`. Une description de l'offre de service des VM.
— `availability-zone`. Le nom de la Zone
— `local-ipv4`. L'adresse IP invitée de la VM
— `local-hostname`. Le nom d'hôte de la VM
— `public-ipv4`. La première IP publique pour le routeur. (E.g. la première IP d'eth2)
— `public-hostname`. Identique à public-ipv4
— `instance-id`. Le nom d'instance de la VM

Utiliser Cloud-Init

Cloud-Init peut être utiliser pour accéder aux données utilisateurs depuis les machines virtuelles. Cloud-init peut être installé dans les modèles et néssite aussi les scripts CloudStack password et sshkey (adding-password-management-to-templates et utiliser les clefs ssh). La gestion du mot de passe utilisateur et l'API `resetSSHKeyForVirtualMachine` ne sont pas encore supportés par cloud-init.

1. Installer le paquet cloud-init dans le modèle :

```
# yum install cloud-init
  or
$ sudo apt-get install cloud-init
```

2. Créer un fichier de configuration de source de données : `/etc/cloud/cloud.cfg.d/99_cloudstack.cfg`

```
datasource:
  CloudStack: {}
  None: {}
datasource_list:
  - CloudStack
```

Exemple de donnée utilisateur

Cet exemple utilise cloud-init pour mettre à jour le système d'exploitation d'une VM nouvellement crée :

```
#cloud-config

# Upgrade the instance on first boot
# (ie run apt-get upgrade)
#
# Default: false
# Aliases: apt_upgrade
package_upgrade: true
```

formatée en base64 :

```
I2Nsb3VkLWNvbmZpZw0KDQojIFVwZ3JhZGUgdGhlIGluc3RhbmNlIG9uIGZpcnN0IGJvb3QNCiMgKGllIHJ1biBhcHQtZ2V0IHVwZ
```

Se référer à la documentation Cloud-Init CloudStack datasource pour les dernières possibilitées. Cloud-Init et source de données Cloud-Init CloudStack ne sont pas supportées par la communauté Apache CloudStack.

6.1.18 Assigning GPU/vGPU to Guest VMs

CloudStack can deploy guest VMs with Graphics Processing Unit (GPU) or Virtual Graphics Processing Unit (vGPU) capabilities on XenServer hosts. At the time of VM deployment or at a later stage, you can assign a physical GPU (known as GPU-passthrough) or a portion of a physical GPU card (vGPU) to a guest VM by changing the Service Offering. With this capability, the VMs running on CloudStack meet the intensive graphical processing requirement by means of the high computation power of GPU/vGPU, and CloudStack users can run multimedia rich applications, such as Auto-CAD, that they otherwise enjoy at their desk on a virtualized environment. CloudStack leverages the XenServer support for NVIDIA GRID Kepler 1 and 2 series to run GPU/vGPU enabled VMs. NVIDIA GRID cards allows sharing a single GPU cards among multiple VMs by creating vGPUs for each VM. With vGPU technology, the graphics commands from each VM are passed directly to the underlying dedicated GPU, without the intervention of the hypervisor. This allows the GPU hardware to be time-sliced and shared across multiple VMs. XenServer hosts use the GPU cards in following ways :

GPU passthrough : GPU passthrough represents a physical GPU which can be directly assigned to a VM. GPU passthrough can be used on a hypervisor alongside GRID vGPU, with some restrictions : A GRID physical GPU can either host GRID vGPUs or be used as passthrough, but not both at the same time.

GRID vGPU : GRID vGPU enables multiple VMs to share a single physical GPU. The VMs run an NVIDIA driver stack and get direct access to the GPU. GRID physical GPUs are capable of supporting multiple virtual GPU devices (vGPUs) that can be assigned directly to guest VMs. Guest VMs use GRID virtual GPUs in the same manner as a physical GPU that has been passed through by the hypervisor : an NVIDIA driver loaded in the guest VM provides direct access to the GPU for performance-critical fast paths, and a paravirtualized interface to the GRID Virtual GPU Manager, which is used for nonperformant management operations. NVIDIA GRID Virtual GPU Manager for XenServer runs in dom0. CloudStack provides you with the following capabilities :

- Adding XenServer hosts with GPU/vGPU capability provisioned by the administrator.
- Creating a Compute Offering with GPU/vGPU capability.
- Deploying a VM with GPU/vGPU capability.
- Destroying a VM with GPU/vGPU capability.
- Allowing an user to add GPU/vGPU support to a VM without GPU/vGPU support by changing the Service Offering and vice-versa.
- Migrating VMs (cold migration) with GPU/vGPU capability.
- Managing GPU cards capacity.
- Querying hosts to obtain information about the GPU cards, supported vGPU types in case of GRID cards, and capacity of the cards.

Prerequisites and System Requirements

Before proceeding, ensure that you have these prerequisites :

- The vGPU-enabled XenServer 6.2 and later versions. For more information, see Citrix 3D Graphics Pack.
- GPU/vPGU functionality is supported for following HVM guest operating systems : For more information, see Citrix 3D Graphics Pack.
- Windows 7 (x86 and x64)
- Windows Server 2008 R2
- Windows Server 2012
- Windows 8 (x86 and x64)
- Windows 8.1 (“Blue”) (x86 and x64)
- Windows Server 2012 R2 (server equivalent of “Blue”)
- CloudStack does not restrict the deployment of GPU-enabled VMs with guest OS types that are not supported by XenServer for GPU/vGPU functionality. The deployment would be successful and a GPU/vGPU will also get allocated for VMs ; however, due to missing guest OS drivers, VM would not be able to leverage GPU resources. Therefore, it is recommended to use GPU-enabled service offering only with supported guest OS.
- NVIDIA GRID K1 (16 GiB video RAM) AND K2 (8 GiB of video RAM) cards supports homogeneous virtual GPUs, implies that at any given time, the vGPUs resident on a single physical GPU must be all of the same type. However, this restriction doesn’t extend across physical GPUs on the same card. Each physical GPU on a K1 or K2 may host different types of virtual GPU at the same time. For example, a GRID K2 card has two physical GPUs, and supports four types of virtual GPU ; GRID K200, GRID K220Q, GRID K240Q, AND GRID K260Q.
- NVIDIA driver must be installed to enable vGPU operation as for a physical NVIDIA GPU.
- XenServer tools are installed in the VM to get maximum performance on XenServer, regardless of type of vGPU you are using. Without the optimized networking and storage drivers that the XenServer tools provide, remote graphics applications running on GRID vGPU will not deliver maximum performance.
- To deliver high frames from multiple heads on vGPU, install XenDesktop with HDX 3D Pro remote graphics.

Before continuing with configuration, consider the following :

- Deploying VMs GPU/vGPU capability is not supported if hosts are not available with enough GPU capacity.
- A Service Offering cannot be created with the GPU values that are not supported by CloudStack UI. However, you can make an API call to achieve this.

— Dynamic scaling is not supported. However, you can choose to deploy a VM without GPU support, and at a later point, you can change the system offering to upgrade to the one with vGPU. You can achieve this by offline upgrade : stop the VM, upgrade the Service Offering to the one with vGPU, then start the VM.
— Live migration of GPU/vGPU enabled VM is not supported.
— Limiting GPU resources per Account/Domain is not supported.
— Disabling GPU at Cluster level is not supported.
— Notification thresholds for GPU resource is not supported.

Supported GPU Devices

Device	Type
GPU	— Group of NVIDIA Corporation GK107GL [GRID K1] GPUs — Group of NVIDIA Corporation GK104GL [GRID K2] GPUs — Any other GPU Group
vGPU	— GRID K100 — GRID K120Q — GRID K140Q — GRID K200 — GRID K220Q — GRID K240Q — GRID K260Q

GPU/vGPU Assignment Workflow

CloudStack follows the below sequence of operations to provide GPU/vGPU support for VMs :

1. Ensure that XenServer host is ready with GPU installed and configured. For more information, see Citrix 3D Graphics Pack.
2. Add the host to CloudStack. CloudStack checks if the host is GPU-enabled or not. CloudStack queries the host and detect if it's GPU enabled.
3. Create a compute offering with GPU/vGPU support : For more information, see *Creating a New Compute Offering*..
4. Continue with any of the following operations :
   — Deploy a VM.
   Deploy a VM with GPU/vGPU support by selecting appropriate Service Offering. CloudStack decide which host to choose for VM deployment based on following criteria :
   — Host has GPU cards in it. In case of vGPU, CloudStack checks if cards have the required vGPU type support and enough capacity available. Having no appropriate hosts results in an InsufficientServerCapacity exception.
   — Alternately, you can choose to deploy a VM without GPU support, and at a later point, you can change the system offering. You can achieve this by offline upgrade : stop the VM, upgrade the Service Offering to the one with vGPU, then start the VM. In this case, CloudStack gets a list of hosts which have enough capacity to host the VM. If there is a GPU-enabled host, CloudStack reorders this host list and place the GPU-enabled hosts at the bottom of the list.
   — Migrate a VM.
   CloudStack searches for hosts available for VM migration, which satisfies GPU requirement. If the host is available, stop the VM in the current host and perform the VM migration task. If the VM migration is successful, the remaining GPU capacity is updated for both the hosts accordingly.

— Destroy a VM.
GPU resources are released automatically when you stop a VM. Once the destroy VM is successful, CloudStack will make a resource call to the host to get the remaining GPU capacity in the card and update the database accordingly.

CHAPITRE 7

Travailler avec des modèles

7.1 Travailler avec des modèles

Un modèle est une configuration réutilisable pour les machines virtuelles. Quand les utilisateurs lancent des VMs, ils peuvent choisir un modèle depuis une liste dans CloudStack.

Plus spécifiquement, un modèle est une image d'un disque virtuel qui inclue un des nombreux systèmes d'exploitations, des logiciels additionnels optionnels comme des applications de bureautique, et des configurations comme les contrôles d'accès pour déterminer qui peut utiliser le modèle. Chaque modèle est associé à un type d'hyperviseur particulier, qui est spécifié lorsque le modèle est ajouté à CloudStack.

CloudStack est livré avec un modèle par défaut. Dans le but de fournir plus de choix aux utilisateurs, les administrateurs CloudStack et les utilisateurs peuvent créer des modèles et les ajouter à CloudStack.

7.1.1 Créer des modèles : vue d'ensemble

CloudStack est livré avec un modèle par défaut pour le système d'exploitation CentOS. Il y a de nombreuses façon d'ajouter plus de modèles. Les administrateurs et les utilisateurs finaux peuvent ajouter des modèles. La suite typique des évènements est :

1. Lancer une instance de VM du système d'exploitation que vous voulez. Faire tout changement de configuration désiré à la VM.
2. Arrêter la VM.
3. Convertir le volume en modèle.

Il y a d'autres façons d'ajouter des modèles à CloudStack. Par exemple, vous pouvez prendre un instantané du volume de la VM et créer un modèle depuis l'instantané, ou importer un VHD depuis un autre système dans CloudStack.

Les techniques variées pour créer des modèles sont décries dans les quelques sections suivantes.

7.1.2 Conditions requises pour les modèles

— Pour XenServer, installer les drivers PV / outils Xen sur chaque modèle que vous créez. Ceci va activer la migration à chaud et l'arrêt propre des invités.
— Pour vSphere, installer les outils VMware sur chaque modèle que vous créez. Cela va permettre à la vue Console de fonctionner correctement.

7.1.3 Meilleurs pratiques pour les modèles

Si vous planifiez d'utiliser des modèles conséquents (100 GB ou plus), assurez vous d'avoir un réseau 10Gbts pour supporter des modèles conséquents. Un réseau plus lent peut entraîner des dépassements de délais et autres erreurs lorsque des modèles plus gros sont utilisés.

7.1.4 Le modèle par défaut

CloudStack inclue un modèle CentOS. Le modèle est téléchargé par la VM de Stockage Secondaire après que le stockage primaire et secondaire aient étés configurés. Vous pouvez utiliser ce modèle dans votre déploiement de production ou vous pouvez le supprimer et utiliser des modèles personnalisés.

Le mot de passe root du modèle par défaut est "password".

Un modèle par défaut est fourni pour XenServer, KVM et vSphere. Les modèles qui sont téléchargés dépendent du type d'hyperviseur qui est disponible dans votre cloud. Chaque modèle fait une taille d'approximativement 2.5 GB.

Le modèle par défaut inclue les règles standard iptables lesquelles vont bloquer la plupart des accès au modèle en excluant ssh.

```
# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere        anywhere       icmp any
ACCEPT     esp  --  anywhere        anywhere
ACCEPT     ah   --  anywhere        anywhere
ACCEPT     udp  --  anywhere        224.0.0.251    udp dpt:mdns
ACCEPT     udp  --  anywhere        anywhere       udp dpt:ipp
ACCEPT     tcp  --  anywhere        anywhere       tcp dpt:ipp
ACCEPT     all  --  anywhere        anywhere       state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere        anywhere       state NEW tcp dpt:ssh
REJECT     all  --  anywhere        anywhere       reject-with icmp-host-
```

7.1.5 Modèles privés et publics

Lorsqu'un utilisateur crée un modèle, il peut être désigné comme privé ou public.

Les modèles privés ne sont disponibles qu'à l'utilisateur qui l'a créé. Par défaut, un modèle téléchargé est privé.

Quand un utilisateur marque un modèle comme "public", le modèle devient disponible aussi bien pour tous les utilisateurs de tous les comptes du domaine de l'utilisateur que pour les utilisateurs de tous les autres domaines qui ont accès à la Zone dans laquelle le modèle est stocké. Tout dépend si la Zone, à son tour, a été définie comme privée ou public. Une Zone privée est assignée à un seul domaine et une Zone publique est accessible par n'importe quel domaine. Si un modèle public est créé dans une Zone privée, il n'est disponible qu'aux seuls utilisateurs du domaine assigné à

cette Zone. Si un modèle public est créé dans une Zone publique, il est disponible à tous les utilisateurs de tous les domaines.

7.1.6 Créer un modèle depuis une machine virtuelle existante

Une fois que vous avez au moins une VM de configurée de la façon que vous voulez, vous pouvez l'utiliser comme prototype pour les autres VMs.

1. Créer et démarrer une machine virtuelle en utilisant n'importe quelle technique donnée dans "Créer des VMs".
2. Faire toutes les changements de configuration désirés sur la VM en cours de fonctionnement, puis cliquer sur Stop.
3. Attendre l'arrêt de la VM. Quand le statut affiche Stoppée, aller à l'étape suivante.
4. Aller dans "Voir volumes" et sélectionner le Volume ayant le type "ROOT".
5. Cliquer sur Créer un modèle et fournir les informations suivantes :
   - ** Nom et texte affiché**. Ceux-ci seront affichés dans l'interface, alors choisir quelque chose de descriptif.
   - **Type d'OS**. Ceci aide CloudStack et l'hyperviseur à effectuer certaines opérations et à faire des choix qui améliorent les performances de l'invité. Sélectionner une des options.
     - Si le système d'exploitation de la VM arrêtée est listé, le choisir.
     - Si le type d'OS de la VM stoppée n'est pas listé, choisir Autres.
     - Si vous voulez démarrer depuis ce modèle dans le mode PV, choisir Autre PV (32-bit) ou Autre PV (64-bit). Ce choix n'est disponible que pour XenServer :

       Note : Généralement vous ne devriez pas choisir une version plus ancienne de l'OS que la version de l'image. Par exemple, choisir Cent0S 5.4 pour supporter une image CentOS 6.2 ne va pas en général fonctionner. Dans ces cas vous devriez choisir Autres.

   - **Public**. Choisir Oui pour rendre le modèle accessible à tous les utilisateurs de cette installation de CloudStack. Le modèle va apparaître dans la liste Modèles Communautaires. Voir *"Modèles privés et publics"*.
   - **Mot de passe activé**. Choisir Oui si votre modèle a le script CloudStack de changement de mot de passe d'installé. Voir adding-password-management-to-templates.
6. Cliquer sur Ajouter.

Le nouveau modèle sera visible dans la section Modèles lorsque le processus de création du modèle sera terminé. Le modèle est alors disponible lorss de la création d'une nouvelle VM.

7.1.7 Créer un modèle depuis un instantanné

Si vous ne voulez pas stopper la VM pour créer l'entrée de menu Créer un modèle (comme décris dans *"Créer un modèle depuis une machine virtuelle existante"*), vous pouvez créer un modèle directement depuis n'importe quel instantané depuis l'interface CloudStack.

7.1.8 Télécharger des modèles

7.1.9 Modèles vSphere et ISOs

Si vous téléchargez un modèle qui a été créé en utilisant un client vSphere, assurez vous que le fichier OVA ne contienne pas d'ISO. Si c'est le cas, le déploiement de VMs depuis le modèle ne fonctionnera pas.

Les modèles sont téléchargés par une URL. HTTP est le protocole d'accès supporté. Les modèles sont souvent de gros fichiers. Vous pouvez optionnellement les gzipper pour réduire les temps de téléchargement.

Pour télécharger un modèle :

1. Dans la barre de navigation de gauche, cliquer sur Modèles.
2. Cliquer sur Enregistrer un modèle.
3. Fournir les informations suivantes :
   — **Nom et Description**. Ceux-ci seront affichés dans l'interface, alors choisir quelque chose de descriptif.
   — **URL**. Le serveur de gestion va télécharger le fichier depuis l'URL spécifiée, comme par exemple : `http://my.web.server/filename.vhd.gz`.
   — **Zone**. Choisir la zone dans laquelle vous aller rendre le modèle disponible, ou Toutes les Zones pour le rendre disponible dans tout CloudStack.
   — **Type d'OS**. Ceci aide CloudStack et l'hyperviseur à effectuer certaines opérations et à faire des choix qui améliorent les performances de l'invité. Sélectionner une des options :
      — Si le système d'exploitation de la VM arrêtée est listé, le choisir.
      — Si le type d'OS de la VM stoppée n'est pas listé, choisir Autres.

      Note : Vous ne devriez pas choisir une version plus ancienne de l'OS que la version de l'image. Par exemple, choisir Cent0S 5.4 pour supporter une image CentOS 6.2 ne va pas en général fonctionner. Dans ces cas vous devriez choisir Autres.

   — **Hypervisor** : Les hyperviseurs supportés sont listés. Choisir celui désiré.
   — **Format**. Le format du fichier du modèle téléchargé, comme par exemple VHD ou OVA.
   — **Mot de passe activé**. Choisir Oui si votre modèle a le script CloudStack de changement de mot de passe d'installé. Voir adding-password-management-to-templates.
   — **Extractible**. Choisir Oui si le modèle est disponible pour l'extraction. Si cette option est sélectionnée, les utilisateurs finaux peuvent télécharger une image complète du modèle.
   — **Public**. Choisir Oui pour rendre le modèle accessible à tous les utilisateurs de cette installation de CloudStack. Le modèle va apparaître dans la liste Modèles Communautaires. Voir *"Modèles privés et publics"*.
   — **Subventionné**.Choisir Oui si vous voulez que votre modèle soit mis plus en évidence lors de la sélection par l'utilisateur. Le modèle va apparaître dans la liste des modèles subventionnés. Seul un administrateur peut faire un modèle subventionné.

7.1.10 Exporter des modèles

Les utilisateurs finaux et les administrateurs peuvent exporter des modèles depuis CloudStack. Naviguer jusqu'au modèle dans l'interface et choisir la fonction Télécharger depuis le menu Actions.

7.1.11 Créer un modèle Linux

Les modèles Linux devraient être préparé en utilisant cette documentation dans le but de préparer vos VMs linux pour le déploiement de modèle. Pour les besoins de la documentation, la VM que vous être en train de configurer pour faire office de modèle sera référencer comme "Template Master". Ce guide pour le moment ne couvre que les configurations n'utilisant pas les UserData et cloud-init et présume qu'un serveur openssh est installé durant l'installation.

Une vue d'ensemble de la procédure est :

1. Télécharger votre ISO Linux
   Pour plus d'informations, voir "Ajouter une ISO".
2. Créer une instance de VM avec cet ISO.
   Pour plus d'informations, voir "Créer des VMs".
3. Préparer la VM Linux
4. Créer un modèle depuis la VM.
   Pour plus d'informations, voir *"Créer un modèle depuis une machine virtuelle existante"*.

Préparation du système pour Linux

Les étapes suivantes vont préparer une installation Linux basique pour devenir un modèle.

1. **Installation**

   C'est une bonne pratique de nommer votre VM avec quelque chose de générique durant l'installation, ce qui va assurer que des composants comme LVM n'apparaisse pas unique à une machine. Il est recommandé que le nom "localhost" soit utilisé pour l'installation.

   Avertissement : Pour CentOS, il est nécessaire de supprimer l'identifiant unique du fichier de configuration, pour cela éditer le fichier /etc/sysconfig/network-scripts/ifcfg-eth0 et changer le contenu pour celui-ci.

```
DEVICE=eth0
TYPE=Ethernet
BOOTPROTO=dhcp
ONBOOT=yes
```

   Les étapes suivantes mettent à jour les paquets sur le modèle maître.

   — Ubuntu

```
sudo -i
apt-get update
apt-get upgrade -y
apt-get install -y acpid ntp
reboot
```

   — CentOS

```
ifup eth0
yum update -y
reboot
```

2. **Gestion du mot de passe**

   Note : De préférence, les utilisateurs personnalisés (comme comme ceux créés durant l'installation d'Ubuntu) doivent être retirés. D'abord s'assurer que compte de l'utilisateur root est activé en lui donnant un mot de passe et ensuite se connecter en root pour continuer.

```
sudo passwd root
logout
```

   En tant que root, supprimer tous les comptes utilisateurs personnalisés créés durant le processus d'installation.

```
deluser myuser --remove-home
```

   Voir adding-password-management-to-templates pour les instructions pour configurer le script de gestion du mot de passe, qui permettra à CloudStack de changer le mot de passe root depuis l'interface web.

3. **Gestion du nom de machine**

   CentOS configure le nom d'hôte par défaut au démarrage. Malheureusement, Ubuntu n'a pas cette fonctionnalité, pour les installations d'Ubuntu utiliser les étapes suivantes :

   — Ubuntu

   Le nom d'hôte d'une VM déployée depuis un modèle est fixé par un script personnalisé dans */etc/dhcp/dhclient-exit-hooks.d*, ce script vérifie d'abord si la valeur courante est localhost, si c'est le cas, il va obtenir le nom d'hôte, le nom de domaine et l'adresse IP fixe depuis le fichier de bail DHCP et utiliser ces valeurs pour fixer le nom d'hôte et l'ajouter le fichier */etc/hosts* pour la résolution locale du nom d'hôte. Une fois que ce script, ou un utilisateur, a changé le nom d'hôte, il ne va plus ajuster les fichiers systèmes en relation avec son nouveau nom d'hôte. Le script recrée également les clefs du serveur SSH, qui ont été

supprimées juste avant la transformation en modèle (voir ci-dessous). Sauvegarder le script suivant sous */etc/dhcp/dhclient-exit-hooks.d/sethostname*, et ajuster les permissions.

```
#!/bin/sh
# dhclient change hostname script for Ubuntu
oldhostname=$(hostname -s)
if [ $oldhostname = 'localhost' ]
then
    sleep 10 # Wait for configuration to be written to disk
    hostname=$(cat /var/lib/dhcp/dhclient.eth0.leases  |  awk ' /host-name/ { host = $3 }  E
    fqdn="$hostname.$(cat /var/lib/dhcp/dhclient.eth0.leases  |  awk ' /domain-name/ { domai
    ip=$(cat /var/lib/dhcp/dhclient.eth0.leases  |  awk ' /fixed-address/ { lease = $2 }  EN
    echo "cloudstack-hostname: Hostname _localhost_ detected. Changing hostname and adding h
    printf " Hostname: $hostname\n FQDN: $fqdn\n IP: $ip"
    # Update /etc/hosts
    awk -v i="$ip" -v f="$fqdn" -v h="$hostname" "/^127/{x=1} !/^127/ && x { x=0; print i,f,
    mv /etc/hosts /etc/hosts.dhcp.bak
    mv /etc/hosts.dhcp.tmp /etc/hosts
    # Rename Host
    echo $hostname > /etc/hostname
    hostname -b -F /etc/hostname
    echo $hostname > /proc/sys/kernel/hostname
    # Recreate SSH2
    export DEBIAN_FRONTEND=noninteractive
    dpkg-reconfigure openssh-server
fi
### End of Script ###

chmod 774  /etc/dhcp/dhclient-exit-hooks.d/sethostname
```

Avertissement : Les étapes suivantes devraient être lancée lorsque vous être prêt à transformer votre Modèle Maître en modèle. Si le Modèle Maître est redémarré durant ces étapes vous devrez relancer toutes les étapes à nouveau. A la fin de ce processus, le Modèle Maître devrait être arrêté et le modèle créé pour créer et déployer le modèle final.

4. **Supprimer les règles udev des périphériques persistants**

   Cet étape retire les informations unique de votre Modèle Maître comme les adresses réseaux MAC, les fichiers de baux et les périphériques de type bloc comme les CD. Les fichiers sont générés automatiquement au démarrage suivant ;

   — Ubuntu

```
rm -f /etc/udev/rules.d/70*
rm -f /var/lib/dhcp/dhclient.*
```

   — CentOS

```
rm -f /etc/udev/rules.d/70*
rm -f /var/lib/dhclient/*
```

5. **Supprimer les clefs SSH**

   Cet étape s'assure que toutes vos VMs issuent de modèles n'aient pas les mêmes clefs SSH, ce qui réduirait la sécurité de vos machines dramatiquement.

```
rm -f /etc/ssh/*key*
```

6. **Nettoyer les fichiers de logs**

   C'est une bonne habitude de supprimer les vieux fichiers de logs du Modèle Maître.

```
cat /dev/null > /var/log/audit/audit.log 2>/dev/null
cat /dev/null > /var/log/wtmp 2>/dev/null
logrotate -f /etc/logrotate.conf 2>/dev/null
rm -f /var/log/*-* /var/log/*.gz 2>/dev/null
```

7. **Configurer le nom d'hôte**
   Pour que le script DHCP pour Ubuntu fonctionne et que le client dhclient de CentOS puisse fixer le nom d'hôte ils nécessitent tous les deux que le nom d'hôte du Modèle Maître soit "localhost". Lancer les commandes suivantes pour changer le nom d'hôte.

```
hostname localhost
echo "localhost" > /etc/hostname
```

8. **Forcer l'expiration du mot de passe utilisateur**
   Cet étape force l'utilisateur à changer le mot de passe de la VM après que le modèle ait été déployé.

```
passwd --expire root
```

9. **Nettoyer l'historique utilisateur**
   L'étape suivante retire les commandes bash que vous venez de lancer.

```
history -c
unset HISTFILE
```

10. **Éteindre la VM**
    Vous êtes maintenant prêt pour éteindre votre Modèle Maître et créer un modèle !

```
halt -p
```

11. **Créer le modèle !**
    Vous êtes maintenant prêts à créer le modèle, pour plus d'informations voir *"Créer un modèle depuis une machine virtuelle existante"*.

Note : Les VMs provenant d'un modèle sous Ubuntu ou CentOS peuvent nécessiter un redémarrage après le provisionnement afin de changer le nom d'hôte.

7.1.12 Créer un modèle Windows

Les modèles Windows doivent être préparées avec Sysprep avant de pouvoir être provisionnés sur plusieurs machines. Sysprep vous permet de créer un modèle générique Windows et supprime toute possibilité de conflits de SID.

Note : (XenServer) Les VMs Windows fonctionnant sous XenServer nécessitent des drivers PV, qui peuvent être fourni dans le modèle ou ajouter après que la VM soit créée. Les drivers PV sont nécessaires pour les fonctions essentielles de gesion comme monter des volumes additionels et des images ISO, la migration à chaud, et l'arrêt correcte.

Une vue d'ensemble de la procédure est :

1. Télécharger votre ISO Windows.
   Pour plus d'informations, voir "Ajouter une ISO".
2. Créer une instance de VM avec cet ISO.
   Pour plus d'informations, voir "Créer des VMs".

3. Suivre les étapes dans Sysprep pour Windows Server 2008 R2 (ci-dessous) ou Sysprep pour Windows Server 2003 R2, en fonction de votre version de Windows Server.
4. Les étapes de préparations sont terminées. Vous pouvez maintenant créer un modèle comme décrit dans Créer un modèle Windows.

Préparation du système pour Windows Server 2008 R2

Pour Windows 2008 R2, vous lancer Windows System Image Manager pour créer un fichier XML de réponse sysprep personnalisé. Windows System Image Manager est installé comme partie du Windows Automated Installation Kit (AIK). Windows AIK peut être téléchargé depuis Microsoft Download Center.

Utiliser les étapes suivantes pour lancer sysprep pour Windows 2008 R2 :

Note : Les étapes décrites ici proviennent de l'excellent guide de Charity Shelbourne, publié à l'origine à Windows Server 2008 Sysprep Mini-Setup.

---

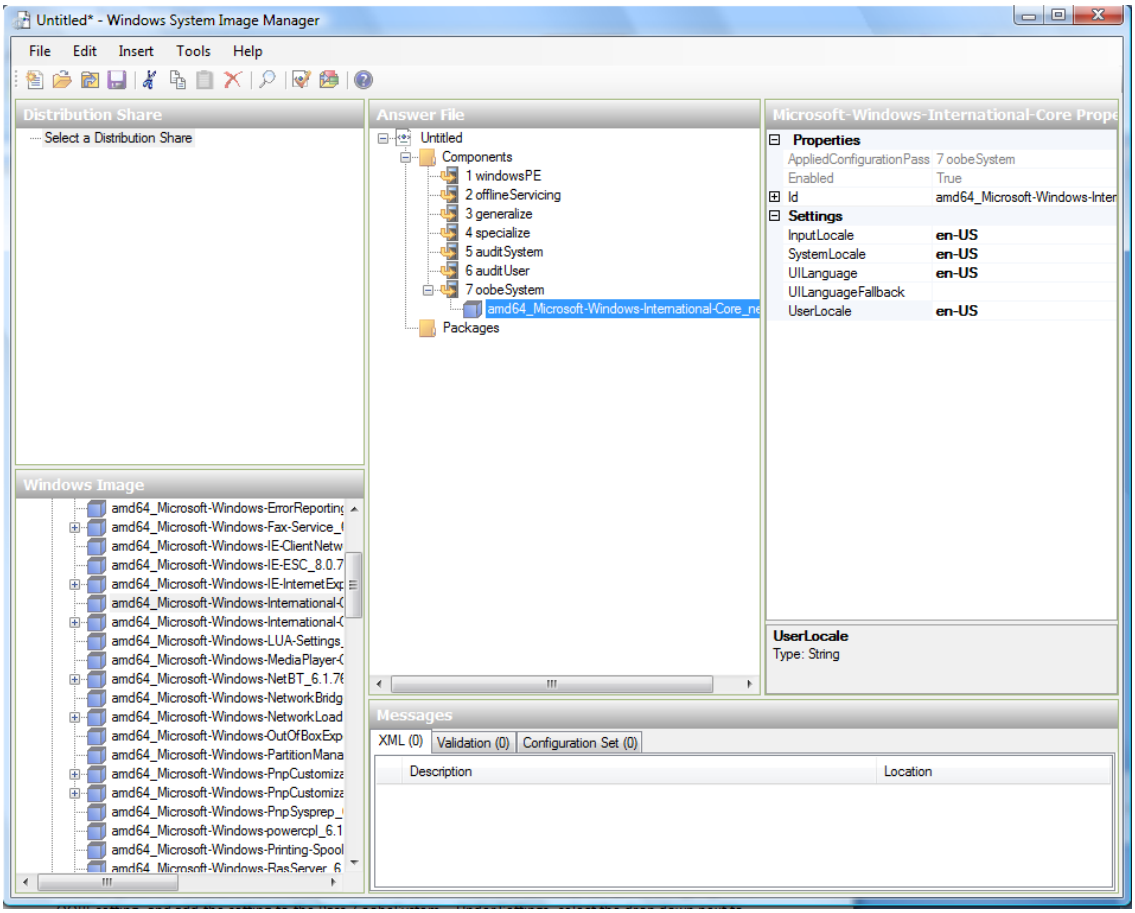
1. Télécharger et installer Windows AIK

   Note : Windows AIK ne devrait pas être installé sur la VM Windows 2008 R2 que vous venez de créer. Windows AIK ne devrait pas faire partie d'un modèle que vous créez. Il est juste utilisé pour créer le fichier de réponse sysprep.

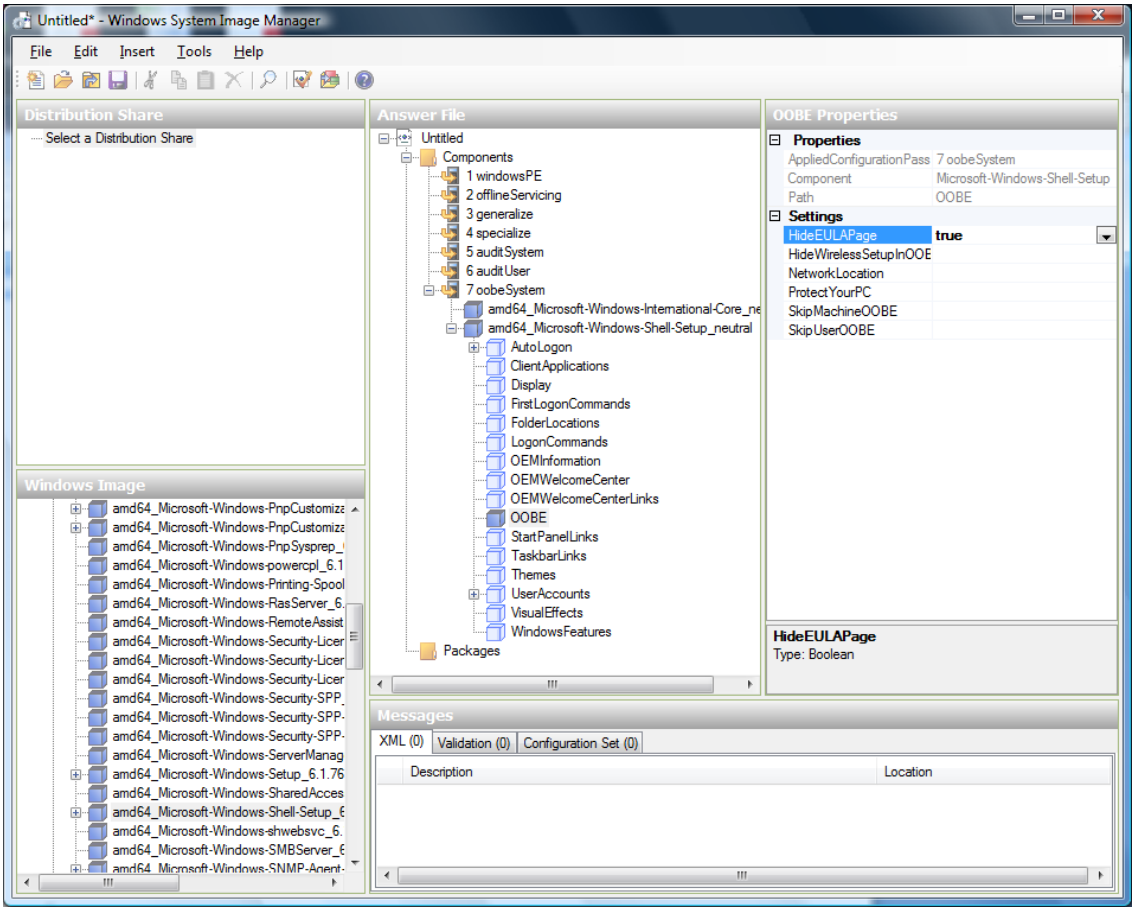
   ---

2. Copier le fichier install.wim du répertoire \sources du DVD d'installation Windows 2008 R2 sur le disque dur. C'est un très gros fichier et peut mettre du temps à se copier. Windows AIK nécessite que le fichier WIM soit en écriture.
3. Démarrer le Windows System Image Manager, qui est une partie du Windows AIK.
4. Dans le paneau Image Windows, clic-droit sur Sélectionner une image Windows ou sur option Fichier catalogue pour charger le fichier install.wim que vous venez de copier.
5. Sélectionner Windows 2008 R2 Edition.

   Vous pouvez être avertit par une alerte que le fichier catalogue ne peut pas être ouvert. Cliquer sur Oui pour créer un nouveau fichier catalogue.
6. Dans le paneau Fichier Réponse, cliquer droit pour créer un nouveau fichier de réponse.
7. Générer un fichier de réponse depuis Windows System Image Manager en utilisant les étapes suivantes :
   (a) La première page que vous devez automatiser est la page de Selection de Langage et de Pays ou de Région. Pour automatiser cela, développer les composants dans votre panneau Image Windows, clic-droit et ajouter le paramètre Microsoft-Windows-International-Core pour passer 7 oobeSystem. Dans votre panneau Fichier de réponse, configurer le InputLocale, SystemLocale, UILanguage et UserLocale avec les paramètres appropriés pour votre langue et pays ou région. Si vous avez une question à propos de n'importe quel paramètre, vous pouver faire un clic-droit sur le paramètre spécifique et sélectionner Aide. Cela va ouvrir le fichier d'aide CHM approprié avec plus d'informations, incluant des examples sur le paramètre que vous êtes en train d'essayer de configurer.

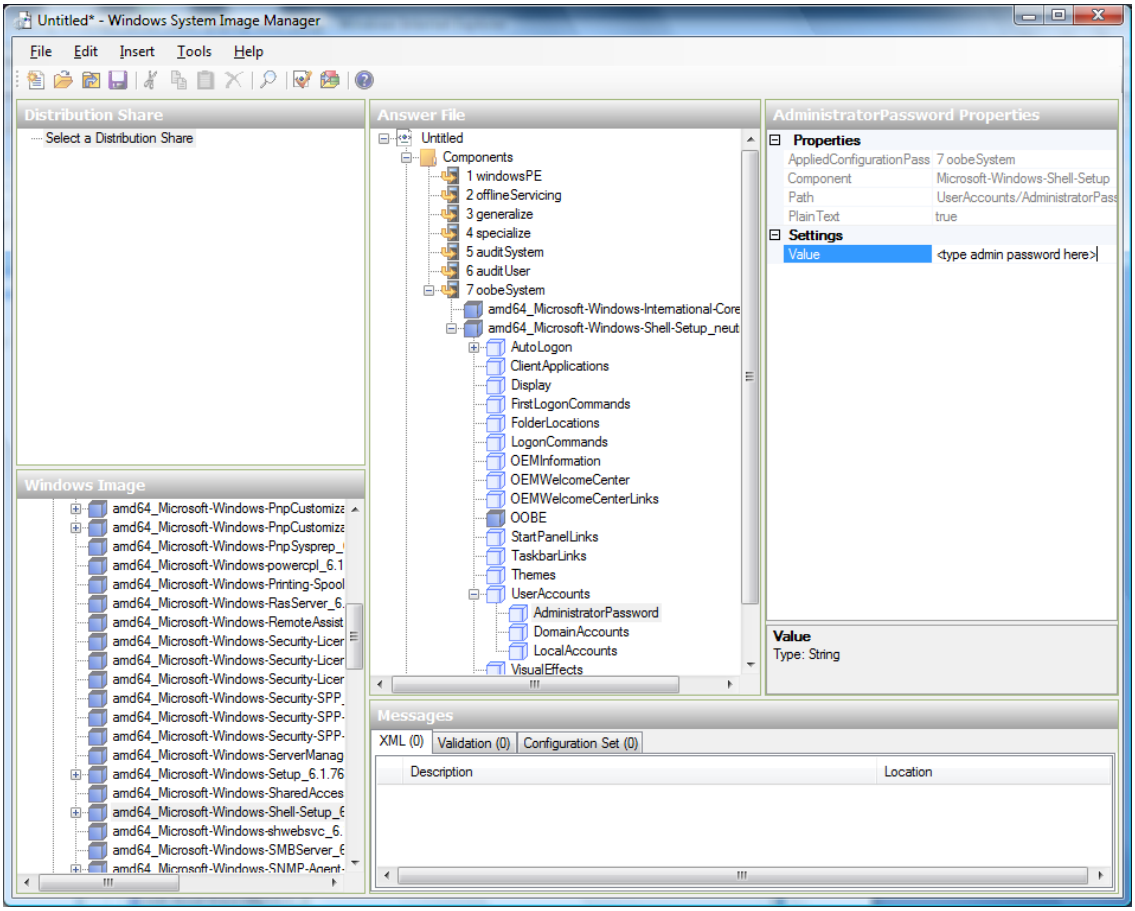


(b) Vous devez automatiser la page de Sélection des Termes de Licence Logiciel, aussi connue comme End-User Licence Agreement (EULA). Pour cela, étendre le composant Microsoft-Windows-Shell-Setup. Surligner le paramètre OOBE et ajouter le paramètre à la Pass 7 oobeSystem. Dans paramètres, fixer HideEULAPage à vrai.



(c) Assurez vous que la clé de licence est correctement configurée. Si vous utilisez une clé MAK, vous pouvez juste saisir la clé MAK sur la VM Windows 2008 R2. Vous ne devez pas introduire la MAK dans le Windows System Image Manager. Si vous utilisez un hôte KMS pour l'activation vous ne devez pas saisir de clé de produit. Des détails sur l'activation en volume de Windows peuvent être trouvés ici http://technet.microsoft.com/en-us/library/bb892849.aspx

(d) Vous devez automatiser la page Modifier le mot de passe administrateur. Développez le composant Microsoft-Windows-Shell-Setup (s'il n'est pas encore développé), développez UserAccounts, cliquez avec le bouton droit sur AdministratorPassword et ajoutez le paramètre de configuration Pass 7 oobeSystem de votre fichier de réponses. Sous Paramètres, spécifiez un mot de passe après Valeur.



Vous devriez lire la documentation AIK et configurer beaucoup plus d'options pour pour convenir à votre déploiement Les étapes ci-dessus sont le minimum requis pour rendre fonctionnel la configuration sans assistance de Windows.

8. Sauvegarder le fichier de réponse sous unattend.xml. Vous pouvez ignorer les messages d'alertes qui apparaissent dans la fenêtre de validation.
9. Copier le fichier unattend.xml sous le dossier c :\windows\system32\sysprep de la machine virtuelle Windows 2008 R2.
10. Une fois que vous avez placé le fichier unattend.xml dans le dossier c :\windows\system32\sysprep, vous lancer l'outil sysprep comme ci-dessous :

```
cd c:\Windows\System32\sysprep
sysprep.exe /oobe /generalize /shutdown
```

La VM Windows 2008 R2 va s'éteindre automatiquement après que le sysprep soit terminé.

Préparation du système pour Windows Server 2003 R2

Les versions précédentes de Windows ont un outil sysprep différent. Suivre ces étapes pour Windows Server 2003 R2.

1. Extrayez le contenu de \support\tools\deploy.cab du CD d'installation de Windows dans le répertoire appelé c :\sysprep dans la VM Windows 2003 R2.
2. Lancer c :\sysprep\setupmgr.exe pour créer le fichier sysprep.inf.
   (a) Sélectionner Créer un nouveau pour créer un nouveau fichier de réponses.
   (b) Entrer "Sysprep setup" pour le type de Setup.
   (c) Sélectionner la version et l'édition appropriée d'OS.

(d) Dans l'écran Agrément Licence, sélectionner "Oui automatisation complète de l'installation".

(e) Fournir le nom et l'organisation.

(f) Laisser les paramètres d'affichage par défaut.

(g) Sélectionner la zone horaire appropriée.

(h) Fournir votre clef de produit.

(i) Sélectionner un mode de licence approprié pour votre déploiement

(j) Sélectionner "Générer automatiquement un nom d'ordinateur".

(k) Saisissez un mot de passe par défaut pour l'administrateur. Si vous activez la fonctionnalité de réinitialisation de mot de passe, les utilisateurs n'utiliseront pas ce mot de passe. Ce mot de passe sera réinitialisé par le gestionnaire d'instance après les démarrage des invités.

(l) Laisser les Composants Réseaux à "Paramètres par défaut".

(m) Sélectionner l'option "WORKGROUP".

(n) Laisser les options Téléphonie par défaut.

(o) Sélectionner les paramètres Régionaux appropriés.

(p) Sélectionner les paramètres de langage approprié.

(q) Ne pas installer d'imprimantes.

(r) Ne pas spécifier "Lancer une fois les commandes".

(s) Vous ne devez pas spécifier une chaîne d'identification.

(t) Sauvegarde le fichier de réponse sous c :\sysprep\sysprep.inf.

3. Lancer la commande suivante pour syspreper l'image :

```
c:\sysprep\sysprep.exe -reseal -mini -activated
```

Après cette étape la machine va automatiquement s'arrêter

7.1.13 Importer des images de Machines Amazon

The following procedures describe how to import an Amazon Machine Image (AMI) into CloudStack when using the XenServer hypervisor.

Assume you have an AMI file and this file is called CentOS_6.2_x64. Assume further that you are working on a CentOS host. If the AMI is a Fedora image, you need to be working on a Fedora host initially.

You need to have a XenServer host with a file-based storage repository (either a local ext3 SR or an NFS SR) to convert to a VHD once the image file has been customized on the Centos/Fedora host.

Note : Lors du copier/coller d'une commande, soyez certain que la commande est collée sur une seule ligne avant de l'exécuter. Certains lecteur de document peuvent introduire un saut de ligne indésirable dans le texte copié.

Pour importer un AMI

1. Configurer la boucle interne sur le fichier image :

```
# mkdir -p /mnt/loop/centos62
# mount -o loop  CentOS_6.2_x64 /mnt/loop/centos54
```

2. Install the kernel-xen package into the image. This downloads the PV kernel and ramdisk to the image.

```
# yum -c /mnt/loop/centos54/etc/yum.conf --installroot=/mnt/loop/centos62/ -y install kernel-xe
```

3. Créer une entrée grub dans /boot/grub/grub.conf.

```
# mkdir -p /mnt/loop/centos62/boot/grub
# touch /mnt/loop/centos62/boot/grub/grub.conf
# echo "" > /mnt/loop/centos62/boot/grub/grub.conf
```

4. Déterminer le nom du kernel PV qui a été installé dans l'image.

```
# cd /mnt/loop/centos62
# ls lib/modules/
2.6.16.33-xenU  2.6.16-xenU  2.6.18-164.15.1.el5xen  2.6.18-164.6.1.el5.centos.plus  2.6.18-xen
# ls boot/initrd*
boot/initrd-2.6.18-164.6.1.el5.centos.plus.img boot/initrd-2.6.18-164.15.1.el5xen.img
# ls boot/vmlinuz*
boot/vmlinuz-2.6.18-164.15.1.el5xen  boot/vmlinuz-2.6.18-164.6.1.el5.centos.plus  boot/vmlinuz-
```

   Xen kernels/ramdisk always end with "xen". For the kernel version you choose, there has to be an entry for that version under lib/modules, there has to be an initrd and vmlinuz corresponding to that. Above, the only kernel that satisfies this condition is 2.6.18-164.15.1.el5xen.

5. Based on your findings, create an entry in the grub.conf file. Below is an example entry.

```
default=0
timeout=5
hiddenmenu
title CentOS (2.6.18-164.15.1.el5xen)
   root (hd0,0)
   kernel /boot/vmlinuz-2.6.18-164.15.1.el5xen ro root=/dev/xvda
   initrd /boot/initrd-2.6.18-164.15.1.el5xen.img
```

6. Editer le fichier /etc/fstab, changer "sda1" par "svda" et changer "sdb" par "svdb"

```
# cat etc/fstab
/dev/xvda  /         ext3    defaults        1 1
/dev/xvdb  /mnt      ext3    defaults        0 0
none       /dev/pts  devpts  gid=5,mode=620  0 0
none       /proc     proc    defaults        0 0
none       /sys      sysfs   defaults        0 0
```

7. Enable login via the console. The default console device in a XenServer system is xvc0. Ensure that etc/inittab and etc/securetty have the following lines respectively :

```
# grep xvc0 etc/inittab
co:2345:respawn:/sbin/agetty xvc0 9600 vt100-nav
# grep xvc0 etc/securetty
xvc0
```

8. Ensure the ramdisk supports PV disk and PV network. Customize this for the kernel version you have determined above.

```
# chroot /mnt/loop/centos54
# cd /boot/
# mv initrd-2.6.18-164.15.1.el5xen.img initrd-2.6.18-164.15.1.el5xen.img.bak
# mkinitrd -f /boot/initrd-2.6.18-164.15.1.el5xen.img --with=xennet --preload=xenblk --omit-scs
```

9. Changer le mot de passe.

```
# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

10. Sortir du chroot.

```
# exit
```

11. Vérifier que */etc/ssh/sshd_config* contienne les lignes autorisant la connexion SSH par mot de passe.

```
# egrep "PermitRootLogin|PasswordAuthentication" /mnt/loop/centos54/etc/ssh/sshd_config
PermitRootLogin yes
PasswordAuthentication yes
```

12. If you need the template to be enabled to reset passwords from the CloudStack UI or API, install the password change script into the image at this point. See adding-password-management-to-templates.
13. Démonter et supprimer le montage en boucle interne.

```
# umount /mnt/loop/centos54
# losetup -d /dev/loop0
```

14. Copy the image file to your XenServer host's file-based storage repository. In the example below, the Xenserver is "xenhost". This XenServer has an NFS repository whose uuid is a9c5b8c8-536b-a193-a6dc-51af3e5ff799.

```
# scp CentOS_6.2_x64 xenhost:/var/run/sr-mount/a9c5b8c8-536b-a193-a6dc-51af3e5ff799/
```

15. Log in to the Xenserver and create a VDI the same size as the image.

```
[root@xenhost ~]# cd /var/run/sr-mount/a9c5b8c8-536b-a193-a6dc-51af3e5ff799
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]#  ls -lh CentOS_6.2_x64
-rw-r--r-- 1 root root 10G Mar 16 16:49 CentOS_6.2_x64
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# xe vdi-create virtual-size=10GiB sr-uuid=a
cad7317c-258b-4ef7-b207-cdf0283a7923
```

16. Importer le fichier image dans le VDI. Cela peut prendre 10-20 minutes.

```
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# xe vdi-import filename=CentOS_6.2_x64 uuid
```

17. Locate a the VHD file. This is the file with the VDI's UUID as its name. Compress it and upload it to your web server.

```
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# bzip2 -c cad7317c-258b-4ef7-b207-cdf0283a7
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# scp CentOS_6.2_x64.vhd.bz2 webserver:/var/
```

7.1.14 Convertir une VM Hyper-V en modèle

To convert a Hyper-V VM to a XenServer-compatible CloudStack template, you will need a standalone XenServer host with an attached NFS VHD SR. Use whatever XenServer version you are using with CloudStack, but use XenCenter 5.6 FP1 or SP2 (it is backwards compatible to 5.6). Additionally, it may help to have an attached NFS ISO SR.

For Linux VMs, you may need to do some preparation in Hyper-V before trying to get the VM to work in XenServer. Clone the VM and work on the clone if you still want to use the VM in Hyper-V. Uninstall Hyper-V Integration Components and check for any references to device names in /etc/fstab :

1. From the linux_ic/drivers/dist directory, run make uninstall (where "linux_ic" is the path to the copied Hyper-V Integration Components files).
2. Restore the original initrd from backup in /boot/ (the backup is named *.backup0).
3. Remove the "hdX=noprobe" entries from /boot/grub/menu.lst.
4. Check /etc/fstab for any partitions mounted by device name. Change those entries (if any) to mount by LABEL or UUID. You can get that information with the blkid command.

The next step is make sure the VM is not running in Hyper-V, then get the VHD into XenServer. There are two options for doing this.

Option une :

1. Importer le VHD en utilisant XenCenter. Dans XenCenter, aller à Outils>Outils d'Appliance Virtuelle>Importation d'image disque.
2. Choose the VHD, then click Next.
3. Name the VM, choose the NFS VHD SR under Storage, enable "Run Operating System Fixups" and choose the NFS ISO SR.
4. Click Next, then Finish. A VM should be created.

Option deux :

1. Run XenConvert, under From choose VHD, under To choose XenServer. Click Next.
2. Choose the VHD, then click Next.
3. Input the XenServer host info, then click Next.
4. Name the VM, then click Next, then Convert. A VM should be created.

Once you have a VM created from the Hyper-V VHD, prepare it using the following steps :

1. Boot the VM, uninstall Hyper-V Integration Services, and reboot.
2. Install XenServer Tools, then reboot.
3. Prepare the VM as desired. For example, run sysprep on Windows VMs. See *"Creating a Windows Template"*.

Either option above will create a VM in HVM mode. This is fine for Windows VMs, but Linux VMs may not perform optimally. Converting a Linux VM to PV mode will require additional steps and will vary by distribution.

1. Shut down the VM and copy the VHD from the NFS storage to a web server ; for example, mount the NFS share on the web server and copy it, or from the XenServer host use sftp or scp to upload it to the web server.
2. In CloudStack, create a new template using the following values :
   — URL. Give the URL for the VHD
   — OS Type. Use the appropriate OS. For PV mode on CentOS, choose Other PV (32-bit) or Other PV (64-bit). This choice is available only for XenServer.
   — Hyperviseur. XenServer
   — Format. VHD

The template will be created, and you can create instances from it.

7.1.15 Ajouter un mot de passe de gestion à votre modèle

CloudStack fourni une fonctionnalité optionnelle de réinitialisation de mot de passe qui permet aux utilisateurs de fournir un mot de passe root ou admin temporaire ou de réinitialiser un mot de passe root ou admin existant depuis l'interface CloudStack.

Pour activer la fonctionnalité de Réinitialisation de Mot de passe, vous aurez besoin de télécharger un script additionnel pour patcher votre modèle. Lorsque plus tard vous téléchargerez votre modèle dans CloudStack, vous pourrez spécifier si la fonctionnalité de réinitailisation de mot de passe admin/root doit être activée pour ce modèle.

La fonctionnalité de mot de passe de gestion fonctionne toujours par réinitialisation du mot de passe du compte lors du démarrage de l'instance. Le script effectue un appel HTTP au routeur virtuel pour recupérer le mot de passe du compte qui doit être changé. Aussi longtemps que le routeur virtuel est accessible l'invité aura accès au mot de passe du compte qui doit être utilisé. Quand l'utilisateur demande une réinitialisation du mot de passe, le serveur de gestion génère et envoie un nouveau mot de passe au routeur virtuel pour ce compte. Ainsi un redémarrage de l'instance est nécessaire pour effectuer un changement de mot de passe.

Si le script n'est pas capable de contacter le routeur virtuel durant le démarrage de l'instance le mot de passe ne sera pas réinitialisé mais le démarrage va continuer normalement.

Installation d'un OS Linux

Utiliser les étapes suivantes pour commencer l'installation d'un OS Linux :

1. Télécharger le fichier du script cloud-set-guest-password :
   — http://download.cloud.com/templates/4.2/bindir/cloud-set-guest-password.in
2. Renommer le fichier :

```
mv cloud-set-guest-password.in cloud-set-guest-password
```

3. Copier ce fichier sous /etc/init.d.
   Sur certaines distributions Linux, copier le fichier sous `/etc/rc.d/init.d`.
4. Lancer la commande suivante pour rendre le script exécutable :

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

5. En fonction de la distribution Linux, continuer avec l'étape appropriée.
   Sous Fedora, CentOS/RHEL et Debian, lancer :

```
chkconfig --add cloud-set-guest-password
```

Installation d'un OS Windows

Télécharger l'installateur, CloudInstanceManager.msi depuis la page de Téléchargement et lancer l'installateur dans la VM windows nouvellement créée.

7.1.16 Supprimer des modèles

Des modèles peuvent être supprimés. En général, lorsqu'un modèle concerne plusieurs zones, seule la copie qui est selectionnée pour la suppression sera supprimée ; le même modèle dans les autres zones ne seront pas supprimés. Le modèle CentOS fourni est une exception à cela. Si le modèle CentOS fourni est supprimé, il sera supprimé de toutes les zones.

Quand un modèle est supprimé, les VMs instanciées depuis celui-ci continueront de fonctionner. Toutefois, les nouvelles VMs ne pourront plus être créées en se basant sur le modèle supprimé.

CHAPITRE 8

Travailler avec des hôtes

8.1 Travailler avec les hôtes

8.1.1 Ajouter des hôtes

Des hôtes complémentaires peuvent être ajoutés à tout moment pour fournir plus de capacité pour des VMs invités. Pour les pré-requis et les instructions, voir “Ajouter un hôte”.

8.1.2 Maintenance Planifiée et Mode Maintenance pour les hôtes

Vous pouvez faire entrer un hôte en mode maintenance. Quand le mode maintenance est activé, l’hôte devient indisponible pour recevoir de nouvelles VMs, et les VMs invitées déjà en fonctionnement sur l’hôte sont migrées de façon transparente vers un autre hôte qui n’est pas en mode maintenance. Cette migration utilise la technologie de migration à chaud et n’interrompt pas l’exécution de l’invité.

Le vCenter et le Mode de Maintenance

Pour entrer en mode maintenance sur un hôte du vCenter, à la fois le vCenter et CloudStack doivent être utilisés de concert. CloudStack et vCenter ont des modes de maintenance séparés qui fonctionnent en étroite collaboration.

1. Placer l’hôte dans le mode de “maintenance planifiée” de CloudStack. Cela n’invoque pas le mode de maintenance du vCenter, mais cause la migration des VMs hors de l’hôte.

   Quand le mode de maintenance de CloudStack est demandée, l’hôte se met d’abord dans l’état Préparation pour Maintenance. Dans cet état, il ne peut pas être la cible du démarrage d’une nouvelle VM. Alors toutes les VMs vont être migrée hors du serveur. La migration à chaud sera utilisée pour bouger les VMs hors de l’hôte. Cela permet de migrer les invités de l’hôte sans causer de perturbation pour les invités. Après que la migration soit finie, l’hôte va entrer dans le mode Prêt pour Maintenance.
2. Attendre l’apparition de l’indicateur “Prêt pour la Maintenance” dans l’interface.
3. Maintenant utiliser le vCenter pour accomplir toutes les actions nécessaires pour entretenir l’hôte. Durant ce temps, l’hôte ne peut pas être la cible de l’allocation d’une nouvelle VM.
4. Lorsque les tâches de maintenance sont terminées, sortir l’hôte du mode maintenance comme ceci :
   (a) Utiliser d’abord le vCenter pour sortir du mode maintenance du vCenter.

   Cela rend le hôte prêt pour que CloudStack puisse le réactiver.

   (b) Utiliser alors l’interface d’administration de CloudStack pour annuler le mode de maintenance de CloudStack

   Quand l’hôte reviens en ligne, les VMs qui ont étés migrées peuvent être re-migrées manuellement et de nouvelles VMs peuvent être ajoutées.

Le XenServer et le Mode Maintenance

Pour le XenServer, vous pouvez mettre un serveur hors ligne temporairement en utilisant la fonctionnalité de Mode Maintenance dans XenCenter. Quand vous placer un serveur dans le mode maintenance, toutes les VMs sont automatiquement migrées vers un autre hôte du même groupe. Si le serveur est le maître du groupe, un nouveau maître sera aussi sélectionné pour le groupe. Pendant qu'un serveur est en Mode Maintenance, vous ne pouvez pas créer ou démarrer de VMs sur lui.

Pour basculer un serveur en Mode Maintenance :

1. Dans le panneau Ressources, sélectionner le serveur, puis effectuer l'une des actions suivantes :
   — Clic-droit, puis Entrer en Mode Maintenance dans le menu de raccourcis.
   — Dans le menu Serveur, cliquer Entrer en Mode Maintenance.
2. Cliquer sur Entrer en Mode Maintenance.

Le statut du serveur dans le panneau Ressources affichera lorsque toutes les VMs fonctionnant auront étés migrées avec succès du serveur.

Pour sortir un serveur du Mode Maintenance :

1. Dans le panneau Ressources, sélectionner le serveur, puis effectuer l'une des actions suivantes :
   — Clic-droit, puis Sortir dun Mode Maintenance dans le menu de raccourcis.
   — Dans le menu Serveur, cliquer Sortir du Mode Maintenance.
2. Cliquer sur Sortir du Mode Maintenance

8.1.3 Désactiver et activer des Zones, Pods et Clusters

Vous pouvez activer ou désactiver une zone, un pod ou cluster sans le supprimer définitivement du cloud. C'est utile pour la maintenance ou lorsqu'il y a des problèmes qui rendent une partie de l'infrastructure du Cloud non fiable. Aucune nouvelle allocation ne sera faîte à une zone, pod ou cluster désactivé tant que son état n'est pas de nouveau Activé. Quand une zone, pod ou cluster est ajouté au cloud, il est désactivé par défaut.

Pour déactiver et activer une zone, un pod ou un cluster :

1. Se connecter à l'interface de CloudStack comme administrateur
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Dans Zones, cliquer sur Voir plus.
4. Si vous êtes en train de désactiver ou d'activer une zone, trouver le nom de la zone dans la liste, et cliquer sur le bouton Activer/Désactiver. 
5. Si vous êtes en train de désactiver ou d'activer un pod ou un cluster, cliquer sur le nom de la zone qui contient le pod ou le cluster.
6. Cliquer sur l'onglet Offre de calcul.
7. Dans les noeuds Pods ou les Clusters du diagramme, cliquer sur Totu voir.
8. Cliquer sur le nom du pod ou du cluster dans la liste.
9. Cliquer sur le bouton Activer/Désactiver. 

8.1.4 Retirer des hôtes

Les hôtes peuvent être supprimés du cloud si besoin. La procédure pour supprimer un hôte dépend du type de l'hyperviseur.

Retirer des hôtes XenServer et KVM

Un noeud ne peut pas être supprimé d'un cluster jusqu'à ce qu'il ait été placé en mode maintenance. Cela va assurer que toutes les VM ont été migrées vers d'autres hôtes. Pour retirer un hôte du cloud :

1. Placer le noeud en mode maintenance.
   Voir *"Maintenance programmée et mode de maintenance pour les hôtes"*.
2. Pour KVM, stopper le service cloud-agent.
3. Utiliser l'option de l'interface pour supprimer le noeud.
   Alors vous pouvez éteindre l'hôte, réutiliser son adresse IP, le réinstaller, etc.

Retirer des hôtes vSphere

Pour retirer ce type d'hôte, dans un premier temps, le placer en mode maintenance, comme décrit dans *"Maintenance programmée et mode de maintenance pour les hôtes"*. Utiliser ensuite CloudStack pour supprimer l'hôte. CloudStack ne va pas diriger de commandes à un hôte qui a été supprimé en utilisant CloudStack. Toutefois l'hôte peut toujours exister dans le cluster dans le vCenter.

8.1.5 Ré-installer des hôtes

Vous pouvez réinstaller un hôte après l'avoir placé dans le mode maintenance et l'avoir supprimé. Si un hôte est arrêté et ne peut pas être placé en mode maintenance, il pourra toujours être supprimé après l'avoir ré-installé.

8.1.6 Entretenir les hyperviseurs sur les hôtes

Lorsque vous utilisez des logiciels hyperviseur sur des hôtes, assurez-vous que toutes les mises à jour fournies par le vendeur de l'hyperviseur soit appliquées. Suivez les sorties des correctifs de l'hyperviseur via les moyens du support du vendeur de l'hyperviseur, et appliquez les correctifs aussitôt que possible après leurs sorties. CloudStack ne va pas suivre ni vous notifier des correctifs requis pour l'hyperviseur. Il est essentiel que vos hôtes soient totalement à jour de leurs correctifs. Le vendeur de l'hyperviseur refusera probablement de supporter un système qui n'est pas à jour de correctifs.

Note : L'absence des dernières mise à jour peut mener à la corruption de données et la perte de VM.

(XenServer) Pour plus d'informations, voir **'Mises à jour hautement recommandées pour XenServer dans la base de connaissance CloudStack<http ://docs.cloudstack.org/Knowledge_Base/Possible_VM_corruption_if_XenServer_Hotfix_is_no**

8.1.7 Changer le mot de passe de l'Hôte

Le mot de passe pour un noeud XenServer, un noeud KVM ou un noeud vSphere peut être changé dans la base de données. Notez que tous les noeuds d'un cluster doivent avoir le même mot de passe.

Pour changer un mot de passe sur un noeud :

1. Identifier tous les hôtes dans le cluster.
2. Changer le mot de passe sur tous les hôtes du cluster. Maintenant le mot de passe pour l'hôte et le mot de passe connu par CloudStack ne correspondent plus. Les opérations dans le cluster vont échouer jusqu'à ce que les 2 mots de passe correspondent.
3. Si le mot de passe dans la base de données est crypté, il est (probablement) nécessaire de crypter le nouveau mot de passe en utilisant la clef de la base de données avant de l'ajouter dans la base de données.

```
java -classpath /usr/share/cloudstack-common/lib/jasypt-1.9.0.jar \
org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI \
encrypt.sh input="newrootpassword" \
password="databasekey" \
verbose=false
```

4. Obtenir la liste des ID d'hôte pour les hôtes du même cluster pour lequel vous être en train de changer le mot de passe. Vous allez avoir besoin d'accéder à la base de données pour déterminer ces ID d'hôtes. Pour chaque nom d'hôte "h" (ou cluster vSphere) pour lequel vous voulez changer le mot de passe, exécuter :

```
mysql> SELECT id FROM cloud.host WHERE name like '%h%';
```

5. Cela devrait retourner un seul ID. L'enregistrer l'ensemble de ces ID pour ces hôtes. Maintenant récupérer le numéro de la ligne host_details pour cet hôte.

```
mysql> SELECT * FROM cloud.host_details WHERE name='password' AND host_id={previous step ID};
```

6. Mettre à jour les mots de passe pour l'hôte dans la base de données. Dans cet exemple, nous changeons les mots de passe pour les hôtes avec les ID d'hôte 5 et 12 et les ID host_details 8 et 22 avec le mot de passe "password".

```
mysql> UPDATE cloud.host_details SET value='password' WHERE id=8 OR id=22;
```

8.1.8 Sur-allocation et Limites d'Offre de Service.

(Supporté par XenServer, KVM et VMware)

Les facteurs de sur-allocation de CPU et de mémoire (RAM) peuvent être paramétrés pour chaque cluster pour changer le nombre de VM qui peuvent fonctionner sur chaque hôte du cluster. Cela aide à optimiser l'utilisation des ressources. En augmentant le ration de sur-allocation, une plus grosse capacité de la ressource va être utilisée. Si le ration est fixé à 1, aucune sur-allocation n'est effectuée.

L'administrateur peut aussi paramétrer les facteurs globaux par défaut de sur-allocation dans les variables de la configuration globale cpu.overprovisioning.factor et mem.overprovisioning.factor. La valeur par défaut de ces variables est de 1 : la sur-allocation est désactivée par défaut.

Les facteurs d'Over-provisionning sont dynamiquement substitué dans les calculs de capacités de CloudStack. Par exemple :

Capacité = 2 GB facteur d'Over-provisionning = 2 Capacité après over-provisionning = 4 GB

Avec cette configuration, en supposant que vous déployez 3 VM de 1 GB chacune :

Utilisé = 3 GB Libre = 1 GB

L'administrateur peut spécifier un facteur de sur-allocation de mémoire, et peut spécifier à la fois les facteurs de sur-allocation de CPU et de mémoire par cluster.

Dans n'importe quel cloud, le nombre optimal de VM par hôte est affecté par des variables comme l'hyperviseur, le stockage et la configuration matérielle. Ils peuvent être différent pour chaque cluster dans le même cloud. Un simple paramètre global de sur-allocation ne peut pas représenter le meilleur moyen pour tous les différents cluster du cloud. Il doit être défini au niveau du plus petit dénominateur commun. La configuration par cluster fournie une granularité plus fine pour une meilleur utilisation des ressources, sans relation avec l'endroit où l'algorithme de placement de CloudStack décide de placer une VM.

Les paramètres de sur-allocation peuvent être utilisés avec les ressources dédiées (assigner un cluster spécifique à un compte) pour effectivement offrir des niveaux de services différents à différents comptes. Par exemple, un compte payant pour un niveau de service plus cher peut être assigné à un cluster dédié avec un rapport de sur-allocation de 1, et un compte moins onéreux à un cluster avec un rapport de 2.

Lorsqu'un nouvel hôte est ajouté à un cluster, CloudStack supposera que l'hôte à la capacité d'exécuter la sur-allocation en CPU et en RAM configurée pour ce cluster. Il appartient à l'administrateur d'être sur que l'hôte est actuellement approprié au niveau de sur-allocation paramétré.

Limitations de la sur-allocation pour XenServer et KVM

— Dans XenServer, à cause d'une limitation de cet hyperviseur, vous ne pouvez pas utiliser un facteur plus grand que 4.
— L'hyperviseur KVM ne peut pas gérer l'allocation de mémoire dynamique aux VM. CloudStack défini le minimum et le maximum de quantité de mémoire qu'une VM peut utiliser. L'hyperviseur ajuste la mémoire dans les limites définies en fonction de la contention de la mémoire.

Pré-requis pour la sur-allocation

Plusieurs conditions préalables sont requises pour que la sur-allocation fonctionne correctement. Cette fonctionnalité est dépendante du type d'OS, des capacités de l'hyperviseur et de certains scripts. Il est de la responsabilité de l'administrateur de s'assurer que ces exigences soient réunies.

Driver pour le ballooning

Toutes les machines virtuelles devraient avoir un driver de ballooning installé. L'hyperviseur communique avec le driver du ballooning pour libérer ou rendre la mémoire disponible à une machine virtuelle.

XenServer Le driver de ballooning sont fournis par les xen pv ou les drivers PVHVM. Les drivers pvhvm xen sont inclus dans les kernels linux supérieurs à 2.6.36+.

VMware Les drivers de ballooning sont fournis par les VMware tools. Toutes les VM qui sont déployées dans un cluster avec sur-allocation devraient avoir les VMware tools d'installés.

KVM Toutes les VM doivent supporter les drivers virtio. Ces drivers sont installés dans toutes les versions du kernel Linux 2.6.25 et supérieur. L'administrateur doit paramètrer CONFIG_VIRTIO_BALLOON=y dans la configuration virtio.

Capacités de l'hyperviseur

L'hyperviseur doit être capable d'utiliser le memory-balloning.

XenServer La capacité DMC (Dynamic Memory Control) de l'hyperviseur devrait être activée. Seul XenServer Advanced et versions supérieures disposent de cette fonctionnalité.

VMware, KVM Le memory ballooning est supporté par défaut.

Fixer les ratios de sur-allocation

Il existe deux façons pour l'administrateur racine de définir des rapport de sur-allocation du CPU et de la RAM. Tout d'abord, les paramètres de configuration globaux cpu.overprovisioning.factor et mem.overprovisioning.factor seront appliqués lors de la création d'un nouveau cluster. Puis les facteurs pourront être modifiés pour un cluster existant.

Seules les machines virtuelles déployées après la modification sont affectées par le nouveau paramètre. Si vous voulez que les machines virtuelles déployées avant la modification adoptent le nouveau facteur de sur-allocation, vous devrez arrêter et redémarrer les machines virtuelles. Lorsque cela est fait, CloudStack recalculera ou évaluera les capacités utilisées et réservées en fonction des nouveaux facteurs de sur-allocation pour s'assurer que CloudStack calcule correctement la quantité de capacité disponible.

Note : Il est plus prudent de ne pas déployer de nouvelles machines virtuelles supplémentaires pendant que le re-calcul des capacités est en cours, au cas où les nouvelles valeurs de la capacité disponible ne seraient pas suffisamment élevées pour accueillir les nouvelles machines virtuelles. Il suffit d'attendre que les nouvelles valeurs utilisées / disponibles deviennent disponibles, pour être sûr qu'il y ait de la place pour toutes les nouvelles machines virtuelles que vous désirez.

Pour changer les facteurs de sur-allocation pour un cluster existant :

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Sous Clusters, cliquer sur Voir tout.
4. Sélectionner le cluster sur lequel vous voulez travailler, et cliquer sur le bouton Editer.
5. Saisissez vos multiplicateurs de sur-allocation désirés dans les champs CPU overcommit ratio et RAM overcommit ratio. La valeur indiquée initialement dans ces champs est la valeur par défaut héritée des paramètres de configuration globaux.

   Note : Dans XenServer, à cause d'une limitation de cet hyperviseur, vous ne pouvez pas utiliser un facteur plus grand que 4.

Limites d'offre de service et sur-allocation

Les limites d'offre de service (par exemple 1 GHz, 1 coeur) sont strictement appliquées pour le nombre de noyaux. Par exemple, un invité disposant d'une offre de service d'un coeur n'aura qu'un seul coeur disponible, indépendamment de toute autre activité sur l'hôte.

Les limites de service offertes en gigahertz sont appliquées uniquement lorsqu'il y a contention des ressources CPU. Par exemple, supposons qu'un invité ait été créé avec une offre de service de 1 GHz sur un hôte disposant de coeurs à 2 GHz et que cet invité est le seul client en cours d'exécution sur l'hôte. L'invité aura à sa disposition la totalité des 2 GHz. Lorsque plusieurs invités tentent d'utiliser le CPU, un facteur de pondération est utilisé pour planifier les ressources CPU. Le poids est basé sur la vitesse d'horloge de l'offre de service. Les clients reçoivent une allocation CPU proportionnelle au GHz de leur offre de service. Par exemple, un invité créé à partir d'une offre de service à 2 GHz recevra l'équivalent de deux fois l'allocation CPU d'un invité créé à partir d'une offre de service à 1 GHz. CloudStack n'effectue pas de sur-allocation de la mémoire.

8.1.9 Approvisionnement de VLAN

CloudStack crée et détruit automatiquement les interfaces reliées aux VLAN sur les hôtes. En général, l'administrateur n'a pas besoin de gérer ce processus.

CloudStack gère les VLAN différemment en fonction du type d'hyperviseur. Pour XenServer ou KVM, les VLAN sont créés uniquement sur les hôtes où ils seront utilisés, puis ils sont détruits lorsque tous les invités qui en ont besoin ont été supprimés ou déplacés vers un autre hôte.

Pour vSphere, les VLAN sont provisionnés sur tous les hôtes du cluster, même s'il n'y a pas d'invité nécessitant le VLAN en cours d'exécution sur un hôte particulier. Cela permet à l'administrateur d'effectuer une migration à chaud et autres fonctions du vCenter sans avoir à créer le VLAN sur l'hôte de destination. De plus, les VLAN ne sont pas supprimés des hôtes lorsqu'ils ne sont plus nécessaires.

Vous pouvez utiliser les mêmes VLAN sur différents réseaux physiques à condition que chaque réseau physique possède sa propre infrastructure de niveau 2, comme des commutateurs. Par exemple, vous pouvez spécifier une plage de VLAN de 500 à 1000 lors du déploiement des réseaux physiques A et B dans une configuration de type zone avancée. Cette fonctionnalité vous permet de configurer une infrastructure physique de niveau 2 supplémentaire sur une carte réseau physique différente et d'utiliser le même ensemble de VLAN si vous veniez à être à court de VLAN. Un autre avantage est que vous pouvez utiliser le même ensemble d'IP pour différents clients, chacun avec leurs propres routeurs et réseaux invités sur différentes interfaces physiques.

Exemple d'allocation de VLAN

Les VLAN sont requis pour le trafic public et privé. Voici un exemple de schéma d'allocation VLAN :

ID VLAN	Type de trafic	Portée
Moins de 500	Trafic de gestion.	Réservé pour des besoins administratifs. Le logiciel CloudStack, les hyperviseurs et les VMs système peuvent y accéder.
500-599	VLAN transportant le trafic public.	Comptes CloudStack.
600-799	VLAN transportant le trafic invité.	Comptes CloudStack. Le VLAN spécifique au compte est choisi depuis cette réserve.
800-899	VLAN transportant le trafic invité.	Comptes CloudStack. Le VLAN spécifique au compte choisi par l'administrateur CloudStack pour être assigneé à ce compte.
900-999	VLAN transportant le trafic public.	Comptes CloudStack. Peut être limité à un projet, à un domaine ou pour tous les comptes.
Supérieur à 1000	Réservé pour un usage futur.	

Ajouter des intervalles de VLAN non contiguës.

CloudStack vous offre la flexibilité d'ajouter des plages de VLAN non contiguës à votre réseau. L'administrateur peut mettre à jour une plage de VLAN existante ou ajouter plusieurs plages de VLAN non contiguës lors de la création d'une zone. Vous pouvez également utiliser l'API UpdatephysicalNetwork pour étendre la plage de VLAN.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. S'assurer que l'intervalle VLAN n'existe pas déjà.
3. Choisissez Infrastructure dans le panneau de navigation à gauche.
4. Sur Zones, cliquer sur Voir plus, puis cliquer sur la zone avec laquelle vous voulez travailler.
5. Cliquer sur le réseau physique.
6. Dans le noeud Invité du diagramme, cliquer sur Configurer.
7. Cliquer sur Editer  .
   Le champ intervalle VLAN est maintenant éditable.
8. Spécifier le début et la fin de l'intervalle VLAN dans une liste séparée par une virgule.
   Spécifier tous les VLAN que vous voulez utiliser, les VLAN non spécifiés seront supprimés si vous ajoutez une nouvelle plage à la liste existante.

9. Cliquer sur Appliquer.

Assigner les VLAN à des réseaux isolés.

CloudStack vous offre la possibilité de contrôler l'assignation de VLAN aux réseaux isolés. En tant qu'administrateur racine, vous pouvez attribuer un ID de VLAN lorsqu'un réseau est créé, comme c'est le cas pour les réseaux partagés.

Le comportement précédent est également pris en charge - un VLAN est alloué de façon aléatoire à un réseau à partir de la plage VNET du réseau physique lorsque le réseau passe à l'état Implémenté. Le VLAN est libéré dans le pool VNET lorsque le réseau s'arrête par le Network Garbage Collection. Le VLAN peut être réutilisé soit par le même réseau lors de sa remise en œuvre, soit par n'importe quel autre réseau. Sur chaque implémentation ultérieure d'un réseau, un nouveau VLAN peut être assigné.

Seul l'administrateur racine peut attribuer des VLAN car les utilisateurs réguliers ou l'administrateur de domaine ne connaissent pas la topologie du réseau physique. Ils ne peuvent même pas voir quel VLAN est affecté à un réseau.

Pour vous permettre d'assigner des VLAN à des réseaux isolés,

1. Créer une offre de réseau en spécifiant ce qui suit :
   — **Type d'invité** : Sélectionner Isolé.
   — **Spécifier le VLAN** : Sélectionner l'option.
   Pour plus d'informations, voir le Guide d'Installation de CloudStack.
2. Utiliser l'offre de réseau, créer un réseau.
   Vous pouvez créer un tier VPC ou un réseau isolé.
3. Spécifier le VLAN lorsque vous créez le réseau.
   Lorsqu'un VLAN est spécifié, un CIDR et une passerelle sont affectés à ce réseau et l'état est changé à Setup. Dans cet état, le réseau ne sera pas récupérés.

Note : Vous ne pouvez pas changer un VLAN une fois qu'il est affecté à un réseau. Le VLAN reste avec le réseau pendant tout son cycle de vie.

Gestion des Out-of-band

CloudStack fournit aux administrateurs racine la possibilité de configurer et d'utiliser les interfaces out-of-band supportées (par exemple, IPMI, iLO, DRAC, etc.) sur un hôte physique pour gérer les opérations d'alimentation de l'hôte telles que marche, arrêt, reset, etc. Par défaut, les controlleurs IPMI 2.0 sont pris en charge nativement par le pilote de gestion *IPMITOOL* out-of-band dans CloudStack qui utilise *ipmitool* pour effectuer des opérations de gestion IPMI 2.0.

Voici quelques paramètres globaux qui contrôlent différents aspects de cette fonctionnalité.

Configuration globale	Valeurs par défaut	Description
outofbandmanagement.action.timeout	60	Le délai d'attente de l'action du out of band management en secondes, configurable par cluster
outofbandmanagement.ipmitool.interface	lanplus	L'interface du pilote IpmiTool pour le out of band management à utiliser. Les valeurs valides sont : lan, lanplus, etc.
outofbandmanagement.ipmitool.path	/usr/bin/ipmitool	Le chemin de l'ipmitool du out of band management utilisé par le pilote de l'IpmiTool
outofbandmanagement.ipmitool.retries	1	L'option de nouvelle essais -R du pilote IpmiTool du out of band management
outofbandmanagement.sync.interval	300	L'intervalle en secondes du thread de synchronisation en arrière-plan du gestionnaire out of band.
outofbandmanagement.sync.poolsize	50	The out of band management background sync thread pool size 50

Une modification des paramètres *outofbandmanagement.sync.interval* ou‘ outofbandmanagement.sync.poolsize‘ requiert le redémarrage des serveurs de gestion puisque le pool de threads et un thread de synchronisation en arrière-plan (état d'alimentation) sont configurés pendant le chargement lorsque le serveur de gestion CloudStack démarre. Le reste des paramètres globaux peut être modifié sans nécessiter le redémarrage du ou des serveurs de gestion.

Le *Outofbandmanagement.sync.poolsize* est le nombre maximal de scanners ipmitool en arrière plan d'état d'alimentation pouvant être exécutés à la fois. En fonction du nombre maximal d'hôtes que vous avez, vous pouvez augmenter / diminuer la valeur en fonction de la quantité de stress que votre serveur hôte de gestion peut supporter. Il faudra calculer le plus grand nombre d'hôtes out-of-band activés par la formule * *outofbandmanagement.action.timeout* / *outofbandmanagement.sync.poolsize* secondes pour compléter une analyse de synchronisation de l'état d'alimentation en arrière-plan en un seul tour.

Pour utiliser cette fonctionnalité, l'administrateur racine doit d'abord configurer la gestion out-of-band pour un hôte à l'aide de l'interface utilisateur ou de l'API *configureOutOfBandManagement*. Ensuite, l'administrateur racine doit l'activer. La fonction peut être activée ou désactivée dans une zone, un cluster ou un hôte,

Une fois que le management out-of-band est configuré et activé pour un hôte (et pourvu qu'il ne soit pas désactivée au niveau de la zone ou du cluster), les administrateurs racines sont en mesure d'exécuter des actions de gestion de l'alimentation telles que marche, arrêt, réinitialisation, cycle, logiciel et statut.

Si un hôte est en mode maintenance, les administrateurs Root sont toujours autorisés à effectuer des actions de gestion d'allumage ou d'extinction mais dans l'interface une alerte est affichée.

CHAPITRE 9

Travailler avec le stockage

9.1 Travailler avec le stockage

9.1.1 Vue d'ensemble du stockage

CloudStack définit 2 types de stockage : primaire et secondaire. Le stockage primaire peut être accédé soit en iSCSI ou en NFS. En complément, le stockage directement attaché (DAS) peut être utilisé comme stockage primaire. Le stockage secondaire est toujours accédé en utilisant NFS.

Il n'y a pas de stockage éphémère dans CloudStack. Tous les volumes sur tous les noeuds sont persistents.

9.1.2 Stockage primaire

Cette section donne les concepts et les détails techniques sur le stockage primaire de CloudStack. Pour des informations sur la façon d'installer et de configurer le stockage primaire par l'interface CloudStack, consultez le guide d'installation.

"A propos du stockage primaire"

Meilleurs pratiques pour le stockage primaire

— La vitesse du stockage primaire va impacter les performances des invités. Si possible, choisissez des disques plus petits, avec des RPM plus élevés ou des disques SSD pour le stockage primaire.
— Il y a deux façons pour CloudStack d'exploiter le stockage primaire :
Static : This is CloudStack's traditional way of handling storage. In this model, a preallocated amount of storage (ex. a volume from a SAN) is given to CloudStack. CloudStack then permits many of its volumes to be created on this storage (can be root and/or data disks). If using this technique, ensure that nothing is stored on the storage. Adding the storage to CloudStack will destroy any existing data.
Dynamic : This is a newer way for CloudStack to manage storage. In this model, a storage system (rather than a preallocated amount of storage) is given to CloudStack. CloudStack, working in concert with a storage plug-in, dynamically creates volumes on the storage system and each volume on the storage system maps to a single CloudStack volume. This is highly useful for features such as storage Quality of Service. Currently this feature is supported for data disks (Disk Offerings).

Comportement à l'exécution du stockage primaire

Root volumes are created automatically when a virtual machine is created. Root volumes are deleted when the VM is destroyed. Data volumes can be created and dynamically attached to VMs. Data volumes are not deleted when VMs

are destroyed.

Administrators should monitor the capacity of primary storage devices and add additional primary storage as needed. See the Advanced Installation Guide.

Administrators add primary storage to the system by creating a CloudStack storage pool. Each storage pool is associated with a cluster or a zone.

With regards to data disks, when a user executes a Disk Offering to create a data disk, the information is initially written to the CloudStack database only. Upon the first request that the data disk be attached to a VM, CloudStack determines what storage to place the volume on and space is taken from that storage (either from preallocated storage or from a storage system (ex. a SAN), depending on how the primary storage was added to CloudStack).

Hypervisor Support for Primary Storage

The following table shows storage options and parameters for different hypervisors.

Media de stockage \ hyperviseur	VMware vSphere	Citrix XenServer	KVM	Hyper-V
Format des disques, des modèles et des instantanés	VMDK	VHD	QCOW2	VHD Snapshots are not supported.
iSCSI support	VMFS	Clustered LVM	Oui, par point de montage partagé	Non
Fiber Channel support	VMFS	Yes, via Existing SR	Oui, par point de montage partagé	Non
Support NFS	Oui	Oui	Oui	Non
Local storage support	Oui	Oui	Oui	Oui
Storage over-provisioning	NFS et iSCSI	NFS	NFS	Non
SMB/CIFS	Non	Non	Non	Oui
Ceph/RBD	Non	Non	Oui	Non

XenServer uses a clustered LVM system to store VM images on iSCSI and Fiber Channel volumes and does not support over-provisioning in the hypervisor. The storage server itself, however, can support thin-provisioning. As a result the CloudStack can still support storage over-provisioning by running on thin-provisioned storage volumes.

KVM supports “Shared Mountpoint” storage. A shared mountpoint is a file system path local to each server in a given cluster. The path must be the same across all Hosts in the cluster, for example /mnt/primary1. This shared mountpoint is assumed to be a clustered filesystem such as OCFS2. In this case the CloudStack does not attempt to mount or unmount the storage as is done with NFS. The CloudStack requires that the administrator insure that the storage is available

With NFS storage, CloudStack manages the overprovisioning. In this case the global configuration parameter storage.overprovisioning.factor controls the degree of overprovisioning. This is independent of hypervisor type.

Local storage is an option for primary storage for vSphere, XenServer, and KVM. When the local disk option is enabled, a local disk storage pool is automatically created on each host. To use local storage for the System Virtual Machines (such as the Virtual Router), set system.vm.use.local.storage to true in global configuration.

CloudStack supports multiple primary storage pools in a Cluster. For example, you could provision 2 NFS servers in primary storage. Or you could provision 1 iSCSI LUN initially and then add a second iSCSI LUN when the first approaches capacity.

Storage Tags

Storage may be “tagged”. A tag is a text string attribute associated with primary storage, a Disk Offering, or a Service Offering. Tags allow administrators to provide additional information about the storage. For example, that is a “SSD”

or it is “slow”. Tags are not interpreted by CloudStack. They are matched against tags placed on service and disk offerings. CloudStack requires all tags on service and disk offerings to exist on the primary storage before it allocates root or data disks on the primary storage. Service and disk offering tags are used to identify the requirements of the storage that those offerings have. For example, the high end service offering may require “fast” for its root disk volume.

The interaction between tags, allocation, and volume copying across clusters and pods can be complex. To simplify the situation, use the same set of tags on the primary storage for all clusters in a pod. Even if different devices are used to present those tags, the set of exposed tags can be the same.

Maintenance Mode for Primary Storage

Primary storage may be placed into maintenance mode. This is useful, for example, to replace faulty RAM in a storage device. Maintenance mode for a storage device will first stop any new guests from being provisioned on the storage device. Then it will stop all guests that have any volume on that storage device. When all such guests are stopped the storage device is in maintenance mode and may be shut down. When the storage device is online again you may cancel maintenance mode for the device. The CloudStack will bring the device back online and attempt to start all guests that were running at the time of the entry into maintenance mode.

9.1.3 Stockage secondaire

This section gives concepts and technical details about CloudStack secondary storage. For information about how to install and configure secondary storage through the CloudStack UI, see the Advanced Installation Guide.

“About Secondary Storage”

9.1.4 Working With Volumes

A volume provides storage to a guest VM. The volume can provide for a root disk or an additional data disk. CloudStack supports additional volumes for guest VMs.

Volumes are created for a specific hypervisor type. A volume that has been attached to guest using one hypervisor type (e.g, XenServer) may not be attached to a guest that is using another hypervisor type, for example :vSphere, KVM. This is because the different hypervisors use different disk image formats.

CloudStack defines a volume as a unit of storage available to a guest VM. Volumes are either root disks or data disks. The root disk has “/” in the file system and is usually the boot device. Data disks provide for additional storage, for example : “/opt” or “D :”. Every guest VM has a root disk, and VMs can also optionally have a data disk. End users can mount multiple data disks to guest VMs. Users choose data disks from the disk offerings created by administrators. The user can create a template from a volume as well ; this is the standard procedure for private template creation. Volumes are hypervisor-specific : a volume from one hypervisor type may not be used on a guest of another hypervisor type.

Note : CloudStack supports attaching up to
- 13 data disks on XenServer hypervisor versions 6.0 and above, And all versions of VMware.
- 64 data disks on Hyper-V.
- 6 data disks on other hypervisor types.

Creating a New Volume

You can add more data disk volumes to a guest VM at any time, up to the limits of your storage capacity. Both CloudStack administrators and users can add volumes to VM instances. When you create a new volume, it is stored as an entity in CloudStack, but the actual storage resources are not allocated on the physical storage device until you

attach the volume. This optimization allows the CloudStack to provision the volume nearest to the guest that will use it when the first attachment is made.

Using Local Storage for Data Volumes

You can create data volumes on local storage (supported with XenServer, KVM, and VMware). The data volume is placed on the same host as the VM instance that is attached to the data volume. These local data volumes can be attached to virtual machines, detached, re-attached, and deleted just as with the other types of data volume.

Local storage is ideal for scenarios where persistence of data volumes and HA is not required. Some of the benefits include reduced disk I/O latency and cost reduction from using inexpensive local disks.

In order for local volumes to be used, the feature must be enabled for the zone.

You can create a data disk offering for local storage. When a user creates a new VM, they can select this disk offering in order to cause the data disk volume to be placed in local storage.

You can not migrate a VM that has a volume in local storage to a different host, nor migrate the volume itself away to a different host. If you want to put a host into maintenance mode, you must first stop any VMs with local data volumes on that host.

To Create a New Volume

1. Log in to the CloudStack UI as a user or admin.
2. In the left navigation bar, click Storage.
3. Dans la Sélection de Vue, choisissez Volumes.
4. To create a new volume, click Add Volume, provide the following details, and click OK.
   — Name. Give the volume a unique name so you can find it later.
   — Availability Zone. Where do you want the storage to reside ? This should be close to the VM that will use the volume.
   — Disk Offering. Choose the characteristics of the storage.
   The new volume appears in the list of volumes with the state “Allocated.” The volume data is stored in CloudStack, but the volume is not yet ready for use
5. To start using the volume, continue to Attaching a Volume

Uploading an Existing Volume to a Virtual Machine

Existing data can be made accessible to a virtual machine. This is called uploading a volume to the VM. For example, this is useful to upload data from a local file system and attach it to a VM. Root administrators, domain administrators, and end users can all upload existing volumes to VMs.

The upload is performed using HTTP. The uploaded volume is placed in the zone’s secondary storage

You cannot upload a volume if the preconfigured volume limit has already been reached. The default limit for the cloud is set in the global configuration parameter max.account.volumes, but administrators can also set per-domain limits that are different from the global default. See Setting Usage Limits

To upload a volume :

1. (Optional) Create an MD5 hash (checksum) of the disk image file that you are going to upload. After uploading the data disk, CloudStack will use this value to verify that no data corruption has occurred.
2. Log in to the CloudStack UI as an administrator or user
3. In the left navigation bar, click Storage.
4. Click Upload Volume.

5. Provide the following :
   — Name and Description. Any desired name and a brief description that can be shown in the UI.
   — Availability Zone. Choose the zone where you want to store the volume. VMs running on hosts in this zone can attach the volume.
   — Format. Choose one of the following to indicate the disk image format of the volume.

Hypervisor	Disk Image Format
XenServer	VHD
VMware	OVA
KVM	QCOW2

   — URL. The secure HTTP or HTTPS URL that CloudStack can use to access your disk. The type of file at the URL must match the value chosen in Format. For example, if Format is VHD, the URL might look like the following :
   `http://yourFileServerIP/userdata/myDataDisk.vhd`
   — MD5 checksum. (Optional) Use the hash that you created in step 1.
6. Wait until the status of the volume shows that the upload is complete. Click Instances - Volumes, find the name you specified in step 5, and make sure the status is Uploaded.

Attacher un Volume

Vous pouvez attacher un volume à une VM pour lui fournir plus d'espace disque de stockage. Vous pouvez attacher un volume lors de sa création, lorsque vous déplacer un volume d'une VM existante vers une autre, ou après avoir migré le volume d'un groupe de stockage à un autre.

1. Log in to the CloudStack UI as a user or admin.
2. Dans la navigation à gauche, cliquez sur Stockage.
3. Dans la Sélection de Vue, choisissez Volumes.
4. Click the volume name in the Volumes list, then click the Attach Disk button 
5. Dans la popup d'instance, choisissez la VM sur laquelle vous désirez attacher le volume. Vous ne verrez que les instances sur lesquelles vous êtes autorisé à attacher le volume ; par exemple, un utilisateur ne verra que ses propres instances, mais l'administrateur aura plus de choix.
6. Lorsqu'un volume a été attaché, vous devriez pouver le voir en cliquant sur instances, puis le nom de l'instance et "Voir les Volumes".

Detaching and Moving Volumes

Note : This procedure is different from moving volumes from one storage pool to another as described in *"VM Storage Migration"*.

A volume can be detached from a guest VM and attached to another guest. Both CloudStack administrators and users can detach volumes from VMs and move them to other VMs.

If the two VMs are in different clusters, and the volume is large, it may take several minutes for the volume to be moved to the new VM.

1. Log in to the CloudStack UI as a user or admin.
2. In the left navigation bar, click Storage, and choose Volumes in Select View. Alternatively, if you know which VM the volume is attached to, you can click Instances, click the VM name, and click View Volumes.
3. Click the name of the volume you want to detach, then click the Detach Disk button. 
4. To move the volume to another VM, follow the steps in *"Attaching a Volume"*.

VM Storage Migration

Supported in XenServer, KVM, and VMware.

Note : This procedure is different from moving disk volumes from one VM to another as described in *"Detaching and Moving Volumes"*.

You can migrate a virtual machine's root disk volume or any additional data disk volume from one storage pool to another in the same zone.

You can use the storage migration feature to achieve some commonly desired administration goals, such as balancing the load on storage pools and increasing the reliability of virtual machines by moving them away from any storage pool that is experiencing issues.

On XenServer and VMware, live migration of VM storage is enabled through CloudStack support for XenMotion and vMotion. Live storage migration allows VMs to be moved from one host to another, where the VMs are not located on storage shared between the two hosts. It provides the option to live migrate a VM's disks along with the VM itself. It is possible to migrate a VM from one XenServer resource pool / VMware cluster to another, or to migrate a VM whose disks are on local storage, or even to migrate a VM's disks from one storage repository to another, all while the VM is running.

Note : Because of a limitation in VMware, live migration of storage for a VM is allowed only if the source and target storage pool are accessible to the source host ; that is, the host where the VM is running when the live migration operation is requested.

Migrating a Data Volume to a New Storage Pool

There are two situations when you might want to migrate a disk :

— Move the disk to new storage, but leave it attached to the same running VM.
— Detach the disk from its current VM, move it to new storage, and attach it to a new VM.

Migrating Storage For a Running VM (Supported on XenServer and VMware)

1. Log in to the CloudStack UI as a user or admin.
2. In the left navigation bar, click Instances, click the VM name, and click View Volumes.
3. Click the volume you want to migrate.
4. Detach the disk from the VM. See *"Detaching and Moving Volumes"* but skip the "reattach" step at the end. You will do that after migrating to new storage.
5. Click the Migrate Volume button  and choose the destination from the dropdown list.
6. Watch for the volume status to change to Migrating, then back to Ready.

Migrating Storage and Attaching to a Different VM

1. Log in to the CloudStack UI as a user or admin.
2. Detach the disk from the VM. See *"Detaching and Moving Volumes"* but skip the "reattach" step at the end. You will do that after migrating to new storage.
3. Click the Migrate Volume button  and choose the destination from the dropdown list.

4. Watch for the volume status to change to Migrating, then back to Ready. You can find the volume by clicking Storage in the left navigation bar. Make sure that Volumes is displayed at the top of the window, in the Select View dropdown.
5. Attach the volume to any desired VM running in the same cluster as the new storage server. See *"Attaching a Volume"*

Migrating a VM Root Volume to a New Storage Pool

(XenServer, VMware) You can live migrate a VM's root disk from one storage pool to another, without stopping the VM first.

(KVM) When migrating the root disk volume, the VM must first be stopped, and users can not access the VM. After migration is complete, the VM can be restarted.

1. Log in to the CloudStack UI as a user or admin.
2. In the left navigation bar, click Instances, and click the VM name.
3. (KVM only) Stop the VM.
4. Click the Migrate button  and choose the destination from the dropdown list.

   Note : If the VM's storage has to be migrated along with the VM, this will be noted in the host list. CloudStack will take care of the storage migration for you.

5. Watch for the volume status to change to Migrating, then back to Running (or Stopped, in the case of KVM). This can take some time.
6. (KVM only) Restart the VM.

Resizing Volumes

CloudStack provides the ability to resize data disks ; CloudStack controls volume size by using disk offerings. This provides CloudStack administrators with the flexibility to choose how much space they want to make available to the end users. Volumes within the disk offerings with the same storage tag can be resized. For example, if you only want to offer 10, 50, and 100 GB offerings, the allowed resize should stay within those limits. That implies if you define a 10 GB, a 50 GB and a 100 GB disk offerings, a user can upgrade from 10 GB to 50 GB, or 50 GB to 100 GB. If you create a custom-sized disk offering, then you have the option to resize the volume by specifying a new, larger size.

Additionally, using the resizeVolume API, a data volume can be moved from a static disk offering to a custom disk offering with the size specified. This functionality allows those who might be billing by certain volume sizes or disk offerings to stick to that model, while providing the flexibility to migrate to whatever custom size necessary.

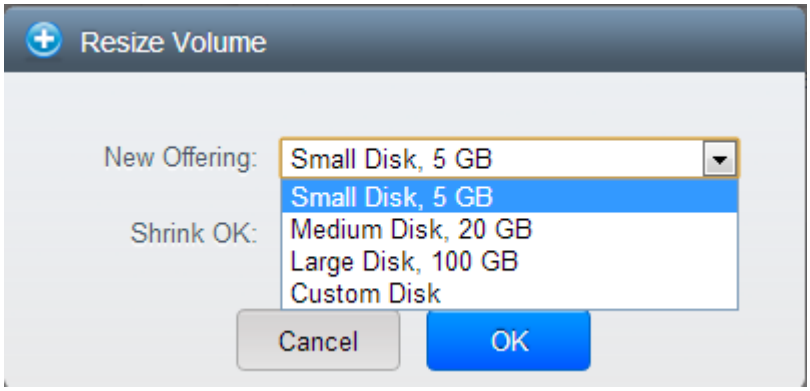
This feature is supported on KVM, XenServer, and VMware hosts. However, shrinking volumes is not supported on VMware hosts.

Before you try to resize a volume, consider the following :
- The VMs associated with the volume are stopped.
- The data disks associated with the volume are removed.
- When a volume is shrunk, the disk associated with it is simply truncated, and doing so would put its content at risk of data loss. Therefore, resize any partitions or file systems before you shrink a data disk so that all the data is moved off from that disk.

To resize a volume :

1. Log in to the CloudStack UI as a user or admin.
2. In the left navigation bar, click Storage.
3. Dans la Sélection de Vue, choisissez Volumes.

4. Select the volume name in the Volumes list, then click the Resize Volume button 
5. In the Resize Volume pop-up, choose desired characteristics for the storage.



   (a) If you select Custom Disk, specify a custom size.

   (b) Click Shrink OK to confirm that you are reducing the size of a volume.
   This parameter protects against inadvertent shrinking of a disk, which might lead to the risk of data loss. You must sign off that you know what you are doing.

6. Cliquez sur OK.

Reset VM to New Root Disk on Reboot

You can specify that you want to discard the root disk and create a new one whenever a given VM is rebooted. This is useful for secure environments that need a fresh start on every boot and for desktops that should not retain state. The IP address of the VM will not change due to this operation.

To enable root disk reset on VM reboot :

When creating a new service offering, set the parameter isVolatile to True. VMs created from this service offering will have their disks reset upon reboot. See “Creating a New Compute Offering”.

Volume Deletion and Garbage Collection

The deletion of a volume does not delete the snapshots that have been created from the volume

When a VM is destroyed, data disk volumes that are attached to the VM are not deleted.

Volumes are permanently destroyed using a garbage collection process. The global configuration variables expunge.delay and expunge.interval determine when the physical deletion of volumes will occur.

- *expunge.delay* : determines how old the volume must be before it is destroyed, in seconds
- *expunge.interval* : determines how often to run the garbage collection check

Administrators should adjust these values depending on site policies around data retention.

9.1.5 Working with Volume Snapshots

(Supported for the following hypervisors : **XenServer**, **VMware vSphere**, and **KVM**)

CloudStack supports snapshots of disk volumes. Snapshots are a point-in-time capture of virtual machine disks. Memory and CPU states are not captured. If you are using the Oracle VM hypervisor, you can not take snapshots, since OVM does not support them.

Snapshots may be taken for volumes, including both root and data disks (except when the Oracle VM hypervisor is used, which does not support snapshots). The administrator places a limit on the number of stored snapshots per user.

Users can create new volumes from the snapshot for recovery of particular files and they can create templates from snapshots to boot from a restored disk.

Users can create snapshots manually or by setting up automatic recurring snapshot policies. Users can also create disk volumes from snapshots, which may be attached to a VM like any other disk volume. Snapshots of both root disks and data disks are supported. However, CloudStack does not currently support booting a VM from a recovered root disk. A disk recovered from snapshot of a root disk is treated as a regular data disk ; the data on recovered disk can be accessed by attaching the disk to a VM.

A completed snapshot is copied from primary storage to secondary storage, where it is stored until deleted or purged by newer snapshot.

How to Snapshot a Volume

1. Log in to the CloudStack UI as a user or administrator.
2. In the left navigation bar, click Storage.
3. In Select View, be sure Volumes is selected.
4. Click the name of the volume you want to snapshot.
5. Click the Snapshot button. 

Automatic Snapshot Creation and Retention

(Supported for the following hypervisors : **XenServer**, **VMware vSphere**, and **KVM**)

Users can set up a recurring snapshot policy to automatically create multiple snapshots of a disk at regular intervals. Snapshots can be created on an hourly, daily, weekly, or monthly interval. One snapshot policy can be set up per disk volume. For example, a user can set up a daily snapshot at 02 :30.

With each snapshot schedule, users can also specify the number of scheduled snapshots to be retained. Older snapshots that exceed the retention limit are automatically deleted. This user-defined limit must be equal to or lower than the global limit set by the CloudStack administrator. See “Globally Configured Limits”. The limit applies only to those snapshots that are taken as part of an automatic recurring snapshot policy. Additional manual snapshots can be created and retained.

Incremental Snapshots and Backup

Snapshots are created on primary storage where a disk resides. After a snapshot is created, it is immediately backed up to secondary storage and removed from primary storage for optimal utilization of space on primary storage.

CloudStack does incremental backups for some hypervisors. When incremental backups are supported, every N backup is a full backup.

	VMware vSphere	Citrix XenServer	KVM
Support incremental backup	Non	Oui	Non

Volume Status

When a snapshot operation is triggered by means of a recurring snapshot policy, a snapshot is skipped if a volume has remained inactive since its last snapshot was taken. A volume is considered to be inactive if it is either detached or attached to a VM that is not running. CloudStack ensures that at least one snapshot is taken since the volume last became inactive.

When a snapshot is taken manually, a snapshot is always created regardless of whether a volume has been active or not.

Snapshot Restore

There are two paths to restoring snapshots. Users can create a volume from the snapshot. The volume can then be mounted to a VM and files recovered as needed. Alternatively, a template may be created from the snapshot of a root disk. The user can then boot a VM from this template to effect recovery of the root disk.

Snapshot Job Throttling

When a snapshot of a virtual machine is requested, the snapshot job runs on the same host where the VM is running or, in the case of a stopped VM, the host where it ran last. If many snapshots are requested for VMs on a single host, this can lead to problems with too many snapshot jobs overwhelming the resources of the host.

To address this situation, the cloud's root administrator can throttle how many snapshot jobs are executed simultaneously on the hosts in the cloud by using the global configuration setting concurrent.snapshots.threshold.perhost. By using this setting, the administrator can better ensure that snapshot jobs do not time out and hypervisor hosts do not experience performance issues due to hosts being overloaded with too many snapshot requests.

Set concurrent.snapshots.threshold.perhost to a value that represents a best guess about how many snapshot jobs the hypervisor hosts can execute at one time, given the current resources of the hosts and the number of VMs running on the hosts. If a given host has more snapshot requests, the additional requests are placed in a waiting queue. No new snapshot jobs will start until the number of currently executing snapshot jobs falls below the configured limit.

The admin can also set job.expire.minutes to place a maximum on how long a snapshot request will wait in the queue. If this limit is reached, the snapshot request fails and returns an error message.

VMware Volume Snapshot Performance

When you take a snapshot of a data or root volume on VMware, CloudStack uses an efficient storage technique to improve performance.

A snapshot is not immediately exported from vCenter to a mounted NFS share and packaged into an OVA file format. This operation would consume time and resources. Instead, the original file formats (e.g., VMDK) provided by vCenter are retained. An OVA file will only be created as needed, on demand. To generate the OVA, CloudStack uses information in a properties file (*.ova.meta) which it stored along with the original snapshot data.

Note : For upgrading customers : This process applies only to newly created snapshots after upgrade to CloudStack 4.2. Snapshots that have already been taken and stored in OVA format will continue to exist in that format, and will continue to work as expected.

Travailler avec les machines virtuelles systèmes

10.1 Travailler avec les machines virtuelles systèmes

CloudStack utilise divers types de machines virtuelles systèmes pour effectuer des tâches dans le cloud. En général, CloudStack gère ces VMs systèmes et les créé, démarre, arrête en fonction des changements et des besoins immédiats. Toutefois, l'administrateur devrait les connaître et leur rôle pour aider dans le dépannage des problèmes.

10.1.1 Le modèle de VM système

Les VMs systèmes proviennent toutes du même modèle. La VM système dispose des caractéristiques suivantes :

- Debian 7.8 ("wheezy"), noyau 3.2.0 avec les derniers patchs de sécurité du dépôts APT de sécurité de Debian
- Elle a le minimum d'ensemble de paquets installés réduisant ainsi la surface d'attaque
- 64 bits pour des performances améliorées sur Xen/VMware
- noyau pvops avec les drivers PV Xen, les drivers KVM virtio et les outils VMware pour des performances optimum sur tous les hyperviseurs
- les outils Xen inclus permettre un contrôle des performances
- Les dernières versions de HAProxy, iptables, IPsec et Apache depuis les dépots debian assurent une sécurité et une vitesse améliorées
- Les dernières version de la JRE depuis Sun/Oracle garantissent la sécurité et la vitesse

10.1.2 Changer le modèle de la VM système par défaut

Utiliser le modèle 64 bits devrait être utilisé avec une offre de service d'au moins 512Mo de mémoire.

1. En fonction de l'hyperviseur que vous utilisés, télécharger le modèle 64 bits depuis l'emplacement suivant :

Hyperviseur	Emplacement de téléchargement
XenServer	http://cloudstack.apt-get.eu/systemvm/4.6/systemvm64template-4.6.0-xen.vhd.bz2
KVM	http://cloudstack.apt-get.eu/systemvm/4.6/systemvm64template-4.6.0-kvm.qcow2.bz2
VMware	http://cloudstack.apt-get.eu/systemvm/4.6/systemvm64template-4.6.0-vmware.ova
Hyper-V	http://cloudstack.apt-get.eu/systemvm/4.6/systemvm64template-4.6.0-hyperv.vhd.zip

2. En tant qu'administrateur, se connecter dans l'interface CloudStack
3. Enregistrer un modèle 64 bits
   Par exemple : KVM64bitTemplate
4. Pendant l'enregistrement du modèle, sélectionner Routage.
5. Naviguer jusqu'à Infrastructure > Zone > Paramètres

6. Saisir le nom du modèle 64 bits, KVM64bitTemplate, dans le paramètre global *''router.template.kvm''*.
   Si vous utilisez un modèle 64 bits XenServer, saisir le nom dans le paramètre global *''router.template.xen''*.
   N'importe quel routeur virtuel créé dans cette Zone choisira automatiquement ce template.
7. Redémarrez votre serveur de gestion.

10.1.3 Support de VM Systèmes multiple pour VMware

Toute zone CloudStack a une seule VM système pour les tâches de traitement de modèles, comme le téléchargement des modèles et le téléchargement des ISOs. Dans une zone où VMware est utilisée, des VMs systèmes additionnelles peuvent être lancée pour effectuer des tâches spécifiques à VMware comme prendre des instantannés et créer des modèles privés. Le serveur de gestion CloudStack lance des VMs Systèmes additionnelles pour des tâches spécifiques à VMware lorsque la charge augmente. Le serveur de gestion surveillent et jauge toutes les commandes envoyées à ces VMs systèmes et effectue une répartition de charge dynamique et augmente proportionnellement les VMs systèmes.

10.1.4 Console Proxy

La console Proxy est un type de machine virtuelle système qui a un rôle dans la visualisation de la console via l'interface Web. Elle connecte le navigateur de l'utilisateur au port VNC rendu disponible via l'hyperviseur pour la console de l'invité. Les deux interfaces web administrateur et utilisateur final propose la connexion à la console.

Cliquer sur l'icône console fait apparaître une nouvelle fenêtre. Le code AJAX téléchargé dans cette fenêtre fait référence à l'adresse IP publique de la VM Console Proxy. Il y a exactement une adresse IP publique allouée par VM Console Proxy. L'application AJAX se connecte à cette IP. La console proxy mandate alors la connexion au port VNC pour la VM demandée sur l'hôte gérant l'invité.

Note : Les hyperviseurs vont avoir plusieurs ports dédiés à l'utilisation de VNC si bien que plusieurs sessions VNC peuvent être ouvertes simultanément.

Il n'y a jamais aucun trafic vers l'adresse IP virtuelle de l'invité, et il n'y a pas besoin d'activer VNC dans l'invité lui-même.

La VM console proxy va régulièrement reporter son compte de sessions actives au serveur de gestion. L'intervalle par défaut est de 5 secondes. Cela peut être modifié via la configuration standard du serveur de gestion avec le paramètre consoleproxy.loadscan.interval.

L'affectation d'une VM invitée à une console proxy est déterminée par premièrement si la VM invitée a une session précédente qui est associée à une console proxy. Si c'est le cas, le serveur de gestion va affecter cette VM invitée à la VM Console Proxy cible sans regard sur la charge de la VM Proxy. En cas d'échec, la première VM Console Proxy disponible qui a la capacité d'accueillir une nouvelle session est utilisée.

Les consoles proxys peuvent être redémarrées par les administrateurs mais cela va interrompre les sessions utilisateurs existantes.

Utiliser un certificat SSL pour la Console Proxy

Par défaut, la fonctionnalité de visualisation de la console utilise le HTTP en clair. Dans n'importe quel environnement de production, la connexion à la console proxy devrait être cryptée via SSL au minimum.

Un administrateur CloudStack dispose de 2 façons pour sécuriser la communication à la console proxy avec SSL :
- Configurer un certificat générique SSL et la résolution de nom de domaine
- Configurer un certificat pour un FQDN spécifique et configurer la répartition de charge

Changer le Certificat SSL et le domaine de la Console Proxy

L'administrateur peut configurer le cryptage SSL en sélectionnant un domaine et en téléchargent un nouveau certificat et une clef privée. Le domaine doit fournir le service DNS capable de résoudre les requêtes pour les adresses de la forme aaa-bbb-ccc-ddd.votre.domaine en adresses IPv4 dans la forme aaa.bbb.ccc.ddd, par exemple, 202.8.44.1. Pour modifier le domaine de la console proxy, le certificat SSL et la clef privée :

1. Configurer la résolution de nom dynamique ou peupler tous les noms DNS possibles de votre plage d'adresses IP publique au sein de votre serveur DNS avec le format aaa-bbb-ccc-ddd.consoleproxy.societe.com -> aaa.bbb.ccc.ddd.

   Note : Dans ces étapes, vous noterez consoleproxy.societe.com – Pour des raisons de sécurité, nous recommandons de créer un certificat SSL générique pour un sous-domaine séparé. Dans le cas où ce certificat serait compromis, un utilisateur mal intentionné ne pourrait pas usurper l'identité du domaine societe.com.

2. Générer la clef privée et la demande de certificat signé (CSR). Lorsque vous utilisez openssl pour générer les paires de clefs privées/publiques et les CSRs, pour la clef privée que vous allez copier dans l'interface de CloudStack, assurez-vous de convertir dans le format PKCS#8.

   (a) Générer une nouvelle clef privée de 2048 bits

```
openssl genrsa -des3 -out yourprivate.key 2048
```

   (b) Générer un nouveau certificat CSR. Assurez-vous de la création d'un certificat générique, comme *.consoleproxy.societe.com

```
openssl req -new -key yourprivate.key -out yourcertificate.csr
```

   (c) Sur le site web de votre Autorité de Certification favorite, commander un certificate SSL et soumettre le CSR. Vous devriez recevoir un certificat valide en retour.

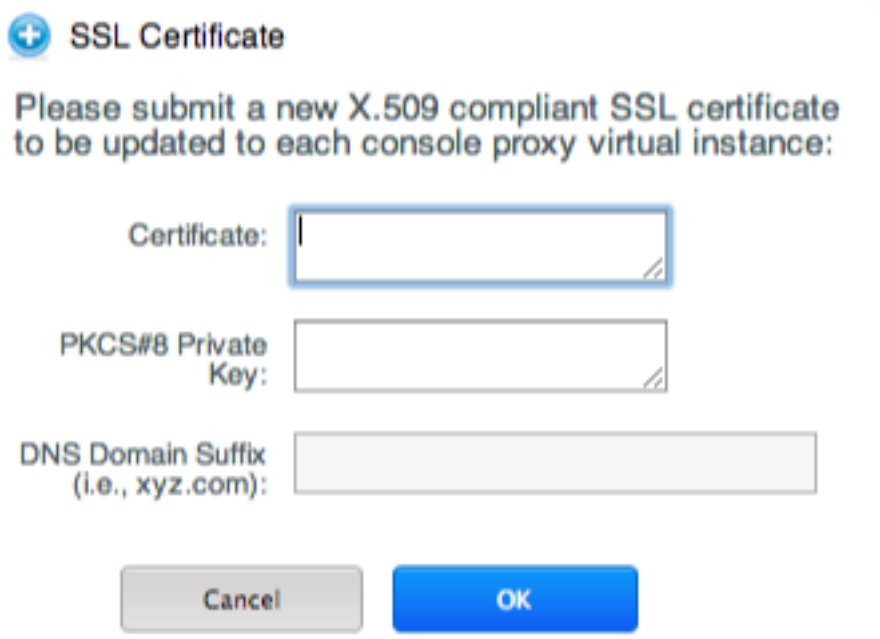
   (d) Convertir votre clef privée au format PKCS#8 crypté.

```
openssl pkcs8 -topk8 -in yourprivate.key -out yourprivate.pkcs8.encrypted.key
```

   (e) Convertir votre clef privée cryptée PKCS#8 au format PKCS#8 conforme avec CloudStack.

```
openssl pkcs8 -in yourprivate.pkcs8.encrypted.key -out yourprivate.pkcs8.key
```

3. Dans l'écran de mise à jour du certificate SSL de l'interface CloudStack, coller ce qui suit :
   — Le certificat que vous venez de générer.
   — La clef privée que vous venez juste de générer.
   — Le nom de domaine souhaité, préfixé d'un `*.` ; par exemple : `*.consoleproxy.societe.com`



4. Cela va arrêter toutes les VM console proxy en fonctionnement, et les redémarrer avec le nouveau certificat et la clef. Les utilisateurs peuvent noter une brève interruption de la disponibilité de la console.

Le serveur de gestion génère des URLS de la forme “aaa-bbb-ccc-ddd.consoleproxy.societe.com” après que les changements aient été effectués. Les nouvelles requêtes aux consoles seront faîtes avec le nouveau nom de domaine, certificat et clef.

Télécharger la CA Racine et la CA intermédiaire

Si vous avez besoin de télécharger un certificat personnalisé avec la CA racine et la CA intermédiaire, vous pouvez trouver plus de détails ici : https://cwiki.apache.org/confluence/display/CLOUDSTACK/Procedure+to+Replace+realhostip.com+with+Your+Own+Domain+Name

NOTES IMPORTANTES :

Dans le but d’éviter toutes erreurs et problèmes durant le téléchargement de certificats personnalisés, merci de vérifier ce qui suit :

1. While doing URL encoding of ROOT CA and any Intermediate CA, be sure that the plus signs (“+”) inside certificates are not replaced by space (” ”), because some URL/string encoding tools tend to do that.

2. If you are renewing certificates it might happen you need to upload new ROOT CA and Intermediate CA, together with new Server Certificate and key. In this case please be sure to use same names for certificates during API upload of certificate, example :

http://123.123.123.123:8080/client/api?command=uploadCustomCertificate&...&name=root1...
http://123.123.123.123:8080/client/api?command=uploadCustomCertificate&...&name=intermed1...

Ici les noms “root1” et “intermed1”. Si vous utilisiez d’autres noms auparavant, merci de vérifier la table cloud.keystore pour obtenir les noms utilisés.

Si vous avez toujours des problèmes et les erreurs suivantes dans le management.log lors de la destruction du CPVM :

- Unable to build keystore for CPVMCertificate due to CertificateException
- Cold not find and construct a valid SSL certificate

cela signifie toujours que certains certificats racine/intermédiaire/serveur ou la clef n'est pas dans le bon format, ou encodée incorrectement ou plusieurs CA racine/CA intermédiaire sont présente dans la base de données par erreur.

Une autre façon de renouveller les certificats (racine, intermédiaires, certificats serveurs ou clef) - bien que non recommandée sauf si vous la trouvez confortable, est d'éditer directement la base de données, tant que vous respectez la principale exigence que la clef soit encodée en PKCS8, alors que la CA racine, intermédiaire et les certificats serveurs sont toujours au format par défaut PEM (pas besoin d'encodage d'URL ici). Après avoir éditer la base de données, merci de redémarrer le serveur de gestion, de détruire la machine SSVM et CPVM après ça, pour que les nouvelles SSVM et CPVM soient créées avec les nouveaux certificats.

Les consoles proxys de répartition de charge

Une alternative à utiliser les DNS dynamique ou de créer une plage d'entrées DNS comme décrit ans la section précédente serait de créer un certificat SSl pour un nom de domaine spécifique, de configurer CloudStack pour utiliser ce FQDN particulier et alors de configurer un répartiteur de charge pour l'adresse IP de la console proxy derrière ce FQDN. Comme cette fonctionnalitée est toujours nouvelle, merci de voir https://cwiki.apache.org/confluence/display/CLOUDSTACK/Realhost+IP+changes pour plus de détails.

10.1.5 Routeur virtuel

Le routeur virtuel est un type de machine virtuel système. Le routeur virtuel est un des fournisseurs de service le plus utilisé dans CloudStack. L'utilisateur final n'a pas d'accès direct à ce routeur virtuel. Les utilisateurs peuvent pinguer le routeur virtuel et prendre les actions qui l'affectent (comme configurer la redirection de port), mais les utilisateurs n'ont pas d'accès SSH sur le routeur virtuel.

Il n'y a pas de mécanisme pour l'administrateur afin de se connecter sur le routeur virtuel. Les routeurs virtuels peuvent être redémarrés par les administrateurs, mais cela interrompt l'accès au réseau publique et les autres services pour les utilisateurs finaux. Un test de base dans le dépannage des problèmes réseaux est d'essayer de pinguer le routeur virtuel depuis une VM invitée. Certaines des caractéristiques du routeur virtuel sont déterminées par les offres de services systèmes associées.

Configurer le routeur virtuel

Vous pouvez paramétrer :[2]

- Plage IP
- Services réseaux supportés
- Le nom de domaine par défaut pour les services servis par le routeur virtuel
- Adresse IP de la passerelle
- A quelle fréquence CloudStack rapporte les statistiques d'utilisation du réseau depuis les routeurs virtuels CloudStack. Si vous voulez collecter les données métriques du trafic depuis les routeur virtuel, fixer le paramètre de configuration global router.stats.interval. Si vous n'utilisez pas de routeur virtuel pour recueillir les statistiques d'utilisation du réseau, le positionner à 0.

Mettre à jour un routeur virtuel avec les offres de service système

Quand CloudStack crée un routeur virtuel, il utilise des paramètres par défaut qui sont définis dans une offre de service système par défaut. Voir *"Offres de service système"*. Tous les routeurs virtuels du même réseau invité utilise la même offre de service système. Vous pouvez mettre à jour les capacités du routeur virtuel en créant et appliquant une offre de service système personnalisée.

1. Définir votre offre de service système personnalisé. Voir *"Créer une nouvelle offre de service système"*. Dans le type de VM système, choisir Routeur de domaine.

2. Associer l'offre de service système avec l'offre de service. Voir "Créer une nouvelle offre de réseau".
3. Appliquer l'offre de réseau au réseau dans lequel vous voulez les routeurs virtuels utilisant la nouvelle offre de service système. S'il s'agit d'un nouveau réseau, suivre les étapes de Ajouter un réseau invité additionnel de la page 66. Pour changer l'offre de service d'un routeur virtuel existant, suivre les étapes de "Changer l'offre réseau d'un réseau invité".

Meilleurs pratiques pour les routeurs virtuels

— ATTENTION : rédémarrer un routeur virtuel depuis une console de l'hyperviseur efface toutes les règles iptables. Pour contourner ce probluème, stopper le routeur virtuel et le démarrer depuis l'interface CloudStack.

— **Avertissement :** N'utilisez pas l'API destroyRouter lorsqu'un seul routeur n'est disponible dans le réseau, parce que l'API restartNetwork avec le paramètre cleanup=false ne pourra pas le récréer plus tard. Si vous voulez détruire et recréer un seul routeur disponible dans le réseau, utiliser l'API restartNetwork avec le paramètre cleanup=true.

Outil de surveillance de service pour Routeur Virtuelle

Des services variés fonctionnant sur les routeurs virtuels CloudStack peuvent être surveillés en utilisant l'outil de Surveillance Système. L'outil garantit que les services fonctionnent correctement jusqu'à ce que CloudStack les désactive délibérément. Si un service tombe, l'outil redémarre automatiquement le service et si cela n'aide pas à remonter le service, une alerte et un évènement sont générés indiquant la panne. A nouveau paramètre global, `network.router.enableservicemonitoring`, a été introduit pour contrôler cette fonctionnalité. La valeur par défaut est à false, ce qui implique que la surveillance est désactivée. Quand vous l'activez, s'assurer que le serveur de gestion et le routeur soient redémarrer.

Les outils de surveillance peuvent aider à démarrer un service VR, qui est planté à cause d'une raison inconnue. Par exemple :

— Le service a planté à cause de défauts dans le code source.
— Les services qui sont arrêtés par l'OS quand la mémoire ou le CPU ne sont plus suffisamment disponible pour le service.

Note : Seulement les services avec des démons sont surveillés. Les services qui sont échoués à cause d'erreurs dans le fichier de configuration du service/démon ne peuvent pas être redémarrés par l'outil de supervision. Les réseaux VPC ne sont pas supportés.

Les services suivants sont contrôlés par un VR :

— DNS
— HA Proxy
— SSH
— Apache Web Server

Les réseaux suivant sont supportés :

— Les réseaux isolés
— Les réseaux partagés dans les zones Avancées et Basiques

Note : Les réseaux VPC ne sont pas supportés

Cette fonctionnalité est supporté sur les hyperviseurs suivants : XenServer, VMware et KVM.

Mise à jour améliorée pour les routeurs virtuels

Mettre à jour un VR est rendu souple. L'administrateur CloudStack est capable de contrôler la séquence des mises à jour du VR. Le séquencement est basé sur la hiérarchie de l'infrastructure, comme par Cluster, Pod ou Zone et la hiérarchie (de comptes) administrative, comme par Utilisateur ou Domain. En tant qu'administrateur, vous pouvez aussi déterminer quand un service client particulier, comme les VR, est mis à jour dans les limites d'un intervalle de mise à jour spécifiée. L'opération de mise à jour est améliorée pour augmenter la vitesse de mise à jour en autorisant autant d'opérations en parallèle que possible.

Durant la durée complète de la mise à jour, les utilisateurs ne peuvent pas lancer de nouveaux services ou faire des modifications sur un service existant.

En complément, utiliser plusieurs versions de VRs dans une seule instance est supporté. Dans l'onglet Détails d'un VR, vous pouvez voir la version et si il nécessite une mise à jour. Durant la mise à jour du serveur de gestion, CloudStack vérifie si le VR est à la dernière version avant d'effectuer toute opération sur le VR. Pour supporter cela, un nouveau paramètre global, *''router.version.check''*, a été ajouté. Ce paramètre est fixé à true par défaut, ce qui implique que la version minimum requise est vérifiée avant d'effectuer toute opération. Aucune opération n'est effectuée si le VR n'est pas à la version requise. Les services de la vieille version du VR continue d'être disponible, mais aucune nouvelle opération ne peut être effectuée sur le VR jusqu'à ce qu'il soit mis à jour à la dernière version. Cela va assurer que la disponibilité des services VR et l'état des VR n'est pas impacté à cause de la mise à jour du serveur de gestion.

Le service suivant sera disponible même si le VR n'est pas mis à jour. Toutefois, aucun changement pour aucun des services ne peut être envoyé au VR jusqu'à ce qu'il soit mis à jour :

- Groupe de sécurité
- Données utilisateur
- DHCP
- DNS
- LB
- Redirection de port
- VPN
- NAT statique
- Source NAT
- Parefeu
- Passerelle
- ACL réseau

Routeurs virtuels supportés

- VR
- VPC VR
- VR redondant

Mettre à jour les routeurs virtuels

1. Télécharger les derniers modèles de VM système.
2. Télécharger les dernières VM systèmes sur tous les ensembles de stockage primaire.
3. Mettre à jour le serveur de gestion.
4. Mettre à jour CPVM et SSVM depuis au choix l'interface ou en utilisant le script suivant :

```
# cloudstack-sysvmadm -d <IP address> -u cloud -p -s
```

Même lorsque les VRs sont toujours dans une ancienne versions, les services existants vont continuer à être disponible pour les VMs. Le serveur de gestion ne peut plus effectuer d'opération sur les VRs jusqu'à ce qu'ils soient mis à jour.

5. Mettre à jour les VRs sélectivement :
   (a) Se connecter à l'interface de CloudStack comme administrateur racine.
   (b) Choisissez Infrastructure dans le panneau de navigation à gauche.
   (c) Dans Routeurs virtuels, cliquer sur Voir Plus.
   Tous les VRs sont listés dans la page Routeurs virtuels
   (d) Dans la liste de choix de sélection de vue, sélectionner le regroupement de base désiré selon vos exigences.
   Vous pouvez utiliser n'importe lequel parmi :
   — Grouper par zones
   — Grouper par pods
   — Grouper par clusters
   — Grouper par comptes
   (e) Cliquer sur le groupe dont les VRs doivent être mis à jour.
   Par exemple, si vous avez selectionné Grouper par zone, sélectionner le nom de la zone désirée.
   (f) Cliquer sur le bouton Mettre à jour pour mettre à jour tous les VRs. 
   (g) Cliquer OK pour confirmer.

10.1.6 VM de stockage secondaire

En plus des hôtes, la VM de Stockage Secondaire CloudStack monte et écrit sur le stockage secondaire.

Les dépots vers le stockage secondaire passe par la VM de stockage secondaire. La VM de stockage secondaire peuvent récupérer les modèles et les images ISO depuis des URLs en utilisant une diversité de protocoles.

La VM de stockage secondaire fourni une tâche en arrière plan qui prend soin d'une variété d'activités de stockage secondaire : télécharger un nouveau modèle à une Zone, copier des modèles entres Zones, et la sauvegarde des instantanés.

Les administrateurs peuvent se logger sur la VM de stockage secondaire au besoin.

CHAPITRE 11

Travailler avec les statistiques d'utilisation

11.1 Working with Usage

The Usage Server is an optional, separately-installed part of CloudStack that provides aggregated usage records which you can use to create billing integration for CloudStack. The Usage Server works by taking data from the events log and creating summary usage records that you can access using the listUsageRecords API call.

The usage records show the amount of resources, such as VM run time or template storage space, consumed by guest instances.

The Usage Server runs at least once per day. It can be configured to run multiple times per day.

11.1.1 Configuring the Usage Server

To configure the usage server :

1. Be sure the Usage Server has been installed. This requires extra steps beyond just installing the CloudStack software. See Installing the Usage Server (Optional) in the Advanced Installation Guide.
2. Log in to the CloudStack UI as administrator.
3. Click Global Settings.
4. In Search, type usage. Find the configuration parameter that controls the behavior you want to set. See the table below for a description of the available parameters.
5. In Actions, click the Edit icon.
6. Type the desired value and click the Save icon.
7. Restart the Management Server (as usual with any global configuration change) and also the Usage Server :

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

The following table shows the global configuration settings that control the behavior of the Usage Server.

Parameter Name Description

enable.usage.server Whether the Usage Server is active.

usage.aggregation.timezone

Time zone of usage records. Set this if the usage records and daily job execution are in different time zones. For example, with the following settings, the usage job will run at PST 00 :15 and generate usage records for the 24 hours from 00 :00 :00 GMT to 23 :59 :59 GMT :

```
usage.stats.job.exec.time = 00:15
usage.execution.timezone = PST
usage.aggregation.timezone = GMT
```

Valid values for the time zone are specified in Appendix A, *Time Zones*

Default : GMT

usage.execution.timezone

The time zone of usage.stats.job.exec.time. Valid values for the time zone are specified in Appendix A, *Time Zones*

Default : The time zone of the management server.

usage.sanity.check.interval

The number of days between sanity checks. Set this in order to periodically search for records with erroneous data before issuing customer invoices. For example, this checks for VM usage records created after the VM was destroyed, and similar checks for templates, volumes, and so on. It also checks for usage times longer than the aggregation range. If any issue is found, the alert ALERT_TYPE_USAGE_SANITY_RESULT = 21 is sent.

usage.stats.job.aggregation.range

The time period in minutes between Usage Server processing jobs. For example, if you set it to 1440, the Usage Server will run once per day. If you set it to 600, it will run every ten hours. In general, when a Usage Server job runs, it processes all events generated since usage was last run.

There is special handling for the case of 1440 (once per day). In this case the Usage Server does not necessarily process all records since Usage was last run. CloudStack assumes that you require processing once per day for the previous, complete day's records. For example, if the current day is October 7, then it is assumed you would like to process records for October 6, from midnight to midnight. CloudStack assumes this "midnight to midnight" is relative to the usage.execution.timezone.

Default : 1440

usage.stats.job.exec.time

The time when the Usage Server processing will start. It is specified in 24-hour format (HH :MM) in the time zone of the server, which should be GMT. For example, to start the Usage job at 10 :30 GMT, enter "10 :30".

If usage.stats.job.aggregation.range is also set, and its value is not 1440, then its value will be added to usage.stats.job.exec.time to get the time to run the Usage Server job again. This is repeated until 24 hours have elapsed, and the next day's processing begins again at usage.stats.job.exec.time.

Default : 00 :15.

For example, suppose that your server is in GMT, your user population is predominantly in the East Coast of the United States, and you would like to process usage records every night at 2 AM local (EST) time. Choose these settings :

- enable.usage.server = true
- usage.execution.timezone = America/New_York
- usage.stats.job.exec.time = 07 :00. This will run the Usage job at 2 :00 AM EST. Note that this will shift by an hour as the East Coast of the U.S. enters and exits Daylight Savings Time.
- usage.stats.job.aggregation.range = 1440

With this configuration, the Usage job will run every night at 2 AM EST and will process records for the previous day's midnight-midnight as defined by the EST (America/New_York) time zone.

Note : Because the special value 1440 has been used for usage.stats.job.aggregation.range, the Usage Server will ignore the data between midnight and 2 AM. That data will be included in the next day's run.

11.1.2 Setting Usage Limits

CloudStack provides several administrator control points for capping resource usage by users. Some of these limits are global configuration parameters. Others are applied at the ROOT domain and may be overridden on a per-account basis.

Globally Configured Limits

In a zone, the guest virtual network has a 24 bit CIDR by default. This limits the guest virtual network to 254 running instances. It can be adjusted as needed, but this must be done before any instances are created in the zone. For example, 10.1.1.0/22 would provide for ~1000 addresses.

The following table lists limits set in the Global Configuration :

Parameter Name	Definition
max.account.public.ips	Number of public IP addresses that can be owned by an account
max.account.snapshots	Number of snapshots that can exist for an account
max.account.templates	Number of templates that can exist for an account
max.account.user.vms	Number of virtual machine instances that can exist for an account
max.account.volumes	Number of disk volumes that can exist for an account
max.template.iso.size	Maximum size for a downloaded template or ISO in GB
max.volume.size.gb	Maximum size for a volume in GB
network.throttling.rate	Default data transfer rate in megabits per second allowed per user (supported on XenServer)
snapshot.max.hourly	Maximum recurring hourly snapshots to be retained for a volume. If the limit is reached, early snapshots from the start of the hour are deleted so that newer ones can be saved. This limit does not apply to manual snapshots. If set to 0, recurring hourly snapshots can not be scheduled
snapshot.max.daily	Maximum recurring daily snapshots to be retained for a volume. If the limit is reached, snapshots from the start of the day are deleted so that newer ones can be saved. This limit does not apply to manual snapshots. If set to 0, recurring daily snapshots can not be scheduled
snapshot.max.weekly	Maximum recurring weekly snapshots to be retained for a volume. If the limit is reached, snapshots from the beginning of the week are deleted so that newer ones can be saved. This limit does not apply to manual snapshots. If set to 0, recurring weekly snapshots can not be scheduled
snapshot.max.monthly	Maximum recurring monthly snapshots to be retained for a volume. If the limit is reached, snapshots from the beginning of the month are deleted so that newer ones can be saved. This limit does not apply to manual snapshots. If set to 0, recurring monthly snapshots can not be scheduled.

To modify global configuration parameters, use the global configuration screen in the CloudStack UI. See Setting Global Configuration Parameters

Limiting Resource Usage

CloudStack allows you to control resource usage based on the types of resources, such as CPU, RAM, Primary storage, and Secondary storage. A new set of resource types has been added to the existing pool of resources to support the new customization model—need-basis usage, such as large VM or small VM. The new resource types are now broadly classified as CPU, RAM, Primary storage, and Secondary storage. The root administrator is able to impose resource usage limit by the following resource types for Domain, Project, and Accounts.

- CPU
- Memory (RAM)
- Primary Storage (Volumes)
- Secondary Storage (Snapshots, Templates, ISOs)

To control the behaviour of this feature, the following configuration parameters have been added :

Parameter Name	Description
max.account.cpus	Maximum number of CPU cores that can be used for an account. Default is 40.
max.account.ram (MB)	Maximum RAM that can be used for an account. Default is 40960.
max.account.primary.storage (GB)	Maximum primary storage space that can be used for an account. Default is 200.
max.account.secondary.storage (GB)	Maximum secondary storage space that can be used for an account. Default is 400.
max.project.cpus	Maximum number of CPU cores that can be used for an account. Default is 40.
max.project.ram (MB)	Maximum RAM that can be used for an account. Default is 40960.
max.project.primary.storage (GB)	Maximum primary storage space that can be used for an account. Default is 200.
max.project.secondary.storage (GB)	Maximum secondary storage space that can be used for an account. Default is 400.

User Permission

The root administrator, domain administrators and users are able to list resources. Ensure that proper logs are maintained in the `vmops.log` and `api.log` files.

- The root admin will have the privilege to list and update resource limits.
- The domain administrators are allowed to list and change these resource limits only for the sub-domains and accounts under their own domain or the sub-domains.
- The end users will the privilege to list resource limits. Use the listResourceLimits API.

Limit Usage Considerations

- Primary or Secondary storage space refers to the stated size of the volume and not the physical size— the actual consumed size on disk in case of thin provisioning.
- If the admin reduces the resource limit for an account and set it to less than the resources that are currently being consumed, the existing VMs/templates/volumes are not destroyed. Limits are imposed only if the user under that account tries to execute a new operation using any of these resources. For example, the existing behavior in the case of a VM are :
  - migrateVirtualMachine : The users under that account will be able to migrate the running VM into any other host without facing any limit issue.
  - recoverVirtualMachine : Destroyed VMs cannot be recovered.
- For any resource type, if a domain has limit X, sub-domains or accounts under that domain can have there own limits. However, the sum of resource allocated to a sub-domain or accounts under the domain at any point of time should not exceed the value X.
  For example, if a domain has the CPU limit of 40 and the sub-domain D1 and account A1 can have limits of 30 each, but at any point of time the resource allocated to D1 and A1 should not exceed the limit of 40.
- If any operation needs to pass through two of more resource limit check, then the lower of 2 limits will be enforced, For example : if an account has the VM limit of 10 and CPU limit of 20, and a user under that account requests 5 VMs of 4 CPUs each. The user can deploy 5 more VMs because VM limit is 10. However, the user cannot deploy any more instances because the CPU limit has been exhausted.

Limiting Resource Usage in a Domain

CloudStack allows the configuration of limits on a domain basis. With a domain limit in place, all users still have their account limits. They are additionally limited, as a group, to not exceed the resource limits set on their domain. Domain limits aggregate the usage of all accounts in the domain as well as all the accounts in all the sub-domains of

that domain. Limits set at the root domain level apply to the sum of resource usage by the accounts in all the domains and sub-domains below that root domain.

To set a domain limit :

1. Se connecter à l'interface CloudStack.
2. In the left navigation tree, click Domains.
3. Select the domain you want to modify. The current domain limits are displayed.
   A value of -1 shows that there is no limit in place.
4. Click the Edit button 
5. Edit the following as per your requirement :
   — Parameter Name
   — Description
   — Instance Limits
   The number of instances that can be used in a domain.
   — Public IP Limits
   The number of public IP addresses that can be used in a domain.
   — Volume Limits
   The number of disk volumes that can be created in a domain.
   — Snapshot Limits
   The number of snapshots that can be created in a domain.
   — Template Limits
   The number of templates that can be registered in a domain.
   — VPC limits
   The number of VPCs that can be created in a domain.
   — CPU limits
   The number of CPU cores that can be used for a domain.
   — Memory limits (MB)
   The number of RAM that can be used for a domain.
   — Primary Storage limits (GB)
   The primary storage space that can be used for a domain.
   — Secondary Storage limits (GB)
   The secondary storage space that can be used for a domain.
6. Cliquer sur Appliquer.

Default Account Resource Limits

You can limit resource use by accounts. The default limits are set by using Global configuration parameters, and they affect all accounts within a cloud. The relevant parameters are those beginning with max.account, for example : max.account.snapshots.

To override a default limit for a particular account, set a per-account resource limit.

1. Se connecter à l'interface CloudStack.
2. In the left navigation tree, click Accounts.
3. Select the account you want to modify. The current limits are displayed.
   A value of -1 shows that there is no limit in place.
4. Click the Edit button. 
5. Edit the following as per your requirement :
   — Parameter Name
   — Description

— Instance Limits
The number of instances that can be used in an account.
The default is 20.
— Public IP Limits
The number of public IP addresses that can be used in an account.
The default is 20.
— Volume Limits
The number of disk volumes that can be created in an account.
The default is 20.
— Snapshot Limits
The number of snapshots that can be created in an account.
The default is 20.
— Template Limits
The number of templates that can be registered in an account.
The default is 20.
— VPC limits
The number of VPCs that can be created in an account.
The default is 20.
— CPU limits
The number of CPU cores that can be used for an account.
The default is 40.
— Memory limits (MB)
The number of RAM that can be used for an account.
The default is 40960.
— Primary Storage limits (GB)
The primary storage space that can be used for an account.
The default is 200.
— Secondary Storage limits (GB)
The secondary storage space that can be used for an account.
The default is 400.

6. Cliquer sur Appliquer.

11.1.3 Usage Record Format

Virtual Machine Usage Record Format

For running and allocated virtual machine usage, the following fields exist in a usage record :

— account – name of the account
— accountid – ID of the account
— domainid – ID of the domain in which this account resides
— zoneid – Zone where the usage occurred
— description – A string describing what the usage record is tracking
— usage – String representation of the usage, including the units of usage (e.g. 'Hrs' for VM running time)
— usagetype – A number representing the usage type (see Usage Types)
— rawusage – A number representing the actual usage in hours
— virtualMachineId – The ID of the virtual machine
— name – The name of the virtual machine
— offeringid – The ID of the service offering
— templateid – The ID of the template or the ID of the parent template. The parent template value is present when the current template was created from a volume.
— usageid – Virtual machine
— type – Hypervisor
— startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

Network Usage Record Format

For network usage (bytes sent/received), the following fields exist in a usage record.

- account – name of the account
- accountid – ID of the account
- domainid – ID of the domain in which this account resides
- zoneid – Zone where the usage occurred
- description – A string describing what the usage record is tracking
- usagetype – A number representing the usage type (see Usage Types)
- rawusage – A number representing the actual usage in hours
- usageid – Device ID (virtual router ID or external device ID)
- type – Device type (domain router, external load balancer, etc.)
- startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

IP Address Usage Record Format

For IP address usage the following fields exist in a usage record.

- account - name of the account
- accountid - ID of the account
- domainid - ID of the domain in which this account resides
- zoneid - Zone where the usage occurred
- description - A string describing what the usage record is tracking
- usage - String representation of the usage, including the units of usage
- usagetype - A number representing the usage type (see Usage Types)
- rawusage - A number representing the actual usage in hours
- usageid - IP address ID
- startdate, enddate - The range of time for which the usage is aggregated ; see Dates in the Usage Record
- issourcenat - Whether source NAT is enabled for the IP address
- iselastic - True if the IP address is elastic.

Disk Volume Usage Record Format

For disk volumes, the following fields exist in a usage record.

- account – name of the account
- accountid – ID of the account
- domainid – ID of the domain in which this account resides
- zoneid – Zone where the usage occurred
- description – A string describing what the usage record is tracking
- usage – String representation of the usage, including the units of usage (e.g. 'Hrs' for hours)
- usagetype – A number representing the usage type (see Usage Types)
- rawusage – A number representing the actual usage in hours
- usageid – The volume ID
- offeringid – The ID of the disk offering
- type – Hypervisor
- templateid – ROOT template ID
- size – The amount of storage allocated
- startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

Template, ISO, and Snapshot Usage Record Format

- account – name of the account
- accountid – ID of the account

- domainid – ID of the domain in which this account resides
- zoneid – Zone where the usage occurred
- description – A string describing what the usage record is tracking
- usage – String representation of the usage, including the units of usage (e.g. 'Hrs' for hours)
- usagetype – A number representing the usage type (see Usage Types)
- rawusage – A number representing the actual usage in hours
- usageid – The ID of the the template, ISO, or snapshot
- offeringid – The ID of the disk offering
- templateid – – Included only for templates (usage type 7). Source template ID.
- size – Size of the template, ISO, or snapshot
- startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

Load Balancer Policy or Port Forwarding Rule Usage Record Format

- account - name of the account
- accountid - ID of the account
- domainid - ID of the domain in which this account resides
- zoneid - Zone where the usage occurred
- description - A string describing what the usage record is tracking
- usage - String representation of the usage, including the units of usage (e.g. 'Hrs' for hours)
- usagetype - A number representing the usage type (see Usage Types)
- rawusage - A number representing the actual usage in hours
- usageid - ID of the load balancer policy or port forwarding rule
- usagetype - A number representing the usage type (see Usage Types)
- startdate, enddate - The range of time for which the usage is aggregated ; see Dates in the Usage Record

Network Offering Usage Record Format

- account – name of the account
- accountid – ID of the account
- domainid – ID of the domain in which this account resides
- zoneid – Zone where the usage occurred
- description – A string describing what the usage record is tracking
- usage – String representation of the usage, including the units of usage (e.g. 'Hrs' for hours)
- usagetype – A number representing the usage type (see Usage Types)
- rawusage – A number representing the actual usage in hours
- usageid – ID of the network offering
- usagetype – A number representing the usage type (see Usage Types)
- offeringid – Network offering ID
- virtualMachineId – The ID of the virtual machine
- virtualMachineId – The ID of the virtual machine
- startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

VPN User Usage Record Format

- account – name of the account
- accountid – ID of the account
- domainid – ID of the domain in which this account resides
- zoneid – Zone where the usage occurred
- description – A string describing what the usage record is tracking
- usage – String representation of the usage, including the units of usage (e.g. 'Hrs' for hours)
- usagetype – A number representing the usage type (see Usage Types)

— rawusage – A number representing the actual usage in hours
— usageid – VPN user ID
— usagetype – A number representing the usage type (see Usage Types)
— startdate, enddate – The range of time for which the usage is aggregated ; see Dates in the Usage Record

11.1.4 Usage Types

The following table shows all usage types.

Type ID	Type Name	Description
1	RUNNING_VM	Tracks the total running time of a VM per usage record period. If the VM is upgraded during the usage period, you will get a separate Usage Record for the new upgraded VM.
2	ALLOCATED_VM	Tracks the total time the VM has been created to the time when it has been destroyed. This usage type is also useful in determining usage for specific templates such as Windows-based templates.
3	IP_ADDRESS	Tracks the public IP address owned by the account.
4	NETWORK_BYTES_SENT	Tracks the total number of bytes sent by all the VMs for an account. Cloud.com does not currently track network traffic per VM.
5	NETWORK_BYTES_RECEIVED	Tracks the total number of bytes received by all the VMs for an account. Cloud.com does not currently track network traffic per VM.
6	VOLUME	Tracks the total time a disk volume has been created to the time when it has been destroyed.
7	TEMPLATE	Tracks the total time a template (either created from a snapshot or uploaded to the cloud) has been created to the time it has been destroyed. The size of the template is also returned.
8	ISO	Tracks the total time an ISO has been uploaded to the time it has been removed from the cloud. The size of the ISO is also returned.
9	SNAPSHOT	Tracks the total time from when a snapshot has been created to the time it have been destroyed.
11	LOAD_BALANCER_POLICY	Tracks the total time a load balancer policy has been created to the time it has been removed. Cloud.com does not track whether a VM has been assigned to a policy.
12	PORT_FORWARDING_RULE	Tracks the time from when a port forwarding rule was created until the time it was removed.
13	NETWORK_OFFERING	The time from when a network offering was assigned to a VM until it is removed.
14	VPN_USERS	The time from when a VPN user is created until it is removed.

11.1.5 Example response from listUsageRecords

All CloudStack API requests are submitted in the form of a HTTP GET/POST with an associated command and any parameters. A request is composed of the following whether in HTTP or HTTPS :

```
<listusagerecordsresponse>
   <count>1816</count>
   <usagerecord>
      <account>user5</account>
      <accountid>10004</accountid>
      <domainid>1</domainid>
      <zoneid>1</zoneid>
      <description>i-3-4-WC running time (ServiceOffering: 1) (Template: 3)</description>
      <usage>2.95288 Hrs</usage>
```

```
      <usagetype>1</usagetype>
      <rawusage>2.95288</rawusage>
      <virtualmachineid>4</virtualmachineid>
      <name>i-3-4-WC</name>
      <offeringid>1</offeringid>
      <templateid>3</templateid>
      <usageid>245554</usageid>
      <type>XenServer</type>
      <startdate>2009-09-15T00:00:00-0700</startdate>
      <enddate>2009-09-18T16:14:26-0700</enddate>
   </usagerecord>

   ... (1,815 more usage records)
</listusagerecordsresponse>
```

11.1.6 Dates in the Usage Record

Usage records include a start date and an end date. These dates define the period of time for which the raw usage number was calculated. If daily aggregation is used, the start date is midnight on the day in question and the end date is 23 :59 :59 on the day in question (with one exception ; see below). A virtual machine could have been deployed at noon on that day, stopped at 6pm on that day, then started up again at 11pm. When usage is calculated on that day, there will be 7 hours of running VM usage (usage type 1) and 12 hours of allocated VM usage (usage type 2). If the same virtual machine runs for the entire next day, there will 24 hours of both running VM usage (type 1) and allocated VM usage (type 2).

Note : The start date is not the time a virtual machine was started, and the end date is not the time when a virtual machine was stopped. The start and end dates give the time range within which usage was calculated.

For network usage, the start date and end date again define the range in which the number of bytes transferred was calculated. If a user downloads 10 MB and uploads 1 MB in one day, there will be two records, one showing the 10 megabytes received and one showing the 1 megabyte sent.

There is one case where the start date and end date do not correspond to midnight and 11 :59 :59pm when daily aggregation is used. This occurs only for network usage records. When the usage server has more than one day's worth of unprocessed data, the old data will be included in the aggregation period. The start date in the usage record will show the date and time of the earliest event. For other types of usage, such as IP addresses and VMs, the old unprocessed data is not included in daily aggregation.

Gérer les réseaux et le trafic

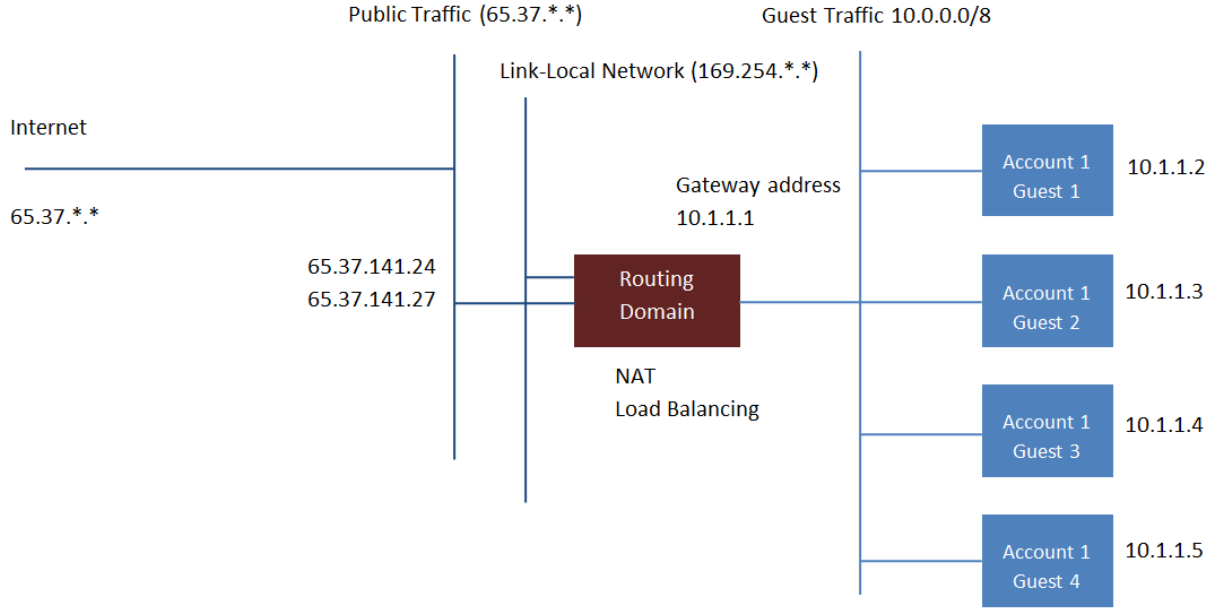
12.1 Gérer les réseaux et le trafic

Dans CloudStack, les VMs invitées peuvent communiquer ensemble en utilisant les infrastructures partagées avec la sécurité et la perception que les utilisateurs ont un LAN privé. Le routeur virtuel CloudStack est le composant principal fournissant les fonctionnalités réseaux pour le trafic invité.

12.1.1 Trafic invité

Un réseau peut transporter le trafic invité seulement entre VMs à l'intérieur d'une zone. Les machines virtuelles de zones différentes ne peuvent pas communiquer ensemble en utilisant leurs adresses IP ; elles doivent communiquer avec les autres par le routage de leurs adresses IP publiques.

Voir une configuration typique du trafic invité ci dessous :



Guest Traffic Setup

Typiquement, le serveur de gestion crée automatiquement un routeur virtuel pour chaque réseau. Un routeur virtuel est une machine virtuelle spéciale qui fonctionne sur les hôtes. Chaque routeur virtuel dans un réseau isolé à trois

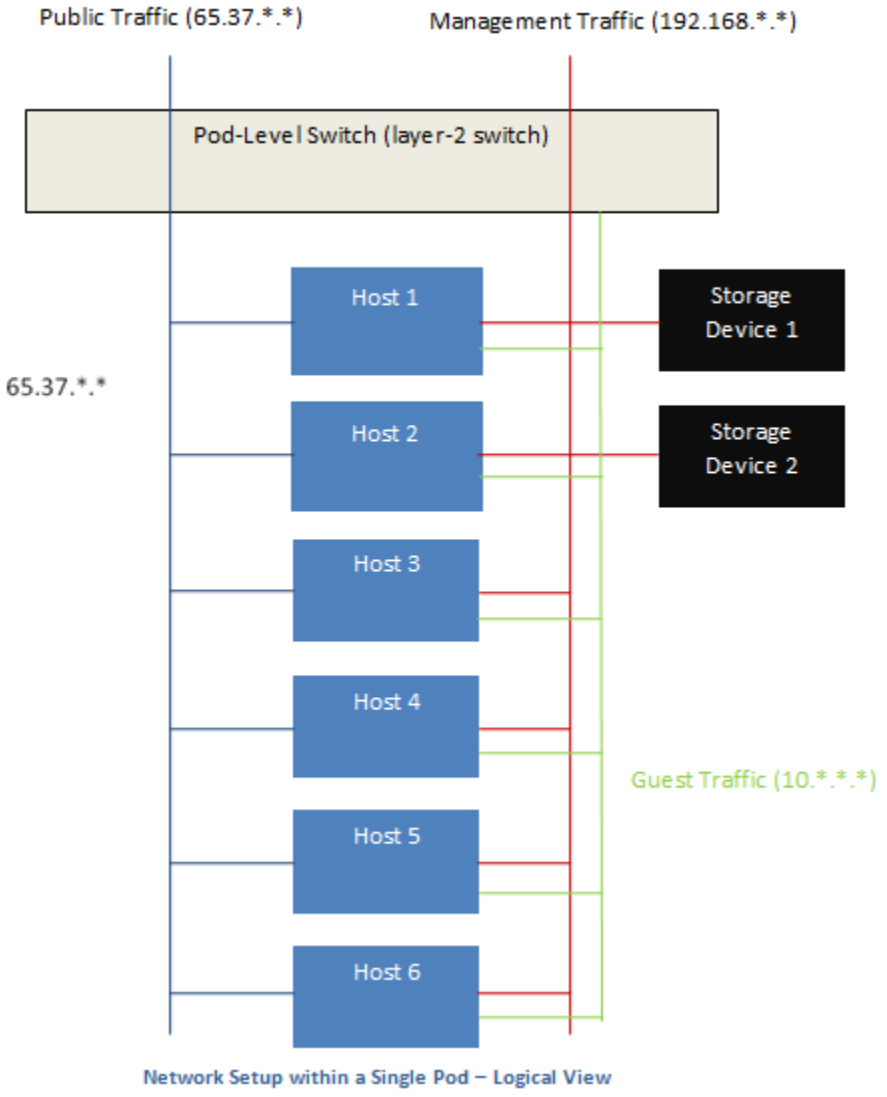
interfaces réseaux. Si plusieurs VLAN publics sont utilisés, le routeur aura plusieurs interfaces publiques. Son interface eth0 servira de passerelle pour le trafic invité et a comme adresse IP 10.1.1.1. Son interface eth1 est utilisée par le système pour configurer le routeur virtuel. Son interface eth2 a une adresse IP publique d'assignée pour le trafic publique. Si de multiples VLAN publics sont utilisés, le routeur aura plusieurs interfaces publiques.

Le routeur virtuel fournit le service DHCP qui va automatiquement assigner une adresse IP pour chaque VM invitée dans l'intervalle d'IP assignées au réseau. L'utilisateur peut manuellement reconfigurer les VMs invités pour adopter différentes adresses IP.

Le Source Nat est automatiquement configuré dans le routeur virtuel pour transférer le trafic sortant de toutes les VMs invitées.

12.1.2 Le réseau dans un Pod

L'image suivante illustre la configuration du réseau au sein d'un seul pod ; Les hôtes sont connectés à un commutateur de niveau pod. Au minimum, les hôtes devraient avoir un lien montant vers chaque commutateur. Les agrégats d'interfaces réseaux sont également supportés. Le commutateur du pod est une pair de commutateurs gigabits redondants avec des liens à 10G.



Network Setup within a Single Pod – Logical View

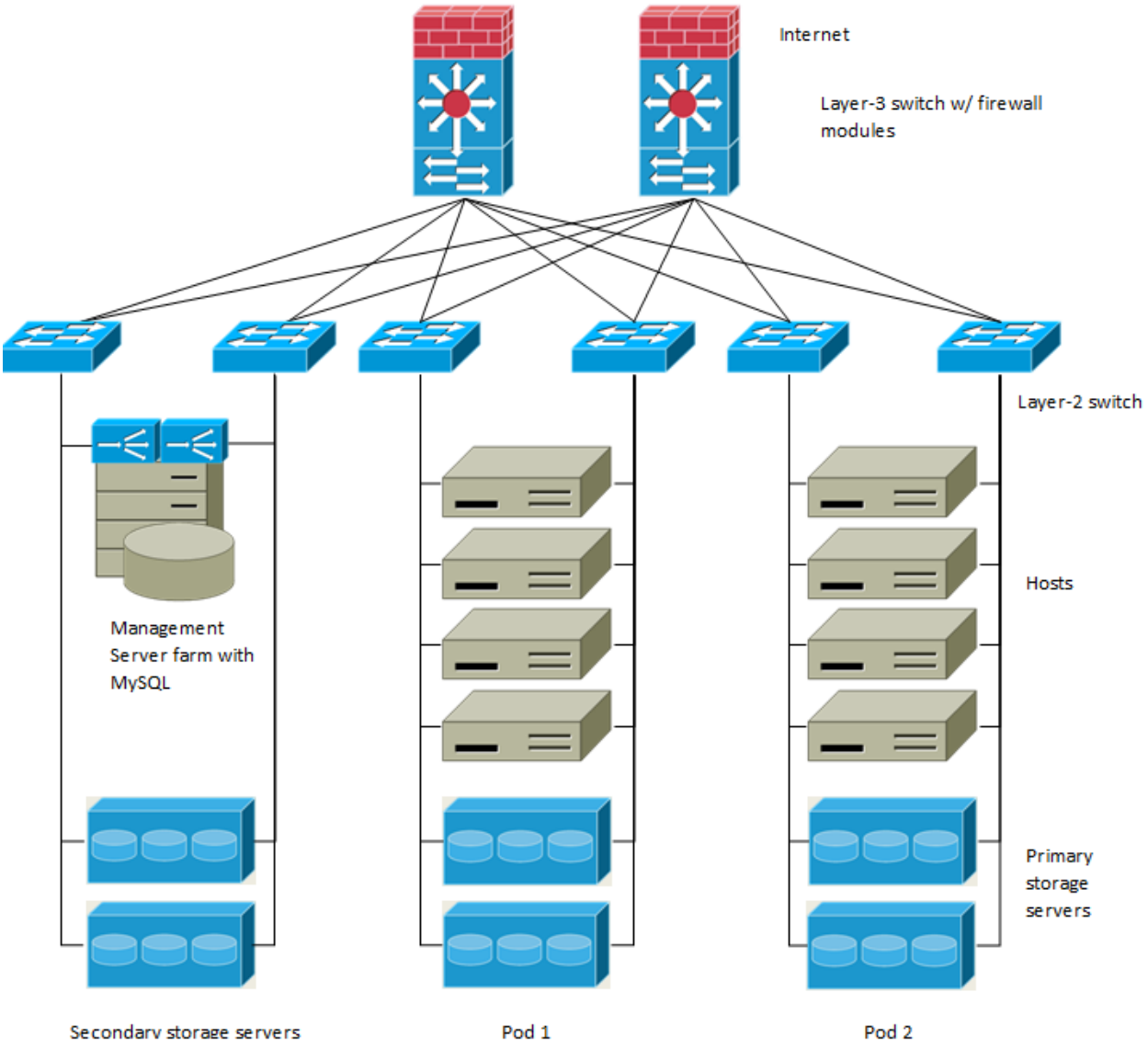
Les serveurs sont connectés comme ceci :

— Les périphériques de stockages ne sont connectés qu'au réseau qui transporte le trafic de gestion.
— Les hôtes sont connectés aux réseaux pour à la fois le trafic de gestion et le trafic publique.
— Les hôtes sont aussi connectés à un ou plusieurs réseaux qui transportent le trafic invité.

Nous recommandons l'utilisation de plusieurs cartes physique Ethernet qui implémente chacune interface réseau comme une fabrique redondante de commutateur dans le but d'optimiser le débit et améliorer la fiabilité.

12.1.3 Le réseau dans une Zone

La figure suivante illustre la configuration du réseau au sein d'une seule zone.



Un parefeu pour le trafic de gestion opère dans le mode NAT. Le réseau assigne typiquement des adresses IP dans l'espace d'adressage du réseau privé de classe B 192.168.0.0/16. Chaque pod se voit assigné des adresses IP dans l'espace privé de classe C 192.168.*.0/24.

Chaque zone à son propre ensemble d'adresses IP publiques. Les adresses IP publiques depuis différentes zones ne doivent pas se chevaucher.

12.1.4 Configuration du réseau physique d'une zone basique

Dans un réseau basique, configurer le réseau physique est assez simple. Vous devez seulement configurer un réseau invité pour transporter le trafic généré par les VMs invitées. Quand vous ajouter pour la première fois une zone à CloudStack, vous configurer le réseau invité par les écrans Ajouter une zone.

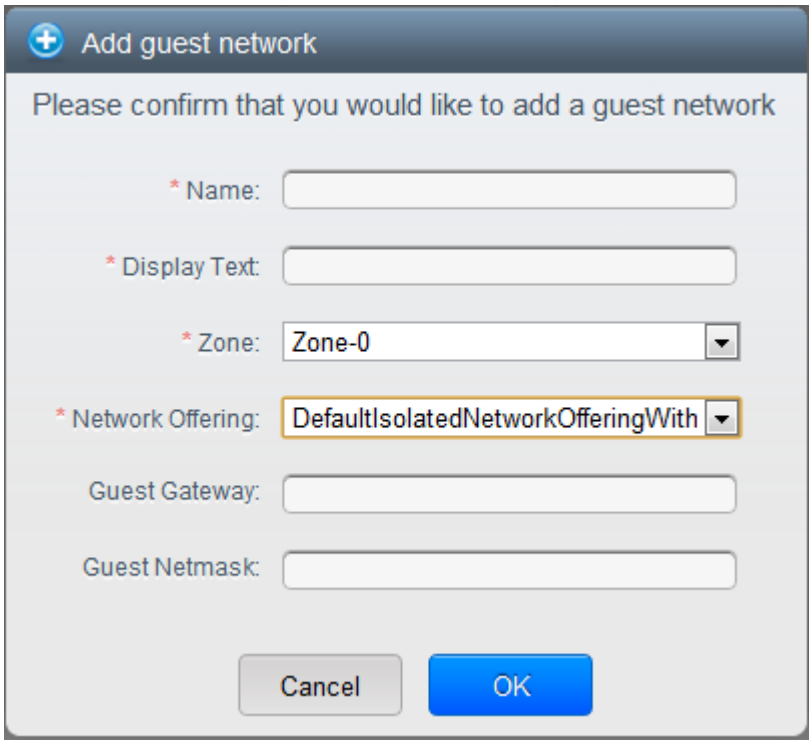
12.1.5 Configuration du réseau physique d'une zone basique

A l'intérieur d'une zone qui utilise le réseau avancé, vous devez dire au serveur de gestion comment le réseau physique est configuré pour transporter différents types de trafics isolés.

Configurer le trafic invité dans une Zone Avancée

Ces étapes assume que vous êtes déjà connecté dans l'interface CloudStack. Pour configurer le réseau invité de base :

1. Dans le menu de gauche, choisir Infrastructure. Dans Zones, cliquer sur Voir Plus, puis cliquer sur la zone à laquelle vous voulez ajouter un réseau.
2. Cliquer sur l'onglet Réseau.
3. Cliquer sur Ajouter un réseau invité.
   La fenêtre Ajouter un réseau invité est affichée :



4. Fournir l'information suivante :
   — **Nom** : Le nom du réseau. Cela sera visible de l'utilisateur.
   — **Texte affiché** : La description du réseau. Cela sera visible de l'utilisateur.
   — **Zone** : La zone pour laquelle vous êtes en train de configurer le réseau invité.
   — **Offre réseau** : Si l'administrateur a configuré plusieurs offres de réseau, sélectionner celui que vous voulez utiliser pour ce réseau.
   — **Passerelle invitée** : La passerelle que les invités devraient utiliser.
   — **Masque de sous réseau invité** : Le masque de sous réseau utilisé sur le sous réseau que les invités vont utiliser.

5. Cliquez sur OK.

Configurer le trafic public dans une Zone Avancée

Dans une zone qui utilise un réseau avancé, vous devez configurer au moins une plage d'adresses IP pour le trafic Internet.

Configurer un réseau invité partagé

1. Se connecter à l'interface de CloudStack comme administrateur
2. Choisissez Infrastructure dans le panneau de navigation à gauche.
3. Dans zones, cliquez sur Voir tout.
4. Cliquer sur la zone à laquelle vous voulez ajouter un réseau invité.
5. Cliquer sur l'onglet Réseau.
6. Cliquer sur le réseau physique avec lequel vous voulez travailler.
7. Sur le noeud Invité du diagramme, cliquer sur Configurer.
8. Cliquer sur l'onglet Réseau.
9. Cliquer sur Ajouter un réseau invité.
   La fenêtre Ajouter un réseau invité est affichée :
10. Spécifier les informations suivantes :
    - **Nom** : Le nom du réseau. Cela sera visible de l'utilisateur.
    - **Description** : La description courte du réseau qui peut être affichée aux utilisateurs
    - **ID VLAN** : L'ID unique du VLAN.
    - **ID du VLAN isolé** : L'ID unique du VLAN secondaire isolé.
    - **Portée** : Les portées possibles sont Domaine, Compte, Projet et Tous.
      - **Domaine** : Sélectionner Domaine limite la partée de ce réseau invité au domaine que vous spécifiez. Le réseau ne sera pas disponible pour les autres domaines.Si vous sélectionnez Accès Sous Domaine, le réseau invité est disponible à tous les sous domaines au sein du domaine sélectionné.
      - **Compte** : Le compte pour lequel le réseau invité est créé. Vous devez spécifier le domaine auquel appartient le compte.
      - **Projet** : Le projet pour lequel le réseau invité est créé. Vous devez spécifier le domaine auquel le projet appartient.
      - **Tous** : Le réseau invité est disponible pour tous les domaines, comptes, projets au sein de la zone sélectionnée.
    - **Offre réseau** : Si l'administrateur a configuré plusieurs offres de réseau, sélectionnez celle que vous voulez utiliser pour ce réseau.
    - **Passerelle** : La passerelle que les invités devraient utiliser.
    - **Masque de sous réseau** : Le masque de sous réseau du réseau que les utilisateurs vont utiliser.
    - **Plage IP** : Une plage d'adresses IP qui sont accessibles depuis l'Internet est qui sont assignées aux VMs invitées.
      Si une interface est utilisée, ces IP devrait être dans le même CIDR dans le cas de l'IPv6.
    - **IPv6 CIRD** : Le préfixe réseau qui défini le sous réseau du réseau invité. C'est le CIDR qui décrit les adresses IPv6 en usage dans les réseaux invités de cette zone. Pour autoriser les adresses IP depuis un bloc d'adresse particulier, entrer un CIDR.
    - **Domaine Réseau** : Un suffixe DNS personnalisé au niveau du réseau. Si vous voulez assigner un nom de domaine spécial au réseau des VM invitées, spécifier un suffixe DNS.
11. Cliquer OK pour confirmer.

12.1.6 Utiliser plusieurs Réseaux d'Invités

Dans les zones qui utilisent le réseau avancé, des réseaux additionnels pour le trafic invité peuvent être ajouté à n'importe quel moment après l'installation initiale. Vous pouvez aussi personnaliser le nom de domaine associé avec le réseau en spécifiant un suffix DNS pour chaque réseau.

Les réseaux d'une VM sont définie à la création de la VM. Une VM ne peut pas ajouter ou supprimer des réseaux après qu'elle ait été créée, bien que l'utilisateur peut aller dans son inviter et supprimer l'adresse IP sur la carte réseau d'un réseau particulier.

Chaque VM a juste un réseau par défaut. La réponse du serveur DHCP du routeur virtuel configurera la passerelle par défaut de l'invité comme ça pour le réseau par défaut. Plusieurs réseaux qui ne sont pas par défaut peuvent être ajoutés à un invité en complément du seul réseau, ce qui nécessite le réseau par défaut. L'administrateur peut contrôler quels réseaux sont disponible comme réseau par défaut.

Des réseaux supplémentaire peuvent être disponible pour tous les comptes ou être assigné à un compte spécifique. Les réseaux qui sont disponibles à tous les comptes sont à l'échelle de la zone. Tout utilisateur avec un accès à la zone peut créer une VM avec un accès à ce réseau. Ces réseaux à l'échelle de la zone fournissent un peu ou pas du tout d'isolation entre les invités. Les réseaux qui sont assignés à un compte spécifique fournissent une isolation plus solide.

Ajouter un réseau invité supplémentaire

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur Ajouter un réseau invité. Donnez les informations suivantes :
   - **Nom** : Le nom du réseau. Cela sera visible de l'utilisateur.
   - **Texte affiché** : La description du réseau. Cela sera visible de l'utilisateur.
   - **Zone**. Le nom de la zone à laquelle le réseau s'applique. Chaque zone est un domaine de diffusion, et par conséquent, chaque zone a une plage d'IP différente comme réseau d'invité. L'administrateur doit configurer la plage d'IP pour chaque zone.
   - **Offre réseau** : Si l'administrateur a configuré plusieurs offres de réseau, sélectionnez celle que vous voulez utiliser pour ce réseau.
   - **Passerelle invitée** : La passerelle que les invités devraient utiliser.
   - **Masque de sous réseau invité** : Le masque de sous réseau utilisé sur le sous réseau que les invités vont utiliser.
4. Cliquer sur Créer.

Reconfigurer les Réseaux dans les VMs

CloudStack vous offre la possibilité de déplacer des VMs d'un réseau à un autre et de reconfigurer son réseau. Vous pouvez retirer une VM d'un réseau et l'ajouter à un nouveau réseau. Vous pouvez aussi changer le réseau par défaut d'une machine virtuelle. Avec cette fonctionnalité, les charges d'un serveur traditionnel ou hybride peut être facilement adapté.

Cette fonctionnalité est supportée sur les hyperviseurs XenServer, VMware et KVM.

Prérequis

S'assurer que les vm-tools fonctionnent sur les VMs invités pour ajouter ou retirer les réseaux pour que cela fonctionne sur les hyperviseur VMware.

Ajouter un réseau

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Sur la gauche, cliquez sur Instances
3. Choisir la VM avec laquelle vous voulez travailler.
4. Cliquer sur l'onglet Interface.
5. Cliquer sur Ajouter un réseau à une VM.
   La boîte de dialogue Ajouter un réseau à une VM est affichée.
6. Dans la liste déroulante, sélectionner le réseau que vous aimeriez ajouter à cette VM.
   Une nouvelle interface réseau est ajoutée pour ce réseau. Vous pouvez voir les détails suivants dans la page de l'interface :
   — ID
   — Nom du réseau
   — Type
   — Adresse IP
   — Passerelle
   — Masque de sous-réseau
   — Par défaut ?
   — CIDR (pour IPv6)

Supprimer un réseau

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Sur la gauche, cliquez sur Instances
3. Choisir la VM avec laquelle vous voulez travailler.
4. Cliquer sur l'onglet Interface.
5. Repérer l'interface que vous voulez retirer.
6. Cliquer sur le bouton Supprimer une interface. 
7. Cliquer sur Oui pour confirmer.

Sélectionner le réseau par défaut.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Sur la gauche, cliquez sur Instances
3. Choisir la VM avec laquelle vous voulez travailler.
4. Cliquer sur l'onglet Interface.
5. Repérer l'interface avec laquelle vous voulez travailler.
6. Cliquer sur le bouton Définir une interface par défaut.  .
7. Cliquer sur Oui pour confirmer.

Changer l'offre de réseau pour un réseau invités.

Un utilisateur ou un administrateur peut changer l'offre de réseau qui est associée avec un réseau d'invité existant.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.

2. Si vous êtes en train de changer d'une offre de réseau qui utilise le routeur virtuel CloudStack vers une qui utilise des périphériques externes comme fournisseurs de services réseaux, vous devez d'abord stopper toutes les VMs de ce réseau.
3. Dans la navigation à gauche, choisissez Réseau.
4. Cliquer sur le nom du réseau que vous voulez modifier.
5. Dans l'onglet Détails, cliquer sur Editer. 
6. Dans Offre de Réseau, choisir la nouvelle offre de réseau, puis cliquer sur Appliquer.
   Une invite est affichée demandant si vous voulez conserver le CIDR existant. Ceci vous permet de savoir que si vous changer l'offre de réseau, le CIDR sera réaffecté.
   Si vous évoluez entre un routeur virtuel comme fournisseur et un périphérique réseau externe comme fournisseur, accepter le changement du CIDR pour continuer en cliquant sur Oui.
7. Attendre que la mise à jour soit finie. Ne pas essayer de redémarrer les VMs tant que le changement du réseau ne soit pas fini.
8. Si vous avez stoppé des VMs, redémarrer les.

12.1.7 La réservation d'IP dans les réseaux isolés invité.

Dans les réseaux d'invités isolés, une partie de l'espace d'adresse IP invité peut être réservée aux VM non CloudStack ou aux serveurs physiques. Pour ce faire, vous configurez une plage d'adresses IP réservées en spécifiant le CIDR lorsqu'un réseau invité est dans l'état Implémenté. Si vos clients souhaitent disposer de VM non contrôlées par CloudStack ou de serveurs physiques sur le même réseau, ils peuvent partager une partie de l'espace d'adressage IP qui est normalement fournie au réseau invité.

Dans une zone Avancée, une plage d'adresses IP ou un CIDR est affecté à un réseau lorsque celui-ci est défini. Le routeur virtuel CloudStack agit comme serveur DHCP et utilise le CIDR pour attribuer des adresses IP aux machines virtuelles invitées. Si vous décidez de réserver le CIDR à des fins autres que CloudStack, vous pouvez spécifier une partie de la plage d'adresses IP ou le CIDR qui ne devrait être attribuée que par le service DHCP du routeur virtuel aux machines virtuelles invitées créées dans CloudStack. Les adresses IP restantes de ce réseau sont appelées Plage d'IP Réservée. Lorsque la réservation d'IP est configurée, l'administrateur peut ajouter des machines virtuelles ou des serveurs physiques qui ne font pas partie de CloudStack au même réseau et leur attribuer les adresses IP réservées. Les VM invitées CloudStack ne peuvent plus acquérir d'IP de cette plage d'IP réservée.

Considérations sur la réservation d'IP

Prenez en compte ce qui suit avant de réserver une plage d'IP pour les machines externes à CloudStack :

- La réservation IP est prise en charge uniquement dans les réseaux isolés.
- La réservation IP ne peut être appliquée que lorsque le réseau est dans l'état Implemenété.
- Aucune réservation d'IP n'est effectuée par défaut.
- Le CIDR des VM Invités que vous spécifiez doit être un sous-réseau du CIDR du réseau.
- Spécifiez un CIDR de VM Invités valide. La réservation d'IP n'est appliquée que si aucune IP active n'existe à l'extérieur du CIDR des VM invités.
  Vous ne pouvez pas appliquer une réservation d'IP si une machine virtuelle s'est vue allouer une adresse IP se trouvant en dehors du CIDR des VM Invités.
- Pour réinitialiser une réservation d'IP existante, appliquez la réservation IP en spécifiant la valeur du réseau CIDR dans le champ CIDR.
  Par exemple, le tableau suivant décris trois scénarios de création de réseau invité :

Cas	CIDR	CIDR du réseau	Interval d'IP réservées pour les VMs Non-CloudStack	Description
1	10.1.1.0/24	Aucun	Aucun	Aucune réservation d'IP.
2	10.1.1.0/24	10.1.1.0/26	10.1.1.64 à 10.1.1.254	La réservation d'IP est configurée par l'API UpdateNetwork avec guestvmcidr=10.1.1.0/26 ou saisir 10.1.1.0/26 dans le champ CIDR de l'interface utilisateur.
3	10.1.1.0/24	Aucun	Aucun	La suppression d'une réservation d'IP est effectuée par l'API UpdateNetwork avec guestvmcidr=10.1.1.0/24 ou saisir 10.1.1.0/24 dans le champ CIDR de l'interface utilisateur.

Limitations

— La réservation d'IP n'est pas supportée si des IP actives sont trouvées à l'extérieur du CIDR des VM invités.
— La mise à niveau d'une offre réseau qui provoque une modification de son CIDR (comme une mise à niveau d'une offre sans périphériques externes vers une avec un périphérique externe), fait que la réservation d'IP devient nulle, le cas échéant. Reconfigurez la réservation d'IP dans le nouveau réseau ré-implémenté.

Recommandations

Appliquez la Réservation d'IP à un réseau invité dès que l'état du réseau passe à Implementé. Si vous appliquez la réservation peu de temps après le déploiement de la première VM invitée, des conflits mineurs surviennent lors de l'application de la réservation.

Réserver un intervalle d'IP

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquer sur le nom du réseau que vous voulez modifier.
4. Dans l'onglet Détails, cliquer sur Editer. 
   Le champ CIDR devient éditable.
5. Dans CIDR, spécifier le CIDR des VM invités.
6. Cliquer sur appliquer.
   Attendre que la mise à jour soit finie. Le CIDR du réseau et la plage d'IP réservée sont affichées dans la page de Détails.

12.1.8 Reserving Public IP Addresses and VLANs for Accounts

CloudStack provides you the ability to reserve a set of public IP addresses and VLANs exclusively for an account. During zone creation, you can continue defining a set of VLANs and multiple public IP ranges. This feature extends the functionality to enable you to dedicate a fixed set of VLANs and guest IP addresses for a tenant.

Note that if an account has consumed all the VLANs and IPs dedicated to it, the account can acquire two more resources from the system. CloudStack provides the root admin with two configuration parameter to modify this default behavior : use.system.public.ips and use.system.guest.vlans. These global parameters enable the root admin to disallow an account from acquiring public IPs and guest VLANs from the system, if the account has dedicated

resources and these dedicated resources have all been consumed. Both these configurations are configurable at the account level.

This feature provides you the following capabilities :

- Reserve a VLAN range and public IP address range from an Advanced zone and assign it to an account
- Disassociate a VLAN and public IP address range from an account
- View the number of public IP addresses allocated to an account
- Check whether the required range is available and is conforms to account limits.
  The maximum IPs per account limit cannot be superseded.

Dédier un intervalle d'adressses IP à un compte

1. Se connecter à l'interface de CloudStack comme administrateur
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Dans Zones, cliquer sur Voir toutes.
4. Choisir la zone avec laquelle vous voulez travailler.
5. Cliquer sur l'onglet Réseau.
6. Dans le noeud Public du diagramme, cliquer sur Configure.
7. Cliquer sur l'onglet intervalle IP.
   You can either assign an existing IP range to an account, or create a new IP range and assign to an account.
8. Pour assigner un intervalle d'IP existant à un compte, effectuer les actions suivantes :
   (a) Localiser l'intervalle d'IP avec lequel vous voulez travailler.
   (b) Cliquer sur le bouton Ajouter un compte  .
   La boîte de dialogue Ajouter un compte est affichée.
   (c) Spécifier les informations suivantes :
   - **Account** : The account to which you want to assign the IP address range.
   - **Domain** : The domain associated with the account.

   To create a new IP range and assign an account, perform the following :
   i. Spécifier les informations suivantes :
   - Passerelle
   - Masque de sous-réseau
   - **VLAN**
   - **IP de départ**
   - **IP de fin**
   - **Compte** : Effectuer au choix :

   A. Cliquer sur Compte.
   La page Ajouter un compte est affichée.
   B. Spécifier les informations suivantes :
   - **Account** : The account to which you want to assign an IP address range.
   - **Domain** : The domain associated with the account.

   C. Cliquez sur OK.
   ii. Cliquer sur Ajouter.

Dédier des plages de VLAN à un compte

1. After the CloudStack Management Server is installed, log in to the CloudStack UI as administrator.
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Dans Zones, cliquer sur Voir toutes.

4. Choisir la zone avec laquelle vous voulez travailler.
5. Cliquer sur l'onglet Réseau.
6. Dans le noeud Invité du diagramme, cliquer sur Configurer.
7. Select the Dedicated VLAN Ranges tab.
8. Cliquersur Dédié un intervalle de VLAN
   The Dedicate VLAN Range dialog is displayed.
9. Spécifier les informations suivantes :
   — **VLAN Range** : The VLAN range that you want to assign to an account.
   — **Account** : The account to which you want to assign the selected VLAN range.
   — **Domain** : The domain associated with the account.

12.1.9 Configurer plusieurs adresses IP sur une seule interface réseau.

CloudStack offre la possibilité d'associer plusieurs adresses IP privées par interface NIC sur les VM clients. En plus de l'IP primaire, vous pouvez affecter des adresses IP supplémentaires à l'interface NIC de la VM invitée. Cette fonctionnalité est prise en charge sur toutes les configurations réseau : Basique, Avancée et VPC. Les services de Groupes de sécurité, de NAT statique et de transfert de port sont pris en charge sur ces IP supplémentaires.

Comme toujours, vous pouvez spécifier une IP à partir du sous-réseau invité ; si elle n'est pas spécifiée, une IP est automatiquement récupérée à partir du sous-réseau VM invité. Vous pouvez afficher les IP associées à chaque NIC de la VM invité sur l'interface utilisateur. Vous pouvez appliquer du NAT sur ces IP supplémentaires de l'invité en utilisant l'option de configuration réseau dans l'interface utilisateur CloudStack. Vous devez spécifier la carte réseau à laquelle l'adresse IP doit être associée.

Cette fonctionnalité est supportée sur les hyperviseurs XenServer, KVM et VMware. Notez que les groupes de sécurité dans les zones Basiques ne sont pas supportés sur VMware.

Cas d'usages

Les exemples suivants sont des cas d'usages :
— Les périphériques réseaux, comme les pare-feu ou les répartiteurs de charge, fonctionnent généralement mieux lorsqu'ils ont accès à plusieurs adresses IP sur l'interface réseau.
— Déplacer des adresses IP privées entre interfaces ou instances. Les applications qui sont liées à des adresses IP spécifiques peuvent être déplacées entre les instances.
— Héberger plusieurs sites webs SSL sur une seule instance. Vous pouvez installer plusieurs certificats sur une seule instance, chacun associé avec une adresse IP distincte.

Lignes directrices

Pour éviter des conflits IP, configurer différents sous-réseaux lorsque plusieurs réseaux sont connectés à la même VM.

Assigner des IPs additionnelles à une VM

1. Se connecter à l'interface CloudStack.
2. Dans la barre de navigation de gauche, cliquer sur Instances.
3. Cliquez sur le nom de l'instance avec laquelle vous souhaitez travailler.
4. Dans l'onglet Détails, cliquer sur Interfaces.
5. Cliquer sur Voir les IPs secondaires.

6. Cliquez sur Obtenir une nouvelle adresse IP, et cliquez sur Oui dans la boîte de dialogue de confirmation.
   Vous devez configurer l'IP sur l'interface de la VM invitée manuellement. CloudStack ne va pas automatiquement configurer l'IP acquise sur la VM. Assurez vous que la configuration de l'adresse IP soit persistante après le redémarrage.
   Au bout de quelques instants, la nouvelle adresse IP devrait apparaître dans l'état Allouée. Vous pouvez maintenant utiliser l'adresse IP pour la redirection de port ou les règles de NAT statiques.

Changements de services de redirection de port et de StaticNAT

Étant donné que plusieurs IP peuvent être associées par carte réseau, vous êtes autorisé à sélectionner l'adresse IP désirée pour les services Port Forwarding et StaticNAT. La valeur par défaut est l'adresse IP principale. Pour activer cette fonctionnalité, un paramètre optionnel supplémentaire 'vmguestip' est ajouté aux API du port forwarding et du StaticNAT (enableStaticNat, createIpForwardingRule) pour indiquer sur quelle adresse IP le NAT doit être configuré. Si vmguestip est passé, le NAT est configuré sur l'IP privée spécifiée de la VM. Si elle n'est pas passée, le NAT est configuré sur l'adresse IP principale de la VM.

12.1.10 A propos des intervalles IP multiples

Note : Cette fonctionnalité ne peut être implémentée que sur les adresses IPv4.

CloudStack offre la flexibilité d'ajouter des plages d'IP d'invité de différents sous-réseaux dans les zones Basiques et dans les zones Avancées avec groupes de sécurité. Pour les zones avancées avec groupes de sécurité, cela implique que plusieurs sous-réseaux puissent être ajoutés au même VLAN. Grâce à cette fonctionnalité, vous pourrez ajouter des plages d'adresses IP à partir du même sous-réseau ou à partir d'un autre lorsque les adresses IP sont épuisées. Cela permet au final d'utiliser un plus grand nombre de sous-réseaux et de réduire ainsi la charge de travail liée à la gestion des adresses. Pour prendre en charge cette fonctionnalité, la capacité de l'API '' createVlanIpRange'' est étendue pour ajouter des plages d'adresses IP à partir d'un autre sous-réseau.

Assurez-vous d'avoir manuellement configuré la passerelle du nouveau sous-réseau avant d'ajouter la plage d'IP. Notez que CloudStack supporte une seule passerelle par sous-réseau ; le chevauchement de réseau n'est pas actuellement pris en compte.

Utilisez l'API `deleteVlanRange` pour supprimer les plages IP. Cette opération échoue si une IP parmi celles de la plage de suppression est en cours d'utilisation. Si la plage de suppression contient l'adresse IP d'un serveur DHCP est en cours d'exécution, CloudStack acquiert une nouvelle adresse IP à partir du même sous-réseau. Si aucune adresse IP n'est disponible dans le sous-réseau, l'opération de suppression échoue.

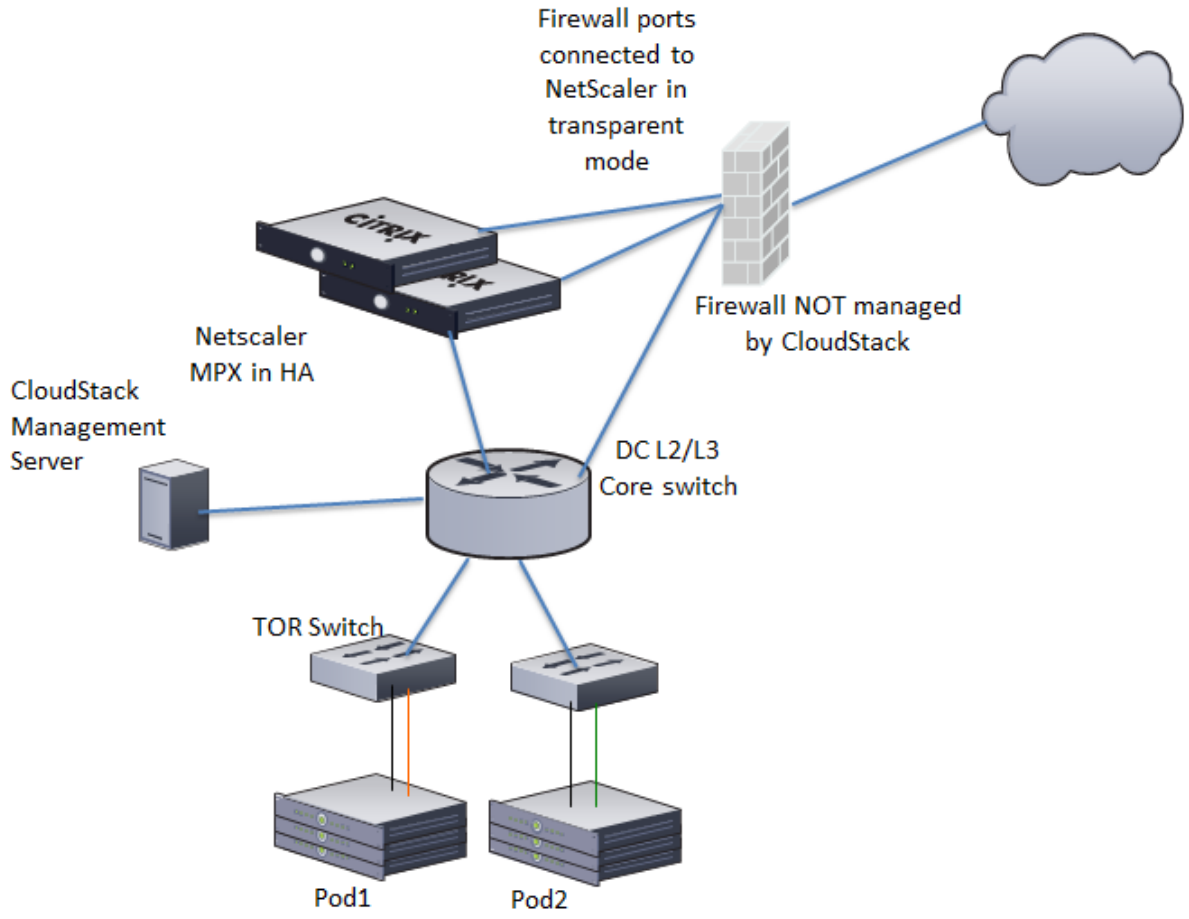
Cette fonctionnalité est supportée sur les hyperviseurs XenServer, VMware et KVM.

12.1.11 A propos d'Elastic IP

Les adresses Elastic IP (EIP) sont les adresses IP associées à un compte et qui agissent comme des adresses IP statiques. Le propriétaire du compte a le contrôle complet sur les adresses IP Elastic qui appartiennent au compte. En tant que propriétaire d'un compte, vous pouvez allouer une IP élastique à une machine virtuelle de votre choix depuis la réserve d'EIP de votre compte. Plus tard, si nécessaire, vous pouvez réaffecter l'adresse IP à une machine virtuelle différente. Cette fonctionnalité est extrêmement utile lors de la défaillance d'une VM. Au lieu de remplacer la machine virtuelle qui est en panne, l'adresse IP peut être réaffectée à une nouvelle VM de votre compte.

De manière similaire à une adresse IP publique, les adresses Elastic IP sont mappées à leurs adresses IP privées associées en utilisant du StaticNAT. Le service EIP est équipé du service StaticNAT (1 :1) dans une zone basique avec EIP activé. L'offre réseau par défaut, DefaultSharedNetscalerEIPandELBNetworkOffering, fournit à votre réseau des

services réseau EIP et ELB si un périphérique NetScaler est déployé dans votre zone. Considérez l'illustration suivante pour plus de détails.



Dans l'illustration, une appliance NetScaler est le point d'entrée ou de sortie par défaut pour les instances CloudStack et le pare-feu est l'entrée ou le point de sortie par défaut pour le reste du centre de données. Le Netscaler fournit des services de LB et un service staticNAT aux réseaux invités. Le trafic invité dans les pods et le serveur d'administration se trouvent sur différents sous-réseaux / VLAN. Le routage basé sur les stratégies dans le coeur de réseau du centre de données envoie le trafic public via le NetScaler, tandis que le reste du centre de données passe par le pare-feu.

Le workflow de l'EIP est le suivant :

- Lorsqu'une VM utilisateur est déployée, une IP publique est automatiquement acquise depuis la réserve d'IPs publiques configurée dans la zone. Cette IP appartient au compte de la VM.
- Chaque VM va avoir sa propre IP privée. Lorsque la VM de l'utilisateur démarre, le Static Nat est provisionné sur le périphérique NetScaler en utilisant des règles d'Inbound Network Address Translation (INAT) et de Reverse NAT (RNAT) entre l'IP publique et l'IP privée

  Note : L'Inbound NAT (INAT - NAT entrant) est un type de NAT pris en charge par les NetScaler, dans lequel l'adresse IP de destination est remplacée dans les paquets provenant du réseau public, comme Internet, par l'adresse IP privée d'une machine virtuelle dans le réseau privé. Le Reverse NAT (RNAT) est un type de NAT pris en charge par les NetScaler, dans lequel l'adresse IP source dans les paquets générés par une machine virtuelle dans le réseau privé est remplacée par l'adresse IP publique.

- Cette adresse IP publique par défaut sera libérée dans deux cas :
  - Lorsque la VM est stoppée. Lorsque la VM redémarre, elle reçoit à nouveau une nouvelle IP publique, qui

n'est pas nécessairement la même qui avait été initialement attribuée, depuis la réserve d'IP publiques.
— L'utilisateur acquiert une IP public (Elastic IP). Cette IP publique est associée au compte, mais ne sera pas mappée à une IP privée. Toutefois, l'utilisateur peut activer le NAT statique pour associer cette adresse IP à l'adresse IP privée d'une machine virtuelle de son compte. La règle de NAT statique pour l'IP publique peut être désactivée à tout moment. Lorsque le NAT statique est désactivé, une nouvelle IP publique est allouée à partir de la réserve, qui n'est pas nécessairement la même ayant été allouée initialement.

Pour les déploiements où les IP publiques sont des ressources limitées, vous avez la possibilité de choisir de ne pas allouer une IP publique par défaut. Vous pouvez utiliser l'option Associer une IP publique pour activer ou désactiver l'affectation d'IP publique automatique dans les zones basiques ayant l'EIP activé. Si vous désactivez l'affectation d'IP publique automatique lors de la création d'une offre réseau, seule une adresse IP privée est affectée à une machine virtuelle lorsque la machine virtuelle est déployée avec cette offre réseau. Plus tard, l'utilisateur peut acquérir une adresse IP pour la VM et activer le NAT statique.

Pour plus d'informations sur l'option d'association d'IP publique, consulter "Créer une nouvelle offre de réseau".

Note : La fonctionnalité d'association d'IP publique est conçue uniquement pour les VM utilisateur. Les VM systèmes continuent d'obtenir à la fois une adresse IP publique et une privée par défaut, sans tenir compte de la configuration de l'offre réseau.

Les nouveaux déploiements qui utilisent l'offre de réseau partagé par défaut avec services EIP et ELB pour créer un réseau partagé dans une zone basique vont continuer d'allouer des IP publiques à chaque VM utilisateur.

12.1.12 IPs portable

A propos des IP portables

Les IP portables dans CloudStack sont des réserves d'adresses IP de niveau région, qui sont élastiques de nature, qui peuvent être transférées entre zones géographiquement séparées. En tant qu'administrateur, vous pouvez provisionner un ensemble d'IP publiques portables au niveau de la région et les rendre disponibles pour utilisation par les utilisateurs. Les utilisateurs peuvent acquérir des adresses IP portables si l'administrateur a fourni des IP portables au niveau de la région dont ils font partie. Ces IP peuvent être utilisées pour n'importe quel service dans une zone avancée. Vous pouvez également utiliser des adresses IP portables pour les services EIP dans les zones basiques.

Les principales caractéristiques d'une IP portable sont :
— L'IP est attribuée de manière statique
— Il n'est pas nécessaire d'associer une IP à un réseau
— L'association IP est transférable entre les réseaux
— Les IP sont transférables entre à la fois les zones basiques et les zones avancées.
— Une IP est transférable entre VPC et les réseaux partagés ou isolés non-VPC
— Le transfert d'IP portable n'est disponible que pour le NAT static.

Lignes directrices

Avant de transférer à un autre réseau, assurez vous qu'aucune règle réseau (Pare-feu, Static Nat, Redirection de port, etc.) n'existe sur cette IP portable.

Configuration des IP portables

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la barre de navigation de gauche, cliquer sur Régions.
3. Choisir les régions avec lesquelles vous voulez travailler.

4. Cliquer sur voir l'IP Portable.
5. Cliquer sur la plage d'IP portable
   La fenêtre Ajouter une plage d'IP portable s'affiche.
6. Spécifier les informations suivantes :
   — **IP de début, IP de fin** : Une plage d'adresses IP qui sera accessible depuis Internet et sera associée aux VM invités. Saisir la première et la dernière adresse qui définissent une plage que CloudStack peut assigner aux VM invités.
   — **Passerelle** : La passerelle à utiliser pour les adresses IP portables que vous êtes en train de configurer.
   — **Masque de sous-réseau** : Le masque de sous-réseau associé avec la plage d'IP portable.
   — **VLAN** : Le VLAN qui va être utilisé pour le trafic public.
7. Cliquez sur OK.

Aquérir une IP portable

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur le nom du réseau avec lequel vous souhaitez travailler.
4. Cliquez sur Voir les adresses IP.
5. Cliquer sur Acquérir une nouvelle IP.
   La fenêtre Acquérir une nouvelle IP est affichée.
6. Spécifier si vous voulez une IP transverse à la zone ou non.
7. Cliquer sur Oui dans la boite de dialogue de confirmation.
   Après quelques instants, la nouvelle adresse IP devrait apparaître avec l'état Allouée. Vous pouvez utiliser l'adresse IP dans la redirection de port ou les règles de NATage statiques.

Transférer une IP Portable

Une IP peut être transférée depuis un réseau vers un autre seulement si le Static NAT est activé. Cependant, lorsqu'une IP portable est associée à un réseau, vous pouvez l'utiliser pour n'importe quel service du réseau.

Pour transférer une IP portable entre des réseaux, exécutez l'API suivante :

```
http://localhost:8096/client/api?command=enableStaticNat&response=json&ipaddressid=a4bc37b2-4b4e-461c
```

Remplacez l'UUID par l'UUID approprié. Par exemple, si vous souhaitez transférer une adresse IP portable vers le réseau X et une VM Y dans un réseau, exécutez les opérations suivantes :

```
http://localhost:8096/client/api?command=enableStaticNat&response=json&ipaddressid=a4bc37b2-4b4e-461c
```

12.1.13 Plusieurs sous-réseaux au sein d'un Réseau Partagé

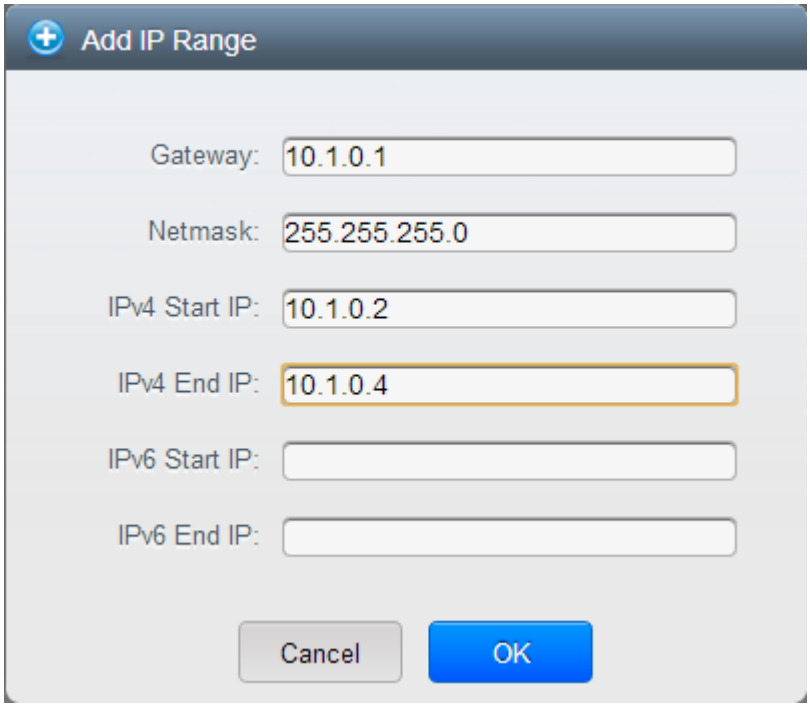
CloudStack offre la flexibilité d'ajouter des plages d'IP d'invité à partir de différents sous-réseaux dans les zones Basiques et dans les zones Avancées avec groupes de sécurité. Pour les zones avancées avec groupes de sécurité, cela implique que plusieurs sous-réseaux puissent être ajoutés au même VLAN. Grâce à cette fonctionnalité, vous pourrez ajouter des plages d'adresses IP à partir du même sous-réseau ou à partir d'un autre lorsque les adresses IP sont épuisées. Cela permet au final d'utiliser un plus grand nombre de sous-réseaux et de réduire ainsi la charge de travail liée à la gestion des adresses. Vous pouvez supprimer les plages IP que vous avez ajoutées.

Prérequis et lignes directrives

- Cette fonctionnalité ne peut seulement être implémentée :
  - Sur des adresses IPv4
  - Si le routeur virtuel est le fournisseur DHCP
  - Sur les hyperviseurs KVM, xenServer et VMware
- Configurez manuellement la passerelle du nouveau sous-réseau avant d'ajouter la plage d'IP.
- CloudStack supporte une seule passerelle par sous-réseau ; le chevauchement de réseau n'est pas actuellement pris en compte.

Ajout de plusieurs sous-réseaux à un Réseau Partagé

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Choisissez Infrastructure dans le panneau de navigation à gauche.
3. Sur Zones, cliquer sur Voir plus, puis cliquer sur la zone avec laquelle vous voulez travailler.
4. Cliquer sur le réseau physique.
5. Dans le noeud Invité du diagramme, cliquer sur Configurer.
6. Cliquer sur Réseaux.
7. Choisir les réseaux avec lesquelles vous voulez travailler.
8. Cliquer sur Voir les intervalles IP.
9. Cliquer sur Ajouter une plage d'IP.
   La boîte de dialogue Ajouter une plage d'IP s'affiche comme suit :



10. Spécifier les informations suivantes :
    Tous les champs sont obligatoires.
    - **Passerelle** : La passerelle pour le segment que vous créez. S'assurer que la passerelle est inclue dans l'intervalle du Super CIDR que vous avez spécifié lors de la création du VPC et qu'elle n'est pas en conflit avec un segment du VPC.

— **Masque de sous-réseau** : Le masque de sous-réseau pour le segment que vous créez.
Par exemple, si le CIDR du VPC est 10.0.0.0/16 et que le réseau CIDR du tiers est 10.0.1.0/24, la passerelle du tiers est 10.0.1.1, et le masque de sous réseau du tiers est 255.255.255.0.
— **IP de début, IP de fin** : Une plage d'adresses IP qui sera accessible depuis Internet et sera associée aux VM invités. Saisir la première et la dernière adresse qui définissent une plage que CloudStack peut assigner aux VM invités.

11. Cliquez sur OK.

12.1.14 Isolation in Advanced Zone Using Private VLAN

Isolation of guest traffic in shared networks can be achieved by using Private VLANs (PVLAN). PVLANs provide Layer 2 isolation between ports within the same VLAN. In a PVLAN-enabled shared network, a user VM cannot reach other user VM though they can reach the DHCP server and gateway, this would in turn allow users to control traffic within a network and help them deploy multiple applications without communication between application as well as prevent communication with other users' VMs.

— Isolate VMs in a shared networks by using Private VLANs.
— Supportée par les hyperviseurs KVM, XenServer et VMware.
— PVLAN-enabled shared network can be a part of multiple networks of a guest VM.

A propos des VLAN Privés

In an Ethernet switch, a VLAN is a broadcast domain where hosts can establish direct communication with each another at Layer 2. Private VLAN is designed as an extension of VLAN standard to add further segmentation of the logical broadcast domain. A regular VLAN is a single broadcast domain, whereas a private VLAN partitions a larger VLAN broadcast domain into smaller sub-domains. A sub-domain is represented by a pair of VLANs : a Primary VLAN and a Secondary VLAN. The original VLAN that is being divided into smaller groups is called Primary, which implies that all VLAN pairs in a private VLAN share the same Primary VLAN. All the secondary VLANs exist only inside the Primary. Each Secondary VLAN has a specific VLAN ID associated to it, which differentiates one sub-domain from another.

Three types of ports exist in a private VLAN domain, which essentially determine the behaviour of the participating hosts. Each ports will have its own unique set of rules, which regulate a connected host's ability to communicate with other connected host within the same private VLAN domain. Configure each host that is part of a PVLAN pair can be by using one of these three port designation :

— **Promiscuous** : A promiscuous port can communicate with all the interfaces, including the community and isolated host ports that belong to the secondary VLANs. In Promiscuous mode, hosts are connected to promiscuous ports and are able to communicate directly with resources on both primary and secondary VLAN. Routers, DHCP servers, and other trusted devices are typically attached to promiscuous ports.
— **Isolated VLANs** : The ports within an isolated VLAN cannot communicate with each other at the layer-2 level. The hosts that are connected to Isolated ports can directly communicate only with the Promiscuous resources. If your customer device needs to have access only to a gateway router, attach it to an isolated port.
— **Community VLANs** : The ports within a community VLAN can communicate with each other and with the promiscuous ports, but they cannot communicate with the ports in other communities at the layer-2 level. In a Community mode, direct communication is permitted only with the hosts in the same community and those that are connected to the Primary PVLAN in promiscuous mode. If your customer has two devices that need to be isolated from other customers' devices, but to be able to communicate among themselves, deploy them in community ports.

For further reading :

— Understanding Private VLANs
— Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment
— Private VLAN (PVLAN) on vNetwork Distributed Switch - Concept Overview (1010691)

Prérequis

- Use a PVLAN supported switch.
  See Private VLAN Catalyst Switch Support Matrix for more information.
- All the layer 2 switches, which are PVLAN-aware, are connected to each other, and one of them is connected to a router. All the ports connected to the host would be configured in trunk mode. Open Management VLAN, Primary VLAN (public) and Secondary Isolated VLAN ports. Configure the switch port connected to the router in PVLAN promiscuous trunk mode, which would translate an isolated VLAN to primary VLAN for the PVLAN-unaware router.
  Note that only Cisco Catalyst 4500 has the PVLAN promiscuous trunk mode to connect both normal VLAN and PVLAN to a PVLAN-unaware switch. For the other Catalyst PVLAN support switch, connect the switch to upper switch by using cables, one each for a PVLAN pair.
- Configure private VLAN on your physical switches out-of-band.
- Before you use PVLAN on XenServer and KVM, enable Open vSwitch (OVS).

Note : OVS on XenServer and KVM does not support PVLAN natively. Therefore, CloudStack managed to simulate PVLAN on OVS for XenServer and KVM by modifying the flow table.

Creating a PVLAN-Enabled Guest Network

1. Se connecter à l'interface de CloudStack comme administrateur
2. Choisissez Infrastructure dans le panneau de navigation à gauche.
3. Dans zones, cliquez sur Voir tout.
4. Cliquer sur la zone à laquelle vous voulez ajouter un réseau invité.
5. Cliquer sur l'onglet Réseau.
6. Cliquer sur le réseau physique avec lequel vous voulez travailler.
7. Sur le noeud Invité du diagramme, cliquer sur Configurer.
8. Cliquer sur l'onglet Réseau.
9. Cliquer sur Ajouter un réseau invité.
   La fenêtre Ajouter un réseau invité est affichée :
10. Spécifier les informations suivantes :
    - **Nom** : Le nom du réseau. Cela sera visible de l'utilisateur.
    - **Description** : La description courte du réseau qui peut être affichée aux utilisateurs
    - **ID VLAN** : L'ID unique du VLAN.
    - **Secondary Isolated VLAN ID** : The unique ID of the Secondary Isolated VLAN.
      For the description on Secondary Isolated VLAN, see *About Private VLAN"*.
    - **Portée** : Les portées possibles sont Domaine, Compte, Projet et Tous.
      - **Domaine** : Sélectionner Domaine limite la partée de ce réseau invité au domaine que vous spécifiez. Le réseau ne sera pas disponible pour les autres domaines.Si vous sélectionnez Accès Sous Domaine, le réseau invité est disponible à tous les sous domaines au sein du domaine sélectionné.
      - **Compte** : Le compte pour lequel le réseau invité est créé. Vous devez spécifier le domaine auquel appartient le compte.
      - **Projet** : Le projet pour lequel le réseau invité est créé. Vous devez spécifier le domaine auquel le projet appartient.
      - **Tous** : Le réseau invité est disponible pour tous les domaines, comptes, projets au sein de la zone sélectionnée.
    - **Offre réseau** : Si l'administrateur a configuré plusieurs offres de réseau, sélectionnez celle que vous voulez utiliser pour ce réseau.
    - **Passerelle** : La passerelle que les invités devraient utiliser.
    - **Masque de sous réseau** : Le masque de sous réseau du réseau que les utilisateurs vont utiliser.

— **Plage IP** : Une plage d'adresses IP qui sont accessibles depuis l'Internet est qui sont assignées aux VMs invitées.
— **Domaine Réseau** : Un suffixe DNS personnalisé au niveau du réseau. Si vous voulez assigner un nom de domaine spécial au réseau des VM invitées, spécifier un suffixe DNS.

11. Cliquer OK pour confirmer.

12.1.15 Groupes de sécurités

A propos des groupes de sécurité

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.

Note : In a zone that uses advanced networking, you can instead define multiple guest networks to isolate traffic to VMs.

Each CloudStack account comes with a default security group that denies all inbound traffic and allows all outbound traffic. The default security group can be modified so that all new VMs inherit some other desired set of rules.

Any CloudStack user can set up any number of additional security groups. When a new VM is launched, it is assigned to the default security group unless another user-defined security group is specified. A VM can be a member of any number of security groups. Once a VM is assigned to a security group, it remains in that group for its entire lifetime ; you can not move a running VM from one security group to another.

You can modify a security group by deleting or adding any number of ingress and egress rules. When you do, the new rules apply to all VMs in the group, whether running or stopped.

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.

Ajouter un groupe de sécurité

Un utilisateur ou un administrateur peut définir un nouveau groupe de sécurité.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la zone de sélection, choisir Groupes de Sécurité.
4. Cliquer sur Ajouter un groupe de sécurité.
5. Fournir un nom et une description.
6. Cliquez sur OK.
   Le nouveau groupe de sécurité apparaît dans l'onglet Détails des Groupes de Sécurité.
7. Pour rendre le groupe de sécurité utile, continuez par Ajouter des règles Ingress et Egress à un groupe de sécurité.

Groupes de Sécurité dans les Zones Avancées (KVM uniquement)

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

Les éléments suivants ne sont pas pris en charge pour cette fonctionnalité :

- Deux plages d'IP avec le même VLAN et une passerelle ou masque de réseau différent dans un réseau partagé avec groupes de sécurité.
- Deux plages d'IP avec le même VLAN et une passerelle ou un masque de réseau différent dans des réseaux partagés spécifiques à un compte.
- Plusieurs plages de VLAN dans un réseau partagé avec groupes de sécurité.
- Plusieurs plages de VLAN dans des réseaux partagés spécifiques à un compte.

Les groupes de sécurité doivent être activés dans la zone pour que cette fonctionnalité soit utilisée.

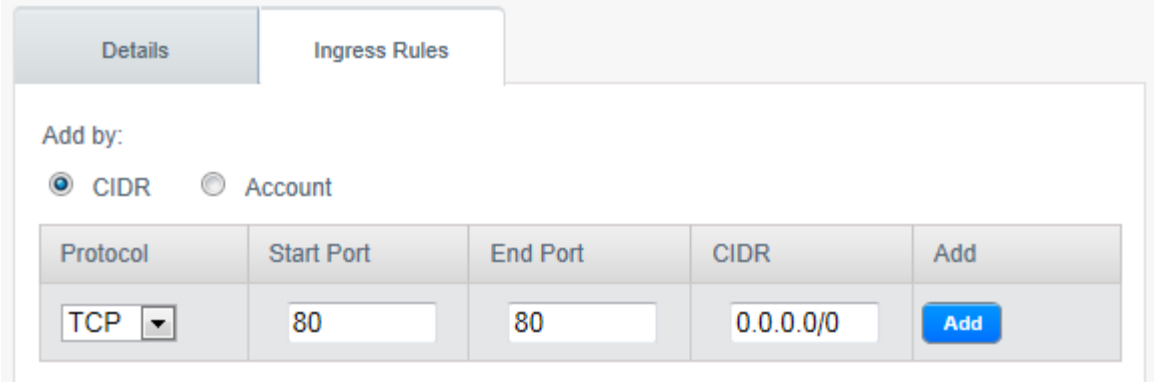
Activer les groupes de sécurités.

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.

Ajout de règles Ingress et Egress à un Groupe de Sécurité

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la liste de choix, choisir Groupes de sécurité puis cliquer sur le groupe de sécurité désiré.
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.

   L'exemple qui suit autorise l'accès HTTP entrant depuis n'importe où :



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.
   - **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. Cliquer sur Ajouter.

12.1.16 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.

About Using a NetScaler Load Balancer

Citrix NetScaler is supported as an external network element for load balancing in zones that use isolated networking in advanced zones. Set up an external load balancer when you want to provide load balancing through means other than CloudStack's provided virtual router.

Note : In a Basic zone, load balancing service is supported only if Elastic IP or Elastic LB services are enabled.

When NetScaler load balancer is used to provide EIP or ELB services in a Basic zone, ensure that all guest VM traffic must enter and exit through the NetScaler device. When inbound traffic goes through the NetScaler device, traffic is routed by using the NAT protocol depending on the EIP/ELB configured on the public IP to the private IP. The traffic

that is originated from the guest VMs usually goes through the layer 3 router. To ensure that outbound traffic goes through NetScaler device providing EIP/ELB, layer 3 router must have a policy-based routing. A policy-based route must be set up so that all traffic originated from the guest VM's are directed to NetScaler device. This is required to ensure that the outbound traffic from the guest VM's is routed to a public IP by using NAT.For more information on Elastic IP, see *"About Elastic IP"*.

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.

To install and enable an external load balancer for CloudStack management, see External Guest Load Balancer Integration in the Installation Guide.

The Citrix NetScaler comes in three varieties. The following summarizes how these variants are treated in CloudStack.

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 on ESXi and XenServer. 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 life cycle 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.

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) :

   Note : 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
```

Note : 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
```

Initial Setup of External Firewalls and Load Balancers

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).

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.

Règles de répartition de charge

A CloudStack user or administrator may create load balancing rules that balance traffic received at a public IP to one or more VMs. A user creates a rule, specifies an algorithm, and assigns the rule to a set of VMs.

Note : If you create load balancing rules while using a network service offering that includes an external load balancer device such as NetScaler, and later change the network service offering to one that uses the CloudStack virtual router, you must create a firewall rule on the virtual router for each of your existing load balancing rules so that they continue to function.

Ajouter une règle de répartition de charge

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Click the name of the network where you want to load balance the traffic.
4. Cliquez sur Voir les adresses IP.
5. Click the IP address for which you want to create the rule, then click the Configuration tab.
6. In the Load Balancing node of the diagram, click View All.
   In a Basic zone, you can also create a load balancing rule without acquiring or selecting an IP address. CloudStack internally assign an IP when you create the load balancing rule, which is listed in the IP Addresses page when the rule is created.
   To do that, select the name of the network, then click Add Load Balancer tab. Continue with #7.
7. Remplissez les champs suivants :
   - **Name** : A name for the load balancer rule.
   - **Public Port** : The port receiving incoming traffic to be balanced.
   - **Private Port** : The port that the VMs will use to receive the traffic.
   - **Algorithm** : Choose the load balancing algorithm you want CloudStack to use. CloudStack supports a variety of well-known algorithms. If you are not familiar with these choices, you will find plenty of information about them on the Internet.
   - **Stickiness** : (Optional) Click Configure and choose the algorithm for the stickiness policy. See Sticky Session Policies for Load Balancer Rules.
   - **AutoScale** : Click Configure and complete the AutoScale configuration as explained in *Configuring AutoScale*.
   - **Health Check** : (Optional ; NetScaler load balancers only) Click Configure and fill in the characteristics of the health check policy. See *Health Checks for Load Balancer Rules*.
     - **Ping path (Optional)** : Sequence of destinations to which to send health check queries. Default : / (all).
     - **Response time (Optional)** : How long to wait for a response from the health check (2 - 60 seconds). Default : 5 seconds.
     - **Interval time (Optional)** : Amount of time between health checks (1 second - 5 minutes). Default value is set in the global configuration parameter lbrule_health check_time_interval.
     - **Healthy threshold (Optional)** : Number of consecutive health check successes that are required before declaring an instance healthy. Default : 2.
     - **Unhealthy threshold (Optional)** : Number of consecutive health check failures that are required before declaring an instance unhealthy. Default : 10.
8. Click Add VMs, then select two or more VMs that will divide the load of incoming traffic, and click Apply.
   The new load balancer rule appears in the list. You can repeat these steps to add more load balancer rules for this IP address.

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.

Health Checks for Load Balancer Rules

(NetScaler load balancer only ; requires NetScaler version 10.0)

Health checks are used in load-balanced applications to ensure that requests are forwarded only to running, available services. When creating a load balancer rule, you can specify a health check policy. This is in addition to specifying the stickiness policy, algorithm, and other load balancer rule options. You can configure one health check policy per load balancer rule.

Any load balancer rule defined on a NetScaler load balancer in CloudStack can have a health check policy. The policy consists of a ping path, thresholds to define "healthy" and "unhealthy" states, health check frequency, and timeout wait interval.

When a health check policy is in effect, the load balancer will stop forwarding requests to any resources that are found to be unhealthy. If the resource later becomes available again, the periodic health check will discover it, and the resource will once again be added to the pool of resources that can receive requests from the load balancer. At any given time, the most recent result of the health check is displayed in the UI. For any VM that is attached to a load balancer rule with a health check configured, the state will be shown as UP or DOWN in the UI depending on the result of the most recent health check.

You can delete or modify existing health check policies.

To configure how often the health check is performed by default, use the global configuration setting healthcheck.update.interval (default value is 600 seconds). You can override this value for an individual health check policy.

For details on how to set a health check policy using the UI, see *Ajouter une règle de répartition de charge*.

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. Thus it helps you save compute costs by terminating underused VMs automatically and launching new VMs when you need them, without the need for manual intervention.

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.

Note : AutoScale is supported on NetScaler Release 10 Build 74.4006.e and beyond.

Prérequis

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.

  Note : 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 RHELServer"* to configure SNMP on a RHEL machine.

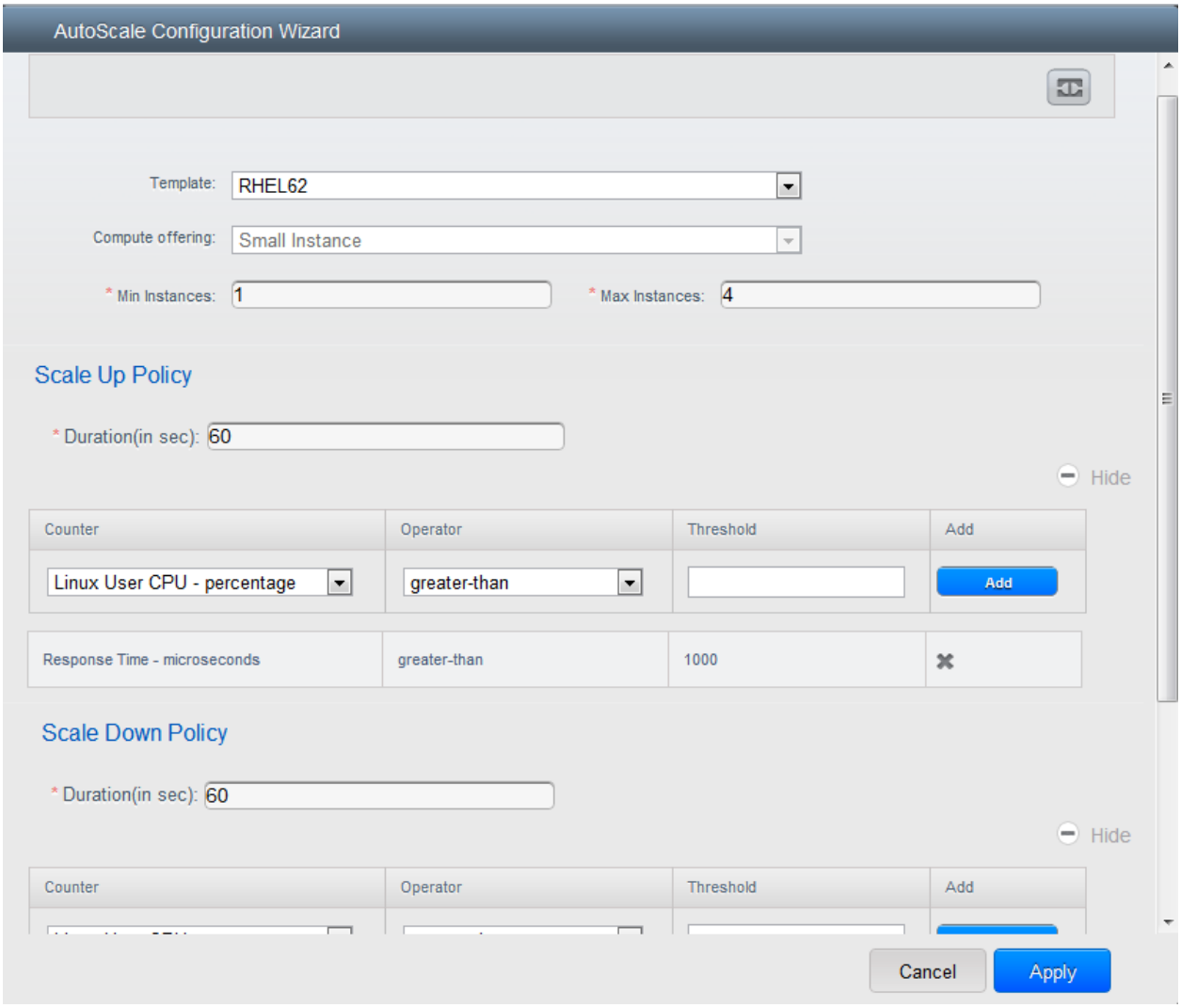
— Ensure that the endpointe.url parameter present in the Global Settings is set to the Management Server API URL. For example, `http://10.102.102.22:8080/client/api`. In a multi-node Management Server deployment, use the virtual IP address configured in the load balancer for the management server's cluster. 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

Spécifier les informations suivantes :



— **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.

Note : 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.

Note : 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 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.

12.1.17 Global Server Load Balancing Support

CloudStack supports Global Server Load Balancing (GSLB) functionalities to provide business continuity, and enable seamless resource movement within a CloudStack environment. CloudStack achieve this by extending its functionality of integrating with NetScaler Application Delivery Controller (ADC), which also provides various GSLB capabilities, such as disaster recovery and load balancing. The DNS redirection technique is used to achieve GSLB in CloudStack.

In order to support this functionality, region level services and service provider are introduced. A new service 'GSLB' is introduced as a region level service. The GSLB service provider is introduced that will provider the GSLB service. Currently, NetScaler is the supported GSLB provider in CloudStack. GSLB functionality works in an Active-Active data center environment.

About Global Server Load Balancing

Global Server Load Balancing (GSLB) is an extension of load balancing functionality, which is highly efficient in avoiding downtime. Based on the nature of deployment, GSLB represents a set of technologies that is used for various purposes, such as load sharing, disaster recovery, performance, and legal obligations. With GSLB, workloads can be distributed across multiple data centers situated at geographically separated locations. GSLB can also provide an alternate location for accessing a resource in the event of a failure, or to provide a means of shifting traffic easily to simplify maintenance, or both.

Components of GSLB

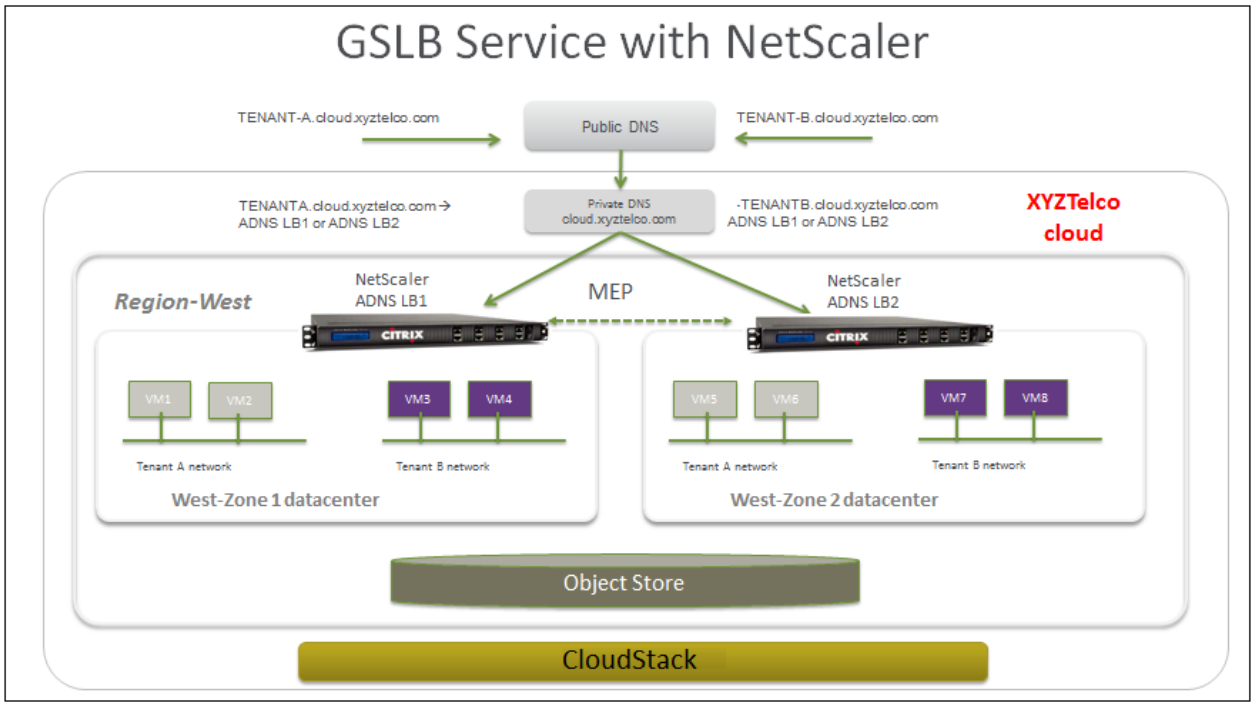
A typical GSLB environment is comprised of the following components :

- **GSLB Site** : In CloudStack terminology, GSLB sites are represented by zones that are mapped to data centers, each of which has various network appliances. Each GSLB site is managed by a NetScaler appliance that is local to that site. Each of these appliances treats its own site as the local site and all other sites, managed by other appliances, as remote sites. It is the central entity in a GSLB deployment, and is represented by a name and an IP address.
- **GSLB Services** : A GSLB service is typically represented by a load balancing or content switching virtual server. In a GSLB environment, you can have a local as well as remote GSLB services. A local GSLB service represents a local load balancing or content switching virtual server. A remote GSLB service is the one configured at one of the other sites in the GSLB setup. At each site in the GSLB setup, you can create one local GSLB service and any number of remote GSLB services.
- **GSLB Virtual Servers** : A GSLB virtual server refers to one or more GSLB services and balances traffic between traffic across the VMs in multiple zones by using the CloudStack functionality. It evaluates the configured GSLB methods or algorithms to select a GSLB service to which to send the client requests. One or more virtual servers from different zones are bound to the GSLB virtual server. GSLB virtual server does not have a public IP associated with it, instead it will have a FQDN DNS name.
- **Load Balancing or Content Switching Virtual Servers** : According to Citrix NetScaler terminology, a load balancing or content switching virtual server represents one or many servers on the local network. Clients send their requests to the load balancing or content switching virtual server's virtual IP (VIP) address, and the virtual server balances the load across the local servers. After a GSLB virtual server selects a GSLB service representing either a local or a remote load balancing or content switching virtual server, the client sends the request to that virtual server's VIP address.
- **DNS VIPs** : DNS virtual IP represents a load balancing DNS virtual server on the GSLB service provider. The DNS requests for domains for which the GSLB service provider is authoritative can be sent to a DNS VIP.
- **Authoritative DNS** : ADNS (Authoritative Domain Name Server) is a service that provides actual answer to DNS queries, such as web site IP address. In a GSLB environment, an ADNS service responds only to DNS requests for domains for which the GSLB service provider is authoritative. When an ADNS service is configured, the service provider owns that IP address and advertises it. When you create an ADNS service, the NetScaler responds to DNS queries on the configured ADNS service IP and port.

How Does GSLB Works in CloudStack ?

Global server load balancing is used to manage the traffic flow to a web site hosted on two separate zones that ideally are in different geographic locations. The following is an illustration of how GLSB functionality is provided in CloudStack : An organization, xyztelco, has set up a public cloud that spans two zones, Zone-1 and Zone-2, across geographically separated data centers that are managed by CloudStack. Tenant-A of the cloud launches a highly available solution by using xyztelco cloud. For that purpose, they launch two instances each in both the zones : VM1 and VM2 in Zone-1 and VM5 and VM6 in Zone-2. Tenant-A acquires a public IP, IP-1 in Zone-1, and configures a load balancer rule to load balance the traffic between VM1 and VM2 instances. CloudStack orchestrates setting up a virtual server on the LB service provider in Zone-1. Virtual server 1 that is set up on the LB service provider in Zone-1 represents a publicly accessible virtual server that client reaches at IP-1. The client traffic to virtual server 1 at IP-1 will be load balanced across VM1 and VM2 instances.

Tenant-A acquires another public IP, IP-2 in Zone-2 and sets up a load balancer rule to load balance the traffic between VM5 and VM6 instances. Similarly in Zone-2, CloudStack orchestrates setting up a virtual server on the LB service provider. Virtual server 2 that is setup on the LB service provider in Zone-2 represents a publicly accessible virtual server that client reaches at IP-2. The client traffic that reaches virtual server 2 at IP-2 is load balanced across VM5 and VM6 instances. At this point Tenant-A has the service enabled in both the zones, but has no means to set up a disaster recovery plan if one of the zone fails. Additionally, there is no way for Tenant-A to load balance the traffic intelligently to one of the zones based on load, proximity and so on. The cloud administrator of xyztelco provisions a GSLB service provider to both the zones. A GSLB provider is typically an ADC that has the ability to act as an ADNS (Authoritative Domain Name Server) and has the mechanism to monitor health of virtual servers both at local and remote sites. The cloud admin enables GSLB as a service to the tenants that use zones 1 and 2.



Tenant-A wishes to leverage the GSLB service provided by the xyztelco cloud. Tenant-A configures a GSLB rule to load balance traffic across virtual server 1 at Zone-1 and virtual server 2 at Zone-2. The domain name is provided as A.xyztelco.com. CloudStack orchestrates setting up GSLB virtual server 1 on the GSLB service provider at Zone-1. CloudStack binds virtual server 1 of Zone-1 and virtual server 2 of Zone-2 to GLSB virtual server 1. GSLB virtual server 1 is configured to start monitoring the health of virtual server 1 and 2 in Zone-1. CloudStack will also orchestrate setting up GSLB virtual server 2 on GSLB service provider at Zone-2. CloudStack will bind virtual server 1 of Zone-1 and virtual server 2 of Zone-2 to GLSB virtual server 2. GSLB virtual server 2 is configured to start monitoring the health of virtual server 1 and 2. CloudStack will bind the domain A.xyztelco.com to both the GSLB virtual server 1 and 2. At this point, Tenant-A service will be globally reachable at A.xyztelco.com. The private DNS server for the domain xyztelcom.com is configured by the admin out-of-band to resolve the domain A.xyztelco.com to the GSLB providers at both the zones, which are configured as ADNS for the domain A.xyztelco.com. A client when sends a DNS request to resolve A.xyztelcom.com, will eventually get DNS delegation to the address of GSLB providers at zone 1 and 2. A client DNS request will be received by the GSLB provider. The GSLB provider, depending on the domain for which it needs to resolve, will pick up the GSLB virtual server associated with the domain. Depending on the health of the virtual servers being load balanced, DNS request for the domain will be resolved to the public IP associated with the selected virtual server.

Configuring GSLB

To configure a GSLB deployment, you must first configure a standard load balancing setup for each zone. This enables you to balance load across the different servers in each zone in the region. Then on the NetScaler side, configure both NetScaler appliances that you plan to add to each zone as authoritative DNS (ADNS) servers. Next, create a GSLB site for each zone, configure GSLB virtual servers for each site, create GLSB services, and bind the GSLB services to the GSLB virtual servers. Finally, bind the domain to the GSLB virtual servers. The GSLB configurations on the two appliances at the two different zones are identical, although each sites load-balancing configuration is specific to that site.

Perform the following as a cloud administrator. As per the example given above, the administrator of xyztelco is the one who sets up GSLB :

1. In the cloud.dns.name global parameter, specify the DNS name of your tenant's cloud that make use of the GSLB service.

2. On the NetScaler side, configure GSLB as given in Configuring Global Server Load Balancing (GSLB) :
   (a) Configuring a standard load balancing setup.
   (b) Configure Authoritative DNS, as explained in Configuring an Authoritative DNS Service.
   (c) Configure a GSLB site with site name formed from the domain name details.
   Configure a GSLB site with the site name formed from the domain name.
   As per the example given above, the site names are A.xyztelco.com and B.xyztelco.com.
   For more information, see Configuring a Basic GSLB Site.
   (d) Configurer un serveur virtuel GSLB
   For more information, see Configuring a GSLB Virtual Server.
   (e) Configure a GSLB service for each virtual server.
   For more information, see Configuring a GSLB Service.
   (f) Bind the GSLB services to the GSLB virtual server.
   For more information, see Binding GSLB Services to a GSLB Virtual Server.
   (g) Bind domain name to GSLB virtual server. Domain name is obtained from the domain details.
   For more information, see Binding a Domain to a GSLB Virtual Server.
3. In each zone that are participating in GSLB, add GSLB-enabled NetScaler device.
   For more information, see *Enabling GSLB in NetScaler*.

As a domain administrator/ user perform the following :

1. Add a GSLB rule on both the sites.
   Voir "*Adding a GSLB Rule*".
2. Assign load balancer rules.
   Voir "*Assigning Load Balancing Rules to GSLB*".

Prérequis et lignes directrives

— The GSLB functionality is supported both Basic and Advanced zones.
— GSLB is added as a new network service.
— GSLB service provider can be added to a physical network in a zone.
— The admin is allowed to enable or disable GSLB functionality at region level.
— The admin is allowed to configure a zone as GSLB capable or enabled.
A zone shall be considered as GSLB capable only if a GSLB service provider is provisioned in the zone.
— When users have VMs deployed in multiple availability zones which are GSLB enabled, they can use the GSLB functionality to load balance traffic across the VMs in multiple zones.
— The users can use GSLB to load balance across the VMs across zones in a region only if the admin has enabled GSLB in that region.
— The users can load balance traffic across the availability zones in the same region or different regions.
— The admin can configure DNS name for the entire cloud.
— The users can specify an unique name across the cloud for a globally load balanced service. The provided name is used as the domain name under the DNS name associated with the cloud.
The user-provided name along with the admin-provided DNS name is used to produce a globally resolvable FQDN for the globally load balanced service of the user. For example, if the admin has configured xyztelco.com as the DNS name for the cloud, and user specifies 'foo' for the GSLB virtual service, then the FQDN name of the GSLB virtual service is foo.xyztelco.com.
— While setting up GSLB, users can select a load balancing method, such as round robin, for using across the zones that are part of GSLB.
— The user shall be able to set weight to zone-level virtual server. Weight shall be considered by the load balancing method for distributing the traffic.
— The GSLB functionality shall support session persistence, where series of client requests for particular domain name is sent to a virtual server on the same zone.
Statistics is collected from each GSLB virtual server.

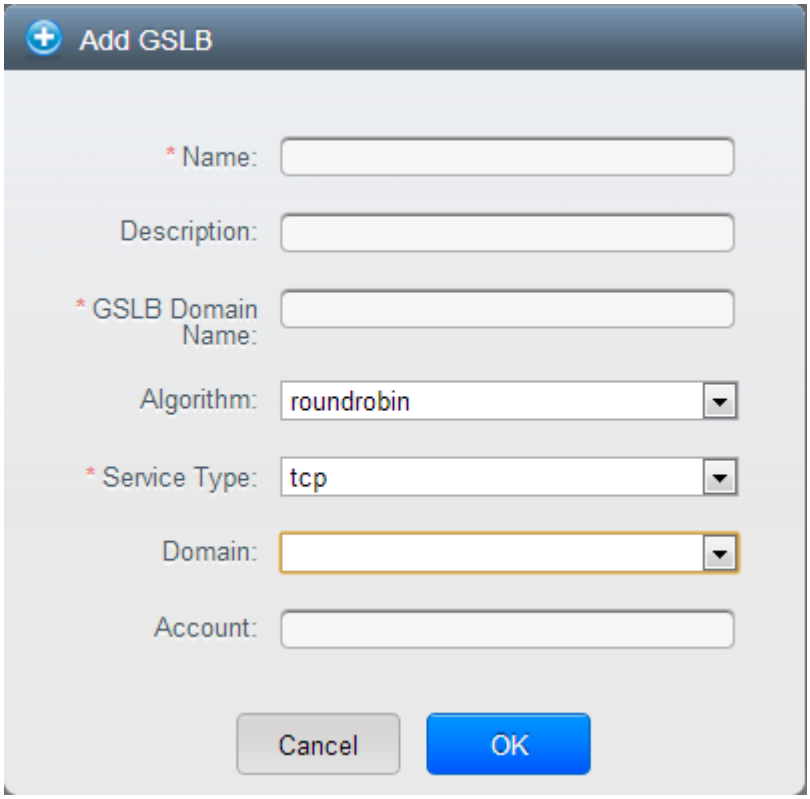
Enabling GSLB in NetScaler

In each zone, add GSLB-enabled NetScaler device for load balancing.

1. Log in as administrator to the CloudStack UI.
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Dans Zones, cliquez sur Voir plus.
4. Choisir la zone avec laquelle vous voulez travailler.
5. Click the Physical Network tab, then click the name of the physical network.
6. In the Network Service Providers node of the diagram, click Configure.
   You might have to scroll down to see this.
7. Citrix NetScaler.
8. Click Add NetScaler device and provide the following :
   Pour les NetScaler :
   — **IP Address** : The IP address of the SDX.
   — **Username/Password** : The authentication credentials to access the device. CloudStack uses these credentials to access the device.
   — **Type** : The type of device that is being added. It could be F5 Big Ip Load Balancer, NetScaler VPX, NetScaler MPX, or NetScaler SDX. For a comparison of the NetScaler types, see the CloudStack Administration Guide.
   — **Public interface** : Interface of device that is configured to be part of the public network.
   — **Private interface** : Interface of device that is configured to be part of the private network.
   — **GSLB service** : Select this option.
   — **GSLB service Public IP** : The public IP address of the NAT translator for a GSLB service that is on a private network.
   — **GSLB service Private IP** : The private IP of the GSLB service.
   — **Number of Retries**. Number of times to attempt a command on the device before considering the operation failed. Default is 2.
   — **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.
9. Cliquez sur OK.

Adding a GSLB Rule

1. Log in to the CloudStack UI as a domain administrator or user.
2. In the left navigation pane, click Region.
3. Select the region for which you want to create a GSLB rule.
4. In the Details tab, click View GSLB.
5. Cliquer sur Ajouter un GSLB.
   The Add GSLB page is displayed as follows :



6. Spécifier les informations suivantes :
   - **Name** : Name for the GSLB rule.
   - **Description** : (Optional) A short description of the GSLB rule that can be displayed to users.
   - **GSLB Domain Name** : A preferred domain name for the service.
   - **Algorithm** : (Optional) The algorithm to use to load balance the traffic across the zones. The options are Round Robin, Least Connection, and Proximity.
   - **Service Type** : The transport protocol to use for GSLB. The options are TCP and UDP.
   - **Domain** : (Optional) The domain for which you want to create the GSLB rule.
   - **Account** : (Optional) The account on which you want to apply the GSLB rule.
7. Cliquer OK pour confirmer.

Assigning Load Balancing Rules to GSLB

1. Log in to the CloudStack UI as a domain administrator or user.
2. In the left navigation pane, click Region.
3. Select the region for which you want to create a GSLB rule.
4. In the Details tab, click View GSLB.
5. Select the desired GSLB.
6. Click view assigned load balancing.
7. Click assign more load balancing.
8. Select the load balancing rule you have created for the zone.
9. Cliquer OK pour confirmer.

Limitations connues

Currently, CloudStack does not support orchestration of services across the zones. The notion of services and service providers in region are to be introduced.

12.1.18 Plages IP invités

Les plages d'IP pour le trafic réseau invité est configuré par compte par l'utilisateur. Cela permet aux utilisateurs de configurer leur réseau de façon qui va activer le lien VPN entre son réseau invité et ses clients.

Sur des réseaux partagés dans une zone Basique et dans les réseaux Avancés avec Groupes de Sécurité, vous aurez la souplesse d'ajouter de nombreuses plages d'adresses IP invité depuis différents sous-réseaux. Vous pouvez ajouter ou supprimer une plage IP à la fois. Pour plus d'informations, voir *"A propos des plages IP multiples"*.

12.1.19 Acquérir une nouvelle adresse IP

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur le nom du réseau avec lequel vous souhaitez travailler.
4. Cliquez sur Voir les adresses IP.
5. Cliquer sur Acquérir une nouvelle IP.
   La fenêtre Acquérir une nouvelle IP est affichée.
6. Spécifier si vous voulez une IP transverse à la zone ou non.
   Si vous voulez une IP portable, cliquez sur Oui dans la boîte de dialogue de confirmation. Si vous voulez une IP public normale, cliquez sur Non.
   Pour plus d'information sur l'IP Portable, voir *"IPs Portables"*.
   Après quelques instants, la nouvelle adresse IP devrait apparaître avec l'état Allouée. Vous pouvez utiliser l'adresse IP dans la redirection de port ou les règles de NATage statiques.

12.1.20 Libérer une adresse IP

Lorsque la dernière règle pour une adresse IP est supprimée, vous pouvez libérer cette adresse IP. L'adresse IP appartient toujours au VPC ; toutefois elle peut être à nouveau reprise pour n'importe quel réseau invité.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur le nom du réseau avec lequel vous souhaitez travailler.
4. Cliquez sur Voir les adresses IP.
5. Cliquer sur l'adresse IP que vous voulez libérer.
6. Cliquer sur le bouton Libérer. 

12.1.21 Static NAT

Une règle de NAT statique associe une adresse IP publique à l'adresse IP privée d'une VM afin de permettre le trafic Internet vers la machine virtuelle. L'adresse IP publique reste toujours la même, raison pour laquelle cette solution est appelée static NAT. Cette section explique comment activer ou désactiver le static NAT pour une adresse IP particulière.

Activer ou désactiver un NAT Statique

Si les règles de redirection de port sont déjà mise en oeuvre pour une adresse IP, vous ne pouvez pas activer le static NAT pour cette IP.

Si une VM invitée fait partie de plus d'un réseau, les règles de static NAT ne fonctionneront uniquement si elle sont définies sur le réseau par défaut.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur le nom du réseau avec lequel vous souhaitez travailler.
4. Cliquez sur Voir les adresses IP.
5. Cliquer sur l'adresse IP avec laquelle vous voulez travailler.
6. Cliquer sur le bouton Static NAT  .
   Le bouton bascule entre Activer et Désactiver, selon que le static NAT est actuellement activé pour l'adresse IP.
7. Si vous activez le static NAT, une boite de dialogue apparaît dans laquelle vous pouvez choisir la VM cible et cliquer sur Appliquer.

12.1.22 Redirection IP et pare-feu

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 *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.

Règles du pare-feu

By default, all incoming traffic to the public IP address is rejected by the firewall. To allow external traffic, you can open firewall ports by specifying firewall rules. You can optionally specify one or more CIDRs to filter the source IPs. This is useful when you want to allow only incoming requests from certain IP addresses.

You cannot use firewall rules to open ports for an elastic IP address. When elastic IP is used, outside access is instead controlled through the use of security groups. See *"Adding a Security Group"*.

In an advanced zone, you can also create egress firewall rules by using the virtual router. For more information, see "*Egress Firewall Rules in an Advanced Zone*".

Firewall rules can be created using the Firewall tab in the Management Server UI. This tab is not displayed by default when CloudStack is installed. To display the Firewall tab, the CloudStack administrator must set the global configuration parameter firewall.rule.ui.enabled to "true."

Pour créer une règle de pare-feu :

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Cliquez sur le nom du réseau avec lequel vous souhaitez travailler.
4. Cliquez sur Voir les adresses IP.
5. Cliquer sur l'adresse IP avec laquelle vous voulez travailler.

6. Click the Configuration tab and fill in the following values.
   — **Source CIDR** : (Optional) To accept only traffic from IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. Example : 192.168.0.0/22. Leave empty to allow all CIDRs.
   — **Protocol** : The communication protocol in use on the opened port(s).
   — **Start Port and End Port** : The port(s) you want to open on the firewall. If you are opening a single port, use the same number in both fields
   — **ICMP Type and ICMP Code** : Used only if Protocol is set to ICMP. Provide the type and code required by the ICMP protocol to fill out the ICMP header. Refer to ICMP documentation for more details if you are not sure what to enter
7. Cliquer sur Ajouter.

Egress Firewall Rules in an Advanced Zone

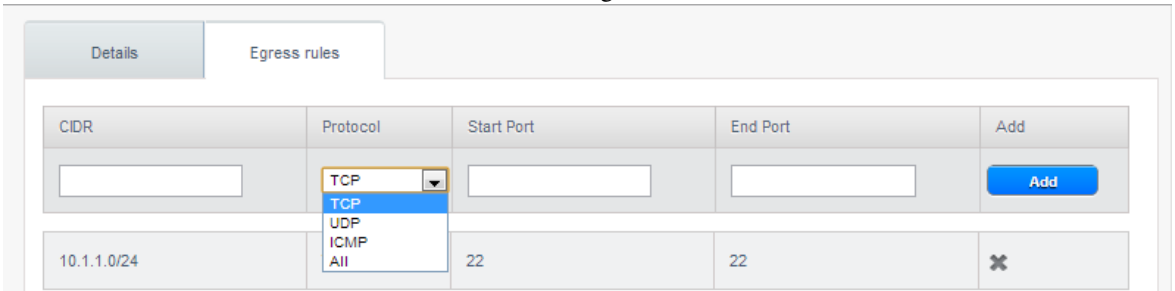
The egress traffic originates from a private network to a public network, such as the Internet. By default, the egress traffic is blocked in default network offerings, so no outgoing traffic is allowed from a guest network to the Internet. However, you can control the egress traffic in an Advanced zone 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.

Prérequis et lignes directrives

Consider the following scenarios to apply egress firewall rules :
— Egress firewall rules are supported on Juniper SRX and virtual router.
— The egress firewall rules are not supported on shared networks.
— Allow the egress traffic from specified source CIDR. The Source CIDR is part of guest network CIDR.
— Allow the egress traffic with protocol TCP,UDP,ICMP, or ALL.
— Allow the egress traffic with protocol and destination port range. The port range is specified for TCP, UDP or for ICMP type and code.
— The default policy is Allow for the new network offerings, whereas on upgrade existing network offerings with firewall service providers will have the default egress policy Deny.

Configuring an Egress Firewall Rule

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
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. Cliquer sur Ajouter.

Configurer la Stratégie par défaut Egress

The default egress policy for Isolated guest network is configured by using Network offering. Use the create network offering option to determine whether the default policy should be block or allow all the traffic to the public network from a guest network. Use this network offering to create the network. If no policy is specified, by default all the traffic is allowed from the guest network that you create by using this network offering.

Vous avez 2 options : Autoriser et Refuser.

Autoriser If you select Allow for a network offering, by default egress traffic is allowed. However, when an egress rule is configured for a guest network, rules are applied to block the specified traffic and rest are allowed. If no egress rules are configured for the network, egress traffic is accepted.

Refuser If you select Deny for a network offering, by default egress traffic for the guest network is blocked. However, when an egress rules is configured for a guest network, rules are applied to allow the specified traffic. While implementing a guest network, CloudStack adds the firewall egress rule specific to the default egress policy for the guest network.

This feature is supported only on virtual router and Juniper SRX.

1. Create a network offering with your desirable default egress policy :
   (a) Se connecter avec les droits d'administrateur à l'interface CloudStack.
   (b) Dans la barre de navigation de gauche, cliquer sur Offres de Service.
   (c) Dans Sélectionner une offre, choisir une offre réseau.
   (d) Cliquer sur Ajouter une offre de réseau.
   (e) In the dialog, make necessary choices, including firewall provider.
   (f) In the Default egress policy field, specify the behaviour.
   (g) Cliquez sur OK.
2. Create an isolated network by using this network offering.
   Based on your selection, the network will have the egress public traffic blocked or allowed.

Redirection de port

A port forward service is a set of port forwarding rules that define a policy. A port forward service is then applied to one or more guest VMs. The guest VM then has its inbound network access managed according to the policy defined by the port forwarding service. You can optionally specify one or more CIDRs to filter the source IPs. This is useful when you want to allow only incoming requests from certain IP addresses to be forwarded.

A guest VM can be in any number of port forward services. Port forward services can be defined but have no members. If a guest VM is part of more than one network, port forwarding rules will function only if they are defined on the default network

You cannot use port forwarding to open ports for an elastic IP address. When elastic IP is used, outside access is instead controlled through the use of security groups. See Security Groups.

Pour configurer la redirection de port :

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. If you have not already done so, add a public IP address range to a zone in CloudStack. See Adding a Zone and Pod in the Installation Guide.
3. Add one or more VM instances to CloudStack.
4. Dans la barre de navigation de gauche, cliquer sur Réseau.
5. Click the name of the guest network where the VMs are running.
6. Choose an existing IP address or acquire a new IP address. See *"Acquiring a New IP Address"*. Click the name of the IP address in the list.
7. Cliquer sur l'onglet Configuration.
8. In the Port Forwarding node of the diagram, click View All.
9. Remplissez les champs suivants :
   — **Public Port** : The port to which public traffic will be addressed on the IP address you acquired in the previous step.
   — **Private Port** : The port on which the instance is listening for forwarded public traffic.
   — **Protocol** : The communication protocol in use between the two ports
10. Cliquer sur Ajouter.

12.1.23 Répartition de charge IP

L'utilisateur peut choisir d'associer la même IP publique pour plusieurs invités. CloudStack implémente un répartiteur de charge de niveau TCP avec les règles suivantes.

— Round-robin
— La plus petite connexion
— IP source

C'est similaire à la redirection de port mais la destination peut être plusieurs adresses IP.

12.1.24 DNS et DHCP

Le routeur virtuel fourni les services DNS et DHCP aux invités. Il relaie les requêtes DNS aux serveurs DNS configurés dans la Zone disponible.

12.1.25 Accès distant VPN

CloudStack account owners can create virtual private networks (VPN) to access their virtual machines. If the guest network is instantiated from a network offering that offers the Remote Access VPN service, the virtual router (based on the System VM) is used to provide the service. CloudStack provides a L2TP-over-IPsec-based remote access VPN service to guest virtual networks. Since each network gets its own virtual router, VPNs are not shared across the networks. VPN clients native to Windows, Mac OS X and iOS can be used to connect to the guest networks. The account owner can create and manage users for their VPN. CloudStack does not use its account database for this purpose but uses a separate table. The VPN user database is shared across all the VPNs created by the account owner. All VPN users get access to all VPNs created by the account owner.

Note : Make sure that not all traffic goes through the VPN. That is, the route installed by the VPN should be only for the guest network and not for all traffic.

— **Road Warrior / Remote Access**. Users want to be able to connect securely from a home or office to a private network in the cloud. Typically, the IP address of the connecting client is dynamic and cannot be preconfigured on the VPN server.
— **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*".

Configuring Remote Access VPN

To set up VPN for the cloud :

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. In the left navigation, click Global Settings.
3. Set the following global configuration parameters.
   — 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 - Length of the IPSec key.
   — remote.access.vpn.user.limit - Maximum number of VPN users per account.

To enable VPN for a particular network :

1. Log in as a user or administrator to the CloudStack UI.
2. In the left navigation, click Network.
3. Click the name of the network you want to work with.
4. Cliquez sur Voir les adresses IP.
5. Click one of the displayed IP address names.
6. Click the Enable VPN button. 
   The IPsec key is displayed in a popup window.

Configuring Remote Access VPN in VPC

On enabling Remote Access VPN on a VPC, any VPN client present outside the VPC can access VMs present in the VPC by using the Remote VPN connection. The VPN client can be present anywhere except inside the VPC on which the user enabled the Remote Access VPN service.

To enable VPN for a VPC :

1. Log in as a user or administrator to the CloudStack UI.
2. In the left navigation, click Network.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées

— Adresses IP publiques
— Site-to-Site VPNs
— Listes d'ACL réseau

5. In the Router node, select Public IP Addresses.
   The IP Addresses page is displayed.
6. Click Source NAT IP address.
7. Click the Enable VPN button. 
   Click OK to confirm. The IPsec key is displayed in a pop-up window.

Now, you need to add the VPN users.

1. Click the Source NAT IP.
2. Select the VPN tab.
3. Add the username and the corresponding password of the user you wanted to add.
4. Cliquer sur Ajouter.
5. Repeat the same steps to add the VPN users.

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. You can also establish a secure connection between two VPC setups or high availability zones in your environment. Having this facility eliminates the need to establish VPN connections to individual VMs.

The difference from Remote VPN is that Site-to-site VPNs connects entire networks to each other, for example, connecting a branch office network to a company headquarters network. In a site-to-site VPN, hosts do not have VPN client software ; they send and receive normal TCP/IP traffic through a VPN gateway.

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
— CloudStack virtual routers

Note : 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 :

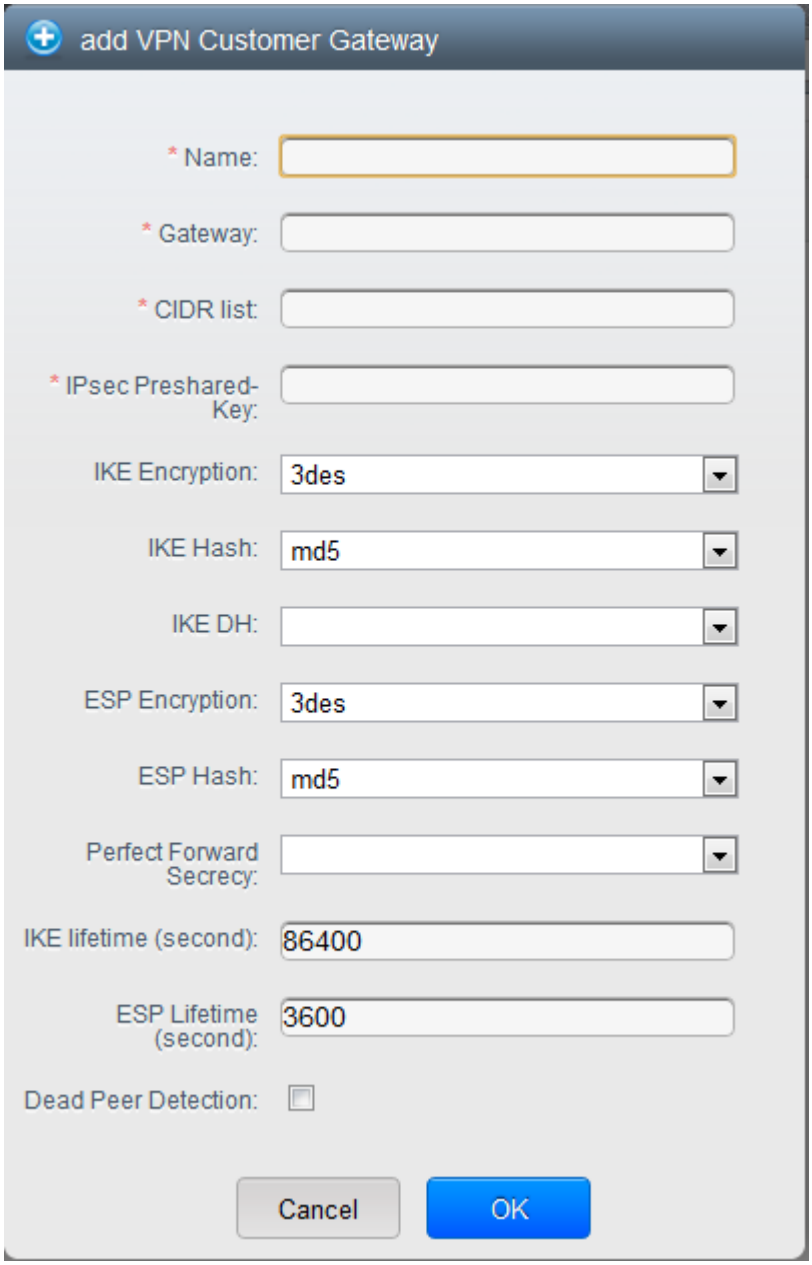
1. Create a Virtual Private Cloud (VPC).
   See "*Configurer un Cloud Privé Virtuel*".
2. Create a VPN Customer Gateway.
3. Create a VPN gateway for the VPC that you created.
4. Create VPN connection from the VPC VPN gateway to the customer VPN gateway.

Creating and Updating a VPN Customer Gateway

Note : A VPN customer gateway can be connected to only one VPN gateway at a time.

To add a VPN Customer Gateway :

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. In the Select view, select VPN Customer Gateway.
4. Click Add VPN Customer Gateway.



Fournir l'information suivante :

— **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. The sequence cannot contain a newline or double-quote.

Note : 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.

Note : 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.

Note : 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.

Note : 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. Cliquez sur OK.

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. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
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. Cliquez sur OK.

Creating a VPN gateway for the VPC

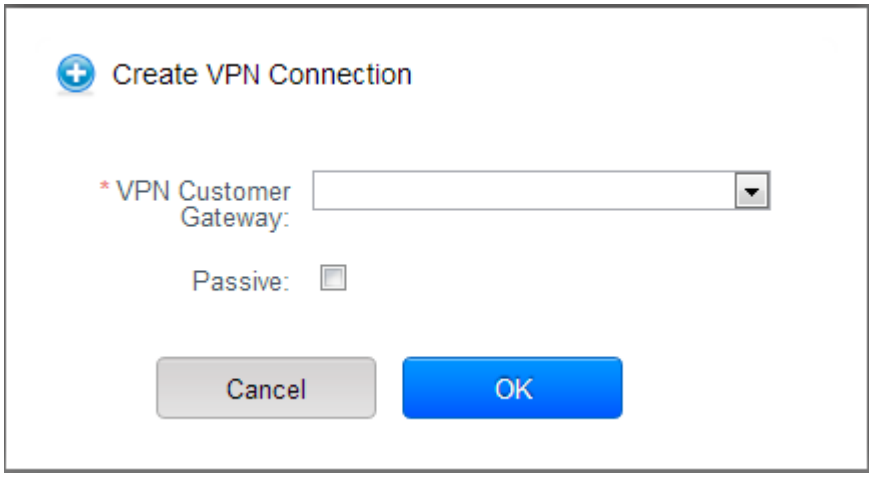
1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. Select Site-to-Site VPN.
   If you are creating the VPN gateway for the first time, selecting Site-to-Site VPN prompts you to create a VPN gateway.
6. In the confirmation dialog, click Yes to confirm.
   Within a few moments, the VPN gateway is created. You will be prompted to view the details of the VPN gateway you have created. Click Yes to confirm.
   The following details are displayed in the VPN Gateway page :
   — Adresse IP
   — Compte
   — Domaine

Creating a VPN Connection

Note : CloudStack supports creating up to 8 VPN connections.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.

3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you create for the account are listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
5. Cliquer sur l'icône Paramètres.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
6. Select Site-to-Site VPN.
   The Site-to-Site VPN page is displayed.
7. From the Select View drop-down, ensure that VPN Connection is selected.
8. Click Create VPN Connection.
   The Create VPN Connection dialog is displayed :



9. Select the desired customer gateway.
10. Select Passive if you want to establish a connection between two VPC virtual routers.
    If you want to establish a connection between two VPC virtual routers, select Passive only on one of the VPC virtual routers, which waits for the other VPC virtual router to initiate the connection. Do not select Passive on the VPC virtual router that initiates the connection.
11. Cliquer OK pour confirmer.
    Within a few moments, the VPN Connection is displayed.
    The following information on the VPN connection is displayed :
    — Adresse IP
    — Passerelle
    — Etat
    — IPSec Preshared Key
    — IKE Policy
    — ESP Policy

Site-to-Site VPN Connection Between VPC Networks

CloudStack provides you with the ability to establish a site-to-site VPN connection between CloudStack virtual routers. To achieve that, add a passive mode Site-to-Site VPN. With this functionality, users can deploy applications in multiple Availability Zones or VPCs, which can communicate with each other by using a secure Site-to-Site VPN Tunnel.

This feature is supported on all the hypervisors.

1. Create two VPCs. For example, VPC A and VPC B.
   For more information, see "*Configurer un Cloud Privé Virtuel*".
2. Create VPN gateways on both the VPCs you created.
   For more information, see *"Creating a VPN gateway for the VPC"*.
3. Create VPN customer gateway for both the VPCs.
   For more information, see *"Creating and Updating a VPN Customer Gateway"*.
4. Enable a VPN connection on VPC A in passive mode.
   For more information, see *"Creating a VPN Connection"*.
   Ensure that the customer gateway is pointed to VPC B. The VPN connection is shown in the Disconnected state.
5. Enable a VPN connection on VPC B.
   Ensure that the customer gateway is pointed to VPC A. Because virtual router of VPC A, in this case, is in passive mode and is waiting for the virtual router of VPC B to initiate the connection, VPC B virtual router should not be in passive mode.
   The VPN connection is shown in the Disconnected state.
   Creating VPN connection on both the VPCs initiates a VPN connection. Wait for few seconds. The default is 30 seconds for both the VPN connections to show the Connected state.

Restarting and Removing a VPN Connection

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
5. Cliquer sur l'icône Paramètres.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
6. Select Site-to-Site VPN.
   The Site-to-Site VPN page is displayed.
7. From the Select View drop-down, ensure that VPN Connection is selected.
   All the VPN connections you created are displayed.

8. Select the VPN connection you want to work with.
   The Details tab is displayed.

9. To remove a VPN connection, click the Delete VPN connection button 

   To restart a VPN connection, click the Reset VPN connection button present in the Details tab. 

12.1.26 A propos du routage Inter-VLAN (Applications NTiers)

Le routage Inter-VLAN (Applications nTiers) est la capacité de router le réseau entre les VLANs. Cette fonctionnalité vous permet de bâtir des Clouds Privés Virtuels (VPC), un segment isolé de votre cloud, qui peut contenir des applications multi-tier. Ces tiers sont déployés sur des différents VLANs qui peuvent communiquer avec les uns les autres. Vous provisionnez les VLANs aux tiers que vous créez, et les VMs peuvent être déployées sur différents tiers. Les VLANs sont connectés à un routeur virtuel, ce qui facilite la communication entre les VMs. En effet, vous pouvez segmenter les VMs au moyen de VLANs en différents réseaux qui peuvent accueillir des applications multi-tier, comme le Web, l'Application ou la base de données. Une telle segmentation au moyen de VLANs sépare les VMs de l'application logiquement pour plus de sécurité et pour des domaines de broadcasts réduit, alors qu'elles restent connectées physiquement au même périphérique.

Cette fonctionnalité est supportée sur les hyperviseurs XenServer, KVM et VMware.

Les avantages majeurs sont :

— L'administrateur peut déployer un ensemble de VLAN et permettre aux utilisateurs de déployer des VM sur ces VLAN. Un VLAN invité est alloué aléatoirement à un compte à partir d'un ensemble prédéfini de VLAN invités. Toutes les machines virtuelles d'un segment spécifique d'un compte résident sur le VLAN invité réservé à ce compte.

Note : Un VLAN alloué pour un compte ne peut pas être partagé entre plusieurs comptes.

— L'administrateur peut autoriser les utilisateurs à créer leur propre VPC et déployer l'application. Dans ce scénario, les VM qui appartiennent au compte sont déployées sur les VLAN alloués à ce compte.

— A la fois les administrateurs et les utilisateurs peuvent créer plusieurs VPC. L'interface NIC du réseau invité est connectée au routeur virtuel du VPC lorsque la première VM est déployée dans un segment.

— L'administrateur peut créer les passerelles suivantes pour envoyer ou recevoir le trafic depuis les VM :

  — **Passerelle VPN** : Pour plus d'informations, consultez "Créer une passerelle VPN pour le VPC" <#creating-a-vpn-gateway-for-the-vpc>'_.

  — **Passerelle publique** : La passerelle publique pour le VPC est ajoutée au routeur virtuel lorsque le routeur virtuel est créé pour le VPC. La passerelle publique n'est pas exposée aux utilisateurs finaux. Vous n'êtes pas autorisés à la lister, ni autorisé à créer des routes statiques.

  — **Passerelle privée** : Pour plus d'informations consultez "*Ajouter une passerelle privée à un VPC*".

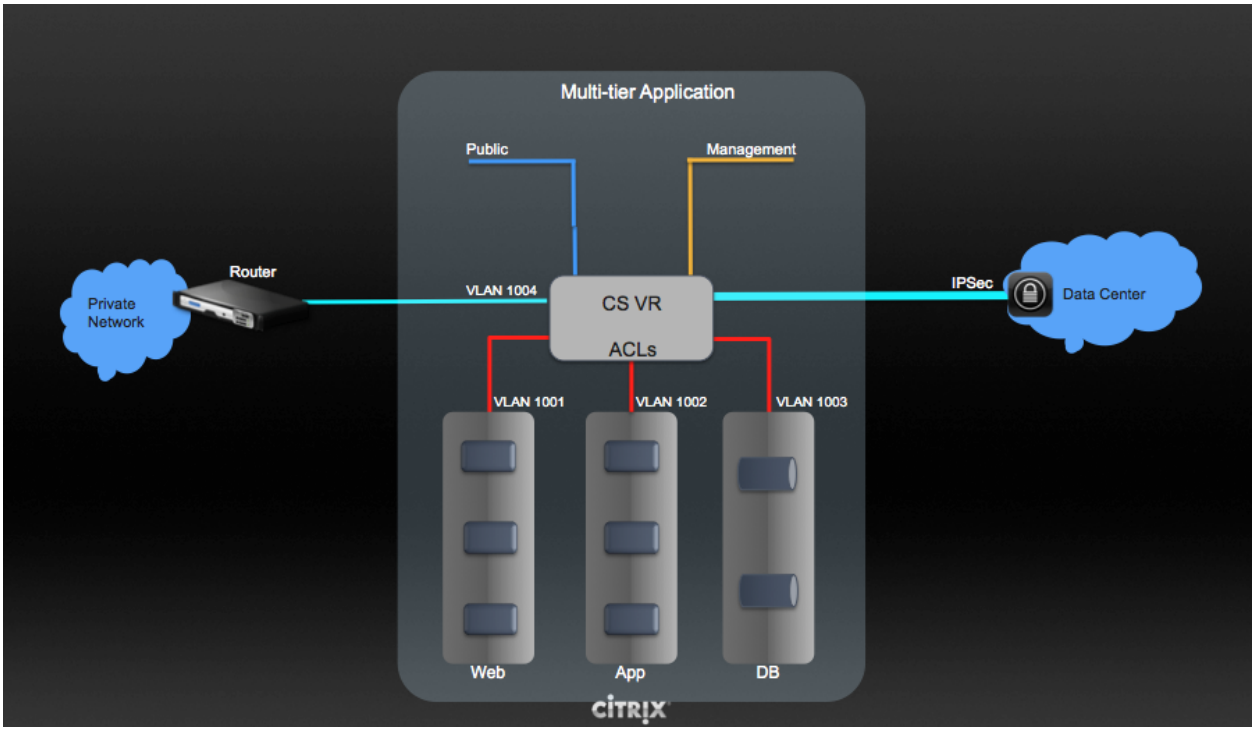
— Les administrateurs et les utilisateurs peuvent créer diverses combinaisons possibles de destinations-passerelles. Cependant, une seule passerelle de chaque type peut être utilisée dans un déploiement.
  Par exemple :

  — **VLAN et Passerelle publique** : Par exemple, une application est déployée dans le cloud, et les VM des serveurs d'applications Web communiquent avec Internet.

  — **VLAN, passerelle VPN et passerelle publique** : Par exemple, une application est déployée dans le cloud ; les VM des serveurs d'applications Web communiquent avec Internet ; et les VM de base de données communiquent avec les dispositifs en local.

— L'administrateur peut définir la liste de contrôle d'accès réseau (ACL) sur le routeur virtuel pour filtrer le trafic entre les VLAN ou entre Internet et un VLAN. Vous pouvez définir des ACL en fonction du CIDR, de la plage de ports, du protocole, du code de type (si le protocole ICMP est sélectionné) et du type Ingress / Egress.

La figure suivante montre les scénarios possibles d'une configuration Inter-VLAN :



Pour configurer un déploiement multi-tiers Inter-VLAN, voir "*Configurer un Cloud Privé Virtuel*".

12.1.27 Configurer un Cloud Privé Virtuel

A propos des Clouds Privés Virtuels

Un Cloud Privé Virtuel CloudStack est une partie privée, isolée de CloudStack. Un VPC peut avoir sa propre topologie de réseau virtuel qui ressemble à un réseau physique traditionnel. Vous pouvez lancer des VMs dans le réseau virtuel qui peuvent avoir des adresses privées dans l'intervalle de votre choix, par exemple : 10.10.10.0/16. Vous pouvez définir des parties de réseau dans l'étendue du réseau de votre VPC, permettant le regroupement des types d'instances similaires en fonction de leur intervalle d'adresse IP.

Par exemple, si un VPC dispose de la plage privée d'adresses IP 10.0.0.0/16, ses réseaux invités peuvent être dans les plages réseaux 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, etc.

Composants majeurs d'un VPC

Un VPC est constitué des composants réseaux suivants :

- **VPC** : Un VPC agit comme un conteneur pour plusieurs réseaux isolés qui peuvent communiquer les uns les autres via son routeur virtuel.
- **Segments réseaux** : chaque segment agit comme un réseau isolé avec ses propres VLANs et listes CIDR, dans lequel vous pouvez placer des groupes de ressources, comme des VM. Les segments sont segmentés par l'utilisation des VLANs. L'interface de chaque segment agit comme sa passerelle.
- **Routeur Virtuel** : Un routeur virtuel est automatiquement créé et démarré lorsque vous créez un VPC. Le routeur virtuel connecte les segments et dirige le trafic entre la passerelle publique, les passerelles VPN et les instances NAT. Pour chaque segment, une interface et une IP correspondante existent dans le routeur virtuel. Le routeur virtuel fourni les services DNS et DHCP via ses IP.

— **Passerelle publique** : Le trafic vers et provenant d'Internet est routé vers le VPC par la passerelle publique. Dans un VPC, la passerelle publique n'est pas exposée à l'utilisateur final ; en conséquence, les routes statiques ne sont pas supportées pour la passerelle publique.
— **Passerelle privée** : tout le trafic provenant ou à destination d'un réseau privé est routé vers le VPC par la passerelle privée. Pour plus d'information, voir "*Ajouter une passerelle privée à un VPC*".
— **Passerelle VPN** : Le pendant VPC d'une connexion VPN.
— **Connexion VPN site-à-site** : Une connexion VPN matérielle entre votre PVC et votre datacenter, votre réseau domestique ou autres installations. Pour plus d'information, voir "*Setting Up a Site-to-Site VPN Connection*".
— **Passerelle client** : le pendant client d'une connexion VPN. Pour plus d'informations, voir *"Créer et mettre à jour une passerelle client"*.
— **Instance NAT** : Une instance qui fourni la translation de port pour que les instances puissent accéder à Internet via la passerelle publique. Pour plus d'informations, voir "*Enabling or Disabling Static NAT on a VPC*".
— **ACL Réseau** : Une ACL réseau est un groupe d'entrées d'ACL réseau. Les entrées d'ACL réseau ne sont rien d'autre qu'un nombre de règles qui sont évaluées dans l'ordre, en commençant par la règle avec le plus petit numéro. Ces règles déterminent si le trafic est autorisé en entrée ou en sortie de n'importe quel segment associé avec l'ACL réseau. Pour plus d'informations, voir "*Configurer une liste de contrôle d'accès réseau*".

Architecture Réseau dans un VPC

Dans un VPC, les quatres options basiques d'architectures réseaux suivantes sont présentes :
— VPC avec une passerelle publique seulement
— VPC avec des passerelles publiques et privées
— VPC avec des passerelles publiques et privées et un accès VPN site à site
— VPC avec une passerelle privée seulement et un accès VPN site à site

Options de connectivité pour un VPC

Vous pouvez connecter votre VPC à :
— à Internet en passant par la passerelle publique.
— au centre de données de l'entreprise en utilisant une connexion VPN site à site en passant par la passerelle VPN.
— A la fois à Internet et à votre centre de données interne en utilisant à la fois la passerelle publique et une passerelle VPN.

Considérations sur le réseau du VPC

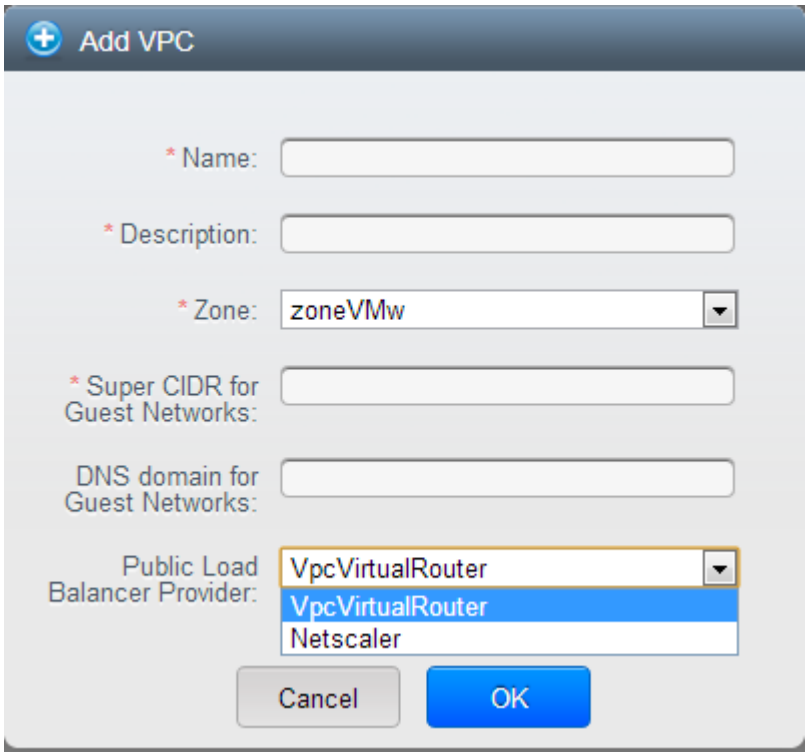
Prendre en compte ce qui suit avant de créer un VPC :
— Un VPC, par défaut, est créé dans l'état activé.
— Un VPC peut être créé dans une zone avancée seulement, et ne peut pas appartenir à plus d'une zone à la fois.
— Le nombre par défaut de VPC qu'un compte peut créer est de 20. Toutefois, vous pouvez le changer en utilisant le paramètre global max.accounts.vpcs, qui contrôle le nombre maximum de VPCs qu'un compte est autorisé à créer.
— Le nombre par défaut de segment qu'un compte peut créer dans un VPC est de 3. Vous pouvez configurer ce nombre en utilisant le paramètre vpc.max.networks.
— Chaque segment devrait avoir un CIDR unique dans le VPC. Assurez vous que le CIDR du segment est bien dans l'intervalle CIDR du VPC.
— Un segment n'appartient qu'à un seul VPC.
— Tout segment réseau à l'intérieur du VPC doit appartenir au même compte.
— Lorsqu'un VPC est créé, par défaut, une IP Source NAT lui est allouée. L'adresse IP source NAT est libérée seulement lorsque le VPC est supprimé.

— Une IP publique ne peut être utilisée que pour un seul besoin à la fois. Si l'IP est une IP source NAT, elle ne pourra pas être utilisée pour le NAT Statique ou la redirection de port.
— Les instances peuvent seulement avoir une adresse IP privée que vous provisionnez. Pour communiquer avec Internet, activer le NAT pour une instance que vous lancez dans votre VPC.
— Seulement les nouveaux réseaux peuvent être ajoutés à un VPC. Le nombre maximum de réseaux par VPC est limité par la valeur que vous spécifiez dans le paramètre vpc.max.networks. La valeur par défaut est trois.
— La service de répartition de charge ne peut être supporté que par un seul segment à l'intérieur du VPC.
— Si une adresse IP est attribuée à un segment :
  — Cette IP ne peut pas être utilisée par plus d'un segment à la fois dans le VPC. Par exemple, si vous avez les segments A et B et une IP1 publique, vous pouvez créer une règle de transmission de port en utilisant l'IP soit pour A ou B mais pas pour les deux.
  — Cette IP ne peut pas être utilisée pour du NAT Statique, pour la répartition de charge ou pour les règles de transmission de port pour un autre réseau invité au sein du VPC.
— Les accès distants VPN ne sont pas supportés dans les réseaux du VPC.

Ajouter un Cloud Privé Virtuel

Lorsque vous créer le VPC, vous fournissez simplement la zone et un ensemble d'adresses IP pour l'espace d'adresse du réseau du VPC. Vous spécifiez cet ensemble d'adresses dans le format d'un bloc Classless Inter-Domain Routing (CIDR).

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
4. Cliquer sur Ajouter VPC. La page Ajouter VPC est affichée comme suivant :



Fournir l'information suivante :
— **Nom** : Un nom court pour le VPC que vous êtes en train de créer.
— **Description** : Une description courte du VPC.
— **Zone** : Choisir la zone dans laquelle vous voulez que le VPC soit disponible.

— **Super CIDR pour les réseaux invités** : définir l'intervalle CIDR pour tous les segments (réseaux invités) au sein du VPC. Lorsque vous créez un segment, assurez vous que son CIDR soit compris dans la valeur du Super CIDR que vous avez entré. Le CIDR doit être conforme à la RFC1918.
— **Domaine DNS pour les réseaux invités** : si vous voulez assigner un nom de domaine spécial, spécifier le suffixe DNS. Ce paramètre est appliqué à tous les segments au sein du VPC. Cela implique que tous les segments que vous créez dans le VPC appartiennent au même domaine DNS. Si le paramètre n'est pas spécifié, un nom de domaine DNS est généré automatiquement.
— **Fournisseur publique de répartition de charge** : Vous avez deux options : Routeur Virtuel VPC et Netscaler.

5. Cliquez sur OK.

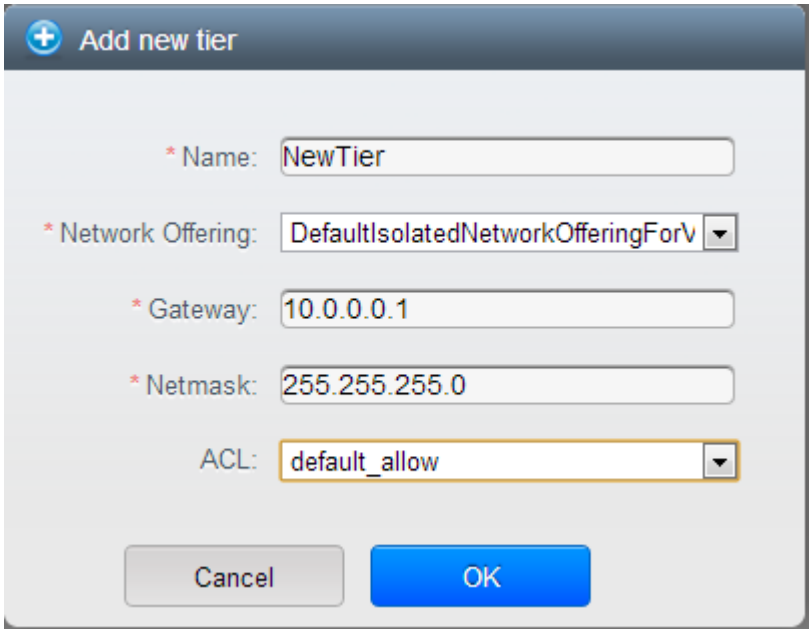
Ajouter des segments

Les Segments sont des endroits distincts à l'intérieur d'un VPC qui agissent comme des réseaux isolés, et qui n'ont pas accès aux autres tiers par défaut. Les Segments sont configurés sur différents VLANs qui peuvent communiquer entre eux en utilisant un routeur virtuel. Les Tiers fournissent un moyen simple et à faible latence pour se connecter avec d'autres tiers au sein d'un VPC.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   Tous les VPC que vous avez créé sur ce compte sont listés dans cette page.

   Note : L'utilisateur final peut voir ses propres VPCs, alors que l'administrateur du domaine ou le root peuvent voir n'importe quel VPC qu'ils sont autorisés à visualier.

4. Cliquez sur le bouton Configurer du VPC pour lequel vous désirez configurer un segment.
5. Cliquer sur Créer un réseau.
   La boîte de dialogue Ajouter un nouveau segment s'affiche comme suit :



   Si vous avez déjà créé un segment, le diagramme du VPC est affiché. Cliquez sur Créer un segment pour en ajouter un nouveau.

6. Spécifier les informations suivantes :
   Tous les champs sont obligatoires.
   — **Nom** : Un nom unique pour le segment que vous créez.
   — **Offre réseau** : Les offres par défaut de réseaux sont listées : Internal LB, DefaultIsolatedNetworkOffering-ForVpcNetworksNoLB, DefaultIsolatedNetworkOfferingForVpcNetworks
   Dans un VPC, un seul segment peut être créé en utilisant une offre réseau avec répartition de charge activée.
   — **Passerelle** : La passerelle pour le segment que vous créez. S'assurer que la passerelle est inclue dans l'intervalle du Super CIDR que vous avez spécifié lors de la création du VPC et qu'elle n'est pas en conflit avec un segment du VPC.
   — **VLAN** : L'ID du VLAN pour le segment que l'administrateur root créé.
   Cette option n'est seulement visible que si l'offre réseau que vous avez sélectionné est VLAN-enabled. Pour plus d'informations, voir "Assigner des VLANs à des réseaux isolés".
   — **Masque de sous-réseau** : Le masque de sous-réseau pour le segment que vous créez.
   Par exemple, si le CIDR du VPC est 10.0.0.0/16 et que le réseau CIDR du tiers est 10.0.1.0/24, la passerelle du tiers est 10.0.1.1, et le masque de sous réseau du tiers est 255.255.255.0.
7. Cliquez sur OK.
8. Continuer avec la configuration des contrôle d'accès pour ce segment.

Configurer une liste de contrôle d'accès réseau

Définissez la liste de contrôle d'accès réseau (ACL) sur le routeur virtuel VPC pour contrôler le trafic entrant (ingress) et sortant (egress) entre les VPC des segments, les segments et Internet. Par défaut, tout le trafic entrant vers les réseaux invités est bloqué et tout le trafic sortant des réseaux invités est autorisé, une fois que vous ajoutez une règle ACL pour le trafic sortant, seul le trafic sortant spécifié dans cette règle ACL est autorisé, le reste est bloqué. Pour ouvrir les ports, vous devez créer une nouvelle ACL réseau. Les ACL réseau ne peuvent être créées pour les segments que si le service NetworkACL est pris en charge.

A propos des listes d'ACL réseau

Dans la terminologie CloudStack, une ACL réseau est un groupe d'entrées d'ACL réseau. Les entrées d'ACL réseau ne sont rien d'autre que des règles numérotées qui sont évaluées dans l'ordre, en commençant par la règle numérotée la plus faible. Ces règles déterminent si le trafic est autorisé en entrée ou en sortie de n'importe quel segment associé à l'ACL réseau. Vous devez ajouter les entrées d'ACL réseau à la liste d'ACL réseau, puis associer la liste ACL réseau à un segment. L'ACL réseau est associée à un VPC et peut être affectée à plusieurs VPC de segments dans un VPC. Un segment peut être associé à une ACL réseau à tout moment. Chaque segment peut être associé à une seule ACL.

L'ACL réseau par défaut est utilisée lorsqu'aucune ACL n'est associée. Le comportement par défaut est de bloquer tout le trafic entrant et d'autoriser le trafic sortant depuis les segments. L'ACL réseau par défaut ne peut pas être supprimée ou modifiée. Le contenu de l'ACL réseau par défaut est :

Règle	Protocole	Type de trafic	Action	CIDR
1	Tout	Règles entrantes	Refuser	0.0.0.0/0
2	Tout	Règles sortantes	Refuser	0.0.0.0/0

Créer les listes d'ACL

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.

4. Click the Configure button of the VPC.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. Sélectionner les listes d'ACL réseaux.
   Les règles par défaut suivantes sont affichées dans la page d'ACL réseau : default_allow, default_deny.
6. Cliquer sur Ajouter des listes d'ACL et spécifier ce qui suit :
   — **Nom de la liste d'ACL** : Un nom pour la liste d'ACL.
   — **Description** : Une description courte de la liste d'ACL qui peut être affichée aux utilisateurs.

Créer une règle d'ACL

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC.
5. Sélectionner les listes d'ACL réseaux.
   En complément aux listes d'ACL personnalisées que vous avez créés, les règles par défaut suivantes sont affichées dans la page d'ACL réseaux : default_allow, default_deny.
6. Sélectionner la liste d'ACL désirée.
7. Sélectionner l'onglet Règles de liste d'ACL.
   Pour ajouter une règle d'ACL, remplir les champs suivants pour spécifier quel type de trafic réseau est autorisé dans le VPC.
   — **Numéro de règle** : L'ordre dans lequel les règles sont évaluées.
   — **CIDR** : Le CIDR agit en tant que CIDR source pour les règles Ingress et en tant que CIDR de destination pour les règles Egress. Pour accepter le trafic uniquement depuis ou vers les adresses IP d'un bloc d'adresses particulier, entrez un CIDR ou une liste séparée par des virgules de CIDR. Le CIDR est l'adresse IP de base du trafic entrant. Par exemple, 192.168.0.0/22. Pour autoriser tous les CIDR, saisissez 0.0.0.0/0.
   — **Action** : Quelle action doit être prise. Autoriser le trafic ou le bloquer.
   — **Protocole** : Le protocole réseau que les sources utilisent pour envoyer le trafic vers le segment. Les protocoles TCP et UDP sont généralement utilisés pour l'échange de données et les communications avec l'utilisateur final. Le protocole ICMP est généralement utilisé pour envoyer des messages d'erreur ou des données de surveillance du réseau. All supporte tout le trafic. La dernière option est de fournir le numéro de protocole.
   — **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.
   — **Protocol Number** : The protocol number associated with IPv4 or IPv6. For more information, see Protocol Numbers.
   — **ICMP Type**, **ICMP Code** (ICMP only) : The type of message and error code that will be sent.
   — **Traffic Type** : The type of traffic : Incoming or outgoing.

8. Cliquer sur Ajouter. La règle ACL est ajouée.
   Vous pouvez éditer les étiquettes assignées aux règles d'ACL et supprimer les règles d'ACL que vous avez créées. Cliquer sur le bouton approprié dans l'onglet Détails.

Créer un segment avec une liste d'ACL personnalisée.

1. Créer un VPC.
2. Créer une liste d'ACL personnalisée.
3. Ajouter des règles d'ACL à une liste d'ACL.
4. Créer un segment dans le VPC.
   Sélectionner la liste d'ACL désirée lors de la création du segment.
5. Cliquez sur OK.

Assigner une liste d'ACL personnalisée à un segment

1. Créer un VPC.
2. Créer un segment dans le VPC.
3. Associer le segment avec la règle d'ACL par défaut.
4. Créer une liste d'ACL personnalisée.
5. Ajouter des règles d'ACL à une liste d'ACL.
6. Sélectionner le segment pour lequel vous voulez assigner l'ACL personnalisée.
7. Cliquer sur l'icone Remplacer la liste d'ACL. 
   La boîte de dialogue Remplacer la liste d'ACL est affichée.
8. Sélectionner la liste d'ACL désirée.
9. Cliquez sur OK.

Ajouter une passerelle privée à un VPC

A private gateway can be added by the root admin only. The VPC private network has 1 :1 relationship with the NIC of the physical network. You can configure multiple private gateways to a single VPC. No gateways with duplicated VLAN and IP are allowed in the same data center.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to configure load balancing rules.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
5. Cliquer sur l'icône Paramètres.
   Les options suivantes sont affichées.
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :

— Passerelles privées
— Adresses IP publiques
— Site-to-Site VPNs
— Listes d'ACL réseau

6. Sélectionner Passerelles privées.
   La page Passerelles est affichée.
7. Cliquer sur Ajouter une nouvelle passerelle :
   add-new-gateway-vpc.png|
8. Spécifier les informations suivantes :
   — **Réseau physique** : Le réseau physique que vous avez créé dans la zone.
   — **Adresse IP** : L'adresse IP associée avec la passerelle du VPC.
   — **Passerelle** : La passerelle par laquelle le trafic est routé depuis et vers le VPC.
   — **Masque de sous-réseaux** : Le masque de sous-réseaux associé avec la passerelle du VPC.
   — **VLAN** : Le VLAN associé avec la passerelle du VPC.
   — **Source NAT** : Sélectionner cette option pour activer le service de NAT source sur la passerelle privée du VPC.
   Voir "*Source NAT on Private Gateway*".
   — **ACL** : Controls both ingress and egress traffic on a VPC private gateway. By default, all the traffic is blocked.
   Voir "*ACL sur une passerelle privée*".
   The new gateway appears in the list. You can repeat these steps to add more gateway for this VPC.

Source NAT on Private Gateway

You might want to deploy multiple VPCs with the same super CIDR and guest tier CIDR. Therefore, multiple guest VMs from different VPCs can have the same IPs to reach a enterprise data center through the private gateway. In such cases, a NAT service need to be configured on the private gateway to avoid IP conflicts. If Source NAT is enabled, the guest VMs in VPC reaches the enterprise network via private gateway IP address by using the NAT service.

The Source NAT service on a private gateway can be enabled while adding the private gateway. On deletion of a private gateway, source NAT rules specific to the private gateway are deleted.

To enable source NAT on existing private gateways, delete them and create afresh with source NAT.

ACL sur une passerelle privée

The traffic on the VPC private gateway is controlled by creating both ingress and egress network ACL rules. The ACLs contains both allow and deny rules. As per the rule, all the ingress traffic to the private gateway interface and all the egress traffic out from the private gateway interface are blocked.

You can change this default behaviour while creating a private gateway. Alternatively, you can do the following :

1. In a VPC, identify the Private Gateway you want to work with.
2. In the Private Gateway page, do either of the following :
   — Use the Quickview. See 3.
   — Use the Details tab. See 4 through .
3. In the Quickview of the selected Private Gateway, click Replace ACL, select the ACL rule, then click OK
4. Click the IP address of the Private Gateway you want to work with.
5. Dans l'onglet Détail, cliquer sur le bouton Remplacer les ACL. 
   La boîte de dialogue Remplacer la liste d'ACL est affichée.
6. Sélectionner la règle d'ACL puis cliquer sur OK.
   Wait for few seconds. You can see that the new ACL rule is displayed in the Details page.

Creating a Static Route

CloudStack enables you to specify routing for the VPN connection you create. You can enter one or CIDR addresses to indicate which traffic is to be routed back to the gateway.

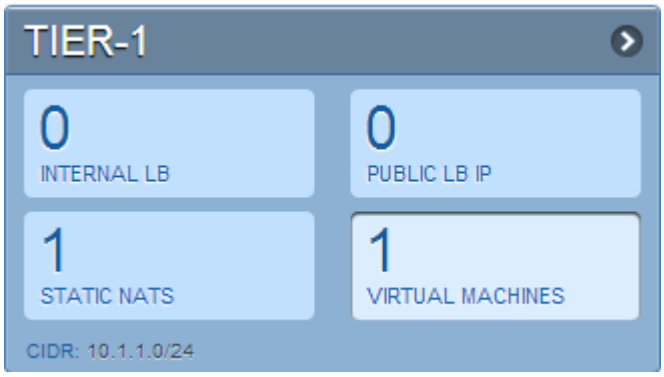
1. In a VPC, identify the Private Gateway you want to work with.
2. In the Private Gateway page, click the IP address of the Private Gateway you want to work with.
3. Select the Static Routes tab.
4. Specify the CIDR of destination network.
5. Cliquer sur Ajouter.
   Wait for few seconds until the new route is created.

Blacklisting Routes

CloudStack enables you to block a list of routes so that they are not assigned to any of the VPC private gateways. Specify the list of routes that you want to blacklist in the `blacklisted.routes` global parameter. Note that the parameter update affects only new static route creations. If you block an existing static route, it remains intact and continue functioning. You cannot add a static route if the route is blacklisted for the zone.

Déployer des VM dans un segment

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you have created are listed.
5. Click Virtual Machines tab of the tier to which you want to add a VM.



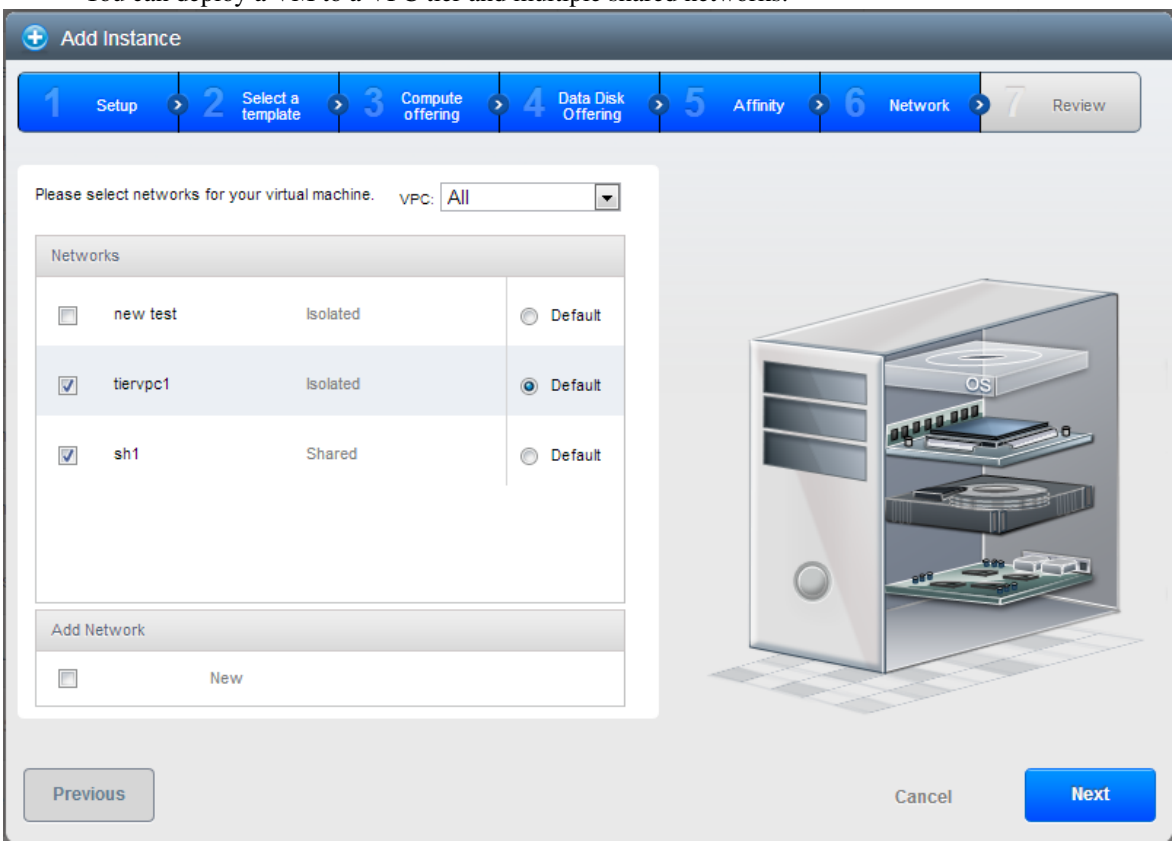
   The Add Instance page is displayed.
   Follow the on-screen instruction to add an instance. For information on adding an instance, see the Installation Guide.

Deploying VMs to VPC Tier and Shared Networks

CloudStack allows you deploy VMs on a VPC tier and one or more shared networks. With this feature, VMs deployed in a multi-tier application can receive monitoring services via a shared network provided by a service provider.

1. Se connecter à l'interface de CloudStack comme administrateur.

2. Dans la barre de navigation de gauche, choisir Instances.
3. Cliquer sur Ajouter une instance.
4. Sélectionner une zone.
5. Select a template or ISO, then follow the steps in the wizard.
6. Ensure that the hardware you have allows starting the selected service offering.
7. Under Networks, select the desired networks for the VM you are launching.
   You can deploy a VM to a VPC tier and multiple shared networks.



8. Click Next, review the configuration and click Launch.
   Your VM will be deployed to the selected VPC tier and shared network.

Acquérir une nouvelle adresse IP pour un VPC

When you acquire an IP address, all IP addresses are allocated to VPC, not to the guest networks within the VPC. The IPs are associated to the guest network only when the first port-forwarding, load balancing, or Static NAT rule is created for the IP or the network. IP can't be associated to more than one network at a time.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
   Les options suivantes sont affichées.
   — Internal LB
   — Public LB IP

— Static NAT
— Machines Virtuelles
— CIDR
The following router information is displayed :
— Passerelles privées
— Adresses IP publiques
— Site-to-Site VPNs
— Listes d'ACL réseau

5. Sélectionner les adresses IP.
   La page des Adresses IP Publiques est affichée.
6. Cliquez sur Obtenir une nouvelle adresse IP, et cliquez sur Oui dans la boîte de dialogue de confirmation.
   You are prompted for confirmation because, typically, IP addresses are a limited resource. Within a few moments, the new IP address should appear with the state Allocated. You can now use the IP address in port forwarding, load balancing, and static NAT rules.

Releasing an IP Address Alloted to a VPC

The IP address is a limited resource. If you no longer need a particular IP, you can disassociate it from its VPC and return it to the pool of available addresses. An IP address can be released from its tier, only when all the networking (port forwarding, load balancing, or StaticNAT) rules are removed for this IP address. The released IP address will still belongs to the same VPC.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC whose IP you want to release.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
   Les options suivantes sont affichées.
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. Sélectionner Adresses IP Publiques.
   The IP Addresses page is displayed.
6. Cliquer sur l'IP que vous voulez rendre.
7. In the Details tab, click the Release IP button 

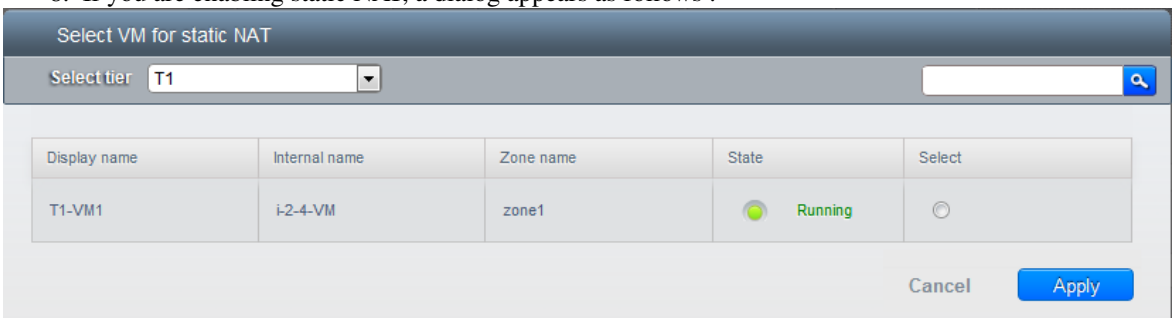
Enabling or Disabling Static NAT on a VPC

A static NAT rule maps a public IP address to the private IP address of a VM in a VPC to allow Internet traffic to it. This section tells how to enable or disable static NAT for a particular IP address in a VPC.

Si les règles de redirection de port sont déjà mise en oeuvre pour une adresse IP, vous ne pouvez pas activer le static NAT pour cette IP.

Si une VM invitée fait partie de plus d'un réseau, les règles de static NAT ne fonctionneront uniquement si elle sont définies sur le réseau par défaut.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
   For each tier, the following options are displayed.
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. In the Router node, select Public IP Addresses.
   The IP Addresses page is displayed.
6. Cliquer sur l'IP avec laquelle vous voulez travailler.
7. In the Details tab,click the Static NAT button.  The button toggles between Enable and Disable, depending on whether static NAT is currently enabled for the IP address.
8. If you are enabling static NAT, a dialog appears as follows :



9. Select the tier and the destination VM, then click Apply.

Adding Load Balancing Rules on a VPC

In a VPC, you can configure two types of load balancing : external LB and internal LB. External LB is nothing but a LB rule created to redirect the traffic received at a public IP of the VPC virtual router. The traffic is load balanced within a tier based on your configuration. Citrix NetScaler and VPC virtual router are supported for external LB. When you use internal LB service, traffic received at a tier is load balanced across different VMs within that tier. For example, traffic reached at Web tier is redirected to another VM in that tier. External load balancing devices are not supported for internal LB. The service is provided by a internal LB VM configured on the target tier.

Load Balancing Within a Tier (External LB)

A CloudStack user or administrator may create load balancing rules that balance traffic received at a public IP to one or more VMs that belong to a network tier that provides load balancing service in a VPC. A user creates a rule, specifies an algorithm, and assigns the rule to a set of VMs within a tier.

Enabling NetScaler as the LB Provider on a VPC Tier

1. Add and enable Netscaler VPX in dedicated mode.
   Netscaler can be used in a VPC environment only if it is in dedicated mode.
2. Create a network offering, as given in "*Creating a Network Offering for External LB*".
3. Create a VPC with Netscaler as the Public LB provider.
   For more information, see *"Adding a Virtual Private Cloud"*.
4. For the VPC, acquire an IP.
5. Create an external load balancing rule and apply, as given in *Creating an External LB Rule*.

Creating a Network Offering for External LB To have external LB support on VPC, create a network offering as follows :

1. Log in to the CloudStack UI as a user or admin.
2. From the Select Offering drop-down, choose Network Offering.
3. Cliquer sur Ajouter une offre de réseau.
4. In the dialog, make the following choices :
   - **Name** : Any desired name for the network offering.
   - **Description** : A short description of the offering that can be displayed to users.
   - **Network Rate** : Allowed data transfer rate in MB per second.
   - **Traffic Type** : The type of network traffic that will be carried on the network.
   - **Guest Type** : Choose whether the guest network is isolated or shared.
   - **Persistent** : Indicate whether the guest network is persistent or not. The network that you can provision without having to deploy a VM on it is termed persistent network.
   - **VPC** : This option indicate whether the guest network is Virtual Private Cloud-enabled. A Virtual Private Cloud (VPC) is a private, isolated part of CloudStack. A VPC can have its own virtual network topology that resembles a traditional physical network. For more information on VPCs, see *"About Virtual Private Clouds"*.
   - **Specify VLAN** : (Isolated guest networks only) Indicate whether a VLAN should be specified when this offering is used.
   - **Supported Services** : Select Load Balancer. Use Netscaler or VpcVirtualRouter.
   - **Load Balancer Type** : Select Public LB from the drop-down.
   - **LB Isolation** : Select Dedicated if Netscaler is used as the external LB provider.
   - **System Offering** : Choose the system service offering that you want virtual routers to use in this network.
   - **Conserve mode** : Indicate whether to use conserve mode. In this mode, network resources are allocated only when the first virtual machine starts in the network.
5. Click OK and the network offering is created.

Creating an External LB Rule

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.

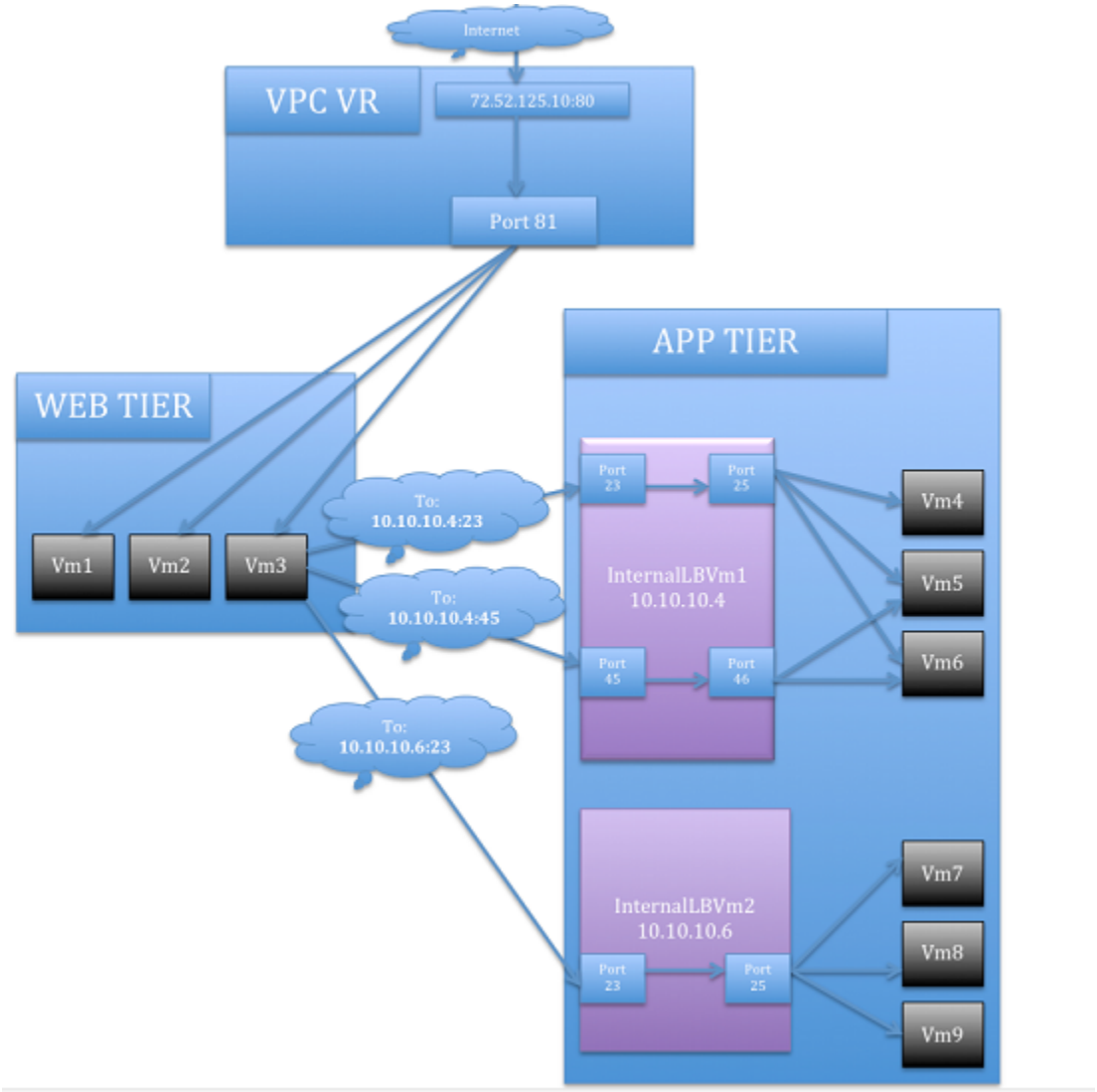
4. Click the Configure button of the VPC, for which you want to configure load balancing rules.
   The VPC page is displayed where all the tiers you created listed in a diagram.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. In the Router node, select Public IP Addresses.
   The IP Addresses page is displayed.
6. Click the IP address for which you want to create the rule, then click the Configuration tab.
7. In the Load Balancing node of the diagram, click View All.
8. Select the tier to which you want to apply the rule.
9. Spécifier les informations suivantes :
   — **Name** : A name for the load balancer rule.
   — **Public Port** : The port that receives the incoming traffic to be balanced.
   — **Private Port** : The port that the VMs will use to receive the traffic.
   — **Algorithm**. Choose the load balancing algorithm you want CloudStack to use. CloudStack supports the following well-known algorithms :
      — Round-robin
      — Le moins de connexions
      — Source
   — **Stickiness**. (Optional) Click Configure and choose the algorithm for the stickiness policy. See Sticky Session Policies for Load Balancer Rules.
   — **Add VMs** : Click Add VMs, then select two or more VMs that will divide the load of incoming traffic, and click Apply.

The new load balancing rule appears in the list. You can repeat these steps to add more load balancing rules for this IP address.

Load Balancing Across Tiers

CloudStack supports sharing workload across different tiers within your VPC. Assume that multiple tiers are set up in your environment, such as Web tier and Application tier. Traffic to each tier is balanced on the VPC virtual router on the public side, as explained in *"Adding Load Balancing Rules on a VPC"*. If you want the traffic coming from the Web tier to the Application tier to be balanced, use the internal load balancing feature offered by CloudStack.

How Does Internal LB Work in VPC ? In this figure, a public LB rule is created for the public IP 72.52.125.10 with public port 80 and private port 81. The LB rule, created on the VPC virtual router, is applied on the traffic coming from the Internet to the VMs on the Web tier. On the Application tier two internal load balancing rules are created. An internal LB rule for the guest IP 10.10.10.4 with load balancer port 23 and instance port 25 is configured on the VM, InternalLBVM1. Another internal LB rule for the guest IP 10.10.10.4 with load balancer port 45 and instance port 46 is configured on the VM, InternalLBVM1. Another internal LB rule for the guest IP 10.10.10.6, with load balancer port 23 and instance port 25 is configured on the VM, InternalLBVM2.



Lignes directrices

- Internal LB and Public LB are mutually exclusive on a tier. If the tier has LB on the public side, then it can't have the Internal LB.
- Internal LB is supported just on VPC networks in CloudStack 4.2 release.
- Only Internal LB VM can act as the Internal LB provider in CloudStack 4.2 release.
- Network upgrade is not supported from the network offering with Internal LB to the network offering with Public LB.
- Multiple tiers can have internal LB support in a VPC.
- Only one tier can have Public LB support in a VPC.

Enabling Internal LB on a VPC Tier

1. Create a network offering, as given in *Creating a Network Offering for Internal LB*.
2. Create an internal load balancing rule and apply, as given in *Creating an Internal LB Rule*.

Creating a Network Offering for Internal LB To have internal LB support on VPC, either use the default offering, DefaultIsolatedNetworkOfferingForVpcNetworksWithInternalLB, or create a network offering as follows :

1. Log in to the CloudStack UI as a user or admin.
2. From the Select Offering drop-down, choose Network Offering.
3. Cliquer sur Ajouter une offre de réseau.
4. In the dialog, make the following choices :
   — **Name** : Any desired name for the network offering.
   — **Description** : A short description of the offering that can be displayed to users.
   — **Network Rate** : Allowed data transfer rate in MB per second.
   — **Traffic Type** : The type of network traffic that will be carried on the network.
   — **Guest Type** : Choose whether the guest network is isolated or shared.
   — **Persistent** : Indicate whether the guest network is persistent or not. The network that you can provision without having to deploy a VM on it is termed persistent network.
   — **VPC** : This option indicate whether the guest network is Virtual Private Cloud-enabled. A Virtual Private Cloud (VPC) is a private, isolated part of CloudStack. A VPC can have its own virtual network topology that resembles a traditional physical network. For more information on VPCs, see *"About Virtual Private Clouds"*.
   — **Specify VLAN** : (Isolated guest networks only) Indicate whether a VLAN should be specified when this offering is used.
   — **Supported Services** : Select Load Balancer. Select `InternalLbVM` from the provider list.
   — **Load Balancer Type** : Select Internal LB from the drop-down.
   — **System Offering** : Choose the system service offering that you want virtual routers to use in this network.
   — **Conserve mode** : Indicate whether to use conserve mode. In this mode, network resources are allocated only when the first virtual machine starts in the network.
5. Click OK and the network offering is created.

Creating an Internal LB Rule When you create the Internal LB rule and applies to a VM, an Internal LB VM, which is responsible for load balancing, is created.

You can view the created Internal LB VM in the Instances page if you navigate to **Infrastructure > Zones >** <zone_name> **>** <physical_network_name> **> Network Service Providers > Internal LB VM**. You can manage the Internal LB VMs as and when required from the location.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Locate the VPC for which you want to configure internal LB, then click Configure.
   The VPC page is displayed where all the tiers you created listed in a diagram.
5. Locate the Tier for which you want to configure an internal LB rule, click Internal LB.
   In the Internal LB page, click Add Internal LB.
6. Dans la boîte de dialogue, spécifiez ce qui suit :
   — **Name** : A name for the load balancer rule.
   — **Description** : A short description of the rule that can be displayed to users.
   — **Source IP Address** : (Optional) The source IP from which traffic originates. The IP is acquired from the CIDR of that particular tier on which you want to create the Internal LB rule. If not specified, the IP address is automatically allocated from the network CIDR.
   For every Source IP, a new Internal LB VM is created for load balancing.
   — **Source Port** : The port associated with the source IP. Traffic on this port is load balanced.
   — **Instance Port** : The port of the internal LB VM.
   — **Algorithm**. Choose the load balancing algorithm you want CloudStack to use. CloudStack supports the following well-known algorithms :
      — Round-robin
      — Le moins de connexions
      — Source

Adding a Port Forwarding Rule on a VPC

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Click the Configure button of the VPC to which you want to deploy the VMs.
   The VPC page is displayed where all the tiers you created are listed in a diagram.
   For each tier, the following options are displayed :
   — Internal LB
   — Public LB IP
   — Static NAT
   — Machines Virtuelles
   — CIDR
   The following router information is displayed :
   — Passerelles privées
   — Adresses IP publiques
   — Site-to-Site VPNs
   — Listes d'ACL réseau
5. In the Router node, select Public IP Addresses.
   The IP Addresses page is displayed.
6. Click the IP address for which you want to create the rule, then click the Configuration tab.
7. In the Port Forwarding node of the diagram, click View All.
8. Select the tier to which you want to apply the rule.
9. Spécifier les informations suivantes :
   — **Public Port** : The port to which public traffic will be addressed on the IP address you acquired in the previous step.
   — **Private Port** : The port on which the instance is listening for forwarded public traffic.
   — **Protocol** : The communication protocol in use between the two ports.
      — TCP
      — UDP
   — **Add VM** : Click Add VM. Select the name of the instance to which this rule applies, and click Apply.
      You can test the rule by opening an SSH session to the instance.

Retirer des segments

You can remove a tier from a VPC. A removed tier cannot be revoked. When a tier is removed, only the resources of the tier are expunged. All the network rules (port forwarding, load balancing and staticNAT) and the IP addresses associated to the tier are removed. The IP address still be belonging to the same VPC.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   Tous les VPC que vous avez créé sur ce compte sont listés dans cette page.
4. Cliquez sur le bouton Configurer du VPC pour lequel vous désirez configurer un segment.
   The Configure VPC page is displayed. Locate the tier you want to work with.
5. Choisir le segment que vous voulez supprimer.
6. In the Network Details tab, click the Delete Network button. 
   Click Yes to confirm. Wait for some time for the tier to be removed.

Editing, Restarting, and Removing a Virtual Private Cloud

Note : Ensure that all the tiers are removed before you remove a VPC.

1. Se connecter à l'interface de CloudStack comme administrateur ou utilisateur final.
2. Dans la navigation à gauche, choisissez Réseau.
3. Dans la vue de Sélection, choisissez VPC.
   All the VPCs that you have created for the account is listed in the page.
4. Select the VPC you want to work with.
5. In the Details tab, click the Remove VPC button 
   You can remove the VPC by also using the remove button in the Quick View.

   You can edit the name and description of a VPC. To do that, select the VPC, then click the Edit button. 

   Pour redémarrer un VPC, sélectionner le VPC puis cliquer sur le bouton Redémarrer. 

12.1.28 Réseaux persistants

Un réseau que vous pouvez provisionner sans avoir à déployer une quelconque VM est appelé réseau persistant. Un réseau persistant peut faire partie d'un environnement VPC ou non-VPC.

Lorsque vous créez d'autres types de réseau, un réseau n'est qu'une entrée de base de données jusqu'à ce que la première VM soit créée sur ce réseau. Lors de la création de la première VM, un ID de VLAN est attribué et le réseau est provisionné. En outre, lorsque la dernière VM est détruite, l'ID du VLAN est libéré et le réseau n'est plus disponible. Avec l'ajout d'un réseau persistant, vous aurez la possibilité de créer un réseau dans CloudStack dans lequel les périphériques physiques peuvent être déployés sans avoir à exécuter une quelconque machine virtuelle. En outre, vous pouvez déployer des périphériques physiques sur ce réseau.

L'un des avantages d'avoir un réseau persistant est de pouvoir créer un VPC avec un segment composé uniquement de périphériques physiques. Par exemple, vous pouvez créer un VPC pour une application à trois tiers, déployer des VM pour le couche Web et Application et utiliser des machines physiques pour la couche Base de données. Un autre cas d'utilisation est que si vous fournissez des services en utilisant du matériel physique, vous pouvez définir le réseau comme persistant et donc même si toutes ses machines virtuelles sont détruites, ses services ne seront pas interrompus.

Considérations sur le Réseau Persistant

— Le réseau persistant est conçu pour les réseaux isolés.
— Toutes les offres de réseau par défaut sont non-persistantes.
— Une offre de réseau ne peut pas être éditable parce la changer affectent le fonctionnement des réseaux existants qui ont été créés en utilisant cette offre de service.
— Lorsque vous créez un réseau invité, l'offre de réseau que vous sélectionnez définie la persistance du réseau. Cela dépend en fait si la persistance du réseau est activée dans l'offre de réseau sélectionnée.
— Un réseau existant peut devenir persistant en changeant son offre de réseau pour une offre qui a l'option de persistance activée. Lorsque cette propriété est configurée, même si le réseau n'a pas de VM en fonctionnement, le réseau est provisionné.
— Un réseau existant peut devenir non-persistent en changeant son offre de réseau pour une offre qui a l'option de persistance désactivée. SI le réseau n'a pas de VM en fonctionnement durant le prochain lancement du garbage collector, il sera stoppé.
— Lorsque la dernière VM d'un réseau est détruite, le garbage collector du réseau vérifie si l'offre de réseau associée avec le réseau est persistante et arrête ce réseau seulement si c'est non-persistant.

Créer un réseau invité Persistant.

Pour créer un réseau persistant, suivre les instructions suivantes :

1. Créer une offre réseau avec l'option Persistant activée.
   Voir "Créer une Nouvelle Offre Réseau".
2. Sélectionnez le réseau depuis le panneau de navigation à gauche.
3. Sélectionnez le réseau invité avec lequel vous voulez offrir ce service réseau.
4. Cliquer sur le bouton Editer.
5. Dans la liste de sélection Offre Réseau, sélectionnez l'offre de réseau persistant que vous venez à l'instant de créer.
6. Cliquez sur OK.

12.1.29 Setup a Palo Alto Networks Firewall

Functionality Provided

This implementation enables the orchestration of a Palo Alto Networks Firewall from within CloudStack UI and API.

The following features are supported :

— List/Add/Delete Palo Alto Networks service provider
— List/Add/Delete Palo Alto Networks network service offering
— List/Add/Delete Palo Alto Networks network using the above service offering
— Add an instance to a Palo Alto Networks network
— Source NAT management on network create and delete
— List/Add/Delete Ingress Firewall rule
— List/Add/Delete Egress Firewall rule (both 'Allow' and 'Deny' default rules supported)
— List/Add/Delete Port Forwarding rule
— List/Add/Delete Static NAT rule
— Apply a Threat Profile to all firewall rules (more details in the Additional Features section)
— Apply a Log Forwarding profile to all firewall rules (more details in the Additional Features section)

Initial Palo Alto Networks Firewall Configuration

Anatomy of the Palo Alto Networks Firewall

— In **'Network > Interfaces'** there is a list of physical interfaces as well as aggregated physical interfaces which are used for managing traffic in and out of the Palo Alto Networks Firewall device.
— In **'Network > Zones'** there is a list of the different configuration zones. This implementation will use two zones ; a public (defaults to 'untrust') and private (defaults to 'trust') zone.
— In **'Network > Virtual Routers'** there is a list of VRs which handle traffic routing for the Palo Alto Firewall. We only use a single Virtual Router on the firewall and it is used to handle all the routing to the next network hop.
— In **'Objects > Security Profile Groups'** there is a list of profiles which can be applied to firewall rules. These profiles are used to better understand the types of traffic that is flowing through your network. Configured when you add the firewall provider to CloudStack.
— In **'Objects > Log Forwarding'** there is a list of profiles which can be applied to firewall rules. These profiles are used to better track the logs generated by the firewall. Configured when you add the firewall provider to CloudStack.
— In **'Policies > Security'** there is a list of firewall rules that are currently configured. You will not need to modify this section because it will be completely automated by CloudStack, but you can review the firewall rules which have been created here.

— In **'Policies > NAT'** there is a list of the different NAT rules. You will not need to modify this section because it will be completely automated by CloudStack, but you can review the different NAT rules that have been created here. Source NAT, Static NAT and Destination NAT (Port Forwarding) rules will show up in this list.

Configure the Public / Private Zones on the firewall

No manual configuration is required to setup these zones because CloudStack will configure them automatically when you add the Palo Alto Networks firewall device to CloudStack as a service provider. This implementation depends on two zones, one for the public side and one for the private side of the firewall.

— The public zone (defaults to 'untrust') will contain all of the public interfaces and public IPs.
— The private zone (defaults to 'trust') will contain all of the private interfaces and guest network gateways.

The NAT and firewall rules will be configured between these zones.

Configure the Public / Private Interfaces on the firewall

This implementation supports standard physical interfaces as well as grouped physical interfaces called aggregated interfaces. Both standard interfaces and aggregated interfaces are treated the same, so they can be used interchangeably. For this document, we will assume that we are using 'ethernet1/1' as the public interface and 'ethernet1/2' as the private interface. If aggregated interfaces where used, you would use something like 'ae1' and 'ae2' as the interfaces.

This implementation requires that the 'Interface Type' be set to 'Layer3' for both the public and private interfaces. If you want to be able to use the 'Untagged' VLAN tag for public traffic in CloudStack, you will need to enable support for it in the public 'ethernet1/1' interface (details below).

Steps to configure the Public Interface :

1. Log into Palo Alto Networks Firewall
2. Navigate to 'Network > Interfaces'
3. Click on 'ethernet1/1' (for aggregated ethernet, it will probably be called 'ae1')
4. Select 'Layer3' from the 'Interface Type' list
5. Click 'Advanced'
6. Check the 'Untagged Subinterface' check-box
7. Cliquez sur 'OK'.

Steps to configure the Private Interface :

1. Click on 'ethernet1/2' (for aggregated ethernet, it will probably be called 'ae2')
2. Select 'Layer3' from the 'Interface Type' list
3. Cliquez sur 'OK'.

Configure a Virtual Router on the firewall

The Virtual Router on the Palo Alto Networks Firewall is not to be confused with the Virtual Routers that CloudStack provisions. For this implementation, the Virtual Router on the Palo Alto Networks Firewall will ONLY handle the upstream routing from the Firewall to the next hop.

Steps to configure the Virtual Router :

1. Log into Palo Alto Networks Firewall
2. Navigate to 'Network > Virtual Routers'
3. Select the 'default' Virtual Router or Add a new Virtual Router if there are none in the list
   — If you added a new Virtual Router, you will need to give it a 'Name'
4. Navigate to 'Static Routes > IPv4'

5. 'Add' a new static route
   — **Name** : next_hop (you can name it anything you want)
   — **Destination** : 0.0.0.0/0 (send all traffic to this route)
   — **Interface** : ethernet1/1 (or whatever you set your public interface as)
   — **Next Hop** : (specify the gateway IP for the next hop in your network)
   — Cliquez sur 'OK'.
6. Cliquez sur 'OK'.

Configure the default Public Subinterface

The current implementation of the Palo Alto Networks firewall integration uses CIDRs in the form of 'w.x.y.z/32' for the public IP addresses that CloudStack provisions. Because no broadcast or gateway IPs are in this single IP range, there is no way for the firewall to route the traffic for these IPs. To route the traffic for these IPs, we create a single subinterface on the public interface with an IP and a CIDR which encapsulates the CloudStack public IP range. This IP will need to be inside the subnet defined by the CloudStack public range netmask, but outside the CloudStack public IP range. The CIDR should reflect the same subnet defined by the CloudStack public range netmask. The name of the subinterface is determined by the VLAN configured for the public range in CloudStack.

To clarify this concept, we will use the following example.

Example CloudStack Public Range Configuration :
— **Gateway** : 172.30.0.1
— **Netmask** : 255.255.255.0
— **IP Range** : 172.30.0.100 - 172.30.0.199
— **VLAN** : Untagged

Configure the Public Subinterface :

1. Log into Palo Alto Networks Firewall
2. Navigate to 'Network > Interfaces'
3. Select the 'ethernet1/1' line (not clicking on the name)
4. Click 'Add Subinterface' at the bottom of the window
5. Enter 'Interface Name' : 'ethernet1/1' . '9999'
   — 9999 is used if the CloudStack public range VLAN is 'Untagged'
   — If the CloudStack public range VLAN is tagged (eg : 333), then the name will reflect that tag
6. The 'Tag' is the VLAN tag that the traffic is sent to the next hop with, so set it accordingly. If you are passing 'Untagged' traffic from CloudStack to your next hop, leave it blank. If you want to pass tagged traffic from CloudStack, specify the tag.
7. Select 'default' from the 'Config > Virtual Router' drop-down (assuming that is what your virtual router is called)
8. Click the 'IPv4' tab
9. Select 'Static' from the 'Type' radio options
10. Click 'Add' in the 'IP' section
11. Enter '172.30.0.254/24' in the new line
    — The IP can be any IP outside the CloudStack public IP range, but inside the CloudStack public range netmask (it can NOT be the gateway IP)
    — The subnet defined by the CIDR should match the CloudStack public range netmask
12. Cliquez sur 'OK'.

Commit configuration on the Palo Alto Networks Firewall

In order for all the changes we just made to take effect, we need to commit the changes.

1. Click the 'Commit' link in the top right corner of the window
2. Click 'OK' in the commit window overlay
3. Click 'Close' to the resulting commit status window after the commit finishes

Setup the Palo Alto Networks Firewall in CloudStack

Add the Palo Alto Networks Firewall as a Service Provider

1. Navigate to 'Infrastructure > Zones > ZONE_NAME > Physical Network > NETWORK_NAME (guest) > Configure ; Network Service Providers'
2. Click on 'Palo Alto' in the list
3. Cliquer sur 'Voir les périphériques'
4. Click 'Add Palo Alto Device'
5. Enter your configuration in the overlay. This example will reflect the details previously used in this guide.
   - **IP Address** : (the IP of the Palo Alto Networks Firewall)
   - **Username** : (the admin username for the firewall)
   - **Password** : (the admin password for the firewall)
   - **Type** : Palo Alto Firewall
   - **Public Interface** : ethernet1/1 (use what you setup earlier as the public interface if it is different from my examples)
   - **Private Interface** : ethernet1/2 (use what you setup earlier as the private interface if it is different from my examples)
   - **Number of Retries** : 2 (the default is fine)
   - **Timeout** : 300 (the default is fine)
   - **Public Network** : untrust (this is the public zone on the firewall and did not need to be configured)
   - **Private Network** : trust (this is the private zone on the firewall and did not need to be configured)
   - **Virtual Router** : default (this is the name of the Virtual Router we setup on the firewall)
   - **Palo Alto Threat Profile** : (not required. name of the 'Security Profile Groups' to apply. more details in the 'Additional Features' section)
   - **Palo Alto Log Profile** : (not required. name of the 'Log Forwarding' profile to apply. more details in the 'Additional Features' section)
   - **Capacity** : (not required)
   - **Dedicated** : (not required)
6. Cliquez sur 'OK'.
7. Click on 'Palo Alto' in the breadcrumbs to go back one screen.
8. Click on 'Enable Provider' 

Add a Network Service Offering to use the new Provider

There are 6 'Supported Services' that need to be configured in the network service offering for this functionality. They are DHCP, DNS, Firewall, Source NAT, Static NAT and Port Forwarding. For the other settings, there are probably additional configurations which will work, but I will just document a common case.

1. Navigate to 'Service Offerings'
2. In the drop-down at the top, select 'Network Offerings'

3. Click 'Add Network Offering'
   - **Name** : (name it whatever you want)
   - **Description** : (again, can be whatever you want)
   - **Guest Type** : Isolated
   - **Supported Services** :
     - **DHCP** : Provided by 'VirtualRouter'
     - **DNS** : Provided by 'VirtualRouter'
     - **Firewall** : Provided by 'PaloAlto'
     - **Source NAT** : Provided by 'PaloAlto'
     - **Static NAT** : Provided by 'PaloAlto'
     - **Port Forwarding** : Provided by 'PaloAlto'
   - **System Offering for Router** : System Offering For Software Router
   - **Supported Source NAT Type** : Per account (this is the only supported option)
   - **Default egress policy** : (both 'Allow' and 'Deny' are supported)
4. Cliquez sur 'OK'.
5. Click on the newly created service offering
6. Click 'Enable network offering' 

When adding networks in CloudStack, select this network offering to use the Palo Alto Networks firewall.

Fonctionnalités complémentaires

In addition to the standard functionality exposed by CloudStack, we have added a couple additional features to this implementation. We did not add any new screens to CloudStack, but we have added a couple fields to the 'Add Palo Alto Service Provider' screen which will add functionality globally for the device.

Palo Alto Networks Threat Profile

This feature allows you to specify a 'Security Profile Group' to be applied to all of the firewall rules which are created on the Palo Alto Networks firewall device.

To create a 'Security Profile Group' on the Palo Alto Networks firewall, do the following :

1. Log into the Palo Alto Networks firewall
2. Navigate to 'Objects > Security Profile Groups'
3. Click 'Add' at the bottom of the page to add a new group
4. Give the group a Name and specify the profiles you would like to include in the group
5. Cliquez sur 'OK'.
6. Click the 'Commit' link in the top right of the screen and follow the on screen instructions

Once you have created a profile, you can reference it by Name in the 'Palo Alto Threat Profile' field in the 'Add the Palo Alto Networks Firewall as a Service Provider' step.

Palo Alto Networks Log Forwarding Profile

This feature allows you to specify a 'Log Forwarding' profile to better manage where the firewall logs are sent to. This is helpful for keeping track of issues that can arise on the firewall.

To create a 'Log Forwarding' profile on the Palo Alto Networks Firewall, do the following :

1. Log into the Palo Alto Networks firewall
2. Navigate to 'Objects > Log Forwarding'

3. Click 'Add' at the bottom of the page to add a new profile
4. Give the profile a Name and specify the details you want for the traffic and threat settings
5. Cliquez sur 'OK'.
6. Click the 'Commit' link in the top right of the screen and follow the on screen instructions

Once you have created a profile, you can reference it by Name in the 'Palo Alto Log Profile' field in the 'Add the Palo Alto Networks Firewall as a Service Provider' step.

Limitations

— The implementation currently only supports a single public IP range in CloudStack
— Usage tracking is not yet implemented

12.2 Using Remote Access VPN

Clients

Per Operating System instructions

Remote Access VPN connection to VPC or Guest Network to access Instances and applications. This section consider you have enable Remonte acccess VPN, refer to : *Accès distant VPN*.

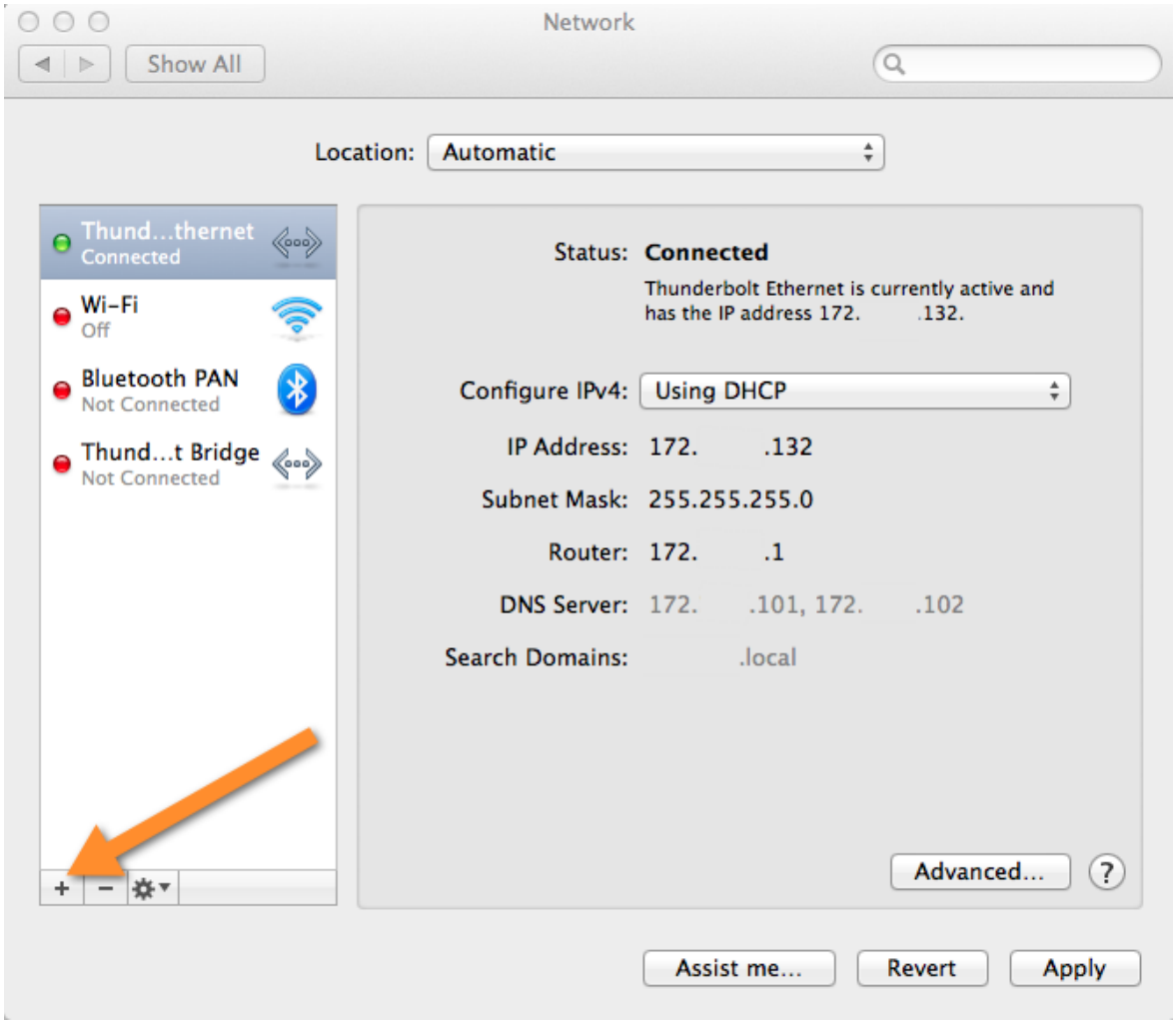
When connected to a VPC via VPN, the client have access to all Tiers.

Following information is required to confiture VPN client :
— `Public IP` : source NAT with VPN enabled.
— `IPsec pre-shared key` : Provide at the VPN activation.
— `Username` VPN account username.
— `Password` VPN account password.

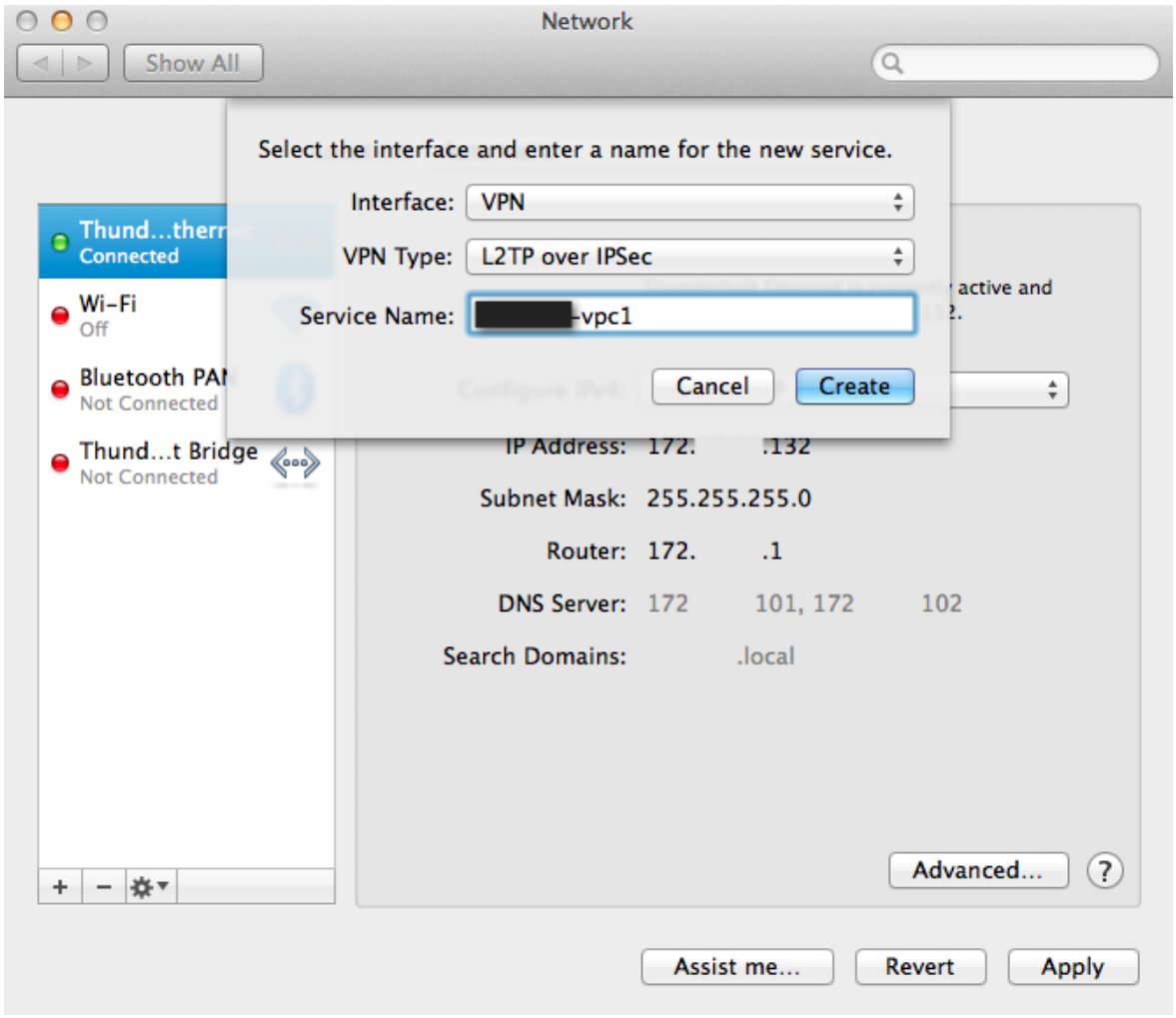
12.2.1 Mac OSX

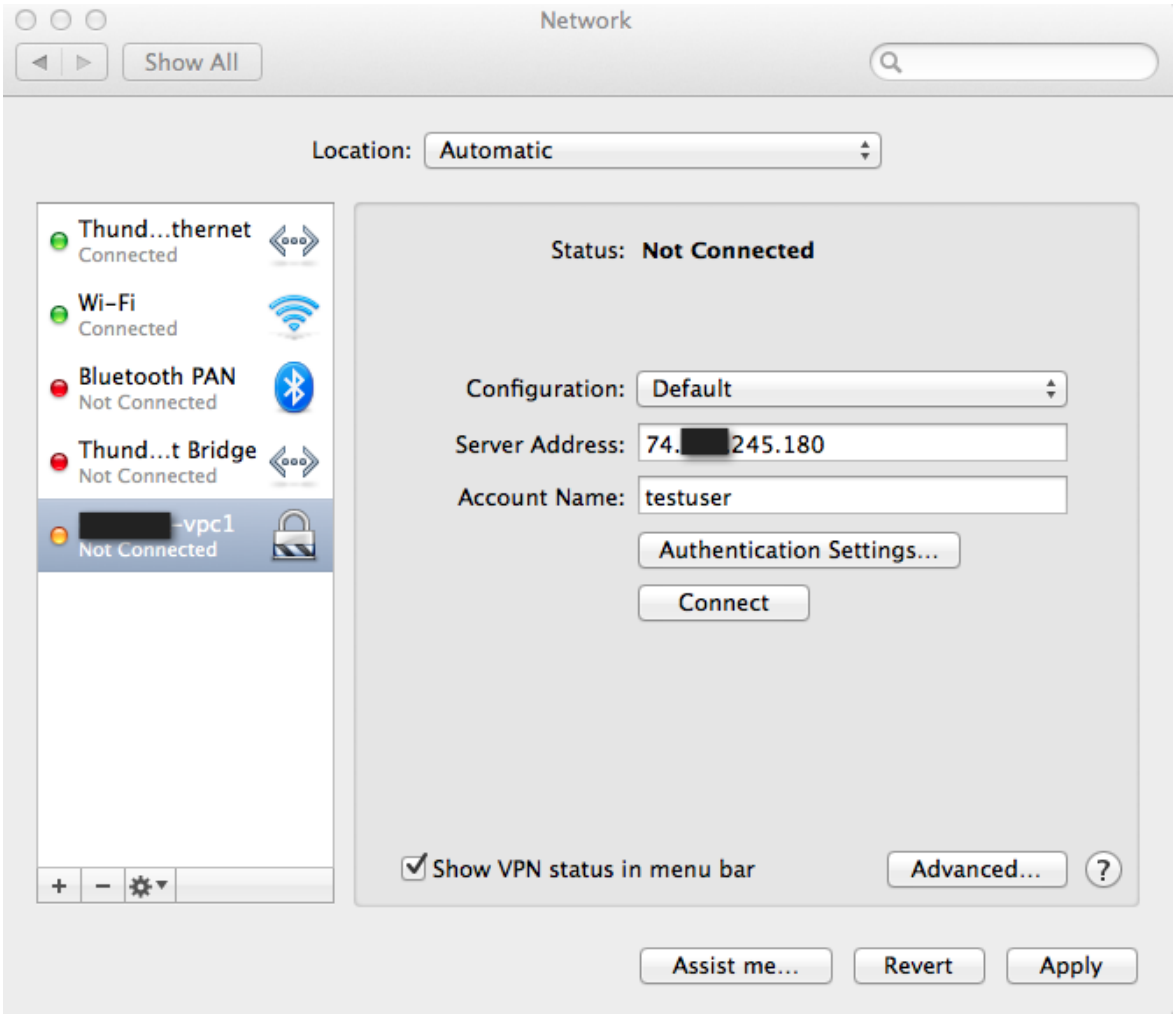
Mac OSX provide native IPsec VPN client.

1. Into System Preferences -> Network
2. Click "+" button and add a VPN :
   — Interface : VPN
   — VPN Type : L2TP over IPSec
   — Service Name : (ex : test-vpc1)

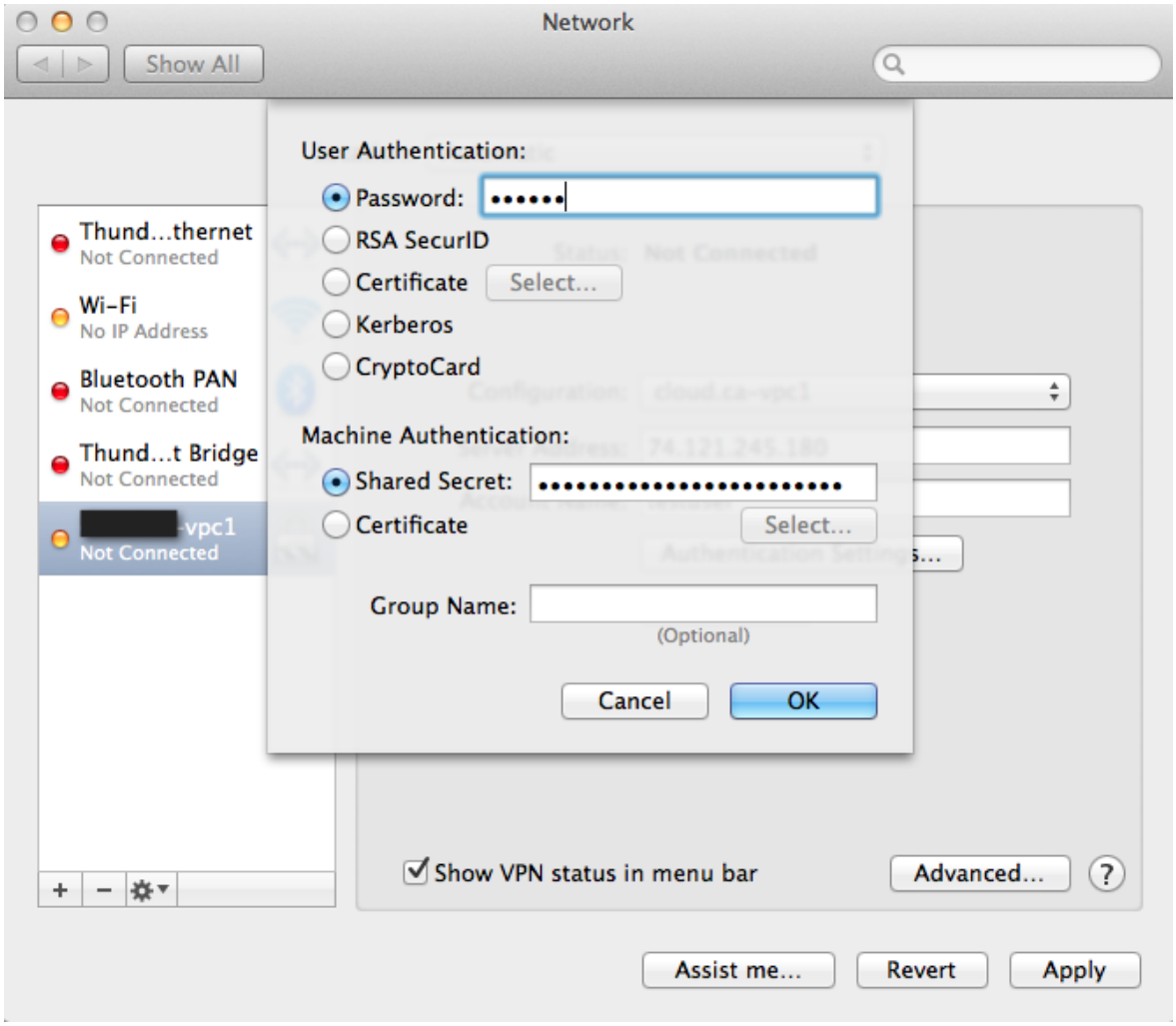


3. Configure L2TP over IPsec

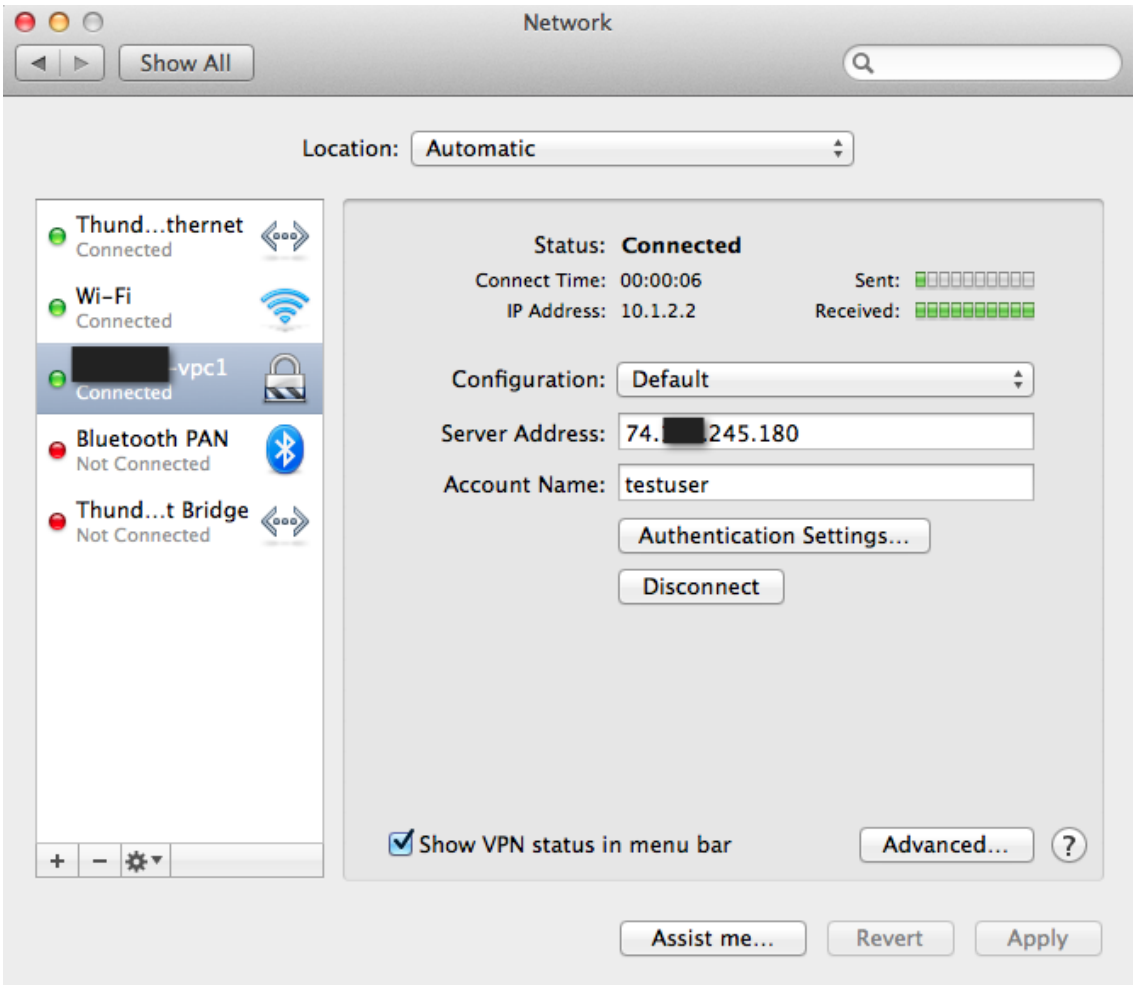

Network
Show All
Select the interface and enter a name for the new service.
Interface: VPN
VPN Type: L2TP over IPSec
Service Name: [redacted]-vpc1
Cancel
Create
Thund...therr
Connected
Wi-Fi
Off
Bluetooth PAN
Not Connected
Thund...t Bridge
Not Connected
IP Address: 172. .132
Subnet Mask: 255.255.255.0
Router: 172. .1
DNS Server: 172 101, 172 102
Search Domains: .local
Advanced...
Assist me...
Revert
Apply



4. Inside Authentication Settings...



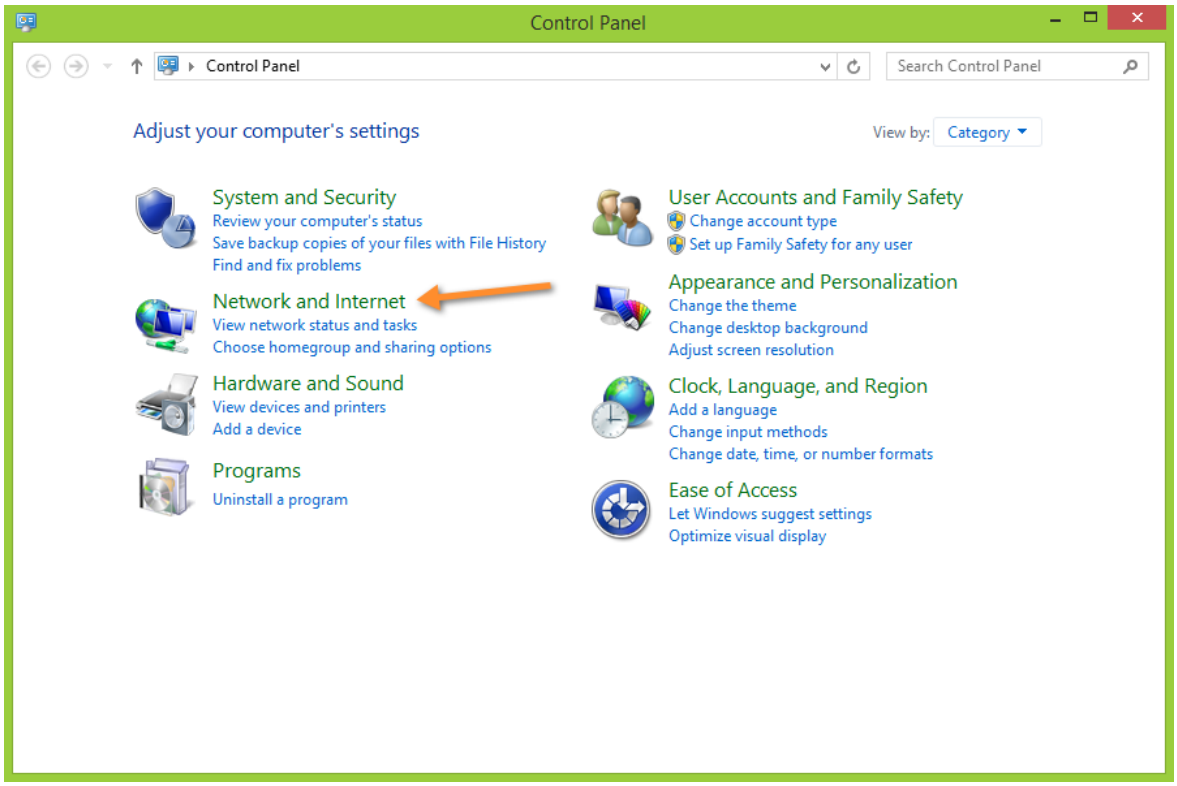
5. Connect into VPN
   (a) Click Apply to apply Network configuration changes.
   (b) Click Connect to initiate VPN connection.

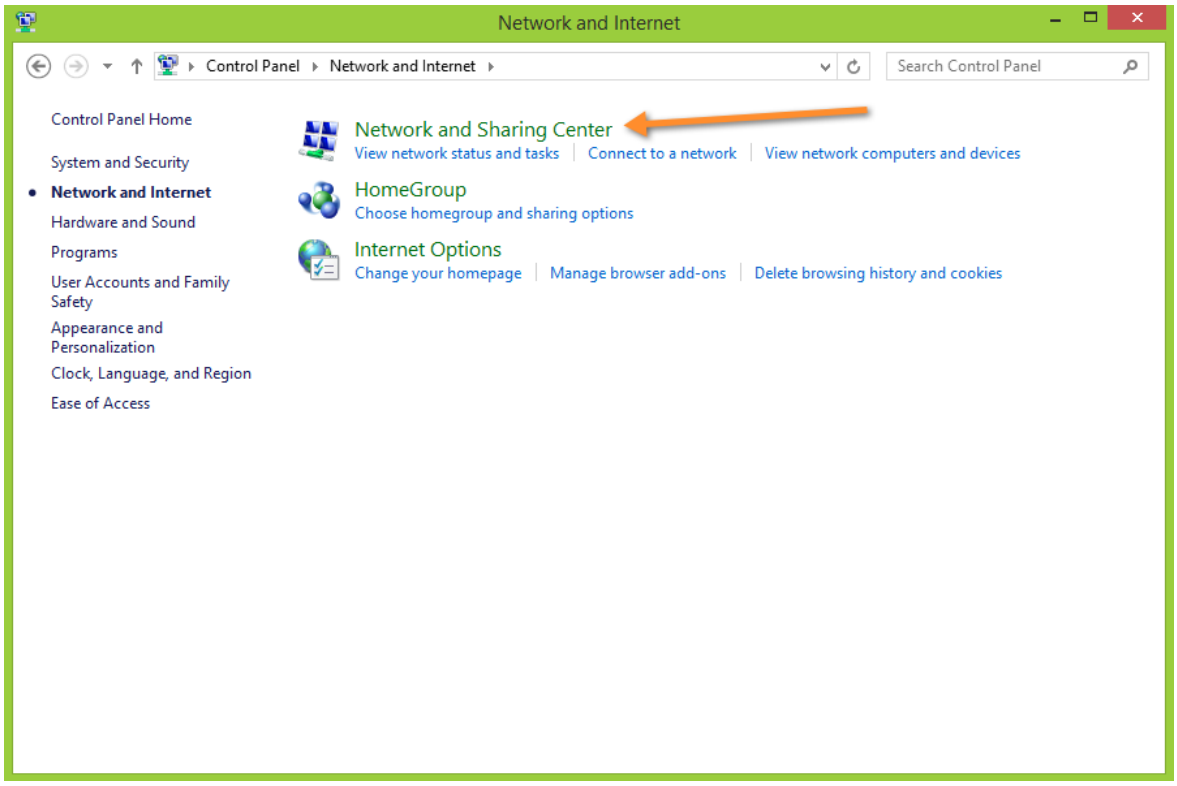


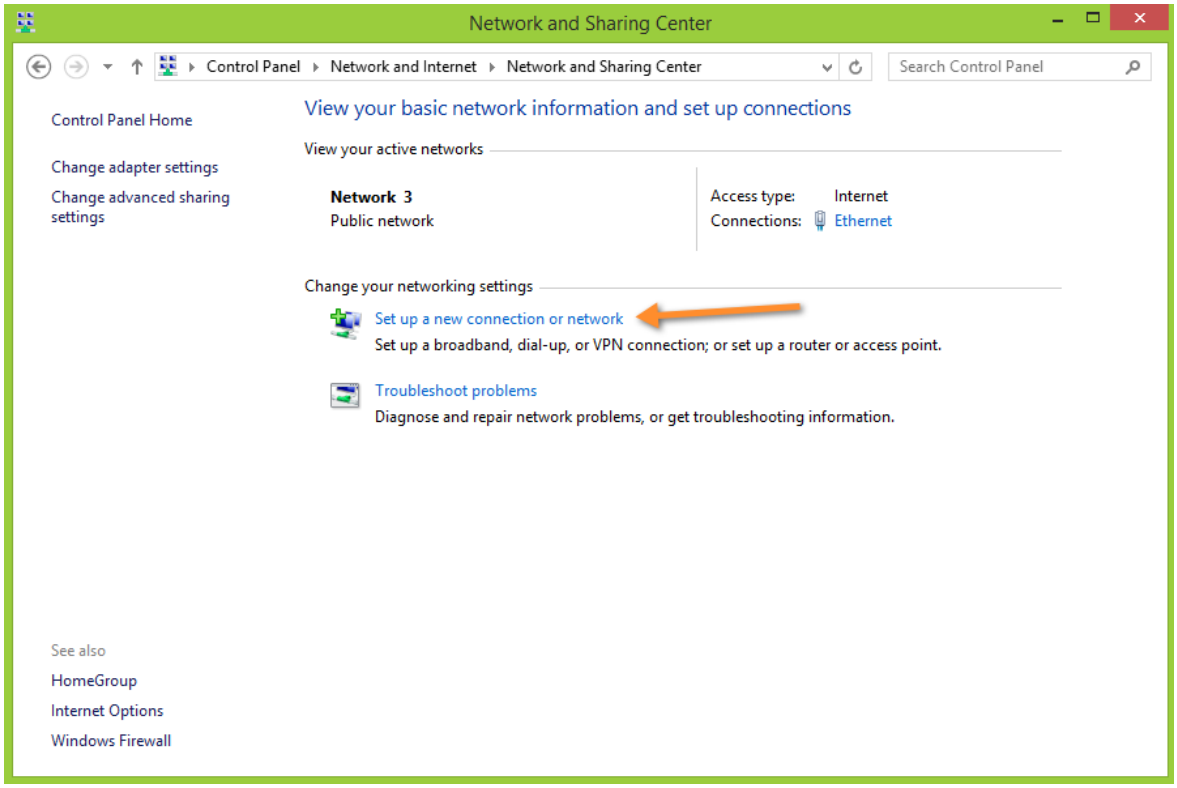
12.2.2 Microsoft Windows 8

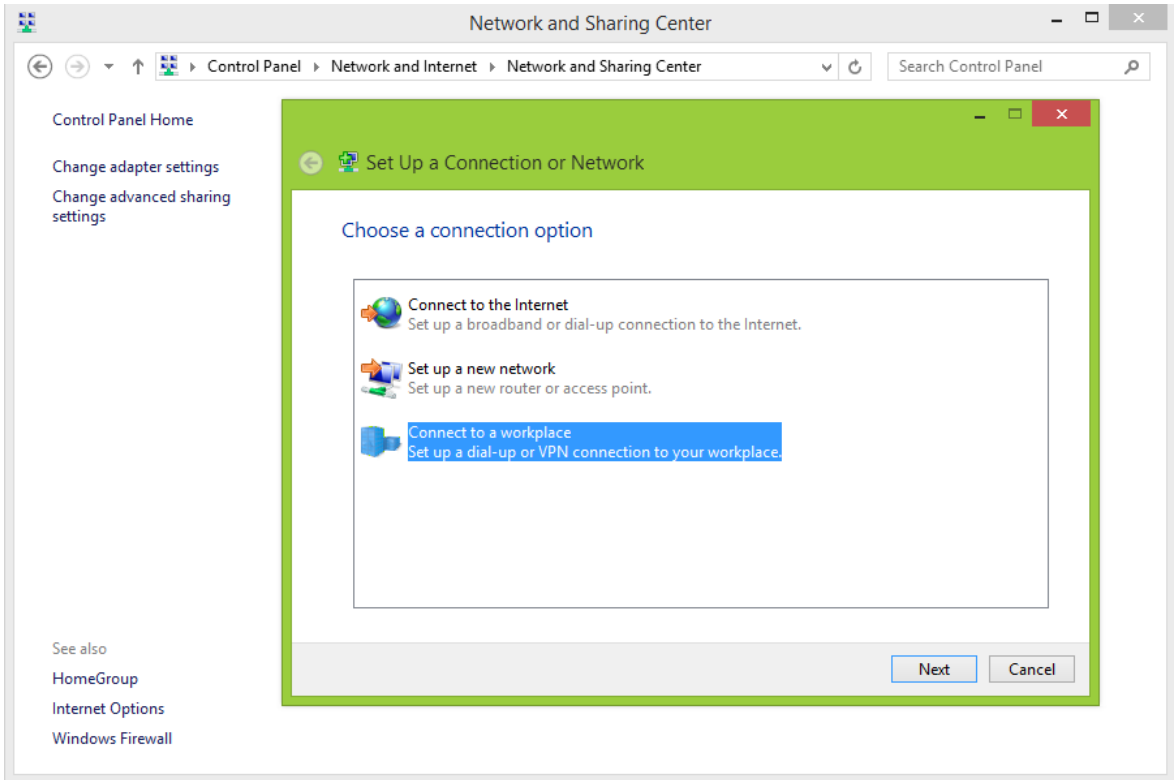
Following instruction have been perform using Windows 8.1 using Native VPN client.

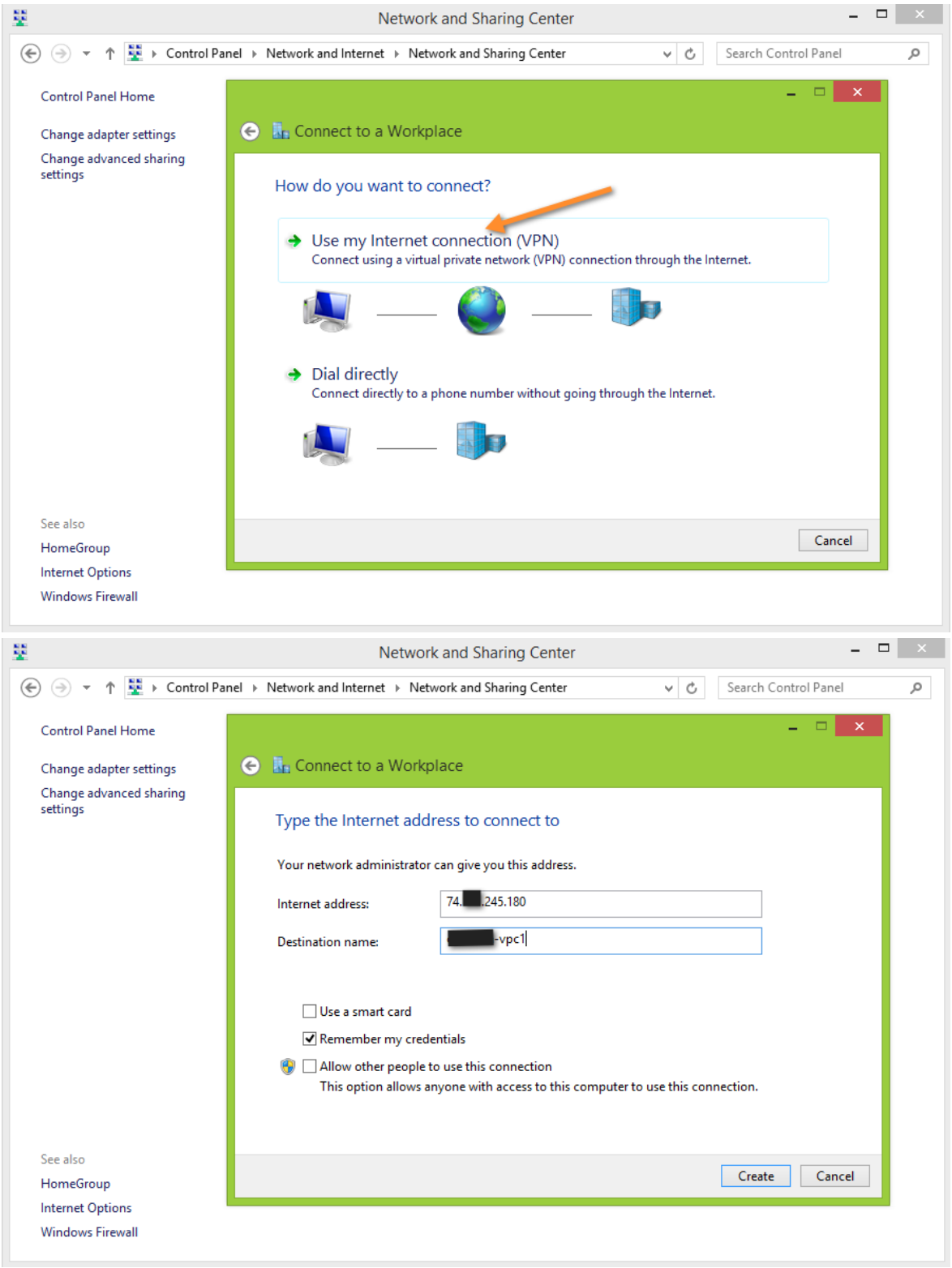
1. Create network VPN connection


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Change account type
Set up Family Safety for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

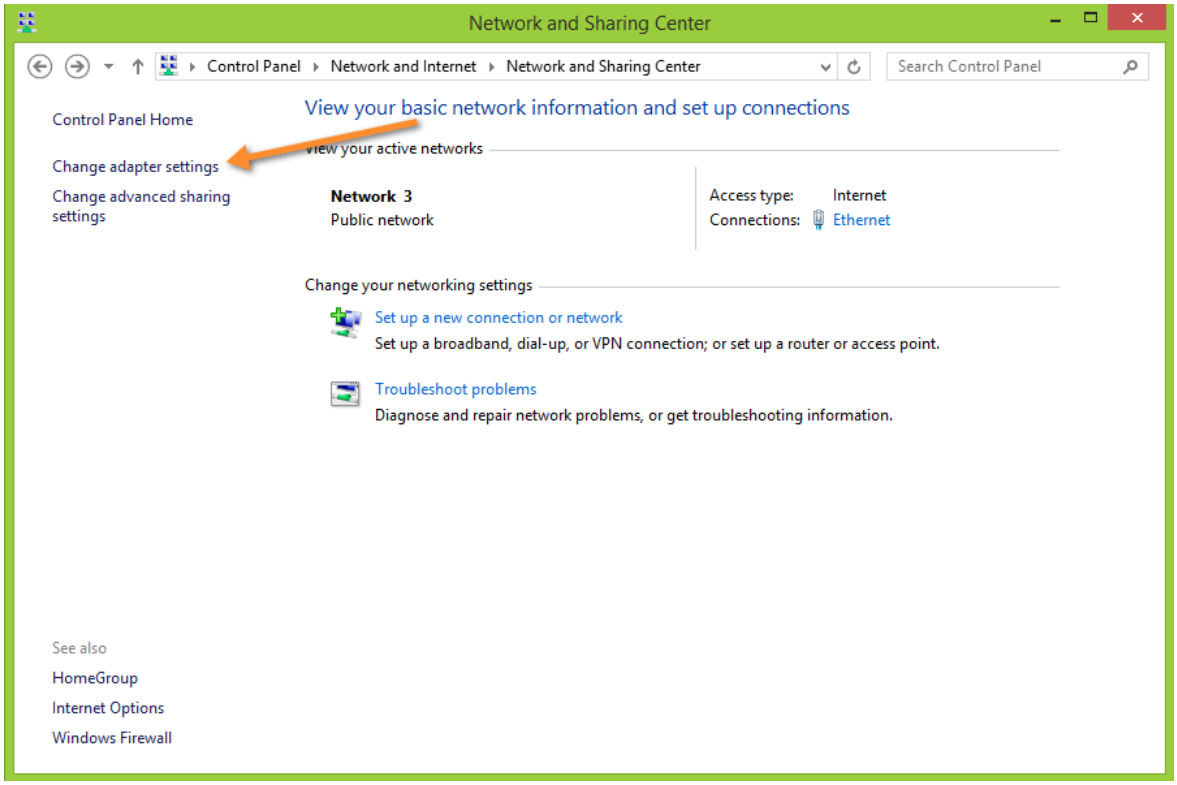

Network and Internet
Control Panel
Network and Internet
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

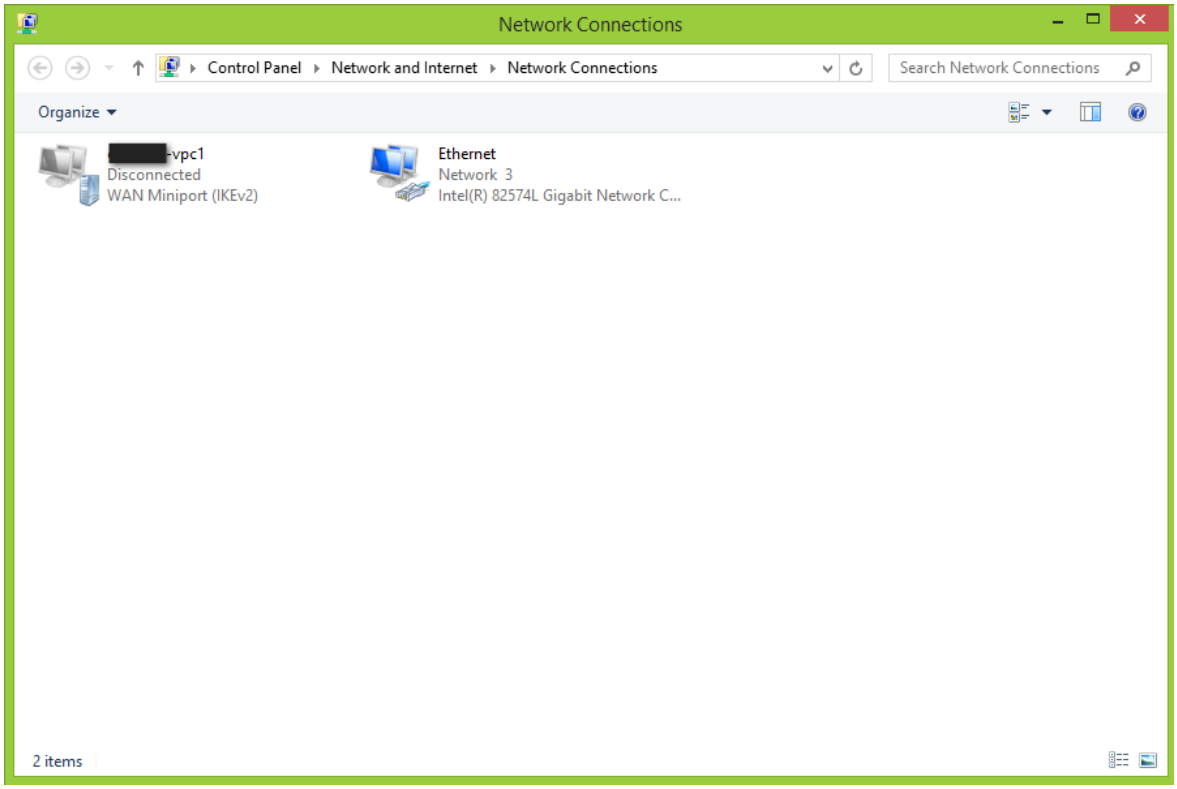

Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Network 3
Public network
Access type: Internet
Connections: Ethernet
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

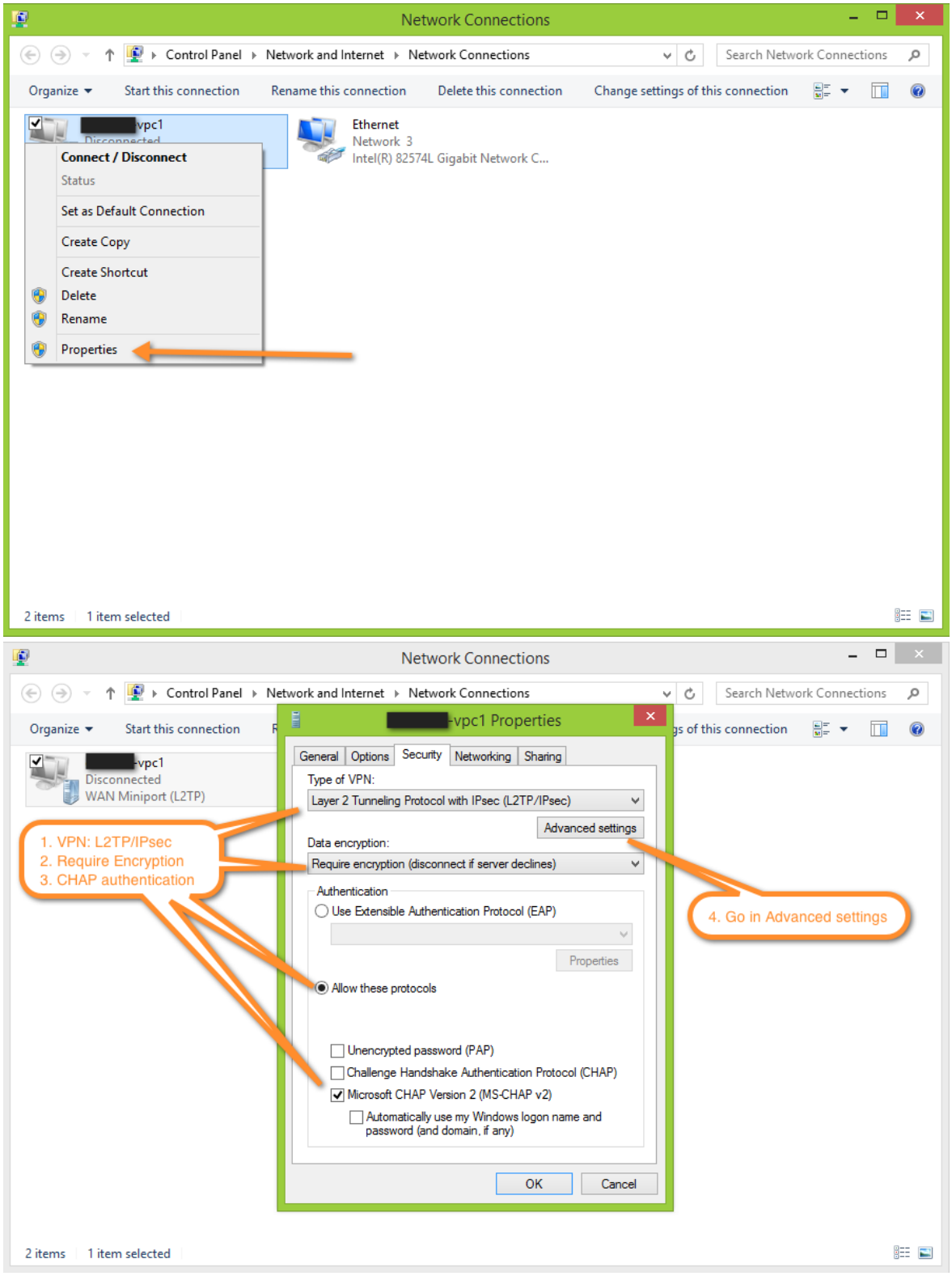

Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel
See also
HomeGroup
Internet Options
Windows Firewall

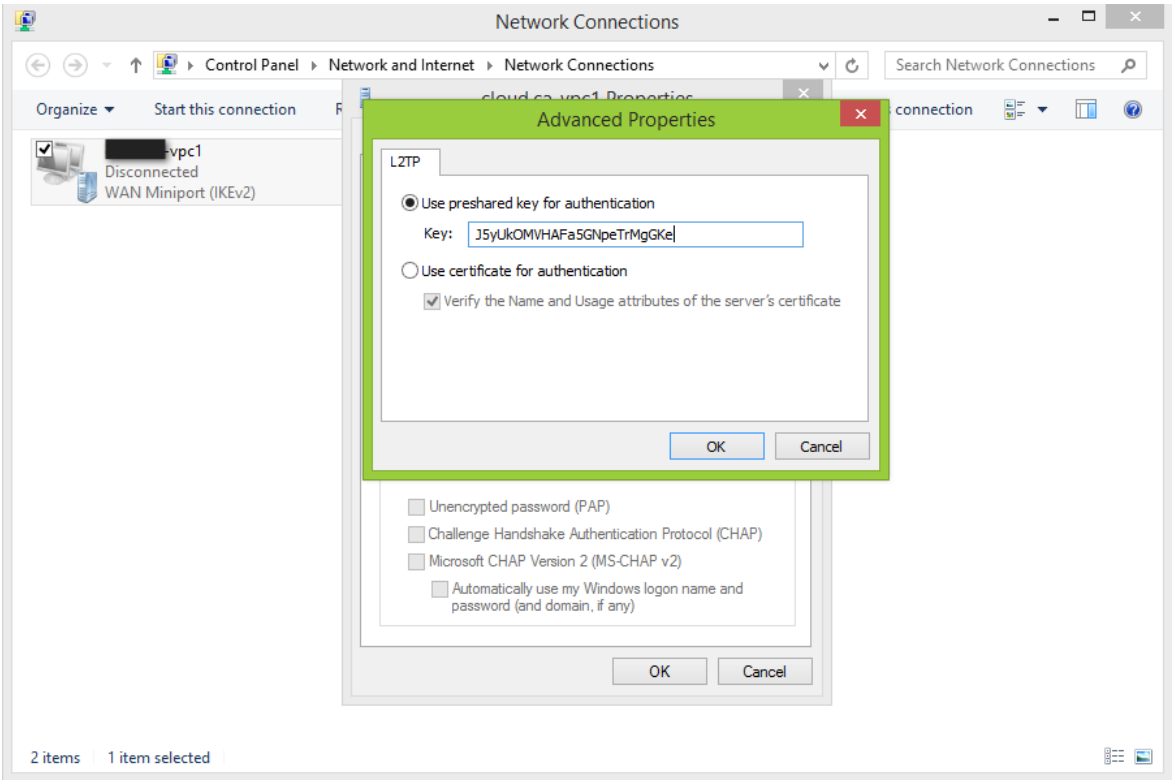


2. Configure VPN settings

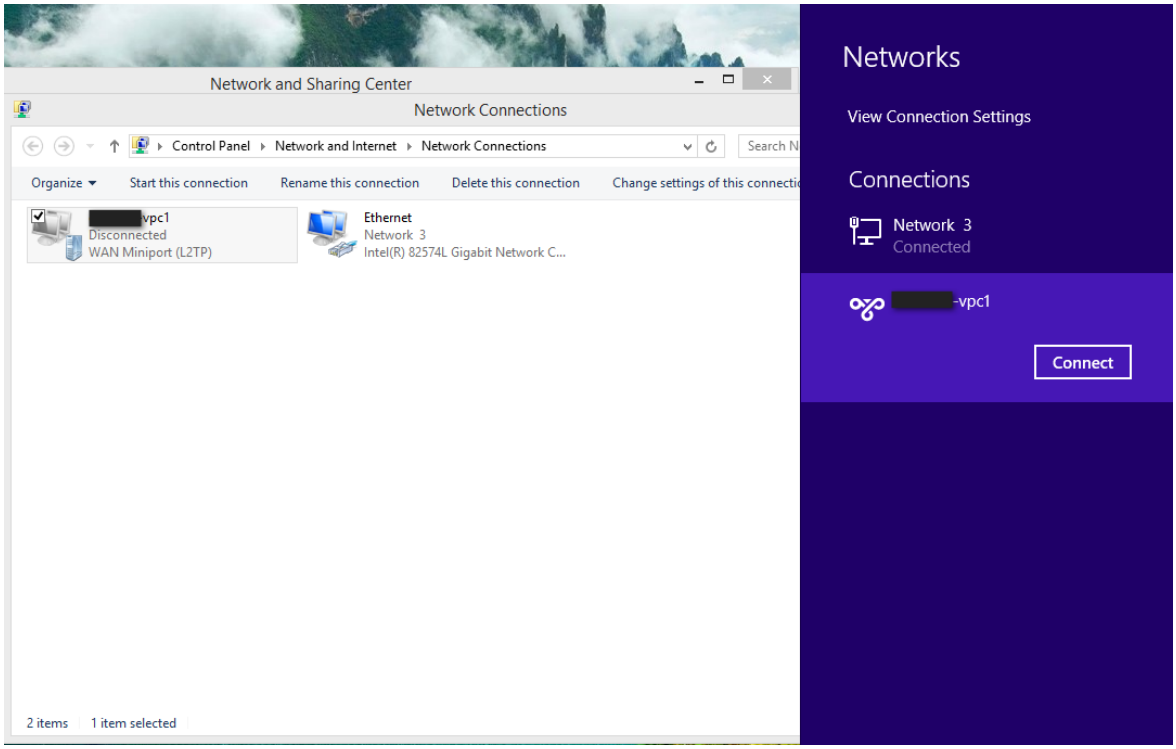

Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
Change adapter settings
Change advanced sharing settings
View your active networks
Network 3
Public network
Access type: Internet
Connections: Ethernet
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

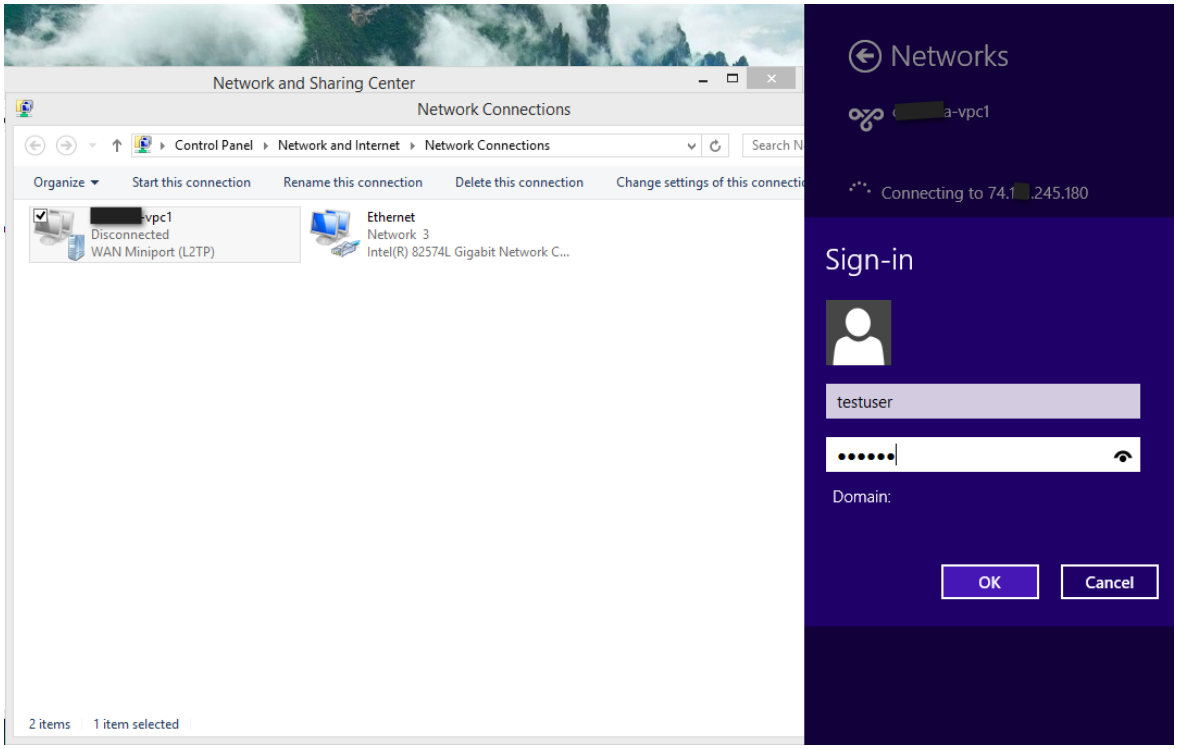

Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize
[redacted]-vpc1
Disconnected
WAN Miniport (IKEv2)
Ethernet
Network 3
Intel(R) 82574L Gigabit Network C...
2 items

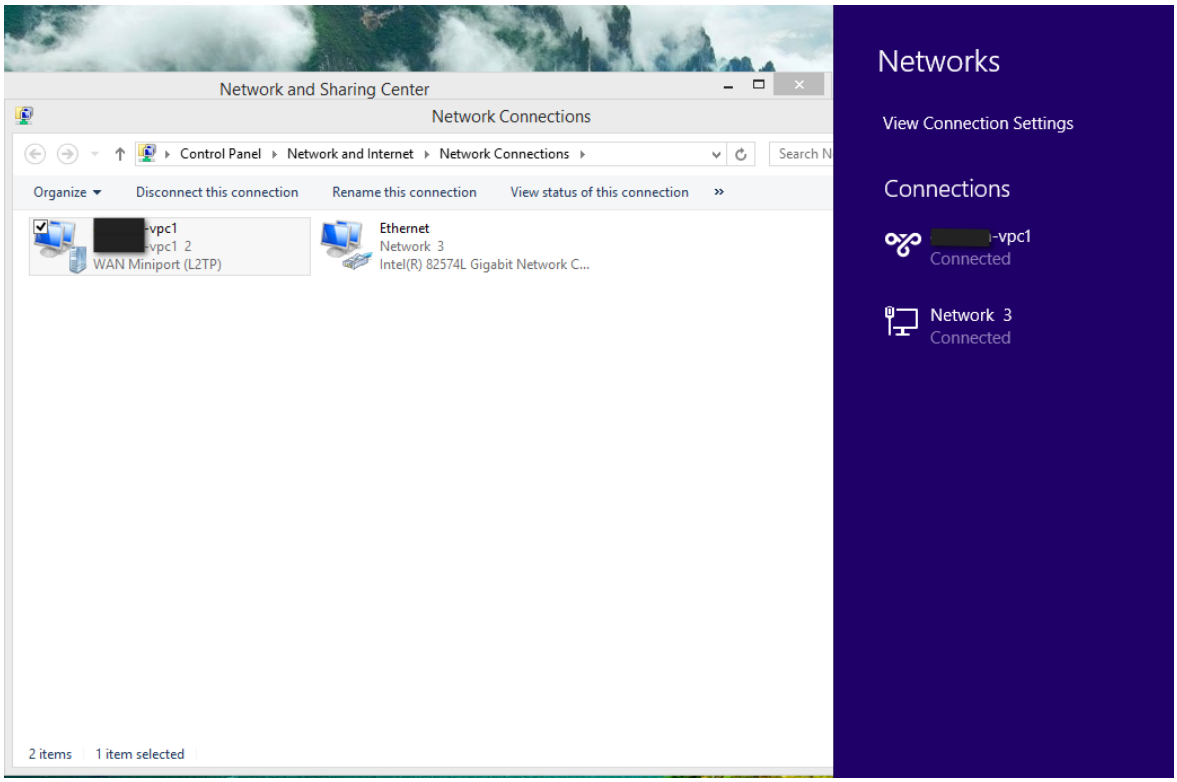

Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
[redacted]vpc1
Disconnected
Ethernet
Network 3
Intel(R) 82574L Gigabit Network C...
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties
2 items
1 item selected
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize
Start this connection
[redacted]vpc1
Disconnected
WAN Miniport (L2TP)
[redacted]vpc1 Properties
General
Options
Security
Networking
Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
Advanced settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK
Cancel
1. VPN: L2TP/IPsec
2. Require Encryption
3. CHAP authentication
4. Go in Advanced settings
2 items
1 item selected



3. Initiate VPN connection




Network and Sharing Center
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
[redacted]-vpc1
Disconnected
WAN Miniport (L2TP)
Ethernet
Network 3
Intel(R) 82574L Gigabit Network C...
2 items
1 item selected
Networks
[redacted]a-vpc1
Connecting to 74.1[redacted].245.180
Sign-in
testuser
Domain:
OK
Cancel


Network and Sharing Center
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Organize
Disconnect this connection
Rename this connection
View status of this connection
[redacted]-vpc1
[redacted]-vpc1 2
WAN Miniport (L2TP)
Ethernet
Network 3
Intel(R) 82574L Gigabit Network C...
2 items
1 item selected
Networks
View Connection Settings
Connections
[redacted]-vpc1
Connected
Network 3
Connected

CHAPITRE 13

Gérer le cloud

13.1 Gérer le cloud

13.1.1 Utiliser les étiquettes pour organiser les ressources dans le Cloud

Une étiquette est une paire clé-valeur qui stocke des métadonnées sur une ressource dans le cloud. Les étiquettes sont utiles pour catégoriser les ressources. Par exemple, vous pouvez étiqueter une VM utilisateur avec une valeur qui indique la ville de résidence de l'utilisateur. Dans ce cas, la clé serait «ville» et la valeur pourrait être «Toronto» ou «Tokyo». Vous pouvez alors demander à CloudStack de trouver toutes les ressources qui ont une étiquette donnée ; Par exemple, les VM pour les utilisateurs d'une ville donnée.

Vous pouvez étiqueter une machine virtuelle utilisateur, un volume, un instantané, un réseau invité, un modèle, une ISO, une règle de pare-feu, une règle de transfert de port, une adresse IP publique, un groupe de sécurité, une règle de répartition de charge, un projet, un VPC, une ACL réseau ou une route statique. Vous ne pouvez pas marquer un VPN à accès distant.

Vous pouvez travailler avec des étiquettes via l'interface utilisateur ou via les commandes API createTags, deleteTags et listTags. Vous pouvez définir plusieurs étiquettes pour chaque ressource. Il n'y a pas de limite sur le nombre d'étiquettes que vous pouvez définir. Chaque étiquette peut comporter jusqu'à 255 caractères. Les utilisateurs peuvent définir des étiquettes sur les ressources dont ils sont les propriétaires et les administrateurs peuvent définir des étiquettes sur toutes les ressources du cloud.

Un paramètre d'entrée optionnel, "tags", existe sur plusieurs commandes list* API. L'exemple suivant montre comment utiliser ce nouveau paramètre pour trouver tous les volumes ayant l'étiquette region=canada OR etiquette city=Toronto :

```
command=listVolumes
   &listAll=true
   &tags[0].key=region
   &tags[0].value=canada
   &tags[1].key=city
   &tags[1].value=Toronto
```

Les commandes d'API suivantes ont le paramètre d'entrée "tags" :

- listVirtualMachines
- listVolumes
- listSnapshots
- listNetworks
- listTemplates
- listIsos
- listFirewallRules

— listPortForwardingRules
— listPublicIpAddresses
— listSecurityGroups
— listLoadBalancerRules
— listProjects
— listVPCs
— listNetworkACLs
— listStaticRoutes

13.1.2 Rapport sur les sockets CPU

PRODUCT gère différents types d'hôtes qui contiennent une ou plusieurs sockets de CPU physiques. La socket du CPU est considéré comme une unité de mesure utilisée les licences et la facturation de l'infrastructure cloud. PRODUCT fournit à la fois l'interface utilisateur et le support API pour collecter les statistiques du socket du CPU à des fins de facturation. L'onglet Infrastructure comporte un nouvel onglet pour les sockets CPU. Vous pouvez afficher les statistiques des sockets CPU gérés par PRODUCT, qui reflètent en retour la taille du cloud. La page Socket CPU vous donnera le nombre d'hôtes et de sockets utilisés pour chaque type d'hôte.

1. Se connecter à l'interface utilisateur PRODUCT.
2. Dans la barre de navigation de gauche, cliquer sur Infrastructure.
3. Sur Sockets CPU, cliquer sur Voir tout
   La page Socket CPU est affichée. La page montre le nombre d'hôtes et de sockets CPU basé sur le type d'hyperviseur.

13.1.3 Changer la configuration de la base de données

Le serveur de gestion CloudStack stocke les informations de configuration de sa base de données (par exemple nom de machine, port, mot de passes) dans le fichier `/etc/cloudstack/management/db.properties`. Pour prendre en compte les changements, editer ce fichier sur chaque serveur de Gestion, puis redémarrer le serveur de gestion.

13.1.4 Changer le mot de passe de la base de données

Vous devrez peut-être modifier le mot de passe du compte MySQL utilisé par CloudStack. Dans ce cas, vous devrez changer le mot de passe dans MySQL, puis ajouter le mot de passe crypté dans `/etc/cloudstack/management/db.properties`.

1. Avant de changer le mot de passe, vous devrez stopper le serveur de gestion de CloudStack et le moteur d'usage si vous avez déployé ce composant.

```
# service cloudstack-management stop
# service cloudstack-usage stop
```

2. Ensuite, vous allez mettre à jour le mot de passe pour l'utilisateur CloudStack sur le serveur MySQL.

```
# mysql -u root -p
```

   Au prompt de MySQL, vous allez changer le mot de passe et appliquer les privilèges :

```
update mysql.user set password=PASSWORD("newpassword123") where User='cloud';
flush privileges;
quit;
```

3. L'étape suivante consiste à crypter le mot de passe et à copier le mot de passe crypté dans la configuration de la base de données de CloudStack (`/etc/cloudstack/management/db.properties`).

```
# java -classpath /usr/share/cloudstack-common/lib/jasypt-1.9.0.jar \ org.jasypt.intf.cli.Jasyp
```

13.1.5 Type de cryptage de fichiers

Notez que cela concerne le type de cryptage de fichier. Si vous utilisez le type de cryptage web alors vous allez utiliser password="management_server_secret_key"

1. Maintenant, vous allez mettre à jour `/etc/cloudstack/management/db.properties` avec le nouveau ciphertext. Ouvrez `/etc/cloudstack/management/db.properties` dans un éditeur de texte et mettez à jour ces paramètres :

```
db.cloud.password=ENC(encrypted_password_from_above)
db.usage.password=ENC(encrypted_password_from_above)
```

2. Après avoir copier le nouveau mot de passe, vous pouvez maintenant démarrer CloudStack (et le moteur d'usage, si nécessaire).

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

13.1.6 Alertes pour administrateur

Le système fournit des alertes et des évènements pour aider à la gestion du cloud. Les alertes sont des avis pour les administrateurs, généralement délivrés par mail, le notifiant qu'une erreur s'est produite dans le cloud. Le comportement des alertes est configurable.

Les événements tracent toutes les actions de l'utilisateur et de l'administrateur dans le cloud. Par exemple, chaque VM invitée démarrée crée un événement associé. Les événements sont stockés dans la base de données du serveur d'administration.

Des emails seront envoyés aux administrateurs dans les circonstances suivantes :
- Les ressources du cluster de serveurs de gestion sont faibles en CPU, en mémoire ou en ressources de stockage
- Le serveur de gestion a perdu le battement de coeur d'un hôte depuis plus de 3 minutes.
- Les ressources du cluster d'hôtes sont faibles en CPU, en mémoire ou en ressources de stockage

Envoyer les alertes à un SNMP externe et à des serveurs Syslog

En plus de montrer les alertes aux administrateurs sur le tableau de bord de l'interface utilisateur CloudStack et de leur envoyer par e-mail, CloudStack peut également envoyer les mêmes alertes à un logiciel externe de gestion SNMP ou Syslog. Ceci est utile si vous préférez utiliser un gestionnaire SNMP ou Syslog pour surveiller votre nuage.

Les alertes qui peuvent être envoyées sont :

Voici la liste des numéros de type d'alerte. Les alertes actuelles peuvent être trouvées en appelant listAlerts.

```
MEMORY = 0 // Available Memory below configured threshold
```

```
CPU = 1 // Unallocated CPU below configured threshold
```

```
STORAGE =2 // Available Storage below configured threshold
```

```
STORAGE_ALLOCATED = 3 // Remaining unallocated Storage is below configured threshold

PUBLIC_IP = 4 // Number of unallocated virtual network public IPs is below configured threshold

PRIVATE_IP = 5 // Number of unallocated private IPs is below configured threshold

SECONDARY_STORAGE = 6 //  Available Secondary Storage in availability zone is below configured thresh

HOST = 7 // Host related alerts like host disconnected

USERVM = 8 // User VM stopped unexpectedly

DOMAIN_ROUTER = 9 // Domain Router VM stopped unexpectedly

CONSOLE_PROXY = 10 // Console Proxy VM stopped unexpectedly

ROUTING = 11 // Lost connection to default route (to the gateway)

STORAGE_MISC = 12 // Storage issue in system VMs

USAGE_SERVER = 13 // No usage server process running

MANAGMENT_NODE = 14 // Management network CIDR is not configured originally

DOMAIN_ROUTER_MIGRATE = 15 // Domain Router VM Migration was unsuccessful

CONSOLE_PROXY_MIGRATE = 16 // Console Proxy VM Migration was unsuccessful

USERVM_MIGRATE = 17 // User VM Migration was unsuccessful

VLAN = 18 // Number of unallocated VLANs is below configured threshold in availability zone

SSVM = 19 // SSVM stopped unexpectedly

USAGE_SERVER_RESULT = 20 // Usage job failed

STORAGE_DELETE = 21 // Failed to delete storage pool

UPDATE_RESOURCE_COUNT = 22 // Failed to update the resource count

USAGE_SANITY_RESULT = 23 // Usage Sanity Check failed

DIRECT_ATTACHED_PUBLIC_IP = 24 // Number of unallocated shared network IPs is low in availability zor

LOCAL_STORAGE = 25 // Remaining unallocated Local Storage is below configured threshold

RESOURCE_LIMIT_EXCEEDED = 26 //Generated when the resource limit exceeds the limit. Currently used fo
```

Vous pouvez également afficher la liste la plus à jour en appelant la commande d'API `listAlerts`.

Détails des alertes SNMP

Le protocole supporté est le SNMP version 2.

Chaque trap SNMP contient les informations suivantes : message, podId, dataCenterId, clusterId, et generationTime.

Détails des alertes Syslog

CloudStack génère un message syslog pour chaque alerte. Chaque message syslog inclut les champs alertType, message, podId, dataCenterId et clusterId, dans le format suivant. Si un champ ne possède pas de valeur valide, il ne sera pas inclus.

```
Date severity_level Management_Server_IP_Address/Name  alertType:: value dataCenterId:: value  podId
```

Par exemple :

```
Mar  4 10:13:47    WARN    localhost    alertType:: managementNode message:: Management server node 1
```

Configurer SNMP et les serveurs Syslog

Pour configurer un ou plusieurs gestionnaire SNMP ou Syslog pour qu'ils reçoivent les alertes depuis CloudStack :

1. Dans le cadre d'un gestionnaire SNMP, installez le fichier de la MIB CloudStack sur votre système de gestion SNMP. Cela fait correspondre les OID SNMP aux traps d'interruption qui peuvent être plus facilement lus par les utilisateurs. Le fichier doit être accessible publiquement. Pour plus d'informations sur l'installation de ce fichier, consultez la documentation fournie avec le gestionnaire SNMP.
2. Editer le fichier /etc/cloudstack/management/log4j-cloud.xml.

```
# vi /etc/cloudstack/management/log4j-cloud.xml
```

3. Ajoutez une entrée en utilisant la syntaxe ci-dessous. Suivez l'exemple approprié selon que vous ajoutez un gestionnaire SNMP ou un gestionnaire Syslog. Pour spécifier plusieurs gestionnaires externes, séparez les adresses IP et les autres valeurs de configuration par des virgules (,).

   Note : Le nombre maximum recommandé de gestionnaires SNMP ou Syslog est de 20 de chaque.

   L'exemple suivant montre comment configurer deux gestionnaires SNMP aux adresses IP 10.1.1.1 et 10.1.1.2. Remplacez avec vos propres adresses IP, ports et communautés. Ne modifiez pas les autres valeurs (nom, seuil, classe et valeurs de mise en page).

```
<appender name="SNMP" class="org.apache.cloudstack.alert.snmp.SnmpTrapAppender">
  <param name="Threshold" value="WARN"/>  <!-- Do not edit. The alert feature assumes WARN. -->
  <param name="SnmpManagerIpAddresses" value="10.1.1.1,10.1.1.2"/>
  <param name="SnmpManagerPorts" value="162,162"/>
  <param name="SnmpManagerCommunities" value="public,public"/>
  <layout class="org.apache.cloudstack.alert.snmp.SnmpEnhancedPatternLayout"> <!-- Do not edit
    <param name="PairDelimeter" value="//"/>
    <param name="KeyValueDelimeter" value="::"/>
  </layout>
</appender>
```

   L'exemple suivant montre comment configurer deux gestionnaires Syslog aux adresses IP 10.1.1.1 et 10.1.1.2. Remplacez par vos propres adresses IP. Vous pouvez définir le niveau de Facility par une valeur définie par syslog, telle que LOCAL0 - LOCAL7. Ne modifiez pas les autres valeurs.

```
<appender name="ALERTSYSLOG">
  <param name="Threshold" value="WARN"/>
  <param name="SyslogHosts" value="10.1.1.1,10.1.1.2"/>
  <param name="Facility" value="LOCAL6"/>
  <layout>
    <param name="ConversionPattern" value=""/>
  </layout>
</appender>
```

4. Si votre cloud est composé de plusieurs serveur de gestion, répéter ces étapes pour éditer log4j-cloud.xml sur chaque instance.
5. Si vous avez effectué ces changements alors que le serveur de gestion fonctionnait, attendre quelques minutes pour que les changements prennent effets.

Dépannage : Si aucune alerte ne s'affiche sur le gestionnaire SNMP ou Syslog configuré après un délai raisonnable, il est probable qu'il y ait une erreur dans la syntaxe de l'entrée <appender> dans log4j-cloud.xml. Assurez-vous que le format et les paramètres soient corrects.

Retirer un serveur SNMP ou un serveur Syslog

Pour retirer un gestionnaire externe SNMP ou Syslog de manière à ce qu'il ne reçoive plus d'alertes depuis CloudStack, retirer l'entrée correspondante dans le fichier `/etc/cloudstack/management/log4j-cloud.xml`.

13.1.7 Personnaliser le Nom de domaine du réseau

L'administrateur racine peut optionnellement affecter un suffixe DNS personnalisé au niveau d'un réseau, d'un compte, d'un domaine, d'une zone ou de toute l'installation de CloudStack, et un administrateur de domaine peut le faire dans son propre domaine. Pour spécifier un nom de domaine personnalisé et le mettre en œuvre, procédez comme ceci :

1. Définir le suffixe DNS sur la portée souhaitée
   - Au niveau du réseau, le suffixe DNS peut être attribué via l'interface utilisateur à la création d'un nouveau réseau, comme décrit dans "Ajout d'un réseau d'invités supplémentaire" ou via la commande updateNetwork de l'API CloudStack.
   - Au niveau du compte, du domaine ou de la zone, le suffixe DNS peut être attribué avec les commandes appropriées de l'API CloudStack : createAccount, editAccount, createDomain, editDomain, createZone ou editZone.
   - Au niveau global, utilisez le paramètre de configuration guest.domain.suffix. Vous pouvez également utiliser la commande updateConfiguration de l'API CloudStack. Après avoir modifié cette configuration globale, redémarrez le serveur de gestion pour prendre en compte le nouveau paramètre.
2. Pour que le nouveau suffixe DNS prenne effet pour un réseau existant, appelez la commande updateNetwork de l'API CloudStack. Cette étape n'est pas nécessaire lorsque le suffixe DNS a été spécifié lors de la création d'un nouveau réseau.

La source du domaine du réseau qui est utilisée dépend des règles suivantes.

- Pour tous les réseaux, si un domaine réseau est spécifié comme faisant partie de la configuration propre à son réseau, cette valeur est utilisée.
- Pour un réseau spécifique à un compte, le domaine réseau spécifié pour le compte est utilisé. Si aucun n'est spécifié, le système recherche une valeur dans le domaine, la zone et la configuration globale, dans cet ordre.
- Pour un réseau spécifique à un domaine, le domaine réseau spécifié pour le domaine est utilisé. Si aucun n'est spécifié, le système recherche une valeur dans la zone et dans la configuration globale, dans cet ordre.
- Pour un réseau spécifique à une zone, le domaine réseau spécifié pour la zone est utilisé. Si aucun n'est spécifié, le système recherche une valeur dans la configuration globale.

13.1.8 Arrêter et redémarrer le serveur de gestion

L'administrateur racine va devoir stopper et redémarrer le serveur de gestion de temps en temps.

Par exemple, après avoir changé un paramètre de configuration global, un redémarrage est requis. Si vous avez plusieurs noeuds de serveurs de gestion, tous les redémarrer pour rendre la nouvelle valeur du paramètre effectivement permanente dans le cloud.

Pour stopper le serveur de gestion, exécuter la commande suivante à l'invite de commande du système d'exploitation sur le noeud du serveur de gestion.

```
# service cloudstack-management stop
```

Pour démarrer le serveur de gestion :

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

Fiabilité et disponibilité du système

14.1 System Reliability and High Availability

14.1.1 HA for Management Server

The CloudStack Management Server should be deployed in a multi-node configuration such that it is not susceptible to individual server failures. The Management Server itself (as distinct from the MySQL database) is stateless and may be placed behind a load balancer.

Normal operation of Hosts is not impacted by an outage of all Management Serves. All guest VMs will continue to work.

When the Management Server is down, no new VMs can be created, and the end user and admin UI, API, dynamic load distribution, and HA will cease to work.

14.1.2 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)	Oui
8250	8250	TCP	Oui
8096	8096	HTTP	Non

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.

14.1.3 HA-Enabled Virtual Machines

The user can specify a virtual machine as HA-enabled. By default, all virtual router VMs and Elastic Load Balancing VMs are automatically configured as HA-enabled. When an HA-enabled VM crashes, CloudStack detects the crash and restarts the VM automatically within the same Availability Zone. HA is never performed across different Availability Zones. CloudStack has a conservative policy towards restarting VMs and ensures that there will never be two

instances of the same VM running at the same time. The Management Server attempts to start the VM on another Host in the same cluster.

HA features work with iSCSI or NFS primary storage. HA with local storage is not supported.

14.1.4 HA for Hosts

The user can specify a virtual machine as HA-enabled. By default, all virtual router VMs and Elastic Load Balancing VMs are automatically configured as HA-enabled. When an HA-enabled VM crashes, CloudStack detects the crash and restarts the VM automatically within the same Availability Zone. HA is never performed across different Availability Zones. CloudStack has a conservative policy towards restarting VMs and ensures that there will never be two instances of the same VM running at the same time. The Management Server attempts to start the VM on another Host in the same cluster.

HA features work with iSCSI or NFS primary storage. HA with local storage is not supported.

Dedicated HA Hosts

One or more hosts can be designated for use only by HA-enabled VMs that are restarting due to a host failure. Setting up a pool of such dedicated HA hosts as the recovery destination for all HA-enabled VMs is useful to :

- Make it easier to determine which VMs have been restarted as part of the CloudStack high-availability function. If a VM is running on a dedicated HA host, then it must be an HA-enabled VM whose original host failed. (With one exception : It is possible for an administrator to manually migrate any VM to a dedicated HA host.).
- Keep HA-enabled VMs from restarting on hosts which may be reserved for other purposes.

The dedicated HA option is set through a special host tag when the host is created. To allow the administrator to dedicate hosts to only HA-enabled VMs, set the global configuration variable ha.tag to the desired tag (for example, “ha_host”), and restart the Management Server. Enter the value in the Host Tags field when adding the host(s) that you want to dedicate to HA-enabled VMs.

Note : If you set ha.tag, be sure to actually use that tag on at least one host in your cloud. If the tag specified in ha.tag is not set for any host in the cloud, the HA-enabled VMs will fail to restart after a crash.

14.1.5 Primary Storage Outage and Data Loss

When a primary storage outage occurs the hypervisor immediately stops all VMs stored on that storage device. Guests that are marked for HA will be restarted as soon as practical when the primary storage comes back on line. With NFS, the hypervisor may allow the virtual machines to continue running depending on the nature of the issue. For example, an NFS hang will cause the guest VMs to be suspended until storage connectivity is restored.Primary storage is not designed to be backed up. Individual volumes in primary storage can be backed up using snapshots.

14.1.6 Secondary Storage Outage and Data Loss

For a Zone that has only one secondary storage server, a secondary storage outage will have feature level impact to the system but will not impact running guest VMs. It may become impossible to create a VM with the selected template for a user. A user may also not be able to save snapshots or examine/restore saved snapshots. These features will automatically be available when the secondary storage comes back online.

Secondary storage data loss will impact recently added user data including templates, snapshots, and ISO images. Secondary storage should be backed up periodically. Multiple secondary storage servers can be provisioned within each zone to increase the scalability of the system.

14.1.7 Database High Availability

To help ensure high availability of the databases that store the internal data for CloudStack, you can set up database replication. This covers both the main CloudStack database and the Usage database. Replication is achieved using the MySQL connector parameters and two-way replication. Tested with MySQL 5.1 and 5.5.

How to Set Up Database Replication

Database replication in CloudStack is provided using the MySQL replication capabilities. The steps to set up replication can be found in the MySQL documentation (links are provided below). It is suggested that you set up two-way replication, which involves two database nodes. In this case, for example, you might have node1 and node2.

You can also set up chain replication, which involves more than two nodes. In this case, you would first set up two-way replication with node1 and node2. Next, set up one-way replication from node2 to node3. Then set up one-way replication from node3 to node4, and so on for all the additional nodes.

References :

- http://dev.mysql.com/doc/refman/5.0/en/replication-howto.html
- https://wikis.oracle.com/display/CommSuite/MySQL+High+Availability+and+Replication+Information+For+Calendar+Server

Configuring Database High Availability

To control the database high availability behavior, use the following configuration settings in the file /etc/cloudstack/management/db.properties.

Required Settings

Be sure you have set the following in db.properties :

- `db.ha.enabled` : set to true if you want to use the replication feature.
  Example : `db.ha.enabled=true`
- `db.cloud.slaves` : set to a comma-delimited set of slave hosts for the cloud database. This is the list of nodes set up with replication. The master node is not in the list, since it is already mentioned elsewhere in the properties file.
  Example : `db.cloud.slaves=node2,node3,node4`
- `db.usage.slaves` : set to a comma-delimited set of slave hosts for the usage database. This is the list of nodes set up with replication. The master node is not in the list, since it is already mentioned elsewhere in the properties file.
  Example : `db.usage.slaves=node2,node3,node4`

Optional Settings

The following settings must be present in db.properties, but you are not required to change the default values unless you wish to do so for tuning purposes :

- `db.cloud.secondsBeforeRetryMaster` : The number of seconds the MySQL connector should wait before trying again to connect to the master after the master went down. Default is 1 hour. The retry might happen sooner if db.cloud.queriesBeforeRetryMaster is reached first.
  Example : `db.cloud.secondsBeforeRetryMaster=3600`
- `db.cloud.queriesBeforeRetryMaster` : The minimum number of queries to be sent to the database before trying again to connect to the master after the master went down. Default is 5000. The retry might happen sooner if db.cloud.secondsBeforeRetryMaster is reached first.
  Example : `db.cloud.queriesBeforeRetryMaster=5000`
- `db.cloud.initialTimeout` : Initial time the MySQL connector should wait before trying again to connect to the master. Default is 3600.
  Example : `db.cloud.initialTimeout=3600`

Limitations on Database High Availability

The following limitations exist in the current implementation of this feature.

- Slave hosts can not be monitored through CloudStack. You will need to have a separate means of monitoring.
- Events from the database side are not integrated with the CloudStack Management Server events system.
- You must periodically perform manual clean-up of bin log files generated by replication on database nodes. If you do not clean up the log files, the disk can become full.

Plugins

15.1 Quota Plugin

Quota service, while allowing for scalability, will make sure that the cloud is not exploited by attacks, careless use and program errors. To address this problem, employ the quota-enforcement service that allows resource usage within certain bounds as defined by policies and available quotas for various entities. Quota service extends the functionality of usage server to provide a measurement for the resources used by the accounts and domains using a common unit referred to as cloud currency in this document. It can be configured to ensure that your usage won't exceed the budget allocated to accounts/domain in cloud currency. It will let user know how much of the cloud resources he is using. It will help the cloud admins, if they want, to ensure that a user does not go beyond his allocated quota. Per usage cycle if an account is found to be exceeding its quota then it is locked. Locking an account means that it will not be able to initiate a new resource allocation request, whether it is more storage or an additional ip. To unlock an account you need to add more credit to it. In case you want the locking to be disabled on global or on account scope those provisions are also provided. Needless to say quota service as well as any action on the account is configurable.

15.1.1 Enabling the Quota Service

Before installing and configuring the quota service you need to make sure that the Usage Server has been installed. This requires extra steps beyond just installing the CloudStack software. See Installing the Usage Server (Optional) in the Advanced Installation Guide.

1. enable.usage.server : Set to true to enable usage server.

The quota plugin is disabled by default. To enable it goto Global Settings and set the following global configuration to true :

1. quota.enable.service

By default Quota service does not lock the accounts that have exceeded the quota usage. To enable quota service to lock accounts set the following global configuration to true :

1. quota.enable.enforcement

The other configurations that are there for quota service are as :

1. quota.currency.symbol : The symbol that is used before any currency figure in various quota forms and reports.
2. quota.usage.smtp.host : Quota SMTP host for sending quota alerts.
3. quota.usage.smtp.port : Quota SMTP port.
4. quota.usage.smtp.user : Quota SMTP user.
5. quota.usage.smtp.password : Quota SMTP password.
6. quota.usage.smtp.sender : Quota SMTP alert sender email address.
7. quota.usage.smtp.useAuth : If true, use secure SMTP authentication when sending emails.
8. quota.usage.smtp.connection.timeout : Quota SMTP server connection timeout duration.

There are several configuration variables that are inherited from usage server, these are listed below :

1. usage.aggregation.timezone

All these are described in details in Usage Server documentation.

Restart the Management Server and the Usage Server to enable the set configuration values.

```
service cloudstack-management restart
service cloudstack-usage restart
```

Once the quota service is running it will calculate the quota balance for each account. The quota usage is calculated as per the quota tariff provided by the site administrator.

15.1.2 Quota Tariff

The following table shows all quota types for which you can specify tariff.

Type ID	Type Name	Tariff Description
1	RUNNING_VM	One month of running Compute-Month
2	ALLOCATED_VM	One month of allocated VM
3	IP_ADDRESS	Quota for a month of allocated IP
4	NETWORK_BYTES_SENT	Quota for 1GB bytes sent
5	NETWORK_BYTES_RECEIVED	Quota for 1GB bytes sent
6	VOLUME	Quota for 1 GB of Volume use for a month
7	TEMPLATE	Quota for 1 GB of Template use for a month
8	ISO	Quota for 1 GB of ISO use for a month
9	SNAPSHOT	Quota for 1 GB of SNAPSHOT use for a month
11	LOAD_BALANCER_POLICY	Quota for load balancer policy month
12	PORT_FORWARDING_RULE	**Quota for port forwarding** policy month
13	NETWORK_OFFERING	Quota for network Offering for a month
14	VPN_USERS	**Quota for VPN usage** for a month
15	CPU_CLOCK_RATE	The tariff for using 1 CPU i100 MHz clock
16	CPU_NUMBER	The quota tariff for using 1 virtual CPU.
17	MEMORY	The quota tariff for using 1MB RAM size.

The quota tariff can be listed using listQuotaTariff API.

quotaTariff : Lists all quota tariff plans

The tariff for each of the above can be set by using the updateQuotaTariff API.

15.1.3 Quota Credits

The quota credit (quotaCredit) API lets you add or remove quota currency credits to an account. With this API you can also control the quota enforcement policy at account level. This will enable you to have some accounts where the quota policy is not enforced. The overall quota enforcement is controlled by the quota.enable.enforcement global setting.

In addition to above the quota API lets you can fine tune the alert generation by specifying the quota threshold for each account. If not explictly stated, the threshold is taken as 80% of the last deposit.

15.1.4 Quota Balance

Quota balance API states the start balance and end balance(optional) from a start date to end date (optional).

15.1.5 Quota Statement

Quota statement for a period consist of the quota usage under various quota types for the given period from a start date to an end date.

15.1.6 Quota Monthly Statement

Quota service emails the monthly quota statement for the last month at the beginning of each month. For this service to work properly you need to ensure that the usage server is running.

15.1.7 Quota Alert Management

Quota module also provides APIs to customize various email templates that are used to alert account owners about quota going down below threshold and quota getting over.

All the above functionality is also available via quota UI plugin.

CHAPITRE 16

Optimisations

16.1 Optimisation

Cette section fournie des astuces sur comment optimiser la performance de votre cloud.

16.1.1 Surveiller la performance

La surveillance de la performance des hôtes et des invités est disponible aux utilisateurs finaux et aux administrateurs. Ceci autorise les utilisateurs à surveiller leur utilisation des ressources et déterminer quand il est approprié de choisir une offre de service plus puissante ou un disque plus grand.

16.1.2 Augmenter la mémoire maximale du serveur de gestion

Si un serveur de gestion est le sujet d'une forte charge, l'allocation par défaut du maximum de mémoire de la JVM peut devenir insuffisante. Pour augmenter la mémoire :

1. Editer le fichier de configuration de Tomcat :

```
/etc/cloudstack/management/tomcat6.conf
```

2. Changer le paramètre de ligne de commande -XmxNNNm pour une valeur supérieure de N.
   Pour exemple, si la valeur en cours est -Xmx128m, la changer pour -Xmx1024m ou plus.
3. Pour rendre les nouveaux paramètres actifs, redémarrer le serveur de gestion.

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

Pour plus d'information à propos des problèmes de mémoire, voir "FAQ : Mémoire" sur le Wiki Tomcat.

16.1.3 Fixer la taille du Tampon du Pool Database

Il est important de fournir suffisamment d'espace mémoire à la base de données MySQL pour cacher les données et les index :

1. Editer le fichier de configuration de MySQL :

```
/etc/my.cnf
```

2. Insérer la ligne suivante dans la section [mysqld], sous la ligne datadir. Utiliser une valeur qui est approprié pour votre situation. Nous recommandons de configurer le pool de mémoires tampons à 40% de la RAM si MySQL est sur le même serveur que le serveur de gestion ou 70% de la RAM si MySQL est sur un serveur dédié. L'exemple suivant assume un serveur dédié avec 1024 de RAM.

```
innodb_buffer_pool_size=700M
```

3. Redémarrer le service MySQL.

```
# service mysqld restart
```

Pour plus d'information à propos du tampon du pool, voir "The InnoDB Buffer Pool" dans le Manuel de Référence de MySQL.

16.1.4 Fixer et surveiller les limites totales de VM par hôte.

L'administrateur CloudStack devrait surveiller le nombre total d'instances de VM dans chaque cluster, et désactiver l'allocation à un cluster si le total s'approche du maximum que l'hyperviseur peut supporter. Soyez sur de laisser une marge de sécurité pour autoriser dans le cas où un ou plusieurs hôtes tomberaient en panne, ce qui augmenterait la charge en VM sur les autres hôtes comme leur VMs seraient automatiquement redéployées. Consulter la documentation de votre hyperviseur pour trouver le nombre maximum de VM par hôte, puis utiliser les paramètres de configuration globale de CloudStack pour le fixer comme limite par défaut. Surveiller l'activité des VM sur chaque cluster à tout moment. Conserver le nombre total de VMs sous un niveau de sécurité qui permet les pannes occasionnelles d'un hôte. Par exemple, si il y a N hôtes dans un cluster et que vous voulez permettre à un hôte dans le cluster d'être éteint à la fois, le nombre total d'instances de VM que vous pouvez permettre dans le cluster est au plus (N-1) * (limite-par-hôte). Une fois que le cluster a atteins le nombre de VMs, utiliser l'interface de CloudStack pour désactiver l'allocation de plus de VMs dans le cluster.

16.1.5 Configurer la mémoire du dom0 XenServer

Configurer les paramètres dom0 du XenServer pour allouer plus de mémoire à dom0. Cela peut activer XenServer pour traiter un plus grand nombre de machines virtuelles. Nous recommandons 2940 MB de RAM pour le dom0 XenServer. Pour les instructions sur comment faire ceci, voir l'Article de la base de connaissance Citrix.L'article se réfère à XenServer 5.6, mais les mêmes informations s'appliquent à XenServer 6.

CHAPITRE 17

Les évènements et le dépannage

17.1 Notification d'évènement

Un évènement est essentiellement un changement important ou significatif de l'état des ressources virtuelles ou physiques associées à l'environnement cloud.

17.1.1 Journal d'évènements

Il y a deux types d'évènements consignés dans le journal des évènements de CloudStack. Les évènements standard enregistrent le succès ou l'échec d'un évènement et peuvent être utilisés pour identifier les travaux ou les processus qui ont échoué. Il peut aussi y avoir des évènements de travaux longs. Les évènements pour les travaux asynchrones enregistrent lorsque le travail est programmé, lorsqu'il démarre et lorsqu'il est terminé. Les autres travaux long synchrones enregistrent quand le travail démarre et quand il est terminé. Les enregistrements d'évènements long synchrones et asynchrones peuvent être utilisés pour obtenir plus d'informations sur le statut d'un travail en cours ou peuvent être utilisés pour identifier un travail qui est suspendu ou qui n'a pas démarré. Les sections suivantes fournissent plus d'informations sur ces évènements.

17.1.2 Notification

Le framework de notification d'évènement fournit un moyen pour les composants du Serveur de Gestion de publier des évènements ou d'y souscrire. La notification d'évènement est obtenue en implémentant le concept d'abstraction de bus d'évènement dans le Serveur de Gestion.

Un nouvel évènement par changement d'état de ressource est inséré au sein du framework de notification d'évènements. Chaque ressource, comme une VM utilisateur, un volume, une interface réseau, une IP publique, un instantané ou un modèle, est associé avec un état de machine et génère des évènements en tant que partie du changement d'état. Cela implique qu'un changement dans l'état d'une ressource résulte à un évènement de changement d'état et que l'évènement est publié dans l'état de la machine correspondant sur le bus d'évènement. Tous les évènements CloudStack (alertes, évènements d'action, évènements d'utilisation) et la catégorie additionnelle des évènements de changement des états de ressources sont publiés sur le bus d'évènements.

Implémentations

Un bus d'évènement est introduit dans le Serveur de Gestion ce qui autorise les composants CloudStack et ses plug-ins d'extension à souscrire aux évènements en utilisant le client Advanced Message Queuing Protocol (AMQP). Dans CloudStack, une implémentation par défaut du bus d'évènement est fourni comme un plug-in qui utilise le client AMQP RabbitMQ. Le client AMQP pousse les évènements publiés à un serveur AMQP compatible. Par conséquent, tous les évènements CloudStack sont publiés sur un échange du serveur AMQP.

En complément, une implémentation en mémoire et une implémentation Apache Kafka sont toutes deux disponibles.

Cas d'usages

Les exemples suivants sont des cas d'usages :

— Moteurs de facturation ou d'utilisation. Une solution tiers d'utilisation du cloud peut implémenter un plugin qui peut se connecter à CloudStack pour s'abonner aux évènements CloudStack et généré des données d'utilisation. La donnée d'utilisation est utilisée par leur logiciel d'utilisation.
— Le plugin AMQP place tous les évènements dans une file de messages, un courtier de messages AMQP peut ensuite fournir une notification basée sur les sujets aux abonnés.
— Publier et souscrire au service de notifications peut être implémenté comme un service enfichable dans CloudStack qui peut fournir un ensemble riche d'API pour la notification d'évènements, comme une souscription ou une notification par sujets.

Configuration AMQP

En tant qu'administrateur CloudStack, effectuer la configuration suivante une fois pour activer le framework de notification d'évènement. En fonctionnement, aucun changement ne peut contrôler le comportement.

1. Créer le dossier `/etc/cloudstack/management/META-INF/cloudstack/core`
2. Dans ce dossier, ouvrir `spring-event-bus-context.xml`.
3. Définir un bean appelé `eventNotificationBus` comme ceci :
   — name : Spécifier un nom pour le bean.
   — server : Le nom ou l'adresse IP du serveur RabbitMQ AMQP.
   — port : Le port sur lequel le serveur RabbitMQ fonctionne.
   — username : Le nom d'utilisateur associé avec le compte pour accéder au serveur RabbitMQ.
   — password : Le mot de passe associé avec le nom d'utilisateur du compte pour accéder au serveur RabbitMQ.
   — exchange : Le nom d'échange sur le serveur RabbitMQ où les évènements sont publiés.
   Un exemple de bean est donné ci-dessous :

```
<beans xmlns="http://www.springframework.org/schema/beans"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:context="http://www.springframework.org/schema/context"
xmlns:aop="http://www.springframework.org/schema/aop"
xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-3.0.xsd
http://www.springframework.org/schema/aop http://www.springframework.org/schema/aop/spring-a
http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context-3.0.xsd">
   <bean id="eventNotificationBus" class="org.apache.cloudstack.mom.rabbitmq.RabbitMQEventBu
      <property name="name" value="eventNotificationBus"/>
      <property name="server" value="127.0.0.1"/>
      <property name="port" value="5672"/>
      <property name="username" value="guest"/>
      <property name="password" value="guest"/>
      <property name="exchange" value="cloudstack-events"/>
   </bean>
</beans>
```

Le bean `eventNotificationBus` bean représente la classe `org.apache.cloudstack.mom.rabbitmq.RabbitMQEventBus`.
Si vous voulez utiliser une valeur chiffré pour le nom d'utilisateur et le mot de passe, vous devez inclure un bean pour fournir ceux-ci comme variable depuis un fichier d'identification.
Un exemple est donné ci-dessous

```
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:aop="http://www.springframework.org/schema/aop"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
        http://www.springframework.org/schema/beans/spring-beans-3.0.xsd
        http://www.springframework.org/schema/aop http://www.springframework.org/schema/aop/
        http://www.springframework.org/schema/context
        http://www.springframework.org/schema/context/spring-context-3.0.xsd"
>

   <bean id="eventNotificationBus" class="org.apache.cloudstack.mom.rabbitmq.RabbitMQEventBu
      <property name="name" value="eventNotificationBus"/>
      <property name="server" value="127.0.0.1"/>
      <property name="port" value="5672"/>
      <property name="username" value="${username}"/>
      <property name="password" value="${password}"/>
      <property name="exchange" value="cloudstack-events"/>
   </bean>

   <bean id="environmentVariablesConfiguration" class="org.jasypt.encryption.pbe.config.Envi
      <property name="algorithm" value="PBEWithMD5AndDES" />
      <property name="passwordEnvName" value="APP_ENCRYPTION_PASSWORD" />
   </bean>

   <bean id="configurationEncryptor" class="org.jasypt.encryption.pbe.StandardPBEStringEncry
      <property name="config" ref="environmentVariablesConfiguration" />
   </bean>

   <bean id="propertyConfigurer" class="org.jasypt.spring3.properties.EncryptablePropertyPla
      <constructor-arg ref="configurationEncryptor" />
      <property name="location" value="classpath:/cred.properties" />
   </bean>
</beans>
```

Créer un nouveau fichier dans le même dossier appelé `cred.properties` et spécifier les valeurs pour le nom d'utilisateur et le mot de passe avec des chaînes de caractères javascripts cryptées.
Par exemple, avec `guest` comme valeurs pour les deux champs :

```
username=nh2XrM7jWHMG4VQK18iiBQ==
password=nh2XrM7jWHMG4VQK18iiBQ==
```

4. Redémarrez votre serveur de gestion.

Configuration Kafka

En tant qu'administrateur CloudStack, effectuer la configuration suivante une fois pour activer le framework de notification d'évènement. En fonctionnement, aucun changement ne peut contrôler le comportement.

1. Créer un fichier de configuration approprié dans `/etc/cloudstack/management/kafka.producer.properties` qui contient les propriétés de configuration valides comme documenté dans http://kafka.apache.org/documentation.html#newproducerconfigs. Les propriétés peuvent contenir une propriété additionnelle `topic` qui, si elle n'est pas fournie, sera par défaut `cloudstack`. Comme `key.serializer` et `value.serializer` sont en général requis pour un producteur pour démarrer correctement, ils peuvent être omis et prendront par défaut la valeur `org.apache.kafka.common.serialization.StringSerializer`.
2. Créer le dossier `/etc/cloudstack/management/META-INF/cloudstack/core`

3. Dans ce dossier, ouvrir `spring-event-bus-context.xml`.
4. Définir un bean appelé `eventNotificationBus``avec un seul attribut ``name`. Un exemple de bean est donné ci-dessous :

```
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:aop="http://www.springframework.org/schema/aop"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
                           http://www.springframework.org/schema/beans/spring-beans-3.0.xsd
                           http://www.springframework.org/schema/aop http://www.springframework
                           http://www.springframework.org/schema/context
                           http://www.springframework.org/schema/context/spring-context-3.0.xsd
   <bean id="eventNotificationBus" class="org.apache.cloudstack.mom.kafka.KafkaEventBus">
     <property name="name" value="eventNotificationBus"/>
   </bean>
 </beans>
```

5. Redémarrez votre serveur de gestion.

17.1.3 Evènements standards :

Le journal d'évènements enregistre trois types d'évènements standards.
- INFO. Cet évènement est généré lorsque une opération a été effectuée avec succès.
- WARN. Cet évènement est généré dans les circonstances suivantes.
  - Quand un réseau est déconnecté lors de la surveillance du téléchargement d'un modèle.
  - Quand un téléchargement de modèle est abandonné.
  - Quand un problème sur le serveur de stockage provoque le basculement des volumes sur le serveur de stockage mirroir.
- ERROR. Cet évènement est généré lorsqu'une opération n'a pas été effectuée avec succès.

17.1.4 Évènements de l'exécution des longs travaux

Le journal d'évènements enregistre trois types d'évènements standards.
- INFO. Cet évènement est généré lorsque une opération a été effectuée avec succès.
- WARN. Cet évènement est généré dans les circonstances suivantes.
  - Quand un réseau est déconnecté lors de la surveillance du téléchargement d'un modèle.
  - Quand un téléchargement de modèle est abandonné.
  - Quand un problème sur le serveur de stockage provoque le basculement des volumes sur le serveur de stockage mirroir.
- ERROR. Cet évènement est généré lorsqu'une opération n'a pas été effectuée avec succès.

17.1.5 Requête sur le journal d'évènements

Les enregistrements de la base de données peuvent être requêtés depuis l'interface utilisateur. La liste des évènements capturés par le système incluent :
- La création, suppression et les opérations de gestion en cours des machines virtuelles
- La création, suppression et les opérations de gestion en cours des routeurs virtuels
- La création et suppression de modèles
- La création et suppression des règles de réseau/répartition de charge
- La création et suppression de volume de stockage
- La connexion et la déconnexion de l'utilisateur

17.1.6 La suppression et l'archivage des évènements et des alertes

CloudStack vous offre la possibilité de supprimé ou d'archiver les alertes et les évènements existant que vous ne voulez plus implémenter. Vous pouvez régulièrement supprimer ou archiver n'importe quelles alertes ou évènements que vous ne pouvez ou ne voulez plus résoudre depuis la base de données.

Vous pouvez supprimer ou archiver des alertes ou des évènements individuels soit en utilisant la vue rapide ou en utilisant la page Détails. Si vous voulez supprimer plusieurs alertes ou évènements en même temps, vous pouvez utiliser le menu contextuel respectif. Vous pouvez supprimer des alertes ou des évènements par catégories pour une période de temps. Par exemple, vous pouvez sélectionner les catégories comme **USER.LOGOUT**, **VM.DESTROY**, **VM.AG.UPDATE**, **CONFIGURATION.VALUE.EDI** etc. Vous pouvez également voir le nombre d'évènements ou d'alertes archivés ou supprimés.

Pour supporter la suppression ou l'archivage des alertes, les paramètres globaux suivants ont été ajoutés :

- **alert.purge.delay** : Les alertes plus vieilles que le nombre de jours spécifié sont purgées. Mettre à 0 pour ne jamais purger les alertes.
- **alert.purge.interval** : L'intervalle en secondes à attendre avant de lancer le processus de purge des alertes. Le défaut est de 86400 secondes (un jour).

Note : Les alertes les évènements archivés ne peuvent pas être visualisés dans l'interface ou en utilisant l'API. Ils sont conservés en base de données à des fins d'audits ou de conformités.

Permissions

Considérer ce qui suit :

- L'administrateur racine peut supprimer ou archiver une ou plusieurs alertes et évènements.
- L'administrateur de domaine ou l'utilisateur peuvent supprimer ou archiver un ou plusieurs évènements.

Procédure

1. Se connecter en tant qu'administrateur dans l'interface de CloudStack.
2. Dans le menu de navigation de gauche, cliquer sur Evènements.
3. Effectuer au choix :
   - Pour archiver les évènements, cliquer sur Archiver les évènements et spécifier le type d'évènement et la date.
   - Pour archiver les évènements, cliquer sur Détruire les évènements et spécifier le type d'évènement et la date.
4. Cliquer sur OK.

17.2 Dépannage

17.2.1 Travailler avec les logs du serveur

Le serveur de gestion de CloudStack consigne toutes les activités du site web, du middle tier, et de la base de données à des fins de diagnostique dans */var/log/cloudstack/management/*. CloudStack enregistre une variété de messages d'erreurs. Nous recommandons cette commande pour trouver la sortie problématique parmi les enregistrements du serveur de gestion :

Note : Lors du copier/coller d'une commande, soyez certain que la commande est collée sur une seule ligne avant de l'exécuter. Certains lecteur de document peuvent introduire un saut de ligne indésirable dans le texte copié.

```
grep -i -E 'exception|unable|fail|invalid|leak|warn|error' /var/log/cloudstack/management/management-
```

CloudStack traite les requêtes avec un identifiant de travail. Si vous trouver une error dans les logs et que vous êtes intéressés dans le dépannage de ce problème, vous pouvez faire un grep pour cet ID de travail dans les logs du serveur de gestion. Par example, en supposant que vous trouviez le message ERROR suivant :

```
2010-10-04 13:49:32,595 ERROR [cloud.vm.UserVmManagerImpl] (Job-Executor-11:job-1076) Unable to find
```

Noter que l'identifiant du travail est 1076. Vous pouvez tracer les évènements en relation avec le travail 1076 avec le grep suivant :

```
grep "job-1076)" management-server.log
```

L'agent CloudStack enregistre ses activités dans */var/log/cloudstack/agent/*.

17.2.2 Données perdues sur un stockage primaire exporté.

Symptôme

La perte de données existante sur le stockage primaire qui a été exposé comme un export de serveur Linux NFS sur un volume ISCSI.

Cause

Il est possible qu'un client depuis l'extérieur du pool attendu ait monté le stockage. Lorsque cela arrive, le LVM est corrompu et toutes les données du volume sont perdus.

Solution

Lors de la configuration de l'exportation d'un LUN, restreindre la plage des adresses IP autorisées à y accéder en spécifiant un masque de sous réseau. Par exemple :

```
echo "/export 192.168.1.0/24(rw,async,no_root_squash,no_subtree_check)" > /etc/exports
```

Ajuster la commande ci-dessous pour correspondre aux besoins de votre déploiement.

Plus d'information

Voir la procédure d'exportation dans la section "Stockage secondaire" du guide d'installation de CloudStack

17.2.3 Récupérer un routeur virtuel perdu

Symptôme

Un routeur virtuel fonctionne, mais l'hôte est déconnecté. Un routeur virtuel ne fonctionne plus comme attendu.

Cause

Le routeur virtuel est perdu ou stoppé.

Solution

Si vous êtes certain que le routeur est définitivement stoppé, ou qu'il ne fonctionne plus comme attendu, le détruire. Vous devez en créer un de nouveau tout en conservant le routeur de secours démarré et en fonctionnement (ceci suppose qu'il s'agit d'une configuration avec routeur redondant) :

- Forcer l'arrêt du routeur. Utiliser l'API stopRouter avec le paramètre forced=true pour le faire.
- Avant de continuer avec la destruction de ce routeur, assurez vous que le routeur de secours est en fonctionnement. Sinon la connexion au réseau sera perdue.
- Détruire le routeur en utilisant l'API destroyRouter.

Recréer le routeur manquant en utilisant l'API restartNetwork avec le paramètre cleanup=false. Pour plus d'information à propos de la configuration redondante des routeurs, voir Créer une nouvelle offre de réseau.

Pour plus d'information sur la syntaxe de l'API, voir la Référence de l'API à l'adresse http://cloudstack.apache.org/docs/api/.

17.2.4 Le mode de maintenance ne fonctionne pas sur un vCenter

Symptôme

L'hôte a été placé en mode maintenance, mais apparaît toujours vivant dans le vCenter.

Cause

L'interface d'administration de CloudStack a été utilisée pour basculer l'hôte en mode de maintenance programmée. Ce mode est différent du mode de maintenance du vCenter.

Solution

Utiliser le vCenter pour basculer l'hôte en mode maintenance.

17.2.5 Impossible de déployer des VMs depuis un modèle téléchargé depuis vSphere

Symptôme

Lors de la tentative de création d'une VM, la VM ne va pas se déployer.

Cause

Si le modèle a été créé en téléchargeant un fichier OVA qui a été créé en utilisant un client vSphere, il est possible que l'OVA contienne une image ISO. Si c'est le cas, le déploiement des VMs depuis le modèle va échouer.

Solution

Ejecter l'ISO et télécharger de nouveau le modèle.

17.2.6 Impossible d'allumer une machine virtuelle sur VMware

Symptôme

La machine virtuelle ne démarre pas. Vous devriez voir des erreurs comme :
- Impossible d'ouvrir le fichier Swap
- Accès impossible à un fichier avec verrou
- Accès impossible à la configuration d'une machine virtuelle

Cause

Une erreur connue sur les machines VMware. Les hôtes ESX verrouille certains fichiers et systèmes de fichiers de machine virtuelle critique pour prévenir de changement concurrent. Parfois, les fichiers ne sont pas déverouillés quand la machine virtuelle est éteinte. Quand la machine virtuelle essaie de redémarrer, elle ne peut pas accéder à ces fichiers critiques, et la machine virtuelle n'est pas capable de démarrer.

Solution

Voir ce qui suit :

Article de la base de connaissance VMware

17.2.7 Les règles du répartiteur de charge échouent après un changement d'offre réseau

Symptôme

Après le changement d'offre réseau sur un réseau, les règles du répartiteur de charge ne fonctionnent plus.

Cause

Les règles de répartitions de charge ont été créées lors de l'utilisation d'une offre de service qui inclue un répartiteur de charge physique externe comme un NetScaler, et plus tard l'offre de service réseau à changée pour une qui utilise un routeur virtuel CloudStack.

Solution

Créer une règle de firewall sur le routeur virtuel pour chacune de vos règles de répartition de charge afin qu'elles continuent à fonctionner.

17.2.8 Dépanner le trafic Internet

Ci-dessous les quelques étapes de dépannage pour vérifier ce qui ne va pas avec votre réseau...

Étapes de dépannage

1. Les commutateurs doivent être configurés correctement pour laisser passer le trafic VLAN. Vous pouvez vérifier si le trafic VLAN fonctionne en montant une interface sur les hôtes et en pinguant entre eux comme ci-dessous...

   Sur *host1 (kvm1)*

```
kvm1 ~$ vconfig add eth0 64
kvm1 ~$ ifconfig eth0.64 1.2.3.4 netmask 255.255.255.0 up
kvm1 ~$ ping 1.2.3.5
```

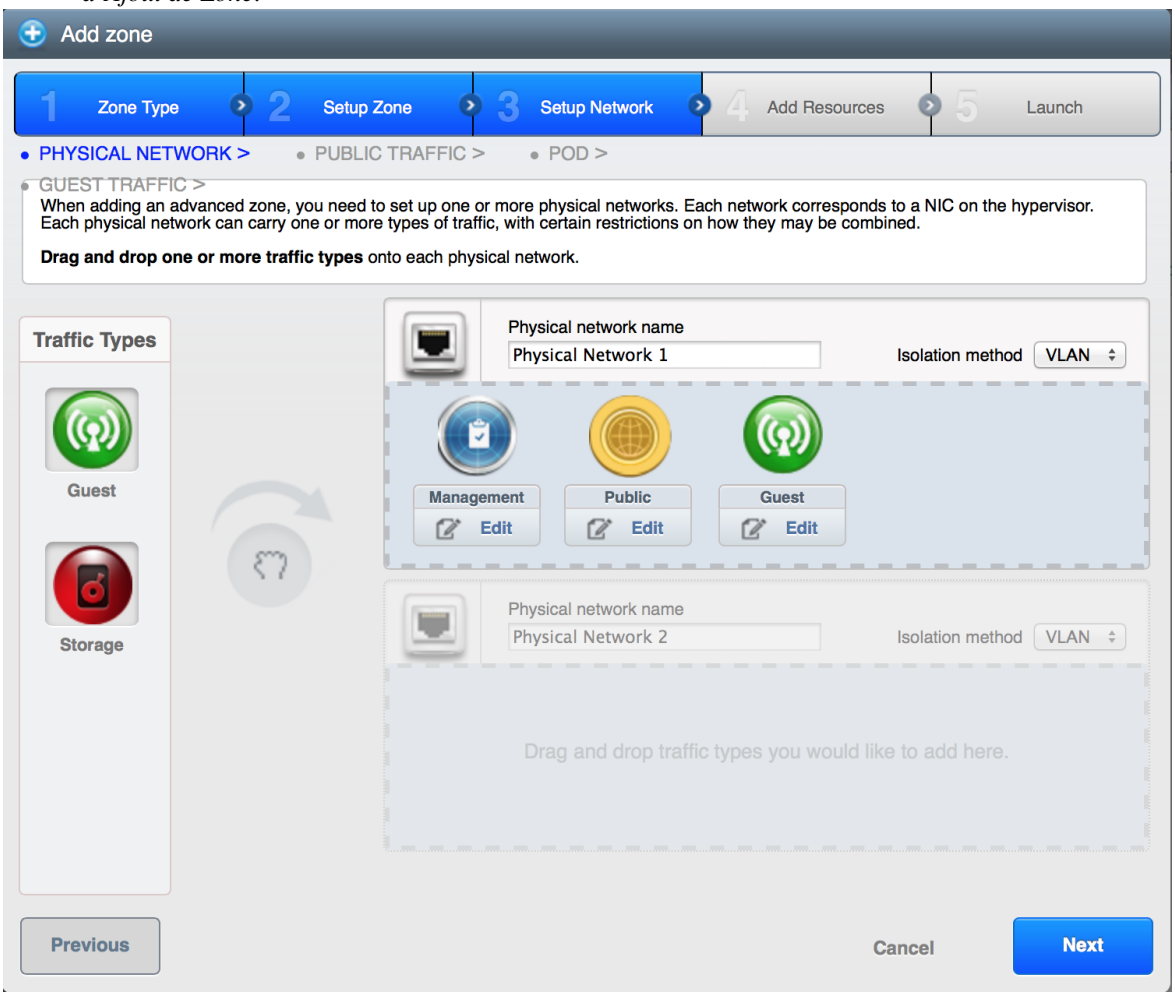
   Sur *host2 (kvm2)*

```
kvm2 ~$ vconfig add eth0 64
kvm2 ~$ ifconfig eth0.64 1.2.3.5 netmask 255.255.255.0 up
kvm2 ~$ ping 1.2.3.4
```

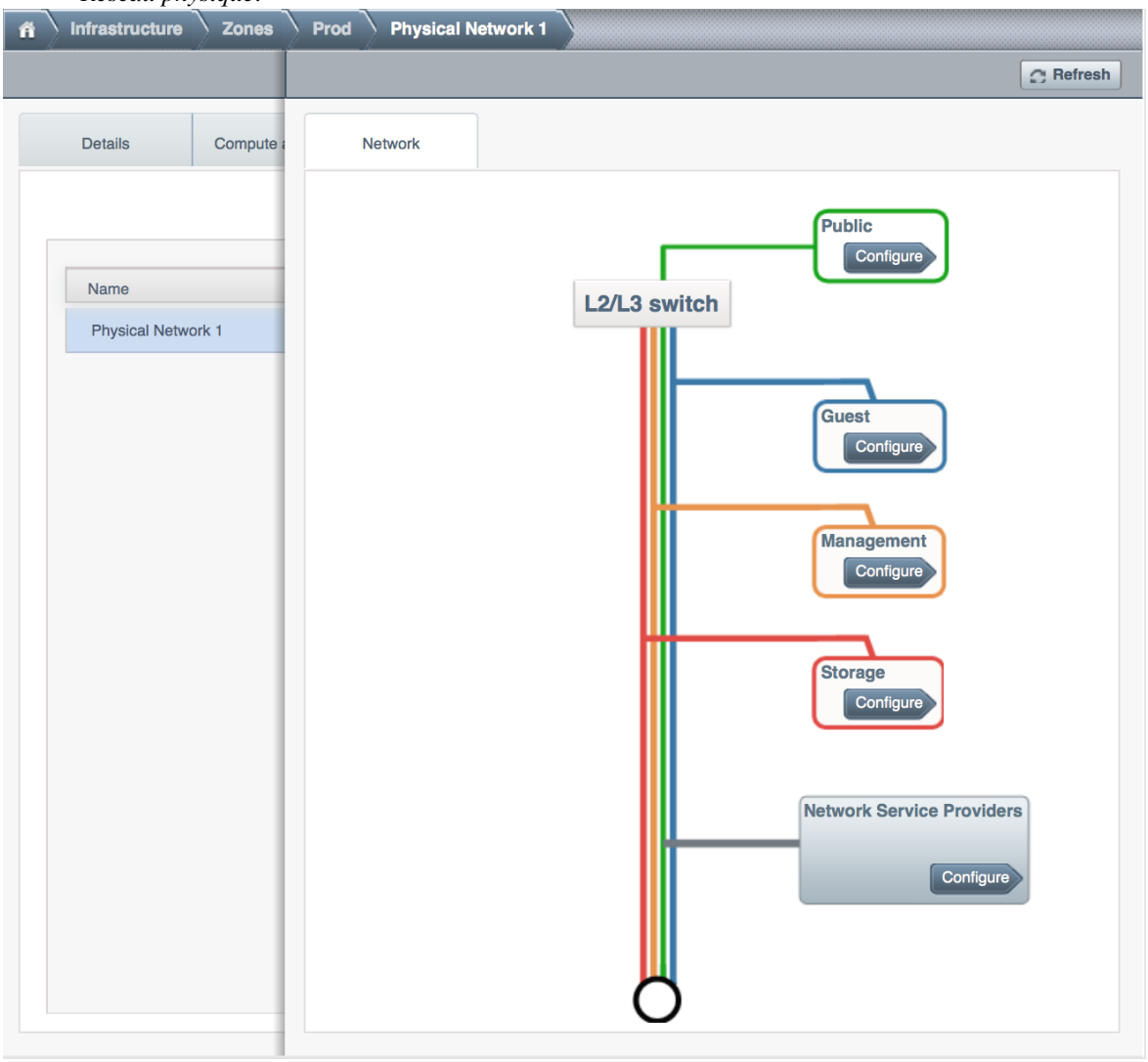
   Si les pings ne fonctionne pas, utiliser *tcpdump(8)* un peu partout pour vérifier qui absorbe les paquets. En définitive, si les commutateurs ne sont pas configurés correctement, le réseau CloudStack ne fonctionnera pas alors corriger les pannes réseaux physiques avant de poursuivre avec les étapes suivantes

2. S'assurer que les Labels Trafics sont renseignés pour cette Zone.

   Les labels de trafic doivent être renseignés sur tous les hyperviseurs incluant les types XenServer, KVM et VMware. Vous pouvez configurer les labels de trafic quand vous créez une nouvelle zone depuis l'*Assistant d'Ajout de Zone*.



Sur une zone existante, vous pouvez modifier les labels de trafic en allant sur l'onglet *Infrastructure, Zones, Réseau physique*.



Lister les labels en utilisant *CloudMonkey*

```
acs-manager ~$ cloudmonkey list traffictypes physicalnetworkid=41cb7ff6-8eb2-4630-b577-1da25e0e
count = 4
traffictype:
id = cd0915fe-a660-4a82-9df7-34aebf90003e
kvmnetworklabel = cloudbr0
physicalnetworkid = 41cb7ff6-8eb2-4630-b577-1da25e0e1145
traffictype = Guest
xennetworklabel = MGMT
=============================================================
id = f5524b8f-6605-41e4-a982-81a356b2a196
kvmnetworklabel = cloudbr0
physicalnetworkid = 41cb7ff6-8eb2-4630-b577-1da25e0e1145
traffictype = Management
xennetworklabel = MGMT
=============================================================
id = 266bad0e-7b68-4242-b3ad-f59739346cfd
kvmnetworklabel = cloudbr0
```

```
physicalnetworkid = 41cb7ff6-8eb2-4630-b577-1da25e0e1145
traffictype = Public
xennetworklabel = MGMT
==========================================================
id = a2baad4f-7ce7-45a8-9caf-a0b9240adf04
kvmnetworklabel = cloudbr0
physicalnetworkid = 41cb7ff6-8eb2-4630-b577-1da25e0e1145
traffictype = Storage
xennetworklabel = MGMT
==========================================================
```

3. Les labels de trafic KVM nécessitent d'être nommés comme *"cloudbr0"*, *"cloudbr2"*, *"cloudbrN"* etc et le pont correspondant doit exister sur les hôtes KVM. Si vous créez des labels/ponts avec n'importe quel autre nom, CloudStack (au moins les versions anciennes le font) semble les ignorer. CloudStack ne crée pas les ponts physiques sur les hôtes KVM, vous devez les créer **avant** d'ajouter l'hôte dans CloudStack.

```
kvm1 ~$ ifconfig cloudbr0
cloudbr0  Link encap:Ethernet  HWaddr 00:0C:29:EF:7D:78
   inet addr:192.168.44.22  Bcast:192.168.44.255  Mask:255.255.255.0
   inet6 addr: fe80::20c:29ff:feef:7d78/64 Scope:Link
   UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
   RX packets:92435 errors:0 dropped:0 overruns:0 frame:0
   TX packets:50596 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:0
   RX bytes:94985932 (90.5 MiB)  TX bytes:61635793 (58.7 MiB)
```

4. L'interface publique du Routeur Virtuel, de la SSVM et de la CPVM doivent être attachées à l'interface physique sur l'hôte. Dans l'exemple ci-dessous, *cloudbr0* est l'interface publique et CloudStack a correctement crée le pont des interfaces virtuelles. L'attachement de l'interface virtuelle à l'interface physique est automatiquement effectuée par CloudStack, en s'appuyant sur le paramètre de label du trafic pour la zone. Si vous avez fourni les paramètres correctes et que vous n'avez toujours pas de connexion Internet, vérifier la couche réseau avant de débugger plus loin. Vous pouvez vérifier le trafic en utilisant tcpdump sur les interfaces virtuelles, les interfaces physiques et les ponts.

```
kvm-host1 ~$ brctl show
bridge name  bridge id           STP enabled interfaces
breth0-64    8000.000c29ef7d78   no          eth0.64
                                             vnet2
cloud0       8000.fe00a9fe0219   no          vnet0
cloudbr0     8000.000c29ef7d78   no          eth0
                                             vnet1
                                             vnet3
virbr0       8000.5254008e321a   yes         virbr0-nic
```

```
xenserver1 ~$ brctl show
bridge name  bridge id           STP enabled interfaces
xapi0    0000.e2b76d0a1149       no          vif1.0
xenbr0   0000.000c299b54dc       no          eth0
                                            xapi1
                                            vif1.1
                                            vif1.2
```

5. Pré-créer les labels sur les hôtes XenServer. Similaire à la configuration du pont KVM, les labels de trafics doivent aussi être pré-créés sur les hôtes XenServer avant de les ajouter à CloudStack.

```
xenserver1 ~$ xe network-list
uuid ( RO)                : aaa-bbb-ccc-ddd
          name-label ( RW): MGMT
```

```
        name-description ( RW):
                  bridge ( RO): xenbr0
```

6. Internet devrait être accessible depuis à la fois les instances SSVM et CPVM par défaut. Leurs IP publiques seront également directement pingable depuis Internet. Merci de prendre note que ces tests ne fonctionneront que si vos commutateurs et les labels de trafic sont correctement configurés dans votre environnement. Si vos SSVM/CPVM ne peuvent pas joindre Internet, il y a peu de chance que le Routeur Virtuel puisse également le faire, ce qui indique un problème de commutateur ou de labels de trafic mal attribués. Fixer les problèmes SSVM/CPVM avant de débugger les problèmes de VR.

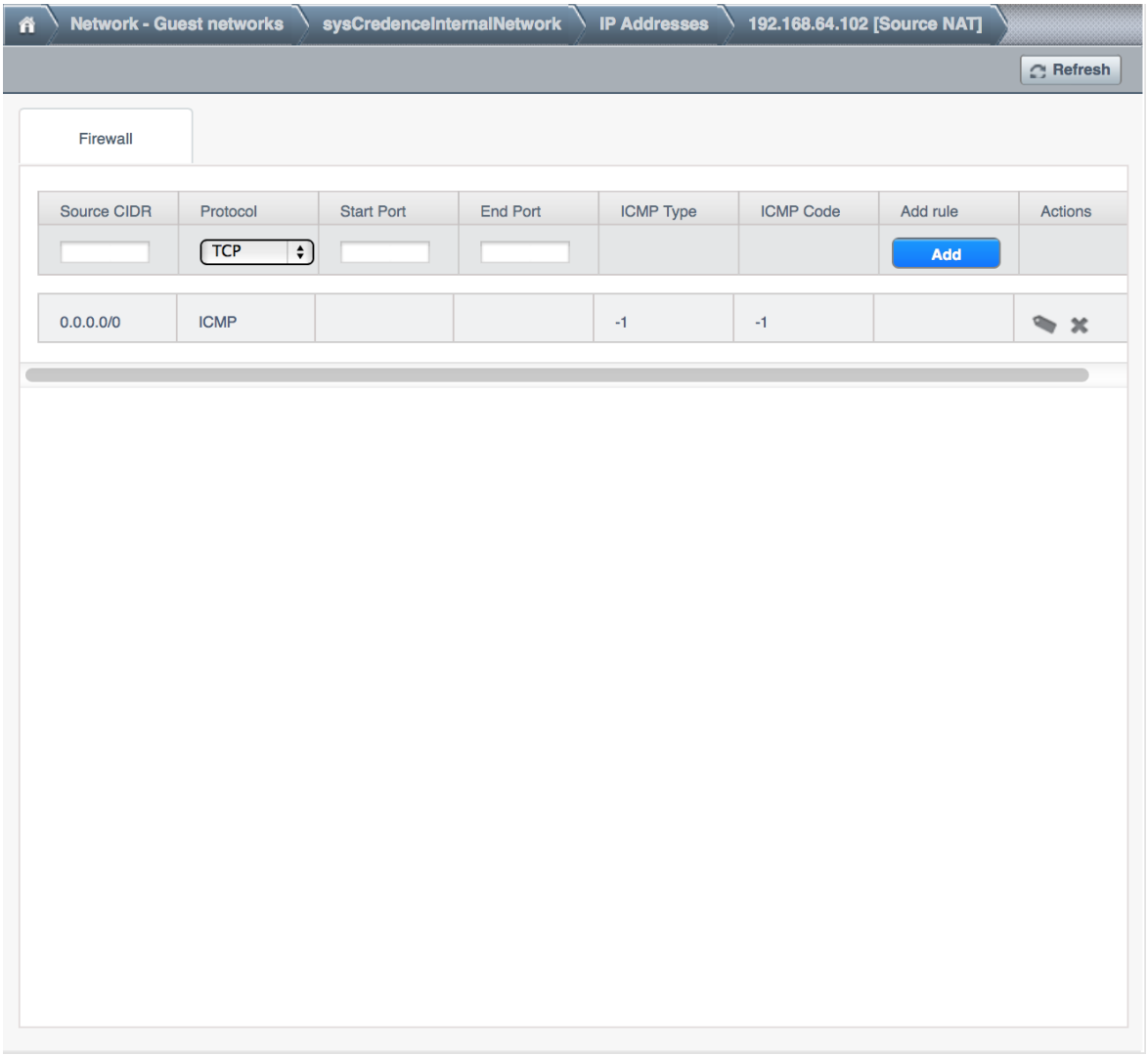
```
root@s-1-VM:~# ping -c 3 google.com
PING google.com (74.125.236.164): 56 data bytes
64 bytes from 74.125.236.164: icmp_seq=0 ttl=55 time=26.932 ms
64 bytes from 74.125.236.164: icmp_seq=1 ttl=55 time=29.156 ms
64 bytes from 74.125.236.164: icmp_seq=2 ttl=55 time=25.000 ms
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 25.000/27.029/29.156/1.698 ms
```

```
root@v-2-VM:~# ping -c 3 google.com
PING google.com (74.125.236.164): 56 data bytes
64 bytes from 74.125.236.164: icmp_seq=0 ttl=55 time=32.125 ms
64 bytes from 74.125.236.164: icmp_seq=1 ttl=55 time=26.324 ms
64 bytes from 74.125.236.164: icmp_seq=2 ttl=55 time=37.001 ms
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 26.324/31.817/37.001/4.364 ms
```

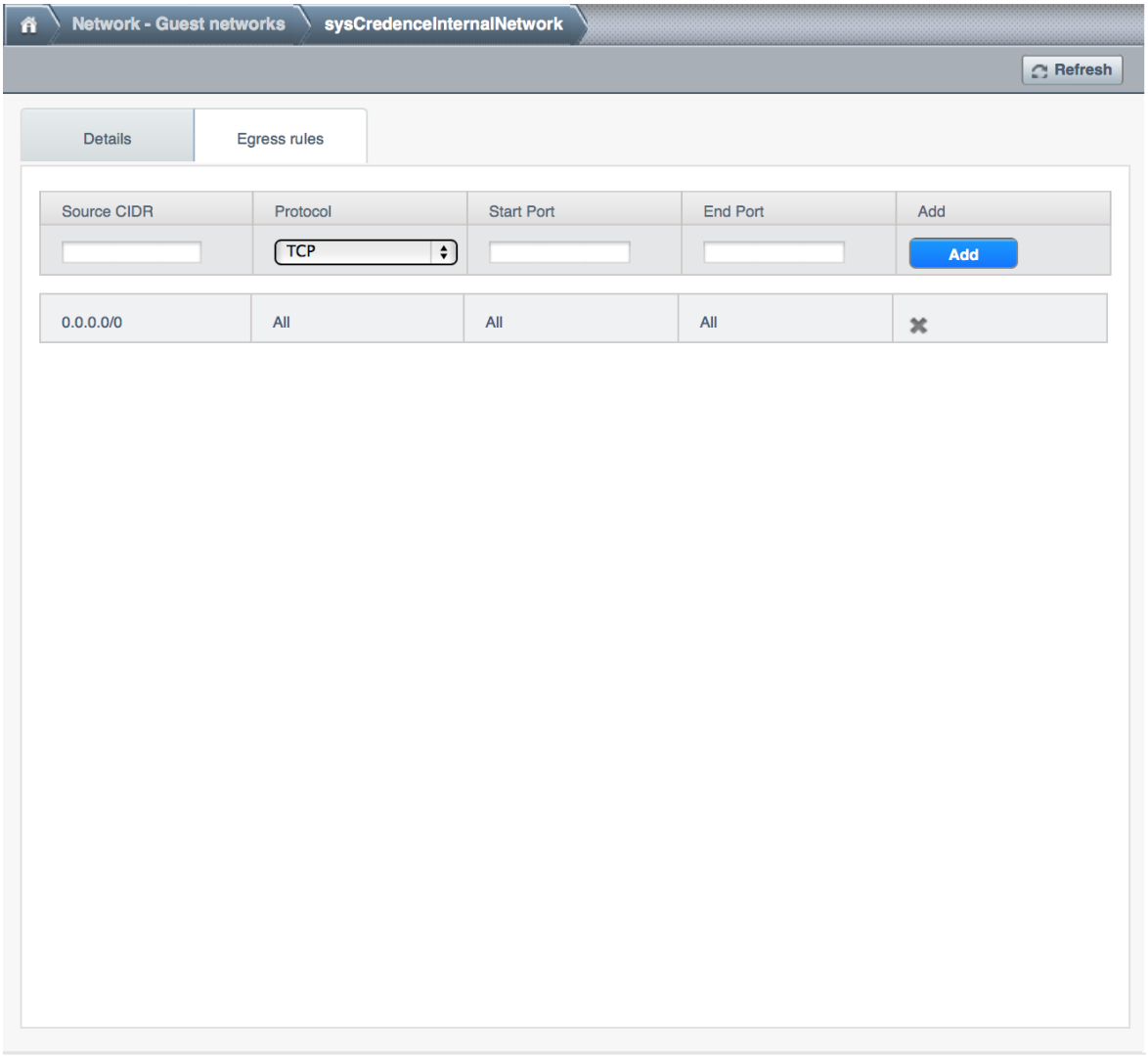
7. Le routeur virtuel (VR) devrait aussi être capable d'atteindre Internet sans avoir des règles Egress. Les règles Egress contrôlent seulement le trafic transféré et pas le trafic qui provient du VR lui-même.

```
root@r-4-VM:~# ping -c 3 google.com
PING google.com (74.125.236.164): 56 data bytes
64 bytes from 74.125.236.164: icmp_seq=0 ttl=55 time=28.098 ms
64 bytes from 74.125.236.164: icmp_seq=1 ttl=55 time=34.785 ms
64 bytes from 74.125.236.164: icmp_seq=2 ttl=55 time=69.179 ms
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 28.098/44.021/69.179/17.998 ms
```

8. Toutefois, les adresses IP publique de Source NAT du Routeur Virtuel (VR) **ne seront pas** accessible tant que les règles entrantes ne sont pas en place. Vous pouvez ajouter les règles *Ingress* sous la page de configuration *Réseau, Réseau Invité, Adresse IP, Parefeu*.



9. Les instances de VM ne peuvent pas accéder par défaut à Internet. Ajouter les règles Egress pour permettre le trafic.



10. Certains utilisateurs ont rapportés qu'en réinitialisant les règles IPTables (ou en changeant les routes) sur la SSVM, CPVM ou sur le Routeur Virtuel font fonctionner internet. Ce n'est pas un comportement normal et cela suggère que vos paramètres réseaux sont incorrectes. Aucun changement de règles IPTables ou de route ne sont nécessaires sur la SSVM, CPVM ou le VR. Revenir et refaire une vérification de tous vos paramètres.

Dans une grande majorité des cas, le problème s'est avéré être un problème de commutateur où la couche 3 des commutateurs était incorrectement configurée.

Cette section est une contribution de Shanker Balan et a été publié à l'origine sur le Blog Shapeblue