Version 2.0
January 2012

AT&T CLOUD SERVICES

AT&T Synaptic Compute as a Service^{SM}: How to Get Started

Notice

This document is not an offer, commitment, representation or warranty by AT&T and is subject to change.

The information contained in this document should not be duplicated, transmitted, or disclosed, in whole or in part without the expressed written consent of AT&T. Information in this document is subject to change without notice. AT&T assumes no responsibility for any errors or omissions in this document. Use of this document and the information is pursuant to the terms and conditions of your service agreement with AT&T.

Windows and Internet Explorer are registered trademarks of the Microsoft group of companies.

Firefox® is trademark of Mozilla® Community

Safari®, iPhone®, and iPod Touch®, are trademarks of the Apple Corporation.

Chrome® and Android® are trademarks of Google, Inc.

BlackBerry® is a trademark of Research In Motion (RIM)

Table of Contents

Overview

AT&T Synaptic Compute as a Service offers on-demand virtual machines and associated networking resources in a self-service, pay-as-you-go model. With AT&T Synaptic Compute as a Service you can provision, run, manage, and remove virtual assets as needed.

Key features available via the simple, intuitive browser interface and/or the VMware vCloud API include the following:

- Creation of **virtual data centers (VDCs)**, each with its own VLAN and IP address space
- Connection to VDC using Internet or an AT&T VPN ServiceAbility to create up to 100 **virtual machines** per VDC, and group those virtual machines into **virtual applications**
- Choice from a menu of **operating system images** available in our public catalog
- Flexible **resource sizing** options for processing power, memory and storage
- A user-configurable **firewall policy** for Internet-accessible VDCs
- Optional **load balancing** to distribute traffic among your virtual machines

For more information about AT&T Synaptic Compute as a Service, please refer to the following links:

- AT&T Cloud Services Website & Portal
- AT&T Enterprise Services Website
- AT&T Enterprise Hosting Service Guide

Planning Your Compute Environment

After you have ordered and gained access to AT&T Synaptic Compute as a Service, you are ready to begin building your compute environment. A high-level view of the steps that users often take is provided below:

1. **Plan your environment.** Before creating anything in AT&T Synaptic Compute as a Service, it's always a good idea to have a plan. This typically involves defining your application's technical requirements and then mapping those requirements to the basic building blocks available in AT&T Synaptic Compute as a Service, such as virtual data centers (VDCs), virtual applications (vApps), virtual machines, firewall rules and load balancer policies. You may wish to sketch a rough design to help you get started, and then fill in details as they become more known while building your environment (such as IP addresses).

2. **Create a VDC.** The first step in building your compute environment is to create a VDC. In the portal you have the option to create one or more VDCs; each of which includes a virtual LAN (VLAN) with contiguous public IP address space, an internet-facing firewall policy and (optionally) a load balancing policy. If you are using AT&T VPN service, AT&T will create the VDC on your behalf and it'll be ready for you in the portal.

3. **Create a vApp.** In the portal you have the option to create one or more virtual applications (vApps) within each VDC. A vApp additionally segregates virtual machine groups within a VDC (for example, within one VDC you might have a grouping of web VMs separate from a grouping of database VMs).

4. **Create virtual machines (VMs).** After creating the VDC and the vApp, you can create virtual machines using images available in the AT&T-provided public catalog of OS images.

   As you create each virtual machine, the IP address will be dynamically allocated from the IP subnet associated with that VDC.

5. **Modify the Internet-facing firewall policy.** The default firewall policy for Internet-accessible VDCs has a few standard ports open, including HTTP, HTTPS, RDP, SSH and SCP. If you need to change or delete these rules (or open other ports) you'll have to modify the firewall policy. Additionally, you might want to define firewall policies for FTP (port 21), ISS, and other services the Operating System will supply.

   Note: VDCs accessed by AT&T VPN service do not include an Internet-facing firewall policy.

6. **Administer your virtual machines.** Once you have created one or more virtual machines, use standard, off-the-shelf server administration tools such as Remote Desktop Protocol (RDP) or Secure Shell (SSH) to gain access and begin remote administration of your virtual servers. You may choose to install application software and utilities, such as monitoring or data backup agents. Additionally, you'll need to enter the appropriate license keys to activate your operating system and other software running on the machine.

7. **Create one or more load balancer policies** (optional). If you selected load balancing as an option when first creating your VDC, you can later update the load balancing policy to distribute traffic to multiple virtual machines in the VDC. Each load balancer policy will be associated with a virtual IP address.

Refer to the Glossary for additional information about VDCs, vApps, virtual machine resources, load balancing, and other parameters.

The sections that follow provide step-by-step instructions on how to manage your AT&T Synaptic Compute as a Service environment via the AT&T Cloud Services Portal.

Service Management

The Service Management section of the portal is a key area providing the tools you need to manage your AT&T Synaptic Compute as a Service environment, including these major functions:

- Create a new VDC
- Create a new vApp
- Create and configure your virtual machines
- Manage and modify your virtual machines
- View your VDCs
- View frequent requests
- View recent activity

After you have logged in, click the **Service Management** link under the My Account menu to access this area of the AT&T Cloud Services Portal.

CREATE A VDC

From the main Service Management page, follow the steps below to create your first virtual datacenter (VDC):

1. Click **Service Management** under the My Account menu.
2. Click **VDCs**.
3. Click **+Add VDC**.
4. Use the form to specify details, and then click **Create** in the bottom right-hand corner of the form.
    a. Plan your virtual environment to meet your needs. Enter the expected number of VMs within the VDC (for example, 10 VMs for a typical web application environment) and decide now whether you might need load balancing to manage traffic to the VMs.

THE VDC CREATION FORM

The VDC creation form has crucial fields and options:

- **Name.** Specify a name, up to 30 characters, for your virtual datacenter.

- **Description**. Specify a description, up to 250 characters.

- **Expected Number of VMs**. Enter the expected number of VMs within the VDC (for example, 10 VMs for a typical web application environment). Each VDC has a maximum of 120 VMs.

- **Load Balancer.** Decide now whether you might need load balancing to manage traffic to the VMs. If you are unsure, go ahead and check **Yes**. Load balancing cannot be added later.

After you click **Create** at the bottom of the form, the form will close and you'll be returned to the VDC section of the Service Management area; you should see a "Successfully created" message at the top of the screen.

CREATE A VAPP

From the main Service Management page, follow the steps below to create a virtual application (vApp) within a VDC:

1. Click **Service Management** under the My Account menu.

2. Click the **vApps** tab, then choose the VDC in which to create the vApp.

3. Click **+Add vApp** on the upper right side of the page.

4. Use the form to specify details for your vApp, and then click **Create** in the bottom right-hand corner of the form.

    a. Plan your virtual environment to meet your needs. Each vApp groups together virtual machines (VMs) within your VDC. Consider separate vApps for each grouping of VMs (e.g., one vApp for web application VMs and one vApp for database VMs).

THE VAPP CREATION FORM

The vApp creation form has crucial fields and options:

- **Name.** Specify a name, up to 30 characters, for your virtual application.

- **Description**. Specify a description, up to 250 characters.

- **Create from Template** or **Create New.** Select **Create from Template** to choose an OS template with which to create the first VM in your vApp; select **Create New** to create a blank vApp (you can later select individual templates from which to create VMs within the vApp).

After you click **Create** at the bottom of the form, the form will close and you'll be returned to the vApp section of the Service Management area; you should see a "Successfully created" message at the top of the screen.

CREATE A VM

From the main Service Management page, follow the steps below to create a virtual machine (VM) within a virtual application (vApp) within a VDC:

1. Click **Service Management** under the My Account menu.

2. Click the **VM** tab, then choose the VDC and vApp in which to create the VM.

3. Click **+Add VM** on the upper right side of the page.

4. Use the form to specify details for your VM, and then click **Create** in the bottom right-hand corner of the form.

    a. Plan your virtual environment to meet your needs. Create unique VM names within the same parent VDC, even if the VMs reside in separate vApps.

THE VM CREATION FORM

The VM creation form has crucial fields and options:

- **Name.** Specify a name, up to 30 characters, for your virtual machine.

- **Computer (Host Name):** Specify a host name, up to 30 characers, for your VM.

- **Description**. Specify a description, up to 250 characters.

- **Password.** Specify an appropriate, secure password for your virtual machine. Please use the correct password creation rules for the desired OS.

- **Select VM Template.** Select a template with which to create the VM.

After you click **Create** at the bottom of the form, the form will close and you'll be returned to the home section of the Service Management area. To view the recently created VM, click the VMs tab and choose the desired VDC and vApp.

MODIFY SERVER RESOURCES

During the creation of each virtual machine, you specify the resources (CPU, memory and storage) allocated. You can subsequently change these values.

Note: Be careful to choose only as much storage as you need for your virtual machine at any given time. Currently the virtual machine storage allocation can be increased, but it cannot be decreased.

To modify the CPU, memory or storage allocated to a specific virtual machine, follow these steps:

1. Click **Service Management** under the My Account menu

2. Click the **VM** tab, then choose the VDC and vApp in which the VM resides.

3. Click the **Actions** dropdown next to the VM to be updated, and then choose **Update**.

    a. Note: if necessary, first choose **Power Off** to power off the VM. A VM must be powered off to modify its resources.

4. Use the form to specify details for your VM, and then click **Submit** in the bottom right-hand corner of the form.

    a. As of this release you cannot *reduce* storage allocated to a virtual machine.

CLONE VIRTUAL MACHINE

You have the ability to create a copy ("clone") of a virtual machine (VM). Cloning reduces the time required to install and configure the operating system and applications. With clones you can conveniently make complete copies of a virtual machine, without browsing a host file system or worrying if you have located all the configuration files. To clone a virtual machine, follow these steps:

1. Click **Service Management** under the My Account menu

2. Click the **VM** tab, then choose the VDC and vApp in which the VM resides.

3. Click the **Actions** dropdown next to the VM to be updated, and then choose **Clone**.

    a. Note: if necessary, first choose **Power Off** to power off the VM. A VM must be powered off to clone it.

4. Use the form to specify details for your new VM, and then click **Submit** in the bottom right-hand corner of the form.

    a. Note: the cloned (target) VM does not have to reside in the same vApp or even VDC as the original (source) VM. If you choose a different VDC for the cloned (target) VM, it will have an IP address in a different subnet/VLAN.

RESET VIRTUAL MACHINE PASSWORD

When creating each virtual machine, you specify the root (for Linux) or Administrator (for Windows) password. You will need this password to remotely log in your virtual machine for server administration, so keep that password in a secure place for future reference.

To reset the password for a virtual machine, follow these steps:

1. Click **Service Management** under the My Account menu

2. Click the **VM** tab, then choose the VDC and vApp in which the VM resides.

3. Click the **Actions** dropdown next to the VM to be updated, and then choose **Reset Password**.

    a. Note: if necessary, first choose **Power Off** to power off the VM. A VM must be powered off to reset its password.

4. Use the form to specify details for your VM, and then click **Submit** in the bottom right-hand corner of the form.

CREATE LOAD BALANCING POLICY

You are able to add one or more virtual machines (VMs) to the load balancing policies only if you selected the load balancing option when you originally created your VDC.

Each load balancer policy is mapped to a virtual IP address, which your application uses as the target IP address. The load balancer distributes traffic in a round-robin fashion to the virtual machines that you designate.

To configure a load balancer policy, follow these steps after you have installed and configured a web server (e.g., Apache or Microsoft IIS) on your virtual machine:

1. Click **Service Management** under the My Account menu

2. Click **VDCs**

3. Select the **Actions** drop-down next to the VDC for which you want to update the load balancing policy

4. Click **Create Load Balancing Policy**

5. Complete the fields in the dialog box, then click **Create**

Note: If Create Load Balancing Policy is greyed out and cannot be selected, the VDC was created without a load balancer resource. The only solution is to recreate the VDC with the load balancing option.

THE LOAD BALANCING POLICY CREATION FORM

The load balancing policy creation form has crucial fields and options:

- **Policy Name.** Specify a name, up to 30 characters, for your load balancing policy.

- **Protocols:** Choose the appropriate protocol (TCP, UDP, HTTP or HTTPS) for your web servers.

- **Virtual Port**. Specify the port on which the web servers listen. This should correspond to the protocol chosen.

- **Sticky.** Specify whether to enable session persistence to track and store session data, such as the specific pool member that serviced a client request. This will ensure that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.

- **Health Check Protocol.** Select the protocol for the health check.

- **Health Check Interval.** Enter the number of seconds (between 3-6) for the health check interval.

- **Load Balanced VMs.** Enter the individual IP address and port number of each VM; press **Add** after entering each one.

    - To find the IP address of a VM, click **Details** next to the VM name listed on the VMs section of the Service Management area.

    - Be sure that you enter the same port number as entered in **Virtual Port**, and that the web server application on the VM is configured to listen on that port.

- **Description.** Specify a description, up to 250 characters.

After you click **Create** at the bottom of the form, the form will close and you'll be returned to the VDCs section of the Service Management area; you should see a "Successfully created" message at the top of the screen.

UPDATE LOAD BALANCING POLICY

To update a load balancer policy, follow these steps after you have initially created the load balancing policy:

1. Click **Service Management** under the My Account menu

2. Click **VDCs.**

3. Select the **Actions** drop-down next to the VDC for which you want to update the load balancing policy.

4. Click **Edit Load Balancing Policy**, then click **Edit.**

5. Complete the fields in the dialog box, then click **Submit.**

Note: If Edit Load Balancing Policy is greyed out and cannot be selected, you must first create a load balancing policy; see above.

REMOVE LOAD BALANCER

To remove a load balancer policy, follow these steps:

1. Click **Service Management** under the My Account menu

2. Click **VDCs.**

3. Select the **Actions** drop-down next to the VDC for which you want to update the load balancing policy.

4. Click **Edit Load Balancing Policy**, then click **Delete**. Click **Yes** to confirm deletion.

MODIFY FIREWALL POLICY

A default Internet-facing firewall policy is automatically created for each Internet-accessible VDC; an Internet-facing firewall policy is not provided for VDCs connected via AT&T VPN service.

To modify the Internet-facing firewall policy (add, edit or remove rules), follow these steps:

1. Click **Service Management** under the My Account menu.

2. Click **VDCs.**

3. Select the **Actions** drop-down next to the VDC for which you want to update firewall policy.

4. Click **Edit Firewall**.

5. Click **Modify Firewall Policy**.

6. Use the portal to add, edit, or remove rules as needed.

Note: The operating system firewall running in each virtual machine is on by default. Typically, you must configure these firewalls on the virtual machine:

- You can control the firewall from Red Hat® Enterprise Linux® by editing /etc/sysconfig/iptables and then restarting the service (# service iptables restart).

- On Microsoft® Windows Server® 2008, use the Windows Firewall with Advanced Security under the Administrative Tools to manage the local firewall rules.

As of this release you can*not* remove the Internet-facing firewall policy associated with each VDC; however, you *can* edit the firewall policy (add or remove rules) as desired.

Administering Your Virtual Machines

When creating each virtual machine, you specify the root (for Linux) or Administrator (for Windows) password. You will need this password to remotely log in your virtual machine for server administration, so keep that password in a secure place for future reference. If needed, you can reset the password for each virtual machine.

REMOTE CONNECTION

To remotely access the virtual machine, you initially use Remote Desktop Protocol (RDP) or Secure Shell (SSH) — commonly used tools for PC-to-server remote access. Most PCs with a Microsoft Windows operating system will include the Microsoft Remote Desktop Connection client.

A typical menu path in Microsoft Windows:

Start > All Programs > Accessories > Communications > Remote Desktop Connection

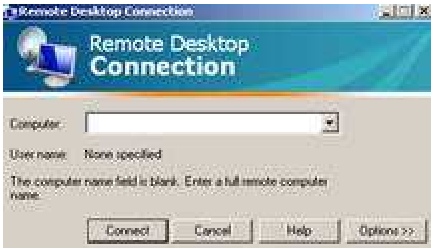
If the Microsoft Remote Desktop Connection client software is not already installed on your PC, it is available as a free download from the Microsoft website. Additionally, other RDP tools are available from other software providers.

To use the Remote Desktop Connection client:

1. Input the destination IP of the virtual machine and click Connect.

2. Input your administrator/root password when prompted.

3. The first time you log into the virtual machine you will be prompted to change the password.



Computer:

User name: None specified

The computer name field is blank. Enter a full remote computer name.

For enhanced security, you can establish a Secure Copy (SCP) tunnel within RDP known as WinSCP, using third-party SCP tools. SCP tools allow you to open a secure session with Windows and encrypt files/transfers of data by creating user names, passwords and ports. However, this can accomplished only after logging into the virtual machine for the first time, and loading SCP client software onto both the virtual machine and your PC to create the tunnel.

Secure Shell (SSH) can also be used and may already exist on PCs with UNIX based or Linux desktop operating systems such as Ubuntu. To use SSH from a Mac or Windows based PC, you typically install SSH client software.

SERVER ADMINISTRATION

After you have logged into the virtual machine via a client-to-server tunnel, you can upload, copy data and applications just as you would remotely for physical or virtual servers hosted in your own data center.

In addition to the software packages you are installing as part of your application, you may also want to set up various tools and utilities such as the following:

- Performance/health monitoring agents
- Anti-virus software
- Patch update tools
- Data backup software
- Directory services

If you are creating numerous virtual servers with an identical or similar software configuration, consider creating an *auxiliary* virtual machine to act as a file server or group policy server internal to your VDC. There are no portal features to specifically set up either of these two server types, but you could, for example, build a Linux VM and enable Network File System (NFS) on it, then use it as a file server.

You may also need to configure firewalls at your location to allow remote user access out of the corporate network.

Images, Patches, and Software Licensing

When you create virtual machines in AT&T Synaptic Compute as a Service, the Portal Service Management section provides a list from the Public Image Library from which you can choose an image.

An image is a template of the Operating System that will run on the Virtual Machine. When setting up the Virtual Machines, you choose the desired OS and it will load when the VM starts.

As for the application of security patches, AT&T Synaptic Compute as a Service as of this release, is an unmanaged Infrastructure-as-a-Service-offering — anything above the virtualization layer (in this case the Operating System and above) is the customer's responsibility.

AT&T manages and maintains public images with updated versioning & patch levels as well as basic hardening. However, once a VM is deployed for a customer and the customer takes positive ownership of that VM, everything to do with patching, hardening, and maintenance of the image becomes the customer's responsibility.

Note: Customers are required to supply licensing for these Images and Applications.

- **Red Hat Enterprise License (RHEL) - Public Image Library Descriptions**

  Users can run the following commands from the command line of their RHEL server to get access to the above-referenced applications in all of the RHEL images:

  - rpm -qa | grep httpd
  - rpm -qa | grep mysql
  - rpm -qa | grep php

  These images are fully functional for as long as necessary without licensing unless users require software updates or technical support from Red Hat. If users require one or both of the following, they must subscribe to a maintenance package directly with Red Hat and download and apply a Red Hat Enterprise Linux subscription.

  - Red Hat Enterprise Linux 5 (64-bit, standard) installed with all applications available in a Red Hat installation DVD. List of applications installed includes, but is not limited to the following:
    - Apache
    - Tomcat
    - MySQL
    - Jboss(*)
  - Red Hat Enterprise Linux 5 (32-bit, standard) installed with all applications available in a Red Hat installation DVD. List of applications installed includes, but is not limited to the following
    - Apache
    - Tomcat
    - MySQL
    - Jboss(*)

- **Microsoft Windows 2008 - Public Image Library Description.**

  Users have 60 days to activate the server with their Microsoft License Keys. A user can execute the slui.exe 3 command from a command line prompt to enter the product key and activate your license with Microsoft.

  AT&T Synaptic Compute as a Service offers three versions of Windows 2008.

  1. Windows 2008 R2
  2. Windows 2008 SP2 32bit
  3. Windows 2008 SP2 64bit

  Important Note: The software activation status does not impact the services running on the server. If software falls out of tolerance you are asked to reactivate it with license key, but services will continue to run even if not reactivated. Not activating generates persistent notifications reminding user to activate the server. Services and remote administration are not affected.

You may be able to re-activate over the internet. If activating over the internet fails, you can call the telephone number displayed on the activation screen.

For more information on activations follow the links below:

http://www.microsoft.com/windowsserver2008/en/us/WS08-product-activation.aspx

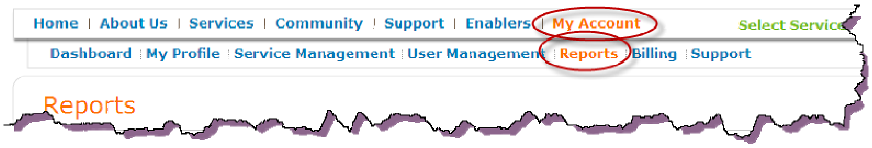
http://www.microsoft.com/windowsserver2008/en/us/R2-product-activation.aspx

Viewing Status and History

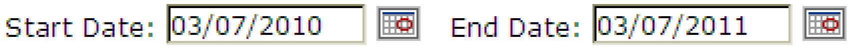
REPORTS

The Reports page allows you to view your usage of AT&T Synaptic Compute as a Service, for a specified time period.

To navigate to the Reports page:

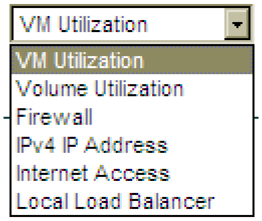

Home | About Us | Services | Community | Support | Enablers | My Account
Select Service
Dashboard | My Profile | Service Management | User Management | Reports | Billing | Support
Reports

Enter the Start Date and End Date of the time period for which you'd like to view a report.



Start Date: 03/07/2010 End Date: 03/07/2011

Choose the Report type:



Not all Report Types are available, depending upon what you have purchased. For example, certain network appliances such as firewalls and load balancers may not appear in the drop-down list-box if you have not purchased them.

Click Run Report . The resulting consumption report will be displayed in an HTML table on the page.

After the report has run, you can export the results as an excel file by clicking the Xcel icon: Run Report ☒

Note: The Consumption/Usage report is a snapshot of usage at the time that you click Run Report. Your billing invoice will show usage for the *billing period* stated on your invoice.

Where to Get Help

AT&T is focused on providing you with a superior cloud services experience. AT&T has a comprehensive approach to providing you with the support you need, when you need it. Below is a description of the support features available to you:

AT&T Cloud Services Support: The AT&T Cloud Services Support page is your central point for service and technical support: http://synaptic.att.com/clouduser/support_center.htm

Some of the most popular support resources:

- **Frequently Asked Questions**: AT&T has compiled a list of commonly asked questions. Your question may be answered here: http://synaptic.att.com/clouduser/support_faq.htm

- **Resource Library**: From API to security documentation, this comprehensive library will be updated on an ongoing basis to provide you with the latest information and support. http://synaptic.att.com/clouduser/support_resource.htm

- **Online Form**: All AT&T Synaptic Compute as a Service customers have the option to communicate with our technical support team via the online web form located here: http://synaptic.att.com/clouduser/contact_us.htm

- **Enhanced Support**: If you have subscribed to the Enhanced Support option, you will have access to a 24 x 7 x 365 toll-free phone number providing live technical support.

Glossary

VDC

A virtual data center (VDC) is a logical grouping of virtual machines into a virtual LAN (VLAN) with a contiguous IP address space. Users can independently create Internet-accessible VDCs; these VDCs use a public IPv4 subnet and include one user-configurable Internet-facing firewall policy. VDCs connected via AT&T VPN service must be configured in advance by AT&T; these VDCs can use either public or private IP addressing and do not include an Internet-facing firewall policy. When creating a VDC you must decide whether load balancing will be available.

VAPP

A virtual application (vApp) is a logical grouping of virtual machines within a VDC.

VIRTUAL MACHINE

A virtual machine is a virtualized server that you can create, start, stop, manage, and delete in a VDC. Each virtual machine consists of an operating system image along with three independently configurable resource parameters: processor, memory, and storage.

When you create a virtual machine, its IP address is automatically assigned from the available IP address space associated with the VDC. You can create virtual machines in batches of up to ten at a time.

After you create a virtual machine, you receive the administrator/root password via an email message. Then you use Remote Desktop Protocol (RDP), Secure Shell (SSH) or an equivalent method to gain access and begin remote administration of your virtual server.

VIRTUAL MACHINE IMAGE

Virtual machine images are available in AT&T's public image library for your use in creating new virtual machines. Each image consists minimally of a base operating system and may include additional software, such as web server and/or database application software. Additionally, each image has a default set of resource parameters (processor, memory, storage) recommended by AT&T; however, you can change these parameters from their default values. AT&T maintains these image templates in the public image library, but after you create a virtual machine you are then responsible for software patching, configuration or updates.

Note: AT&T does not provide activation or licensing of software included in these images. You are required to procure the appropriate software license and enter the registration key as one of the tasks associated with administering your virtual server.

VIRTUAL MACHINE PROCESSOR

When creating or modifying a virtual machine, you can allocate from one to four virtual CPUs (vCPU) in whole integer units (1 - 8). Each vCPU provides the equivalent CPU capacity of 1000 Mhz. Virtual machine processor is metered and billed per vCPU per hour, and the rate is applied upon activation of the virtual machine and in a running state. While a virtual machine is stopped, the virtual machine processor is not metered for billing. The number of vCPU allocated to the virtual machine can be increased or decreased.

VIRTUAL MACHINE MEMORY

When creating or modifying a virtual machine, you can allocate up to 64 GB of memory (RAM) in very granular, decimal units.

Virtual machine memory is metered and billed per GB per hour, and the rate is applied upon activation and power on of the virtual machine. While a virtual machine is stopped (powered off), the virtual machine memory is not metered for billing. The amount of RAM allocated to the virtual machine can be increased or decreased.

VIRTUAL MACHINE STORAGE

When creating or modifying a virtual machine, you can allocate up to 1 TB (1,024 GB) of system storage in granular, single GB units. This storage is used as the operating system partition as well as swap memory, if applicable. The lower boundary of storage depends on the virtual machine image. Currently the smallest possible amount is 10 GB for Red Hat Enterprise Linux.

VM storage is metered and billed per GB per month, calculated as a weighted average of the peak amount of storage used each hour during the month.

VM storage is metered based on the full amount allocated to the virtual machine, both when in a running state and when stopped. The storage allocation can be increased, but it cannot be decreased.

LOAD BALANCER POLICY

Local load balancing with a virtual IP address (VIP) offers the ability to spread user traffic among multiple server instances within a single VDC.

Customers may add, modify, and remove load balancing to their VDCs.

Note: Load Balancing must be chosen when the VDC is created — it cannot be added at a later date.

VIRTUAL IP ADDRESS

A virtual IP address (VIP or VIPA) is a static IP address that is not connected to a specific computer or network interface card (NIC).

Virtual IP addressing enables one IP address to be shared by multiple servers. VIPs are widely used to balance incoming traffic to multiple servers. Packets sent to the virtual IP are forwarded to the real IP address of the server designated to respond.

FIREWALL POLICY

When you create an Internet-accessible VDC, it will include a single Internet-facing firewall policy that manages all of the virtual machines created within that VDC. This firewall policy consists of one or more firewall rules, which you can configure by specifying the port and source/destination IP addresses. When you add, delete or modify firewall rules, these changes take effect automatically and immediately.

Note: VDCs connected via AT&T VPN service will not include a firewall policy.