EduCloud User Guide

Contents

[Overview 1](#_Toc484692075)

[Browser and Plug-in Requirements 1](#_Toc484692076)

[Getting Started with EduCloud 2](#_Toc484692077)

[Log Into the Web Portal 2](#_Toc484692078)

[Catalogs 4](#_Toc484692079)

[Public Catalogs 4](#_Toc484692080)

[My Organization’s Catalogs 5](#_Toc484692081)

[Creating a Catalog 5](#_Toc484692082)

[Adding a vApp to the Catalog 6](#_Toc484692083)

[Publish/Subscribe 6](#_Toc484692084)

[Upload an ISO 8](#_Toc484692085)

[Working with vApps 9](#_Toc484692086)

[Selecting Catalog Images 9](#_Toc484692087)

[Add vApp from Catalog 9](#_Toc484692088)

[Add vApp from OVF 12](#_Toc484692089)

[Build a New vApp 13](#_Toc484692090)

[Adding VMs from a Catalog 14](#_Toc484692091)

[Adding a New VM 15](#_Toc484692092)

[Working with Networks in a vApp 16](#_Toc484692093)

[Adding Networks to a vApp 16](#_Toc484692094)

[Add an Org VDC Network 16](#_Toc484692095)

[Add a vApp Network 17](#_Toc484692096)

[Configure vApp Network Services 18](#_Toc484692097)

[Working with VMs 20](#_Toc484692098)

[Mount a CD/DVD 20](#_Toc484692099)

[Mount an image from the Catalog 20](#_Toc484692100)

[Mount a local CD/DVD 20](#_Toc484692101)

[Install a Guest Operating System 21](#_Toc484692102)

[Guest OS Customization 21](#_Toc484692103)

[Forcing Guest OS Recustomization 22](#_Toc484692104)

[Resetting the Admin/Root Password 22](#_Toc484692105)

[Modify VM CPU and Memory Resources 23](#_Toc484692106)

[VM CPU and Memory Hot Add 23](#_Toc484692107)

[Add a VM Hard Disk 24](#_Toc484692108)

[VM Console 24](#_Toc484692109)

[VMware Tools/Open VM Tools 26](#_Toc484692110)

[Securing EduCloud VMs 27](#_Toc484692111)

[Agent-less vs Agent-based Protection 27](#_Toc484692112)

[Securing Windows VMs 27](#_Toc484692113)

[Windows VMs Provisioned from EduCloud Gold Master Templates 27](#_Toc484692114)

[Custom Built Windows Images 28](#_Toc484692115)

[VMware Tools Preparation 28](#_Toc484692116)

[Deep Security Notifier (Optional) 29](#_Toc484692117)

[Request for Trend Activation for Agent-less Protection for Custom Built Windows Images 30](#_Toc484692118)

[Securing Linux Systems 30](#_Toc484692119)

[Snapshots 31](#_Toc484692120)

[vApp snapshot 31](#_Toc484692121)

[VM snapshot 31](#_Toc484692122)

[Revert a Virtual Machine to a Snapshot 32](#_Toc484692123)

[Organization VDC Networks 33](#_Toc484692124)

[Create an Isolated Org VDC Network 33](#_Toc484692125)

[Create a Routed Org VDC Network 34](#_Toc484692126)

[Multiple VDCs and Shared Networks 35](#_Toc484692127)

[Configuring Edge Gateway Services 36](#_Toc484692128)

[DHCP 37](#_Toc484692129)

[Network Address Translation (NAT) 37](#_Toc484692130)

[Source NAT (SNAT) 37](#_Toc484692131)

[Destination NAT (DNAT) Rule 38](#_Toc484692132)

[Firewall Configuration 38](#_Toc484692133)

[Enable Firewall 38](#_Toc484692134)

[Add Firewall Rule 38](#_Toc484692135)

[Reorder Firewall Rules 40](#_Toc484692136)

[Load Balancer 40](#_Toc484692137)

[Add a Pool Server to an Edge Gateway 41](#_Toc484692138)

[Edit Pool Server Settings 44](#_Toc484692139)

[Delete a Pool Server 44](#_Toc484692140)

[Add a Virtual Server to an Edge Gateway 45](#_Toc484692141)

[VPN 46](#_Toc484692142)

[Intra-Organization VPN Tunnels 46](#_Toc484692143)

[Inter-Organization VPN Tunnels 48](#_Toc484692144)

[Remote Network VPN Tunnels 49](#_Toc484692145)

# 

# Overview

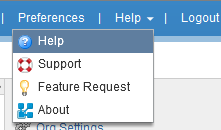
EduCloud Server is a private, higher education cloud service which allows organizations to provision and manage virtual servers at a fraction of the cost of implementing physical servers.

The self-service portal allows organization administrators and users the flexibility to deploy, redistribute, and remove server resources as needed - anytime, anywhere.

More information about the service and its costs can be found on the EduCloud Server service catalogue page at <https://www.bc.net/service-catalogue/educloud>

Please review the “*EduCloud Server: Concepts and Overview*” document first to gain an understanding of the concepts and constructs that underpin this service. It can be downloaded from the “[Support](https://www.bc.net/service-catalogue/educloud)” section of the EduCloud Server service catalogue.

This guide provides step by step instructions on how to perform many common tasks within the self-service portal, but is not a complete guide.

Full documentation for vCloud Director (the product used to implement EduCloud Server) is reachable from the web portal by selecting “Help” from the Help menu. Any vCloud documentation referenced in this document is found at this location.

For the remainder of this document, “EduCloud Server” will be abbreviated as “EduCloud”.

# Browser and Plug-in Requirements

Before you begin, review the “Frequently Asked Questions” section of the EduCloud Server service catalogue page at <https://www.bc.net/service-catalogue/educloud>.

Ensure you are using a supported browser and that supported versions of all other required software and plug-ins is installed.

Also read through the “Known Issues” section to familiarize yourself with any known issues and suggested workarounds.

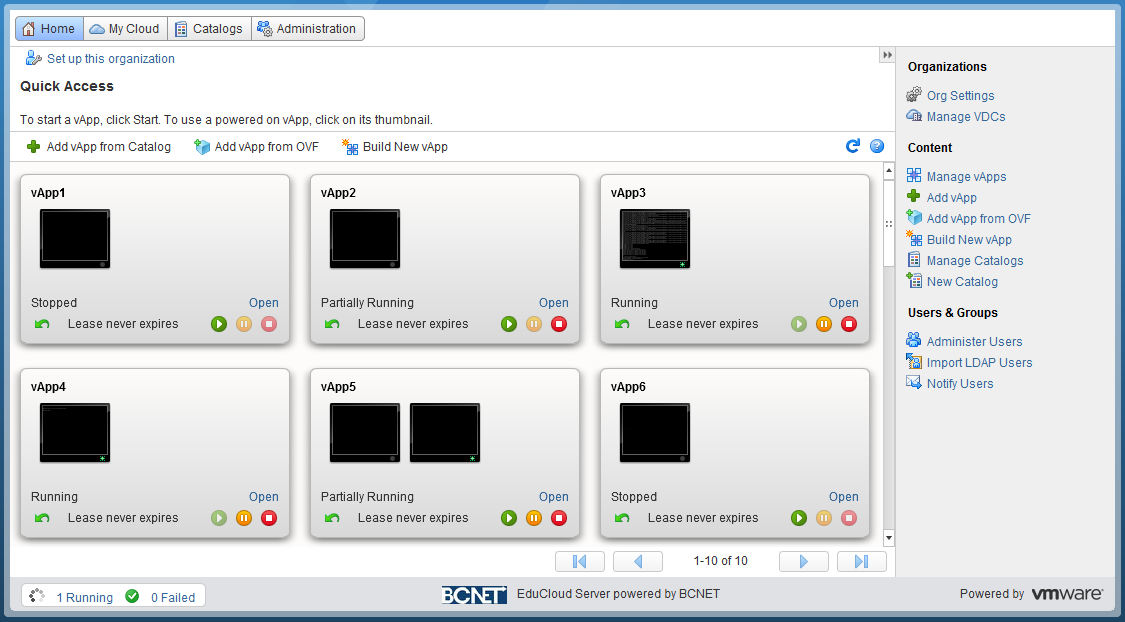
# Getting Started with EduCloud

## Log Into the Web Portal

Obtain your organization code and a user account from your organization administrator prior to logging in. If you are the organization administrator, the organization code and login account is provided to you by the EduCloud administrators when your organization is set up. If you’ve forgotten your organization code or account information please contact us at [**http://web.it.ubc.ca/forms/systems**](http://web.it.ubc.ca/forms/systems)**.**

To log into the EduCloud web portal, open a Web browser and navigate to: [https://bcnet.educloud.ubc.ca/cloud/org/**<***OrganizationCode*](https://bcnet.educloud.ubc.ca/cloud/org/%3cOrganizationCode)**>.** Enter your username and password and click **Login**.

Once you are logged into EduCloud, you will be presented with the EduCloud portal home page, similar to the screenshot below:



Top Menu:

* **Home –** quick access to vApps created within your organization.
* **MyCloud** – work with existing or create new vApps and VMs.
* **Catalogs** – browse and manage catalogs of vApp templates.
* **Administration –** change virtual datacenter properties, view available vApps and templates, set policies and create users

Quick Access Shortcuts:

* **Add vApp from Catalog** – Create a new vApp from a vApp template in a Catalog
* **Add vApp from OVF** – Create a new vApp from an OVF file.
* **Build New vApp** – Build a new vApp where you can pick and choose the VM’s you would like to have in your new vApp.

Common Tasks

* The right menu bar provides quick links to a set of frequently accessed tasks and resources.

# Catalogs

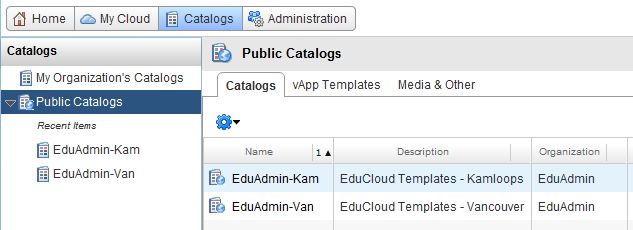
A catalog is a container for vApp templates and media files in an organization. The vApp templates can be used to deploy new vApps or VMs.

## Public Catalogs

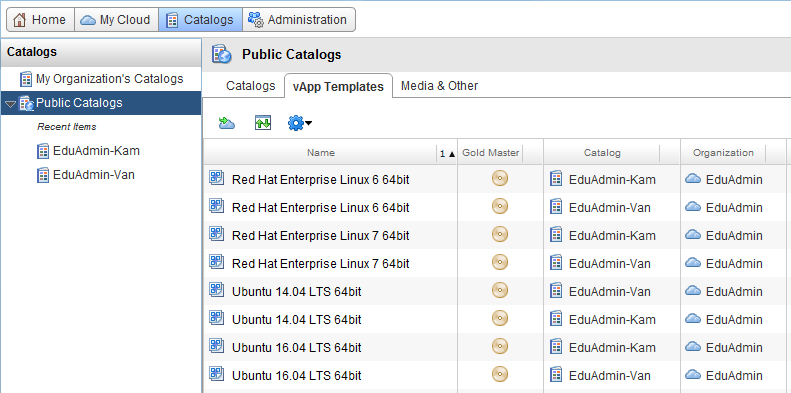
The EduCloud administrators maintain a public catalog at each EduCloud site containing templates of common operating systems.

To view a list of public catalogs:

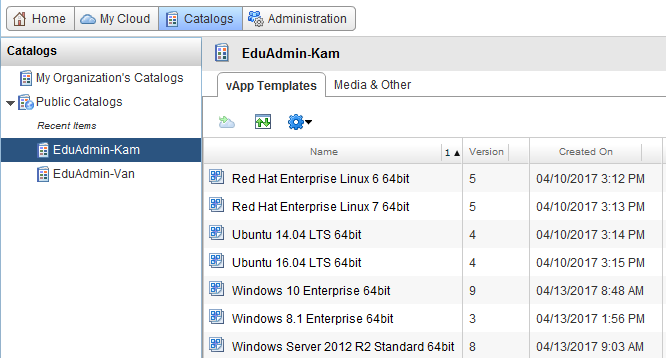
1. In the top menu, select **Catalogs**.
2. In the left pane, select **Public Catalogs.**
3. In the right pane, select the **Catalogs** tab.



To view a list of the **vApp Templates** contained in all public catalogs select the **vApp Templates** tab.



Alternatively, double click on one of the catalog names to view the list of **vApp Templates** contained only within that catalog:



## My Organization’s Catalogs

You can create your own catalogs and publish them to the users of your organization. Once you create a catalog you can add vApp templates and media (e.g. ISO images) to share with the users of your organization.

Cross-site deployment of vApps or VMs (e.g. deploying in Kamloops from a catalog located in Vancouver) is possible, but very inefficient, so we recommend you maintain a catalog at each site. There are two options:

1. Create a catalog at each site and manually maintain the catalog contents
2. Maintain a catalog at one site, and use publish/subscribe to synchronize a copy of the catalog to other sites

## Creating a Catalog

1. In the top menu select **Catalogs**.
2. In the left pane, select **My Organization’s Catalogs**.
3. In the right pane, select the **Catalogs** tab. You will see the current available default catalog(s) created for your organization.
4. To add a new catalog, click on the **Add Catalog** icon ().
5. Select a name and description for your new catalog. Click **Next**.
6. Under **Add Storage** select **Pre-provision on specific storage policy** and select a storage policy located at the site you wish the catalog to reside. You will typically want to select the lowest cost storage policy available at that site.
7. Under **Share this Catalog**, select Add Members.
8. You can choose to share the catalog with **Everyone** in the organization or **Specific users and groups.**
9. Under **Access level**, select the appropriate privileges that the users should have for the catalog. Click **Next**.
10. Review the catalog settings and click **Finish** to create the new catalog.

## Adding a vApp to the Catalog

We recommend that a vApp be fully powered off before being added to a catalog. This ensures all vApp VMs are in a consistent state while it is being added.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the **vApp** you with to add and select **Add to Catalog…**
4. Check **Overwrite catalog item** if you are updating an existing catalog item
5. Enter a name and description for the catalog item
6. The **Storage lease** option is typically set to **Never Expires**
7. The **When using this template** option is typically set to **Customize VM settings**.
8. Click OK to complete the process.

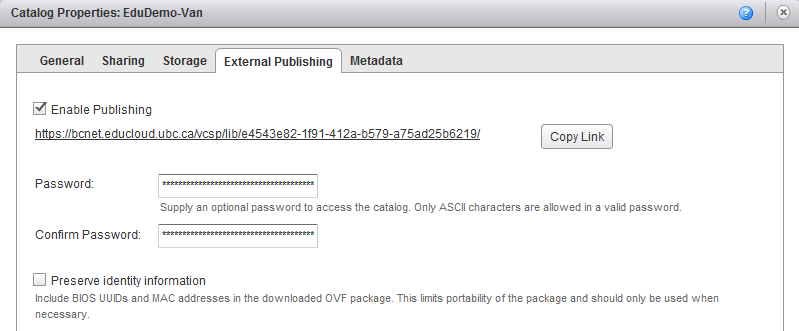
A background task is created to add the vApp to the catalog. For more information on the storage lease and vApp creation (When using this template) options, select the “?” icon while the “Add to Catalog:” dialogue box is still open.

## Publish/Subscribe

A copy of a catalog can be synchronized to other sites by using the “publish/subscribe” feature.

To publish a catalog:

1. In the top menu select **Catalogs**.
2. In the left pane, select **My Organization’s Catalogs**.
3. In the right pane, select the **Catalogs** tab.
4. Right click the catalog you wish to publish and select **Publish/Subscribe Settings…**
5. Select the **External Publishing** tab
6. Check **Enable Publishing**
7. Enter a secure password and record it
8. Press the **Copy Link** button to copy the subscription URL for use in the next step
9. Press **OK** to enable external publishing



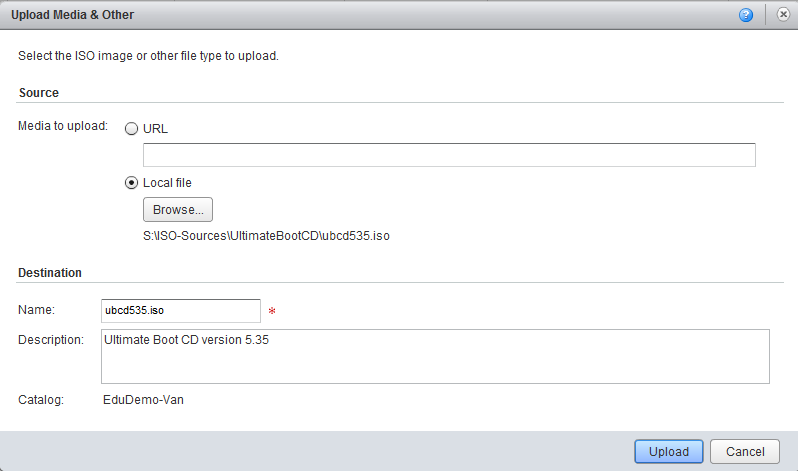
To Create a Subscribed Catalog:

1. In the top menu select **Catalogs**.
2. In the left pane, select **My Organization’s Catalogs**.
3. In the right pane, select the **Catalogs** tab.
4. Click on the **Add Catalog** icon ().
5. Enter a **Name** for the subscribed catalog.
6. Check the **Subscribe to an external catalo**g checkbox
7. Paste in the **Subscription URL** you copied when publishing the catalog
8. Enter the **Password** you assigned to the published catalog.
9. Ensure **Automatically download the content from external catalog** is checked. Click Next.
10. Under **Add Storage** select **Pre-provision on specific storage policy** and select a storage policy located at the site you wish the catalog to reside. You will typically want to select the lowest cost storage policy available at that site.
11. Under **Share this Catalog**, select **Add Members**.
12. You can choose to share the catalog with **Everyone** in the organization or **Specific users and groups**.
13. Under **Access level**, select the appropriate **privileges** that the users should have for the catalog. Click Next.
14. Review the catalog settings and click **Finish** to create the subscribed catalog.

The subscribed catalog will be created, and the contents of the published catalog will begin to synchronize to it. You can watch the status by opening the subscribed catalog and viewing the **vApp Templates** tab.

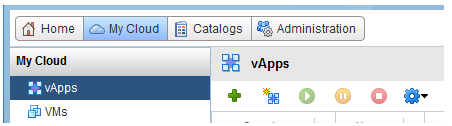
## Upload an ISO

Media frequently connected to and accessed from a VM (e.g. operating system installation ISOs), you can uploaded to and mounted from a catalog. To upload an ISO:

1. In the top menu select **Catalogs**.
2. In the left pane, select **My Organization’s Catalogs**.
3. In the right pane, select the **Catalogs** tab and right click your organizations catalog and click **Open**.
4. Select the **Media & Other** tab.
5. Click the **Upload** icon  (Drive with green up arrow on it).  
     
     
     
   Note: Java JRE 1.6.0 update 10 or later and the newest version of the vCloud Director Client Integration Plug-in must be installed to use this feature. See the service catalogue for full details regarding browser and plug-in requirements.
6. Select the URL or local file containing the media to upload and enter a **Name** and **Description**.
7. Click **Upload**.

# Working with vApps

You can create a new vApp based on a vApp template stored in a **Public Catalogs** (e.g. Gold Images) or in your organization’s catalogs under **My Organization’s Catalogs**. You can also create your own vApp templates.

[](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/vapps.png)

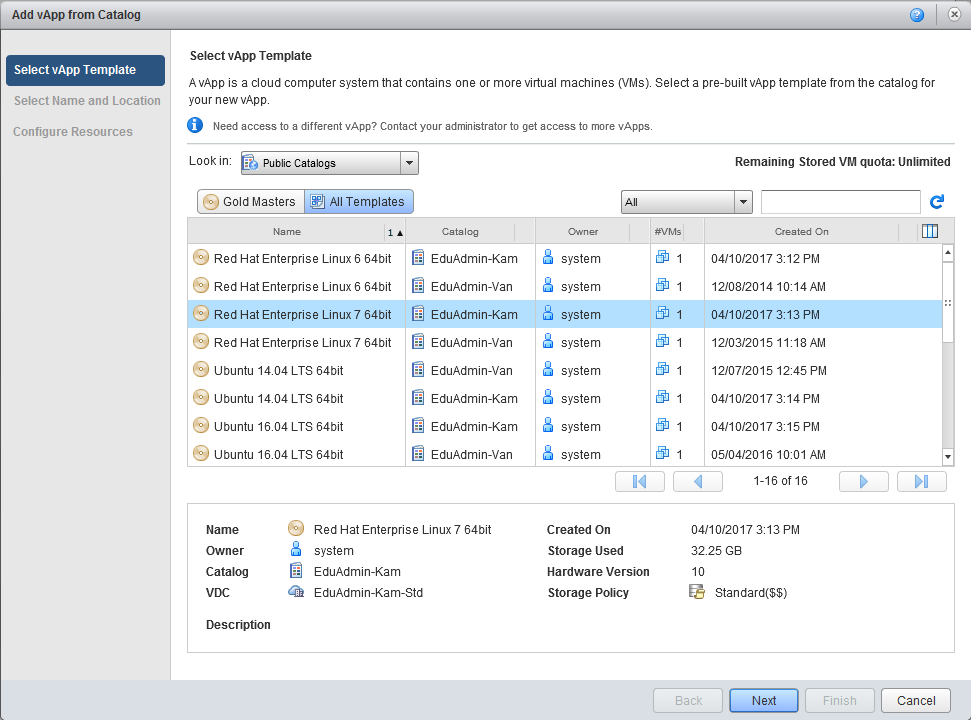
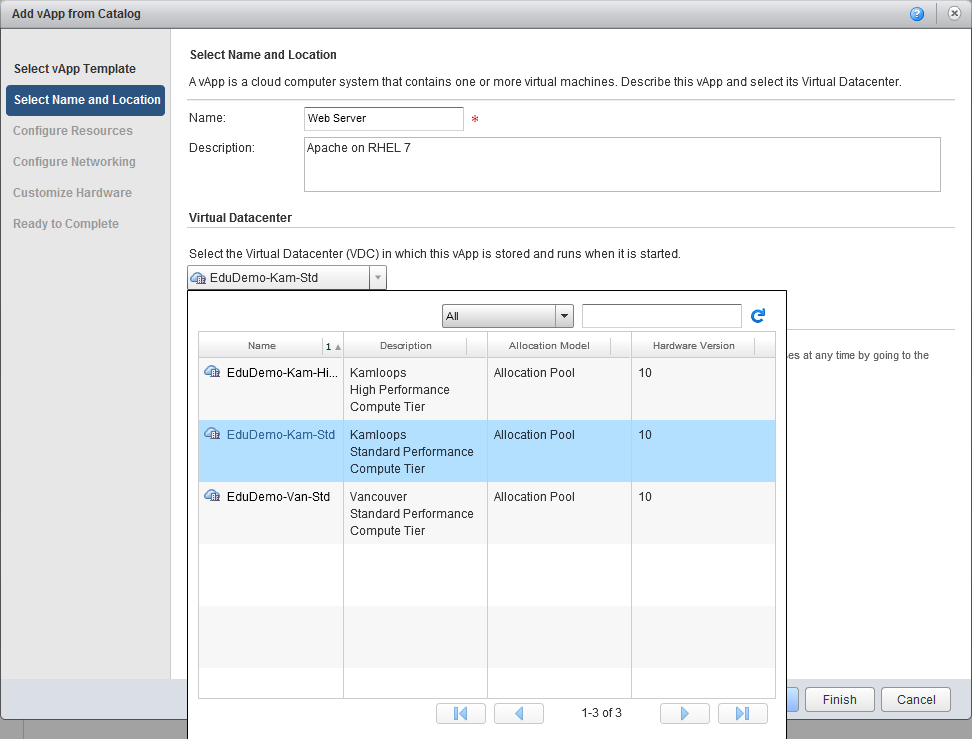
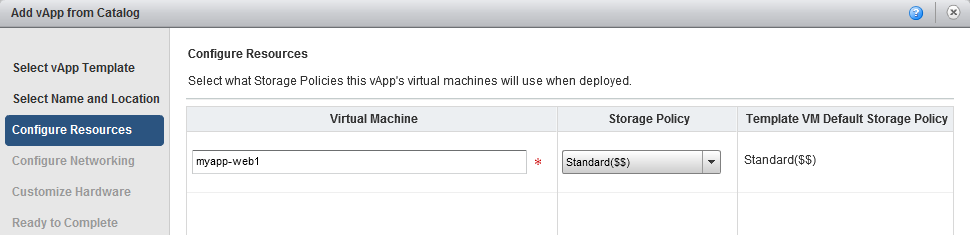
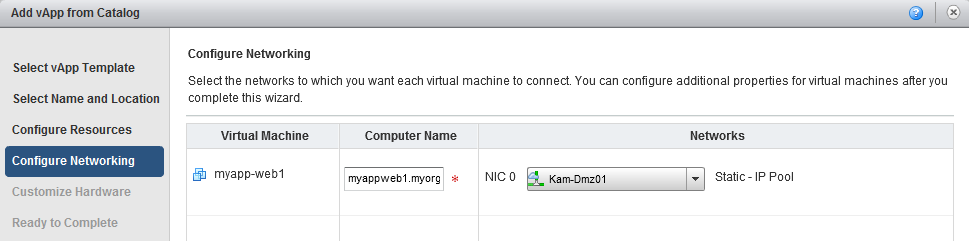
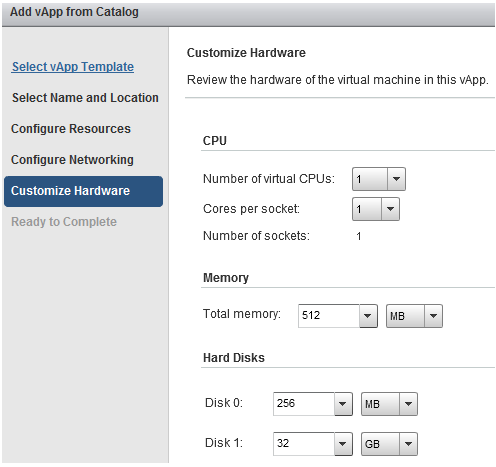
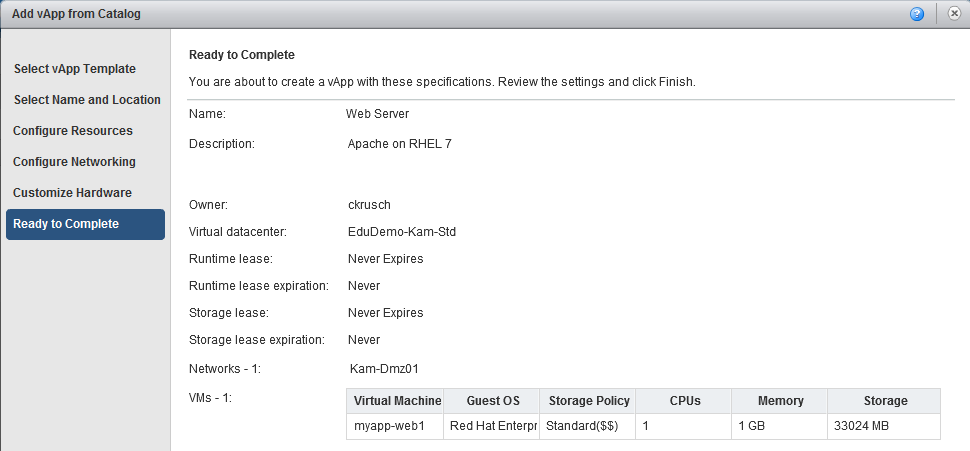
## Selecting Catalog Images

When deploying a vApp or VM from catalogs, where possible, select from a catalog located at the same site that you intend to deploy the image. This has two benefits:

1. Deployment is much faster and more efficient – taking typically only a few minutes (vs 30 to 60 minutes).
2. When deploying from an EduCloud maintained catalog, you are deploying an image optimized for the infrastructure located at that site.

## Add vApp from Catalog

A vApp can be added from a vApp template published in your organization or public catalogs:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps.**
3. In the right pane click on the  icon to start the Add vApp from Catalog wizard.
4. In the **Look in** drop down list, select whether you want to deploy from your organizations catalogs or the public catalogs
5. Select **All Templates** item.
6. Select a vApp template – ideally from a catalog located at the same site that you intend to deploy the vApp. In this example, the Kamloops catalog is chosen:  
     
   
7. Under **Select Name and Location** Type a **name** and **description** for the vApp.
8. Select the **Virtual Datacenter** where the vApp will be deployed and click **Next**.  
     
   
9. Under **Configure Resources** type a **name** for each virtual machine in the list, select a **storage Policy** for the virtual machine and click **Next**.  
     
   
10. Under **Configure Networking** provide a **computer name** and choose a **network** from the drop down list. The drop down list will display your organization VDC networks. If you need to add a vApp network, select **Add Network…**  Click **Next**.  
      
    
11. Under **Customize Hardware** provide the compute resources for VMs and click **Next**.  
      
    [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addvappfromcatalog5.png)
12. Review the summary – do not check “Power on vApp after this wizard is finished”  
      
    
13. Click **Finish** to start creation of the vApp

The configured vApp will now be created in **My Cloud**. You can watch its progress in the **My Cloud** tab in the vApps panel. Wait until the status changes to **Stopped** before proceeding.

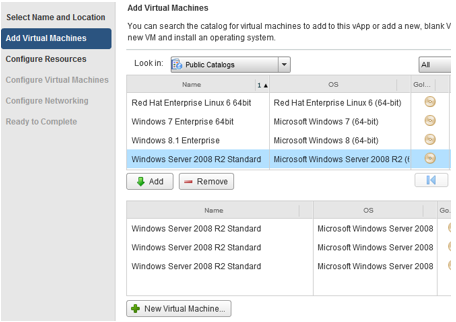
The first time the vApp is powered on, Guest OS customization should run for each VM to set the hostname and network settings within the guest operating system. Please see the **Working With VMs 🡪 Guest OS Customization** section if customization did not occur.

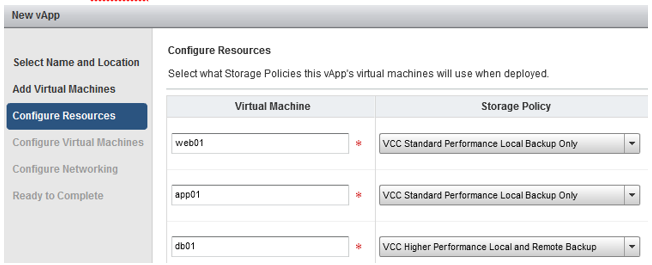
## Add vApp from OVF

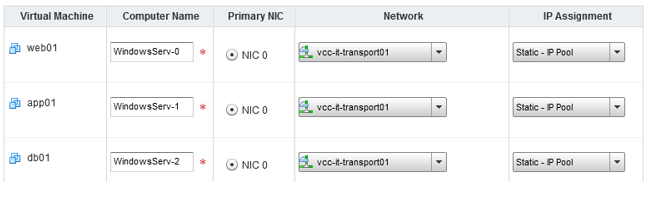
There are many pre-built virtual appliances available from the VMware Solution Exchange or Virtual appliance marketplace. These are packaged in OVF format, and can be downloaded and installed in EduCloud as follows:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps.**
3. In the right pane click on the  icon to start the **Add vApp from OVF** wizard.
4. Under **Select Source** choose a **URL** or click **Browse** to add your OVF package.  
   (You may receive a message that the Client Integration Plug-In needs to be installed. Please install the plug-in before attempting to add a vApp from an OVF package.)
5. Review Details and click Next
6. **Select Name and Location.** (You may only have one VDC for location) Click **Next**
7. Configure Resources. Set Computer Name and Storage Policy.
8. **Network Mapping**: Confirm Destination and IP Allocation
9. **Custom Properties**: Set **Time Zone** and custom network properties if necessary  
   (*Leave blank for defaults*)
10. **Customize Hardware**: Set compute requirements or leave as OVF package default.
11. Ready to Complete: Review and click Finish.

## Build a New vApp

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps.**
3. In the right pane click on the  icon to start the **New vApp** wizard.
4. In the New vApp wizard, under **Select Name and Location** perform the following actions:
   * **Name**: type in the name for the vApp
   * **Description:** enter a brief description of the vApp
   * **Runtime lease:** use the drop down menu to select the desired lease, or leave as Never Expires
   * **Storage lease:** use the drop down menu to select the desired lease, or leave as Never Expires
5. Click **Next**.
6. Under **Add Virtual Machines**, select the desired catalog from the **Look in** drop down menu.
7. Select the virtual machine template you want to add and click the **Add** button.
8. Repeat the previous two steps to add any additional virtual machines that will make up the new vApp. When finished adding the virtual machines, click **Next**.  
     
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addvm.png)
9. Under **Configure Resources**, name each virtual machine and select its **storage policy**. Click **Next**.

[](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/configureresources.png)

1. Under **Configure Virtual Machines**, set the **computer name** and **network settings** for each virtual machine. Select **Static – IP Pool** to automatically assign an IP to the VM or **Static – Manual** to manually assign an IP to the VM. Click **Next**.   
     
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/configurevm2.png)
2. Make any adjustments to the networking for the vApp. Fence the vApp or adjust whether vApp networks are isolated or routed, etc. See the “Working with Networks in a vApp” section for more details. Click **Next**.
3. Verify settings under **Ready to Complete** and click **Finish**.

## Adding VMs from a Catalog

You can add additional VM’s to a vApp by searching your catalogs for virtual machines to add – or add new, blank virtual machines, as follows:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab.
5. Click the **Add VM button** ( icon). The New Virtual Machine wizard will start.
6. Follow the steps as outlined under “Build a New vApp” to add additional VMs from the catalog and configure the VM resources and networking.
7. Click **Finish**.

## Adding a New VM

You can add a new VM instead of adding one from a catalog. This VM will not have an operating system installed.

Create a New Virtual Machine

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab.
5. [addnewvmbutton](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addnewvmbutton.png)Click the **Add VM button** ( icon). The New Virtual Machine wizard will start.
6. Click on the **New Virtual Machine** button to create a new blank VM.
7. Enter the virtual machine **Name** and set its **Host name** and description.
8. Set Virtual hardware version to the highest supported version.
9. Set the **operating system family** and **operating system** type. Please note that not all listed operating systems are supported (e.g. Apple OS is listed, however is not supported and will not run).
10. Set the number of CPUs, memory and disk size requirements. **Note:** these amounts will be allocated from your vDC resource allotment.
11. Do not change the **Bus type** – it is automatically set to the recommended bus type based on the operating system you selected
12. Click **OK** to create the new virtual machine.
13. Continue to add more new VMs or VMs from catalogs as previously outlined.
14. When finished adding the virtual machines, click **Next**.
15. Follow the steps as outlined under “Build a New vApp” to configure the VM resources and networking.
16. Click **Finish**.

Now follow the instructions for “Install a Guest Operating System” in the “Working with VMs” section.

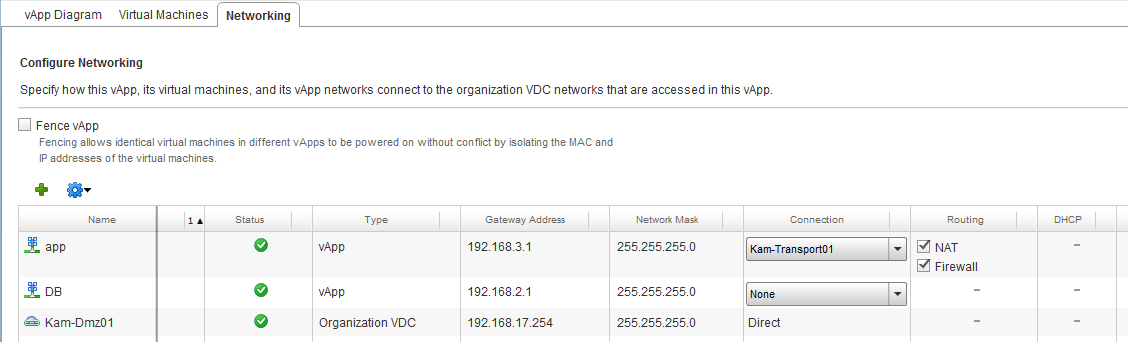
## Working with Networks in a vApp

Review the “*Networking”* section of the “*EduCloud Server: Concepts and Overview*” document for a description of the different types of networks vApps can use. Full documentation on working with Networks in vApp can be found in the “*vCloud Director User’s Guide*” under “*Working with vApps 🡪 Working with Networks in a vApp*”.

The virtual machines in a vApp can connect to vApp networks (isolated or routed) and organization virtual datacenter networks (direct or fenced). You can add networks of different types to a vApp to address multiple networking scenarios. To view the list of networks available in a vApp:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Networking** tab.

The following screen shot shows a vApp that includes a direct Org VDC Network (Kam-Dmz01), an isolated vApp network (DB), and a routed vApp network (app).



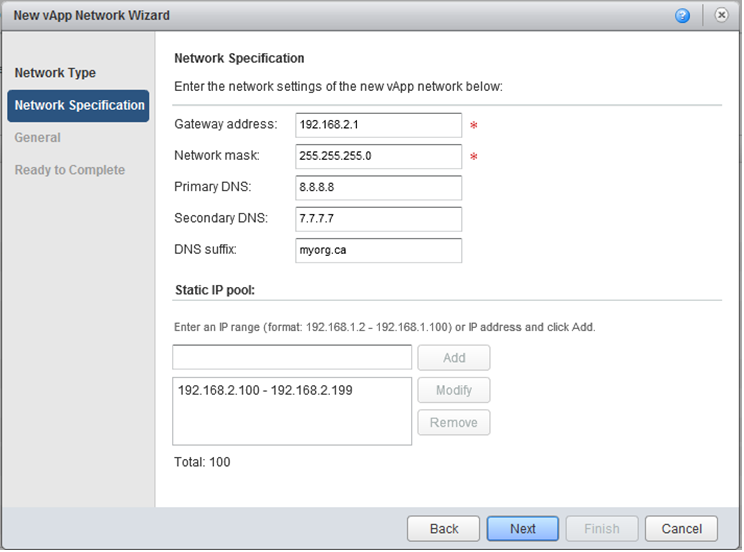
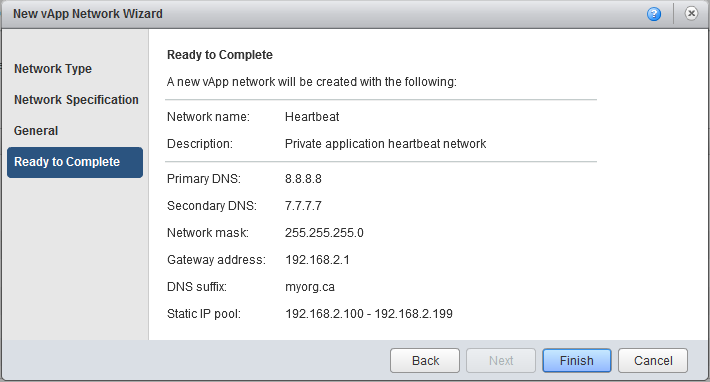
### Adding Networks to a vApp

vApps can only access the networks that are configured for access (in the **networking** tab). If you want to access any additional networks, you must first add them to the vApp.

#### Add an Org VDC Network

1. Navigate to the **Networking** tab of the vApp you wish to modify.
2. Click the **Add Network…** ( icon).
3. Select the “Organization VDC” **Network Type**. Click **Next**
4. Select the **Organization VDC Network** you wish to add and click **Finish**
5. Click the **Apply** button on the Networking tab to apply the changes

#### Add a vApp Network

1. Navigate to the **Networking** tab of the vApp you wish to modify.
2. Click the **Add Network…** ( icon).
3. Select the “vApp Network” **Network Type**. Click **Next**
4. Enter the **Network Specification** and **Static IP pool** settings  
     
   
5. Enter a **Network Name** and **Description**. Click **Next**
6. Review all settings and if correct, click **Finish**.  
     
   
7. You are now returned to the vApp **Networking** tab. The new network will appear highlighted in yellow as an isolated vApp network. If you wish have a routed vApp network, modify the network **Connection** from “None” to the Org VDC Network that the vApp network should be routed through, and select the routing services that are required.
8. Click the **Apply** button on the Networking tab to apply the changes

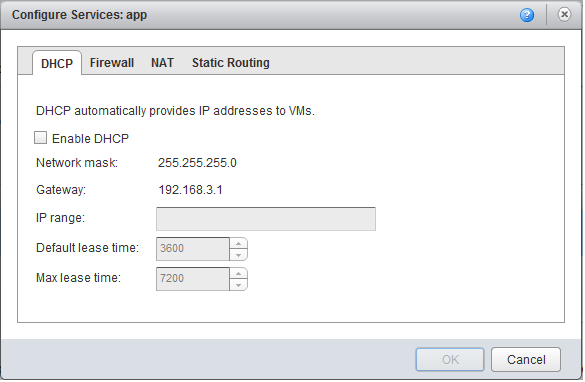
|  |
| --- |
| **Reminder**: the routing appliance used by routed vApp networks cannot be configured for high availability. |

### Configure vApp Network Services

The following network services are available for vApp networks:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **vApp Network Type** | **DHCP** | **Firewall** | **NAT** | **Static Routing** |
| Routed | X | X | X | X |
| Isolated | X |  |  |  |

vApp Network services are configured via the “Configure Services” dialogue. To open the dialogue:

1. Navigate to the **Networking** tab of the vApp you wish to modify.
2. Right click the vApp network for which you wish to modify services and select the **Configure Services…** menu item.  
     
   

Full documentation for configuring DHCP, Firewall, NAT and Static Routing services for a vApp network can be found in the “*vCloud Director User’s Guide*” under “*Working with vApps 🡪 Working with Networks in a vApp 🡪 Configuring Network Services for a vApp Network*”.

# Working with VMs

This section contains information on how to make changes to your VMs like adding additional resources, changing passwords and what to do before the first boot.

## Mount a CD/DVD

Sometimes you need to mount a CD/DVD or a CD/DVD ISO image to install an operating system or software it contains. There are two options:

### Mount an image from the Catalog

To mount a CD/DVD image from an ISO file stored in your catalog:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab.
5. Right click the virtual machine and select **Insert CD/DVD from Catalog**.
6. Select the appropriate media file from the catalog and click **Insert**. See the **Upload an ISO** topic in the **Catalogs** section if your media file is not available in the catalog.

Note: The vCloud Director Client Integration Plug-in must be installed to use this feature.

### Mount a local CD/DVD

You can do a pass-through to a local CD/DVD once the VM is powered on and you are viewing the VM Console. To do a pass-through to local CD/DVD:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab.
5. Right click on the virtual machine you want to attach the local CD/DVD to and select **Popout Console**.
6. In the VM console window, click on the CD/DVD icon on the top right of the VM console window.
7. Review the warnings and select your local CD/DVD to mount it to the VM.
8. Log into the operating system in the VM console and (for Windows) navigate to Windows Explorer, or (for RedHat) mount the CD/DVD.

## Install a Guest Operating System

If you have created a new, blank VM, you must install an operating system on it. The appropriate guest operating system ISO file must be in your catalog.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab.
5. Mount the OS install CD/DVD from your catalog following the instructions in the previous section.
6. Power on the virtual machine by right clicking on it and selecting **Power On**. Pop out the console and watch the boot screen to select boot order in order to boot from the ISO image and start the installer.
7. Follow the guest operating system installation instructions.
8. Be sure to install VMware tools or Open VM Tools after the operating system is installed.

## Guest OS Customization

Most templates in catalogs are configured so guest OS customization will automatically run for each VM the first time the vApp is powered on. This will not always occur if a template is misconfigured or you built your own vApp by importing different VMs. To force a full customization, including changing the System Identifier (SID) for windows systems, do the following for each VM:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the virtual machine you want to customize and select **Properties**.
6. In the Virtual Machine Properties window, select the **Guest OS Customization** tab.
7. Select the **Enable guest customization** check box.
8. Select **Change SID** checkbox, if present.
9. Select the **Allow local administrator password** check box and click **Auto generate password**.
10. Select **Require administrator to change password on first login** checkbox.
11. Click **OK** to make the configuration changes. Wait for the status to change to **Powered Off** before proceeding.

You can now power on each virtual machine by right clicking on the VM and selecting **Power On.** Wait for the status to change to powered on – now you can open up the console window by right clicking on the virtual machine and selecting the **Popout Console** option.

Note: A windows guest may take 5-10 minutes for Guest OS Customizations to complete (to run windows sysprep) the first time it is customized. The VM will reboot several times during the process. Please wait for this procedure to complete before continuing.

## Forcing Guest OS Recustomization

If you change the computer name setting, or make any changes to networking for a VM, you must force guest OS recustomization so the associated changes are reflected within the guest operating system.

To force recustomization:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the virtual machine you want to customize and select **Power On and Force Recustomization**.

## Resetting the Admin/Root Password

Please note that the virtual server needs to be **powered off** in order for the administrator/root password to be changed.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the VM you want to change the password for and select **Power Off**.
6. Wait for the status to change to Powered Off and then right click on the VM and select **Properties**.
7. In the Virtual Machine Properties window, select the **Guest OS Customization** tab.
8. Select the Enable guest customization checkbox.
9. Select the **Allow local administrator password** check box. You can either
   * **Auto generate the password** for the administrator / root user
   * Or Specify a password to use
10. Select Require administrator to change password on first login.
11. Click OK button to update the configuration.
12. Once the status of the virtual machine changes to Powered Off, right click on the VM and select **Power On and Force Recustomization**.

## Modify VM CPU and Memory Resources

You can modify the number of virtual CPUs and memory for a virtual machine. The number of virtual CPUs and memory that a virtual machine supports depends on its virtual hardware version.

You must power off the virtual machine before adding CPUs or memory, unless the virtual machine (supports and) has been enabled for memory and CPU hot add. These options have been preconfigured for all images contained within the public catalogs (e.g. images from the gold catalog).

**Note:** these resources are going to be assigned from your virtual data center resource allotment.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the virtual machine you want to change the resources for and select **Properties**.
6. Select the **Hardware** tab.
7. Adjust the CPU and memory resources as required. Please see next section for adding additional hard disk resources.
8. Click OK when finished.

If you hot added CPU and memory, additional steps may be required within your guest operating system before the resources can be used – locate and follow the memory and CPU hot add procedures for the installed operating system.

## VM CPU and Memory Hot Add

The CPU and Memory hot add options are enabled by default on all UBC IT provided images (e.g. the ones located in the gold images public catalog).

Hot-add options allow you to add additional CPU and memory resources to a virtual machine that is powered on. This feature is only supported on certain guest operating systems and virtual machine hardware versions. The virtual machine must be powered off to modify some general properties.

To enable CPU and Memory hot add:

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the VM you want to change the resources for and select **Properties**.
6. Select the **General** tab.
7. Select the **Virtual CPU hot add** checkbox.
8. Select the **Memory hot add** checkbox.

## Add a VM Hard Disk

You can add additional hard disks to a virtual machine. Depending on the guest operating system, the virtual machine may remain powered on to add an additional disk.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. Right click on the VM you want to change the resources for and select **Properties**.
6. Select the **Hardware** tab.
7. In the Hard Disks section, click the **Add** button to add an additional disk.
8. Select the disk size. The remaining options should **stay as defaults**. Changing these options will result in operational issues with the virtual machine.
9. Click OK when done.

|  |
| --- |
| Note: Make sure you double-check before you delete a disk.Before removing a disk, ensure that you’re deleting the **correct** disk. EduCloud allows you to modify the system disk, which includes deletion. The removal of the system disk will render the VM inoperative. |

Use the guest operating system tools partition, format and mount the new disk.

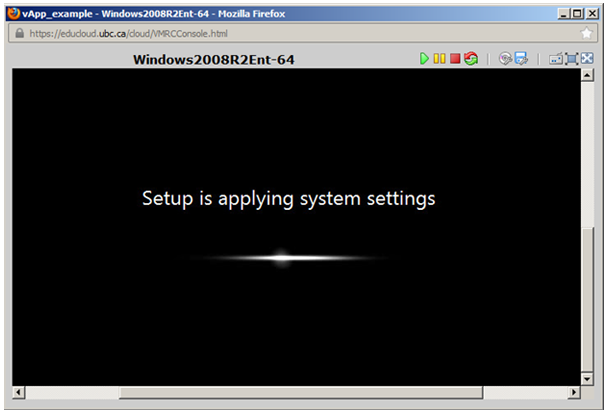
You can edit or remove a hard disk using the same procedure. Some guest operating systems may allow you to edit (grow) disks while powered on, but other actions, including shrinking and removing disks, require the virtual machine to be powered off.

## VM Console

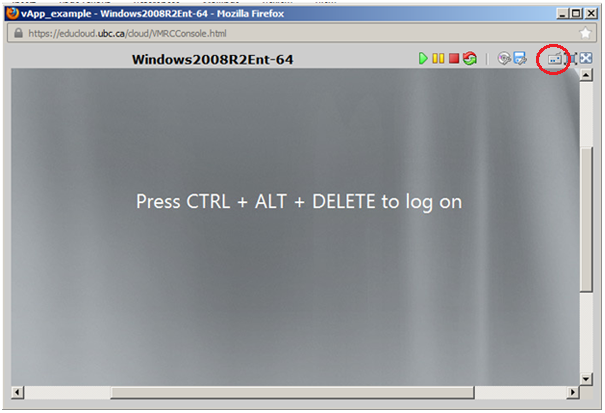
Please note that you have to enable browser pop-ups to be able to open up a virtual machine console.

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to configure and select **Open**.
4. Select the **Virtual Machines** tab to view all VMs associated with this vApp.
5. If the VM is not powered on, right click on it and select **Power On**.
6. Once the status of the VM changes to Powered On, right click on it and select **Popout Console**.

You may see the following the first time the VM is powered on as EduCloud applies the customization changes, such as setting the password:

[](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/applysyssettings.png)

Once completed, you will see the operating system log on prompt.

[](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/ctrlaltdel.png)

For Windows, you will need to click on the keyboard icon in the top right of the window (3rd icon from the right) to simulate the CTRL+ALT+DEL so you can enter the username and password.

**Note**: You may be asked to change the administrator password if this is the first time you are logging in to the virtual machine.

## VMware Tools/Open VM Tools

VMware Tools is a suite of utilities that enhances the performance of a VMs guest operating system, and enables features that allow the infrastructure to properly manage the VM and its guest operating system. VMware develops and distributes VMware Tools

Open VM Tools is an open source implementation of VMware Tools. The primary purpose for open-vm-tools is to enable operating system vendors and/or communities and virtual appliance vendors to bundle VMware Tools into their product releases.

VMware Tools or Open VM Tools must be installed in your guest operating system for your VM and operating system to function properly and reliably within the EduCloud Server service.

Many features, such as Guest OS customization, proper Guest OS shutdown, guest memory management, console display, networking, etc. will not work or will operate in a degraded, less efficient mode if VMware/Open tools are not installed.

VMware recommends that you use Open VM Tools (open-vm-tools) if it is provided with your operating system release, and to download and install VMware Tools if not.

open-vm-tools is available with these operating systems:

* Fedora 19 and later releases
* Debian 7.x and later releases
* openSUSE 11.x and later releases
* Recent Ubuntu releases (12.04 LTS, 13.10 and later)
* Red Hat Enterprise Linux 7.0 and later releases
* CentOS 7 and later releases
* Oracle Linux 7 and later releases
* SUSE Linux Enterprise 12 and later releases

VMware Tools or open-vm-tools is already preinstalled and tested on all EduCloud Public Catalog templates.

For instructions on installing VMware Tools or open-vm-tools for a VM not deployed from one of the Public Catalog templates, please check the Guest Operating System install guides available at <http://partnerweb.vmware.com/GOSIG/home.html>.

# Securing EduCloud VMs

The EduCloud Server service includes anti-virus protection using Trend Micro Deep Security.  The 2 components available are Anti-Malware for virus and malware prevention, and Web Reputation to block black-listed and dangerous websites.

## Agent-less vs Agent-based Protection

Depending on the OS, Deep Security has 2 modes of protection that's either agent-less or agent-based.  Due to the light-weight nature, **agent-less** is preferred when available.  Here's the general rule of thumb:

|  |  |
| --- | --- |
| OS Type | Protection Type |
| Windows | Agent-less |
| Linux | Agent-based |

Agent-less protection is available for all Windows OS except for Windows 10.  It will require up-to-date VMware Tools with the Guest Introspection component installed (not installed by default).

Agent-based protection requires the installation of the Deep Security Agent on the VM.  Trend provides agents for the majority of the Linux distributions and versions we are running in our environment such as Red Hat 6 & 7, and Ubuntu 12 and 14.

 Advantages of agent-less protection:

* No footprint on the VMs
* Minimal traffic on the VMs

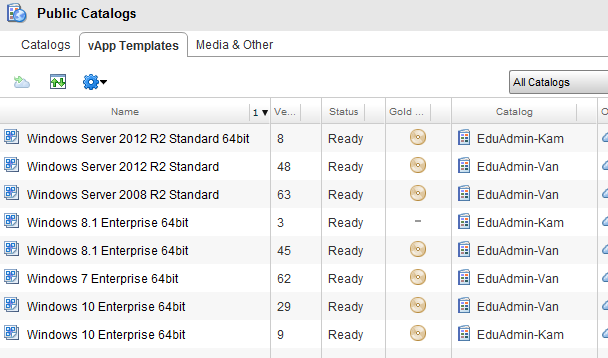
Disadvantages of agent-less protection:

* Lack of in-memory scanning
* No damage cleanup.

## Securing Windows VMs

### Windows VMs Provisioned from EduCloud Gold Master Templates

VMs provisioned from the default Gold Master images below will already have Trend Micro Deep Security components installed and activated. No additional steps need to be done to protect these VMs.

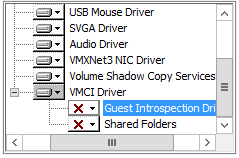
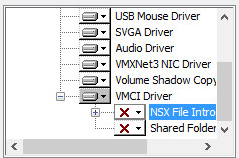


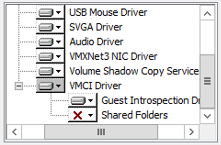
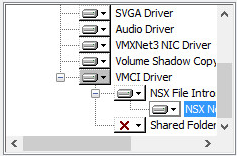
### Custom Built Windows Images

Windows VMs provisioned from uploaded OVF or built from ISO files will need to be prepared for Agent-less protection.

#### VMware Tools Preparation

1. Install VMware tools – right click on the VM and click Install VMware tools
2. Sign into the Windows guest File Explorer > DVD drive > run installer
3. Select Custom Install
4. Expand VMCI Driver at the bottom of the list

If Guest Introspection Driver or NSX File Introspection Driver has a red X next to it, click on the X and select the “Entire feature will be installed on local hard drive option”  
 or 

If Guest Introspection Driver or NSX File Introspection Driver has a solid icon next to it, then this means this component is already installed.  
   
 or 

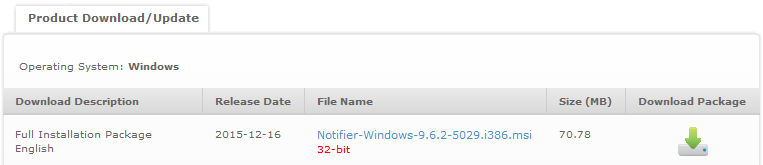
1. Click Next and Change or Install to complete the installation
2. A VM reboot may be required post installation.

#### C:\79928fc73f07e30ff4d5202bc23f7734C:\e8a053cf9220292dbf5e4228451f7aaeDeep Security Notifier (Optional)

The notifier sits in the Tray, and provides notification when a malware or malicious web page has been detected.

It also provides the activation status of Trend as well as information like virus pattern version, and event history.

While this step is optional (it is not necessary for Trend to function properly) it is still recommended that you install the Notifier on your VM.

1. Download the latest Notifier from Trend Micro at this URL: <http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4856&lang_loc=1>.  
     
   
2. Copy the installer to your VM, or download from the VM.
3. Run the installer from the VM and accept all default settings.  No reboots required.
4. The Notifier icon should appear in the tray.  It will show the Anti-Malware and Web Reputation features as "Not configured" until your VM has been activated for Trend protection by Systems.

#### Request for Trend Activation for Agent-less Protection for Custom Built Windows Images

After installing VMware Tools as per the steps above, you can submit a request to activate your VM via the BCNET [web form](http://web.it.ubc.ca/forms/systems/).  Please include:

1. VM Name
2. Which environment (UDC Prod or EduCloud)
3. Please mention that prep steps have been completed, and that agent-less activation is requested

Once the EduCloud administrators confirm the activation has been completed, you can verify the status using the Notifier

Note: VMs provisioned from the default Gold Master images will already have Trend Micro Deep Security components installed and activated. It is not necessary to submit a request to activate Trend protection for these VMs.

## Securing Linux Systems

*Coming soon!*

# Snapshots

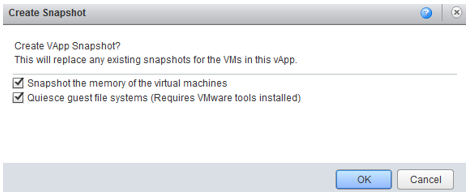
Snapshots preserve the state of a VM or an entire vApp (and all VMs it contains) at a specific point in time and allows you to revert back to it later.

Snapshots are designed to allow for rollback for a short window of time (ideally no more than a few days) – for example during a software upgrade/acceptance window. They should not be left in place for an extended period of time as they have a negative impact on both VM performance and backup performance that will worsen with time.

Create a Snapshot of a Virtual Machine

You can only create a single snapshot of a VM. This can be done either on a vApp level or a VM level. For example, you can snapshot all the VMs contained within a vApp by creating a vApp snapshot. Any subsequent VM snapshots will replace the previous snapshot (taken either on the vApp or VM level).

## vApp snapshot

1. In the top menu select **My Cloud**.
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to snapshot and select **Create Snapshot**.
4. A window will pop up with a warning that previous snapshots will be replaced. Click **OK** to proceed.  
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/createsnapshot.png)

This may take up to 10 minutes depending on how many VMs are contained in the vApp, their size and whether they are powered on.

## VM snapshot

Alternatively, you may only want to create a snapshot for a single virtual machine.

1. In the top menu select **My Cloud**.
2. In the left pane, select **VMs**.
3. In the right pane, right click the VM you want to snapshot and select **Create Snapshot**.
4. Click **OK** button to create the snapshot.

## Revert a Virtual Machine to a Snapshot

You can revert a virtual machine to the state it was in when the snapshot was created. This can be done multiple times until the snapshot is deleted. Please note that you are only reverting to the latest snapshot created.

Verify that the virtual machine has a snapshot by right clicking on the VM. **Revert to snapshot** option should not be greyed out.

1. In the top menu select **My Cloud**.
2. In the left pane, select **VMs**.
3. Right-click the virtual machine you want to revert and and select **Revert to Snapshot**.
4. Click **Yes**.

Remove a Snapshot for vApp

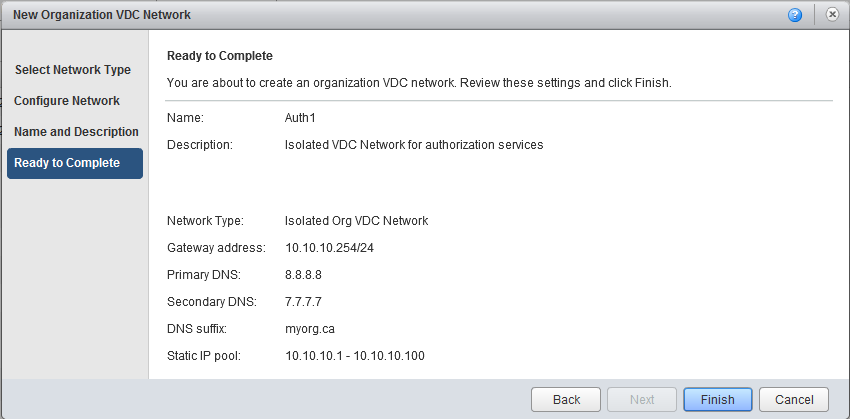
1. In the top menu select **My Cloud** .
2. In the left pane, select **vApps**.
3. In the right pane, right click the vApp you want to snapshot and select **Remove Snapshot**.
4. A window will pop up with a warning that snapshots for all VMs within the vApp will be deleted. Click **OK** to proceed.

Remove a Snapshot for a single VM

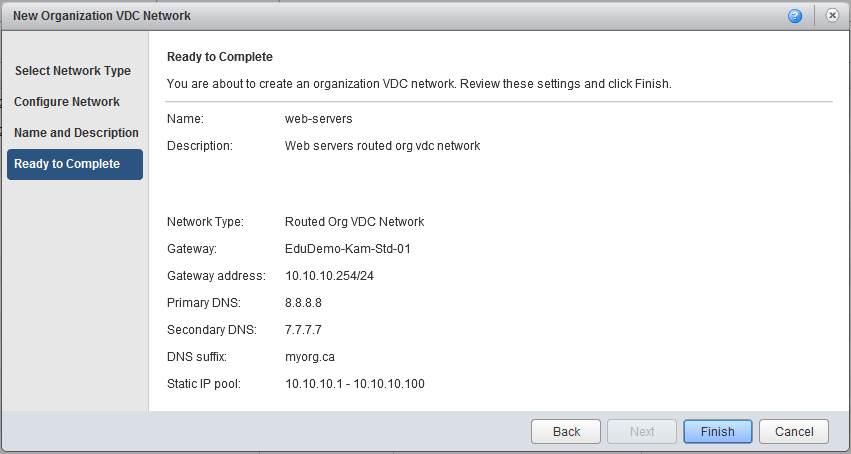
1. In the top menu select **My Cloud**.
2. In the left pane, select **VMs**.
3. In the right pane, right click the VM you want to delete the snapshot for **Remove Snapshot**.
4. Click **Yes.**

# Organization VDC Networks

## Create an Isolated Org VDC Network

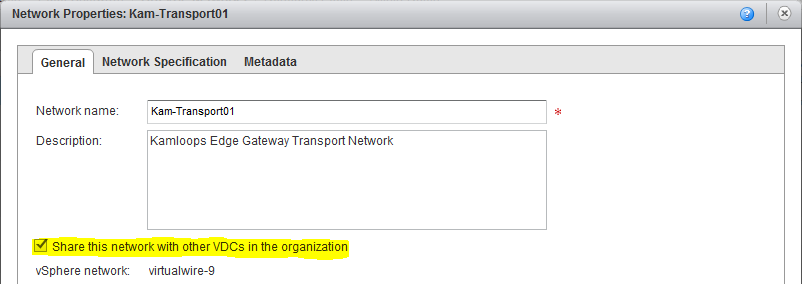
1. In the top menu select **Administration**.
2. In the left pane, select **Virtual Datacenters**
3. Double click the name of the virtual datacenter where you want to create the isolated org VDC Network.
4. Select the **Org VDC Networks** tab
5. Click the**Add Network…** () icon.
6. Select **Create an isolated network within this virtual datacenter** and click **Next.**
7. Enter a **Gateway address** and **Network mask** for the network.
8. (Optional) Enter the **Primary DNS**, **Secondary DNS**, and **DNS Suffix**.
9. (Optional) Enter an IP address or range of IP addresses and click **Add** to add IPs to the **Static IP pool**.
10. (Optional) Repeat step 9 to add more ranges to the **Static IP Pool**.
11. Click **Next**.
12. Enter a network **Name** and **Description**
13. (Optional) Select **Share this network with other VDCs in the organization** to make this Org VDC network available across all of your VDCs located at the same site.
14. Click **Next**.
15. Review the settings and click **Finish** to accept the settings.  
      
    

## Create a Routed Org VDC Network

1. In the top menu select **Administration**.
2. In the left pane, select **Virtual Datacenters**
3. Double click the name of the virtual datacenter where you want to create the routed org VDC Network. You must select a VDC that contains an Edge Gateway
4. Select the **Org VDC Networks** tab
5. Click the**Add Network…** () icon.
6. Select **Create a routed network by connecting to an existing edge gateway**, and select the edge gateway the network will be connected to. Click **Next.**
7. Enter a **Gateway address** and **Network mask** for the network.
8. (Optional) Select **Use gateway DNS** to use the DNS relay of the gateway.  
   This option is available only if the gateway has DNS relay enabled.
9. (Optional) Enter the **Primary DNS**, **Secondary DNS**, and **DNS Suffix**.
10. (Optional) Enter an IP address or range of IP addresses and click **Add** to add IPs to the **Static IP pool**.
11. (Optional) Repeat step 10 to add more ranges to the **Static IP Pool**.
12. Click **Next**.
13. Enter a network **Name** and **Description**
14. (Optional) Select **Share this network with other VDCs in the organization** to make this Org VDC network available across all of your VDCs located at the same site.
15. Click **Next**.
16. Review the settings and click **Finish** to accept the settings.  
      
    

## Multiple VDCs and Shared Networks

If your organization has multiple virtual datacenters (VDCs) at the same site (e.g. you are using the “Standard” and “High” performance compute tiers in Kamloops), be sure to check the **Share this network with other VDCs in the organization** option when defining organization VDC networks.



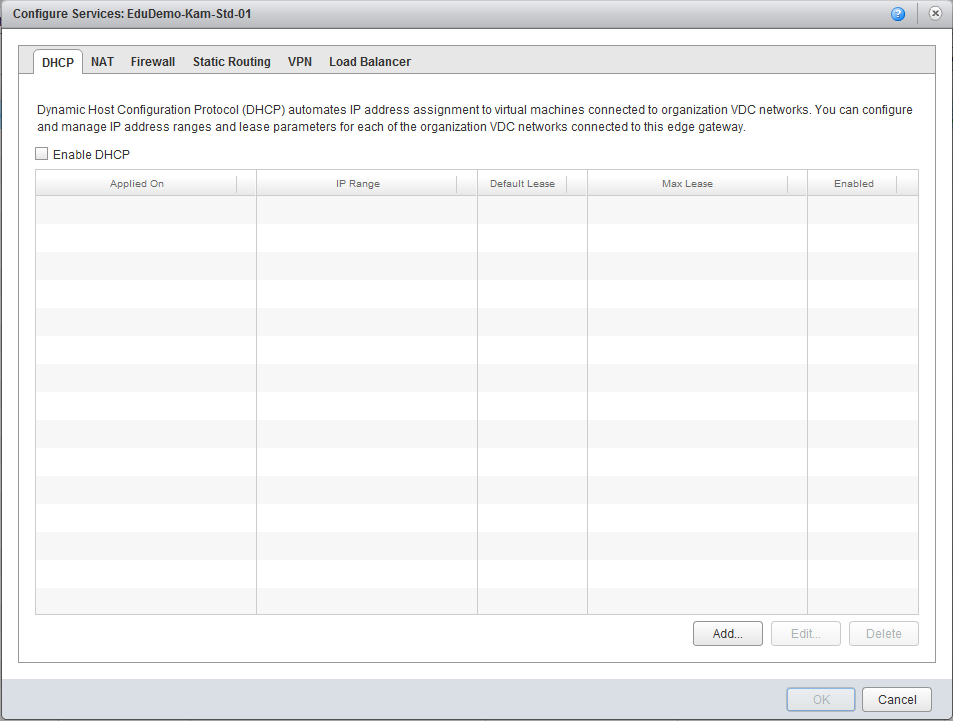
This option allows you to manage all networking at a site using a single edge gateway. If you forget to set this option, the network will only be visible in the VDC in which the edge gateway is running.

# Configuring Edge Gateway Services

Edge gateway services are managed by opening the edge gateways “Configure Services” dialogue. To open this dialogue do the following:

1. In the top menu select **Administration**.
2. In the left pane, select **Virtual Datacenters**
3. Double click the name of the virtual datacenter that contains the edge gateway to be configured.
4. Select the **Edge Gateways** tab
5. Right click the desired edge gateway and select **Edge Gateway Services…**

You should see the edge gateway **Configure Services** dialogue:



## DHCP

The edge gateways can provide basic DHCP services to virtual machines connected to associated organization virtual datacenter networks.

To enable DHCP for an organization VDC network:

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **DHCP** tab.
3. Check the **Enable DHCP** checkbox and click the **Add…** button.
4. Check the **Enable Pool** checkbox.
5. Select the organization VDC network the pool is to be **Applied on**.
6. Enter an **IP range** – first and last IP address in the range, separated by a dash (e.g. 192.68.1.1-192.168.1.100)
7. Set the **default lease time** and **maximum lease time** or use the default values.
8. Click OK.

## Network Address Translation (NAT)

### Source NAT (SNAT)

A source NAT rule translates the source IP address of outgoing packets on an organization virtual datacenter that are being sent to another organization virtual datacenter network or an external network.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **NAT** tab and click the **Add SNAT…**
3. Select the organization VDC network the SNAT rule is to be **Applied on**.
4. Enter a **Description** for the rule
5. Enter the original IP address or range this rule applies to in the **Original (Internal) source IP/range** text box.
6. Enter the translated IP address or range to translate the addresses of outgoing packets to in the **Translated (External) source IP/range** text box.
7. Select **Enabled** and click **OK**.

The IP addresses of any outgoing packets that match the source IP range is translated to one of the IPs specified in the translated IP range.

### Destination NAT (DNAT) Rule

A destination NAT rule translates the IP address and port of packets received by an organization virtual datacenter network coming from another organization virtual datacenter network or an external network.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **NAT** tab and click the **Add DNAT…**
3. Select the organization VDC or external network the DNAT rule is to be **Applied on**.
4. Enter a **Description** for the rule
5. Enter the original IP address or range this rule applies to in the **Original (External) source IP/range** text box.
6. Choose the **Protocol** to apply this rule on from the drop-down menu. To apply this rule on all protocols, select Any.
7. (Optional) Select an **Original port** to apply this rule to.
8. (Optional) Select an **ICMP type** to apply this rule to if this rule applies to ICMP.
9. Type the IP address or range of IP addresses for the destination addresses on inbound packets to be translated to in the **Translated (Internal) IP/range** text box.
10. (Optional) Select a port for inbound packets to be translated to from the **Translated port** drop-down menu.
11. Select **Enabled** and click **OK**.

The destination IP address and port are translated according to the destination NAT rule's specifications.

## Firewall Configuration

### Enable Firewall

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Firewall** tab and select **Enable firewall.**
3. Select the firewall **default action**
4. (Optional) Select the **Log** check box to log events related to the default firewall action.
5. Click **OK**.

### Add Firewall Rule

An organization administrator can configure certain organization virtual datacenter networks to provide firewall services. Enable the firewall on an organization virtual datacenter network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

When you enable the firewall, you can specify a default firewall action to deny all incoming and outgoing traffic or to allow all incoming and outgoing traffic. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the default firewall action.

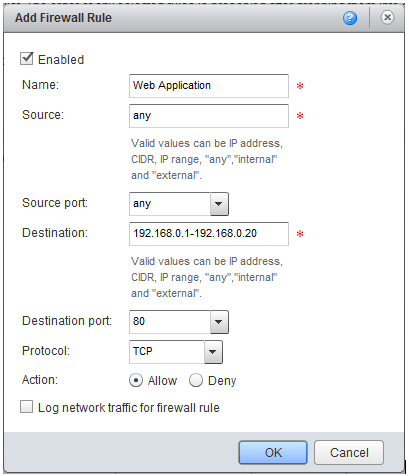
1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Firewall** tab and select **Add…**
3. Enter a **Name** for the rule.
4. Enter the traffic **Source**.

|  |  |
| --- | --- |
| **Option** | **Description** |
| IP address | Enter a source IP address to apply this rule on. |
| Range of IP addresses | Enter a range of source IP addresses to apply this rule on. |
| CIDR | Enter a network in CIDR notation to apply this rule on. |
| internal | Apply this rule to all internal traffic. |
| external | Apply this rule to all external traffic. |
| any | Apply this rule to traffic from any source. |

1. Select a **Source port** to apply this rule on from the drop-down menu.
2. Enter the traffic **Destination**.

|  |  |
| --- | --- |
| **Option** | **Description** |
| IP address | Enter the destination IP address to apply this rule on. |
| Range of IP addresses | Enter a range of destination IP addresses to apply this rule on. |
| CIDR | Enter a network in CIDR notation to apply this rule on. |
| internal | Apply this rule to all internal traffic. |
| external | Apply this rule to all external traffic. |
| any | Apply this rule to traffic from any source. |

1. Select the **Destination port** to apply this rule on from the drop-down menu.
2. Select the **Protocol** to apply this rule on from the drop-down menu.
3. Select the **Action**. A firewall rule can allow or deny traffic that matches the rule.
4. Select the Enabled check box.
5. (Optional) Select the Log network traffic for firewall rule check box. If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.
6. Click **OK** and click **OK** again.

[](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addfwrule.png)

### Reorder Firewall Rules

Firewall rules are enforced in the order in which they appear in the firewall list – top down.

When you add a firewall rule the new rule appears at the bottom of the firewall rule list. To enforce the new rule before an existing rule, reorder the rules.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Firewall** tab
3. Drag the firewall rules to establish the order in which the rules are applied.
4. Click **OK**.

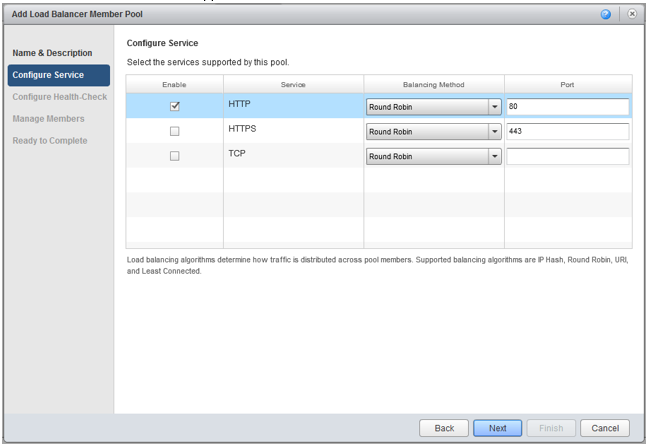
## Load Balancer

Edge gateways provide load balancing for TCP, HTTP, and HTTPS traffic.

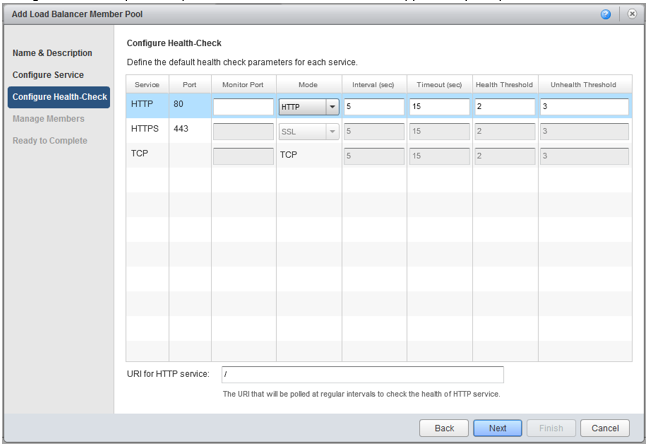
You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 809 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPS.

### Add a Pool Server to an Edge Gateway

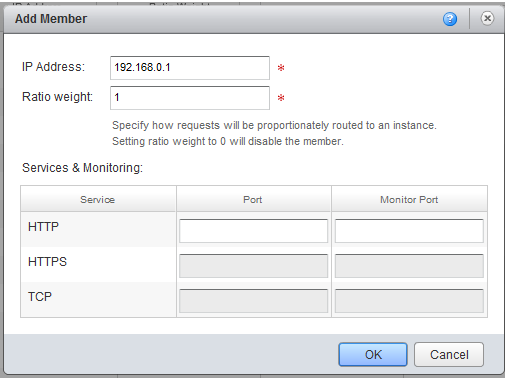
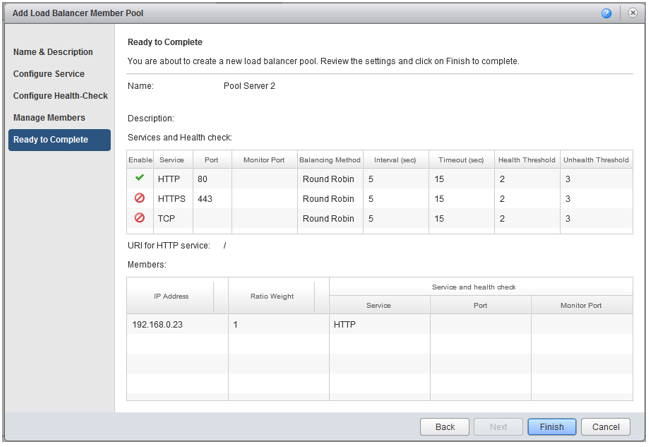
You can add a pool server to manage and share back-end servers flexibly and efficiently. A pool is comprised of one or more back-end servers called members and it manages health check monitors and load balancer distribution methods.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Load Balancer** tab, select **Pool Servers** and click **Add…**
3. Enter a **Name** and optionally a **Description** for the pool server and click **Next**.
4. Click **Enable** for each service to support.  
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addlbmemberpool.png)
5. Select a **Balancing Method** from the drop-down menu for each enabled service.

|  |  |
| --- | --- |
| **Option** | **Description** |
| IP Hash | Selects a server based on a hash of the source and destination IP address of each packet. |
| Round Robin | Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server’s processing time remains equally distributed. |
| URI | The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down. |
| Least Connected | Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections. |

1. (Optional) Change the default **Port** for each enabled service if necessary.
2. Click **Next**.
3. Change the **Monitor Port** if required for each service that is to be supported by this pool.  
     
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addlbmemberpool2.png)
4. Select the health check **Mode** from the drop-down menu for each service
5. (Optional) Change the default health check parameters if necessary.

|  |  |
| --- | --- |
| **Option** | **Description** |
| SSL | Tests servers using SSLv3 client hello messages. The server is considered valid only when the response contains server hello messages. |
| HTTP | The GET / default method is used to detect server status. Only responses 2xx and 3xx are valid. Other responses (including a lack of response) indicate a server failure. |
| TCP | TCP connection check. |
| **Option** | **Description** |
| Interval | Interval at which a server is pinged. |
| Timeout | Time within which a response from the server must be received. |
| Health Threshold | Number of consecutive successful health checks before a server is declared operational. |
| Unhealth Threshold | Number of consecutive unsuccessful health checks before a server is declared dead. |

1. If using HTTP, type the URI referenced in the HTTP ping requests at the bottom of the screen.
2. Click **Next.**
3. Click Add to add a back-end server to the pool.   
     
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addmember.png)
4. Enter the **IP Addres**s of the server and specify the **Ratio weight** to specify what ratio of requests to route to this back end server.
5. Change the default **Port** and **Monitor Port** for the server if required.
6. Click **OK**.
7. (Optional) Repeat Step 15 through Step 19 to add additional servers
8. Click **Next**.
9. Verify that the settings for the pool server are correct and click Finish.   
     
   [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addlbmemberpool3.png)

### Edit Pool Server Settings

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Load Balancer** tab, select **Pool Servers.**
3. Select the pool server to modify and click **Edit**.
4. Make the appropriate changes and click **OK**.

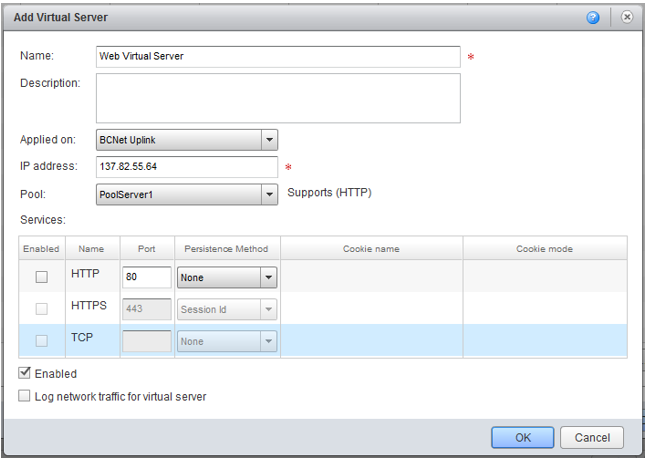
### Delete a Pool Server

Before you can delete a server pool from an edge gateway, verify that no virtual servers are using this pool server.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Load Balancer** tab, select **Pool Servers.**
3. Select the pool server and click **Delete**.

### Add a Virtual Server to an Edge Gateway

A virtual server is a highly scalable and highly available server built on a cluster of servers called members. It serves as the entry point for any external traffic which needs to access the back end servers. The edge gateway must have at least one pool server.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **Load Balancer** tab, select **Virtual Servers.**
3. Enter a **Name** and optionally a **Description** for the virtual server.
4. Select a network for the VIP from the **Applied on** drop-down menu.
5. Enter the **IP address** of the virtual server.
6. Select a P**ool** from the drop-down menu to be associated with the virtual server.
7. In **Services**, select **Enable** for each service to be supported.
8. Change the default **Port**, **Persistence Method**, **Cookie Name**, and **Cookie Mode** values for each enabled service as required.
9. Click **Enabled** to enable the virtual server.
10. (Optional) Click Log network traffic for virtual server.  
    [](http://campuscommunications.sites.olt.ubc.ca/files/2015/01/addvirtualserver.png)
11. Click **OK**.

## VPN

You can create VPN tunnels between edge gateways in the same organization, between edge gateways in different organizations, and between an edge gateway and remote network.

If any firewalls exist between the VPN tunnel endpoints, you must configure them to allow the following IP protocols and UDP ports to pass between the endpoints:

* IP Protocol ID 50 (ESP)
* IP Protocol ID 51 (AH)
* UDP Port 500 (IKE)
* UDP Port 4500

EduCloud does not support multiple VPN tunnels between the same two edge gateways. If there is an existing tunnel between two gateways and you want to add another subnet to the tunnel, delete the existing VPN tunnel and create a new one that includes the new subnet.

You cannot establish a VPN tunnel between edge gateways if any of the networks they contain have overlapping IP space. See the “*Site to Site Communications”* section of the *“EduCloud Server: Concepts and Overview*” guide for more information.

### Intra-Organization VPN Tunnels

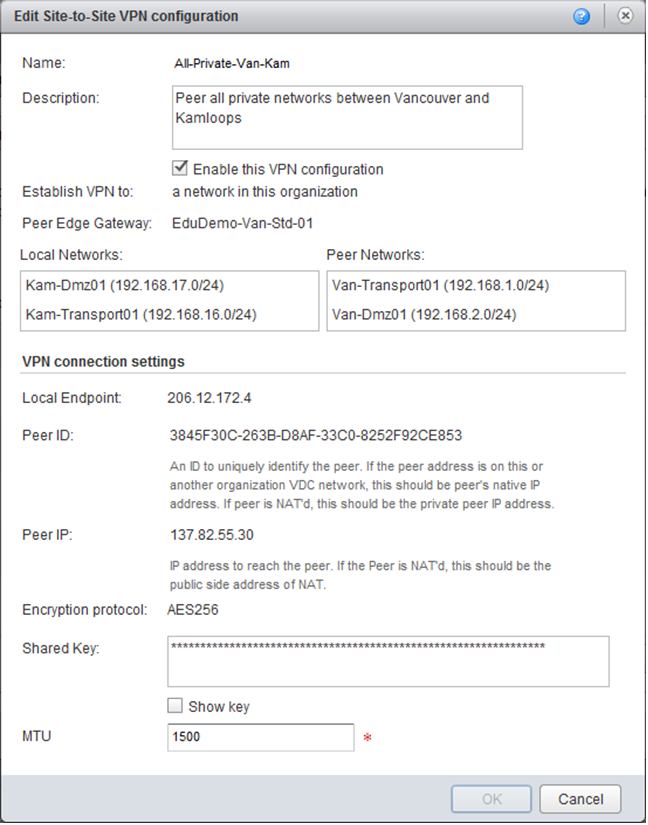
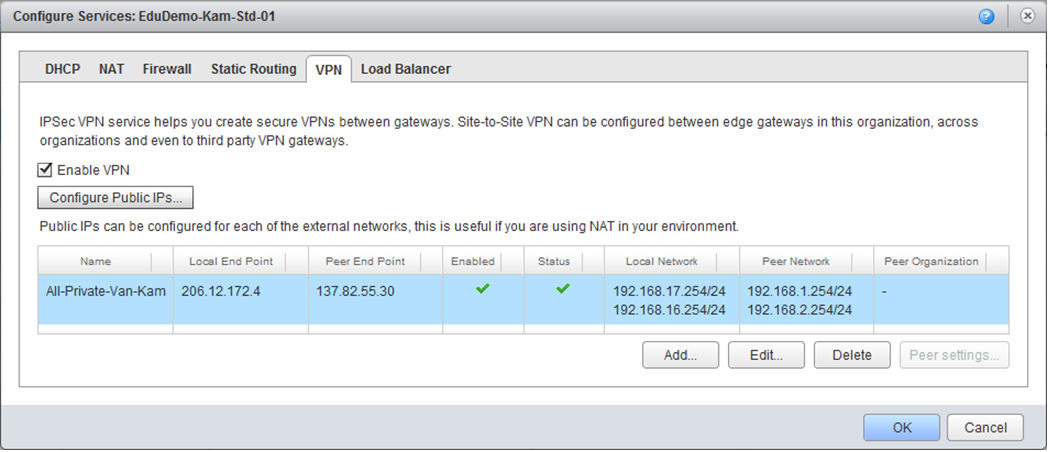
Intra-Organization VPN tunnels are used to establish network peering between two edge gateways within the same organization. It’s often used to peer networks located at different sites (e.g. between the Kamloops and Vancouver sites). Prior to setting up a VPN connection, review the services on each edge gateway and ensure that the firewall and static routing is enabled.

To establish peering between networks on different edge gateways in your organization:

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **VPN** tab
3. Select **Enable VPN** and click **Add…**
4. Enter a **Name** and **Description** for the peering connection
5. Select **Enable this VPN configuration**
6. Set **Establish VPN to**: “a network in this organization”
7. Select the **Peer Edge Gateway** (the other edge gateway you want to peer with)
8. Select the networks on the **Local** and **Peer** edge gateways that are to be peered (multi-select)
9. Leave all other settings at default and click **OK**
10. Click **OK again** to close the “Configure Services” dialogue box and commit the configuration change

Both edge gateways will be configured to establish the connection. It can take up to several hours for the connection to stabilize. You may receive warning emails about the connection state transitioning to red and green status during this time period. Once stabilized, the connection status of the VPN connection on each edge gateway should be green.

Firewall rules must be created on both edge gateways to allow the appropriate network communications to occur between the networks that were peered by the VPN connection.

The following screen shot shows the VPN service tab and a configuration that peers all private networks between the Kamloops and Vancouver sites:  
 

### Inter-Organization VPN Tunnels

You can create a VPN tunnel between two edge gateways in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **VPN** tab and click **Add…**
3. Enter a **Name** and **Description** for the peering connection
4. Select **Enable this VPN configuration**
5. Set **Establish VPN to**: “a network in another organization”
6. Click **Connect to another organization**, type the login information for the peer organization, and click Continue.
   * **vCloud URL** - The base URL of the vCloud instance that contains the peer organization. For example, https://www.example.com. Do not include /cloud or /cloud/org/orgname in the URL.
   * **Organization -** The organization name that is used as the unique identifier in the organization URL. For example, if the organization URL is https://www.example.com/cloud/org/myOrg, enter myOrg.
   * **Username -** The user name of an organization administrator or system administrator that has access to the organization.
   * **Password -** The password associated with the user name.
7. Select the networks on the **Local** and **Peer** edge gateways that are to be peered (multi-select)
8. Leave all other settings at default and click **OK**
9. Click **OK again** to close the “Configure Services” dialogue box and commit the configuration change

Both edge gateways will be configured to establish the connection. It can take up to several hours for the connection to stabilize. You may receive warning emails about the connection state transitioning to red and green status during this time period. Once stabilized, the connection status of the VPN connection on each edge gateway should be green.

Firewall rules must be created on both edge gateways to allow the appropriate network communications to occur between the networks that were peered by the VPN connection.

### Remote Network VPN Tunnels

You can create a VPN tunnel between an organization virtual datacenter network that is backed by an edge gateway and a device capable of acting as an IPSEC VPN tunnel endpoint on a remote network.

1. Open the **Configure Services** dialogue for the edge gateway to be configured.
2. Select the **VPN** tab and click **Add…**
3. Enter a **Name** and **Description** for the peering connection
4. Select **Enable this VPN configuration**
5. Set **Establish VPN to**: “a remote network”
6. Select the local Networks networks to be peered (multi-select)
7. Enter a comma separated list of networks at remote site to be peered (in CIDR format).
8. Enter the **Local ID**, **Peer ID**, and **Peer IP** per instructions in the dialogue box
9. Configure **Encryption protocol**, **Shared Key**, and **MTU** to match the configuration of the remote peer.
10. Review the tunnel settings and click **OK**.
11. Click **OK** again to close the **Configure Services** dialogue box.

The edge gateways will be configured to establish the connection.

Review the vendor instructions for your remote endpoint device, and create an appropriate matching configuration on the device.

It may take some time for the connection to establish and stabilize. You may receive warning emails about the connection state transitioning to red and green status during this time period.

Verify on both endpoints that the connection is established - the connection status of the VPN connection on the edge gateway should be green

Firewall rules must be created on the edge gateway and remote endpoint to allow the appropriate network communications to occur between the networks that were peered by the VPN connection.