EduCloud Server: Concepts and Overview

Contents

Overview 1

EduCloud Concepts 1

Organizations 1

Users and Groups 2

Sites 2

Cloud Resources 3

Hosts 3

Compute Tiers 3

Storage Tiers 4

Provider Virtual Datacenter (pVDC) 4

Organization Virtual Datacenter (VDC) 5

Virtual Applications (vApp) 5

Virtual Machines (VMs) 6

Supported Guest Operating Systems 6

Guest OS Customization 7

VMware Tools and Open VM Tools 7

Affinity and Anti-Affinity 8

Snapshots 8

Catalogs 9

Sharing 10

Publish/Subscribe 10

EduCloud Public Catalogs 10

Networking 11

External Network 12

Organization VDC Network 13

vApp Networking 13

Static IP Pools 14

Edge Gateway 14

Multiple Edge Gateways 15

Site to Site Communications 15

Requesting/Mapping Resources 15

Bringing the Concepts Together 17

# Overview

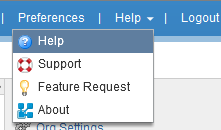
EduCloud Server is a private, higher education cloud service which allows organizations to provision and manage virtual servers at a fraction of the cost of implementing physical servers.

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>

This guide provides an overview of the features available within the EduCloud Server service, the concepts and constructs that underpin the service, and the processes for requesting resources.

Step by step instructions for performing common tasks can be found in the “*EduCloud Server User Guide*” which can be downloaded from the “[Support](https://www.bc.net/service-catalogue/educloud)” section of the EduCloud Server service catalogue.

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”.

# EduCloud Concepts

## Organizations

EduCloud supports multi-tenancy through the use of organizations. An organization is a unit of administration for a collection of users, groups, and computing resources.

Organizations are set up and configured by the EduCloud system administrators.

The organization is then managed by the assigned organization administrators. Organization administrators are responsible for:

* Managing the cloud resources assigned to the organization (via requests to the system administrators)
* Creating organization users and groups and managing the assignment of rights and roles.
* Managing catalogs
* Creating and managing Organization VDC networks
* Managing edge gateway services - firewall access rules, network address translation, static routing, and load balancing.

Organization administrators may delegate some or all of the above responsibilities to other organization users by assigning them appropriate roles.

Organization administrators and users access EduCloud services via their organization URL:

[https://bcnet.educloud.ubc.ca/cloud/org/*<org-name>*/](https://bcnet.educloud.ubc.ca/cloud/org/%3corg-name%3e/)

The EduCloud administrators will provide you with the organization name and URL when setup is complete.

## Users and Groups

An organization can contain an arbitrary number of users and groups.

User accounts can be managed locally or imported from a directory service such as LDAP. Groups must be imported from a directory service – they are not available for local accounts.

Permissions within an organization are controlled through the assignment roles to users and groups.

A full description of the pre-defined roles, and associated rights can be found in the “*vCloud Director Administrator’s Guide*” under “*Roles and Rights*”.

Organization administrators manage all users, groups and assigned roles. They can configure access to an LDAP directory server for user/group management.

## Sites

A site is a geographical location where cloud resources are available. Sites are independent, each having their own physical infrastructure (building, power/generation, cooling), cloud resources, and network uplinks.

Multiple sites can be leveraged for disaster recovery or to build disaster tolerant applications – applications that can continue to function in the event an entire site becomes non-functional.

Sites are currently available in two different geographic locations:

* **Van** – Vancouver
* **Kam** – Kamloops

The site abbreviations (in bold) will appear in EduCloud resource names (e.g. VDCs) to help you identify the site the resource is located at.

Vancouver is located in a moderate to high risk seismic zone, Kamloops in a low risk zone.

## Cloud Resources

Cloud resources are an abstraction of the underlying physical resources used to provide the EduCloud Server service. These resources are:

* Compute – CPU and memory for running virtual servers.
* Storage – disk for storage of operating systems, applications and data.
* Networking – network connectivity and associated features such as firewalls, Network Address Translation (NAT), load balancing, static routes, etc.

Compute and storage are grouped into different performance tiers with associated differences in cost (higher performance = higher cost).

### Hosts

A host is the physical computer on which your virtual machine runs. Your virtual machines can run on any host within the tier they are deployed. The system may automatically move your VM to other hosts to evenly balance loads across the hosts within a tier. Your VM may also be moved when maintenance needs to be performed on a host. These moves occur dynamically and are non-disruptive.

Host failures are infrequent, but when they do occur, all VMs running on that host will experience an outage. The system will detect the host failure and restart all impacted VMs on other hosts within the tier – this typically occurs within 5 minutes of the failure.

How VMs are placed on hosts can be controlled through the use of affinity/anti-affinity rules- described later in this document.

### Compute Tiers

EduCloud Server offers two compute performance tiers – each tier contains hosts with different performance capabilities:

* **Std** – Standard Performance – 2.2 GHz clock speed
* **High** – High Performance – 3.2 GHz clock speed (Kamloops only)

The standard performance tier is the most cost effective and should meet the performance requirements for the majority of your applications.

The high performance tier is available for applications with components that require a higher CPU clock speed and higher degree of dedicated resources in order to achieve the desired application performance.

The performance tier abbreviations (in bold) will appear in EduCloud resource names (e.g. VDCs) to help you identify the performance tier of the resource.

See the service catalogue to obtain tier pricing.

### Storage Tiers

Available storage tiers, tier names, and costs vary by site. See the service catalogue to obtain tier pricing.

|  |  |  |
| --- | --- | --- |
| Vancouver | Kamloops | Description |
| Standard SATA($$) | Standard($$) | Standard performance disk tier designed for everyday application   Provides low to moderate I/O performance. Use for file servers, OS drives, everyday application drives |
| High SAS($$$) | High($$$) | High performance disk tier designed for more demanding I/O workloads   Provides moderate to high I/O performance. Use for high transaction rate DB servers or other I/O intensive workloads that require higher performance than the standard tier. |
|  | Extreme($$$$) | Extreme performance disk tier designed for very I/O intensive workloads  For workloads with very high I/O performance demands. Use for workloads who’s I/O performance cannot be met by the high tier. |

Applications should be deployed and performance validated on the standard disk tier first. Move disks with higher I/O demands to a higher performance tier if performance expectations are not met. Movement of disks between storage tiers is non-disruptive.

All storage tiers are backed up nightly and backups are copied to an offsite location. Backups have the following retention policy:

* Local: 28 daily
* Remote: 28 daily, 12 weekly, and 12 monthly

Standard($$), High($$$), and Extreme($$$$) storage tiers will be made available at the Vancouver site in summer of 2017. The other Vancouver storage tiers will be deprecated and phased out as underlying equipment reaches end of life.

## Provider Virtual Datacenter (pVDC)

A provider virtual datacenter is a collection of physical compute, memory and storage resources that is available to be assigned to organizations. Provider virtual datacenters are created based on the site and the performance capabilities of the assigned compute/memory.

Provider datacenters are created and managed by EduCloud system administrators

## Organization Virtual Datacenter (VDC)

An organization virtual datacenter (VDC) provides a collection of compute, memory and storage resources to an organization. The resources are partitioned out from a provider virtual datacenter. They provide an environment where virtual systems can be stored, deployed and operated. They also provide storage for virtual media, such as CD ROM images.

A single organization can have multiple VDCs - the number depends on the sites and compute performance tiers in which resources are requested. Each VDC will have disk storage from the available disk tiers allocated within it.

An organization using the standard compute performance tier at the Vancouver site + the standard and high performance tiers at the Kamloops site would have three VDCs:

* *<org-name>*-Van-Std
* *<org-name>*-Kam-Std
* *<org-name>*-Kam-High

Organization VDCs are created and resources assigned by the EduCloud system administrators based on the resources requested by your organization administrator.

Organizations are billed for the resources assigned to their VDCs.

## Virtual Applications (vApp)

A vApp (virtual application) is a container that can:

* Contain multiple VMs (virtual machines) - up to 128
* Be powered on, off, or suspended – affecting all VMs they contain
* Control start and stop settings (e.g. start/shutdown order) for each VM they contain
* Be copied or moved as a unit.
* Be added to a catalog so others can deploy copies.
* Contain isolated or routed vApp networks.
* Be shared (read-only, read/write, full-control) with other users in your organization

Service users determine how many VM’s to create and place within a single vApp. When choosing, keep in mind that:

* vApps and their contained VMs cannot span VDCs – all must be deployed in one VDC.
* Some vApp operations (e.g. moving to a different VDC) require the vApp (and therefore all VMs it contains) to be stopped.

A user must have the “*vApp Author*” role to create or modify vApps and the VMs they contain.

A user with the “*vApp User*” role can access a vApp and its VMs, but cannot modify the configuration of a the vApp or the VMs it contains.

More information can be found in the “*EduCloud User Guide*” and the “*vCloud Director Users Guide*” under “*Working with vApps*”.

## Virtual Machines (VMs)

A virtual machine is a “software” computer that, like a physical computer, runs an operating system and applications. Every virtual machine has virtual devices and resources (CPU, memory, disk(s), network adapters, etc.) that provide the same functionality as physical hardware and have additional benefits in terms of portability, manageability, and security.

The virtual machine is the workhorse of the EduCloud service – it runs the operating systems on which your applications run. The CPU, memory, storage and networking associated with each VM can be varied to meet your application needs.

Note that:

* A VM must be contained within a vApp
* The vApps VDC determines the site and compute tier where the VM runs
* A default disk tier is selected when the VM is created.
* The default tier can be overridden/changed for each attached disk. (i.e. The VM can have multiple disks on different storage tiers).

More information can be found in the “*EduCloud User Guide*” and the “*vCloud Director Users Guide*” under “*Working with Virtual Machines*”.

### Supported Guest Operating Systems

A guest operating system is the operating system that runs within a VM.

The following Microsoft Windows guest operating systems are supported. Unless stated otherwise, all OS variants and 32-bit/64-bit editions are supported. Unless specified, all SP, minor and maintenance versions are supported.

* Microsoft Windows Server 2012 R2 64-bit
* Microsoft Windows Server 2012 64-bit
* Microsoft Windows 10
* Microsoft Windows 8
* Microsoft Windows 7
* Microsoft Windows Server 2008 R2 64-bit
* Microsoft Windows Server 2008
* Microsoft Windows Server 2003
* Microsoft Windows Small Business Sever 32-bit
* Microsoft Windows Vista
* Microsoft Windows XP Professional

The following UNIX and Linux guest operating systems are supported. Unless stated otherwise, all OS variants and 32-bit/64-bit editions are supported. Unless specified, all SP, minor or maintenance versions are supported.

* Red Hat Enterprise Linux 4-7
* SUSE Enterprise Linux 10-12
* Oracle Linux 4-7
* CentOS
* Ubuntu Linux
* Other 3.*x* Linux
* Other 2.6.*x* Linux
* Other 2.4.*x* Linux
* Other Linux

### Guest OS Customization

Guest OS customization customizes the configuration of the guest operating system after it has been copied or deployed from a template.

The customization process updates the administrator/root password, hostname, and network settings based on the information you supply when deploying the VM and ensures there are no hostname or network (IP address, mac address) conflicts.

It will run the first time a VM is powered on after it is deployed from a template. You can also initiate guest customization any time you power on a VM. Customization must be re-run after some hardware configuration changes are made (e.g. adding or changing a network) to properly apply the new settings within the guest OS.

The guest OS must have VMware tools or open-vm-tools installed in order for guest customization to work. In some cases, additional components need to be installed in the guest for guest OS customization to work properly.

### VMware Tools and 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 http://partnerweb.vmware.com/GOSIG/home.html.

### Affinity and Anti-Affinity

Affinity and anti-affinity rules allow you to control how the system places VMs across the different hosts in the cluster/compute tier.

An affinity rule specifies that a group of VMs should be placed on the same host whenever possible. In some cases, this can improve performance by reducing network latency for communications between the VMs.

An anti-affinity rule specifies that a group of VMs should be placed on different hosts whenever possible, minimizing how many VMs are impacted when a single host fails. Often used for a group of VM’s that are being load balanced.

More information can be found in the “*vCloud Director Users Guide*” under “*Working with Virtual Machines 🡪Virtual Machine Affinity and Anti-affinity*”.

## 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.

Snapshots do not capture VM networking configuration – any networking changes made after the snapshot is taken will not be reverted if you roll back to a snapshot.

Organization administrators will receive daily warning emails for any VM or vApp that has a snapshot in place for more than seven days. The snapshots will be automatically removed after fourteen days.

More information about vApp and VM level snapshots can be found in the “*EduCloud Users Guide” under “Snapshots” and in the* “*vCloud Director Users Guide*” under “*Working with vApps*” and “*Working with Virtual Machines*”.

## Catalogs

Catalogs store vApp templates and media files (e.g. DVD .iso files). The catalog can be made available to users within your organization and also to other organizations (via publishing).

Users with access to the catalog can deploy their own vApps from any of the vApp templates stored in the catalog. They can also attach any media stored in the catalog to a VM.

If your organization uses multiple EduCloud sites, and has vApps or VMs that will be frequently deployed at those sites, we recommend you maintain a copy of your catalogs 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 the other sites.

When deploying a vApp or VM from catalogs, where possible select from a catalog located at the same site you are deploying to. Deploying from a catalog located at the same site is far more efficient than deploying cross site (e.g. deploying in Kamloops from a catalog in Vancouver). Cross-site deployments can take 30 to 60 minutes to complete. Same-site deployments typically complete in under 5 minutes.

Media files in a catalog can be attached to virtual machines – e.g. a .iso file can be attached to a VM as a virtual CDROM drive. For best performance, select media from a catalog located at the same site.

An organization administrator or user with the “*Catalog Author*” role can create/upload/manage vApp templates and media files.

More information can be found in the “*EduCloud User Guide*” under “*Using Catalogs*”, in the “*vCloud Director Administrators Guide*” under “*Working with Catalogs*”, and in the “*vCloud Director Users Guide*” under “*Working with Catalogs*” and “*Working with vApp Templates*”

### Sharing

Catalogs can be shared to specific users or groups, or to all users within your organization. Sharing to other organizations is not permitted/enabled.

### Publish/Subscribe

Publishing a catalog makes it available for any vCloud organization (within or outside of EduCloud) to subscribe to. A published catalog will be assigned a URL, and a password can be used to restrict whom is allowed to subscribe to the catalog.

Any vCloud organization that knows both the URL and password of the published catalog, can create a subscribed catalog that is linked to it. All items in the published catalog will be synchronized to all subscribed catalogs. The subscribed catalog will consume the same amount of disk space within your organization as the space used by the published catalog.

This mechanism can be used to share your catalogs with other EduCloud organizations, or even within your organization to synchronize a copy of your catalog across multiple sites.

### EduCloud Public Catalogs

The EduCloud administrators maintain a public catalog that contains the following OS images:

* Red Hat Enterprise Linux 6 64-bit
* Red Hat Enterprise Linux 7 64-bit
* Ubuntu Linux 14.04 LTS 64-bit
* Ubuntu Linux 16.04 LTS 64-bit
* Windows 8.1 Enterprise 64-bit
* Windows 10 Enterprise 64-bit
* Windows Server 2012 R2 Standard

All organizations can deploy vApps/VMs contained in the public catalog, but are responsible for obtaining proper licensing for each copy of the operating system being deployed.

A copy of the catalog is maintained at each EduCloud site:

* EduAdmin-Kam – Kamloops catalog
* EduAdmin-Van – Vancouver catalog

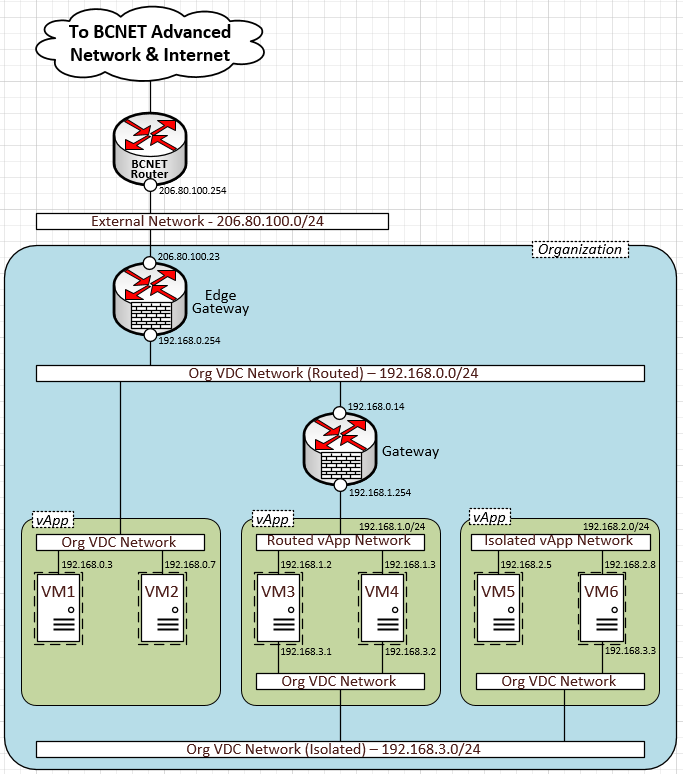
For fast and efficient provisioning, be sure to select from the catalog located at the same site as the services you are deploying.

The EduCloud public catalog OS images fully support guest OS customization and are patched and tested monthly

## Networking

There are 3 layers of networking in EduCloud:

1. External Networks
2. Organization VDC Networks
3. vApp Networks



### External Network

An external network is a network that can be directly routed by the underlying physical network infrastructure located at each EduCloud site. In the EduCloud service, external networks provide the connectivity between the external interface of organization edge gateways and the BCNET Advanced network.

External networks cannot be directly accessed by VMs within an organization – only via the edge gateways.   
  
Only EduCloud system administrators create and manage external networks.

### Organization VDC Network

An organization VDC network is contained within an organization VDC and is available to all the vApps within the VDC. It allows vApps within a VDC to communicate with each other.

Organization VDC networks can be either:

* Isolated - only allowing communication amongst attached VMs.
* Routed - attached to an edge gateway to provide routed connectivity to other organization VDC networks, or the BCNET Advanced network via the external interface/gateway network.

An organization VDC network can also be shared – making it available for use across all VDCs located at the same site (but not across sites).

Organization VDC Networks are created and managed by organization administrators.

### vApp Networking

When building a vApp you must configure the networks that the VMs within the vApp can connect to. You can configure 3 types of networks:

* Org VDC network – maps an existing org VDC network (isolated or routed) into the vApp to allow VMs to be connected directly to the org VDC network.
* Isolated vApp Network – A network that is available only to VMs within the vApp. There is no connection to any other networks.
* Routed vApp Network – A network that is available only to VMs within the vApp, and that is connected to an org VDC network via a gateway that provides routing, and optionally DHCP, NAT and Firewall services.

Routed vApp networks are isolated from other networks – VMs within the vApp can consume the same IPs as VMs in other vApps. This is very useful for repeated deployment of classroom lab or test environments.

Note that use of routed vApp networks is not recommended for critical workloads with high availability requirements - the gateway appliance used to provide network services for a routed vApp network cannot be configured for high-availability (failover).   
  
More information on working with vApp networks can be found in the “*EduCloud User Guide*” and in the “*vCloud Director User’s Guide*” under “*Working with vApps 🡪 Working with networks in a vApp*”

Users with the “vApp Author” or higher role can create and manage vApp networking.

### Static IP Pools

When defining networks, you define a pool (ranges) of static IP’s to be used on the network. When a VM NIC is connected to the network and configured for mode “Static – IP Pool”, an IP is automatically assigned from the pool and associated with the VM NIC. The IP address is automatically configured in the guest operating system when guest customization is run on first power on (or whenever you force guest re-customization).

### Edge Gateway

An edge gateway is a virtual router for routing traffic between your organization VDC networks and external networks. It also provides a suite of additional network services that can be enabled and used:

|  |  |
| --- | --- |
| Service | Description |
| DHCP | Simple DHCP services for automatic IP address assignment. No MAC address pinning so VM could get different IP after lease expiry. |
| NAT | Both source (SNAT) and destination (DNAT) network address translation |
| Firewall | Packet filtering firewall to control inbound/outbound access to each attached network. |
| Static Routing | Configure and manage static routes |
| VPN | IPSec VPN service. Establish site-to-site VPN between EduCloud edge gateways or third party VPN gateways. |
| Load Balancing | Load balancing services for TCP, HTTP, and HTTPS traffic (no SSL offload) |

Edge gateways can be deployed in several sizes (to meet different network bandwidth needs), and can be configured for high availability, which enables automatic failover to a backup instance running in a separate VM. Each edge gateway supports up to 10 network interfaces.

The uplink interface is typically connected to an external network used to route data between the BCNET advanced network and the organization VDC networks deployed at a site. Public IP addresses on the external network are allocated for use by your organization - one is consumed for the edge gateway IP address, the others can be used for NAT or load balancing virtual IPs.

The uplink network will use public IP addresses, while the internal networks will typically use private IP addresses. NAT or load balancing is used to make any servers publicly accessible.

More information on managing edge gateways and associated services can be found in the “*EduCloud Networking Guide*” and in the “*vCloud Director Administrator’s Guide*” under “*Managing Cloud Resources 🡪 Managing Edge Gateways*”

Edge gateways are created by and global configuration performed by EduCloud system administrators (e.g. connecting to external network, assigning public IPs). Organization administrators can add organization VDC networks to the edge gateway (consumes a network interface) and manage all gateway services.

### Multiple Edge Gateways

Each site has independent networking and requires its own edge gateway to manage routing and extended features (firewall, load balancing, VPN, etc.) for that site. If your organization is utilizing resources at both the Vancouver and Kamloops sites, it will have two edge gateways attached to it. Each edge gateway will have a different pool of public IPs allocated to it.

### Site to Site Communications

Communications between services hosted in different EduCloud Server sites will occur through each site’s edge gateway and across the BCNET Advanced Network. You cannot directly route private IP space between the sites – you must either:

* Provide public IPs (via NAT or other means) to servers that must communicate across sites
* Set up a site to site IPsec VPN connection between edge gateways to allow secure direct routing of private IP between sites

Avoid overlapping IP assignments for your Org VDC networks (e.g. assigning 192.168.0.0/24 in both Vancouver and Kamloops) or you will be unable to establish a site to site VPN connection.

Developing a private IP assignment strategy can simplify the site to site setup and routing rules. For example:

* 192.168.0.0/19 – Range used for Org VDC Networks – Vancouver
* 192.168.32.0/19 – Range used for Org VDC Networks – Kamloops

Traffic on the site-to-site connection will traverse the edge gateway firewall – when setting up VPN connections, also be sure to add appropriate firewall rules to allow communication through the connection.

# Requesting/Mapping Resources

When requesting net-new services or adding tiers:

* Review the service catalogue for available sites, the compute and storage tiers offered at each site, and the resource pricing for each site/tier
* Specify which sites services need to be deployed in.
* For each of the sites provide:
  1. The number of public IPs required
  2. The compute performance tiers that will be used.
* For each site and compute performance tier, provide:
  1. The amount of CPU (in GHz) and memory (in GB) to be allocated in the tier.
  2. The storage tiers required, and the amount of space to allocate in each tier (in GB or TB).

The services will be mapped into your organization as follows:

* An edge gateway will be created for each site at which services will be deployed
* The requested number of public IPs will be assigned to each edge gateway
* An organization virtual datacenter (VDC) will be created for each site+compute performance tier you request.
* The storage you requested for each compute tier will be assigned to its associated VDC.

When requesting resource changes, be sure to specify the VDC and which resources need to be increased, decreased, added or removed.

# Bringing the Concepts Together

This example runs through the request, provisioning and deployment process for the EduDemo organization. It demonstrates how compute, storage and networking (Edge-gateways, organization VDC networks) map into your EduCloud organization, and how some simple applications might be deployed.

The following request for resources was received from the EduDemo administrator:

|  |  |
| --- | --- |
| Site: Vancouver |  |
| Public IPs: | 12 |
| Compute Tier: Standard Performance |  |
| CPU | 15 GHz |
| Memory | 50 GB |
| Storage Tier: Standard SATA($$) | 50 TB |
| Storage Tier: High SAS($$$) | 30 TB |
|  |  |
| Site: Kamloops |  |
| Public IPs: | 8 |
| Compute Tier: Standard Performance |  |
| CPU | 10 GHz |
| Memory | 32 GB |
| Storage Tier: Standard($$) | 50 TB |
| Storage Tier: High($$$) | 20 TB |
| Compute Tier: High Performance |  |
| CPU | 20 GHz |
| Memory | 64 GB |
| Storage Tier: Standard($$) | 50 TB |
| Storage Tier: High($$$) | 20 TB |
| Storage Tier: Extreme($$$$) | 10 TB |

The EduCloud administrators’ provision:

**Organization**

The EduDemo organization. The organization administrator is provided with an account with organization administrator permissions and the URL for accessing the organizations EduCloud web portal.

**Virtual Datacenter**

The **EduDemo-Van-Std** VDC is created at the Vancouver site – 15GHz of standard performance CPU and 50 GB of memory are allocated to the VDC. 50 TB of Standard SATA ($$) and 30TB of High SAS($$$) storage are allocated to the VDC.

The **EduDemo-Kam-Std** VDC is created at the Kamloops site – 10GHz of standard performance CPU and 32 GB of memory are allocated to the VDC. 50 TB of Standard($$) and 20TB of High($$$) storage are allocated to the VDC.

The **EduDemo-Kam-High** VDC is created at the Kamloops site – 20GHz of high performance CPU and 64 GB of memory are allocated to the VDC. 50 TB of Standard($$), 20TB of High($$$) and 10TB of Extreme($$$$) storage are allocated to the VDC.

**Edge Gateway**

The **EduDemo-Van-Std-01** edge gateway is created at the Vancouver site. Its external interface is attached to the “Van-Gateway” external network and assigned the public IP address 103.40.50.27. Eleven additional IP addresses (.28 through .38) are reserved for use by edge gateway services (e.g. NAT).

The **EduDemo-Kan-Std-01** edge gateway is created at the Kamloops site. Its external interface is attached to the “Kam-Gateway” external network and assigned the public IP address 206.80.100.12. Seven additional IP addresses (.13 through .19) are reserved for use by edge gateway services (e.g. NAT).

The external “Gateway” networks provide connectivity to the BCNET Advanced Network and internet via the local BCNET routers.

The organization administrator provisions:

**Org VDC Networks**

The **DMZ-Van** organization VDC network is created at the Vancouver site. Subnet 192.168.1.0/24 is assigned to the network. The gateway IP address is set to 192.168.1.254, and the remaining IPs on the subnet are assigned to the networks IP pool.

The **DMZ-Kam** organization VDC network is created at the Vancouver site. Subnet 192.168.32.0/24 is assigned to the network. The gateway IP address is set to 192.168.32.254, and the remaining IPs on the subnet are assigned to the networks IP pool. The “shared” option is selected so the network is available in all VDCs at the site.

**Site-to-Site VPN**

Servers on the DMZ-Kam and DMZ-Van network need to communicate directly with each other. To achieve this, VPN services are enabled on the edge gateway, and a site-to-site VPN configuration entered to peer the DMZ-Van (192.168.1.0/24) and DMZ-Kam (192.168.32.0/24) networks. Firewall rules are created on both the Kamloops and Vancouver edge gateways to allow all IP traffic to flow between these networks.

**vApps/VMs**

The **Email** vApp and associated VMs is built and deployed in the EduDemo-Van-Std VDC. IP addresses are assigned to VM NICs from the network pool. OS Images are selected from the EduAdmin-Van public catalog.

The **DataMart** and **WebSite** vApps and associated VMs are built and deployed in the EduDemo-Kam-High and EduDemo-Kam-Std VDCs. IP addresses are assigned to VM NICs from the network pool. OS Images are selected from the EduAdmin-Kam public catalog.

**NAT/Firewall**

The DataMart and WebSite applications each have a web interface that must be made publicly available on port 443. A NAT rule is put in place for each application to provide a public IP. Firewall rules are put in place to allow access to port 443.

The Email application must make SMTP services publicly available on port 25. A NAT rule is put in place to provide a public IP. A Firewall rule is put in place to allow access to port 25.

The following diagram provides a visual representation of the deployed services:

