Cloud Provisioning Models and User Roles

Version 1.2 – June 2024

Abstract

In a small installation with a few hosts you can use OpenNebula without giving much thought to infrastructure partitioning and provisioning. Yet, for medium and large-scale deployments you will probably want to provide some level of isolation and structure. OpenNebula offers a flexible and powerful cloud provisioning model based on Virtual Data Centers (VDCs) that enables an integrated, comprehensive framework to dynamically provision infrastructure resources in large multi-data center and multi-cloud environments to different customers, business units or groups. Another key management task in an OpenNebula Infrastructure environment involves determining who can use the cloud administrative interfaces and what tasks those users are authorized to perform. This white paper is meant for cloud architects, builders and administrators, to help them understand the OpenNebula models for managing and provisioning virtual resources, and default user roles in OpenNebula.

Contents

1. What is OpenNebula?
2. The Infrastructure Perspective
3. The Organizational Perspective
4. Examples of Provisioning Use Cases
5. Cloud Access Roles
6. Conclusions

Glossary

CLI	Command-Line Interface
OCA	OpenNebula Cloud API
VM	Virtual Machine
VDC	Virtual Data Center

1. What is OpenNebula?

OpenNebula is a **powerful, but easy-to-use, open source solution to build and manage Enterprise Clouds**. It combines existing virtualization technologies with advanced features for multi-tenancy, automatic provision and elasticity to offer on-demand applications and services. OpenNebula provides a single, feature-rich and flexible platform with **unified management of IT infrastructure and applications** that **avoids vendor lock-in** and **reduces complexity, resource consumption and operational costs**. OpenNebula manages:

- **Any Application**: Combine containerized applications from Kubernetes with Virtual Machine workloads in a common shared environment to offer the best of both worlds: mature virtualization technology and orchestration of application containers.
- **Any Infrastructure**: Open cloud architecture to orchestrate compute, storage, and networking driven by software.
- **Any Cloud**: Unlock the power of a true hybrid, edge and multi-cloud platform by combining your private cloud with infrastructure resources from third-party virtual and bare-metal cloud providers such as AWS and Equinix Metal, and manage all cloud operations under a single control panel and interoperable layer.
- **Any Time**: Add and remove new clusters automatically in order to meet peaks in demand, or to implement fault tolerance strategies or latency requirements.

OpenNebula provides the necessary tools for running containerized applications from Kubernetes and Docker Hub, while ensuring enterprise requirements for your DevOps practices. It helps organizations to easily embrace Multi-cloud, Hybrid and Edge Computing, allowing them to grow their Enterprise Cloud on-demand with infrastructure resources from third-party Public Cloud and bare-metal providers such as Amazon Web Services (AWS) and Equinix Metal.

This white paper describes the OpenNebula models for managing and provisioning virtual resources, and the default user roles.If you are interested in building an OpenNebula cloud on premises using open source technologies, please refer to our Open Cloud Reference Architecture.[1] If interested in transitioning from a VMware environment to an OpenNebula cloud ecosystem, please refer to our white paper on Migrating from VMware to OpenNebula.[2]

The development of OpenNebula follows a bottom-up approach driven by the real-world needs of sysadmins, DevOps and corporate users. OpenNebula is an **open source product** with a healthy and active community, commercially supported by OpenNebula Systems through its **OpenNebula Subscription**. Updates are released on a regular basis and delivered as a single package with a smooth migration path. For more information on the benefits of running an OpenNebula cloud, please refer to the Key Features page.[3]

2. The Infrastructure Perspective

A standard OpenNebula Cloud Architecture consists of the **Cloud Management Cluster**—comprising the Front-end master node(s)—and the **Cloud Infrastructure**—comprising one or several workload Clusters with the hypervisor nodes and the storage system. Clusters may reside at multiple geographical locations, all interconnected with multiple networks for internal storage and node management and for private and public VM communications.

Workload Clusters can shape different architectures and software/hardware execution environments to

[1] https://support.opennebula.pro/hc/en-us/articles/204210319-Open-Cloud-Reference-Architecture-White-Paper
[2] https://support.opennebula.pro/hc/en-us/articles/17225311830429-Migrating-from-VMware-to-OpenNebula-White-Paper
[3] https://opennebula.io/discover/

fulfill the needs of different workload profiles. Moreover, many organizations access external public clouds through which they can build true hybrid and edge cloud environments. These environments increase the private capacity of their data centers with resources from external providers, so that they can address peaks in demand, increase service availability or meet requirements for data location or low latency.

Generally speaking, two types of Cluster models can be used with OpenNebula:

- **Edge Clusters:** can be deployed on-demand both on-premises and on public cloud and edge providers, with a high degree of integration and automation.
- **Customized Clusters:** typically deployed on premises to meet specific requirements.

As an example, a company owns two data centers in two different geographic locations: one on the US West Coast, the other in Europe. It also has an agreement with a public cloud provider such as AWS or Equinix. This company can use a single Opennebula Zone for the two data centers, where each data center is configured as a cluster; or, alternatively, each data center can run its own Zone or its own full OpenNebula deployment. If the cloud includes multiple OpenNebula Zones, these can be configured as a federation, in which case they share the same user accounts, groups and permissions across data centers. This type of multi-Zone deployment is typically chosen when data centers reside in different administrative domains, or when connectivity between data centers does not meet requirements for bandwidth and/or latency.

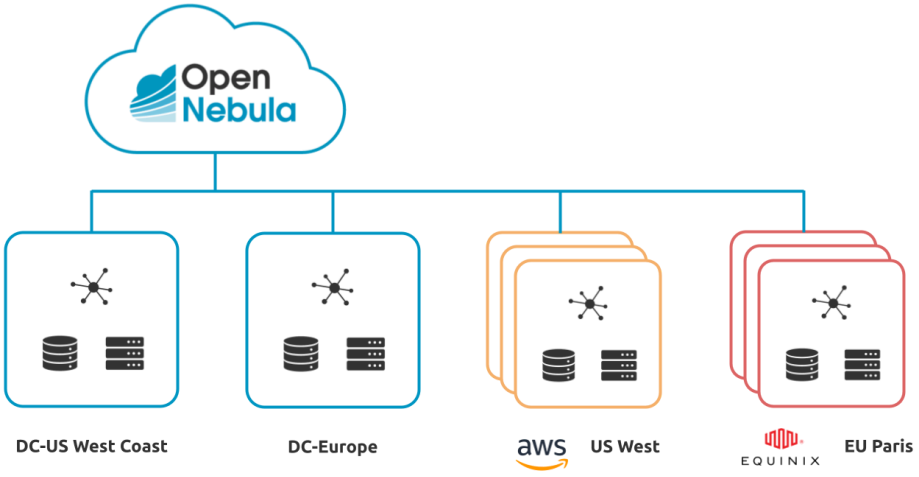

Figure1: Example of VDC resources.

3. The Organizational Perspective

Users are organized into Groups (similar to what other platforms call Projects, Domains or Tenants). A Group is an authorization boundary—it may be considered a business unit if part of a private cloud, or as a separate company if based on a public cloud. While Clusters are used to group physical resources according to common characteristics, such as networking topology or physical location, Virtual Data Centers (VDCs) allow OpenNebula cloud administrators to define “logical” pools of physical resources (which may belong to different Clusters and Zones) and allocate them to specific Groups of users.

A VDC is a fully-isolated virtual infrastructure environment where a Group of users (or, sometimes, several Groups of users), under the control of a Group administrator, can create and manage virtual compute and

storage resources. Users in the Group, including the Group admin, see only these virtual resources and not the underlying physical infrastructure. The physical resources allocated to the Group are managed by the cloud administrator through the VDC. The resources grouped in the VDC can be dedicated exclusively to the Group, thereby also providing isolation at the physical level.

It is also possible to configure the privileges of the Group users and Group admin in relation to what operations they can perform over virtual resources created by other users. For example, in a typical cloud provisioning use case, the users can instantiate VM templates to create the virtual resources they need, while the admins of the Group have full control over other users' resources and can also create new users in the Group.

Users can access their resources through any of the existing OpenNebula interfaces, such as the OpenNebula FireEdge GUI, the CLI, the OpenNebula Cloud API (OCA) or the AWS APIs. Group admins can manage their Groups through the CLI or via the Group Admin View in FireEdge. Cloud administrators can manage the Groups through the CLI or FireEdge.

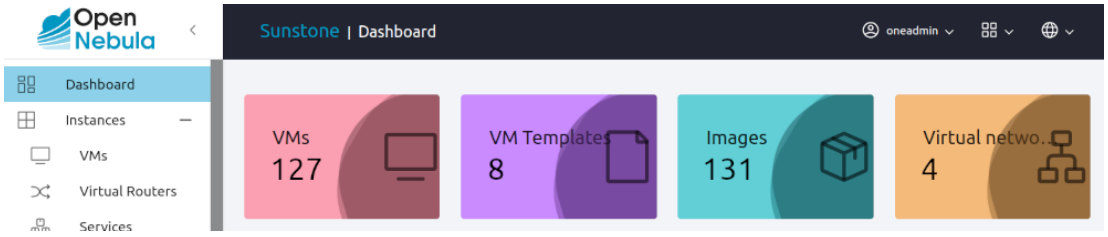

Figure 2: The Dashboard in the FireEdge GUI.

The cloud provisioning model based on VDCs offers the possibility of creating an integrated, comprehensive framework to dynamically provision infrastructure resources in large multi-data center environments to different customers, business units or groups. This approach brings several benefits:

- Effective partitioning of physical resources between Groups of users
- Complete isolation of users, organizations or workloads
- Allocation of Clusters with different levels of security, performance or High Availability (HA)
- Containers for the execution of software-defined data centers
- The possibility of hiding underlying physical resources from Group members
- Simple federation, scalability and cloud bursting of private cloud infrastructures beyond a single cloud instance and data center

4. Examples of Provisioning Use Cases

The following are common enterprise use cases in large cloud computing deployments:

- **On-premises Private Clouds** serving multiple projects, departments, units or organizations: On-premises private clouds in large organizations require powerful and flexible mechanisms to manage access privileges to the virtual and physical infrastructure and to dynamically allocate available resources. In these scenarios, the Cloud Administrator defines a VDC for each department, dynamically allocating resources according to their needs and delegating the internal administration of the Group to the department IT administrator.

- **Cloud Providers** offering Virtual Private Cloud Computing: In this type of service, customers can access a fully-configurable and isolated environment where they have full control and capacity to administer users and resources. This scenario combines a public cloud with the control usually seen in a personal private cloud system.

For example, you can think of Web Development, Human Resources, and Big Data Analysis as business units represented by Groups in a private OpenNebula cloud, and allocate them resources from your data centers and public clouds in order to create three different VDCs:

- VDC Magenta for the Web Development Team, with 2 Clusters in the US (on-premises), 1 Cluster in Europe (on-premises), 1 remote Cluster on AWS (US West) and 1 remote Cluster on Equinix Metal (Paris, Europe)
- VDC Yellow for Human Resources, with 1 Cluster in the US (on-premises), 1 Cluster in Europe (on-premises), 2 remote Clusters on AWS (US West) and 1 remote Cluster on Equinix Metal (Paris, Europe)
- VDC Green for Big Data Analysis, with 1 Cluster in the US (on-premises), 2 Clusters in Europe (on-premises), 1 remote Cluster on AWS (US West) and 2 remote Clusters on Equinix Metal (Paris, Europe).

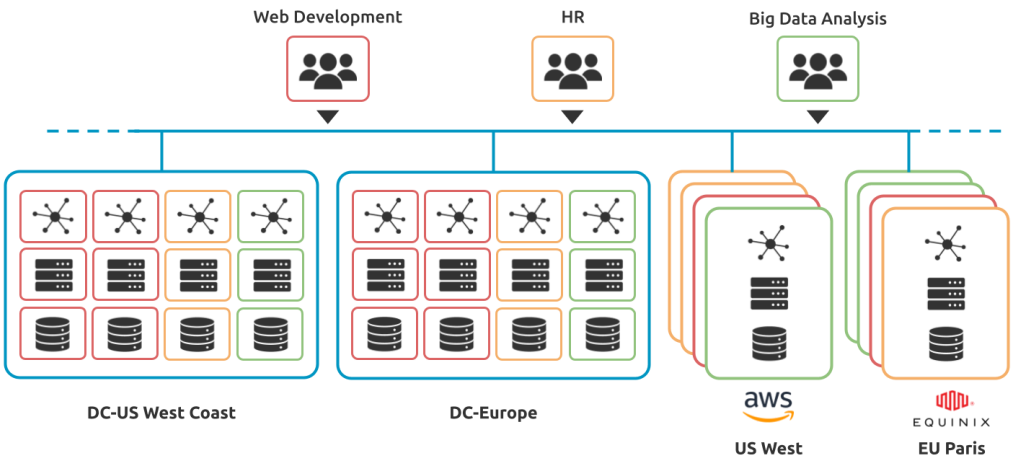

Figure 3: Example of VDC organization

5. Cloud Access Roles

In any OpenNebula infrastructure environment, a key management decision is deciding which users can access the cloud administration interfaces, and what tasks they are authorized to perform. The person with the role of cloud service administrator is authorized to assign the appropriate rights required by other users. Generally speaking, only a very limited number of people should be granted administrator privileges.

This section explains the concept of roles and introduces you to the default type of user roles. The OpenNebula documentation provides information to help in the design of custom roles, and gives recommendations for how to work with roles and privileges in OpenNebula.

Cloud Users

Cloud Users use the CLI or the **User View in FireEdge** to perform the following actions:

ROLE	CAPABILITIES
Cloud User	• **Defining and instantiating virtualized applications**, by following virtual machine service workflows that include one or more VMs. These workflows use templates and images defined by cloud operators, saved from previous running applications or from connected public or private Marketplaces(cluster location is selected depending on the network). • **Managing the life cycles of applications execution**, including elasticity, backups and snapshot policy for fault tolerance. • **Monitoring application information and status**, including IP addresses. • **Managing user accounts**, including language, usage, quotas and SSH keys to access VMs.

An OpenNebula cloud can offer VDCs on-demand to Groups of users (projects, companies, departments or business units). In these cases, each Group can define one or more users as **Group Admins**. Users with Group Admin privileges can also create new Users in the Group, operate on the Group's VM and disk images, share saved Templates with the members of the Group, and check Group usage and quotas. Group Admins typically access the cloud by using the CLI or the **Group Admin View in FireEdge**.

OpenNebula also offers a **Cloud View** interface for users that require a much more limited range of operations. This is a very intuitive, simplified web interface that allows users to launch Virtual Machines from predefined templates, as well as access their VMs and perform basic operations like shutdown. Users can save changes to a VM disk, but cannot create new images.

Cloud Service Administrators (Operators)

Cloud Administrators typically access the cloud using the CLI or the FireEdge web GUI.

ROLE	CAPABILITIES
Cloud Operator	• Using OneProvision to **automatically deploy and configure Edge Clusters** on remote cloud and edge providers. • **Monitoring and managing Clusters and resources** (hosts, networks and datastores) • **Creating and managing users, Groups and VDCs**, including assigning quota limits, and Groups and cloud resources to VDCs • Connecting to **external marketplaces** (e.g. the OpenNebula Public Marketplace) and maintaining contents of any **private marketplaces** • Preparing and managing **Virtual Networks**, **Virtual Machine Images**, **Virtual Machine Templates** and **Multi-VM Service Templates** for use by cloud users • **Managing the extended lifecycle** of Virtual Machine instances and workflows • Generating reports for activity, **accounting** and **showback**

Cloud Operators often provide support to Cloud Users in any aspect related to the Cloud Service.

Cloud Infrastructure Administrators

Cloud Infrastructure Administrators typically perform the following actions:

ROLE	CAPABILITIES
Cloud Admin	• **Installing and configuring OpenNebula** front-end services, namely Core, Authentication, FireEdge, OneFlow and OneGate • **Deploying and configuring Clusters and resources** (hosts, network and datastores) and managing their integration with the underlying infrastructure services: computing nodes, networking fabric and storage servers • Monitoring the **status** and **health** of the cloud services and the infrastructure resources

Cloud Admins often provide support to Cloud Operators and perform any corrective and periodic preventive maintenance tasks related to the infrastructure:

- Capacity planning to match demand with available resources
- Tuning and maintenance of OpenNebula and other software components
- Updates and security patches of OpenNebula and other software components

6. Conclusions

The choices made in designing an enterprise cloud architecture derive from a combination of needs and pre-existing factors such as available data centers and their geographic location, as well as the organizational needs and characteristics of businesses and individual business units.

Defining cloud provisioning models and user roles is a key element in the successful design and implementation of a cloud infrastructure. The capabilities offered by OpenNebula open a wide array of design possibilities for an enterprise cloud. In particular, the cloud provisioning model based on VDCs enables an integrated, comprehensive framework to dynamically provision the infrastructure resources in large multi-data center environments to different customers, business units or groups.

OpenNebula Systems offers Enterprise support for the complete cloud software stack through its OpenNebula **Software Subscription,** which greatly facilitates achieving stability and optimal performance in your OpenNebula infrastructure. Subscribers to OpenNebula's Enterprise Edition can access the Enterprise repository and tools, as well as the Enterprise Portal and the exclusive contents of its Knowledge Base. Standard and Premium Plans offer the assurance and security of counting on OpenNebula experts, who provide support for your solution according to SLA guidelines. The resultant savings in time and resources dedicated to the design and operation of their cloud infrastructure becomes a competitive advantage, by enabling companies to increase their focus on business workloads.

LET US HELP YOU DESIGN, BUILD AND OPERATE YOUR CLOUD

CONSULTING & ENGINEERING

Our experts will help you design, integrate, build and operate an OpenNebula cloud infrastructure

OPENNEBULA SUBSCRIPTION

Get access to our Enterprise Edition and to our support and exclusive services for Corporate Users

CLOUD DEPLOYMENT

Focus on your business and let us take care of setting up your OpenNebula cloud infrastructure

Sign up for updates at OpenNebula.io/getupdated

Rev1.2_20240601