Cloud Provisioning Models and User Roles

Version 1.0 – March 2021

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 the infrastructure resources in large multi-datacenter and multi-cloud environments to different customers, business units or groups. Another key management task in an OpenNebula Infrastructure environment has to do with determining who can use the cloud 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 the default user roles.

Contents

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 virtualization and container technologies with 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 containers 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**: Unlock the power of a true hybrid and multi-cloud platform by combining edge, public, hosted and private cloud operations.
- **Any Virtualization**: Integrate multiple types of virtualization technologies to meet your workload needs, from a fully virtualized environment to system containers and serverless deployments.

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. OpenNebula supports a number of virtualization technologies, including VMware and KVM virtual machines for fully virtualized clouds, LXC system containers for container clouds, and Firecracker microVMs for serverless deployments.

This white paper describes the OpenNebula models for managing and provisioning virtual resources, and the default user roles. If you are interested in designing and deploying a multi-cloud or edge cloud with OpenNebula, please refer to our Edge Cloud Reference Architecture.[1] If you are interested in designing and deploying an OpenNebula cloud on-premises on top of VMware vCenter, please refer to our VMWare Cloud Reference Architecture.[2] If you are interested in building an OpenNebula cloud on-premises using open source technologies, please refer to our Open Cloud Reference Architecture.[3]

The development of OpenNebula follows a bottom-up approach driven by the real need 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**. Releases are produced on a regular basis and delivered as a single package with a smooth migration path. More information on the benefits of running an OpenNebula cloud can be checked on the key features page.[4]

2. The Infrastructure Perspective

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

Those wordload Clusters could present different architectures and software/hardware execution environments to fulfill the needs of different workload profiles. Moreover, many organizations have access

[1] https://support.opennebula.pro/hc/en-us/articles/360050302811-Edge-Cloud-Architecture-White-Paper
[2] https://support.opennebula.pro/hc/en-us/articles/206652953-VMware-Cloud-Reference-Architecture-White-Paper
[3] https://support.opennebula.pro/hc/en-us/articles/204210319-Open-Cloud-Reference-Architecture-White-Paper
[4] https://opennebula.io/discover/

to external public clouds through which they can build true hybrid and edge cloud scenarios where the private capacity of their data centers is expanded with resources from external providers so that they can address peaks of demand, increase service availability or meet data location or low latency requirements.

Generally speaking, there are two types of Cluster models that 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 these are deployed on-premises to meet specific requirements.

Large companies with multiple data centers can run multiple OpenNebula front-end instances (known as "Zones"). For example, a company could have two data centers in different geographic locations, US West Coast and Europe, and an agreement with a public cloud provider such as AWS or Equinix. The company could have a single OpenNebula Zone for both data centers and configure each data center as a Cluster or, alternatively, each data center can run its own Zone or full OpenNebula deployment. Multiple OpenNebula Zones can be configured as a federation, and in this case they will share the same user accounts, groups, and permissions across data centers. A multi-zone deployment is chosen when data centers are in different administrative domains or when the connectivity across data centers does not meet latency and bandwidth requirements.

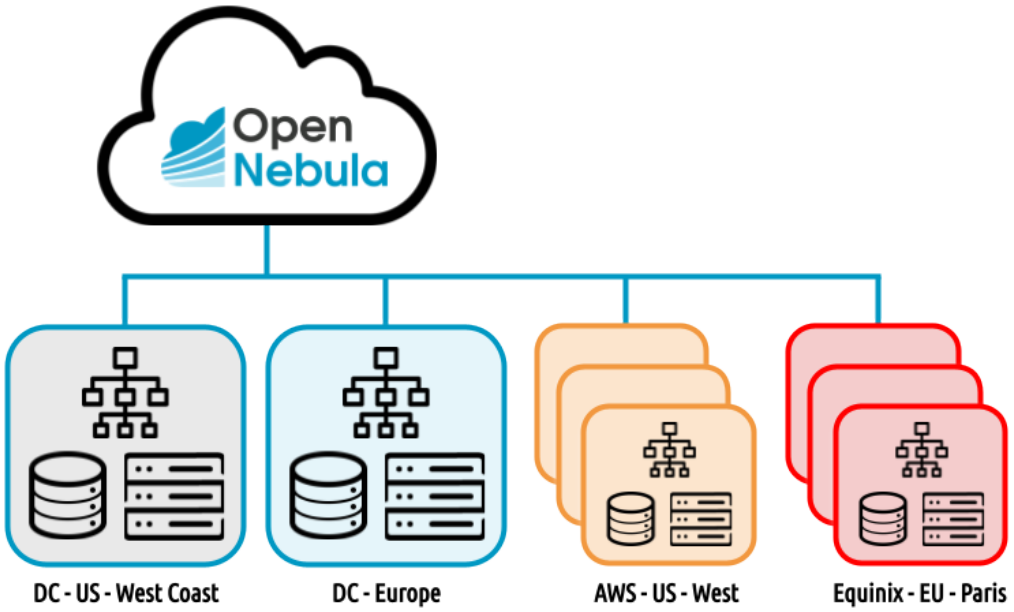

Figure1: Example of VDC resources.

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 that can be seen as a business unit if you are considering it as part of a private cloud, or as a separate company if it is 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 admins to define "logical" pools of physical resources (which could 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 admin, can create and manage virtual compute and storage

resources. The users in the Group, including the Group admin, would only see 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, providing isolation at the physical level too.

The privileges of the Group users and the admin regarding the operations over the virtual resources created by other users can be configured too. 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 WebUI (Sunstone Cloud View), 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 Sunstone. Cloud administrators can manage the Groups through the CLI or Sunstone.

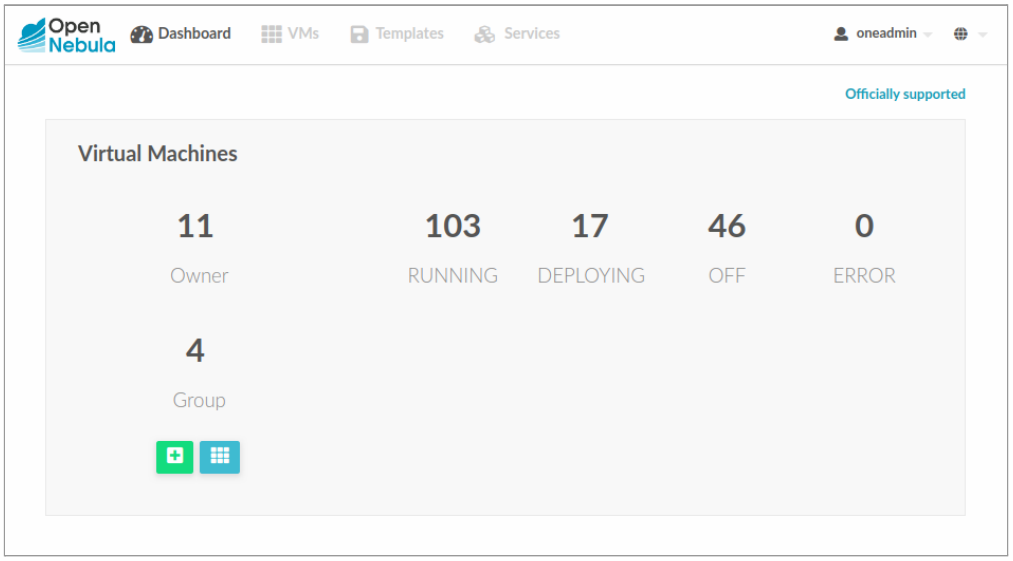

Figure 2: Sunstone Cloud View.

The cloud provisioning model based on VDCs enables an integrated, comprehensive framework to dynamically provision the infrastructure resources in large multi-datacenter environments to different customers, business units or groups. This 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.
- Containers for the execution of software-defined data centers.
- Way 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-premise Private Clouds** serving multiple Projects, Departments, Units or Organizations: On-premise private clouds in large organizations require powerful and flexible mechanisms to

manage the access privileges to the virtual and physical infrastructure and to dynamically allocate the available resources. In these scenarios, the Cloud Administrator would define 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: Cloud providers providing customers with a fully-configurable and isolated environment where they have full control and capacity to administer its users and resources. This 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).

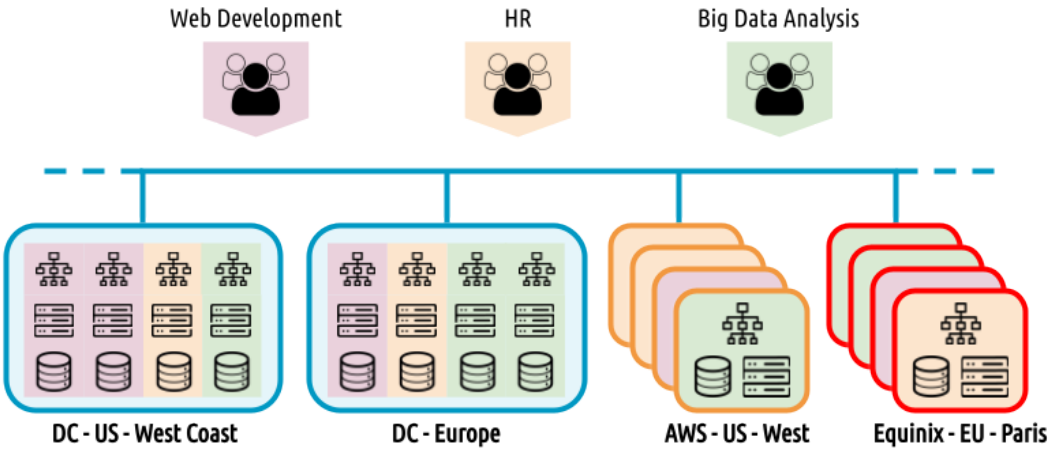

Figure 3: Example of VDC organization

5. Cloud Access Roles

A key management task in any OpenNebula Infrastructure environment has to do with determining who can use the cloud interfaces and what tasks those users 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 set 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 Sunstone** to perform the following actions:

ROLE	CAPABILITIES
Cloud User	• **Defining and instantiating virtualized and containerized applications**, consisting of one or multiple Virtual Machine Service Workflows, using Templates and Images defined by the Cloud Operators, saved from previous running applications, or from a connected public or private Marketplaces (cluster location is selected depending on the network). • **Managing lifecycle 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 the 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 Sunstone**.

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. They can access their VMs, and perform basic operations like shutdown. The changes made to a VM disk can be saved back, but new images cannot be created from scratch.

Cloud Service Administrators (Operators)

Cloud Administrators typically access the cloud using the CLI, the **Admin View in Sunstone,** or **FireEdge**—the GUI of the new provisioning tool (OneProvision).

ROLE	CAPABILITIES
Cloud Operator	• Use OneProvision for the **automatic deployment and setup of Edge Clusters** on remote cloud and edge providers. • **Monitoring and management of Clusters and resources** (Hosts, Networks and Datastores). • **Creating and managing users, Groups and VDCs**, including assignment of Groups and cloud resources to a VDC and quota limits. • Connection 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** to be used by the users. • **Extended lifecycle management** of Virtual Machine instances and workflows. • Generate activity, **accounting** and **showback** reports.

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	• **Installation and configuration of OpenNebula** front-end services, namely Core, Authentication, Sunstone, OneFlow and OneGate. • **Deployment and configuration of Clusters and resources** (Hosts, Network and Datastores) and their integration with the underlying infrastructure services: computing nodes, networking fabric and storage servers. • Monitor the **status** and **health** of the cloud services and the infrastructure resources (OpenNebula on-call).

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.

Cloud Managed Services

OpenNebula Systems operates many private OpenNebula clouds on behalf of corporate users, enabling them to get the benefits of OpenNebula while devoting resources to their business, not to infrastructure. Customers retain complete control of their unique and differentiating workloads while at the same time eliminating any need to deal with management, maintenance, or future upgrade costs for the associated infrastructure and services.

- The OpenNebula Engineering Team assumes the **Cloud Administrator** role, installing and configuring the cloud infrastructure, performing any corrective and periodic preventive maintenance tasks related to the infrastructure, being responsible for the complete cloud infrastructure administration, and providing support to Cloud Operators.
- The customer's Operation Team assumes the **Cloud Operator** role, being responsible for the cloud operation and providing support to the corporate Cloud Users in any aspect related to the day-to-day Cloud Service.

For more details, please refer to our Managed Services Guide.

6. Conclusions

This document outlines the OpenNebula models for managing and provisioning virtual resources, and the default user roles. The cloud provisioning model based on VDCs enables an integrated, comprehensive framework to dynamically provision the infrastructure resources in large multi-datacenter environments to different customers, business units or groups.

OpenNebula Systems offers Enterprise support for the complete cloud software stack through its OpenNebula **Software Subscription** and offers managed cloud services through a new OpenNebula **Managed Subscription** so your team can forget about infrastructure and 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

MANAGED SERVICES

Our team of experts can fully manage and administer your OpenNebula cloud for you

Sign up for updates at OpenNebula.io/getupdated

LINUX FOUNDATION SILVER MEMBER

CLOUD NATIVE COMPUTING FOUNDATION SILVER MEMBER

LF EDGE GENERAL MEMBER

Rev1.0_20210324