­­

SUSE OpenStack Cloud Deployment

Planning an Enterprise OpenStack Deployment

Sucessfully implementing SUSE OpenStack Cloud in an enterprise environment

Formatting Notes

Please use styles preceded by a bullet (●). Styles available for use in this document include:

Heading

Subhead

Body Copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy.

* Bullet list
* Bullet list
* Bullet list
* Bullet list

Heading

Subhead

Body Copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy.

If you need to import an image do so through the Insert > Picture > From file menu. Be sure to import images that are appropriately sized for the column width of this template. And, be sure that the image is placed appropriately in the flow of the copy.

Second Subhead

Body Copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy body copy.

Table of Contents Creation

In order to insert a table of contents (using Microsoft Word 2010):

1. First, complete the content of the document.
2. Insert a page break immediately before your copy begins.
3. On this new blank page position your cursor at the top of the page.
4. Go to the *References* tab.
5. Click on Table of Contents, then select one of the automatic table of content options.
6. Adjust the styles within the table of contents to match the rest of the document.

Introduction

Why do I need this?

The actual physical implementation and deployment of your cloud will be the shortest part of the whole project to get it up and running. The vast majority of your project time will be spent in conference rooms with whiteboards and take-out food hashing out the details of what this project is going to look like. The cloud project will require the cooperation and input from a wide variety of sources, such as the storage team, network team, physical infrastructure management, end-users, legal, procurement and more. Without this coordinated effort, users will get frustrated, your project will not be successful, and the whole thing is doomed from the start

What is the intent of this document?

This document is intended as a *starting point* for a SUSE OpenStack Cloud implementation. Use this guide as a guide to help you prepare for deployment and as a worksheet as you discuss how to configure SUSE Cloud for your environment.

The items below are discussed in greater detail in the SUSE OpenStack Cloud deployment guide. Reference the deployment guide for an understanding of the terms and clarification. Throughout the document you will see references to the section(s) in the deployment guide.

As of the time of this writing, the current version is SUSE OpenStack Cloud 5 (Juno-based release). Deployment guide links are based off of this version and may need to be adjusted for subsequent product versions.

Community documentation may be found on the OpenStack site, <http://docs.openstack.org/> All SUSE-provided documentation, including the deployment guide, is available at: <https://www.suse.com/documentation/suse-cloud-5/>

Preliminary Considerations

Philosophy of your cloud

Before you begin planning the technical details of your implementation, there are several overarching questions you will want to consider that will directly impact the overall architecture

* What problem are you trying to solve by implementing a private Infrastructure-as-a-service (IaaS) cloud?
* Who are the users of your cloud? What do they want out of it?
* What are your business and technical requirements?
* What are the constraints for this project?
* What additional resources will you require to have a successful deployment?

Let's consider each of these questions individually.

What problem are you trying to solve?

This question is probably the most vital one to know before you begin planning your cloud. If you don't know what the goal is that you are trying to accomplish, your likelihood of achieving it is dramatically reduced.

If, for example, your overall goal is to provide a playground for your developers so they will stop annoying IT with constant requests for additional resources, you will make dramatically different decisions than if your overall goal is to streamline your production environment processes.

In the first scenario, you would probably have a single, non-commercial hypervisor such as KVM or Xen. You would likely be looking to implement a relatively cheap backend for volume storage, and high-availability of your control plane may not be significant. You would not likely need to have a large address space reserved for floating IP addresses to expose your cloud workloads to the outside world.

In the second scenario, a production environment, you will be much more stringent in your requirements. You will likely need multiple hypervisors to accommodate varying virtual environments (ie – production will be on VMware, developers will have the cheaper KVM environment, and Windows workloads will be deployed on Hyper-V to maximise the efficiency of licensing costs). You will likely be looking for a more reliable storage infrastructure, leveraging a SAN instead of using local disk storage. You may even have several storage backends that you need to accommodate. You will likely need to reserve a significant number of IP addresses for exposing these production workloads to the outside world.

Without understanding exactly what you are trying to accomplish with your cloud implementation, you are much more likely to make decisions that will be sub-optimal, which may result in significant costs (in time and money) to rectify. Establishing a correct course here will inform every other decision you make for the better.

Who are the users of your cloud?

This question is similar to the first, but it is still worthy of considering individually. If the intended users of the cloud are not in-line with the overall goal of the cloud, then significant frustration will likely emerge. Knowing who all of the intended users are and what their needs and expectations are can help you head that frustration off before it festers and impacts productivity.

If, for example, your stated goal is to provide a playground for developers, but there is also going to be a significant number of less-technical users, you will want to make sure you cater to both user groups. The less-technical users will require significantly more documentation of your processes for using the cloud, and formal training may be appropriate to ensure they don't get frustrated and refuse to use it.

What are the business and technical requirements?

Most enterprise IT environments have specific expectations for uptime, typically in the form of a Service-Level Agreement, or SLA. Stringent SLA's require higher budgets to accommodate higher quality and higher quantities of hardware, networking, and physical infrastructure (power, cooling, disaster-recovery processes, etc). In addition, if you work in government, retail, or healthcare, you will likely have specific compliance requirements for things like PCI, HIPAA, or Common Criteria and these need to be taken into account as well.

What are the constraints of your project?

Every project is short on something, whether it's manpower, money, or time. This falls squarely into the realm of the old adage, “You can pick any two of fast, cheap, and high quality. You can't have all three.” Often-times ill-informed management will attempt to defy the laws of physics and human nature and require all three, but realistically speaking, that's not going to happen. Understanding the priority of your constraints can help you set management expectations appropriately so that you have achievable success criteria.

What additional resources will you need?

Typically it is a fairly small team that is given the charge to build out your private IaaS cloud. You will need to plan on getting input and assistance from a wide variety of other teams, such as storage, networking, and physical infrastructure. Identifying whose help you will need and when you will need it allows them to plan and give your needs the full attention they require.

Performing a Proof-of-Concept

If you are using this guide to deploy a proof-of-concept (POC), here are some additional steps to consider.

Before the POC begins, schedule a meeting to discuss the following topics:

* Is the hardware you are planning to use for the proof-of-concept (POC) certified for SUSE Linux Enterprise Server? You may want to compare your planned hardware setup with the published reference architectures available at <https://www.suse.com/products/suse-cloud/resource-library/#RA>
* Verify your intended method for installing the Admin node. Do you have physical access to the node, and if so can you use a DVD or USB drive to install? If you do not have physical access are you planning on attaching the ISO as a virtual DVD, or will you be using a network-based PXE setup?
* Confirm that the BIOS, fiber-channel cards, network cards, IPMI devices, and BMC' controllers are all **updated to the latest firmware** from the manufacturer.
* Discuss the planned network, including IP address ranges, VLAN tags, Neutron plugins, and, if using the Open vSwitch plugin, the encapsulation method. Make sure there is an established schedule to have that configuration done before you begin the POC.
* Are you planning on having a highly-available control plane? If so, will there be a difference in the hardware between the POC and production? For example, in the POC you may choose to use a two-node cluster hosting all services, but in production use three-node clusters and split out services onto their own individual clusters.
* *If you choose to have a highly available control plane you must choose teaming mode and require that you have at least 2 NIC’s available on all nodes. We recommend that you have at least 4 for redundancy on the network stack.*
* Identify your STONITH method and verify that the appropriate resources are available to implement
* Source for media and SMT repositories (ex. USB drive brought by SE)
* Use Admin Appliance? (Could remove the next requirement for backup/restore)
* Backup/restore plan for the admin server if the installation must be repeated ( Two separate disks, RAID 0, dd copy at point before install-suse-cloud script. This will allow for loading into rescue and dd copy back to that point. )
* What will the patching/upgrade strategy be? (update barclamp, SUSE Manager, none)
* Build a SLE11 SP3 JeOS image using SUSE Studio with supportutils package and setup network configuration with yast at firstboot. This will come in handy for troubleshooting network issues on any hardware so that we can setup the network configuration properly for crowbar.
* On the first day of the POC:
  1. Bring SLE11 SP3 JeOS image
  2. Collect a supportconfig from all systems that will be part of the cloud infrastructure
  3. Use the supportconfigs to review interface map/network conduit/network info in network.json **DG** [**Appendix D**](https://www.suse.com/documentation/suse-cloud-5/singlehtml/book_cloud_deploy/book_cloud_deploy.html#app.deploy.network_json)

Worksheet

High Availability

In order to scale your cloud effectively and still provide the levels of service that your users expect, you will likely need to implement high-availability services for the control plane. The level of clustering will depend greatly on the mixture of your level of paranoia, combined with the practical limits of budget, physical resources, and ability/willingness to introduce additional complexity to your implementation.

If you decide to cluster, you can take two different approaches:

* Build multiple clusters that can each be dedicated to specific OpenStack services-cluster
* Build a single cluster and put all the services on it. If you need to minimize resource contention, you may introduce affinity rules to the cluster that will have it prefer to keep specific services on their own server

This decision directly influences the amount of hardware you will need to have on-hand for your control plane. The absolute minimum number of nodes in a cluster is 2, though 3 is the recommended minimum. A typical proof-of-concept will typically be deployed on a 2-node cluster, but production environments will likely have at least 3 nodes per cluster. **DG** [**2.6.2**](https://www.suse.com/documentation/suse-cloud-5/singlehtml/book_cloud_deploy/book_cloud_deploy.html#sec.depl.reg.ha.control)

How many control nodes will you have in your HA cluster(s):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Clustering your backend database (PostgreSQL) and the messaging queue (RabbitMQ) requires some sort of shared storage. Typical choices include NFS, DRBD, or a SAN. Note that DRBD is currently limited to 2 nodes, and that each node will require a dedicated DRBD disk. DG section 2.7.5

What shared storage method will you use:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

When choosing your cluster layout, keep in mind the HA methodology for the various services.

* Active/Passive
  + Database (PostgreSQL)
  + Messaging queue (RabbitMQ)
* Active/Active (Load balanced with HAProxy)
  + Identity (Keystone)
  + Images (Glance)
  + Block storage (Cinder)
  + Networking (Neutron)
  + Compute (Nova)
  + Dashboard (Horizon)
  + Orchestration (Heat)
  + Monitoring (Ceilometer)

DG section 2.7.2

You will need to identify which method you would like to use for STONITH (Shoot The Other Node In The Head). If you are using a 2-node cluster, you must use the SBD (STONITH Block Device) method. For clusters with 3 or more nodes, there are a wide range of options to choose from, including SBD, IPMI (Dell iDrac, HP ILO, etc), and others. If you don’t know which one you want, use SBD. DG section 2.7.5

Which STONITH mechanism will you use:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

General

Which network mode will you will be using? ((Single, Dual, Teaming) Remember to take into account whether you are using a highly available control plane or not, if so then you must choose Teaming) DG section 2.1.2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is a bastion network required on the Admin server? DG section 3.2.4

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are you going to utilize an existing SMT server or install one on the Admin Server? DG section 2.2

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Admin Server FQDN? (cannot be changed after deployment) DG section 2.1.4

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are there additional DNS servers you want SUSE Cloud to forward to for non-local DNS records? DG section 2.1.4

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which hypervisors will you be supporting in your Cloud? (ESXi, Xen, KVM, Hyper-V) DG sections 1.3, 5.10

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What backend will you be using for your Glance image repository? (local, Swift, Ceph RBD) DG section 5.5

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which backend will you choose for Cinder? (local, raw, eqlx, Netapp, EMC, Ceph RBD) DG section 5.8

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which plugin will you use for Neutron? (linuxbridge, openvswitch, cisco) DG section 5.9

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which encapsulation mode will you use for Neutron? (flat, VLAN, gre) DG section 5.9

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Network

Prior to commencing any cloud proof-of-concept engagement, please define the following network subnets (defaults in parentheses):

* Admin (192.168.124.0/24) – Administrative network that will be used to deploy and maintain all the cloud infrastructure nodes. The size of this subnet is the upper limit to the number of compute/control/storage nodes that can be provisioned. This network will have a PXE boot server on it, and therefore must be isolated from other networks. TFTP service required for PXE does not understand VLAN tags, so it must appear as an untagged network (ie - trunk the ports).
* BMC (192.168.124.0/24) – Administrative network for accessing IPMI devices for the cloud infrastructure
* Fixed (192.168.123.0/24 – tag 500) – Cloud-wide network that most cloud instances will connect to in order to interact with each other and the outside world. While some number of systems may exist in isolated networks and are never connected to the fixed network, generally speaking the range of this subnet defines the maximum number of concurrent cloud workloads that can be run.
* SDN (192.168.130.0/24 – tag 700) – Cloud-wide network that will be used for the software-defined networking stack. The subnet for this needs to be at least as large as the admin network.
* Storage (192.168.125.0/24 – tag 200) – Network used for communicating with Swift storage nodes. Even if there are no plans to use Swift, the Admin server still requires that this network be defined.
* Public (192.168.126.0/24 – tag 300) – Used for exposing OpenStack services and APIs to external users. Must be routable on your existing LAN. Only the control node servers will be on this network, so a small address space may be used when defining the DHCP range.
* Floating (192.168.126.0/24 – tag 300) – Used for exposing cloud instances externally. Must be the same subnet as the public network. The number of IP's designated for this network will be the hard upper limit for the number of cloud instances that can be concurrently exposed to the outside world.

MAC addresses associated with each corresponding host function. (and Cluster if using HA in the control plane. **DG section 2.1.1, 2.7.2**

Cluster = Data, Services, Network (For 1 Cluster just call it Services)

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Cluster | Function | MAC Addresses |
| Admin Server |  |  |  |
|  |  | Admin Network |  |
|  |  | Bastion |  |
| Controller Node(s) |  |  |  |
|  |  | PostgreSQL Database |  |
|  |  | rabbitmq |  |
|  |  | Glance (Images) |  |
|  |  | Keystone (Identity) |  |
|  |  | Neutron (Networking) |  |
|  |  | Cinder (Block Storage) |  |
|  |  | Nova Dashboard (Horizon) |  |
|  |  | Compute Management (Nova and Nova multi-controller) |  |
|  |  | Message Broker  (Rabbit MQ) |  |
|  |  | Swift-proxy, Swift-dispersion |  |
|  |  | Swift Ring |  |
|  |  | Ceph master monitor |  |
| Compute Nodes |  |  |  |
|  |  | Nova-multi-compute-kvm |  |
|  |  | Nova-multi-compute-esxi |  |
|  |  | Nova-multi-compute-xen |  |
| Storage Nodes |  |  |  |
|  |  | cinder-volume |  |
|  |  | Swift-storage |  |

1. Admin/BMC Network Address Allocation (default address allocation included).  The size of this subnet will set the maximum number of compute/storage/controller/admin nodes in your cloud.

DG section 2.1.1

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Addresses | VLAN |  |
| router | 192.168.124.1 | false |  |
| admin | 192.168.124.10 - 192.168.124.11 | false |  |
| dhcp | 192.168.124.21 - 192.168.124.80 | false |  |
| host | 192.168.124.81 - 192.168.124.160 | false |  |
| bmc vlan host | 192.168.124.161 | 100 |  |
| bmc host | 192.168.124.162 - 192.168.124.240 | false |  |
| switch | 192.168.124.241 - 192.168.124.250 | false |  |
| bastion | subnet  netmask  broadcast  gateway  ip address | 10.10.1.0  255.255.255.0  10.10.1.255  10.10.1.1  10.10.1.125 | false |

1. Storage Network Address Allocation (default address allocation included). The size of this subnet defines the maximum number of storage nodes in your Swift/Ceph implementation

DG section 2.1.1

|  |  |  |
| --- | --- | --- |
| Function | Addresses | VLAN |
| host | 192.168.125.10 - 192.168.125.239 | 200 |

1. Private Network/nova-fixed Network Address Allocation (default address allocation included).  The size of this subnet defines the maximum number of concurrent cloud workloads you can run

DG section 2.1.1

|  |  |  |
| --- | --- | --- |
| Function | Addresses | VLAN |
| router | 192.168.123.1 - 192.168.123.49 | 500 |
| dhcp | 192.168.123.50 - 192.168.123.254 | 500 |

1. Public Network nova-floating Network Address Allocation (default address allocation included).  The size of this subnet defines the maximum number of control nodes in your cloud

DG section 2.1.1

|  |  |  |
| --- | --- | --- |
| Function | Addresses | VLAN |
| public Host | 192.168.126.2 - 192.168.126.49 | 300 |
| public dhcp | 192.168.126.50 - 192.168.126.127 | 300 |
| floating host | 192.168.126.129 - 192.168.126.191 | 300 |

1. Software Defined Network Address Allocation (default address allocation included). The size of this subnet defines the maximum number of cloud workloads that can be exposed to an external network

DG section 2.1.1

|  |  |  |
| --- | --- | --- |
| Function | Addresses | VLAN |
| host | 192.168.130.10 - 192.168.130.254 | 700 |

Post POC Considerations

* Identify a patching strategy
  + Updater barclamp
  + SUSE Manager
  + Manual
  + “Set & forget”
* What will you need to modify for a successful move to production?
  + Networking
  + Physical infrastructure
  + Moving from single cluster to multi-cluster control plane
  + Enabling Keystone for LDAP/AD type authentication (hybrid or integrated mode)
  + SUSE Studio integration with glance (webhook)