YaleNUS - YaleNUS Cloudforms and OpenStack Implementation - APAC

June 2, 2015

Red Hat, Inc

Contents

1 Document Information

1.1 Originator

Red Hat Consulting

Hwee Ming - Principal Architect <hwng@redhat.com>

George Goh <ggoh@redhat.com>

1.2 Owner

Red Hat Consulting – Confidential. Restricted distribution.

1.3 Copyright

1.4 Distribution

Do not forward or copy without written permission.

Copies of this document are restricted to the following:

Red Hat, Inc.

YaleNUS

1.5 Confidentiality

All information supplied to YaleNUS for the purpose of this project is to be considered Red Hat confidential.

1.6 Additional copies

Further copies of this document can be obtained from:

Hwee Ming
George Goh

1.7 Points of Contact

Table 1: YaleNUS Contact Information

Wallace		
Darwin		

Table 2: Red Hat Contact Information

Lester Claudio	lester@redhat.com	+1-719-331-0726
Hwee Ming		
George Goh		

1.8 Deliverables

1.8.1 Task List

Red Hat Cloudforms Implementation tasks:

Red Hat OpenStack Implementation tasks:

2 Project Approach

2.1 Introduction

Yale-NUS College, a residential college located in Singapore, aims to redefine liberal arts and science education for a complex, interconnected world.

- A community of learning

We are a diverse group of students, faculty, staff, and supporters, dedicated to building a community in which living and learning are intertwined and habits of creativity, curiosity, and critical thinking are encouraged. Our innovative curriculum integrates knowledge from across the disciplines and around the world.

- Founded by two great universities

An intimate liberal arts college, dedicated to undergraduate education, Yale-NUS draws on the resources and traditions of two great universities. We pursue excellence through innovative teaching and research, and we provide global opportunities for our students.

- In Asia

Our location at the crossroads of Asia informs our pedagogy. Drawing on active modes of learning associated with American liberal arts education, we introduce our students to the diverse intellectual traditions and cultures of Asia and the world.

- For the world

We educate citizens of the world and uphold the principles of free exchange of ideas, pluralism, and respect for diversity. Our extra-curricular and residential programmes support student learning and encourage an ethic of service. By our example, we seek to spur innovation in higher education across the globe.

Red Hat Consulting was engaged by the infrasturecture at Yale NUS to assist in deploying CloudForms 3.1 (Red Hat CloudForms Management Engine, CFME), integrate Cloudforms with Amazon Web Services (AWS), and deploy Red Hat OpenStack in their current infrastructure.

This document details the strategies, implementations, and recommendations that Red Hat Consulting services provided for YaleNUS in Singapore, Singapore.

2.2 Architecture Overview

Cloudforms is a powerful tool that allows customers to build and manage their current virtualization environment as well as their future private or hybrid cloud. The Red Hat CloudForms 3 “Management Engine” delivers the insight, control, and automation enterprises need in order to manage diverse and expanding virtual environments. This technology enables enterprises with existing virtual infrastructures to improve visibility and control, and those just starting virtualization deployments to build and operate a well-managed virtual infrastructure.

2.3 Network Details for YaleNUS

2.3.1 Hostnames / IP Addresses

Host	IP Address	Netmask	Gateway	DNS Server	Notes

2.3.2 VLANs Allocated

VLAN ID	Purpose	Subnet	Netmask	Gateway	Default Gateway

VLAN XXX: Purpose

Hostname	IP

VLAN 804: Management Network

Hostname	IP

VLAN 805: Storage Network

Hostname	IP

3 Activities

3.1 Issue status

Issue	Resolved?
AWS Cloudforms Provisioning	Y
Data Center move	Y
Fibre Optic hardware compatibility	N
OpenStack Cloudforms Provisioning	N

3.2 Lester Claudio's activity log

- Instance tagging is done. We need to discuss how I came up with the use case.
- reated an example Group and Role taxonomy that we will need to show Yale NUS to see if it works for them.
- Sample groups created in support of YaleNUS Self-Service:
  - YaleNUS-Admin - Basic YaleNUS Administrator group. Will have superuser capabilities.
  - YaleNUS-<Project> - User group to be associated with their current project.
  - YaleNUS-<Project>-Admin - This is the Project Administrator . . . Professor. Unfortunately we will have to have one of these for each project/course. The group needs to be created in MS AD and the administrator will import it into Cloudforms.
- Added the EBS dialogs and buttons.
- Rake scripts to import/export dialogs, buttons, service_dialogs etc

3.3 George Goh's activity log

TODO: Please fill

4 YaleNUS Cloudforms Environment

4.1 Overview

TODO

4.2 Pre-requisites

- Web Browsers:
  - Mozilla Firefox for versions supported under Mozilla's Extended Support Release (ESR)
  - Internet Explorer 8 or Higher
- Adobe Flash Player 9 or above.
- The Cloudforms Management Engine Appliance must already be installed and activated in your enterprise.
- The SmartProxy must have visibility to the virtual machines and cloud instances that you want to control.
- Server Racked, Stacked and Cabled
- Switch configuration completed

4.3 Cloudform Appliance Version

OS Version	RHEL 6.6 x86_64
Cloudforms Version	Cloudforms 3.1

4.4 YaleNUS Cloudforms Architecture

At YaleNUS we had some discussions around the size of the environment. Some of the questions that were asked were:

- How many VMs will be managed in your virtualization environment?
- Do you have provisioning templates in place?
- Do you have multiple data centers that need to be managed?
- Do you have a local NTP server?
- Do you have a local DNS or remote DNS service?
- Are forward and reverse DNS resolution configured in your environment?
- Is there at least 42 GB disk space on target virtualization platform?

At Yale NUS the objective of the engagement was to integrate the new Red Hat OpenStack environment and Microsoft AD environment where they housed their users. Yale NUS would like to implement a Self-service provisioning system using Cloudforms as the front end where professors and students would only see the VM's that they owned.

Yale uses Microsoft Active Directory (AD) as their directory service implementation. An AD domain controller authenticates and authorizes Yale NUS users assigning and enforcing security policies. The VMs are used by student, faculty and other users as well as by the operations group.

This information gave us a general idea of the size of the environment and allowed us to figure out how to size the Cloudforms database adequately the first time around. The new appliance does not include the database disk so with the database appliance we are required to create a separate database disk that would be used by the Database Appliance.

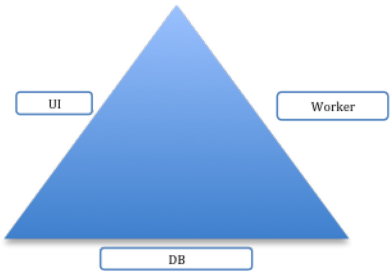
In addition, we briefly discussed the overall Cloudforms architecture which included discussions on Zones and the roles of each appliance.

There are three main roles for an appliance: * UI Appliance – allows the user to interact with the Cloudforms user interface * Worker Appliance – The workhorse which collects all the information from the virtualization environment and sends it to the database to be

persisted. * Database Appliance – one of the most important appliances since it holds all of the data collected by the workers from the virtualization environment.

It is considered a best practice to separate the appliance responsibilities into these three roles. Each appliance can be configured with the appropriate roles and tuned to be more performant in the overall environment.

The Basic Architecture for Cloudforms can be described in a simple Triangle:



The diagram not only depicts the three main roles for the appliances but also the zones that should be created to house each type of appliance. It is best practice to create three zones in a Cloudforms environment:

- UI Zone
- Database Zone
- Worker Zone.

If we were to draw a box around the triangle this would define a Region.

A region should have a Database Zone with only one Database Appliance to house all the virtual environment information. If there are multiple data centers, in different geographic locations, you would replicate the architecture at each data center. The database appliances can be configured to include the Synchronization server role to replicate its contents to a main database. Best practice states that you should only have one database appliance handling the data for one data center.

The current implementation for YaleNUS only has one appliance but this can easily be extended in future phases of the project.

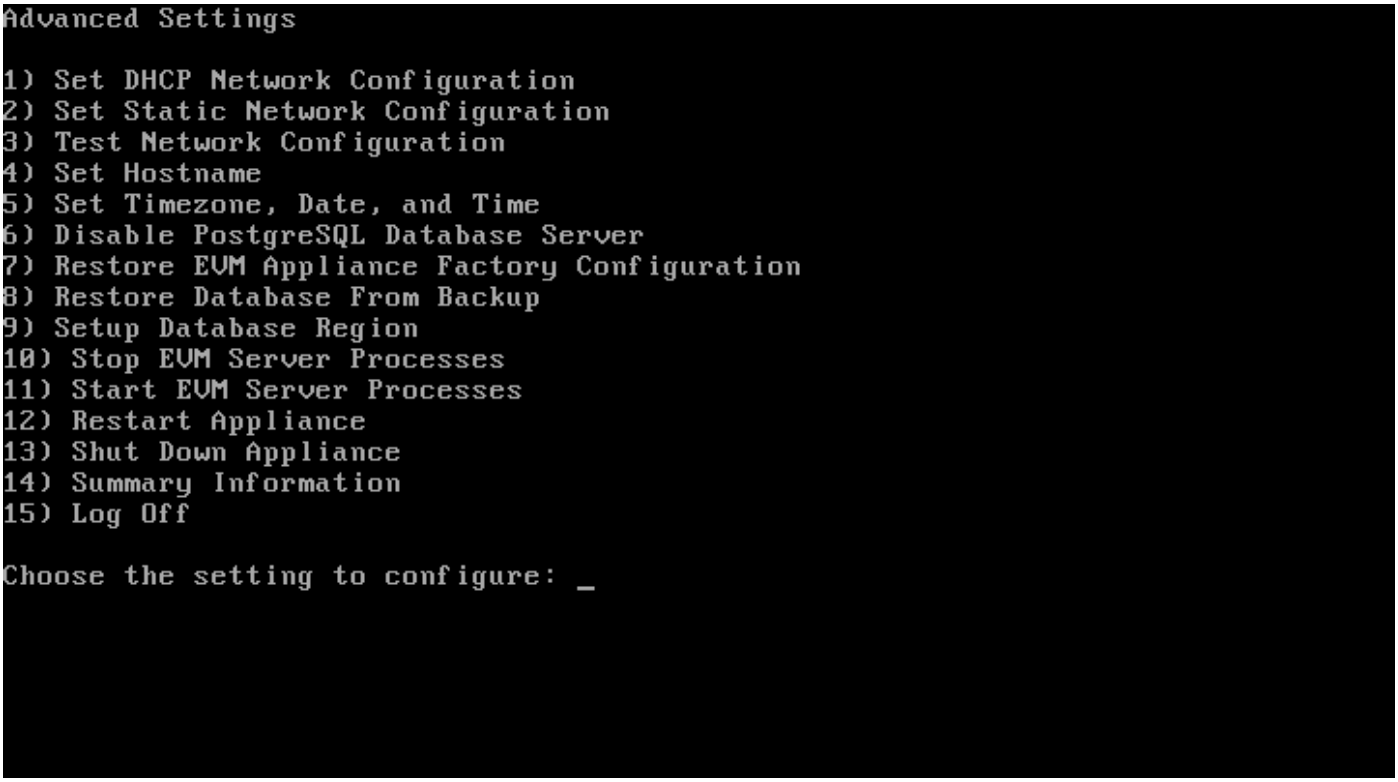
4.4.1 Initial Cloudforms Engine Setup

To manage a 1500 virtual machines workload in a virtualization environment, multiple appliances should be created and the roles distributed for better performance and redundancy: 1 DB, virtual machines, to maintain a 300:1 VM to appliance ratio.

To increase performance, increase the default 4 vCPUs/6GB RAM appliance configuration to 4 vCPUs/8GB RAM for the Web UI appliance and 4 vCPUs/8GB RAM for the DB and the Worker appliances.

With a new CFME appliance the Database is not shipped configured by default. There will need to be a separate Database disk created outside of the appliance and then connected once the appliance has been started. In this case, after looking at where the current VM count and number of VM's that will be coming over the next few years the Database can be sized to 150GB. This will allow for growth over the next few years.

Once started, the appliances need to be configured with basic network settings using the a console in the OpenStack client. Login as admin/smartvm and press Enter to go to the Advanced Settings menu. Set Static Network Configuration, Set Hostname, Set Timezone, Date, and Time. When done entering the settings, select Summary Information to review.



4.4.2 CFME Appliance Configuration

To configure the appliance(s), log on to the web server on each appliance at https://appliance-fqn-name, using the default credentials admin/smartvm in the login screen. Use the Web UI to configure the system(s).

NTP server for network time synchronization and SMTP server information (to enable CFME to send event triggered messages) were configured.

TODO: Screen shots of YaleNUS CFME Engine

4.4.3 CFME Appliance Authentication

The default root password (smartvm) should be changed on all appliances as well as the Web UI Admin password. Here are the steps to change the password:

- Configure > Configuration.
- Select Access Control > Users > Administrator > User Information.
- Password/Confirm Password.
- Click Save.

YaleNUS wants to use LDAP authentication to leverage Yale's Microsoft Active Directory infrastructure.

- Select Configure > Configuration <select zone, server> > Authentication > Mode > LDAPS.
- In Configure > Configuration <select zone, server> > Authentication > LDAP Settings
  - Enter values for LDAP Host Names, LDAP Port, User Type and User Suffix.

4.5 Zones

If YaleNUS decides to add more than one appliance Red hat suggests that the appliaces are organized the into zones to configure failover and isolate traffic. A Management System that is discovered by a Server in a specific zone gets monitored and managed in that zone. All jobs, such as a SmartState Analysis or VM power operation, dispatched by a Server in a specific zone can get processed by any CFME appliance assigned to that same zone.

4.5.1 YaleNUS CFME UI Appliance

The UI appliance is the one that allows the user to interact with the Cloudforms user interface. Access to the UI appliance is achieved by using your favorite web browser such as Firefox or Google Chrome. The UI Appliance has a limited set of roles that it needs to support and they are:

- Notifier
- Provider operations
- Reporting
- Scheduler
- User Interface
- Web Services

YaleNUS has only one appliance in their architecture so ensure that all these roles are selected.

YaleNUS CFME Appliance Tuning Tip

As mentioned, the Worker Appliances will be doing most of the work collecting data from the virtualization environments and persisting the data by sending the information to the Database. The CFME Appliance will be the main appliance that the user will interact with. We want to make sure that it performs adequately for the user. A quick tuning for the YaleNUS CFME Appliance is to change the Count setting on the UI Worker to 2. The Count setting equates to how many threads the UI appliance will have to service the user interface.

To change the setting attach to the UI Appliance, Navigate to Configure→Configuration first and select the Workers tab. Change the UI Worker entry count to 2. If you have other UI Appliances in your environment do ahead and change each of the appliances settings.

4.5.2 YaleNUS Worker Appliance

The Worker Appliance is the work horse which collects all the information from the virtualization environment and sends it to the database to be persisted.The server roles that should be configured in the Worker Appliances are: * Automation Engine * C&U Coordinator * C&U Data Collector * C&U Data Processor * Event Monitor * Notifier * Provider Inventory * Provider Operations * Scheduler * SmartProxy * SmartState Analysis * User Interface * Web Services

Notice that in the YaleNUS environment we currently have one appliance. All the above roles should be checked in that CFME appliance.

4.5.3 YaleNUS CFME Database Appliance

The database appliance is one of the most important appliances since it holds all of the data collected by the workers from the virtualization environment. The server roles that should be configured in the DB appliances are:

- User Interface
- Web Services
- Database Operations

Tip
The Database Appliance will also be working very hard depending on how much data the Worker Appliances are collecting. One of the things that needs to be adjusted are the setting for the shared_buffers in the postgresql.conf file. Since we will have a dedicated database appliance in our environment we will use the DEDICATED CONFIGURATION setting for the shared_buffers variable. This will allow the database to be more performant.

Here are the steps to change the settings from our tip above:

- First ssh to the appliance: ssh root@database-appliance
- Adjust postfix settings [root@vm-dbappliance-01 data]# cd /opt/rh/postgresql92/root/var/lib/pgsql/data
- Make a copy of the configuration file. [root@vm-dbappliance-01 data]# cp -p postgresql.conf{,.20150601}
- Edit the postgresql.conf file: [root@vm-dbappliance-01 data]# vi postgresql.conf
- Comment #shared_buffers = 128MB # MIQ Value SHARED CONFIGURATION
- Uncomment shared_buffers = 1GB # MIQ Value DEDICATED CONFIGURATION

```
[root@vm-dbappliance-01 data]# diff postgresql.conf{.20131021,}

112,113c112,113

< shared_buffers = 128MB  # MIQ Value SHARED CONFIGURATION

< #shared_buffers = 1GB # MIQ Value DEDICATED CONFIGURATION

---

> #shared_buffers = 128MB  # MIQ Value SHARED CONFIGURATION

> shared_buffers = 1GB # MIQ Value DEDICATED CONFIGURATION
```

Note: Services are restarted on the appliance after saving the changes in the database settings.

4.6 YaleNUS Self-Service Requirements

At Yale the objective of the engagement was to integrate the Red Hat OpenStack virtualization environment and Microsoft AD environment where they house their user base. YaleNUS would like to implement a Self-service provisioning system using Cloudforms as the front end where users would only see the VM's that they owned.

Yale uses Microsoft Active Directory (AD) as their directory service implemention. An AD domain controller authenticates and authorizes Yale's users assigning and enforcing security policies.

There are two ways to use LDAP groups with CFME: * Create groups with a specific set of names as provided by Cloudforms. These groups automatically get assigned to a specific role.

- Assign pre-existing groups from your LDAP server to Cloudforms account role.

Note
If the LDAP user is not a member of any defined groups, then the user will be denied access to CFME.

Cloudforms uses role-based access to grant users only the rights they need. Some built-in roles are provided as part of the product. User groups are then assigned to roles and users are assigned to the groups. Finally, you can customize the roles to a fine level of detail, or create your own.

TODO: Document requirements

4.6.1 YaleNUS Taxonomy

During our time at Yale we started discussing briefly the taxonomy of their User and Group environment. The purpose of a taxonomy is to attempt to create an orderly classification of users and groups according to their relationships in the IT environment and associate these relationships in the CFME Appliance. The taxonomy will be derived from analysis of usage patterns and information flow in the YaleNUS environment.

The discussions were very brief due to the data center move activities. Nonetheless the goal of these discussions around User and Group environment is to provide YaleNUS with the following features:

- A view of how their users will be organized in the Microsoft AD environment.
- Enable self-service and accelerate the delivery of IT services by giving Students/Faculty direct access to customizable service catalogs and virtual assets through role-based access.
- Provide Infrastructure-as-a-Service (IaaS) to reduce provisioning and approval times.
- VMs, complex services, and multi-tier applications can all be requested and deployed automatically based on enforceable policies.
- When we build the taxonomy we need to think about the following:
  - The taxonomy will be hierarchical. The classification of users will be multilevel, representing hierarchical relationships between their roles within a defined scope and context.
  - The taxonomy will be used to categorize roles that will define access to different Virtual Machine templates and instances.
  - An authorized user should be given a hierarchical listing of categories from which he or she can assign labels to content items (tagging). The assigned category should then be reviewed as part of the assessment and approval process.

4.6.2 Defined User Groups

For YaleNUS we have defined the following groups: * YaleNUS-Admin - Basic YaleNUS Administrator group. This group will have superuser capabilities. * YaleNUS-<Project> - User group to be associated with their current project. * YaleNUS-<Project>-Admin - This is the Project Administrator i.e. Group for Professors.

Note
Red Hat Consulting and YaleNUS need to have discussions around the requirements around User Groups and Roles.

4.6.3 Defined Roles

As part of the Yale's business requirements document the following AD groups will need to be defined at YaleNUS:

- YaleNUS System Administrator group = (YaleNUS-Admin)
- YaleNUS Projects = (YaleNUS-History, YaleNUS-Geology, ??)
- YaleNUS Project Admins = (YaleNUS-History-Admin, YaleNUS-Geology-Admin, ??)

Note
Red Hat Consulting and YaleNUS need to have discussions around the requirements around User Groups and Roles.

4.7 YaleNUS Network Information

Name	VM?	On hosts	Special attributes	Notes
CFME Engine	Y			The default CFME Engine

5 OpenStack Deployment

5.1 Overview

Overview of YaleNUS OpenStack environment

5.1.1 Pre-requisites

- List pre-requisites
- Server Racked, Stacked and Cabled
- Switch configuration completed

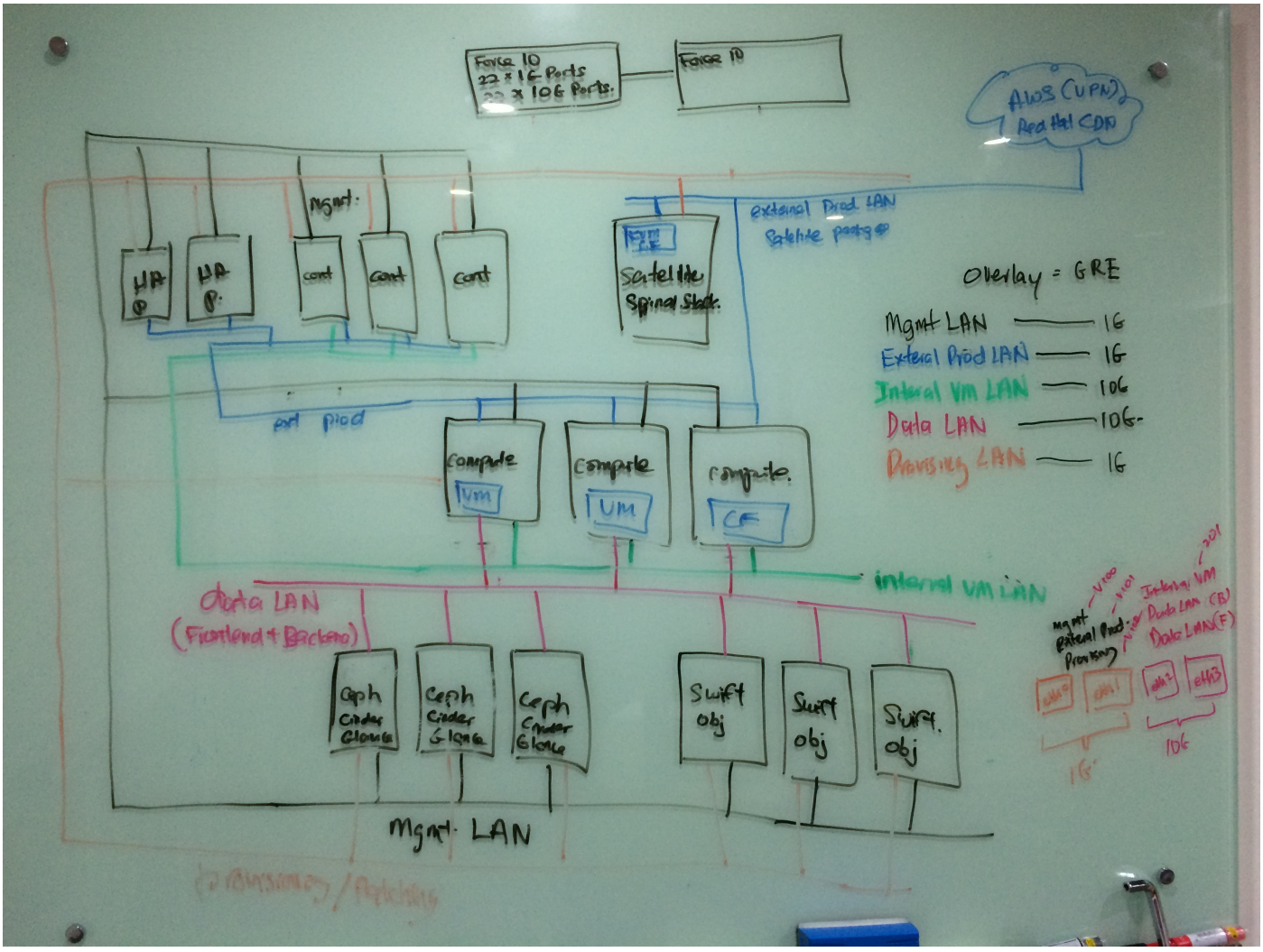
5.1.2 Versions

Enovance Spinal Stack OpenStack Version	Juno Version

5.1.3 Architecture

- 1x Management Node
- 3x Controllers
- 2 Load Balancers
- 4x8 Nova Nodes
- 6 Storage Nodes

Below is a image of the white board depicting the architecture for OpenStack at YaleNUS.



Management, Load Balancer and Controller Hardware

```
Dell PowerEdge R720

Components
1 PowerEdge R720/R720xd Motherboard TPM
1 Intel Xeon E5-2650v2 2.6GHz, 20M Cache, 8.0GT/s Q
```

```
PI, Turbo, HT, 8C, 95W, Max Mem
1866MHz
1 Intel Xeon E5-2650v2 2.6GHz, 20M Cache, 8.0GT/s Q
PI, Turbo, HT, 8C, 95W, Max Mem
1866MHz,2nd Proc
1 3.5-Inch Chassis for PowerEdge R720
1 Risers with up to 6, x8 PCIe Slots + 1, x16 PCIe
Slot
1 Electronic System Documentation and OpenManage DV
D Kit for R720
1 Bezel
1 DIMM Blanks for Systems with 2 Processors
1 1600 MHz RDIMMS
1 Performance Optimized
8 16GB RDIMM, 1600Mhz, Low Volt, Dual Rank, x4 Band
width
4 2TB 7.2K RPM Near Line, 6Gbps SAS 3.5" Hot Plug H
ard Drive
1 PERC H710 Integrated RAID Controller, 512MB NV Ca
che, Mini-Type
2 Heat Sink for PowerEdge R720 and R720xd
1 12.7 Tray DVD ROM
1 Dual, Hot-plug, Redundant Power Supply (1+1), 750
W
2 SFP+, Short Range Optical Tranceiver, LC Connecto
r, 10Gb and 1Gb compatible
1 No Monitor
2 Long Jumper Cord, C13-C14,4m,12a (APCC)
1 Broadcom 57800S 2x10Gb DA/SFP+ + 2x1Gb BT Network
 Daughter Card(Exclude SFP+
Optics/DA Cables)
1 2U Cable Management Arm
1 ReadyRails 2U Sliding Rails
1 C5 - RAID 10 for H710p/H710/H310 (4-16 HDDs in pa
irs)
1 iDRAC7 Enterprise
```

RAM	128 GB
OS Disk	2x 300GB

5.1.4 Yale-NUS Cloud – Existing hardware for compute nodes

Item	Qty
	NOVATTE R2608 multi-node server (Option 3 with Dual

NOVATTE R2608 Server Hardware Details

```
* 10GBASE-T ports per node via PCI-E adapter), comprising:

System:
** (4) node 2U Rackmount Server,
** (12)x 3.5" or (24)x 2.5" drive bays total,
** (2) High efficiency PSUs (platinum level)

Each node supports:
```

```
* (2) Intel® Xeon® processor E5-2600/ E5-2600 v2 product family,
* (16) DDR3 1066/1333/1600/1866 MHz RDIMM slots,
* (6) 2.5" 2.1.1. or (3) 3.5" hot-plug HDDs and (1) optional USB Flash Module,
* (1) PCIe x16 G3 riser slot for low-profile card,
* (2) Intel® I350 GbE RJ45 ports,
* (1) Dedicated 10/100 BASE-T RJ45 management port,
* (2) USB 2.0 ports per node,
* (1) VGA port per node,
* (1) RS232 serial port
* Processors per node: (2) Intel Xeon 8 Core 2.7/ 20M
* 8.0GT/sec (E5-2680)
* Memory per node: 128GB by 16GB DDR3-1600 ECC REG modules
* SSD per node: (2)120GB Intel DCS3500 SATA, MLC
* 10GbE adapter: Intel dual X540 10GbE BASE-T RJ45 ports
```

5.1.5 Networks

Name	VM?	On hosts	Special attributes	Notes

5.1.6 OpenStack Templates

Template creation was explained and the customer was able to create their own templates from VMs. Yale NUS will provide OpenStack templates for provisioning purposes.

5.1.7 Create VM

For demonstration purposes, two VMs were created, one from the RHEL 6 DVD ISO and one from the RHEL 7 ISO. The customer also was able to create virtual machines including demonstrating their ability to provision.

6 Appendix A - YaleNUS Basic Role Base Access

TODO: Add screenshots

The first screen for YaleNUS student for AWS

7 Appendix B - Additional Resources

7.1 Training

For a solid grounding in the products deployed, Red Hat recommends staff be designated to attend the following training classes:

- http://www.redhat.com/en/services/training/cl220-red-hat-cloudforms-hybrid-cloud-management

— CL220 Red Hat CloudForms Hybrid Cloud Management

Red Hat CloudForms Hybrid Cloud Management teaches you how to perform an initial configuration and setup of Red Hat CloudForms.

This course can also help you in your preparation for the Red Hat Certificate of Expertise in Hybrid Cloud Management exam (EX220).

7.2 Course content summary

- Perform initial configuration of CloudForms appliance
- Deploy virtual machines
- Perform policy-based management
- Customize a dashboard
- Create a catalog
- Provision services
- Analyze timelines and events
- Run automations

7.3 Documentation