Dell Red Hat Cloud Solutions Hardware Deployment Guide - Version 2.0

Contents

Trademarks 3

Notes, Cautions, and Warnings 4

Overview 5
- Intended Audience 5

Configuring R620, R720, and R720xd Hardware 6
- IPMI Configuration 6
- Configuring Server User Information 6
- Configuring Server Network Settings 6
- Validating Server IPMI Configuration 6
- Infrastructure and Virtualization Node Settings 7

EqualLogic Storage Group 8

Network Configuration 9
- Configuring the Dell Force 10 S55 and/or S4810 9

References 12
- To Learn More 12

Trademarks

Notes, Cautions, and Warnings

A **Note** indicates important information that helps you make better use of your system.

A **Caution** indicates potential damage to hardware or loss of data if instructions are not followed.

A **Warning** indicates a potential for property damage, personal injury, or death.

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Overview

This guide provides information necessary to deploy the Dell Red Hat Cloud Solutions with Red Hat Enterprise Linux™ OpenStack Platform 5, on Dell R620, R720, and R720xd servers with Dell PowerEdge H710 disk controller; and the network with Dell Force10 S4810 and S55 Switches.

Intended Audience

This guide assumes the reader is familiar with:

- OpenStack
- PowerEdge R620 and R720xd RAID and BIOS configuration
- Red Hat Enterprise Linux (RHEL)
- Network Configuration

Configuring R620, R720, and R720xd Hardware

This section describes manually configuring Dell R720 and R720xd server hardware for the Dell Red Hat Cloud Solutions with Red Hat Enterprise Linux™ OpenStack Platform:

- IPMI Configuration
- BIOS Configuration
- RAID Configuration

IPMI Configuration

You must perform configuration of the iDRAC on supported systems. Dell recommends that you configure these settings from the iDRAC web interface, or directly on the node console.

Configuring Server User Information

1. Set credentials for the root user including changing the password to a new one based on good password standards.
2. Set privileges for the user to Admin level privileges including over LAN.
3. Enable the user, if disabled.

Configuring Server Network Settings

1. Sets the iDRAC IP address, subnet mask, default gateway IP, and default vLAN (id is *10*).
2. Sets the iDRAC IP address source to be *static* IP addressing.
3. Sets the iDRAC NIC mode to *Dedicated* from *Shared*.

Validating Server IPMI Configuration

As part of the IPMI setup, validation that remote commands can be executed is essential.

1. Install to your workstation the IPMI Utilities from SourceForge:
   a. For Linux - *http://sourceforge.net/projects/ipmitool/*
   b. For Windows - *http://ipmiutil.sourceforge.net/*
   c. Validate that you have all the requirements, and that it will run.
2. Plug your Ethernet port into a switch port that has the same vLAN as your iDRACs.
3. Configure your network to use an IP address in the iDRAC network range.
4. Configure the IPMI over LAN Setting to Enabled.
5. Execute an IPMI command:
   a. `for i in $(seq 162 170); do ipmitool –P “password” –U “username” –H 192.168.200.$i power status; done`

      This will perform a simple, non-destructive poll of the iDRAC from *192.168.200.162* to *192.168.200.170*, and then return the power status of *on* or *off*.
   b. You can replace the keyword status with *reset*, *off*, or *on*.
6. Ensure that all machines return responses to the command.

Infrastructure and Virtualization Node Settings

This section describes the settings for nodes that will be used on the Solution Admin Host, OpenStack controllers, and Compute nodes. For the R620 the settings below need to be double-checked.

Table 1: R620 Virtualization Settings

Type	Setting	State
Integrated Devices	SR-IOV Global Enable	Enabled
Processor Setting	Execute Disable	Enabled
Processor Setting	Virtualization Technology	Enabled
Boot Settings	Boot Mode	BIOS
Boot Setting	Boot Order	• Boot mode • Set PXE boot first • Local drive second

EqualLogic Storage Group

The EqualLogic Storage Group can consist of one or more storage arrays with one or more storage groups. The configuration of the arrays is beyond the scope of this document. Please refer to EqualLogic Support Website (*https://eqlsupport.dell.com/secure/login.aspx*) for the latest guides, whitepapers and best practices on how to setup your Storage Group for your application.

Once the Storage Group(s) are setup, the information contained in Table 4 must be collected to configure your software. The san_thin_provision variable should be left at the default if available; if not, then it must be set to False. Refer to *https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux_OpenStack_Platform/5/html/Configuration_Reference_Guide/section_volume-drivers.html#dell-equallogic-driver* for the current list.

Table 2: EqualLogic Information Needed from Configuration

[DEFAULT]	Description
`volume_driver = cinder.volume.drivers.eqlx`	Dell EqualLogic volume driver
`san_ip = <IP_address_of_EQLX>`	IP address used to reach the EqualLogic Group through SSH
`san_login = <user_name>`	User name to login to the Group manager via SSH at the `san_ip`
`san_password = <password>`	Password to login to the Group manager via SSH at the `san_ip` (not used when san_private_key is set)
`san_thin_provision = <true|false>`	Enable/disable creation of thin-provisioned volumes
`san_ssh_port = 22`	Port used for SSH
`ssh_conn_timeout = 30`	Timeout value, in seconds, used by CLI commands over SSH
`san_private_key = <filename>`	Filename of the private key used for SSH authentication
`ssh_min_pool_conn = 1`	Minimum number of SSH connections in the pool
`ssh_max_pool_conn = 5`	Maximum number of SSH connections in the pool
`eqlx_chap_login = admin`	Existing CHAP account name
`eqlx_chap_password = password`	Password for specified CHAP account name
`eqlx_cli_max_retries = 5`	Maximum retry count for reconnection
`eqlx_cli_timeout = 30`	Timeout for the Group Manager CLI command execution
`eqlx_group_name = group-0`	Group name to use for creating volumes
`eqlx_pool = default`	Pool in which volumes will be created
`eqlx_use_chap = False`	Use CHAP authentication for targets?

Network Configuration

If you are not using Dell Force 10 S55 and/or S4810 switches, you will need to program the switches to support your cloud instantiation. Your switches are expected to support the following:

- Support for IEEE 802.1Q vLAN traffic and port tagging
- Support using one untagged and multiple tagged vLANs on the same port
- Ability to provide a minimum of 170 Gigabit Ethernet ports in a non-blocking configuration within Provisioning vLAN
  - Configuration can be a single switch or a combination of stacked switches to meet the additional requirements
- The ability to create link aggregation groups (LAGs) with a minimum of two physical links in each LAG
- If multiple switches are stacked:
  - The ability to create a LAG across stacked switches
  - Full-bisection bandwidth
  - Support for vLANs to be available across all switches in the stack
- 250,000 packets-per-second capability per switch
- A managed switch that supports SSH and serial line configuration
- SNMP v3 support

Configuring the Dell Force 10 S55 and/or S4810

The bundle workbooks are designed to help configure the cluster. Follow the steps outlined to setup your network.

1. Fill each workbook page with all information marked required:
   a. On the switch config page fill in each device name, NIC connected to port.
   b. Using your planning sheet and vLAN information, mark which vlan is either untagged or tagged for each port connected. Not all vLAN will be used on each port.
2. Using the workbook you can now create your configuration:
   a. Individual Port Config Example for S55

```
no ip address
portmode hybrid
switchport
spanning-tree rstp edge-port
```

   b. Individual Port Config example for S4810

```
no ip address
portmode hybrid
switchport
flowcontrol rx on tx off
spanning-tree rstp edge-port
```

   c. Configuring vLANs. With option portmode hybrid on each port, you can program one vLAN to be untagged and other vLANs as tagged. This will send all untagged traffic to the vLAN that is marked untagged. For example, DHCP Request will be placed on that vLAN, and a DHCP server listening on that vLAN will be able to respond.

Example vLAN config with overlapping tagged and untagged ports:

```
nt vlan 100
no ip address
! From your Spread Sheet
tagged TenGigabitEthernet 0/1 - 47
untagged TenGigabitEthernet 0/0
!
int vlan 200
tagged TenGigabitEthernet 0/0-47
int vlan 300
untagged TenGigabitEther 0/1-10
!
!
int vlan 300
tagged TenGigabitEthernet 0/0-47
int vlan 300
untagged TenGigabitEther 0/1-10
!
```

d. General switch options for the S55 and S4810:

```
!
hostname YOUR_HOSTNAME
!
username Tome password 7 MYpassword 1 privilege 15
!
protocol spanning-tree rstp
no disable
hello-time 1
max-age 6
forward-delay 4
bridge-priority 16384
!
no ip telnet server enable
!
arp learn-enable
!
clock timezone EST -5
!
ip ssh server enable
!
protocol lldp
advertise dot1-tlv port-protocol-vlan-id
advertise dot3-tlv max-frame-size
advertise management-tlv system-description system-name
advertise med
no disable
!
reload-type normal-reload
!
```

e. How to create a VLT Domain on the S4810:

```
!
vlt domain 899
peer-link port-channel 100
primary-priority 4096
unit-id 0
!
!
interface Port-channel 100
description Connection to VLT peer
```

```
no ip address
channel-member fortyGigE 0/48
no shutdown
!
```

Note: You do not need to add the port-channel or the vlt to a vLAN. All vLANs will be passed on it.

References

Additional information can be obtained at *http://www.dell.com/openstack* or by e-mailing *openstack@dell.com*.

If you need additional services or implementation help, please contact your Dell sales representative.

To Learn More

For more information on the Dell Red Hat Cloud Solutions with Red Hat Enterprise Linux™ OpenStack Platform visit *http://www.dell.com/openstack*.