## Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2018</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA April 2018.

Dell EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
Table of Contents

Revisions.......................................................................................................................... 2

Audience and Scope........................................................................................................... 8

1 Overview......................................................................................................................... 9

2 Pre-deployment Requirements....................................................................................... 10
   2.1 Datacenter Requirements....................................................................................... 10
   2.2 Site Survey Information......................................................................................... 10
   2.3 Validated Components............................................................................................ 10

3 Physical Layout ............................................................................................................. 12
   3.1 Rack Layout........................................................................................................... 12
   3.2 Cabling.................................................................................................................. 13
   3.3 Hardware Installation Checkpoint.......................................................................... 14

4 Configure Networking.................................................................................................... 15
   4.1 Example Networking Site Survey Information.................................................... 15
   4.2 Configure Dell EMC Networking S5048-ON..................................................... 17
      4.2.1 Begin Setup................................................................................................... 17
      4.2.2 Configure the Management Interface.......................................................... 18
      4.2.3 Configure the VLTi....................................................................................... 19
      4.2.4 Configure the Port-Channel.......................................................................... 21
      4.2.5 Configure the VLANs.................................................................................... 21
   4.3 Configure Dell EMC Networking S3048-ON..................................................... 23
      4.3.1 Begin Setup................................................................................................... 23
      4.3.2 Configure the Management Interface.......................................................... 24
      4.3.3 Configure the Port-Channel.......................................................................... 24
      4.4 Networking Configuration Checklist.................................................................... 26

5 Deploy SAN Storage ........................................................................................................ 27
   5.1 Deploy Dell EMC Unity Storage.......................................................................... 27
   5.2 Deploy Connectrix DS6500 Switches.................................................................... 27
   5.3 Example FC SAN Site Survey.............................................................................. 28
   5.4 Perform Arrays and Hosts Zoning........................................................................ 29
   5.5 Add Cluster Hosts to the Storage Array............................................................... 32
5.6 Create a LUN ........................................................................................................................................... 33
5.7 Storage Configuration Checklist .............................................................................................................. 36

6 Deploy Management Cluster .................................................................................................................... 37
   6.1 Install ESXi on Management Hosts ........................................................................................................ 39
   6.1.1 Prerequisites ...................................................................................................................................... 39
   6.1.2 Configure BIOS Settings and Connect to iDRAC .............................................................................. 40
   6.1.3 Boot to Installation Media .................................................................................................................. 42
   6.1.4 Install VMware ESXi ......................................................................................................................... 44
   6.1.5 Complete the Installation .................................................................................................................. 45
   6.2 Configure the ESXi Management Network ............................................................................................ 46
   6.3 Test Management Network ................................................................................................................... 49
   6.4 Configure Standard Virtual Switches ................................................................................................... 50
   6.4.1 Prerequisites ...................................................................................................................................... 50
   6.4.2 Configure Management Servers' Virtual Switches ......................................................................... 51
   6.4.3 Create vMotion Vmkernel Ports ...................................................................................................... 55
   6.5 Create Management Datastore from Unity LUN .................................................................................. 57
   6.5.1 Multipathing Optimization ............................................................................................................... 59
   6.6 Deploy VMware vCenter Server Appliance .......................................................................................... 59
   6.6.1 Prerequisites ...................................................................................................................................... 59
   6.6.2 Appliance Setup ............................................................................................................................... 62
   6.7 Add the vCenter server to Unisphere .................................................................................................... 63
   6.8 Configure Active Directory Authentication (Optional) ......................................................................... 64
   6.8.1 Join the VCSA to the Domain ........................................................................................................... 64
   6.8.2 Complete Active Directory Authentication Configuration .................................................................. 65
   6.9 Disable SSH on ESXi Hosts .................................................................................................................... 66
   6.10 vSphere Management Cluster Setup Checklist .................................................................................. 68

7 Configure the Management Cluster .......................................................................................................... 69
   7.1 Create Datacenter and Cluster Containers ............................................................................................ 69
   7.2 Add ESXi Hosts to Cluster .................................................................................................................... 71
   7.3 Management Cluster Configuration Checklist ...................................................................................... 72

8 Deploy Compute Cluster ............................................................................................................................ 73
   8.1 Prerequisites .......................................................................................................................................... 73
   8.2 Install VMware ESXi on Compute Hosts ............................................................................................. 73
8.1.1 Configure BIOS Settings and Connect to the iDRAC ................................................................. 73
8.2.2 Boot to Installation Media ........................................................................................................... 76
8.2.3 Install VMware ESXi .................................................................................................................. 77
8.2.4 Configure ESXi Management Network ......................................................................................... 79
8.2.5 Test Management Network ....................................................................................................... 82
8.3 Adding ESXi Hosts to vCenter ...................................................................................................... 83
8.4 Create and Configure Virtual Distributed Switch ........................................................................... 84
8.4.1 Create the vDS .......................................................................................................................... 84
8.4.2 Create Port Groups .................................................................................................................... 86
8.5 Configure Host Networking ........................................................................................................ 89
8.5.1 Add Hosts to the vDS ................................................................................................................. 89
8.5.2 Migrate Networking .................................................................................................................. 92
8.6 Creating Compute Cluster ........................................................................................................... 94
8.6.1 Create vCenter Cluster Object .................................................................................................. 94
8.6.2 Move Hosts to the Cluster ......................................................................................................... 95
8.7 Multipathing Optimization ........................................................................................................... 95
8.8 Compute Cluster Configuration Checklist ...................................................................................... 95
9 Deploy Software Components ........................................................................................................ 96
9.1 Deploy and Configure OpenManage Integration for VMware vCenter ........................................ 96
9.1.1 Prerequisites ............................................................................................................................ 96
9.1.2 Deploy OpenManage Integration ............................................................................................. 97
9.1.3 Configure OpenManage Integration ........................................................................................ 101
9.2 Deploy Dell EMC Virtual Storage Integrator ................................................................................. 107
9.2.1 Deploy the VSI Appliance ......................................................................................................... 107
9.2.2 Register the VSI Plug-in .......................................................................................................... 108
9.3 Data Domain Virtual Edition ...................................................................................................... 110
9.3.1 Prerequisites ........................................................................................................................... 111
9.3.2 Deploy Data Domain Virtual Edition ...................................................................................... 112
9.3.3 Perform Initial DD VE Configuration ....................................................................................... 114
9.3.4 Complete DD VE Configuration .............................................................................................. 116
9.4 Avamar Virtual Edition ................................................................................................................ 118
9.4.1 Deployment Options ................................................................................................................. 118
Audience and Scope

This document covers the steps necessary to deploy Dell EMC Ready Stack for vSphere on PowerEdge Servers, Unity storage, S-Series switches, and Data Domain with Avamar for data protection. This document serves as a deployment guide only; any modifications to the configuration and the impact those may have to the configuration availability are not in scope for this document. For more detailed information regarding the architecture, refer to the appropriate design guide.

This document may make some assumptions about the ability to perform tasks described in this document by the individual performing the deployment. This deployment guide assumes that the individual is familiar with Dell EMC products including the location of buttons, cables and components in the hardware and has functional knowledge of the items included in the Dell EMC owner’s manuals for the products being used. In addition the individual performing the deployment is assumed to have worked with VMware products on a regular basis and understand the components and features of VMware vSphere.

Beyond familiarity with the items described above the deployment personnel are expected to have knowledge of datacenter infrastructure best practices including best practices in the areas of servers, storage, networking, data protection and environmental considerations such as power and cooling.

The scope of this document takes no consideration for existing infrastructure components outside of the Dell EMC Ready Stack. Dell EMC takes no responsibility for any issues that may be caused to existing infrastructure during the deployment. While it is understood that deviations from the configuration described may occur to meet unique requirements, no warranty is implied or given as to the functionality of the Dell EMC Ready Stack when deployed in a modified configuration.
1 Overview

Dell EMC Ready Stack represents best in class hardware from Dell EMC in combination with VMware vSphere 6.5. This is a flexible architecture model; offering a choice in the selection of server, storage and networking components:

- Dell EMC PowerEdge R440, R640, R740, and R740xd.
- Dell EMC Unity 350F, 450F, 550F, and 650F All-Flash models.
- Dell EMC S-Series S5048 and S3048 switches.
- Dell EMC Connectrix DS6500B series switches.

The architecture is designed to scale and multiple clusters can be administered and monitored from the single management cluster.

Dell EMC has gone through an extensive validation process including tests around hardware and software stability as well as feature functionality and interoperability. This additional level of effort is focused around ensuring the design, powered by the best in class hardware from Dell EMC, will provide a stable, highly available platform for your VMware vSphere workloads to run on.
2 Pre-deployment Requirements

This deployment guide for Dell EMC Ready Stack makes several assumptions around your existing infrastructure and services available on your network. Before proceeding further ensure that the pre-deployment requirements are satisfied.

2.1 Datacenter Requirements

To support the solution, the following components are required to be present in the customer environment:

- An existing Ethernet infrastructure with which to integrate. Dell EMC Networking S5048-ON switches support 10/25 GB and 40/100 GB uplinks to the network core switches. Additional components, such as Dell network cables and transceivers, are needed. Ensure you have all necessary components to facilitate connecting to your existing network prior to beginning deployment.
- Domain Name System (DNS) and Network Time Protocol (NTP) services must be available on the management network. A DHCP server is recommended but not required.
- Sufficient power and cooling to support all components must be present. Please refer to product documentation to determine accurate power and cooling needs.

2.2 Site Survey Information

Appendix A, Site Survey, represents the required network information to deploy the Dell EMC Ready Stack solution described in this document. It is recommended that all information be collected prior to starting the deployment. Throughout this document examples from the site survey will be displayed to assist in locating the information necessary.

2.3 Validated Components

The table below list the software and firmware versions that have been validated with the Dell EMC Ready Stack. The Dell EMC Ready Stack Deployment Guide was written using these specific versions. The versions listed below are the recommended minimums for this release of Dell EMC Ready Stack in order to match all of the deployment steps listed in this document.

Table 1: Dell EMC Ready Stack Solution Validated Hardware and Software

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
<th>Version(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>PowerEdge R640/R740/740xd</td>
<td>BIOS 1.3.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iDRAC 3.15.17.15</td>
</tr>
<tr>
<td></td>
<td>Mellanox CX4 LX Dual-port rNDC</td>
<td>Firmware 14.20.18.20, mlx5-core</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.16.10.3</td>
</tr>
<tr>
<td>Layer</td>
<td>Device</td>
<td>Version(s)</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Network</td>
<td>Qlogic 2692 Dual-port Fibre HBA</td>
<td>Firmware 14.02.13, qlnativefc 2.1.57.0-1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Networking S3048 OS 9</td>
<td>FTOS 9.13.0.1P1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Networking S5048 OS 9</td>
<td>FTOS 9.12.1.0</td>
</tr>
<tr>
<td>Storage</td>
<td>Dell EMC Unity x50F</td>
<td>4.2.2</td>
</tr>
<tr>
<td></td>
<td>Connectrix DS6500 Fabric OS</td>
<td>8.1.2a</td>
</tr>
<tr>
<td>Software</td>
<td>VMware vSphere ESXi</td>
<td>6.5.0 U1, Build 7388607</td>
</tr>
<tr>
<td></td>
<td>VMware vCenter Server Appliance</td>
<td>6.5.0 U1, Build 7312210</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Virtual Storage Integrator</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td>Dell EMC OpenManage Integration for VMware vCenter</td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Avamar Virtual Edition</td>
<td>7.5.1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Data Domain Virtual Edition</td>
<td>6.1.1.5</td>
</tr>
</tbody>
</table>
3 Physical Layout

This section describes the physical layout of the components in the Dell EMC Ready Stack if installed in a single rack including cabling for power and network connectivity. Please refer to the specific product documentation available at dell.com/support for instructions on rack installation of individual components.

3.1 Rack Layout

The physical rack layout of Dell EMC Ready Stack is completely flexible, and there can be many datacenter dependencies on power, thermals, and weight. Dell EMC PowerEdge rack servers require either 1U or 2U of rack space depending on model, and the compute server quantity can change depending on customer needs. Dell EMC Unity storage can require fewer/additional disk enclosures, depending on the storage capacity and SSD drive type. Additional items, such as a Data Domain appliance, could also be added within the same rack (space permitting), but this is outside of the scope of this document. The following Figure 1 is an example of the Dell EMC Ready Stack Enterprise Large.

![Rack Layout Diagram]

Figure 1  Rack Layout
3.2 Cabling

All Dell EMC Ready Stack components should follow the cabling diagram below in Figure 2. 100 Gb Ethernet requires QSFP28 cabling and 25 GbE requires SFP28 cabling. Dell EMC Networking Passive Copper Direct Attach cables are recommended and are available in various lengths, depending on rack layout. Dell EMC Networking Active Optical cables are also available for longer distances and dense rack configurations. Connectrix DS6500 switches are pre-populated with the required Fibre Channel optics. Additional 16 GB SFP Fibre Channel adapters are needed for Dell EMC Unity and PowerEdge servers. LC-LC Optical Multimode cable is required between PowerEdge and Unity to Connectrix Fibre Channel switches. Cat 5e or Cat 6 Ethernet cabling is required for iDRAC, Connectrix and Unity management. For small configurations, it is possible to cable 1 GbE devices to TOR using a 1000Base-T SFP Transceiver. This can eliminate the need for the Dell Networking S3048-ON switch in some cases.
3.3 **Hardware Installation Checkpoint**

At this point the following should be completed as part of the Ready Bundle for Virtualization:

- ✔ Installation of hardware components (switches, storage, and servers) into racks
- ✔ Network connections cabled from switches to servers per the above diagram
- ✔ Power cabled to each component per the above diagram
4 Configure Networking

This section describes the steps necessary to configure Dell EMC Ready Stack for the Dell EMC Networking S3048-ON OOB management and S5048-ON TOR switches. The configuration steps detailed are provided as an example of a working configuration. These steps should be reviewed with the site networking team before proceeding.

This section will use information from the Network Topology table in Site Survey. You will also need the core network gateway from the Customer Network Services table. Server port mapping will be used from the Switch Port Mappings table. See the example survey info below.

NOTE: This is intended only as an example. The full blank survey form can be found in Appendix A, and should be completed prior to deployment.

Usernames and passwords are at customer discretion. Ensure all information, especially information related to spanning tree, has been confirmed with the appropriate personnel responsible for the network configuration across your environment.

4.1 Example Networking Site Survey Information

This section presents an example of a networking topology site survey.

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Example Switch Hostnames</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch Hostnames</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Switch</strong></td>
<td><strong>Hostname</strong></td>
</tr>
<tr>
<td>S3048</td>
<td>S3048OOB</td>
</tr>
<tr>
<td>S5048-Top</td>
<td>S5048T</td>
</tr>
<tr>
<td>S5048-Bottom</td>
<td>S5048B</td>
</tr>
</tbody>
</table>
### Table 3  Example VLAN Information

<table>
<thead>
<tr>
<th>Network Type</th>
<th>VLAN ID</th>
<th>S5048-Top IP CIDR</th>
<th>S5048-Bottom IP CIDR</th>
<th>VRRP IP</th>
<th>VRRP Group</th>
<th>S3048 IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Band</td>
<td>100</td>
<td>172.90.100.252/24</td>
<td>172.90.100.253/24</td>
<td>172.90.100.254</td>
<td>1</td>
<td>172.90.100.25</td>
</tr>
<tr>
<td>Management</td>
<td>110</td>
<td>172.90.110.252/24</td>
<td>172.90.110.253/24</td>
<td>172.90.110.254</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>vMotion</td>
<td>120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 4  Example Customer Network Services

<table>
<thead>
<tr>
<th>Customer Network Services</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Network Gateway</td>
<td>172.90.100.250</td>
</tr>
</tbody>
</table>

### Table 5  Example Port Mappings

<table>
<thead>
<tr>
<th>Port Mappings</th>
<th>S5048-Top</th>
<th>S5048-Bottom</th>
<th>S3048</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>NIC Port 1</td>
<td>NIC Port 2</td>
<td>iDRAC</td>
</tr>
<tr>
<td>Mgmt1</td>
<td>Tf 1/1</td>
<td>Tf 1/1</td>
<td>Gi 1/1</td>
</tr>
<tr>
<td>Mgmt2</td>
<td>Tf 1/2</td>
<td>Tf 1/2</td>
<td>Gi 1/2</td>
</tr>
<tr>
<td>Comp1</td>
<td>Tf 1/3</td>
<td>Tf 1/3</td>
<td>Gi 1/3</td>
</tr>
</tbody>
</table>
### Port Mappings

<table>
<thead>
<tr>
<th></th>
<th>Port 1/4</th>
<th>Port 1/5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp2</td>
<td>Tf</td>
<td>Tf</td>
</tr>
<tr>
<td></td>
<td>Gi</td>
<td>Gi</td>
</tr>
<tr>
<td>Comp3</td>
<td>Tf</td>
<td>Tf</td>
</tr>
<tr>
<td></td>
<td>Gi</td>
<td>Gi</td>
</tr>
</tbody>
</table>

### 4.2 Configure Dell EMC Networking S5048-ON

This section provides the procedures necessary to configure your Dell EMC Networking S5048-ON switches in a minimal configuration to support the Dell EMC Ready Stack configuration. Additional configuration may be necessary for your environment and to configure communication to your core datacenter network. If you are not familiar with configuring the Dell EMC Networking S5048-ON you can reference the documentation located at [dell.com/support](http://dell.com/support).

To begin configuring your Dell EMC Networking S5048-ON you will need a laptop with a serial connection and terminal emulation software such as Putty. Commands that include information specific to your environment or site survey have that information placed inside <> symbols. Do not enter this as part the command. See the following example:

**Deployment guide command reference:**

Dell(conf)# hostname <hostname>

On the top S4048 switch enter: Dell(conf)# hostname SW1

On the bottom S4048 switch enter: Dell(conf)# hostname SW2

When a command to enter differs between the top and bottom switch but the information is not part of the site survey an indentation will be used to identify the different commands. Use the command with the preceding hostname for the switch you are configuring. Example:

SW1(conf)# protocol spanning-tree rstp **#Command entered on both switches**

SW1(conf-rstp)# bridge-priority 4096 **#Command for Top S5048**

SW2(conf-rstp)# bridge-priority 8192 **#Command for Bottom S5048**

SW1(conf-rstp)# no disable **#Command entered on both switches**

### 4.2.1 Begin Setup

1. Using the RJ45 to serial cable included with your switch connect one end to your workstation and the other end to the RS-232 console port of the switch located at the upper right hand side of the switch when looking at the back portion near the fans and power supplies.
2. Using terminal emulation software set the appropriate COM port and configure as follows:
   - 15200 baud rate
   - No parity / No flow control
   - 8 data bits / 1 stop bit

3. After successful connection enter configuration mode by first entering the following commands:

   Dell> enable
   Dell# conf

4. Now configure the hostname, timezone, and set a username/password for EXEC mode:

   Dell(conf)# hostname <hostname>
   SW1(conf)# username <username> password <password>
   SW1(conf)# enable sha256-password <password>
   SW1(conf)# clock timezone <timezone>, example CST -6

5. Configure routing to your default gateway, enable SSH, and save the configuration:

   SW1(conf)# ip route 0.0.0.0/0 <core network gateway>
   SW1(conf)# ip ssh server enable
   SW1(conf)# do write

4.2.2 Configure the Management Interface

The VLTi heartbeat uses the management interface located on the back of the Dell EMC Networking S5048-ON switch which is connected with a standard Ethernet network cable from the top S5048-ON to the bottom S5048-ON. To configure VLTi perform the following steps starting in global configuration mode of the switch.

1. Enter the following commands to configure the management port:

   SW1(conf)# interface ManagementEthernet 1/1
   SW1(conf-if-ma-1/1)# ip address 192.168.1.252/24
2. Enable spanning-tree (ensure the personnel responsible for network management have reviewed the configuration for spanning-tree as incorrect settings may cause network issues. The values provided are examples only):

```
SW1(conf)# protocol spanning-tree rstp
SW1(conf-rstp)# bridge-priority 16384
SW2(conf-rstp)# bridge-priority 32768
SW1(conf-rstp)# no disable
```

### 4.2.3 Configure the VLTi

1. Enter the following commands to configure the ports used for VLTi traffic:

```
SW1(conf)# interface range hundredGigE 1/53-1/54
SW1(conf-if-range-hu-1/53-1/54)# description VLTi
SW1(conf-if-range-hu-1/53-1/54)# no ip address
SW1(conf-if-range-hu-1/53-1/54)# mtu 9216
SW1(conf-if-range-hu-1/53-1/54)# no shutdown
SW1(conf-if-range-hu-1/53-1/54)# exit
```

2. Create a port-channel for VLTi:

```
SW1(conf)# interface port-channel 100
SW1(conf-if-po-100)# description VLTi
SW1(conf-if-po-100)# no ip address
SW1(conf-if-po-100)# mtu 9216
SW1(conf-if-po-100)# channel-member hundredGigE 1/53,1/54
SW1(conf-if-po-100)# no shutdown
SW1(conf-if-po-100)# exit
```

3. Create the VLTi domain:

```
SW1(conf)# vlt domain 1
SW1(conf-vlt-domain)# peer-link port-channel 100
    SW1(conf-vlt-domain)# back-up destination 192.168.0.253
    SW1(conf-vlt-domain)# primary-priority 1
    SW1(conf-vlt-domain)# unit-id 0

    SW2(conf-vlt-domain)# back-up destination 192.168.0.252
    SW2(conf-vlt-domain)# primary-priority 2
    SW2(conf-vlt-domain)# unit-id 1
SW1(conf-vlt-domain)# exit
SW1(conf)# do write
```
4. After the VLTi domain has been created on each switch run the following command from enable mode to ensure the VLTi domain is properly configured:

`SW1# show vlt brief`

5. Ensure your output is similar to:

```
VLT Domain Brief
...
ICL Link Status: Up
HeartBeat Status: Up
VLT Peer Status: Up
...
```

6. Configure the ports that the servers are connected to on the switch. Based on the example site survey ports tw 1/1 – tw 1/12 are in use on each switch:

```plaintext
SW1(conf)# interface range twentyFiveGigE 1/1-1/16
SW1(conf-if-range-tw-1/1-1/16)# no ip address
SW1(conf-if-range-tw-1/1-1/16)# mtu 9216
SW1(conf-if-range-tw-1/1-1/16)# portmode hybrid
SW1(conf-if-range-tw-1/1-1/16)# switchport
SW1(conf-if-range-tw-1/1-1/16)# spanning-tree 0 portfast
SW1(conf-if-range-tw-1/1-1/16)# spanning-tree rstp rootguard
SW1(conf-if-range-tw-1/1-1/16)# no shutdown
```

7. Verify the ports are properly configured:

```
SW1(conf-if-range-tw-1/1-1/16)# show config
```

Output for each port should be displayed:

```
interface twentyFiveGigE 1/1
  no ip address
  mtu 9216
  portmode hybrid
  switchport
  spanning-tree 0 portfast
  spanning-tree rstp rootguard
  no shutdown
!
...
```
4.2.4 Configure the Port-Channel

The Dell EMC Networking S3048-ON switch connects to the network through the Dell EMC Networking S5048-ON switches using a port-channel consisting of one twenty-five gigabit port on each Dell EMC Networking S5048-ON.

1. Configure the port that will be used for the port-channel:

   ```
   SW1(conf)# interface twentyFiveGigE 1/48
   SW1(conf-if-tw-1/48)# description OOB uplink
   SW1(conf-if-tw-1/48)# no ip address
   SW1(conf-if-tw-1/48)# mtu 9216
   SW1(conf-if-tw-1/48)# port-channel-protocol LACP
   SW1(conf-if-tw-1/48-lacp)# port-channel 101 mode active
   SW1(conf-if-tw-1/48-lacp)# exit
   SW1(conf-if-tw-1/48)# no shutdown
   SW1(conf-if-tw-1/48)# exit
   ```

2. Create the port-channel:

   ```
   SW1(conf)# interface port-channel 101
   SW1(conf-if-po-101)# description OOB uplink
   SW1(conf-if-po-101)# no ip address
   SW1(conf-if-po-101)# mtu 9216
   SW1(conf-if-po-101)# switchport
   SW1(conf-if-po-101)# vlt-peer-lag port-channel 101
   SW1(conf-if-po-101)# no shutdown
   SW1(conf-if-po-101)# exit
   ```

4.2.5 Configure the VLANs

Configure the VLANs that will exist on the switch. The following examples show the steps to configure each VLAN in the site survey. Server NIC ports 1 and 2 are used for all traffic. If your configuration does not use spine/leaf network architecture or you do not want VLAN traffic routed by the S5048-ON switches skip the commands in bold.

1. Out of Band VLAN:

   ```
   SW1(conf)# interface vlan <VLAN ID>
   SW1(conf-if-vl-100)# description out-of-band VLAN
   SW1(conf-if-vl-100)# ip address <Switch IP CIDR>
   SW1(conf-if-vl-100)# mtu 9216
   SW1(conf-if-vl-100)# untagged twentyFiveGigE 1/1-1/16
   SW1(conf-if-vl-100)# tagged port-channel 101
   SW1(conf-if-vl-100)# vrrp-group 1
   SW1(conf-if-vl-100-vrid-1)# virtual-address <VRRP IP>
   SW1(conf-if-vl-100-vrid-1)# exit
   SW1(conf-if-vl-100)# no shutdown
   ```
SW1(conf-if-vl-100)# exit
SW1(conf)# do write

iDRAC ports can be cabled to TOR as desired using a 1000Base-T SFP Transceivers. In this case, these switchports would require the same configuration above.

2. Management VLAN:

SW1(conf)# interface vlan <VLAN ID>
SW1(conf-if-vl-110)# description Management VLAN
SW1(conf-if-vl-110)# ip address <Switch IP CIDR>
SW1(conf-if-vl-110)# mtu 9216
SW1(conf-if-vl-110)# tagged twentyFiveGigE 1/1-1/16
SW1(conf-if-vl-110)# vrrp-group 2
SW1(conf-if-vl-110-vrid-2)# virtual-address <VRRP IP>
SW1(conf-if-vl-110-vrid-2)# exit
SW1(conf-if-vl-110)# no shutdown
SW1(conf-if-vl-110)# exit
SW1(conf)# do write

3. vMotion VLAN

SW1(conf)# interface vlan <VLAN ID>
SW1(conf-if-vl-120)# description vMotion VLAN
SW1(conf-if-vl-120)# ip address <Switch IP CIDR>
SW1(conf-if-vl-120)# mtu 9216
SW1(conf-if-vl-120)# tagged twentyFiveGigE 1/1-1/16
SW1(conf-if-vl-120)# no shutdown
SW1(conf-if-vl-120)# exit
SW1(conf)# do write

4. Compute VM VLAN:

SW1(conf)# interface vlan <VLAN ID>
SW1(conf-if-vl-210)# description Compute VM VLAN
SW1(conf-if-vl-210)# ip address <Switch IP CIDR>
SW1(conf-if-vl-210)# mtu 9216
SW1(conf-if-vl-210)# tagged twentyFiveGigE 1/1-1/16
SW1(conf-if-vl-210)# vrrp-group 3
SW1(conf-if-vl-210-vrid-3)# virtual-address <VRRP IP>
SW1(conf-if-vl-210-vrid-3)# exit
SW1(conf-if-vl-210)# no shutdown
SW1(conf-if-vl-210)# exit
SW1(conf)# do write

5. To verify that all settings have been properly recorded, review the configuration from enable mode:
6. Repeat these steps to configure the second Dell EMC Networking S5048-ON switch in the configuration.

Before you can reach these switches over the network they must be configured to uplink to the datacenter core network. Many options exist to configure this uplink and your exact configuration will depend on the switches used for the core network and your overall network topology. For this reason these steps are not included in this document.

4.3 Configure Dell EMC Networking S3048-ON

The Dell EMC Networking S3048-ON switch servers as the out-of-band management switch for the Dell EMC Ready Stack. This connectivity is not considered critical for workload operations so a single switch is used. To begin configuring the switch you will need a laptop with a serial connection and a terminal emulator software such as Putty. The same command syntax is in use from the previous configuration steps for the S5048 switches. Perform the following steps to configure the Dell EMC Networking S3048-ON switch.

4.3.1 Begin Setup

1. Using a RJ45 to serial cable included with your switch, connect one end to your workstation and the other end to the RS-232 console port of the switch.

2. Using terminal emulation software set the appropriate COM port and configure as follows:

   115200 baud rate
   No parity
   8 data bits
   1 stop bit
   No flow control

3. After successful connection, enter configuration mode by first entering the following commands:

   Dell> enable
   Dell# conf
4. Configure the hostname and timezone, and set a username/password for EXEC mode:

Dell(conf)# hostname <hostname>
SWOOB(conf)# username <username> password <password>
SWOOB(conf)# enable sha256-password <password>
SWOOB(conf)# clock timezone <timezone, example CST -6>

5. Configure routing to your default gateway, enable SSH and save the configuration:

SWOOB(conf)# ip route 0.0.0.0/0 <VRRP IP for out-of-band VLAN>
SWOOB(conf)# ip ssh server enable
SWOOB(conf)# do write

4.3.2 Configure the Management Interface

Configure the ports that the management servers’ iDRAC cards are connected to on the switch. For this example we will assume that ports 1/1 – 1/3 are used for the management server’s iDRAC.

1. Enter the following commands:

SWOOB(conf)# interface range gigabitEthernet 1/1-1/20
SWOOB(conf-if-range-ge-1/1-1/20)# no ip address
SWOOB(conf-if-range-ge-1/1-1/20)# mtu 9216
SWOOB(conf-if-range-ge-1/1-1/20)# portmode hybrid
SWOOB(conf-if-range-ge-1/1-1/20)# switchport
SWOOB(conf-if-range-ge-1/1-1/20)# spanning-tree 0 portfast
SWOOB(conf-if-range-ge-1/1-1/20)# no shutdown

2. Verify the ports are properly configured:

SWOOB(conf-if-range-ge-1/1-1/20)# show config

Output for each port should be displayed:

interface GigabitEthernet 1/1
   no ip address
   mtu 9216
   portmode hybrid
   switchport
   spanning-tree 0 portfast
   no shutdown
   !
   ... 

4.3.3 Configure the Port-Channel

The Dell EMC Networking S3048-ON switch connects to the network through the Dell EMC Networking S5048-ON switches using a port-channel consisting of two ten gigabit ports on the Dell EMC Networking
S3048-ON. Execute the following procedures to configure the ports for the port-channel, and then create the port-channel.

1. Configure the port that will be used for the port-channel:

   SWOOB(conf)# interface range tengigabitethernet 1/49 - 1/50
   SWOOB(conf-if-range-te-1/49-1/50)# description OOB uplink
   SWOOB(conf-if-range-te-1/49-1/50)# no ip address
   SWOOB(conf-if-range-te-1/49-1/50)# mtu 9216
   SWOOB(conf-if-range-te-1/49-1/50)# port-channel-protocol LACP
   SWOOB(conf-if-range-te-1/49-1/50)# port-channel 101 mode active
   SWOOB(conf-if-range-te-1/49-1/50)# exit
   SWOOB(conf-if-range-te-1/49-1/50)# no shutdown
   SWOOB(conf-if-range-te-1/49-1/50)# exit

2. Create the port-channel:

   SWOOB(conf)# interface port-channel 101
   SWOOB(conf-if-po-101)# description OOB uplink
   SWOOB(conf-if-po-101)# no ip address
   SWOOB(conf-if-po-101)# mtu 9216
   SWOOB(conf-if-po-101)# portmode hybrid
   SWOOB(conf-if-po-101)# switchport
   SWOOB(conf-if-po-101)# no shutdown
   SWOOB(conf-if-po-101)# exit

3. Configure the VLANs the out-of-band VLAN on the switch:

   SWOOB(conf)# interface vlan <vlan ID>
   SWOOB(conf-if-vl-100)# description out-of-band VLAN
   SWOOB(conf-if-vl-100)# ip address <S3048 IP CIDR>
   SWOOB(conf-if-vl-100)# mtu 9216
   SWOOB(conf-if-vl-100)# untagged gigabitethernet 1/1-1/20
   SWOOB(conf-if-vl-100)# tagged port-channel 101
   SWOOB(conf-if-vl-100)# no shutdown
   SWOOB(conf-if-vl-100)# exit
   SWOOB(conf)# do write

4. Verify the port-channel to S4048 is up with the following command:

   SWOOB# show interfaces port-channel brief
   LAG  Mode  Status  Uptime  Ports
   L 101  L2L3  up     00:02:34  Tw 1/49  (up)
   Tw 1/50  (up)
4.4 Networking Configuration Checklist

At this point the following network configurations should be complete:

- S5048 Switches configured
- S5048 Switches connected to the corporate network
- S3048 Switch configured
- S3048 Switch connected to the S5048 Switches
5 **Deploy SAN Storage**

This section describes all procedures you must perform in order to deploy the Unity storage array. It assumes that all storage equipment has been properly powered and cabled to all of the appropriate networks. For enclosure cabling guidelines, please refer to the Dell EMC Ready Stack Design Guide or Dell EMC Unity Hardware Installation Guide.

5.1 **Deploy Dell EMC Unity Storage**

Connect all power cords and management cables before proceeding. If there are additional drive array enclosures, they must be connected as well.

1. Connect Unity to the network:
   a. The management IP address for the Unity system can be assigned statically or dynamically.
      - **Dynamic:** If DHCP is supported on your network, the Unity system automatically obtains a network address when you power it up.
      - **Static:** Download, install, and run the Connection Utility software. This must be done on a computer with access to the subnet where you installed your Unity system. You will need the serial number of the Unity system, the desired IP address, subnet mask, and default gateway.

2. Connect to Unisphere:
   a. Launch your preferred browser and input the IP address from step 1.a above as the destination.
      - Default user: admin
      - Default password: Password123#
   b. An initial configuration wizard steps through basic settings like licensing, storage pool creation, alerts, support, and networking. All of these tasks can be completed from Unisphere at any time in the settings menu (click on the gear icon in upper left), even after the initial wizard. Further, the wizard can be run again any time from the settings menu.

5.2 **Deploy Connectrix DS6500 Switches**

This section describes all procedures you must perform in order to deploy the FC switches. Connect all power cords and management cables before proceeding. For fiber cabling guidelines for storage array and hosts, please see the Dell EMC Ready Stack Design Guide.

1. Connect your setup computer COM port to the serial port on the switch, using the serial cable shipped with the switch. The serial connection settings are as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none

2. Open a terminal emulator program, such as PuTTY, and log into the switch console using the default credentials. (e.g., admin/password).
3. Change the password when prompted.
4. Type `ipAddrSet` and then press **Enter** to start the IP configuration dialogue. The following settings are available in the dialogue:
   - **DHCP**: On or Off (Default setting is Off)
   - **Ethernet IP Address**: Set the desired IP address for the switch
   - **Ethernet Subnetmask**: Set the desired Subnetmask for the switch
   - **Gateway IP Address**: Set the desired default gateway for the switch
5. Once the IP address has been set on the switch, close the terminal emulator program and disconnect the serial cable from the switch.
6. Repeat the process on the second switch if needed.
7. Verify that the FC switches are visible on the network.

### 5.3 Example FC SAN Site Survey

Table 6  Example FC Port Mappings

<table>
<thead>
<tr>
<th>FC Port Mappings</th>
<th>WWN</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-A P0</td>
<td>50:06:01:64:47:e0:01:96</td>
<td>spa_p0</td>
</tr>
<tr>
<td>SP-A P1</td>
<td>50:06:01:65:47:e0:01:96</td>
<td>spa_p1</td>
</tr>
<tr>
<td>SP-A P2</td>
<td>50:06:01:66:47:e0:01:96</td>
<td>spa_p2</td>
</tr>
<tr>
<td>SP-A P3</td>
<td>50:06:01:67:47:e0:01:96</td>
<td>spa_p3</td>
</tr>
<tr>
<td>SP-B P0</td>
<td>50:06:01:6c:47:e0:01:96</td>
<td>spb_p0</td>
</tr>
<tr>
<td>SP-B P1</td>
<td>50:06:01:6d:47:e0:01:96</td>
<td>spb_p1</td>
</tr>
<tr>
<td>SP-B P2</td>
<td>50:06:01:6e:47:e0:01:96</td>
<td>spb_p2</td>
</tr>
<tr>
<td>SP-B P3</td>
<td>50:06:01:6f:47:e0:01:96</td>
<td>spb_p3</td>
</tr>
<tr>
<td>Mgmt1 P1</td>
<td>21:00:00:24:ff:7d:9a:35</td>
<td>mgmt1_p1</td>
</tr>
<tr>
<td>Mgmt1 P2</td>
<td>21:00:00:24:ff:7d:9a:34</td>
<td>mgmt1_p2</td>
</tr>
<tr>
<td>Mgmt2 P1</td>
<td>21:00:00:24:ff:7d:9a:33</td>
<td>mgmt2_p1</td>
</tr>
<tr>
<td>Mgmt2 P2</td>
<td>21:00:00:24:ff:7d:9a:32</td>
<td>mgmt2_p2</td>
</tr>
<tr>
<td>Comp1 P1</td>
<td>21:00:00:24:ff:7f:09:51</td>
<td>comp1_p1</td>
</tr>
<tr>
<td>Comp1 P2</td>
<td>21:00:00:24:ff:7f:09:50</td>
<td>comp1_p2</td>
</tr>
<tr>
<td>Comp2 P1</td>
<td>21:00:00:24:ff:7f:08:f9</td>
<td>comp2_p1</td>
</tr>
</tbody>
</table>
5.4 Perform Arrays and Hosts Zoning

Perform the following steps to zone the management and compute hosts to the storage controllers.

1. From a web browser, start the Brocade Web Tools by entering the switch’s IP address in the address bar. If Web Tools cannot be accessed from the browser due to Java issues, it can be invoked directly from a command prompt with the following command:

   `javaws "http://[your switch ip address]/switchExplorer_installed.html"

2. Create a Zone Configuration:
   a. Log in to Web Tools with admin credentials.
   b. In Brocade Web Tools, click **Configure -> Zone Admin**. The Zone Administration window will open as in Figure 5 below.
c. In the Zone Administration window, navigate to the Zone Config pane, and then click the New Zone Config button.
d. In the Create New Config dialog box, enter a name for the new configuration and click OK.

3. Create aliases for the storage controller front end FC ports:
   a. In the Zone Administration window, navigate to the Alias tab and then click New Alias.
   b. The Create New Alias dialog box is displayed.

   ![Image of Zone Administration window with Zone Config pane highlighted]

   **Figure 6  Alias Pane**
   
   c. In the Create New Alias dialog box, enter a name for the new alias (e.g., Unity_SPA_P0) and click OK.
   d. Expand **Member Selection List** -> **Ports & Attached Devices** to view the nested elements.
   e. Expand the port that contains the WWN needed for the alias being created as shown below. (Unity front end ports’ WWNs can be found in Unisphere.)

   ![Image of Windows with WWNs]

   **Figure 7  Port with WWN**
   
   f. Click the **port WWN**, and then click the **right arrow** to add the WWN to Alias Members.
   g. Repeat steps 3.a through 3.f to create aliases for all storage controller front end ports.
   h. Click **Action** -> **Save Config** to save the configuration changes.

4. Create aliases for the WWN of the management/compute servers:
   a. In the Zone Administration window, navigate to the Alias tab and click New Alias.
   b. The Create New Alias dialog box is displayed.
   c. In the Create New Alias dialog box, enter a name for the new alias (e.g., MGMT_SVR_P1) and click OK.
d. Expand **Member Selection List -> Ports & Attached Devices** to view the nested elements.

e. Expand the port that contains the WWN needed for the alias being created.

f. Click the **port WWN**, and then click the **right arrow** to add the WWN to Alias Members. (Server HBA WWNs can be found in hardware inventory of iDRAC console)

g. Repeat steps 4.a through 4.f to create aliases for all management/compute server HBAs.

h. Click **Action -> Save Config** to save the configuration changes.

5. Create Zones:
   a. In Web Tools, click **Configure -> Zone Admin**.
   b. In the Zone Administration window, navigate to the Zone tab and click **New Zone**.

![Zone Config Pane](image)

Figure 8  **Zone Config Pane**

  c. In the Create New Zone dialog box, enter a name for the new zone, and click **OK**.
  d. Expand **Member Selection List -> Aliases** to view the nested elements.
  e. In Member Selection List, select all **aliases** of the Unity storage ports and alias of the server WWN that will be included in the zone.
  f. Click the **right arrow** to add the aliases to Zone Members.
  g. Repeat steps 5.b through 5.f to create zones for all management and compute servers.
  h. Select **Zoning Actions -> Save Config** to save the configuration changes.

6. Enable configuration:
   a. Select the Zone Config pane.

![Basic Zones](image)
Figure 9  Zone Config Pane

b. Expand Member Selection List -> Zones to view the nested elements.
c. Select all of the zones that were created for the management and compute hosts in previous steps.
d. Click on the right arrow to move the selected zones in Member Selection List to Zone Config Members.
e. Click Save Config to save the configuration. This process will take a few seconds.
f. Click Enable Config and select the name of the zone config. This process will take a few seconds.
g. Click OK to enable the zone configuration.

5.5 Add Cluster Hosts to the Storage Array

1. For each server that needs to be added to the storage array, obtain the HBA’s WWNs. WWNs of the HBA can be viewed from the server’s iDRAC or ESXi shell.
2. To view the WWNs from the iDRAC, log in to the iDRAC, expand Hardware, and then click Fibre Channel devices.
   a. Expand a device under Fibre Channel Ports to view the port’s WWN.
3. To view the WWN from the ESXi shell, run the following command:

   ```
esxcli storage core adapter list
   
esxcli storage core adapter list
   
esxcli storage core adapter list
   
esxcli storage core adapter list
   ```

   The WWN of the ports will be displayed as shown in Figure 10 below.

Figure 10  WWN in ESXi Shell

4. Log in to Unisphere.
5. Under Access, click Hosts.
6. Click the plus sign (+) in the upper left hand corner of the Hosts pane.
7. Name the server in the Name field, and then click Next.
8. All discovered initiators will be shown in the Automatically Discovered Initiators section of the window.
9. Select the WWNs of the server that is being added to the storage array then click Next.
10. Review the selections and click Finish.
11. Repeat steps 5 to 10 for all management and compute servers that need to be added to the storage array.
5.6 Create a LUN

The LUNs created and presented to the management cluster in this procedure will be used as datastores for VCSA deployment as well as other management VMs. These steps can also be used to create additional LUNs that are needed for management and compute clusters.

1. Log in to Unisphere.
2. Create Storage Pools as needed. The number and size of the pools will vary depending on the requirements of each environment and the number of available drive types in the storage array.
3. Click Block on the left hand navigation pane.
4. Click the plus sign (+) in the upper left hand corner of the LUNs pane. The Create LUNs wizard opens as shown in Figure 11 below.

![Create LUNs Wizard](image)

5. Select 1 in the **Number of LUNs** field.
6. Enter the name for the LUN in the **Name** field.
7. Select the Pool from which the LUN is being created, in the **Pool** field.
8. Enter the size of the LUN in the **Size** field. Please reference Table 7 below for VCSA space requirements.
### VCSA Space Requirements

<table>
<thead>
<tr>
<th>Resource</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk storage on the host machine</td>
<td>Default Storage Size:</td>
</tr>
<tr>
<td></td>
<td>- Tiny: 250GB</td>
</tr>
<tr>
<td></td>
<td>- Small: 290GB</td>
</tr>
<tr>
<td></td>
<td>- Medium: 425GB</td>
</tr>
<tr>
<td></td>
<td>- Large: 640GB</td>
</tr>
<tr>
<td></td>
<td>- X-Large: 980GB</td>
</tr>
<tr>
<td></td>
<td>Large Storage Size:</td>
</tr>
<tr>
<td></td>
<td>- Tiny: 775GB</td>
</tr>
<tr>
<td></td>
<td>- Small: 820GB</td>
</tr>
<tr>
<td></td>
<td>- Medium: 925GB</td>
</tr>
<tr>
<td></td>
<td>- Large: 990GB</td>
</tr>
<tr>
<td></td>
<td>- X-Large: 1030GB</td>
</tr>
<tr>
<td></td>
<td>X-Large Storage Size:</td>
</tr>
<tr>
<td></td>
<td>- Tiny: 1650GB</td>
</tr>
<tr>
<td></td>
<td>- Small: 1700GB</td>
</tr>
<tr>
<td></td>
<td>- Medium: 1850GB</td>
</tr>
<tr>
<td></td>
<td>- Large: 1870GB</td>
</tr>
<tr>
<td></td>
<td>- X-Large: 1910GB</td>
</tr>
</tbody>
</table>

9. If a thin LUN is desired, check the **Thin** box. If the Thin box is not checked, a thick LUN will be created.
10. Click **Next**.
11. In the Configure Access pane, click the plus sign (+) in the upper left hand corner of the window.
12. In the Select Host Access window, check the management hosts that require access to the LUN as shown in Figure 12 below, and then click **OK**.
13. In the Access pane, review the host selection and click **Next**.

14. In the Snapshot pane, check the **Enable Automatic Snapshot Creation** box if automatic snapshot creation is desired, and then click **Obtain the HBA’s WWNs**.

15. In the Replication pane, if replication is being configured for the LUN, check the **Enable Replication** box and select the desired settings for replication.

16. Review the selections in the Summary pane, and click **Finish**.

17. In the Results pane, click **Close**.

18. If another datastore is required for additional management VMs such as OMIIVV, VSI and etc., repeat steps 4 through 17 to create a datastore of appropriate size that can accommodate all of the management VMs. In the example given below, a 1 TB LUN should be sufficient.

### Table 8  Management VM Size Example

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>CPU Cores</th>
<th>RAM (GB)</th>
<th>OS (GB)</th>
<th>NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Server Appliance</td>
<td>1</td>
<td>4</td>
<td>16</td>
<td>290</td>
<td>1</td>
</tr>
<tr>
<td>Dell EMC OpenManage Integration for VMware vCenter</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>44</td>
<td>1</td>
</tr>
<tr>
<td>Dell EMC Virtual Storage Integrator</td>
<td>1</td>
<td>2</td>
<td>8</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>Dell EMC Data Domain Virtual Edition</td>
<td>1</td>
<td>8</td>
<td>64</td>
<td>260</td>
<td>1</td>
</tr>
</tbody>
</table>
### Component

<table>
<thead>
<tr>
<th>Component</th>
<th>VMs</th>
<th>CPU Cores</th>
<th>RAM (GB)</th>
<th>OS (GB)</th>
<th>NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC Avamar Virtual Edition</td>
<td>1</td>
<td>2</td>
<td>16</td>
<td>3150</td>
<td>1</td>
</tr>
<tr>
<td>Dell EMC Avamar Proxy</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>21</td>
<td>1</td>
</tr>
</tbody>
</table>

19. Repeat steps 4 through 17 to create additional LUNs as needed and assign them to appropriate hosts.

### 5.7 Storage Configuration Checklist

At this point the following storage configurations should be complete:

- Unity Storage deployment complete
- Connectrix DS6500 deployment complete
- Storage and Server Zoning configured
- Servers provided Fibre channel access to Unity storage
- Management LUN presented to management servers
6 Deploy Management Cluster

This section will cover the steps necessary to deploy the management cluster including the VMware vCenter Server Appliance. The following topics are covered:

- Installing ESXi
- Creating standard virtual switches
- Deploying VMware vCenter Server Appliance
- Configuring Active Directory authentication (optional)

If you have not configured the IP address of the management host iDRAC this must be completed before proceeding. The steps to configure the iDRAC network settings can be found at [dell.com/support](dell.com/support).

Ensure that the workstation you are using has access to a copy of the latest Dell EMC customized ISO for VMware ESX as well as the installation media for VMware vCenter Server Appliance. An SSH client such as Putty will also be needed.

**Downloads Required:**

- VMware Virtual Center Server Appliance – [my.vmware.com](my.vmware.com)
- VMware ESXi 6.5 Dell Customized ISO – [dell.com/support](dell.com/support)

In addition to the information from the site survey, the following is necessary to complete this section:

- iDRAC Credentials
- iDRAC Enterprise License applied on all nodes
- Credentials for vSphere
- (Optional) Records for hostnames added to DNS Server

This section will use information from the Management Virtual Machines table in Site Survey, as well as the Customer Network Services and Network Topology tables. Usernames should be set and recorded at customer discretion. The following tables include the relevant information from these sections of the example site survey.
### Table 9  Management Cluster Site Survey

#### Host Information

#### Management Host Information

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Management VMK0</th>
<th>vMotion VMK1</th>
<th>iDRAC IP</th>
<th>Service Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt01</td>
<td>172.90.100.1</td>
<td>172.90.110.1</td>
<td>172.90.130.1</td>
<td></td>
</tr>
<tr>
<td>Mgmt02</td>
<td>172.90.100.2</td>
<td>172.90.110.2</td>
<td>172.90.130.2</td>
<td></td>
</tr>
</tbody>
</table>

#### Management Virtual Machines

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCSA</td>
<td>172.90.110.100</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>290GB</td>
</tr>
<tr>
<td>OMIVV</td>
<td>172.90.110.101</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>44GB</td>
</tr>
<tr>
<td>VSI</td>
<td>172.90.110.102</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>11GB</td>
</tr>
<tr>
<td>DD VE</td>
<td>172.90.110.103</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>260GB</td>
</tr>
<tr>
<td>AVE</td>
<td>172.90.110.104</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>3150GB</td>
</tr>
<tr>
<td>Avamar Proxy</td>
<td>172.90.110.105</td>
<td>255.255.255.0</td>
<td>172.90.110.254</td>
<td>110</td>
<td>21GB</td>
</tr>
</tbody>
</table>

### Table 10  Customer Network Services Site Survey

#### Customer Network Services

<p>| DNS       | 192.168.1.1 | 192.168.1.2 |</p>
<table>
<thead>
<tr>
<th>Network Type</th>
<th>VLAN ID</th>
<th>S5048-Top IP CIDR</th>
<th>S5048-Bottom IP CIDR</th>
<th>VRRP IP</th>
<th>VRRP Group</th>
<th>S3048 IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Band</td>
<td>100</td>
<td>172.90.100.252/24</td>
<td>172.90.100.253/24</td>
<td>172.90.100.254</td>
<td>1</td>
<td>172.90.100.25</td>
</tr>
<tr>
<td>Management</td>
<td>110</td>
<td>172.90.110.252/24</td>
<td>172.90.110.253/24</td>
<td>172.90.110.254</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>vMotion</td>
<td>120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 6.1 Install ESXi on Management Hosts

Perform the following steps to install VMware ESXi on each of the PowerEdge management hosts that will be part of the management cluster. For convenience, PowerEdge servers can be ordered with VMware ESXi 6.5 preinstalled from the Dell EMC factory. Otherwise, these steps can be performed remotely through the iDRAC web interface or locally. This guide will cover the steps to perform the installation remotely. In this example we are going to assign static IP addresses to the management interfaces of the ESXi hosts. Using DHCP is not recommended for IP allocation of management hosts.

### 6.1.1 Prerequisites

The following is required to complete this section of the deployment guide;

- iDRAC IP Addresses or FQDN
- iDRAC Credentials
- iDRAC Enterprise License applied on all nodes
- Dell customized ESXi (6.5) image. Instructions for downloading can be found [here](#). Make a note of the image location on your system as you will need it when mounting virtual media.
- Host names, Management vLAN ID, IP address information.
- Credentials for vSphere.
- Static IP addresses for each of the management servers
- (Optional) Records for hostnames added to DNS Server

**NOTE:** Instructions for setting up the Dell iDRAC including configuring the IP address can be found in the User Guide located [here](#).
6.1.2 Configure BIOS Settings and Connect to iDRAC

1. Apply the BIOS settings profile optimized for maximum virtualization performance.
   a. Connect to the **iDRAC IP address** of one of the management hosts by using an SSH client (e.g., PuTTY).
   b. Log in with the appropriate credentials. By default these are user: **root** password: **calvin**.
   c. At the /admin1-> prompt, type `racadm set bios.sysprofilesettings.WorkloadProfile VtOptimizedProfile`, and then press Enter.

```
/admin1-> racadm set bios.sysprofilesettings.WorkloadProfile
[Rey=BIOS.Setup.1-1#sysprofilesettings]
RAC1017: Successfully modified the object value and the change is in pending state.
To apply modified value, create a configuration job and reboot the system. To create the commit and reboot jobs, use "jobqueue" command. For more information about the "jobqueue" command, see RACADM help.
```

   d. You must create a job in order for the change to be processed. To create a job, type `racadm jobqueue create BIOS.Setup.1-1` and press Enter.

```
/admin1-> racadm jobqueue create BIOS.Setup.1-1
RAC1024: Successfully scheduled a job.
Verify the job status using "racadm jobqueue view -i JIDxxxxx" command. Commit JID = JID 241674975086
```

   e. Reboot the management host.
   f. Repeat steps 1.a through 1.e for all remaining management hosts.

```
NOTE: The result achieved in step 1 can be completed through other means (like remote racadm). The process documented in this guide should generally be the quickest approach for most environments.
```

2. Using a web browser, navigate to the **iDRAC web interface** at https://<iDRAC Address>.
3. Log in with the appropriate credentials. By default these are user: **root** password: **calvin**.
4. Click the Virtual Console Preview to open the remote console, ensuring that you enable pop-ups support for each iDRAC in your chosen browser.
5. Once connected to the Virtual Console, attach the virtual media by clicking the Virtual Media -> Connect Virtual Media option.

6. After the Virtual Media is connected, mount the VMware ESXi 6.5 Dell ISO image by clicking Virtual Media again, and then selecting Map CD/DVD.
7. Click **Browse** to specify and select the location of the VMware ESXi 6.5 Dell Customized ISO.
8. Click **Open**.

**IMPORTANT:** This location must be available through the installation of the ESXi on all servers.

![Browse to ISO File](image)

**Figure 16**  **Browse to ISO File**

You will be returned to Virtual Media – Map CD/DVD screen.

### 6.1.3 Boot to Installation Media

1. Click on **Map Device**.
2. From the Virtual Console menu bar, select **Next Boot**.
3. From the drop down, click **Virtual CD/DVD/ISO**.

![Image](image.png)

**Figure 17  Virtual CD/DVD/ISO**

4. Click **OK** to continue.
   a. Ensure that the location of the ISO you have mapped will be available through the full installation process.

5. From the Virtual Console menu bar, select **Power**.
6. From the drop-down, click **Power on System**.
7. Or, if already on, select **Power Cycle System (cold boot)**.

![Image](image.png)

**Figure 18  Power On-System**

8. After the server posts, the ESXi installer will begin to load.
6.1.4 Install VMware ESXi

1. In the iDRAC Virtual Console’s Welcome screen, press **Enter**.

   ![Welcome Screen](image)

   **Figure 19  Welcome Screen**

2. Review the terms of the license agreement.
3. If you agree, press **F11** to continue.

   ![End User License Agreement (EULA)](image)

   **Figure 20  End User License Agreement**

4. When prompted for Disk to Install, use the cursor keys to select the desired boot device upon which to install ESXi.
5. If the disk has been used for ESXi before, use the cursor keys to navigate to **Install**.
6. Press the **Space Bar** before, navigate to **Install**.
7. Press **Enter**.
Choose the appropriate keyboard layout for your environment.

a. In this example we will keep the default option by pressing Enter to continue.

9. Enter the password you would like to use for the root account.

10. Re-enter the password to validate.

11. Press Enter.

12. On the confirm install screen, press F11 to install VMware ESXi 6.5.

6.1.5 Complete the Installation

1. When the installation completes from the Virtual Console menu bar, select Virtual Media -> Disconnect Virtual Media.

2. When prompted, click Yes to confirm that you want to close the Virtual Media Session.
3. Press **Enter** to reboot the server.

![Installation Complete](image)

Figure 24  Installation Complete

4. Wait for the installation to complete.

6.2  Configure the ESXi Management Network

1. After the server reboots, open the iDRAC Virtual Console.
2. Press **F2** to log into the Direct Console User Interface (DCUI).

![F2 Customize System/View Logs](image)

Figure 25  DCUI Login Screen

3. Enter the credentials that you created during setup, and then press **Enter**.

![Authentication Required](image)

Figure 26  Authentication Screen

4. After you login successfully from the System Customization screen, choose **Configure Management Network**.
5. Ensure your NIC registers as connected by selecting **Network Adapters** from the menu.

6. Ensure that **vmnic0** (and any other NIC ports that are already connected) show the status of **Connected** (...).

7. Press the **Esc** key to exit the Network Adapters menu.
NOTE: If it is not connected, check the cabling and status of the port on the switch and correct any issues. Then, press Esc to return to the previous screen.

8. Choose VLAN (optional) from the menu, and then press Enter.
9. Enter the VLAN ID for the management network (110 in the example site survey), and then press Enter.

![VLAN (optional)](image)

Figure 30 Enter VLAN ID

10. Select IPv4 Configuration, and then press Enter.
11. Using the cursor keys, choose Set static IPv4 address, and then press the Space Bar.
12. Enter the IPv4 Address, Subnet Mask, and Default Gateway obtained from the Management Host Information section of the site survey.
13. Press Enter to confirm.

![IPv4 Configuration](image)

Figure 31 IPv4 Address

14. Select DNS Configuration, and then press Enter.
15. Type the IP address of the DNS servers and the fully qualified domain name (FQDN) of the host.

DNS information can be found in the Customer Network Services information of the site survey
16. If the environment has multiple domains, or subdomains and short names are used, add the suffixes by selecting **Custom DNS Suffixes**.
17. Press the `Esc` key to return to the main menu.
18. Press `Y` to confirm changes and restart management network.

### 6.3 Test Management Network

Before continuing to the next section, test the management network setup.

1. Choose **Test Management Network**.

![Test Management Network Navigation](image)

**NOTE:** On the next screen you will see a summary of what will be tested. Figure 34 is from a test deployment. **Do not** change your environment to match the figure.
2. Press Enter to continue.
3. Once the test has completed, assuming the records are setup on your DNS servers, you will see results similar to the following.

**Figure 34  Test Management Network**

- By default, this test will attempt to ping your default gateway and DNS servers, and resolve your hostname.
- ping address #0: [172.90.110.254]
- ping address #1: [172.0.100.1]
- ping address #2: [172.0.100.2]
- resolve hostname: [mgmt1.vcse.lab]

**Figure 35  Test Network Results**

- ping address #1 (172.90.110.254): OK
- ping address #2 (172.0.100.1): OK
- ping address #3 (172.0.100.2): OK
- resolving hostname (mgmt1.vcse.lab): OK

**6.4 Configure Standard Virtual Switches**

This section provides the procedures necessary to configure your virtual switches for the Dell EMC Ready Stack.

**6.4.1 Prerequisites**

The following is required to complete this section:

- Web Browser with Adobe Flash required for the vSphere Web Client.
- VLAN Assignments mapped to Virtual Switches
6.4.2 Configure Management Servers’ Virtual Switches

To configure virtual switches on each of the management servers:

1. Connect to the ESXi host using the HTML5 host web interface (https://<hostname or IP Address>/ui), and then log in using the host credentials you created during the installation.

![VMware ESXi Login][1]

**Figure 36 VMware ESXi Login**

2. If this is the first time you have logged in to the vSphere Web Console, please read the information box and decide if you want to join VMware’s Customer Experience Improvement Program. There is a link for more information.

3. Once decided, click OK to continue.

![CEIP Opt-in/Opt-out Screen][2]

**Figure 37 CEIP Opt-in/Opt-out Screen**

The Home screen displays.

4. On the left of the screen, select **Navigator -> Networking.**
5. Click the **Virtual Switches** tab.

6. Click **vSwitch0**.

You will see a warning that the virtual switch has no uplink redundancy.

7. Click **Add uplink**.
8. Change the MTU to 9000.
9. Ensure that Uplink 2 is mapped to **vmnic1**.
10. Click **Save**.
Add Uplink

11. Return to the Networking home screen by clicking on Networking in the Navigator pane.
12. To complete the network configuration for each host, create port groups for each VLAN, specifying
   a. Name
   b. VLAN ID
   c. Which vSwitch to assign each Port Group

Table 12 presents the minimum recommended configuration.

<table>
<thead>
<tr>
<th>Port Group Name</th>
<th>VLAN ID</th>
<th>Virtual Network Adapters</th>
<th>Load Balancing Algorithm</th>
<th>MTU</th>
<th>vSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Management</td>
<td></td>
<td>vnic0 – active, vnic1 – standby</td>
<td>Route based on originating virtual port ID</td>
<td>9000</td>
<td>vSwitch0</td>
</tr>
<tr>
<td>vMotion</td>
<td></td>
<td>vnic0 – standby, vnic1 – active</td>
<td>Route based on originating virtual port ID</td>
<td>9000</td>
<td>vSwitch0</td>
</tr>
<tr>
<td>Compute VM</td>
<td></td>
<td>vnic0 – active, vnic1 – active</td>
<td>Route based on originating virtual port ID</td>
<td>9000</td>
<td>vSwitch0</td>
</tr>
<tr>
<td>Out-of-Band</td>
<td></td>
<td>vnic0 – active, vnic1 – active</td>
<td>Route based on originating virtual port ID</td>
<td>1500</td>
<td>vSwitch0</td>
</tr>
</tbody>
</table>

NOTE: It is important that VLAN IDs and Names (spelling & capitalization) match across the 3 management servers in order to support vMotion and DRS. Also, the Compute VM port group is optional for inclusion in management host vSwitch configuration.

13. Click the Port groups tab.
14. Click Add port group.
15. Fill in the requested information for the vMotion port group.
NOTE: Leave Security as default.

### Figure 41  Port Groups

In this example we have removed the default VM Network, as it will not be used in the example environment. After all the Port Groups have been created, they should look similar to the example.

### Figure 42  Port Groups Configuration

16. Right-click on each Port Group, and then left-click **Edit settings**.

### Figure 43  Edit Settings

17. Ensure that the values match the properties in Table 12, Virtual Switch Configuration, for every Port Group. The example is for the vMotion Port Group.
6.4.3 Create vMotion Vmkernel Ports

To complete setting up the virtual standard switches, create VMkernel ports for vMotion:

1. While still in the networking section of vSphere Web Client, click the VMkernel NICs tab.
2. Click Add VMkernel NIC.

Figure 45  VMkernel NICs Tab
The Add VMkernel NIC dialog displays.

![Add VMkernel NIC Dialog](image)

3. Select **vMotion** from the Port group drop-down list.
4. Set the MTU to **9000**.
5. If using a static IP address:
   a. Change the IPv4 settings Configuration radio button to **Static**.
   b. Enter the appropriate **Address** and **Subnet mask** information into the text boxes.
6. In the Services field select the **vMotion** checkbox.
7. Confirm settings and Click **Create**.
8. Confirm all VMkernel NICs have been created and what services have been assigned to them.

---

**Figure 46  Add VMkernel NIC Dialog**

56  Dell EMC Ready Stack Deployment Guide for VMware vSphere and Unity
Create Management Datastore from Unity LUN

In preparation for vCenter and other management VM deployments, create a shared datastore for the management cluster.

1. In the vCenter Web Client, navigate to **Hosts and Clusters**, and then select the first management host.
2. In the right hand pane, click **Storage Adapters**.

3. Click **Rescan**.
4. Click **Datastores**, and then click **New datastore**.
5. In the New datastore wizard, select **Create new VMFS datastore**, and then click **Next**.
6. In the Select device pane, provide a name for the datastore in the **Name** field.
7. Select the LUN that was created for the management cluster in Add Cluster Hosts to the Storage Array, and then click Next.

8. If the LUN is not visible, verify the zoning configuration on the FC switches as well as the management host access in Unisphere.

9. In the VMFS version pane, select the desired VMFS version.

10. In the Partition configuration pane, adjust the Datastore Size if desired, and then click Next.

11. In the Ready to complete pane, click Finish.

NOTE: Complete sections 6.1 and 6.2 on all ESXi management hosts before proceeding to section 6.4. Please note that the management datastore needs to be created only on one of the management hosts.

NOTE: Datastore heartbeat is a function of vSphere HA which, in the event a network issue arises, helps HA determine whether a host has failed, is in a network partition, or is network isolated. This feature requires a minimum of two shared datastores per cluster. A default set of datastores is selected by vCenter automatically. It is best practice to configure at least two shared datastores per cluster.
6.5.1 Multipathing Optimization
Block storage presented to vSphere hosts from Dell EMC Unity has the native Path Selection Policy (PSP) of round robin (RR) applied by default. While RR is the recommended PSP to apply to Dell EMC Unity block storage, the default number of I/Os between switching paths is 1000. By reducing this value, all paths are more efficiently utilized.

1. The CLI command to make this change for all Dell EMC Unity LUNs on each vSphere host is:

   ```bash
   for i in `esxcfg-scsidevs -c | awk '{print $1}' | grep naa.XXXX`; do esxcli storage nmp psp roundrobin deviceconfig set --type=iops --iops=# --device=$i; done
   ```

   Where XXXX = the first four digits of the Dell EMC Unity disk (or endpoint) devices found using:

   ```bash
   esxcli storage nmp device list
   ```

   And # = the number of desired I/Os between the switching of paths.

2. Additionally, a claim rule can be created to automatically set this value on future LUNs mapped to the host by executing the following command in the CLI:

   ```bash
   esxcli storage nmp satp rule add -s "VMW_SATP_ALUA_CX" -V "DGC" -P "VMW_PSP_RR" -O "iops=1"
   ```

6.6 Deploy VMware vCenter Server Appliance
This section describes the steps necessary to deploy the vCenter Server Appliance with Embedded Platform Service Controller. If you wish to deploy with an External Platform Services Controller, please refer to the appropriate documentation from VMware.

6.6.1 Prerequisites
Requirements include:

- vCenter Server Appliance ISO downloaded in a location that will be available through the installation process.
- IP address for vCenter Server Appliance
- Hostname and record created on DNS server, if required.
- vCenter datastore LUN created in section 5.6

To deploy the vCenter Virtual Appliance:

1. Open the VCSA installation ISO. In this example we are using a Windows workstation.
   a. Depending on your workstation operating system you may need to use an external utility to mount the ISO.
2. From the root of the ISO image, navigate to the `vcsa-ui-installer\win32` directory.
3. Double-click the `installer.exe` application.
4. On the Main Menu of the installer utility, click **Install**.

![Install]

Install a new vCenter Server Appliance or Platform Services Controller Appliance

5. Review the introduction and click **Next** to continue.

6. Review the End User License Agreement (EULA) carefully.
   a. If you agree check I **accept the terms of the license agreement**.
   b. Click **Next** to continue.

7. Select **vCenter Server with an Embedded Platform Services Controller**, and then click **Next**.

8. On the next screen, enter the appropriate information for the first management host.

9. Click "**Next**" after confirming the details are correct.

<table>
<thead>
<tr>
<th>ESXi host or vCenter Server name</th>
<th>FQDN or IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>User name</td>
<td>root or Username@DomainName</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 50  vCenter Server Information**

10. Verify the certificate thumbprint, and then click **Yes**.

11. Enter the name for the VCSA virtual machine and then create a password.

![Set up appliance VM]

Set up appliance VM
Specify the VM settings for the appliance to be deployed.

| VM name                     |                |
| Root password               |                |
| Confirm root password       |                |

**Figure 51  VM Name and Password**

12. Click **Next**.

13. The deployment sizing screen provides a chart to assist in selecting the deployment size. Select the appropriate sizes you desire for your environment and click **Next**.
Deployment Size

14. Select the management datastore that was created in section 6.5, and click Next.

Selected Datastore

15. Fill in the appropriate details on the configure network settings page, and then click Next.
16. Verify all the information displayed is correct and then click Finish.

When the VCSA installation completes you will see a message stating “You have successfully deployed the vCenter Server with an Embedded Platform Services Controller.”

Deployment Complete
17. Click **Continue** to proceed to the second stage of the deployment, **Appliance Setup**.

### 6.6.2 Appliance Setup

Complete the following steps for stage 2 of the vCenter installation.

1. Review the introduction, and then click **Next** to continue.
2. Select the time synchronization mode, enter the NTP server information, and then click **Next**.

![NTP Information](image)

**Figure 55  NTP Information**

3. Enter the SSO information requested, including SSO domain name and site name, and then click **Next**.

![SSO Information](image)

**Figure 56  SSO Information**

4. Review the information about VMware Customer Experience Improvement Program.
   a. Choose whether or not to contribute.
   b. Click **Next**.
5. Review the information; if it is correct, click **Finish**.
6. Review the warning dialog information, and then click **OK**.
After the setup completes:
   a. Note the URLs provided.
   b. Close to exit the installer.

6.7 Add the vCenter server to Unisphere
vCenter server needs to be added to Unisphere in order for certain vSphere features such as VVols to work properly.

1. Log in to Unisphere.
2. Navigate to Access, and click VMware.
3. Click the plus sign (+) in the upper left hand corner of the right pane, to invoke the Add vCenter wizard.
4. In the Network Name or Address field, enter the IP address of the vCenter server. If DNS has been configured in the environment, the hostname of the vCenter server can be used as well.
5. Enter the administrator credentials for the vCenter server into the User Name and Password fields, and then click Find.
6. Select the ESXi hosts to be imported to Unisphere, and then click Next.
7. On the Configure VASA Provider page:
   a. Select the Register VASA Provider checkbox.
   b. Enter the vCenter credentials in the User Name and Password fields.
   c. Click Next.
8. In the Summary page:
   a. Review the information provided.
   b. Click Finish.

6.8 Configure Active Directory Authentication (Optional)
This section describes the optional, additional steps necessary to configure Active Directory authentication to vCenter. The first step to configure Active Directory authentication is to join the VCSA to the domain.

6.8.1 Join the VCSA to the Domain
1. Open a web browser and navigate to the vSphere Web Client at https://<VCSA FQDN or IP>/vsphere-client.
2. Login as the SSO administrator (example: administrator@vsphere.local).
3. Click Administration -> Deployment -> System Configuration.

![System Configuration Navigation](image)

Figure 59 System Configuration Navigation

4. Click Nodes, and then click on the VCSA node.
5. Under the Manage tab, click Settings -> Active Directory.

6. Click Join, and enter the requested information for your domain.

7. When done, click OK.

8. Under the context menu, right click the VCSA, and then click Reboot.

6.8.2 Complete Active Directory Authentication Configuration

When the VCSA has completed restarting, perform the following steps to finish configuring Active Directory authentication.

1. Open a web browser and navigate to the vSphere Web Client at https://<VCSA FQDN or IP>/vsphere-client.
2. Login as the SSO administrator (example: administrator@vsphere.local)
3. Click Administration -> Single Sign-On -> Configuration.
4. Click on the Identity Sources tab.
5. Click the green plus sign (+) to add an identity source.
On the Identity Source Type screen, select **Active Directory (Integrated Windows Authentication)**.

Enter the domain name, and then click **OK**.

Now that the setup is complete we can disable SSH access to the ESXi hosts. These steps are optional; please refer to your organization’s security policy when deciding whether or not to leave SSH enabled.

1. Log into the VCSA web console.
2. Click **Hosts and Clusters** on the left navigator menu.
3. Click an ESXi host on the left, and then click the **Configure** tab.
4. Click -> System -> Security Profile.

![Security Profile Navigation](image)

Figure 64  Security Profile Navigation

5. Scroll down to Services and then click Edit.

![Services](image)

Figure 65  Services

On the Edit Security Profile screen, select SSH then click Stop.

![Edit Security Profile](image)

Figure 66  Edit Security Profile

6. On the confirmation screen, click Yes.
7. Change the Startup Policy to Start and stop manually.
8. Click OK.

6.10 vSphere Management Cluster Setup Checklist

The following should now be complete:

- ESXi Installed on Management servers
- Created standard virtual switches
- Deployed VMware vCenter Server Appliance
- Configured Active Directory authentication (optional)
Configure the Management Cluster

This section will cover the steps necessary to complete setting up the management cluster. The following topics will be covered:

- Creating virtual datacenter and cluster
- Joining hosts to management cluster
- Configuring vSphere DRS and HA

NOTE: This chapter uses the information from the Management Cluster section of the site survey.

Table 13  Management Cluster Site Survey Information

<table>
<thead>
<tr>
<th>Management Cluster Site Survey Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Cluster Information</td>
</tr>
<tr>
<td>Virtual Datacenter Name</td>
</tr>
<tr>
<td>Cluster Hosts</td>
</tr>
</tbody>
</table>

Create Datacenter and Cluster Containers

Perform the following steps to create the datacenter and cluster containers inside vSphere.

1. Open a web browser and navigate to the vSphere Web Client, at `https://<VCSA FQDN or IP>/vsphere-client`.
2. Log in with an account that has administrator privileges.
3. On the Home screen, navigate to **Hosts and Clusters**.

On the left hand Navigator menu, right-click the **top level VCSA object**, and then click **New Datacenter**.

**Figure 67**  New Datacenter Navigation

4. Enter the name for the datacenter, and then click **OK**.
5. Right-click on the **new virtual datacenter object** that appeared in the Navigator menu, and then click **New Cluster**.

![New Cluster dialog box](image)

**Figure 68  New Cluster**

6. Enter the **cluster name**.
7. Enable DRS and HA by selecting the appropriate **Turn ON** checkbox next to each item. Admission Control should be **Disabled** for a two node management cluster.
8. Click **OK** to complete creating the cluster.

**NOTE:** Datastore heartbeat is a function of vSphere HA (which, in the event a network issue arises, helps HA determine whether a host has failed), is in a network partition, or is network isolated. This feature requires a minimum of two shared datastores per cluster. A default set of datastores is selected by vCenter automatically. To change heartbeat settings within the vSphere Web Client, go to **Hosts and Clusters -> Cluster_Name -> Configure -> vSphere Availability -> Edit -> Heartbeat Datastores.**
7.2 Add ESXi Hosts to Cluster

The next step is to add the three management hosts to the newly created management cluster.

NOTE: Perform these steps on the management server that is running the VCSA first, and then repeat for the remaining hosts.

1. Open a web browser and navigate to the vSphere Web Client at https://<VCSA FQDN or IP>/vsphere-client.
2. Log in with an account that has administrator privileges.
3. On the Home screen, navigate to Hosts and Clusters.
4. Right-click the management cluster object, and then select Add host.

Figure 69 Add Host Navigation

5. Enter the appropriate DNS name or IP address for the first management host.
6. Complete the remainder of the Add Host wizard by entering the username root and the ESXi host password.

Figure 70 Add Host Wizard

7. Wait for the first host to finish adding and configuring HA before adding the remaining hosts.
8. Repeat this procedure for the remaining hosts.

NOTE: You may receive any or all of the cluster-level alerts inside vCenter. These alarms and alerts can be ‘Reset to Green’ during the setup process. A health check will be conducted at the end of the setup.
7.3 Management Cluster Configuration Checklist

Upon completing the above sections the following items should be completed:

- Creating a virtual datacenter and cluster for the management cluster
- Joining ESXi management hosts to the management cluster in vCenter
- Configuring vSphere DRS and HA for the management cluster
8 Deploy Compute Cluster
This section will cover the steps necessary to deploy the compute server infrastructure.

8.1 Prerequisites
The following is required to complete this section of the deployment guide:

- iDRAC IP Addresses or FQDN
- iDRAC Credentials
- iDRAC Enterprise License applied on all nodes
- Dell customized ESXi (6.5) image. Instructions for downloading can be found here. Make a note of the image location on your system as you will need it when mounting virtual media.
- Host names, Management vLAN ID, IP address information.
- Credentials for vSphere.
- Static IP addresses for each of the management servers
- (Optional) Records for hostnames added to DNS Server

NOTE: Instructions for setting up the Dell iDRAC including configuring the IP address can be found in the User Guide located here.

8.2 Install VMware ESXi on Compute Hosts
Perform the following steps to install VMware ESXi on each of the servers that will be part of the compute cluster. These steps can be performed remotely through the iDRAC web interface or locally.

NOTE: This guide describes the steps to perform the installation remotely.

8.2.1 Configure BIOS Settings and Connect to the iDRAC
1. Apply the BIOS settings profile optimized for maximum virtualization performance.
   a. Connect to the iDRAC IP address of one of the compute hosts by using an SSH client (e.g., PuTTY).
   b. Log in with the appropriate credentials. By default these are user: root password: calvin.
   c. At the /admin1-> prompt, type racadm set bios.sysprofilessettings.WorkloadProfile VtOptimizedProfile, and then press Enter.
   d. You must create a job in order for the change to be processed. To create a job, type racadm jobqueue create BIOS.Setup.1-1 and press Enter.
36. Reboot the compute host.
37. Repeat 1.a through 1.e for all remaining compute hosts.

NOTE: The result achieved in step 1 can be completed through other means (like remote racadm). The process documented in this guide should generally be the quickest approach for most environments.

2. Using a web browser navigate to the iDRAC web interface at https://<iDRAC Address>.
3. Log in with the appropriate credentials. By default they are:
   - User: root
   - Password: calvin
4. Next to the Virtual Console Preview, click Launch to open the remote console, ensuring that you enable pop-ups support in your chosen browser for each iDRAC.

![Virtual Console Preview](image)

Figure 72  Virtual Console Preview

5. Once connected to the Virtual Console, attach the virtual media by:
   a. Navigating to the Virtual Media menu
6. Clicking **Connect Virtual Media**

![Connect Virtual Media](image)

**Figure 73  Connect Virtual Media**

7. After the Virtual Media is connected, mount the VMware ESXi 6.5 Dell ISO image by Clicking **Virtual Media** again.
8. Select “**Map CD/DVD**”.

![Map CD/DVD](image)

**Figure 74  Map CD/DVD**

9. Click **Browse** to specify the location of the VMware ESXi 6.5 Dell Customized ISO.
10. Once you have selected the Dell Customized ISO, click **Open**.

**IMPORTANT: This location must be available through the ESXi install on all servers.**

![Select ISO](image)

**Figure 75  Select ISO**
You will be returned to Virtual Media – Map CD/DVD screen.

11. Click on **Map Device**.
12. From the Virtual Console menu bar, select **Next Boot**.

From the drop-down, click **Virtual CD/DVD/ISO**.

![Next Boot Dialog](image)

13. Click **OK** to continue, and to ensure that the location of the ISO you have mapped will be available throughout the full installation process.

### 8.2.2 Boot to Installation Media

1. From the Virtual Console menu bar, select **Power**, and then click **Power on System**.

Or, if already on, click **Power Cycle System (cold boot)**

![Power Dialog](image)

2. After the server posts, the ESXi installer will begin to load.
8.2.3 **Install VMware ESXi**

1. On the iDRAC Virtual Console’s, Welcome screen, press Enter.

![Welcome Dialog](Image)

**Figure 78  Welcome Dialog**

2. After reviewing the terms of the license agreement, and if you agree, press F11 to continue.

![EULA](Image)

**Figure 79  EULA**

3. When prompted for Disk to Install, use the cursor keys to select the desired boot device upon which to install ESXi.

4. If the disk has been used for ESXi before:
   a. Use the cursor keys to navigate to **Install**.
   b. Press the **Space Bar** to perform a fresh install.
c. Press **Enter**.

![ESXi Install](image)

**Figure 80 Install ESXi**

5. Choose the appropriate keyboard layout for your environment. In this example we will keep the default option.
   a. Press **Enter** to continue.

6. Enter the password you would like to use for the root account.
   a. Confirm the password.
   b. Press **Enter**.

![Enter Root Password](image)

**Figure 81 Enter Root Password**

7. On the confirm install screen, press **F11** to install VMware ESXi 6.5.

8. When the installation completes:
   a. From the Virtual Console menu bar, select Virtual Media -> **Disconnect Virtual Media**.
   b. When prompted, click **Yes** to confirm you want to close the Virtual Media Session.

![Virtual Media](image)

**Figure 82 Disconnect Virtual Media**
9. Press **Enter** to reboot the server

![Installation Complete]

**Figure 83  Installation Complete**

8.2.4 **Configure ESXi Management Network**

1. After the server reboots, from iDRAC Virtual Console, press **F2** to login to the Direct Console User Interface (DCUI).

![DCUI Login]

**Figure 84  DCUI Login**

2. Enter the credentials that you created during setup and press **Enter**.

![Authentication Credentials]

**Figure 85  Authentication Credentials**

3. After you log in successfully from the System Customization screen, choose **Configure Management Network**.

![System Customization]

---

Dell EMC Ready Stack Deployment Guide for VMware vSphere and Unity
4. Ensure your NIC registers as connected:
   a. Select **Network Adapters** from the menu.

   ![Network Adapters Menu](image)

   **Figure 86 Configure Management Network**

   b. Ensure that vmnic0 (and any other NIC ports that are already connected) show a status of “Connected (…)”.

   ![Network Adapters Table](image)

   **Figure 87 Network Adapters**

   c. Press the **Esc** key to exit the Network Adapters menu.

   ![Management VLAN Status](image)

   **Figure 88 Management VLAN Status**

   NOTE: If it is not connected, check the cabling and status of the port on the switch and correct any issues. Press **Esc** to return to the previous screen.
5. Choose **VLAN (optional)** from the menu, press **Enter**. Enter the VLAN ID for the management network (110 in the example site survey) and press **Enter**.

![VLAN ID](image)

**Figure 89  Management VLAN Name**

6. Select **IPv4 Configuration**, and then press **Enter**.
7. Press the **Space Bar** to choose **Set static IPv4 address**.
8. Enter the IP Address, Subnet Mask and Default Gateway obtained from the **Compute Host Information** section of the site survey.
9. Press **Enter** to confirm.

![IPv4 Configuration](image)

**Figure 90  IPV4 Configuration**

10. Select **DNS Configuration**, and then press **Enter**.
11. Type the **DNS server’s IP address** and the **host's fully qualified domain name (FQDN)**. DNS information can be found in the **Customer Network Services** information of the site survey.

![DNS Configuration](image)

**Figure 91  DNS Configuration**

12. If the environment has multiple domains, or subdomains and short names are used, add the **Custom DNS Suffixes**.
13. Press **Esc** to return to the main menu.
14. Press **Y** to confirm changes and restart the management network.

![Confirm Management Network](image)

**Figure 92  Confirm Management Network**

### 8.2.5 Test Management Network

Before continuing to the next section, test the management network setup.

1. Choose **Test Management Network**.

**NOTE**: On the next screen you will see a summary of what will be tested. Figure 93 is from a test deployment. **Do not change your environment to match the figure**.
2. Once the test has completed, assuming the records are setup on your DNS servers, you will see results similar to the following.

![Testing Management Network](image)

**Figure 93 Test Management Network**

8.3 **Adding ESXi Hosts to vCenter**

The next step is to add the hosts to vCenter.

**NOTE:** Perform these steps on each of the servers that will be part of the compute cluster.

1. Open a web browser and navigate to the vSphere Web Client at `https://<VCSA FQDN or IP>/vsphere-client`.
2. Log in with an account that has administrator privileges.
3. On the home screen, navigate to **Hosts and Clusters**.
4. Right-click the **datacenter object**, and then select **Add host**.

![Add Host](image)

**Figure 95  Add Host**

5. Enter the appropriate DNS name or IP for the first compute host.
6. Complete the remainder of the add host wizard.

![Compute Host Name and Location](image)

**Figure 96  Compute Host Name and Location**

7. Repeat steps 3-6 for each host.

### 8.4 Create and Configure Virtual Distributed Switch

The Dell EMC Ready Stack uses virtual distributed switches (vDS) in the compute cluster. vDS allows a single vSwitch configuration to be used by multiple hosts.

#### 8.4.1 Create the vDS

To create the vDS:

1. Open a web browser and navigate to the vSphere Web Client at `https://<VCSA FQDN or IP>/vsphere-client`.
2. Log in with an account that has administrator privileges.
3. On the home screen click **Networking**.
4. Right-click the **datacenter object**, and then select **Distributed Switch -> New Distributed Switch**.

![New Distributed Switch](image)

**Figure 97  New Distributed Switch**
5. Enter a **Name** for your vDS, and then click **Next**.

![New Distributed Switch]

**Figure 98  vDS Name and Location**

6. Ensure that **Distributed switch: 6.5.0** is selected, and then click **Next**.

![New Distributed Switch]

**Figure 99  Select Version**

7. Set the number of uplinks to **2**.
8. Choose to Enable **Network I/O Control**.
9. **Do not** create a default port group.
10. Click **Next**, and then **Finish**, to create the vDS.

![New Distributed Switch]

**Figure 100  Edit Settings**
11. Right-click the vDS and select “Edit Settings” under the “Settings” menu.

![Select vDS](image1)

**Figure 101** Select vDS

12. Under Advanced, set the MTU to 9000, and then click OK.

![Advanced Settings](image2)

**Figure 102** Advanced Settings

### 8.4.2 Create Port Groups

The next step is to create the necessary port groups on the vDS. At a minimum, port groups for Management and vMotion are required. For each port group perform the following steps:

1. Right-click the vDS, and select Distributed Port Group -> New Distributed Port Group.
2. Enter a **Name** for the port group (example: MgmtVL110), and then click **Next**.

![Select Name and Location](image1)

**Figure 103 Select Name and Location**

3. For tagged VLANs choose **VLAN** from the drop-down next to the **VLAN type** field.
4. Enter the appropriate **VLAN ID**.

![Configure VLAN Settings](image2)

**Figure 104 Configure VLAN Settings**

5. Select the **Customize default policies configuration** checkbox, and then click **Next**.
6. Review the security policies and traffic shaping options; click **Next** on each to proceed.
7. Set the **Load balancing** drop-down option to **Route based on originating virtual port**.
8. Ensure **Uplink 1** and **Uplink 2** are both active.
9. Click **Next**.
10. Click **Next** to proceed through the remaining menus.
11. Click the **Finish** button when it becomes active.

12. Repeat these steps for each distributed port group.
8.5 Configure Host Networking
Configuring host networking consists of the following procedures:

- Joining the compute cluster hosts to the virtual distributed switch (vDS)
- Migrating the existing networking
- Configuring new VMkernel ports for vMotion

8.5.1 Add Hosts to the vDS
To add the hosts to the virtual distributed switch:

1. Log into the vCenter web client at https://<vCenter Address>/vsphere-client.
2. On the Home screen, click the Networking icon.
3. Right-click the vDS for management traffic, and then click Add and Manage Hosts.
4. Ensure that Add hosts is selected, and then click Next.

![Add and Manage Hosts](image)

Figure 107  Select Task

5. Click ➔ New hosts icon, and select the hosts to add.

![Select new hosts](image)

Figure 108  Select New Hosts

6. Click OK, and then click Next.
7. Ensure that "Manage Physical Adapters" and "Manage VMkernel Adapters" are selected, and then click "Next"

8. Select a host vmnic1, and then click Assign Uplink.
9. Select Uplink 2 and then click OK.
10. Repeat steps 8-9 for each host and then click Next.
11. Select the first vmk0 that appears, and then click Assign Port Group.
12. Select the management traffic port group.

13. Repeat steps 11-12 for each additional vmk0.
14. Select a host, and then click New adapter to add a vmkernel port for vMotion.
15. Click Select an existing network, and then browse to select the vMotion port group.
16. Click OK, and then click Next.
17. On the Port Group Properties screen, check the **vMotion Traffic** checkbox, and then click **Next**.

18. Select **Use Static IPv4 settings**, and then enter the appropriate information into the text boxes:
   - a. IPv4 address
   - b. Subnet mask
   - c. Default gateway
   - d. DNS server addresses

19. Click **Next**, and then click **Finish**.

20. Select the **new vmkernel adapter**, and then click **Edit adapter**.

21. Click **NIC Settings** on the left, change the MTU value to **9000**, and then click **OK**.

22. Repeat steps 8–21 for each host being added to the vDS

23. Click **Next**.
Ensure that all hosts return **No impact.**

![Analyze Impact](image)

**Figure 114  Analyze Impact**

24. Click **Next** and then click **Finish.**

### 8.5.2 Migrate Networking

After the hosts have been added to the vDS and vmkernel ports migrated, **vmnic0** can be migrated over to the management traffic vDS. While still in the wizard, perform the following steps:

1. Right-click the **vDS for management traffic**, and then click **Add and Manage Hosts**.
2. Select **Manage Host Networking**, and then click **Next**.

![Select Task](image)

**Figure 115  Select Task**

3. Click **Attached hosts**, and then select **all hosts attached to the vDS**.
4. Select the **Configure identical networking settings** checkbox, located at the bottom of the wizard, and then click **Next**.
5. Select **any host** to use for template mode, and then click **Next**.
6. Ensure that only **Manage physical adapters** is selected, and then click **Next**.

![Select Network Adapter Tasks](image)

**Figure 116** Select Network Adapter Tasks

7. Select **vmnic0** on the top half of the wizard, and then click **Assign Uplink**.

Select ‘**Uplink 1**’ and click ‘**OK**’.

![Assign Uplink](image)

**Figure 117** Assign Uplink

8. In the middle of the wizard, click **Apply to all**, and then click **Next**.

![Assign to All](image)

**Figure 118** Assign to All
Ensure that all hosts return **No Impact.**

![Add and Manage Hosts](image)

**Figure 119  Analyze Impact**

9. Click **Next**, and then then click **Finish**.

### 8.6 Creating Compute Cluster

With the hosts joined to vCenter and connected to the appropriate virtual distributed switches the configuration is ready to be joined to a cluster. This section describes the steps to:

- Create the vCenter cluster object with DRS and HA enabled
- Moving the hosts to the cluster. Refer to the section on Management Cluster Setup if screenshots are necessary.

#### 8.6.1 Create vCenter Cluster Object

1. Open a web browser and navigate to the vSphere Web Client at [https://<VCSA FQDN or IP>/vsphere-client](https://<VCSA FQDN or IP>/vsphere-client).
2. Log in with an account that has administrator privileges.
3. On the home screen, navigate to **Hosts and Clusters**.
4. In the Navigator menu, right-click on the **virtual datacenter object**, and then click **New Cluster**.
5. Enter a **name** for the cluster (example: *Compute01*).
6. Enable DRS and HA by selecting the appropriate **Turn ON** checkbox next to each item.
7. Click **OK** to complete creating the cluster.

**NOTE:** Datastore heartbeat is a function of vSphere HA which, in the event a network issue arises, helps HA determine whether a host has failed, is in a network partition, or is network isolated. This feature requires a minimum of two shared datastores per cluster. A default set of datastores is selected by vCenter automatically. To change heartbeat settings within the vSphere Web Client, go to **Hosts and Clusters > Cluster_Name > Configure > vSphere Availability > Edit > Heartbeat Datastores.**
8.6.2 Move Hosts to the Cluster
After the cluster has been created the compute hosts are moved into the cluster by performing the following steps:

1. On the left pane displaying the host and cluster objects, select the first compute host.
2. Left-click the host, and hold the mouse button down.
3. Drag the host over the cluster object, and release the mouse.
4. After HA configuration completes for the first host, repeat step 3 for the remaining hosts.

8.7 Multipathing Optimization
Block storage presented to vSphere hosts from Dell EMC Unity has the native Path Selection Policy (PSP) of round robin (RR) applied by default. While RR is the recommended PSP to apply to Dell EMC Unity block storage, the default number of I/Os between switching paths is 1000. By reducing this value, all paths are more efficiently utilized.

1. The CLI command to make this change for all Dell EMC Unity LUNs on each vSphere host is:

```
for i in `esxcfg-scsidevs -c | awk '{print $1}' | grep naa.XXXX`; do esxcli storage nmp psp roundrobin deviceconfig set --type=iops --iops=# --device=$i; done
```

Where XXXX = the first four digits of the Dell EMC Unity disk (or endpoint) devices found using:

```
esxcli storage nmp device list
```

And # = the number of desired I/Os between the switching of paths.

2. Additionally, a claim rule can be created to automatically set this value on future LUNs mapped to the host by executing the following command in the CLI:

```
esxcli storage nmp satp rule add -s "VMW_SATP_ALUA_CX" -V "DGC" -P "VMW_PSP_RR" -O "iops=1"
```

8.8 Compute Cluster Configuration Checklist
Upon completing the sections above, the following items should be completed:

- VMware ESXi installed on compute hosts and added to vCenter
- Virtual Distributed Switch created and compute Networking configured in vCenter
- ESXi compute hosts joined to compute cluster in vCenter
9 Deploy Software Components

The Dell EMC Ready Stack includes OpenManage Integration for VMware vCenter, Dell EMC Virtual Storage Integrator, Avamar Virtual Edition, and Data Domain Virtual Edition in order to integrate the management of the Dell EMC hardware components into VMware vSphere. This section will describe the steps necessary to deploy these software applications. Additional steps are provided as examples for configuring the applications; however, Dell EMC recommends that you consult individual product documentation for a detailed set of instructions and to review advanced configuration options.

9.1 Deploy and Configure OpenManage Integration for VMware vCenter

The OpenManage Integration for VMware vCenter (OMIVV) is designed to streamline the management processes in your data center environment by enabling you to use VMware vCenter to manage your entire server infrastructure - both physical and virtual.

9.1.1 Prerequisites

Ensure your licenses are downloaded and ready to go. The license file format is XML.

You must have adequate system resources available for the OMIVV appliance VM, based on the number of managed nodes. See Table 14 below.

<table>
<thead>
<tr>
<th>Deployment Size</th>
<th>Number of Managed Nodes</th>
<th>Number of vCPUs</th>
<th>Memory (in GB)</th>
<th>Minimum Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Up to 250</td>
<td>2</td>
<td>8</td>
<td>44 GB</td>
</tr>
<tr>
<td>Medium</td>
<td>Up to 500</td>
<td>4</td>
<td>16</td>
<td>44 GB</td>
</tr>
<tr>
<td>Large</td>
<td>Up to 1000</td>
<td>8</td>
<td>32</td>
<td>44 GB</td>
</tr>
</tbody>
</table>

Ensure that:

- You use reservations (see vSphere documentation) to ensure that necessary memory resources are available to the OMIVV appliance VM
- The OMIVV appliance should have network access to iDRACs, hosts, and vCenter.
9.1.2 Deploy OpenManage Integration

Execute the following procedures to deploy OpenManage Integration to your data center environment.

9.1.2.1 Download the Zip File

1. Download the DellEMC_OpenManage_Integration_<version number>.<build number>.zip file from the Dell support website at www.dell.com/support.
2. Navigate to the location where you have downloaded the file.
   a. Extract its contents.

9.1.2.2 Deploy the Open Virtualization Format (OVF) File

To deploy the Open Virtualization Format (OVF) file that contains the OMIVV appliance by using the vSphere web client:

1. Locate the OMIVV virtual disk that you downloaded and extracted.
2. Run Dell_OpenManage_Integration.exe from a Windows client (Win7 SP1 or later) or a Windows server (2008 R2 or later).
3. Accept the EULA, and save the .OVF file.
4. Select a host from the VMware vSphere Web Client, and then in the main menu click Actions > Deploy OVF Template (or right-click Host and select Deploy OVF Template).
5. From the Deploy OVF Template wizard, click Browse.
6. Select the local files with filenames which start with OpenManage_Integration.

NOTE: For a quick installation, Dell EMC recommends that you host the files on a local drive.

7. In the Name field, enter the name of the VM which will be created (up to 80 characters).
8. In the Select a folder or datacenter list, select a location for deploying the template. Click Next.
9. Select the management cluster, and then click Next.

The Review Details window is displayed.

10. Click Next again.
11. In the Select Virtual Disk Format drop-down list, select Thick Provision (lazy or eager Zeroed) or Thin Provision.

NOTE: Thick Provision (Lazy Zeroed) offers the best balance of performance and deployment time.

12. In the VM Storage Policy drop-down list, select a policy, and then click Next.
13. In the Setup Networks window, click Next.

NOTE: Dell EMC recommends that the OMIVV appliance and the vCenter server are located in the same network.

14. In the Ready to Complete window, review the selected options for the OVF deployment and click Finish.

The deployment job runs and provides a completion status window where you can track the job progress.
9.1.2.3 Perform Initial OMIVV VM Configuration

To perform the initial configuration of the OMIVV VM:

1. From the vSphere web client:
   a. Locate and select the OMIVV VM you just deployed.
   b. Power on the virtual machine.

   NOTE: If you selected **Power on after Deployment** during step 2 above, the VM is powered on automatically.

2. Access the VM console by clicking the **Console** tab.
3. Allow OMIVV to complete booting up.
4. Enter the user name as **admin** (the default is admin), and press **Enter**.
5. Type in a new admin password that complies with the password complexity rules displayed in the interface, and press **Enter**.
   a. Reenter the password and then press **Enter**.
6. Once the basic configuration UI is displayed (see Figure 120 below), click **Date/Time Properties**.

   ![Configuration UI](image)

   **Figure 120 Configuration UI**
7. In the Date and Time tab, select **Synchronize date and time over the network**.
8. Add valid NTP server details (ideally use same NTP servers to which your vCenter is synchronized). Click **Time Zone** and select the applicable time zone, and click OK.
9. To configure a static IP to the OMIVV appliance, click **Network Configuration**, or skip to step 10.
   - Select **Auto eth0**, and then click **Edit**.
   - Select the **IPV4 Settings** tab, and select **Manual** in the **Method** drop-down.
   - Click **Add**, and then add a valid IP, Netmask, and Gateway information.
   - In the **DNS Servers** field, provide the DNS server detail and then click **Apply**.
10. To change the host name of the OMIVV appliance, click **Change Hostname**.
    a. Enter a valid host name, and click **Update hostname**.

   **IMPORTANT**: After host name and NTP are changed, ensure that the OMIVV VM is rebooted.

11. Open your preferred web browser and connect to https://<OMIVV Appliance IP or Hostname>, making sure to substitute the IP address or hostname of the appliance VM in the URL.
12. When prompted, enter the password you selected in step 5 above. See Figure 121 below.

![Login Screen](image)

**Figure 121  Login Screen**

The Administration Console displays. See Figure 122 below.
To register the vCenter server:

1. In the vCenter Registration window, click Register a New vCenter Server.
2. In the vCenter Name -> vCenter Server IP or Hostname text box, enter the server IP or host name.
3. Enter a description in the Description text box (optional).

NOTE: Dell EMC recommends that you use a Fully Qualified Domain Name (FQDN). If so, ensure that the host name of the vCenter is properly resolvable by the DNS server.

4. In the vCenter User Account -> vCenter User Name text box, enter the Admin user name or the user name with necessary privileges.
   a. Enter the username as domain\user or domain/user or user@domain. OMIVV uses the Admin user account, or the user with necessary privileges, for vCenter administration.
5. In Password, enter the password.
6. In Verify Password, enter the password again.
7. Click Register.
9.1.2.5 **Upload the License File**

To upload the license file:

1. Click **Upload License**.
2. In the **Upload License** window, click **Browse** to navigate to the license file.
3. Click **Upload** to import the license file.

9.1.2.6 **Verify the Installation**

To verify the OpenManage Integration installation:

1. Close any vSphere client windows.
2. Start a new vSphere web client.
3. Confirm that the OMIVV icon appears inside vSphere web client.
   a. Click **Home**, and then in **Administration** section look for the **Open Manage Integration** icon.
4. Ensure that vCenter can communicate with OMIVV by attempting a ping command from the vCenter server to the virtual appliance IP address or host name.
5. In vSphere Web Client, click **Home > Administration > Solutions**, and then click **Client Plug-Ins**.
6. In the **Client Plug-Ins** window, verify that OMIVV is installed and enabled.

9.1.3 **Configure OpenManage Integration**

This section describes the procedures required to configure the appliance.

9.1.3.1 **Open the Initial Configuration Wizard**

1. In vSphere web client, click **Home**, and then click the **OpenManage Integration** icon.

![vSphere Web Client](image-url)
2. The first time you click the OpenManage Integration icon, the Initial Configuration Wizard is displayed automatically.

NOTE: In the future, the wizard can also be accessed by navigating to OpenManage Integration > Getting Started, and then clicking Start Initial Configuration Wizard.

3. In the Welcome dialog box, review the steps, and then click Next.
4. Select the vCenter from the drop-down list.
5. Click Next.

9.1.3.2 Begin Creating a Connection Profile

A connection profile stores the iDRAC and host credentials that OMIVV uses to communicate with the Dell EMC servers. Each Dell EMC server must be associated with a connection profile to be managed by OMIVV. You can assign multiple servers to a single connection profile. Active Directory is supported but not required. Prerequisites include:

- If you wish to use Active Directory credentials with a connection profile, ensure that the user's account exists in Active Directory.
- The iDRAC and host should be configured for Active Directory based authentication.

NOTE: You cannot create a connection profile if the number of added hosts exceeds the license limit for creating a connection profile.

1. In the Connection Profile Description dialog box, click Next.
2. In the Connection Profile Name and Credentials dialog box, enter:
   a. The connection profile name (required)
   b. The description (optional)

![Name and Credentials Dialog]

Figure 124 Name and Credentials Dialog
9.1.3.3 To Use Active Directory

NOTE: If you wish to use Active Directory, perform the following steps. Otherwise, proceed directly to To Not Use Active Directory below.

1. If you wish to use Active Directory, execute the following steps:
2. Scroll down to iDRAC Credentials, and select Use Active Directory.
3. In Active Directory User Name, type the user name. Type the user name in one of these formats: domain\username or username@domain. The user name is limited to 256 characters.
4. In Active Directory Password, type the password. The password is limited to 127 characters.
5. In Verify Password, type the password again.
6. To download and store the iDRAC certificate and validate it during all future connections, select Enable Certificate Check.
7. Scroll down to Host Root section, and select Use Active Directory.
8. In Active Directory User Name, type the user name. Type the user name in one of these formats: domain\username or username@domain. The user name is limited to 256 characters.
9. In Active Directory Password, type the password. The password is limited to 127 characters.
10. In Verify Password, type the password again.
11. To download and store the host certificate and validate it during all future connections, select Enable Certificate Check.
12. Proceed directly to Continue Creating a Connection Profile below.

9.1.3.4 To Not Use Active Directory

NOTE: If you do not wish to use Active Directory, perform the following steps.

1. Scroll down to iDRAC Credentials section.
2. In User Name, type the user name. The user name is limited to 16 characters.
3. In Password, type the password. The password is limited to 20 characters.
4. In Verify Password, type the password again.
5. To download and store the iDRAC certificate, and validate it during all future connections, select Enable Certificate Check.
6. Scroll down to Host Root section.
7. The user name is root, which is the default and cannot be changed.
8. In Password, type the password.

NOTE: The password is limited to 127 characters.

9. In Verify Password, type the password again.
10. To download and store the iDRAC certificate, and validate it during all future connections, select Enable Certificate Check.
11. Proceed directly to Continue Creating a Connection Profile below.

9.1.3.5 Continue Creating a Connection Profile

1. Click Next.
2. In the Connection Profile Associated Hosts dialog box, select the hosts for the connection profile and then click OK.
3. To test the connection profile, select one or more hosts and then click Test Connection.
4. To complete the creation of profile, click **Next**.

### 9.1.3.6 Configure Inventory Jobs Schedule

To configure a schedule for inventory jobs:

1. From the **Inventory Schedule** dialog box, select **Enable Inventory Data Retrieval**.
2. Select the check box next to each day of the week that you want to run the inventory.
3. In **Data Retrieval Time**, enter the time in HH:MM format.

   **NOTE:** The time you enter is your local time.

4. To apply the changes and continue, click **Next**.

### 9.1.3.7 Configure Warranty Retrieval Jobs Schedule

To configure a schedule for warranty retrieval jobs:

1. In the **Warranty Schedule** dialog box, select **Enable Warranty Data Retrieval**.
2. Select the check box next to each day of the week that you want to run the warranty.
3. Enter the time in HH:MM format.

   **NOTE:** The time you enter is your local time.

4. To apply the changes and continue, click **Next**.

### 9.1.3.8 Configure Events and Alarms

To configure vCenter hardware events and alarms:

1. Select **Enable Alarms for all Dell EMC Hosts**.
2. Under **Event Posting Levels**, select the desired alert level.

   **IMPORTANT:** Dell EMC hosts which have alarms enabled respond to some specific critical events by entering in to maintenance mode.

   The Enabling Dell EMC Alarm Warning dialog box is displayed.

3. To accept the change, click **Continue**.
   a. Or, to cancel the change, click **Cancel**.
9.1.3.9 Close the Initial Configuration Wizard

1. Click Finish to conclude the initial configuration wizard.

9.1.3.10 Resolve Host Non-compliance

1. For vSphere 6.5 or later hosts, OMIVV requires that the WBEM service is enabled. Also, SNMP settings must be configured. Hosts must also be part of a connection profile. To address these compliance items through OMIVV, open OpenManage Integration for VMware vCenter.
2. Navigate to Manage > Compliance > vSphere Hosts.
3. Refresh the screen. If any hosts are listed, then they are non-compliant.
4. If there are no hosts listed and the screen is greyed-out, move on to section 10.1.3.11.
5. Click the **Fix non-compliant vSphere Hosts** button.
6. Review the text. Click **Next**.
7. Place a check next to any listed hosts.
8. Click **Finish**.
9. Allow OMIVV to process the necessary changes to all hosts.
10. When complete, refresh the screen to confirm there are no longer any non-compliant hosts.

### 9.1.3.11 Collect Inventory from Hosts

11. Validate functionality of OMIVV by running a one-off inventory job. Open **OpenManage Integration for VMware vCenter**.
12. Navigate to **Monitor > Job Queue > Inventory History > Hosts Inventory**.
13. Click the vCenter server in the **vCenters** list.
14. Click the **Run Now** button at the top of the area.
15. Wait for inventory jobs to complete. Refresh the screen and confirm all hosts show **Successful**.

### 9.1.3.12 Configure a Firmware Update Repository

To configure a repository for firmware update packages:

1. Open **OpenManage Integration for VMware vCenter**.
2. Navigate to the **Firmware Update Repository** -> **Appliance Settings** -> **Manage** > **Settings** tab.
3. Click the **Edit** (pencil) icon.
4. In the **Firmware Update Repository** dialog box, select one of the following:
   - **Dell Online** — OpenManage Integration for VMware vCenter downloads selected firmware updates from the Dell repository (ftp.dell.com), and updates the managed hosts.

   **NOTE:** Based on the network settings, enable proxy settings if required.

   - **Shared Network Folder** — A local repository of firmware in a CIFS-based or NFS-based network share. This repository can either be a dump of Server Update Utility (SUU) that Dell releases periodically or a custom repository created using DRM (Dell Repository Manager). This network share must be accessible by OMIVV.

   **NOTE:** If you are using CIFS share, the repository passwords cannot exceed 31 characters, and the special characters [@], [%], and [,] are not allowed. Also, SMB v1.0 is recommended for optimum compatibility.

5. If you select **Shared Network Folder**, enter the Catalog File Location by using the following format:
   - **NFS share for .XML file** — host:/share/filename.xml
   - **NFS share for .gz file** — host:/share/filename.gz
   - **CIFS share for .XML file** — \host\share\filename.xml
   - **CIFS share for .gz file** — \host\share\filename.gz

6. Click **Apply**.

   It may take up to 60 to 90 minutes to read the catalog from the source and update the OMIVV database.

### 9.2 Deploy Dell EMC Virtual Storage Integrator

The EMC Virtual Storage Integrator (VSI) for VMware vSphere Web Client is a plug-in for VMware vCenter that enables administrators to view, manage, and optimize storage.

#### 9.2.1 Deploy the VSI Appliance

To deploy the VSI appliance:

1. Download the **Solutions Integration Service OVA file**.
   a. From EMC Online Support, search for **VSI for VMware vSphere Web Client**.
   b. The downloaded file name for the current version is `emc_solutions_integration_service_v73_x86_64_OVF10.ova`.

2. Log in to the vSphere Web Client.
3. Select **Home** > **Hosts and Clusters**.
4. Right-click the **vCenter cluster**, and then select **Deploy OVF Template**. The following message appears:

   **This site is using the VMware Client integration Plug-In. Do you want to allow it to access your operating system?**

5. Click **Allow**.
The Deploy OVF Template wizard appears.

6. In **Select source**, enter the **location of the Solutions Integration Service OVA file**, and then click **Next**.
7. On the **Review details** screen, verify that the information is correct, and then click **Next**.
8. **Accept** the End User License Agreement (EULA), and then click **Next**.
9. In **Select name and folder**, enter a **name for the destination folder** (or accept the default).
10. Select the **folder or datacenter location** where you want to save the Solutions Integration Service OVA file, and then click **Next**.
11. For **Select a resource**, select the **compute resource**, and then click **Next**.
12. For **Select storage**, select the desired **disk format and datastore**, and then click **Next**.
13. For **Setup network**, use the values in Item 6 to:
   a. Select a **network**.
   b. Select the IP address format **IPV4** for the Solutions Integration Service.
14. For **Customize Template properties**:
   a. Enter the **IP address**, **default gateway**, **netmask** and **DNS server IP address**, if any.
   b. Click **Next**.
15. In the **Ready to Complete** dialog, verify the details, and then click **Finish**.
16. Right-click the **name** of the virtual machine with the newly deployed EMC Solutions Integration Service, and then select **Power On**.
17. Wait for the deployment to finish, and for the Solutions Integration Service to be operational.
18. Verify the **REST web service** as follows:
   a. Open a web browser, and navigate to **https://<Solutions_Integration_Service_IP Address>:8443/vsi_usm/** (example: **https://192.168.0.3:8443/vsi_usm/**)
   b. **Accept** all certificates, or **add** them to exceptions.
19. Change the **root password**:
   a. Log into the vSphere console with the default username **root** and password **root**.
   b. The operating system will prompt for a password change.
   c. Set a new, secure password for the root user.
20. Enable **SSH** on the machine:
   a. Log into the vSphere.
   b. Execute the following commands:

```
# systemctl enable sshd
# systemctl start sshd
```

   The SSH service is now enabled.

**9.2.2 Register the VSI Plug-in**

You must register the VSI plug-in to download and enable the VSI plug-in extensions.

1. Open a web browser and navigate to the **Solutions Integration Service Administrator web page**, logging in with the Solutions Integration Service credentials, at **https://<Solutions_Integration_Service_IP_ADDRESS>:8443/vsi_usm/admin**.
For example, https://192.168.0.3:8443/vsi_usm/admin.

2. Click **VSI Setup**.

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Service Info:</th>
</tr>
</thead>
</table>
| Home                        | **Version Number**: 7.3.2.141  
**Installation Timestamp**: 2018-03-27 07:37:56 PM  
**Local Timestamp**: 2018-04-06 01:41:41 PM |
| Log                         | **Please click one of the functions on the left.**                            |
| VSI Setup                   |                                                                               |
| Database                    |                                                                               |
| User                        |                                                                               |
| Connection Broker           |                                                                               |
| Data Protection             |                                                                               |
| SSH Key                     |                                                                               |
| Log Out                     |                                                                               |

Figure 127  **VSI Administration**

3. Enter the values for the following parameters:
   - **vCenter IP/Hostname** - The IP address that contains the VSI plug-in package.
   - **vCenter Username** - The username that has administrative privileges.
   - **vCenter Password** - The administrator’s password.
   - **Admin Email (Optional)** - The email address to which notifications should be sent.

4. Click **Register**.
5. Browse to the **vSphere Web Client** address.
6. In the vSphere Web Client window, select **vCenter** in the navigation pane to verify that EMC VSI is listed.
9.3 Data Domain Virtual Edition

Dell EMC Data Domain Virtual Edition (DD VE) is a data protection storage system. It is a virtual (software-only) deduplication appliance. Data Domain systems are always paired with backup software. The backup software specified in this guide is Dell EMC Avamar. See conceptual layout below.
NOTE: Data Domain is also available as a physical appliance, although that is outside the scope of this guide. Both physical and virtual Data Domain appliances run the Data Domain Operating System (DD OS). Both provide the DD OS command line interface (CLI) and the Data Domain System Manager graphical user interface (GUI) for performing all system operations.

9.3.1 Prerequisites

This section describes Dell EMC Ready Stack hardware requirements for DD VE.

9.3.1.1 System Resources

Adequate system resources must be available for the DD VE appliance VM, which is based on the number of managed nodes. See Table 15 below.

<table>
<thead>
<tr>
<th>VM Resource</th>
<th>Storage Capacity Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Cores</td>
<td>&lt;500 GB</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 15 Required System Resources
### IMPORTANT: Do not reduce system memory after you have created the file system in DD OS. This makes the file system unusable. Use reservations (see vSphere documentation) to ensure that necessary memory resources are available to the appliance VM.

#### 9.3.1.2 Network Adapters

DD VE can support up to eight virtual network adapters. For VMware environments, the ova package creates two VMXNET3 virtual network adapters by default. DHCP will be configured automatically on these two interfaces inside the DD VE. DHCP can be configured manually on any additional interfaces.

#### 9.3.1.3 Disk Controllers

One SCSI Controller is configured by default. The maximum number of disks for each controller is 15 for vSphere. If the environment requires more than the maximum number of disks, you can add extra SCSI HBA controllers to the DD VE appliance VM. For VMware environments, DD VE supports up to four VMware Paravirtual SCSI Controllers.

**NOTE:** Other types of SCSI controllers are not supported.

**IMPORTANT:** Backend storage for DD VE should already be provisioned and ready. Best practice dictates that backups be stored on separate storage from production VMs/data (i.e., not stored on the Unity array deployed earlier in this guide). Such secondary storage is not part of the scope of this guide.

#### 9.3.2 Deploy Data Domain Virtual Edition

This section describes the procedures required to deploy DD VE in the Dell EMC Ready Stack environment.

**9.3.2.1 Download the Zip File**

To download the zip file:

1. Download the .zip file DD VE package for vSphere from [https://support.emc.com](https://support.emc.com).
2. Navigate to the location where you have downloaded the file, and extract its contents.

**9.3.2.2 Deploy the OVA File**

To deploy the OVA file:

1. From the VMware vSphere Web Client, select a **host**.
2. In the main menu, click **Actions > Deploy OVF Template** (or right-click host and select **Deploy OVF Template**).
The OVF Template Wizard opens.

3. From the Deploy OVF Template wizard:
   a. Click **Browse**.
   b. Select the **local file**.
   c. Click **Next**.

**NOTE:** For a quick installation, Dell EMC recommends that you host the OVA on a local drive.

4. In the Name field, enter the **name** of the VM which will be created (up to 80 characters).
5. In the Select a folder or datacenter list:
   a. Select a **location** for deploying the template.
   b. Click **Next**.
6. Select the **management cluster**, and then click **Next**.

The Review Details window displays.

7. Click **Next**.
8. **Accept** the license agreement and then click **vSphere Web Client**.
9. Select the appropriate configuration.

Default is 4 TB capacity, which requires 2x vCPU cores and 6 GB memory. See below.

![Select Configuration Screen](image)

**Figure 130  Select Configuration Screen**

10. Click **Next**.
11. In the **Select Virtual Disk Format** drop-down list, select **Thick Provision (Lazy Zeroed)** for best balance of performance and deployment time.
12. In the **VM Storage Policy** drop-down list, select a policy.
13. Select desired **datastore destination**, and then click **Next**.
14. In the **Setup Networks** window:
   a. Select network settings.
   b. Click **Next**.
15. In the **Ready to Complete** window:
   a. Review the selected options for the OVF deployment.
   b. Click **Finish**.

The deployment job runs and provides a completion status window, where you can track the job progress.

16. Wait until the deployment job is complete.

### 9.3.3 Perform Initial DD VE Configuration

Perform the initial configuration of DD VE from a VM console command line.

#### 9.3.3.1 Begin Setup

1. From the vSphere web client:
   a. Locate and select the **Data Domain Virtual Edition (DD VE) VM** you just deployed.
   b. **Power on** the virtual machine.

   **NOTE:** If you selected **Power on after Deployment** during deployment, the VM is powered on automatically.

2. Access the VM console by clicking the **Console** tab.
3. Allow DD VE to complete booting up.
4. Log in with the default credentials:
   a. **User** - `sysadmin`
   b. **Password** - `changeme`
5. When prompted to change the default sysadmin password:
   a. **Type** `yes`
   b. **Press** Enter
6. **Type** in a **new password** which complies with the password complexity rules displayed in the interface, and then press Enter.
7. Reenter the password, and then press **Enter**.
8. When prompted if you want to configure the system using the GUI wizard:
   a. **Type** `no`
   b. **Press** Enter

   **NOTE:** Although the built-in default options during deployment assume the user is utilizing DHCP, this guide follows a validated process for manual IP address deployment for maximum compatibility. If using DHCP, a few steps will differ. Those steps will be noted.
9.3.3.2 Configure the Network

1. When prompted if you want to configure the network:
   a. Type yes
   b. Press Enter (unless using DHCP)

2. When prompted if DHCP is to be used:
   a. Type no
   b. Press Enter (unless using DHCP)

3. When prompted for the hostname to be used for the DD VE appliance:
   a. Enter the fully qualified domain name (FQDN)
   b. Press Enter

4. Provide the DNS domain name when requested, and then press Enter.

5. When prompted if Ethernet port ethV0 is to be enabled:
   a. Type yes
   b. Press Enter

6. When prompted if DHCP is to be used on ethV0:
   a. Type no
   b. Press Enter (unless using DHCP)

7. If prompted for IP address:
   a. Enter the desired static IP address
   b. Press Enter (not applicable if using DHCP)

8. Enter the netmask if prompted, and then press Enter (not applicable if using DHCP).

9. Follow the same procedure for the prompts relating to Ethernet port ethV1.

10. When prompted, enter the default gateway address, and then press Enter.

11. When prompted, enter the IPv6 default gateway address (or leave blank), and then press Enter.

12. When prompted, enter the IP addresses of the DNS servers (up to 3), and then press Enter.

13. When prompted whether or not you want to save the configuration:
   a. Type save
   b. Press Enter

14. When prompted whether or not to Configure eLicenses:
   a. Type no
   b. Press Enter

15. When prompted whether or not to Configure System:
   a. Type no
   b. Press Enter

9.3.3.3 Add Virtual Disks

Add one or more virtual disks to DD VE VM to serve as targets for storing Avamar backups.

NOTE: See Prerequisites for important information.

1. From the vSphere web client, locate and select the Data Domain Virtual Edition (DD VE) VM.
2. Right-click on the VM, and then select Edit Settings.
3. At the bottom of the Settings window, open the New Device drop-down list.
4. Choose New Hard Disk from the list, and then click Add.
A new virtual hard disk appears in the list of devices assigned to the VM.

5. Expand the drive details of **New Hard Disk** by:
   a. Clicking the **right arrow** next to it
   b. Inputting the desired **capacity size**

6. Default settings are fine for most settings, but ensure that:
   a. **Location** is set to correct secondary storage (not the Unity array deployed earlier in this guide)
   b. **Disk Provisioning** is set to **Thick provision** (lazy or eager zeroed)

![New Hard Disk Screen](image)

**Figure 131 New Hard Disk Screen**

### 9.3.3.4 Enable the Virtual Disks

Run VM console CLI commands to enable the newly added virtual disk(s).

1. From the vSphere web client, locate and select the **Data Domain Virtual Edition (DD VE) VM**.
2. Access the VM console by clicking the **Console** tab.
3. Login as **sysadmin**, with the password selected in **Begin Setup**.
4. Verify the newly-added disk:
   a. Run the **storage show all** command
   b. Verify the newly added disk is shown (in unknown state). Make note of the device number as it is needed in the next step.
   c. Run the **storage add dev<number>** command, where `<number>` is the device number from step 4.b.
5. Click **OK**.
6. If additional disks were added in Add Virtual Disks, repeat the steps in Enable the Virtual Disks as needed.

### 9.3.4 Complete DD VE Configuration

Connect to the Data Domain System Manager (DDSM) GUI to complete the remaining configuration tasks.
1. Open a web browser and navigate to the DDSM GUI at https://< DD_VE_VM_IP Address_or_Hostname>.
2. Login as sysadmin, with the password selected in Begin Setup.

A screen will pop up, requesting a valid license.

3. Browse for the .XML format license file you received with your purchase.
4. Click Apply.

**NOTE:** Future license management tasks can be performed in the Administration sub-menu.

5. From the DDSM GUI home screen, navigate to Maintenance -> Configure System to launch the initial setup wizard.

**NOTE:** Configuration tasks can be completed elsewhere via GUI or CLI, but this guide leverages the GUI configuration wizard for ease of deployment.

6. At the Network prompt, click No.
7. At the Configure File System prompt, click Yes.
   a. Confirm that the new virtual disks added to the VM in step 5 are listed.

   ![Addable Storage Screen](image)

   **Figure 132 Addable Storage Screen**

   b. Click Next.
   c. Run the storage assessment if desired, or click Skip.
   d. Check Enable file system after creation, and then click Submit.
   e. When complete, click OK.
8. At the Configure System Settings prompt, click Yes.
   a. There is no need to change the sysadmin password again, so leave the password fields blank.
   b. Enter the administrator's email address in the Admin Email field.
   c. Clear the checkboxes of any unwanted notifications, and then click Next.
   d. Provide the mail server and physical location information, and then click Next.
   e. Review the summary details, and then click Submit.

9. At the Configure DD Boost prompt, click No. The Avamar deployment will configure its own DD Boost storage unit automatically.
10. At the Configure CIFS prompt, click No.
11. At the Configure NFS prompt, click No.

This concludes the setup wizard, as well as the necessary configuration tasks for Data Domain within the scope of this guide. After deployment, you should become familiar with the other settings available in the management GUI. Also, more extensive documentation specific to Data Domain can be found at https://support.emc.com.

9.4 Avamar Virtual Edition
Dell EMC Avamar enables fast, efficient backup and recovery by reducing the size of backup data at the client—before it’s transferred across the network and stored. Avamar's variable-length deduplication dramatically reduces network traffic by only sending unique blocks, compressed and encrypted over local area networks (LANs) or wide area networks (WANs). Blocks that were previously stored are never backed up again.

9.4.1 Deployment Options
Avamar Data Store – EMC Avamar Data Store combines an EMC-certified purpose-built backup appliance and Avamar deduplication backup and recovery software in a fully integrated, scalable, prepackaged solution.


Avamar Virtual Edition – Avamar deduplication backup software and virtual appliance deployed in vSphere or Hyper-V and Azure.

9.4.2 Integration
Integration with Data Domain deduplication storage systems – take advantage of Data Domain's performance and scale for all backup workloads. The scope of this guide includes:

- EMC Avamar Virtual Edition (AVE) is a single-node Avamar server that runs as a virtual machine in a VMware ESXi. AVE integrates the latest version of Avamar software with SUSE Linux as a VMware virtual machine. AVE is the backup solution deployed in this guide, with Data Domain (Virtual Edition in this guide) as the storage target and leveraging the powerful integration of the two products.
- For virtual clients, there are two options for backups with AVE.
- Through guest OS backups (requires installing Avamar client software on each virtual machine)
- Through host-based backups (requires a proxy server)

This document describes setting up the latter: host-based backups for virtual clients. As mentioned above, Data Domain provides the backend storage for housing the Avamar backups. See the conceptual taxonomy layout in Figure 129.

9.4.3 Prerequisites
Adequate system resources must be available for the Avamar VM, which is based on backup storage capacity. See Table 16 below.

<table>
<thead>
<tr>
<th></th>
<th>0.5 TB AVE</th>
<th>1 TB AVE</th>
<th>2 TB AVE</th>
<th>4 TB AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>2x 2GHz</td>
<td>2x 2GHz</td>
<td>2x 2GHz</td>
<td>4x 2GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB</td>
<td>8 GB</td>
<td>16 GB</td>
<td>36 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>900 GB</td>
<td>1650 GB</td>
<td>3150 GB</td>
<td>6150 GB</td>
</tr>
</tbody>
</table>

9.4.4 Deploy AVE
This section describes the procedures required to deploy AVE in the Dell EMC Ready Stack environment.

9.4.4.1 Download the Zip File
1. Download the AVE virtual appliance package file from [https://support.emc.com](https://support.emc.com).
2. Extract the contents.

9.4.4.2 Deploy the OVA File
AVE employs a two-step initial deployment process:
- Deploying the OVF – See Deploy the OVA File, and Disable MCS Certificate Authentication
- Software installation – See Install Software

To deploy the OVA file:
1. From the VMware vSphere Web Client:
   a. Select a **host**.
   b. In the main menu, click **Actions > Deploy OVF Template** (or right-click the host, and then select **Deploy OVF Template**).
2. From the **Deploy OVF Template** wizard:
   a. Click **Browse** and select the local file.
NOTE: For a quick installation, Dell EMC recommends that you host the OVA on a local drive.

b. Click Next.
3. In the Name field, enter the name of the VM which will be created (up to 80 characters).
4. In the Select a folder or datacenter list:
   a. Select a location for deploying the template.
   b. Click Next.
5. Select the management cluster, and then click Next to display the Review Details window.
6. Click Next.
7. Accept the license agreement, and then click Next.
8. In the Select Virtual Disk Format drop-down list, select Thick Provision (Lazy Zeroed) for the best balance of performance and deployment time.

IMPORTANT: Thin provisioning is not supported with AVE.

9. In the VM Storage Policy drop-down list, select a policy.
10. Select the desired datastore destination, and then click Next.
11. In the Setup Networks window:
   a. Select Network Settings.
   b. Click Next.
12. In the Customize Template window, enter the following:
   a. DNS Server(s)
   b. Hostname FQDN
   c. IPv4 Address with Mask/Prefix
   d. IPv4 Default Gateway
   e. NTP Server(s)
13. In the Ready to Complete window:
   a. Review the selected options for the OVF deployment.
   b. Click Finish.

The deployment job runs, and provides a completion status window where you can track the job progress.

14. Wait until the job is complete.

9.4.4.3 Disable MCS Certificate Authentication
This section describes the steps required to disable Management Console Server (MCS) certificate authentication, if your environment does not use it.

1. From the vSphere web client:
   a. Locate and select the Avamar VM you just deployed.
   b. Power on the virtual machine.

   NOTE: If you selected Power on after Deployment during Deploy the OVA File, the VM is powered on automatically.

2. Access the VM console by clicking the Console tab.
3. Wait until the login prompt appears.
NOTE: If you do not want to add vCenter authentication certificates to the Avamar MCS keystore, you must disable certificate authentication for all vCenter-to-Avamar MCS communications by running the following commands at the Avamar console command line. Otherwise, the Avamar software installation will fail.

4. Log in as admin, with the password of changeme.
5. Stop the MCS by executing the following command:

   dpnctl stop mcs

6. Open /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml in a UNIX text editor, such as vi.
7. Find the ignore_vc_cert entry key.
   a. For example, type /ignore_vc_cert in vi.
8. Change the ignore_vc_cert setting to true, so that it looks like this:

   <entry_key="ignore_vc_cert" value="true" />

9. Save your changes, and then close mcserver.xml.
10. Start the MCS and the scheduler by executing the following commands:

    dpnctl start mcs
    dpnctl start sched

9.4.4.4 Install Software

To begin software installation:

1. Open a web browser and navigate to Avamar Installation Manager at https://<Avamar-server>:7543/avi, where <Avamar-server> is the IP address or hostname of the AVE VM.

   The Avamar Installation Manager login page appears.

2. Enter the following credentials:
   a. Type root in the User Name field.
   b. Type changeme in the Password field.
3. Click Login.
4. Click SW Releases.
5. Optional: Click the ? button next to the AVE installation package, **ave-config**, to open the help file for the AVE installation workflow.
6. Click **Install** next to the AVE installation package, **ave-config**.

### 9.4.4.5 Complete AVE Installation

The **Installation Setup** screen includes a number of tabs with empty fields. Note that:

- Required fields are displayed in red/orange with exclamation marks next to them.
- All required fields must be completed before proceeding.
- You can save your place at any time using the **Save** button.
1. Fill out the required fields in the **ConnectEMC** tab (see Figure 135 above):
   a. **Email sender address**
   b. **Email server hostname or IP address**
   c. **Site name**
2. Click the **License Upload** tab.
   a. Check the box next to *Show advanced settings* in the lower-left area.
   b. Browse for and upload **Avamar-related license files**.
3. Click the **Passwords** tab.
   a. Enter and re-enter the desired *password* for each item.
   b. If you want a single password for everything, check the box next to *Use common password*.

**NOTE:** Avamar password complexity rules can be viewed by hovering over the **Description** field next to a password. The rules require at least one of the following “,” “-“, or “_” characters (without the quotes).

4. Click the **Customer Contact Info** tab.
   a. Complete required fields.
5. Click the **Server Settings** tab.
   a. Select **time zone** from drop-down list.

**NOTE:** This solution supports encryption. Configuring encryption is outside the scope of this guide.

6. Click the **Data Domain Settings** tab.
a. Check the box next to Add Data Domain.

7. In the **Data Domain Address** field, enter one of the following options for the Data Domain Virtual Edition VM deployed earlier in this guide:
   a. IP address
   b. DNS-resolvable FQDN

8. In the **Data Domain Administrator Name** field, enter **sysadmin**.

9. In the **Data Domain Administrator Password** field, enter the DD VE sysadmin password.

10. Check the box next to **DDBoost create new login account**.

   **NOTE:** If you are not closely following this guide and already created a DDBoost user in advance, you can use it here but it must be configured with admin access. This is required by Avamar.

11. In the **DDBoost Login Name** field, enter the desired user name (for example **BoostUser**).

   This will be a new account created for you in Data Domain for managing the DDBoost integration between Avamar and DD VE.

12. In the **DDBoost Login Password** field, enter the desired password for the new DDBoost account.
   a. Hover over **Description** to view complexity rules.

13. In the **DDBoost Login Password(Confirm)** field, re-enter the password.

14. In the **SNMP Community String** field, enter the desired value.

15. Click **Continue**.

16. Monitor the installation progress on the **Installation Progress** page.

17. Wait until the installation is complete.

   **NOTE:** If the installation fails on **Attaching Data Domain to Avamar**, confirm that Disable MCS Certificate Authentication was observed. Also ensure that steps 10 through 13 in Complete AVE Installation were completed.

### 9.4.4.6 Configure AVE

With software installation fully completed, the remaining configuration tasks can be completed in the AVE GUI known as **Avamar Administrator**, also known as the Management Console (MC).

1. Open a web browser and navigate to the Avamar Administrator (MC) GUI at `https://<Avamar_VM_IP_or_Hostname>/mc-portal/mcgui`.

   **NOTE:** This is a Java app, so Java must be installed and enabled on your client. Also, ensure that the AVE hostname is added to DNS.

2. Login as **root** with password selected in step 2.b.

3. The **Avamar Administrator main screen** appears.
4. Add the vCenter server to Avamar for visibility and access to the VMs requiring backups:
   a. In Avamar Administrator, click **Administration**.
   b. Click the **Account Management** tab.
   c. In the tree view, select the **Top-level (root) domain -> Actions -> Account Management -> New Client(s)**.
   d. In the Client Type list, select **VMware vCenter**.
5. Agentless image-based (as opposed to file-based) backups in AVE require one or more Avamar proxy VMs. AVE will analyze the environment and make a recommendation:
   a. In Avamar Administrator, select VMware -> Proxy Deployment Manager.
   b. Choose a vCenter.
   c. Set the Data change rate. The default data change rate of 12% (.12) is a conservative setting that is known to work with most customer sites.
   d. Set the Backup window (in minutes).
   e. To include virtual machines using direct attached storage in this recommendation, select Protect VM's on local storage.
   f. Click Create Recommendation.

   The tree pane shows the proposed deployment topology. Proposed new proxies appear under each ESX host with the name New proxy.
g. In the tree pane, select a New proxy, and then click Edit.

h. Type the proxy name in the Name field.

i. Select an Avamar Server Domain where this proxy will reside.

j. Type the IP address into the IP field.

k. Select a datastore from the Datastore list.

l. Select a virtual network from the Network list.

m. Type the fully qualified DNS server name or IP address into the DNS String field.

n. Type the network gateway IP address into the Gateway field.

o. Type the network mask into the Netmask field.

p. Click Save.

q. When the proposed deployment topology is satisfactory, click Apply.

NOTE: Alternatively, you can add folders or resource pools of VMs. These are known in AVE as containers. This guide will cover clients only, not containers.

6. Add the VMs you want to backup. These are known in AVE as clients:
a. In Avamar Administrator, click **Administration**.
b. Click the **Account Management** tab.
c. In the upper tree, select a **vCenter domain or subdomain**.
d. Select **Actions -> Account Management -> New Client(s)**.

The Select VMware Entity dialog box appears. In this dialog:

- The **VMs & Templates** tab is equivalent to the vSphere Virtual Machines and Template view.
- The **Hosts & Clusters** tab is equivalent to the vSphere Hosts and Clusters view.

e. In the tree, select a **folder that contains a VMware entity**.
   
i. To view all entities within the selected folder, select **Show sub-entities**.

f. In the right properties pane, select a **virtual machine or vApp to protect** with Avamar backups.

[Image: Select VMware Entity Pane]

- **Figure 139** Select VMware Entity Pane

- To enable changed block tracking, select **Enable changed block tracking**, and then click **OK**.

**NOTE:** If changed block tracking is not enabled, each virtual machine image must be fully processed for each backup, which might result in unacceptably long backup windows, or excessive back-end storage read/write activity. Enabling changed block tracking will not take effect until any of the following actions occur on the virtual machine: **reboot, power on, resume after suspend, or migrate**.

h. Enter **contact information** if needed, and then click **OK**.

i. Click **Close**.

j. If you enabled changed block tracking, the VM to be backed up must be **rebooted, suspended/resumed, or migrated**.

7. Configure the backup policy for the client VM you added:

   a. In Avamar Administrator, click **Policy**.
b. Click the **Policy Management** tab, and then click the **Clients** tab.

c. Double-click a virtual machine (or select a VM, and then click **Edit**).

The Edit Client dialog box appears.

- d. Click the **Retention Policy** tab. You can accept the default policy or override and set custom values.
- e. Click the **Groups** tab. Group membership for the client can be modified. Groups and schedules are discussed in depth in section 10.4.4.7.
- f. Click the **VMware** tab. Shared/clustered datastores used by the client are listed. Changed block tracking can be enabled or disabled.

8. Run a one-time test backup of the client VM:

   a. In **Avamar Administrator**, click **Backup & Restore**.
   b. Click the **Backup** tab.
   c. In the tree view, click the **vCenter server**. Active clients are listed below the tree.
   d. Select a **client VM**. Place a check in the box next to the root level object.
   e. From the pull-down menu, select **Actions -> Back Up Now**.
   f. Accept the default backup settings, or adjust parameters as desired.
   g. Click **OK**.
   h. Click **Close**.
   i. Monitor progress by returning to the main **Avamar Administrator** screen, and then clicking **Activity**.

![Activity Pane](image)

**Figure 140 Activity Pane**

9. Validate DD VE and AVE deployment by testing restore functionality:

   a. Wait for backup in step 8 on to complete.
   b. In Avamar Administrator, click **Backup & Restore**.
c. Click the **Restore** tab.

d. In the tree view, click the **vCenter server**. Active clients are listed below the tree.

e. Select the **client VM** from step 8.d, and then choose the **current date**.

f. Click the **backup image** listed in the upper-right pane.

g. Select the **checkbox next to the root level object** in the lower-left pane.

h. From the pull-down menu, select **Actions -> Restore Now**.

i. In the drop-down list, select **Restore to a new virtual machine**.

**IMPORTANT:** Restoring to original virtual machine can result in data loss! Be careful not to restore to original virtual machine unless you know for certain your use case allows for it (e.g., test VM, static VM). Even restoring to a new VM can cause issues if you connect the VM to the network without changing IP address within guest OS. Restoring critical infrastructure VMs like vCenter is discouraged (unless required and the procedures are well-understood).

j. Click **Configure Destination**, enter a **Name** for the new VM, and then click **Next**.

k. Select a **host or cluster**, and then click **Next**.

l. Select a **datastore**, and then click **Next**.

m. Review the **details**, and then click **Finish**.

n. Click **OK**.

o. Click **Close**.

p. Monitor progress by returning to the main **Avamar Administrator** screen and clicking **Activity**.

**IMPORTANT:** If you choose to power on the restored VM to confirm completeness, make sure to disconnect its virtual network connections to prevent duplicate IP issues with the original.

10. Optionally, you can restore individual files from a VM image backup:

   a. In Avamar Administrator, click **Backup & Restore**.

   b. Click the **Restore** tab.

   c. In the tree view, click the **vCenter server**. Active clients are listed below the tree.

   d. Select the **client VM** from step 8.d, and then choose the **current date**.

   e. Click the **backup image** listed in the upper-right pane.

   f. Click the **Browse for Granular Restore** button.

   ![Contents of Backup](image)

   **Figure 141** **Browse for Granular Restore**

   g. In the **Proxy Selection** window, click **OK**.

   h. Wait for tree view to switch to folder/file list. This may take several minutes.

   i. Select the desired folders and/or files.

   j. From the pull-down menu, select **Actions -> Restore Now**.

   k. Select **Restore everything to a different location**, and then click **Browse** to choose the destination.
l. Click **OK**, and then click **Close**.

m. Monitor progress by returning to the main **Avamar Administrator** screen, and then clicking **Activity**.

**IMPORTANT:** Restoring to original location can result in data loss! Be careful not to restore to original location unless you know for certain your use case allows for it (e.g., test VM, static VM). Restoring to critical infrastructure VMs like vCenter is discouraged (unless required and the procedures are well-understood).

9.4.4.7 Configure Policies and Schedules

Initial deployment is fully completed and backup/restore functionality has been validated. The final process involves setting up policies and schedules.

1. Configure the dataset default target to point to Data Domain.
   a. Open a web browser and navigate to the Avamar Administrator (MC) GUI at https://<Avamar_VM_IP_or_Hostname>/mc-portal/mcgui.
   b. From Avamar Administrator, select **Tools** -> **Manage Datasets**.
   c. Within **Manage All Datasets**, left-click **VMware Image Dataset**, and then click **Edit**.
   d. Within **Edit Dataset**, select the **Options** tab.
   e. In the **Select Plug-in Type** list, choose **Linux VMware Image** (for backing up VMs which run a Linux OS).
   f. Check the box next to **Store backup on Data Domain system**, and then select the **Data Domain system** in the list.
   g. Click **OK**.
   h. Repeat step 1.d for any other datasets you intend to use (example: **Windows VMware Image** for VMs running a Windows OS).
2. Create a backup schedule:
   a. From Avamar Administrator, select **Tools -> Manage Schedules**.
   b. Within **Manage All Schedules**, and then click **New**.
   c. In the **Name** field, enter a descriptive name of your choice (example: Daily Backups).
   d. Choose the desired days and timing (example: **7 days a week from 10:00 pm to 6:00 am**).

   **NOTE**: If backups do not finish by listed end time, default behavior is to terminate at that time. However, the first backup of a client is allowed to go beyond this end time. Although a terminated backup is not visible in Avamar, it is kept for a short time as a continuation point for the next backup (i.e., it picks up where it left off).

   e. Click **OK**.
For ease of administration, Dell EMC recommends that you set up one or more backup groups. A group in Avamar is merely a logical container for organizing clients. Setting attributes at the group level saves the time and effort of setting these at individual client level. Start by creating a group to back up the critical infrastructure appliance VMs.

3. Create a backup group:
   a. From main Avamar Administrator window, click Policy.
   b. From Policy window, go to Actions -> New > Group -> Backup Group.
   c. Enter a descriptive name of your choice (example: Management VMs) in the Name field.
   d. Enable the group by clearing the checkbox next to Disabled.
   e. Click Next.
   f. Ensure that VMware Image Dataset is selected in Select an Existing Dataset list.
   g. Select the desired plug-in type (example: Linux VMware Image in this case for VMs which run a Linux OS).
   h. Click Next.

**Figure 143  Create Backup Schedule**

NOTE: Enabling the group means recurring backups will start being created based on the chosen schedule when this wizard is completed.
i. Choose the desired **schedule** from the list. If you created a schedule in step 2, it will be available in the list.

j. Click **Next**.

k. Choose the desired **retention policy**, and then click **Next**

```
NOTE: Retention refers to the length of time for which the system will keep backups of a client. After that time, the space will be reclaimed for use by the system. This guide does not discuss creation of custom retention schedules, but this can be done from Avamar Administrator by navigating to **Tools -> Manage Retention Policies**.
```

l. Highlight the desired **clients**. For the first group, select the critical management VMs such as vCenter, OMIVV, and VSI.

m. Click **Include**, and then click **Next**.

n. Check the box next to **Auto proxy mapping**, and then click **Finish**.

o. Repeat step 3 as needed to create other logical groupings of VMs for backup.

p. Monitor status regularly over time to ensure that backups are occurring successfully, by navigating to the Avamar Administrator main window, and then clicking **Activity**.

9.5 Monitoring Components Deployment Checklist

The following should be deployed once finished with this section:

- ✔ Deployment of OpenManage Integration for VMware vCenter
- ✔ Deployment of Dell EMC Virtual Storage Integrator
- ✔ Deployment of Dell EMC Avamar Virtual Edition
- ✔ Deployment of Dell EMC DataDomain Virtual Edition
10 References

- Dell EMC PowerEdge R640 Installation and Service Manual
- Integrated Dell Remote Access Controller 9
- iDRAC9 Systems Management – Wiki
- Dell EMC Unity Family Installation Guide
- Dell EMC Unity: Best Practices Guide
- Dell EMC Unity Unisphere CLI User Guide
- VMware vSphere Documentation
- Dell Configuration Guide for the S3048–ON System
- Dell EMC Networking OS Configuration Guide for the S5048F–ON System
- Brocade Fabric OS Web Tools Administrator’s Guide
- VSI for VMware vSphere Web Client Product Guide
- OpenManage Integration for VMware vCenter Web Client Installation Guide
- Avamar Virtual Edition for VMware System Installation Guide
- Data Domain Virtual Edition Installation and Administration Guide
Site Survey

Table 17  Network Topology

<table>
<thead>
<tr>
<th>Network Topology</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Switch Hostnames</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Switch</th>
<th>Hostname</th>
<th>Management IP</th>
<th>VLT Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3048</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5048-Top</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5048-Bottom</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional Configuration Notes (Spanning-Tree, Routing Protocol etc. – if applicable):

Table 18  VLAN Information

<table>
<thead>
<tr>
<th>VLAN Information</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Network Type</th>
<th>VLAN ID</th>
<th>S5048-Top IP CIDR</th>
<th>S5048-Bottom IP CIDR</th>
<th>VRRP IP</th>
<th>VRRP Group</th>
<th>S3048 IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Band</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>110</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### VLAN Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vMotion</td>
<td>120</td>
</tr>
<tr>
<td>Compute VM</td>
<td>210</td>
</tr>
</tbody>
</table>

### Table 19  Customer Network Services

<table>
<thead>
<tr>
<th>Customer Network Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hop/Default Route:</td>
</tr>
<tr>
<td>DNS:</td>
</tr>
<tr>
<td>NTP:</td>
</tr>
</tbody>
</table>

### Table 20  Switch Port Mappings

<table>
<thead>
<tr>
<th>Switch Port Mappings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>S5048 Top</td>
</tr>
<tr>
<td>S5048 Bottom</td>
</tr>
<tr>
<td>S3048</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>NIC Port 1</td>
</tr>
<tr>
<td>NIC Port 2</td>
</tr>
<tr>
<td>iDRAC</td>
</tr>
<tr>
<td>Mgmt1</td>
</tr>
<tr>
<td>Mgmt2</td>
</tr>
<tr>
<td>Comp1</td>
</tr>
<tr>
<td>Comp2</td>
</tr>
</tbody>
</table>
### Switch Port Mappings

<table>
<thead>
<tr>
<th>Comp3</th>
</tr>
</thead>
</table>

### Table 21  Port Channel Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Number</th>
<th>Switch</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLTi</td>
<td>peer-link</td>
<td>100</td>
<td>S5048-Top</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S5048-Bottom</td>
</tr>
<tr>
<td>OOB</td>
<td>standard</td>
<td>101</td>
<td>S5048-Top</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S5048-Bottom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S3408-OOB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S5048-Top</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S5048-Bottom</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S5048-Top</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S5048-Bottom</td>
<td></td>
</tr>
</tbody>
</table>

### Table 22  Host Information

<table>
<thead>
<tr>
<th>Host Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Host Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Management VMK0</th>
<th>vMotion VMK1</th>
<th>iDRAC IP</th>
<th>Service Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMK0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMK1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Host Information

<table>
<thead>
<tr>
<th>Mgmt01</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt02</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Compute Host Information

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Management VMK0</th>
<th>vMotion VMK1</th>
<th>iDRAC IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 23 Management Virtual Machines

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP Addresses</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Size (tiny/sm/md/lg/xl)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OMIVV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DD VE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avamar Proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 24 vSphere Cluster Information

<table>
<thead>
<tr>
<th>vSphere Cluster Information</th>
<th>Site A</th>
<th>Management Cluster Name</th>
<th>MgmtPod</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Datacenter Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cluster Hosts</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Virtual Datacenter Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cluster Hosts</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Virtual Datacenter Name**: Site A
- **Management Cluster Name**: MgmtPod
- **Cluster Hosts**: Mgmt01, Mgmt02
- **Virtual Datacenter Name**: Site A
- **Compute Cluster Name**: ComputePod
- **Cluster Hosts**: Comp01, Comp02, Comp03