Abstract
This deployment guide describes the requirements, configuration, and deployment of a converged infrastructure for VMware IaaS with Dell EMC PowerEdge MX servers, PowerMax storage, S-Series switches, and data protection products.

Dell EMC Solutions
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 © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners.

Published in the USA 02/19 Deployment Guide H17534.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
Chapter 1  Introduction 5
Overview .................................................................................................................. 6
Document purpose and scope .............................................................................. 6
Audience .................................................................................................................. 7
We value your feedback ............................................................................................ 7

Chapter 2  Predeployment Requirements 8
Introduction ........................................................................................................... 9
Datacenter requirements ....................................................................................... 9
Site survey information ........................................................................................ 9
Validated components ............................................................................................ 9

Chapter 3  Physical Layout 11
Introduction ........................................................................................................... 12
Rack layout ............................................................................................................ 12
Cabling ................................................................................................................... 13
Hardware installation checklist ........................................................................... 14

Chapter 4  Network Configuration 15
Introduction ........................................................................................................... 16
Configuring Dell EMC Networking S5248F-ON switches .................................. 17
Configuring the Dell EMC Networking S3048-ON switch .................................. 23
Networking configuration checklist ................................................................... 26

Chapter 5  SAN Storage Deployment and Configuration 27
Introduction ........................................................................................................... 28
Deploying PowerMax storage ............................................................................. 28
Deploying Connectrix DS-6500 switches ............................................................. 29
Site survey example: FC port mappings ............................................................... 29
Zoning host servers to storage controllers ......................................................... 30
Adding cluster hosts to the storage array ......................................................... 32
Creating a LUN ..................................................................................................... 33

Chapter 6  Management Cluster Deployment 36
Installing ESXi on the management hosts ......................................................... 37
Configuring the ESXi management network ..................................................... 40
Configuring standard virtual switches ............................................................. 41
Creating a management datastore from the PowerMax LUN ............................. 45
Deploying vCenter Server Appliance................................................................. 46
Adding vCenter Server to Unisphere storage management.......................... 49
Configuring Active Directory authentication (optional)................................. 49
Disabling SSH on ESXi hosts (optional)......................................................... 50
Configuring the management cluster......................................................... 51

**Chapter 7  Compute Cluster Deployment**

Prerequisites................................................................................................. 54
Installing ESXi on the compute hosts ....................................................... 54
Configuring the ESXi management network on the compute cluster ........ 55
Adding ESXi hosts to vCenter ................................................................. 56
Creating and configuring vSphere Distributed Switch ......................... 56
Configuring host networking................................................................. 59
Creating a compute cluster................................................................. 61

**Chapter 8  Management Software and Data Protection Deployment**

Introduction............................................................................................... 63
Deploying OMIVV .................................................................................. 63
Deploying vRealize Automation ........................................................... 73
Deploying vRealize Log Insight ......................................................... 74
Deploying vRealize Operations Manager ....................................... 75
Deploying ESA .................................................................................. 76
Deploying VSI ................................................................................. 77
Deploying IDPA .............................................................................. 79

**Chapter 9  References**

Dell EMC documentation......................................................................... 81
VMware documentation........................................................................ 81

**Appendix A  Site Survey**

Site survey tables ..................................................................................... 83
This chapter presents the following topics:

Overview................................................................................................................ 6
Document purpose and scope ............................................................................ 6
Audience ............................................................................................................... 7
We value your feedback....................................................................................... 7
Overview

Dell EMC Ready Stack is proven, tested, and optimized to help organizations meet long-term datacenter needs for a variety of mixed workloads. Ready Stack provides the simplicity of a complete, yet flexible, validated converged infrastructure (CI) that is based on the following components:

- Dell EMC PowerMax storage
- Dell EMC PowerEdge MX7000 blade enclosure
- Dell EMC S-Series switches
- VMware datacenter virtualization and management product suites
- Dell EMC Integrated Data Protection Appliance (IDPA) DP4400 backup solution

This Dell EMC Ready Stack includes:

- All CI stack components—compute, storage, networking, and data protection—from one trusted vendor
- Design and deployment guidance that incorporates validation, interoperability testing, and best practices
- Design guidance that focuses on scale, flexibility, and high availability
- A reference architecture that incorporates physical topology diagrams and general connectivity guidelines
- Unified management and system monitoring through VMware vCenter
- Infrastructure as a Service (IaaS) integration that support operations, automation, and analysis through VMware vRealize Automation, VMware vRealize Log Insight, and VMware vRealize Operations Manager

Dell EMC has conducted validation testing, including testing of hardware and software stability as well as feature functionality and interoperability. The validation processes were designed to ensure that the Ready Stack provides a stable, highly available platform for your VMware vSphere workloads.

Document purpose and scope

This guide provides basic guidance for deploying Dell EMC Ready Stack for VMware IaaS. Links to detailed product installation guides are referenced as needed and are listed in Chapter 9, References.

This guide provides deployment guidance only. Information about any modifications to the configuration and their potential impact on configuration availability are outside the scope of this document. For detailed information about the Ready Stack architecture, see the Dell EMC Ready Stack: VMware IaaS on PowerEdge MX Servers and PowerMax Storage Design Guide.

The scope of this document does not include information about existing infrastructure components outside of the Dell EMC Ready Stack. Dell EMC assumes no liability for any issues with existing infrastructure that might occur during a deployment. Although
deviations from the described configuration might be made to meet unique requirements, no warranty is implied or given as to the functionality of a Dell EMC Ready Stack that is deployed in a modified configuration.

**Audience**

This guide is for Dell EMC personnel, channel partners, and customers. It provides sample deployment information that Dell EMC Engineering used to test and validate the Ready Stack. Deployment of individual technology components that are mentioned in this guide might require specific training, certification, Partner Competencies, and other prerequisites. Deployment personnel must have the required prerequisites and knowledge of datacenter infrastructure best practices for servers, storage, networking, data protection, power, and cooling. To learn more about product competency training and requirements, contact your Dell EMC Partner, Dell EMC Channel team, or Dell EMC Sales.

**We value your feedback**

Dell EMC and the authors of this document welcome your feedback on the Ready Stack and the Ready Stack documentation. Contact the Dell EMC Solutions team by email or provide your comments by completing our documentation survey.

**Authors:** David Hartman, Karen Johnson
Chapter 2: Predeployment Requirements

This chapter presents the following topics:

- **Introduction** ........................................................................................................... 9
- **Datacenter requirements** ...................................................................................... 9
- **Site survey information** ........................................................................................ 9
- **Validated components** .......................................................................................... 9
Introduction

This deployment guide for Dell EMC Ready Stack makes several assumptions about your existing infrastructure and the services that are available on your network. Before proceeding further, ensure that the predeployment requirements that are described in this chapter are satisfied.

Datacenter requirements

To support the solution, the environment must include:

- An existing Ethernet infrastructure with which to integrate. Dell EMC Networking S5248F 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 that you have all necessary components to facilitate connecting to the existing network prior to beginning deployment.
- Domain Name System (DNS) and Network Time Protocol (NTP) services on the management network. A Dynamic Host Configuration Protocol (DHCP) server is recommended but not required.
- Sufficient power and cooling to support all components. To determine accurate power and cooling needs, see the product documentation.

Site survey information

Appendix A provides site survey tables that you can use to gather the network information that is required to deploy this Ready Stack. We recommend that you collect all the information before you begin the deployment.

Validated components

The following table lists the software and firmware versions that have been validated with this Ready Stack. Use these or later versions for your Ready Stack deployment.

Table 1. Ready Stack validated hardware and software

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Dell EMC PowerEdge R640/R740/740xd</td>
<td>• BIOS 1.6.12 (R-Series)</td>
</tr>
<tr>
<td></td>
<td>PowerEdge MX7000 blade chassis (containing MX740c and MX840c compute sleds)</td>
<td>• BIOS 1.0.2 (MX-Series)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• iDRAC 3.21.26.22</td>
</tr>
<tr>
<td></td>
<td>Mellanox CX4 LX dual-port rNDC (for R Series servers)</td>
<td>• Firmware 14.21.30.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4.16.10.3</td>
</tr>
<tr>
<td></td>
<td>QLogic 2692 dual-port Fibre Channel HBA</td>
<td>Firmware 14.07.05, qlnativefc 2.1.81.0-1</td>
</tr>
<tr>
<td>Layer</td>
<td>Device</td>
<td>Version</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Dell EMC PERC H730p</td>
<td>• Driver 6.604.06.00, A05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firmware 25.5.5.0005</td>
</tr>
<tr>
<td></td>
<td>Dell EMC BOSS controller card+ with 2 x M.2 sticks 120 GB (RAID 1), LP</td>
<td>• Driver 1.2.0.1048</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firmware 2.5.13.3011</td>
</tr>
<tr>
<td>Network</td>
<td>Dell EMC Networking S3048</td>
<td>OS 10.4.2.0</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Networking S5248F</td>
<td>OS 10.4.2.0</td>
</tr>
<tr>
<td>Storage</td>
<td>Dell EMC PowerMax 2000/8000</td>
<td>• PowerMax OS 5978</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unisphere 9.0</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Connectrix DS-6500 Fabric OS</td>
<td>8.2.0a</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 (VSI)</td>
<td>7.4</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Storage Analytics (ESA)</td>
<td>4.6</td>
</tr>
<tr>
<td></td>
<td>Dell EMC OpenManage Integration for VMware vCenter (OMIVV)</td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC IDPA DP4400</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>VMware vRealize Automation</td>
<td>7.5</td>
</tr>
<tr>
<td></td>
<td>VMware vRealize Log Insight</td>
<td>4.7</td>
</tr>
<tr>
<td></td>
<td>VMware vRealize Operations Manager</td>
<td>7.0</td>
</tr>
</tbody>
</table>
This chapter presents the following topics:

**Introduction** ................................................................. 12

**Rack layout** ................................................................. 12

**Cabling** ................................................................. 13

**Hardware installation checklist** ......................................... 14
Chapter 3: Physical Layout

Introduction

This chapter describes the physical layout of the Ready Stack components when they are installed in a single rack, including cabling for power and network connectivity. For information about rack installation of individual components, see the product documentation on Dell EMC Online Support.

Rack layout

The physical rack layout of Ready Stack is flexible and depends on many datacenter elements such as power, thermals, and weight restrictions. The PowerEdge MX7000 blade chassis with MX740c and MX840c compute sleds requires 7U of rack space. PowerEdge rack servers require either 1U or 2U of rack space, depending on the model, and the compute server quantity can change depending on customer needs.

PowerMax storage can require fewer or additional disk enclosures, depending on the storage capacity and SSD type. Additional items such as IDPA can also be included within the same rack, space permitting. Ready Stacks are currently sized in Enterprise Small, Medium, and Large configurations. The following figure is an example of the Enterprise Large configuration.

Figure 1. Ready Stack components in Enterprise Large configuration—front rack view
Cabling

The following figure shows the required cabling for the Ready Stack components.

100 GbE requires QSFP28 cables, and 25 GbE requires SFP28 cables. We recommend using Dell EMC Networking passive copper direct attach cables, which are available in various lengths to meet your rack layout requirements. Dell EMC Networking active optical cables are also available for longer distances and dense rack configurations.

Connectrix DS-6500 switches are prepopulated with the required Fibre Channel optics. PowerMax storage and PowerEdge servers require additional 16 GB small form-factor pluggable (SFP) Fibre Channel adapters. Dell EMC Multimode LC/LC fiber optic cables are required between the PowerEdge server and PowerMax storage array and the Connectrix Fibre Channel switches. Cat 5e or Cat 6 Ethernet cabling is required for Dell EMC iDRAC, Connectrix, and PowerMax management. For small configurations, it is possible to connect 1 GbE devices to top-of-rack (ToR) switches by using a 1000Base-T SFP transceiver, which can eliminate the need for the Dell S3048-ON switch in some cases.
**Hardware installation checklist**

Before proceeding with the deployment tasks, ensure that:

- Hardware components (switches, storage, and servers) have been installed into racks.
- Network connections from switches to servers have been made, as shown in Figure 2.
- Power has been connected to each component.
This chapter presents the following topics:

- **Introduction**................................................................. 16
- **Configuring Dell EMC Networking S5248F-ON switches**........ 17
- **Configuring the Dell EMC Networking S3048-ON switch** .......... 23
- **Networking configuration checklist**...................................... 26
Chapter 4: Network Configuration

Introduction

This chapter describes how to configure the Ready Stack for Networking S3048-ON out-of-band (OOB) management and S5248F-ON ToR switches. These procedures are provided as an example of a working configuration. Ensure that you review the procedures with your site networking team before performing them.

Networking site survey information

This survey is intended as an example only. Appendix A provides the full site survey. Complete the form before starting the deployment.

The following tables present an example of a networking site survey topology. Confirm all the information, especially Spanning Tree Protocol (STP) information, with the personnel who are responsible for the network configuration in your environment.

Table 2. Switch hostnames example

<table>
<thead>
<tr>
<th>Switch</th>
<th>Hostname</th>
<th>VLT backup address</th>
<th>VLT ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3048-ON</td>
<td>SWOOB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5248F-Top</td>
<td>SW1</td>
<td>192.168.1.253/24</td>
<td>Ethernet 1/1/53-1/1/54</td>
</tr>
<tr>
<td>S5248F-Bottom</td>
<td>SW2</td>
<td>192.168.1.252/24</td>
<td>Ethernet 1/1/53-1/1/54</td>
</tr>
</tbody>
</table>

Table 3. VLAN information example

<table>
<thead>
<tr>
<th>Network type</th>
<th>VLAN ID</th>
<th>S5248F-Top IP CIDR</th>
<th>S5248F-Bottom IP CIDR</th>
<th>VRRP IP address</th>
<th>VRRP group</th>
<th>S3048-ON IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOB</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>VM migration</td>
<td>120</td>
<td>172.90.120.252/24</td>
<td>172.90.120.253/24</td>
<td>172.90.120.254</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Customer network services example

<table>
<thead>
<tr>
<th>Service</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>172.90.100.250</td>
</tr>
</tbody>
</table>

Table 5. Switch port mapping example

<table>
<thead>
<tr>
<th>Component</th>
<th>S5248F-Top</th>
<th>S5248F-Bottom</th>
<th>S3048-ON</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>Ethernet 1/1/1</td>
<td>Ethernet 1/1/1</td>
<td>Ethernet 1/1/1</td>
</tr>
<tr>
<td>Mgmt2</td>
<td>Ethernet 1/2/1</td>
<td>Ethernet 1/2/1</td>
<td>Ethernet 1/2/1</td>
</tr>
<tr>
<td>Comp1</td>
<td>Ethernet 1/3/1</td>
<td>Ethernet 1/3/1</td>
<td>Ethernet 1/3/1</td>
</tr>
<tr>
<td>Comp2</td>
<td>Ethernet 1/4/1</td>
<td>Ethernet 1/4/1</td>
<td>Ethernet 1/4/1</td>
</tr>
<tr>
<td>Comp3</td>
<td>Ethernet 1/5/1</td>
<td>Ethernet 1/5/1</td>
<td>Ethernet 1/5/1</td>
</tr>
</tbody>
</table>
You need a laptop with a serial connection and terminal emulation software such as PuTTY.

This section uses certain typographical conventions to designate commands and screen output. Command syntax is identified by Courier font. Information that is specific to your environment or site survey is placed inside <> symbols and in italics. For example:

- **Deployment guide command reference**: OS10(config)# hostname <hostname>
- **On the top S5248F-ON switch**, enter: OS10(config)# hostname SW1
- **On the bottom S5248F-ON switch**, enter: OS10(config)# hostname SW2

When an input command is different between the top and bottom switch but the information is not part of the site survey, an indentation identifies the different commands. Use the command with the preceding hostname for the switch you are configuring. For example:

```
SW1(config)# spanning-tree mode rstp #Command entered on both switches
  
SW1(config)# spanning-tree rstp priority 4096 #Command for Top S5248F-ON

SW2(config)# spanning-tree rstp priority 8192 #Command for Bottom S5248F-ON
```

Screen output is presented in **bold type**. Optional commands are shown in *italicized bold type*.

### Configuring Dell EMC Networking S5248F-ON switches

This section describes a minimal configuration for your Dell EMC Networking S5248F-ON switches to support the Ready Stack. Additional configuration might 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 S5248F-ON switch, see [Support for Dell Networking S5248F-ON](https://www.dell.com/support) on Dell EMC Online Support.

**Configure the S5248F-ON switches**

Configure the S5248F-ON switches:

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.

   The following figure shows the console and management ports. The console port is located on the upper right of the switch when you are looking at the back portion near the fans and power supplies.
Chapter 4: Network Configuration

Figure 3. Serial port

2. Using terminal emulation software, configure the COM port:
   - 115200 baud rate
   - No parity/no flow control
   - 8 data bits/1 stop bit

3. When the connection is successful, enter configuration mode by running the following command:
   `OS10# configure terminal`

4. Configure the hostname and time zone and set a username and password for EXEC mode by running the following commands:
   `OS10(config)# hostname <hostname>`
   `SW1(config)# username <username> password <password> role sysadmin`
   `SW1(config)# clock timezone <timezone, for example, CST -6 0>`

5. Configure routing to your default gateway, and save the configuration by running the following commands:
   `SW1(config)# ip route 0.0.0.0/0 <core network gateway>`
   `SW1(config)# do write memory`

Configure the management interface

The VLTi heartbeat uses the management interface on the back of the Dell EMC Networking S5248F-ON switch, which is connected with a Cat 5e Ethernet network cable from the top S5248F-ON switch to the bottom S5248F-ON switch. To configure the management interface, enter global configuration mode on the switch and follow these steps:

1. Configure the management port by running the following commands:
   `SW1(config)# interface mgmt 1/1`
   `SW1(conf-if-ma-1/1/1)# no ip address dhcp`
2. **Enable STP by running the following commands.**

   **Caution:** Ensure that the personnel responsible for network management in your environment have reviewed the configuration for STP because incorrect settings may cause network issues. The values provided here are examples only.

   ```
   SW1(config)# spanning-tree mode rstp
   SW1(config)# spanning-tree rstp priority 16384
   SW2(config)# spanning-tree rstp priority 32768
   ```

---

**Configure the VLANs**

This section describes how to configure the VLANs on the S5248F-ON switch. The examples show how 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 if you do not want VLAN traffic routed by the S5248F-ON switches, skip the commands in **bold italics**.

Follow these steps:

1. **Configure the OOB VLAN:**

   ```
   SW1(config)# interface vlan 100
   SW1(conf-if-vl-100)# description "out-of-band VLAN"
   SW1(conf-if-vl-100)# ip address 172.90.100.252/24
   SW1(conf-if-vl-100)# mtu 9216
   SW1(conf-if-vl-100)# vrrp-group 1
   SW1(conf-if-vlan100-vrid-1)# virtual-address 172.90.100.254
   SW1(conf-if-vlan100-vrid-1)# exit
   SW1(conf-if-vl-100)# no shutdown
   SW1(conf-if-vl-100)# exit
   SW1(config)# do write
   ```

2. **Configure the management VLAN:**

   ```
   SW1(config)# interface vlan 110
   SW1(conf-if-vl-110)# description "Management VLAN"
   SW1(conf-if-vl-110)# ip address 172.90.110.252/24
   ```
SW1(conf-if-vl-110)# mtu 9216

SW1(conf-if-vl-110)# vrrp-group 2

SW1(conf-if-vlan110-vrid-2)# virtual-address 172.90.110.254

SW1(conf-if-vlan110-vrid-2)# exit

SW1(conf-if-vl-110)# no shutdown

SW1(conf-if-vl-110)# exit

SW1(config)# do write

3. Configure the VM migration VLAN:

SW1(config)# interface vlan 120

SW1(conf-if-vl-120)# description “VM migration VLAN”

SW1(conf-if-vl-120)# ip address 172.90.120.252/24

SW1(conf-if-vl-120)# mtu 9216

SW1(conf-if-vl-120)# vrrp-group 3

SW1(conf-if-vlan120-vrid-3)# virtual-address 172.90.120.254

SW1(conf-if-vlan120-vrid-3)# exit

SW1(conf-if-vl-120)# no shutdown

SW1(conf-if-vl-120)# exit

SW1(config)# do write

4. Configure the Compute VM VLAN:

SW1(config)# interface vlan 210

SW1(conf-if-vl-210)# description “Compute VM VLAN”

SW1(conf-if-vl-210)# ip address 172.90.210.252/24

SW1(conf-if-vl-210)# mtu 9216

SW1(conf-if-vl-210)# vrrp-group 4

SW1(conf-if-vlan210-vrid-3)# virtual-address 172.90.210.254

SW1(conf-if-vlan210-vrid-3)# exit

SW1(conf-if-vl-210)# no shutdown

SW1(conf-if-vl-210)# exit

SW1(config)# do write
5. To verify that all the settings have been properly recorded, review the configuration from enable mode by running the following command:

   SW1# show running-config

6. Repeat the preceding steps to configure the bottom Dell EMC Networking S5248F-ON switch in the configuration.

Configure the ports to be used for VLTi traffic:

1. Run the following commands:

   SW1(config)# interface range ethernet 1/1/53-1/1/54
   SW1(conf-range-eth1/1/53-1/1/54)# description VLTi
   SW1(conf-range-eth1/1/53-1/1/54)# no switchport
   SW1(conf-range-eth1/1/53-1/1/54)# exit

2. Create the VLT domain and add the discovery interfaces:

   SW1(config)# vlt-domain 1
   SW1(conf-vlt-1)# backup destination 192.168.1.253
   SW2(conf-vlt-1)# backup destination 192.168.1.252
   SW1(conf-vlt-1)# discovery-interface ethernet 1/1/53-1/1/54
   SW1(conf-vlt-1)# do write memory

3. Ensure that the VLT domain is properly configured by running the following command in enable mode:

   SW1# show vlt 1 | find Status

   The following output appears:

   VLTi Link Status
   port-channel1000       : up

   VLT Peer
   Unit ID  System MAC Address  Status  IP Address    Version
   ----------------------  -------  ------  ------------  -------
   1        54:bf:64:be:f7:40   up      192.168.1.253  2.0

4. Run the following commands to configure the ports that the servers are connected to on the switch.

   Based on the site survey example, ports Ethernet 1/1/1 through Ethernet 1/1/16 are in use on each switch.

   SW1(config)# interface range ethernet 1/1/1-1/1/16
   SW1(conf-range-eth1/1/1-1/1/16)# no ip address
SW1(conf-range-eth1/1-1/1-1/16)# mtu 9216
SW1(conf-range-eth1/1-1/1-1/16)# switchport mode trunk
SW1(conf-range-eth1/1-1/1-1/16)# switchport access vlan 100
SW1(conf-range-eth1/1-1/1-1/16)# switchport trunk allowed vlan 110,120,210
SW1(conf-range-eth1/1-1/1-1/16)# spanning-tree port type edge
SW1(conf-range-eth1/1-1/1-1/16)# spanning-tree guard root
SW1(conf-range-eth1/1-1/1-1/16)# no shutdown

5. Verify that the ports are configured correctly by running the following command:

SW1(conf-range-eth1/1-1/1-1/16)# show config

The output for each port appears as follows:

interface ethernet1/1/1
  no shutdown
  switchport mode trunk
  switchport access vlan 100
  switchport trunk allowed vlan 110,120,210
  mtu 9216
  flowcontrol receive off
  spanning-tree guard root
  spanning-tree port type edge
  
...
Chapter 4: Network Configuration

2. Configure the port that will be used for the port channel by running the following commands:

```bash
SW1(config)# port-group 1/1/12
SW1(conf-pg-1/1/12)# mode Eth 10g-4x
SW1(conf-pg-1/1/12)# exit

SW1(config)# interface ethernet 1/1/48:1
SW1(conf-if-eth1/1/48:1)# no shutdown
SW1(conf-if-eth1/1/48:1)# shutdown
SW1(conf-if-eth1/1/48:1)# description “OOB uplink”
SW1(conf-if-eth1/1/48:1)# channel-group 101 mode active
SW1(conf-if-eth1/1/48:1)# mtu 9216
SW1(conf-if-eth1/1/48:1)# exit
```

3. Repeat the preceding steps to configure the bottom Dell EMC Networking S5248F-ON switch in the configuration.

**Configuring the Dell EMC Networking S3048-ON switch**

The Dell EMC Networking S3048-ON switch serves as the OOB management switch for the Ready Stack. A single switch is used because this connectivity is not considered critical for workload operations.

**Configure the S3048-ON switch**

Configure the Dell EMC Networking S3048-ON switch:

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, as shown in the following figure.
2. Using terminal emulation software, configure the COM port:
   - 115200 baud rate
   - No parity/no flow control
   - 8 data bits/1 stop bit

3. When the connection is successful, enter configuration mode by running the following commands:
   
   OS10# configure terminal

4. Configure the hostname and time zone, and set a username and password for EXEC mode by running the following commands:
   
   OS10(config)# hostname SWOOB
   
   SWOOB(config)# username <username> password <password> role sysadmin
   
   SWOOB(config)# clock timezone <timezone, example CST -6 0>

5. Configure routing to your default gateway, and save the configuration by running the following commands:
   
   SWOOB(config)# ip route 0.0.0.0/0 <core network gateway>
   
   SWOOB(config)# do write

Configure the VLANs

This section describes how to configure the VLANs on the S3048-ON switch. The examples show how to configure each VLAN in the site survey.

Follow these steps:

1. Configure the OOB VLAN:
   
   SWOOB(config)# interface vlan 100
   
   SWOOB(conf-if-vl-100)# description “out-of-band VLAN”
   
   SWOOB(conf-if-vl-100)# mtu 9216
   
   SWOOB(conf-if-vl-100)# no shutdown
   
   SWOOB(conf-if-vl-100)# exit
   
   SWOOB(config)# do write

2. To verify that all the settings have been properly recorded, from enable mode, review the configuration by running the following command:
   
   SWOOB# show running-config
Configure the management interface

Configure the ports that the management servers’ iDRAC cards are connected to on the switch. In this example, ports 1/1 to 1/3 are used for the management server’s iDRAC.

1. Run the following commands:

   SWOOB(config)# interface range ethernet 1/1/1-1/1/3
   SWOOB(conf-range-eth1/1/1-1/1/3)# no shutdown
   SWOOB(conf-range-eth1/1/1-1/1/3)# no ip address
   SWOOB(conf-range-eth1/1/1-1/1/3)# switchport access vlan 100
   SWOOB(conf-range-eth1/1/1-1/1/3)# spanning-tree port type edge
   SWOOB(conf-range-eth1/1/1-1/1/3)# mtu 9216

2. Verify that the ports are properly configured by running the following command:

   SWOOB(conf-range-eth1/1/1-1/1/3)# show configuration

   The following output is displayed for each port:

   interface ethernet1/1/1
      no shutdown
      switchport access vlan 100
      mtu 9216
      flowcontrol receive on
      spanning-tree port type edge
      
      ...

Configure the port channel

The Dell EMC Networking S3048-ON switch connects to the network through the Dell EMC Networking S5248F-ON VLT domain using a port channel consisting of two 10 GbE ports on the Networking S3048-ON switch. Follow these steps to configure the port channel and then configure the ports for the port channel:

1. Configure the OOB VLAN on the switch by running the following commands:

   SWOOB(config)# interface vlan 100
   SWOOB(conf-if-vl-100)# description “out-of-band VLAN”
   SWOOB(conf-if-vl-100)# no shutdown
   SWOOB(conf-if-vl-100)# ip address 172.90.100.25/24
   SWOOB(conf-if-vl-100)# mtu 9216


2. Create the port channel by running the following commands:

   SWOOB(config)# interface port-channel 101
   SWOOB(conf-if-po-101)# description “OOB uplink”
   SWOOB(conf-if-po-101)# no shutdown
   SWOOB(conf-if-po-101)# switchport mode trunk
   SWOOB(conf-if-po-101)# switchport trunk allowed vlan 100
   SWOOB(conf-if-po-101)# mtu 9216
   SWOOB(conf-if-po-101)# exit

3. Configure the ports that will be used for the port channel by running the following commands:

   SWOOB(config)# interface range ethernet 1/1/49-1/1/50
   SWOOB(conf-range-eth1/1/49-1/1/50)# description “OOB uplink”
   SWOOB(conf-range-eth1/1/49-1/1/50)# no shutdown
   SWOOB(conf-range-eth1/1/49-1/1/50)# channel-group 101 mode active
   SWOOB(conf-range-eth1/1/49-1/1/50)# mtu 9216
   SWOOB(conf-range-eth1/1/49-1/1/50)# exit

4. Verify that the port channel to the S5248F-ON switch is up by running the following command:

   SWOOB# show interface port-channel summary

<table>
<thead>
<tr>
<th>LAG</th>
<th>Mode</th>
<th>Status</th>
<th>Uptime</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>L2-HYBRID</td>
<td>up</td>
<td>2 days</td>
<td>Eth 1/1/49 (Up)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Eth 1/1/50 (Up)</td>
</tr>
</tbody>
</table>

**Networking configuration checklist**

Ensure that the following network configurations are complete:

- S5248F-ON switches are configured.
- S5248F-ON switches are connected to the corporate network.
- S3048-ON switch is configured.
- S3048-ON switch is connected to the S5248F-ON switches.
This chapter presents the following topics:

Introduction ........................................................................................................... 28
Deploying PowerMax storage ........................................................................... 28
Deploying Connectrix DS-6500 switches ....................................................... 29
Site survey example: FC port mappings ....................................................... 29
Zoning host servers to storage controllers ............................................... 30
Adding cluster hosts to the storage array .................................................. 32
Creating a LUN ................................................................................................. 33
Chapter 5: SAN Storage Deployment and Configuration

Introduction

This chapter describes the procedures that you must perform to deploy and configure the PowerMax storage array. It assumes that all storage equipment has been powered and connected to the appropriate networks. For enclosure cabling guidelines, see the Dell EMC PowerMax Family Site Planning Guide or consult your Dell EMC Sales representative.

Note: PowerMax hardware cannot be installed by customers or Service Partners. Dell EMC Services must perform the initial installation.

Deploying PowerMax storage

Before proceeding, connect all power cords and management cables. Connect any additional drive array enclosures as well.

Deploy the PowerMax storage:

1. Connect the PowerMax system to the network.
   
   The management IP address for the PowerMax system can be assigned dynamically or statically:
   
   - **Dynamic**—If DHCP is supported on your network, the PowerMax system automatically obtains a network address when you power on the system.
   
   - **Static**—On a computer with access to the subnet where you installed the PowerMax system, download, install, and run the Dell EMC Unisphere for PowerMax software. You need the serial number of the PowerMax system and the IP address, subnet mask, and default gateway that you want to use.

2. Connect to Unisphere storage management:
   
   a. Launch your preferred browser.
   
   b. Enter the management IP address as the destination.
   
   c. Enter the following default credentials:
      
      - **User**—admin
      - **Password**—Password123#

   An initial configuration wizard steps through basic settings such as licensing, storage pool creation, alerts, support, and networking. You can configure the Unisphere settings at any time, even after completing the initial wizard. To open the Settings page, click the gear icon in the upper left.

3. Establish a network connection to the Dell EMC Secure Remote Services gateway.

   PowerMax Management Module Control Station (MMCS) modules can communicate with the Customer Support Center through a network connection to the Secure Remote Services gateway. For setup procedures, see the PowerMax Technical Documentation.
Deploying Connectrix DS-6500 switches

Before deploying the FC switches, connect all power cords and management cables. For cabling guidelines for the storage array and hosts, see Dell EMC Online Support.

Deploy the Connectrix DS-6500 switches:

1. Using the serial cable that shipped with the switch, connect the COM port on your setup computer to the serial port on the switch.

   The serial connection settings are:
   - 9600 bits per second
   - No parity/no flow control
   - 8 data bits/1 stop bit

2. Open a terminal emulator program, such as PuTTY, and log in to the switch console using the following default credentials:
   - User—admin
   - Password—password

3. When prompted, change the password.

4. Type `ipAddrSet` and press Enter to open the IP configuration dialog box, and then configure the following settings:
   - DHCP—Select On or Off (default setting is Off).
   - Ethernet IP Address—Set an IP address for the switch.
   - Ethernet Subnetmask—Set a subnetmask for the switch.
   - Gateway IP Address—Set a default gateway for the switch.

5. 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.

Site survey example: FC port mappings

The following table provides an example of the FC port information that is gathered during a site survey.

<table>
<thead>
<tr>
<th>FC port</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>
</tbody>
</table>
### Zoning host servers to storage controllers

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 Java issues prevent you from accessing Web Tools from the browser, invoke the utility by running the following command:

   `javaws "http://<switch_ip_address>/switchExplorer_installed.html"`

2. Create a zone configuration:
   
   a. Log in to Web Tools with administrator credentials.

   b. Select **Configure > Zone Admin**.

   c. In the **Zone Administration** window, click the **Zone Config** tab, and then click **New Zone Config**.

   d. In the **Create New Config** dialog box, enter a name for the configuration and click **OK**.

3. Create aliases for the front-end FC ports of the storage controller:
   
   a. In the **Zone Administration** window, click the **Alias** tab, and then click **New Alias**.

---

<table>
<thead>
<tr>
<th>FC port</th>
<th>WWN</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Comp2 P2</td>
<td>21:00:00:24:ff:7f:08:f8</td>
<td>comp2_p2</td>
</tr>
<tr>
<td>Comp3 P1</td>
<td>21:00:00:24:ff:7f:08:cf</td>
<td>comp3_p1</td>
</tr>
<tr>
<td>Comp3 P2</td>
<td>21:00:00:24:ff:7f:08:ce</td>
<td>comp3_p2</td>
</tr>
</tbody>
</table>
b. In the **Create New Alias** dialog box, enter a name for the new alias—PowerMax_SPA_P0, for example—and click **OK**.

c. Under **Member Selection List**, expand **Ports & Attached Devices** to view the nested elements.

d. Expand the port that contains the WWN for the alias being created, as shown in the following figure.

Note: You can find WWNs for the front-end ports of the PowerMax system in Unisphere storage management.

![PowerMax ports with WWNs](image)

Figure 5. PowerMax ports with WWNs

e. Click the port WWN, and then click the right arrow to add the WWN to **Alias Members**.

f. Repeat the preceding steps to create aliases for all front-end ports of the storage controller.

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

4. Create aliases for the WWNs of the management and compute servers:

   a. In the **Zone Administration** window, click the **Alias** tab, and then click **New Alias**.

   b. In the **Create New Alias** dialog box, enter a name for the new alias—MGMT_SVR_P1, for example—and click **OK**.

   c. Under **Member Selection List**, expand **Ports & Attached Devices** to view the nested elements.

   d. Expand the port that contains the WWN for the alias being created.

   e. Click the port WWN, and then click the right arrow to add the WWN to **Alias Members**.

Note: You can find server host bus adapter (HBA) WWNs in the hardware inventory of the iDRAC console.

f. Repeat the preceding steps to create aliases for all management and compute server HBAs.

g. 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, click the **Zone** tab, and then click **New Zone**.
Chapter 5: SAN Storage Deployment and Configuration

In the **Create New Zone** dialog box, enter a name for the new zone, and click **OK**.

Under **Member Selection List**, expand **Aliases** to view the nested elements.

Select all aliases of the PowerMax storage ports and the alias of the server WWN to be included in the zone.

Click the right arrow to add the aliases to **Zone Members**.

Repeat steps b through f to create zones for all management and compute servers.

Select **Zoning Actions > Save Config** to save the configuration changes.

6. Enable configuration:

   - Select the **Zone Config** tab.
   - Under **Member Selection List**, expand **Zones** to view the nested elements.
   - Select all the zones that you created for the management and compute hosts.
   - Click the right arrow to move the selected zones in **Member Selection List** to **Zone Config Members**.
   - Click **Save Config** to save the configuration.
     This process takes a few seconds.
   - Click **Enable Config** and select the name of the zone config.
   - Click **OK** to enable the zone configuration.

**Adding cluster hosts to the storage array**

Add cluster hosts to the storage array:

1. For each server to be added to the storage array, obtain the HBA’s WWNs.

   You can view the HBA WWNs from the server’s iDRAC or ESXi shell:

   - To view the WWNs from the iDRAC, log in to the iDRAC, expand **Hardware**, and then click **Fibre Channel devices**. Expand a device under **Fibre Channel Ports** to view the port’s WWN.
   - To view the WWN from the ESXi shell, run the following command:

     ```
     esxcli storage core adapter list
     ```

     The port WWNs are displayed, as shown in the following figure.
2. Log in to Unisphere storage management.
3. Under **Access**, click **Hosts**.
4. Click the plus sign (+) in the upper left of the **Hosts** pane.
5. In the **Name** field, name the server, and then click **Next**.
   The **Automatically Discovered Initiators** section of the window shows all discovered initiators.
6. Select the WWN of the server that is being added to the storage array, and then click **Next**.
7. Review the selections and click **Finish**.
8. Repeat the preceding steps for all management and compute servers to be added to the storage array.

### Creating a LUN

This procedure describes how to create LUNs and present them to the management cluster. The LUNs are used as datastores for VMware vCenter Server Appliance deployment as well as other management VMs. You can also use this procedure to create additional LUNs for management and compute clusters.

To create a LUN:
1. Log in to Unisphere storage management.
2. Create storage pools as needed.
   The number and size of the pools depend on the requirements of each environment and the number of available drive types in the storage array.
3. In the left pane, click **Block**.
4. Click the plus sign (+) in the upper left of the LUNs pane.
   The **Create LUNs** wizard opens.
5. On the **Configure LUN(s)** page:
   a. In the **Number of LUNs** field, select 1.
   b. In the **Name** field, enter the name for the LUN.
   c. In the **Pool** field, select the pool from which the LUN is being created.
   d. In the **Size** field, enter the size of the LUN.
   The following table provides vCenter Server Appliance space requirements.
### Table 7. vCenter Server Appliance requirements: Disk storage on the host machine

<table>
<thead>
<tr>
<th>Storage size</th>
<th>Deployment size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tiny (GB)</td>
</tr>
<tr>
<td>Default</td>
<td>250</td>
</tr>
<tr>
<td>Large</td>
<td>775</td>
</tr>
<tr>
<td>X-Large</td>
<td>1,650</td>
</tr>
</tbody>
</table>

To create a thin LUN, select **Thin**.

If **Thin** is not selected, a thick LUN will be created.

Click **Next**.

6. On the **Configure Access** page, click the plus sign (+) in the upper-left corner.

7. In the **Select Host Access** window, select the management hosts that require access to the LUN, as shown in the following figure, and then click **OK**.

![Select Host Access window](image)

8. On the **Access** page, review the host selection and click **Next**.

9. On the **Snapshot** page, select **Enable Automatic Snapshot Creation** if you want snapshots created automatically, and then click **Obtain the HBA’s WWNs**.

10. On the **Replication** page, if replication is being configured for the LUN, select **Enable Replication** and select replication settings.

11. On the **Summary** page, review the selections and click **Finish**.

12. On the **Results** page, click **Close**.
13. If another datastore is required for additional management VMs, repeat steps 4 through 12 to create a datastore that can accommodate all of the management VMs.

The following table provides an example of sizing for additional management VMs. For this example, a 1 TB LUN is 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>Operating system (GB)</th>
<th>NICs</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>
</tbody>
</table>

14. Repeat steps 4 through 12 to create additional LUNs as needed and assign them to appropriate hosts.
Chapter 6 Management Cluster Deployment

This chapter presents the following topics:

- Installing ESXi on the management hosts ............................................................ 37
- Configuring the ESXi management network ....................................................... 40
- Configuring standard virtual switches ............................................................... 41
- Creating a management datastore from the PowerMax LUN .......................... 45
- Deploying vCenter Server Appliance ............................................................... 46
- Adding vCenter Server to Unisphere storage management ........................... 49
- Configuring Active Directory authentication (optional) .................................. 49
- Disabling SSH on ESXi hosts (optional) ......................................................... 50
- Configuring the management cluster ............................................................... 51
Installing ESXi on the management hosts

Install VMware ESXi on each of the PowerEdge management hosts that will be part of the management cluster. For convenience, you can order PowerEdge servers with VMware ESXi 6.5 preinstalled; otherwise, you can install ESXi remotely through the iDRAC web interface or locally. This section describes how to perform the installation remotely. In our example, we assign static IP addresses to the management interfaces of the ESXi hosts. Using DHCP is not recommended for IP allocation of management hosts.

Prerequisites

To complete the procedures in this section, you need:
- iDRAC IP addresses or fully qualified domain names (FQDNs)
- iDRAC credentials
- iDRAC Enterprise license applied on all nodes
- Dell EMC-customized ESXi 6.5 image
  
  For download instructions, see VMware vSphere ESXi 6.5.x on Dell EMC PowerEdge Systems Image Customization Information on Dell EMC Online Support. Make a note of the image location on your system because you will need it when mounting virtual media.

- Host names, Management VLAN ID, IP address information
- vSphere credentials
- Static IP addresses for each of the management servers
- DNS server records for hostnames (optional)

Note: The iDRAC User Guide provides instructions for setting up the iDRAC, including configuring the IP address. For a link to the guide, see the iDRAC page on Dell EMC Online Support.

Configure the BIOS settings and connect to the iDRAC:

1. Apply the BIOS settings profile that provides maximum virtualization performance:
   a. Connect to the iDRAC IP address of one of the management hosts by using an SSH client such as PuTTY.
   b. Log in with the following default credentials:
      - User—root
      - Password—calvin
   c. At the /admin1-> prompt, run the following command:
      racadm set bios.sysprofilesettings.WorkloadProfile VtOptimizedProfile
   d. Run the following command to process the change:
      racadm jobqueue create BIOS.Setup.1-1
   e. Restart the management host.
f. Repeat the preceding steps for each remaining management host.

2. Using a web browser, go to the iDRAC web interface at https://<iDRAC Address>.

3. Log in with the following default credentials:
   - User: root
   - Password: calvin

4. Click the Virtual Console preview, as shown in the following figure, to open the Virtual Console.

   For each iDRAC, ensure that pop-up support is enabled in your browser.

![Virtual Console preview](image)

5. While connected to the Virtual Console, attach the virtual media by selecting Virtual Media > Connect Virtual Media.

6. Select Virtual Media > Map CD/DVD.

7. Click Browse to go to the location of the Dell EMC ISO file for VMware ESXi 6.5, select the file, and then click Open.

   This location must be available throughout the installation of ESXi on all servers.

The Virtual Media – Map CD/DVD page appears.

**Boot to the installation media**

On the Virtual Media – Map CD/DVD page, boot to the installation media:

1. Click Map Device.

2. From the Virtual Console menu bar, select Next Boot.

3. From the Next Boot list, select Virtual CD/DVD/ISO.
4. Click OK to continue.

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 Power list, select Power On System, or, if the system is already on, select Power Cycle System (cold boot).

After the server restarts, the ESXi installer begins to load.

Install VMware ESXi on the management cluster:

1. In the iDRAC Virtual Console, at the Welcome to the VMware ESXi 6.5.0 Installation page, press Enter.

2. Review the terms of the license agreement and, to accept the terms and continue, press F11.

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

If the disk has previously been used to install ESXi, the following message appears.

![ESXi Found message](image)

4. If the ESXi Found message appears:
   a. Use the cursor keys to go to Install.
   b. Press the space bar to perform a fresh installation.
   c. Press Enter.

5. Select the keyboard layout for your environment and press Enter to continue.

6. Enter the password that you want to use for the root account, reenter the password to validate it, and press Enter.

7. On the confirmation page, press F11 to install VMware ESXi 6.5.

8. When the installation is complete, from the Virtual Console menu bar, select Virtual Media > Disconnect Virtual Media.

9. When prompted, click Yes to confirm that you want to close the Virtual Media session.

10. On the Installation Complete page, press Enter to restart the server.
Configuring the ESXi management network

After you install ESXi and restart the server, configure and test the ESXi management network.

Configure the management network:

1. Open the iDRAC Virtual Console, and press F2 to log in to the Direct Console User Interface.
2. Enter the credentials that you created during the ESXi setup, and then press Enter.
3. From the System Customization menu, select Configure Management Network.
4. On the Configure Management Network page, select Network Adapters to ensure that the NIC is registered as connected.
5. On the Network Adapters page, ensure that the Status column displays Connected for vmnic0 and any other NIC ports that are already connected. If the NIC is not connected, check the cabling and status of the switch port and correct any issues. Then, press Esc to return to the previous page.
6. Press Esc to exit the Network Adapters menu.
7. Select VLAN (optional) and press Enter.
8. Enter the VLAN ID for the management network (110 in Table 3, VLAN information example), and then press Enter.
10. Using the cursor keys, select Set static IPv4 address, and then press the space bar.
11. On the IPv4 Configuration page, enter the IPv4 address, subnet mask, and default gateway for the management host.
   See Table 17 of the site survey.
12. Press Enter.
13. Select DNS Configuration and press Enter.
14. Type the IP address of the DNS servers and the FQDN of the host.
   See Table 13 of the site survey.
15. If the environment has multiple domains, or if subdomains and short names are used, select Custom DNS Suffixes and add the suffixes.
16. Press Esc to return to the main menu.
17. Press Y to confirm the changes and restart the management network.
Test the management network setup:

1. Under **System Customization**, select **Test Management Network**.
   **Test Management Network** shows a summary of what will be tested. The following figure is from a test deployment.

   ![Figure 10. Test Management Network](image)

   By default, this test will attempt to ping your default gateway and DNS servers, and resolve your hostname.

   ![Ping Address #0:](image)

   ![Ping Address #1:](image)

   ![Ping Address #2:](image)

   ![Resolve Hostname](image)

   <Up/Down> Select <Enter> OK <Esc> Cancel

2. Press Enter to continue.

   When the test has completed, results that are similar to those in the following figure are displayed.

   ![Figure 11. Test network results](image)

   **Testing Management Network**

   You may interrupt the test at any time.

   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.

   <Enter> OK

### Configuring standard virtual switches

This section describes the procedures that are necessary to configure your virtual switches for the Ready Stack.

### Prerequisites

To configure the virtual switches, you need:

- A web browser with Adobe Flash (required for the vSphere Web Client)
- VLAN assignments mapped to virtual switches
To configure virtual switches on each of the management servers:

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

2. If this is the first time you have logged in to the vSphere Web Console, read the information that is displayed; if you want to join VMware’s Customer Experience Improvement Program, select Join CEIP.

3. Click OK to continue.

4. From the Navigator menu, select Networking.

5. Click the Virtual Switches tab.

6. Select vSwitch0.

   A warning appears, advising that the virtual switch has no uplink redundancy.

7. Click Add uplink.

8. Under Add uplink:

   a. Change the maximum transmission unit (MTU) to 9000.

   b. Ensure that Uplink 2 is mapped to vmnic1.

9. Click Save.

10. From the Navigator menu, select Networking to return to the Networking home page.

11. To complete the network configuration for each host, create port groups for each VLAN, specifying:

    ▪ Name
    ▪ VLAN ID
    ▪ vSwitch to assign to each port group

   The following table shows the minimum recommended configuration.

Table 9. Virtual switch configuration

<table>
<thead>
<tr>
<th>Port group name</th>
<th>VLAN ID</th>
<th>Virtual network adapters</th>
<th>Load balancing algorithm</th>
<th>MTUs</th>
<th>vSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Management</td>
<td>110</td>
<td>• vmnic0 – active</td>
<td>Route based on originating virtual port ID</td>
<td>9,000</td>
<td>vSwitch0</td>
</tr>
<tr>
<td>vMotion</td>
<td>120</td>
<td>• vmnic0 – active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute VM</td>
<td>210</td>
<td>• vmnic0 – active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out-of-Band</td>
<td>1090</td>
<td>• vmnic0 – active</td>
<td></td>
<td>1,500</td>
<td></td>
</tr>
</tbody>
</table>

For vSphere vMotion and vSphere Distributed Resource Scheduler support, the spelling and capitalization of the VLAN IDs and names must match across the three management servers.
Chapter 6: Management Cluster Deployment

Note: Including the Compute VM port group in the management host vSwitch configuration is optional.

a. Click the Port groups tab and select Add port group.
b. Provide the requested information for the vMotion port group, as shown in the following figure.

Keep the default Security setting.

Figure 12. Adding a port group

In this example, we removed the default VM Network because we do not use it in our environment example.

The following figure shows an example of the configuration after all port groups are created.

Figure 13. Port groups configuration

12. Confirm the settings for each port group:

a. Right-click the port group name, and then left-click Edit settings, as shown in the following figure.

Figure 14. Editing settings

b. Ensure that the values match the properties in Table 9, Virtual switch configuration, on page 42.

The following example is for the vMotion port group.
Figure 15. vMotion port group settings

- Confirm the settings and click **Save**.
- Repeat the preceding steps for each additional port group to confirm each group’s settings.

**Create vMotion VMkernel ports**

To complete the setup of the virtual standard switches, create VMkernel ports for vMotion:

1. On the **Networking** page of vSphere Web Client, click the **VMkernel NICs** tab.
2. Click **Add VMkernel NIC**.
3. From the **Port group** list, select **vMotion**.
4. In the **MTU** field, enter **9000**.
5. If you are using a static IP address, under **IPv4 settings**:
   a. Select static for the configuration.
   b. Enter the address and subnet mask information.
6. From the **Services** menu, select **vMotion**.
7. Confirm the settings and click **Create**.
8. Verify that all VMkernel NICs have been created and that the appropriate services have been assigned to them, as shown in the following example.
Creating a management datastore from the PowerMax LUN

In preparation for deployments of vCenter and other management VMs, create a shared datastore for the management cluster:

1. In the vCenter Web Client, go to **Hosts and Clusters** and select the first management host.
2. In the right 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. On the **Name and device selection** page, provide a name for the datastore in the **Datastore name** field.
7. Select the LUN that was created for the management cluster in **Adding cluster hosts to the storage array** on page 32, and then click **Next**.
   
   If the LUN is not visible, verify the zoning configuration on the FC switches and the management host access in Unisphere storage management.
8. On the **VMFS version** page, select a VMFS version.
9. On the **Partition configuration** page, adjust the **Datastore Size** if needed, and then click **Next**.
10. On the **Ready to complete** page, click **Finish**.

**Multipathing optimization**

Block storage that is presented to vSphere hosts from the PowerMax system has the native Path Selection Policy (PSP) of round-robin (RR) applied by default. While RR is the recommended PSP to apply to PowerMax block storage, the default number of IOPS between the switching of paths is 1,000.

You can reduce the default number of IOPS for all PowerMax LUNs on each vSphere host so that all paths are used more efficiently by running the following CLI command:

```
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` is the first four digits of the PowerMax disk (or endpoint) devices found by running the following CLI command:

```
esxcli storage nmp device list
```
and \( # \) is the number of IOPS that you want between the switching of paths.

Additionally, you can create a claim rule to automatically set this value on LUNs that are later mapped to the host by running the following CLI command:

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

### Deploying vCenter Server Appliance

This section describes how to deploy vCenter Server Appliance with an embedded Platform Service Controller. For information about how to deploy vCenter Server Appliance with an external Platform Services Controller, see the VMware documentation.

#### Prerequisites

To deploy vCenter Server Appliance, you need:

- vCenter Server Appliance ISO, downloaded to a location that will be available throughout the deployment process
- IP address for vCenter Server Appliance
- Hostname and, if required, DNS server record for hostname
- vCenter datastore LUN

#### Deploy vCenter Server Appliance

To deploy vCenter Server Appliance:

1. Open the vCenter Server Appliance installation ISO file.
   
   In this example we are using a Windows workstation. Depending on your workstation operating system, you might have to use an external utility to mount the ISO file.

2. From the root of the ISO image, go to the `\vcsa-ui-installer\win32\` directory.

3. Double-click `installer.exe`.

4. On the main menu of the installer utility, click **Install**.

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

6. Review the End User License Agreement (EULA) carefully.
   
   a. If you agree with the terms of the EULA, select **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. Enter the requested information for the first management host, as shown in the following figure.
9. Verify that the details are correct, and then click **Next**.

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

11. Enter the name for the vCenter Server Appliance VM, and then create a password.

12. Click **Next**.
    
    The deployment sizing page provides a chart to assist you in selecting the deployment size.

13. Select a deployment size and storage size, and then click **Next**.

14. Select the management datastore that you previously created and click **Next**.

15. Fill in the appropriate details on the configure network settings page, and then click **Next**.

16. Verify that all the information displayed is correct and click **Finish**.

    When the vCenter Server Appliance installation is complete, the following message appears.

```
Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

You have successfully deployed the vCenter Server with an Embedded Platform Services Controller.

Deployment complete

To proceed with stage 2 of the deployment process, appliance setup, click Continue.
```

17. Click **Continue** to proceed to setting up the appliance.

**Set Up vCenter Server Appliance**

Set up vCenter Server Appliance:

1. Review the introduction and click **Next**.

2. Select the time synchronization mode and enter the NTP server information, as shown in the following figure, and then click **Next**.
Chapter 6: Management Cluster Deployment

Figure 19. NTP information

3. Enter the requested SSO information, as shown in the following figure, and then click **Next**.

![SSO configuration](image)

Figure 20. SSO information

4. Review the information about the VMware Customer Experience Improvement Program.
   a. Choose whether to contribute.
   b. Click **Next**.

5. Review the information for accuracy and click **Finish**.
   A dialog box displays a message to warn you that you cannot pause or stop the installation after it begins.

6. Click **OK** to proceed.

7. After the setup is complete:
   a. Note the URLs that are provided.
   b. Click **Close** to exit the installer.
Adding vCenter Server to Unisphere storage management

Add vCenter Server to Unisphere storage management to ensure that specific vSphere features such as Virtual Volumes (VVols) work properly.

1. Log in to Unisphere storage management.
2. Under Access, select VMware.
3. Click the plus sign (+) in the upper left of the right pane to open 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, you can also use the hostname of the vCenter server.
5. In the User Name and Password fields, enter the administrator credentials for the vCenter server, and then click Find.
6. Select the ESXi hosts to be imported to Unisphere storage management, and then click Next.
7. On the Configure VASA Provider page:
   a. Select Register VASA Provider.
   b. In the User Name and Password fields, enter the vCenter credentials.
   c. Click Next.
8. On the Summary page, review the displayed information and click Finish.

Configuring Active Directory authentication (optional)

This section describes the optional, additional steps that are necessary to configure Active Directory authentication for vCenter.

1. Open a web browser and go to the vSphere Web Client at https://<vCenter Server Appliance FQDN or IP>/vsphere-client.
2. Login as the SSO administrator (example: administrator@vsphere.local).
3. Select Administration > Deployment > System Configuration.
4. Click Nodes, and then click the vCenter Server Appliance node, as shown in the following example.

Figure 21. vCenter Server Appliance node selection
5. Under the Manage tab, click Settings and select Advanced > Active Directory.
6. Click Join and enter the requested information for your domain.
7. Click OK.
8. Under the context menu, right-click the vCenter Server Appliance and select Reboot.
10. Log in as the SSO administrator (example: administrator@vsphere.local).
12. Click the Identity Sources tab.
13. Click the green plus sign (+) to add an identity source.
15. Enter the domain name, and then click OK.

Disabling SSH on ESXi hosts (optional)

After the setup is complete, you might need to disable SSH access to the ESXi hosts to comply with the organization’s security policies. Disable SSH access:

1. Log in to the vCenter Server Appliance web console.
2. From the Navigator menu, select Hosts and Clusters.
3. Select an ESXi host, and then click the Configure tab.
5. Scroll down to Services, as shown in the following figure, and then click Edit.

![Services menu](image)
6. In the **Edit Security Profile** dialog box, as shown in the following figure, select **SSH** and click **Stop**.

![Edit Security Profile page](image)

7. When prompted to confirm the change, click **Yes**.
8. Change the startup policy to **Start and stop manually**.
9. Click **OK**.

### Configuring the management cluster

After completing the preceding procedures, complete the management cluster setup by creating the virtual datacenter and management cluster, and then add the ESXi management hosts to the cluster.

This section uses the following information from Table 19 of the site survey:

- **Management cluster name**—MgmtPod
- **Virtual datacenter name**—Site A
- **Cluster hosts**—Mgmt01, Mgmt02

Create the datacenter and cluster containers within vSphere:

1. Open a web browser and go to the vSphere Web Client at [https://<vCenter Server Appliance FQDN or IP>/vsphere-client](https://<vCenter Server Appliance FQDN or IP>/vsphere-client).
2. Log in with an account that has administrator privileges.
3. On the **Home** page, go to **Hosts and Clusters**.
4. Under **Navigator**, right-click the top-level vCenter Server Appliance object, as shown in the following figure, and click **New Datacenter**.
5. Right-click the new virtual datacenter object that appears in the Navigator menu, and then click New Cluster.

6. Enter the name for the datacenter, and then click OK.

7. In the New Cluster dialog box:
   a. Enter the cluster name.
   b. Enable Distributed Resource Scheduler and HA by selecting Turn ON next to each item.
   c. For a two-node management cluster, do not enable admission control.

8. Click OK to complete creating the cluster.

**Note:** To change heartbeat settings within the vSphere Web Client, go to Hosts and Clusters > <Cluster_Name> > Configure > vSphere Availability > Edit > Heartbeat Datastores.

### Add ESXi hosts to the management cluster

Add the three management hosts to the new management cluster as follows. First perform the following steps on the management server that is running vCenter Server Appliance, and then repeat the steps on the remaining hosts.

1. Open a web browser and go to the vSphere Web Client at https://<vCenter Server Appliance FQDN or IP>/vsphere-client.

2. Log in with an account that has administrator privileges.

3. On the Home page, go to Hosts and Clusters.

4. Right-click the management cluster object, and then select Add host.

5. Enter the 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.

7. Wait for the host to be added and for HA to be configured.

8. Repeat the preceding steps for the remaining hosts.

You might receive vCenter cluster-level alerts. These alerts can be reset to green during the cluster configuration process.
This chapter presents the following topics:

**Prerequisites**............................................................................................................... 54
**Installing ESXi on the compute hosts** .............................................................. 54
**Configuring the ESXi management network on the compute cluster** ........ 55
**Adding ESXi hosts to vCenter** ........................................................................... 56
**Creating and configuring vSphere Distributed Switch** ................................ 56
**Configuring host networking** ............................................................................ 59
**Creating a compute cluster** ............................................................................... 61
Chapter 7: Compute Cluster Deployment

Prerequisites

To deploy the compute cluster, you need:

- iDRAC IP addresses or FQDNs
- iDRAC credentials
- iDRAC Enterprise license applied on all nodes
- Dell EMC-customized ESXi 6.5 image

For download instructions, see VMware vSphere ESXi 6.5.x on Dell EMC PowerEdge Systems Image Customization Information on Dell EMC Online Support. Make a note of the image location on your system because you will need it when mounting virtual media.

- Hostnames, Management VLAN ID, and IP address information
- vSphere credentials
- Static IP addresses for each of the management servers
- (Optional) DNS server records for hostnames

**Note:** The iDRAC User Guide provides instructions for setting up the iDRAC, including configuring the IP address. For a link to the guide, see the iDRAC page on Dell EMC Online Support.

Installing ESXi on the compute hosts

Follow the procedures in this section to install VMware ESXi on each of the servers that will be part of the compute cluster. You can install ESXi remotely through the iDRAC web interface or locally. These procedures provide the steps for performing the installation remotely.

**Configure the BIOS settings and connect to the iDRAC**

Configure the BIOS settings and connect to the iDRAC:

1. Apply the BIOS settings profile that is optimized for maximum virtualization performance:
   a. Connect to the iDRAC IP address of one of the compute hosts by using an SSH client such as PuTTY.
   b. Log in with the appropriate credentials.
      The default credentials are user root and password calvin.
   c. At the /admin1-> prompt, run the following command:
      racadm set bios.sysprofilesettings.WorkloadProfile VtOptimizedProfile
   d. Create a job for processing the change by running the following command:
      racadm jobqueue create BIOS.Setup.1-1
   e. Reboot the compute host.
f. Repeat the preceding steps for all remaining compute hosts.

2. Using a web browser, go to the iDRAC web interface at https://<iDRAC Address>.

3. Log in with the appropriate credentials.
The default credentials are user root and password calvin.

4. Click the Virtual Console preview to open the Virtual Console.
For each iDRAC, ensure that pop-up support is enabled in your browser.

5. From the Virtual Media menu, select Connect Virtual Media to attach the virtual media.

6. From the Virtual Media menu, select Map CD/DVD to mount the Dell EMC ISO image for VMware ESXi 6.5.

7. Click Browse to go to the location of the Dell EMC ISO file for VMware ESXi 6.5, select the file, and click Open.
This location must be available throughout the installation of ESXi on all servers.


9. From the Virtual Console menu bar, select Next Boot > Virtual CD/DVD/ISO.

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

To boot to the installation media, from the Virtual Console menu bar, select Power > Power on System; alternatively, if the power is already on, select Power > Power Cycle System (cold boot). After the server reboots, the ESXi installer begins to load.

To install ESXi on the compute cluster, follow the steps in Install VMware ESXi on the management cluster on page 39.

Configuring the ESXi management network on the compute cluster

Configure and test the ESXi management network on the compute cluster as follows:

- Follow the steps in Configuring the ESXi management network on page 40.
- Follow the steps in in Test the management network on page 41.
Chapter 7: Compute Cluster Deployment

Adding ESXi hosts to vCenter

Add the ESXi hosts to vCenter:
1. Open a web browser and go to the vSphere Web Client at \(<vCenter Server Appliance FQDN or IP>/vsphere-client.\)
2. Log in with an account that has administrator privileges.
3. On the Home page, go to Hosts and Clusters.
4. Right-click the datacenter object, and then select Add host.
5. Enter the appropriate DNS name or IP address for the first compute host.
6. Complete the remainder of the Add Host wizard.
7. Repeat steps 3 through 6 for each host.

Creating and configuring vSphere Distributed Switch

The Dell EMC Ready Stack uses vSphere Distributed Switch (VDS) in the compute cluster. VDS enables multiple hosts to use a single virtual switch configuration.

Create the VDS

To create the VDS:
1. Open a web browser and navigate to the vSphere Web Client at \(<vCenter Server Appliance FQDN or IP>/vsphere-client.\)
2. Log in with an account that has administrator privileges.
4. Right-click the datacenter object, and then select Distributed Switch > New Distributed Switch.
5. Enter a name for the VDS, as shown in the following figure, and then click Next.

![Figure 25. Naming the VDS](image)

6. On the Select version page of the wizard, ensure that Distributed switch: 6.5.0 is selected, and then click Next.
7. On the Edit settings page, as shown in the following figure:
   a. Set Number of uplinks to 2.
   b. Set Network I/O Control to Enabled.
   Do not create a default port group.
8. Click Next and then Finish to create the VDS.

9. Right-click the VDS and select Settings > Edit Settings.

10. Select Advanced, set MTU (Bytes) to 9000, and then click OK.

Create port groups

After you create the VDS, create port groups on the VDS as follows. At a minimum, port groups for management and vMotion traffic are required.

1. Right-click the VDS and select Distributed Port Group > New Distributed Port Group.

2. Enter a name for the port group, as shown in the following figure, and then click Next.

3. On the Configure Settings page, as shown in the following figure:
   a. For tagged VLANs, in the VLAN type field, select VLAN and enter the VLAN ID.
   b. Select Customize default policies configuration.
Chapter 7: Compute Cluster Deployment

Figure 28. Configuring VLAN settings

4. Click Next.

5. Review the security policies and traffic shaping options; click Next on each to proceed.

6. On the Teaming and failover page:
   a. Set Load balancing to Route based on originating virtual port.
   b. Ensure that Uplink 1 and Uplink 2 are both active, as shown in the following figure.

Figure 29. Teaming and failover

7. Click Next to proceed through the remaining menus.

8. On the Ready to complete page, review the settings and click Finish.

9. Repeat the preceding steps for each additional distributed port group.
Configuring host networking

Configuring host networking consists of adding the compute cluster hosts to the VDS and migrating the existing networking.

Add hosts to the VDS

To add the compute cluster hosts to the VDS:

1. Log in to the vCenter web client at https://<vCenter Address>/vsphere-client.
2. On the Home page, click the Networking icon.
3. Right-click the VDS for management traffic, and then click Add and Manage Hosts.
4. In the Add and Manage Hosts wizard:
   a. On the Select task page, ensure that Add hosts is selected, and then click Next.
   b. Click ✨ New hosts, and then select the hosts to be added, as shown in the following example.

![Figure 30. Select new hosts](image)

   c. Click OK, and then click Next.
   d. On the Select network adapter tasks page, ensure that Manage physical adapters and Manage VMkernel adapters are selected, and then click Next.
   e. Select a host vmnic1, and then click Assign Uplink.
   f. Select Uplink 2 and click OK.
   g. Repeat steps e and f for each host, and then click Next.
   h. Select a vmk0, click Assign Port Group, and select the management traffic port group.
   i. Repeat the preceding step for each additional vmk0.
   j. Select a host, and then click ✨ New adapter to add a VMkernel port for vMotion.
   k. Click Select an existing network, and then browse to select the vMotion port group.
   l. Click OK, and then click Next.
   m. On the Port Group Properties page, select vMotion Traffic, and then click Next.
n. Select Use Static IPv4 settings, and then enter the following information:
   - IPv4 address
   - Subnet mask
   - Default gateway
   - DNS server addresses

o. Click Next, and then click Finish.

p. Select the new VMkernel adapter, and then click Edit adapter.

q. Under Edit Settings, select NIC Settings, change the MTU value to 9000, and then click OK.

r. Repeat steps e through q for each host being added to the VDS.

s. Click Next.

t. Ensure that all hosts return a No impact status, as shown in the following example.

![Figure 31. Analyze impact page](image)

u. Click Next and then click Finish.

**Migrate networking**

After adding the hosts to the VDS, migrate vmnic0 to the management traffic VDS. While still in the Add and Manage Hosts wizard:

1. Right-click the vDS for management traffic, and then click Add and Manage Hosts.

2. Select Manage host networking, and then click Next.

3. Click Attached hosts, and then select all hosts that are attached to the vDS.

4. Select Configure identical networking settings at the bottom of the page, 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.

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

8. Select Uplink 1 and click OK.

9. Click Apply to all, and then click Next.
10. Ensure that all hosts return the **No Impact** status.
11. Click **Next**, and then then click **Finish**.

### Creating a compute cluster

With the hosts joined to vCenter and connected to the virtual distributed switches, join the configuration to a cluster as described in this section.

**Create the vCenter cluster object**

1. Open a web browser and navigate to the vSphere Web Client at https://<vCenter Server Appliance FQDN or IP>/vsphere-client.
2. Log in with an account that has administrator privileges.
3. On the **Home** page, go to **Hosts and Clusters**.
4. Under **Navigator**, right-click the virtual datacenter object, and then click **New Cluster**.
5. Enter a name for the cluster (for example, **Compute01**).
6. Enable Distributed Resource Scheduler and HA by selecting **Turn ON** next to each item.
7. Click **OK**.

**Move hosts to the cluster**

After creating the cluster, move the compute hosts into the cluster:

1. On the left pane that displays the host and cluster objects, select the first compute host.
2. Left-click the host and hold down the mouse button.
3. Drag the host over the cluster object and release the mouse.
4. After HA configuration is complete, repeat the preceding step for the remaining hosts.
Chapter 8 Management Software and Data Protection Deployment

This chapter presents the following topics:

- **Introduction** ......................................................................................................... 63
- **Deploying OMIVV** ................................................................................................ 63
- **Deploying vRealize Automation** ........................................................................ 73
- **Deploying vRealize Log Insight** ....................................................................... 74
- **Deploying vRealize Operations Manager** ...................................................... 75
- **Deploying ESA** .................................................................................................... 76
- **Deploying VSI** ..................................................................................................... 77
- **Deploying IDPA** ................................................................................................... 79
Introduction

This Ready Stack includes Dell EMC OpenManage Integration for VMware vCenter (OMIVV) and Dell EMC Virtual Storage Integrator (VSI) to integrate the management of the Dell EMC hardware components with vSphere. Dell EMC Integrated Data Protection Appliance (IDPA) provides data protection and recovery.

This chapter describes the common steps that are necessary to deploy OMIVV, VSI, and IDPA. Additional steps are provided as examples for configuring the applications. However, Dell EMC recommends that you consult the product documentation for a detailed set of instructions and to review advanced configuration options.

Deploying OMIVV

OMIVV is designed to streamline the management processes in your datacenter environment by enabling you to use vCenter to manage your entire server infrastructure—both physical and virtual.

Prerequisites

You must have adequate system resources for the OMIVV VM, based on the number of managed nodes. The following table lists the suggested resources.

<table>
<thead>
<tr>
<th>Deployment size</th>
<th>Number of managed nodes</th>
<th>Number of vCPUs</th>
<th>Memory (GB)</th>
<th>Minimum storage (GB)</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:

- The licenses have been downloaded and are ready for use.
- You use reservations (see vSphere documentation) to ensure that necessary memory resources are available to the OMIVV VM.
- OMIVV has network access to iDRACs, hosts, and vCenter.

Deploy OMIVV

Follow all the procedures in this section to deploy OMIVV.

Download the ZIP file

1. From Dell EMC Online Support, download the following file:
   
   DellEMC_OpenManage_Integration_<version number>_<build number>.zip

2. Go to the location where you have downloaded the file and extract the contents of the ZIP file.
Deploy the OVF file

Deploy the Open Virtualization Format (OVF) file that contains the OMIVV virtual 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 Windows server (2008 R2 or later).
3. Accept the EULA and save the OVF file.
4. Select a host from the vSphere Web Client, and then, in the main menu, select Actions > Deploy OVF Template.
5. In the Deploy OVF Template wizard, click Browse.
6. Select the local files with filenames that start with OpenManage_Integration. 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 to be created. The VM name is limited to 80 characters.
8. In the Select a folder or datacenter list, select a location for deploying the template, and then click Next.
9. Select the management cluster, and then click Next.
11. From the Select Virtual Disk Format list, select Thick Provision (lazy or eager Zeroed) or Thin Provision. Thick provisioning offers the best balance of performance and deployment time.
12. From the VM Storage Policy list, select a policy, and then click Next.
13. In the Setup Networks page, click Next. Dell EMC recommends that the OMIVV appliance and the vCenter server be on the same network.
14. On the Ready to Complete page, review the selected options for the OVF deployment and click Finish. A status window displays the progress of the deployment.

Perform initial OMIVV VM configuration

Perform the initial OMIVV VM configuration:

1. From the vSphere Web Client:
   a. Locate and select the OMIVV VM that you just deployed.
   b. Power on the VM.

   If you selected Power on after Deployment when you deployed the OVF file, the VM is powered on automatically.
2. Click the **Console** tab to access the VM console.
3. Allow OMIVV to complete its startup.
4. Enter the default user name, **admin**, and press Enter.
5. Enter a new administrator password and press Enter.
6. Reenter the administrator password and press Enter.
7. At the following setup page, click **Date/Time Properties**.

![Figure 32. OMIVV configuration UI](image)

8. On the **Date and Time** tab, select **Synchronize date and time over the network**.
9. Add valid NTP server details (ideally use the same NTP servers to which your vCenter is synchronized).
10. Click **Time Zone**, select the applicable time zone, and then click **OK**.
11. To configure a static IP address to the OMIVV appliance:
   a. Click **Network Configuration**.
   b. Select **Auto eth0**, and then click **Edit**.
   c. Select the **IPV4 Settings** tab, and then, from the **Method** list, select **Manual**.
   d. Click **Add**, and then enter the IP, netmask, and gateway information.
   e. In the **DNS Servers** field, enter the DNS server details, and then click **Apply**.
12. To change the host name of the OMIVV appliance:
   a. Click **Change Hostname**.
Enter a valid host name and click **Update hostname**.

13. Ensure that the OMIVV VM is restarted.


15. At the login prompt, enter the password.

The OMIVV Administration Console is displayed, as shown in the following figure.

![OMIVV Administration Console](image)

**Figure 33. OMIVV Administration Console**

### Register the vCenter server

To register the vCenter server:

1. In the **vCenter Registration** window, click **Register a New vCenter Server**.

2. Select **vCenter Name > vCenter Server IP or Hostname**, and enter the server IP address or hostname.

   Dell EMC recommends that you use a FQDN. Ensure that the vCenter hostname is properly resolved by the DNS server.

3. Optionally, enter a description in the **Description** field.

4. Select **vCenter User Account > vCenter User Name**, and enter the Admin username or the username with necessary privileges.

   Enter the username in one of the following formats:

   - `domain\user`
OMIVV uses the Admin user account, or the user with necessary privileges, for vCenter administration.

5. In the **Password** field, enter the password.
6. In the **Verify Password** field, reenter the password.
7. Click **Register**.

**Upload the license file**

To upload the license file:

1. Click **Upload License**.
2. In the **Upload License** window:
   a. Click **Browse** and browse to the license file.
   b. Click **Upload**.

**Verify the installation**

To verify the OMIVV installation:

1. Close any vSphere client windows.
2. Start a new vSphere Web Client.
3. Confirm that the OMIVV icon appears in the **Administration** section of vSphere Web Client.
4. Ensure that vCenter can communicate with OMIVV by running a ping command from the vCenter server to the virtual appliance IP address or hostname.
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.

**Configure OMIVV**

Configure the appliance as described in the following procedures.

**Open the Initial Configuration Wizard**

1. In vSphere Web Client, click **Home**, and then click the **OpenManage Integration** icon, as shown in the following figure.
The first time that you click the **OpenManage Integration** icon, the Initial Configuration Wizard is displayed. In the future, you can access the wizard by navigating to **OpenManage Integration > Getting Started** and then clicking **Start Initial Configuration Wizard**.

2. In the **Welcome** dialog box, review the steps, and then click **Next**.

3. Select the vCenter and click **Next**.

### 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 of the servers must be associated with a connection profile that OMIVV manages. You can assign multiple servers to a single connection profile.

Microsoft Active Directory is supported but not required. Prerequisites include:

- The user’s account exists in Active Directory if you want to use Active Directory credentials with a connection profile.
- The iDRAC and host are 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.

Begin to create a connection profile in the Initial Configuration Wizard:

1. On the **Description** page of the **Connection Profile**, click **Next**.
2. On the Name and Credentials page, as shown in the following figure, enter the connection profile name and, optionally, a description.

![Initial Configuration Wizard: Name and Credentials page](image)

**Figure 35. Initial Configuration Wizard: Name and Credentials page**

3. To use Active Directory, perform the following steps; otherwise, skip to step 4.
   a. Under iDRAC Credentials, select Use Active Directory.
   b. In the **User Name** field, enter the username in one of these formats:
      - domain\username
      - username@domain
      The username is limited to 256 characters.
   c. In the **Password** field, enter the password.
      The password is limited to 127 characters.
   d. In the **Verify Password** box, reenter the password.
   e. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
   f. Scroll down to the **Host Root** section and select **Use Active Directory**.
   g. In the **User Name** field, enter the username in one of these formats:
      - domain\username
      - username@domain
   h. In the **Password** field, enter the password.
   i. In the **Verify Password** field, reenter the password.
   j. To download and store the host certificate and validate it during all future connections, select **Enable Certificate Check**.
   k. Proceed to **Continue creating a connection profile**.
4. If you do not want to use Active Directory:
   a. Under the **iDRAC Credentials** section, in the **User Name** field, enter the username.
      The username is limited to 16 characters.
   b. In the **Password** field, enter the password.
      The password is limited to 20 characters.
   c. In the **Verify Password** field, reenter the password.
   d. To download and store the iDRAC certificate, and validate it during all future connections, select **Enable Certificate Check**.
   e. Scroll down to **Host Root** section.
   f. The user name is **root**, which is the default and cannot be changed.
   g. In **Password**, enter the password.
      The password is limited to 127 characters.
   h. In the **Verify Password** field, reenter the password.
   i. To download and store the iDRAC certificate and validate it during all future connections select **Enable Certificate Check**.
   j. Proceed to Continue creating a connection profile.

**Continue creating a connection profile**

Continue creating the 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 click **Test Connection**.
4. Click **Next** to finish creating the profile.

**Configure an inventory jobs schedule**

To configure a schedule for inventory jobs:

1. In the **Inventory Schedule** dialog box, select **Enable Inventory Data Retrieval**.
2. Select each day of the week that you want to run the job.
3. In the **Data Retrieval Time** field, enter a local time in HH:MM format.
4. Click **Next** to apply the changes and continue.
Configure a 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 each day of the week that you want to run the job.
3. Enter a local time in HH:MM format.
4. Click **Next** to apply the changes and continue.

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 an alert level.

   **Caution**: Dell EMC hosts that have alarms enabled respond to certain critical events by entering maintenance mode.

   The **Enabling Dell EMC Alarm Warning** dialog box is displayed.

3. To accept the change, click **Continue**.

Close the initial configuration wizard

Click **Finish** to close the initial configuration wizard.

Resolve host noncompliance

For vSphere 6.5 and later hosts, OMIVV requires that:

- Web-Based Enterprise Management (WBEM) is enabled.
- SNMP settings are configured.
- Hosts are part of a connection profile.

Ensure that your vSphere hosts are compliant with the OMIVV requirements:

1. In OMIVV, go to **Manage > Compliance > vSphere Hosts**.
2. Refresh the page to see a list of any noncompliant hosts, as shown in the following example.
3. If no hosts are listed and the page is disabled, then skip the remainder of this section.
4. Click **Fix non-compliant vSphere Hosts**.
5. Review the text and click **Next**.
6. Select the listed hosts, and then click **Finish**.
   
   Wait for OMIVV to process the necessary changes to the hosts.
7. Refresh the page to confirm that there are no longer any noncompliant hosts.

**Validate OMIVV functionality**

Validate OMIVV functionality by running a one-off inventory job:

1. In OMIVV, go to **Monitor > Job Queue > Inventory History > Hosts Inventory**.
2. In the **vCenters** list, click the vCenter server.
3. Click **Run Now** and wait for inventory jobs to complete.
4. Refresh the page and confirm that **Successful** is displayed for all hosts.

**Configure a firmware update repository**

To configure a repository for firmware update packages:

1. In OMIVV, go to **Firmware Update Repository > Appliance Settings > Manage > Settings**.
2. Click the **Edit** (pencil) icon.
3. In the **Firmware Update Repository** dialog box, select one of the following:

- **Dell Online**—A Dell EMC repository (ftp.dell.com). OMIVV downloads selected firmware updates from the repository and updates the managed hosts.
  
  Enable proxy settings if required.

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

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

4. If you selected **Shared Network Folder**, enter the **Catalog File Location** 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

5. Click **Apply**.

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

### Deploying vRealize Automation

**Introduction**

VMware vRealize Automation provides self-service IT deployment and delivery through a secure portal. The portal enables users to request new IT services and manage IT resources while ensuring compliance with business policies. Requests are processed through a published service catalog to provide a consistent user experience regardless of the underlying physical hardware configuration.

**Installation overview**

vRealize Automation can be deployed to support configurations of various sizes, which generally align with the deployment size of the Dell EMC Ready Stack. Provision resources for vRealize Automation components from the vCenter system that contains the server, network, and storage resources in the platform management cluster.

The vRealize Automation deployment process includes the following steps:

1. Install the vRealize Automation appliance.

2. Install the vRealize Automation components based on one of the following deployment types:

   - Minimal (proof of concept)
   - Distributed
Chapter 8: Management Software and Data Protection Deployment

- Large distributed and load-balanced

All Ready Stack configuration sizes provide sufficient resources to support these vRealize Automation deployment types.

While multiple installation methods are available, the consolidated vRealize Automation Installation Wizard is the primary installation tool.

As with any complex application, a successful vRealize Automation deployment requires extensive predeployment planning. Ensure that resources are in place before commencing installation, including, but not limited to:

- All necessary service accounts and groups have been created in Active Directory.
- All necessary SSL certificates have been created and are available. Dell EMC does not recommend using the default self-signed certificates in production deployments.
- All necessary services, such as NTP, DHCP, NetBIOS, and DNS, have been configured and are available with host and VM name resolution properly resolvable.
- An external database such as SQL Server is available for infrastructure components. Dell EMC does not recommend using the default internal database in production deployments.

For detailed installation and deployment information, see Installing and Upgrading vRealize Automation.

Deploying vRealize Log Insight

Introduction

VMware vRealize Log Insight provides heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility. vRealize Log Insight provides deep operational visibility and faster troubleshooting across physical, virtual, and cloud environments.

Installation overview

vRealize Log Insight can be deployed in various configurations to support environments of various sizes. As with vRealize Automation, these configurations generally align with the deployment size of the Dell EMC Ready Stack. Provision resources for vRealize Log Insight components from the vCenter system that contains the server, network, and storage resources in the platform management cluster.

The vRealize Log Insight deployment process includes the following steps:

1. Install the vRealize Automation appliance.
2. Install the vRealize Automation components based on one of the following deployment types:
   - Single node
   - Cluster
   - Cluster with forwarders
Log ingestion rate correlated to events per second generally drives vRealize Log Insight sizing, and VM template sizing ranges from extra small (for demo purposes only) to large.

All Ready Stack configuration sizes provide sufficient resources to support all vRealize Log Insight deployment types.

3. Integrate Log Insight with vRealize Operations Manager.
4. Install the following Dell EMC Content Packs for vRealize Log Insight:
   - PowerMax
   - PowerEdge/iDRAC

For detailed installation and deployment information, see the following resources:

- [Getting Started](https://vmware.com)
- [Using the Dell EMC VMAX and PowerMax Content Pack for VMware vRealize Log Insight](https://dellemc.com)
- [Dell - IDRAC](https://vmware.com)

**Deploying vRealize Operations Manager**

### Introduction

vRealize Operations Manager provides comprehensive IT operations management with end-to-end visibility across physical, virtual, and cloud infrastructures. Using policy-based automation, IT operations teams can automate key processes and improve IT efficiency based on real-time events.

### Installation overview

vRealize Operations Manager is designed to be easily expandable to ensure scale-out as your monitoring environment grows. Deployed as VMware vApps, a configuration consisting of small vRealize Operations nodes combined with an optional standard Remote Collector node is typically sufficient for all three Ready Stack deployment sizes. For sizing guidance, see VMware Knowledge Base article 57903: [vRealize Operations Manager 7.0 Sizing Guidelines](https://vmware.com).

For Ready Stack, Dell EMC recommends configuring a minimal vRealize Operations Manager deployment as follows:

- 1 x master node
- 1 x data node
- 1 x replica node

Depending on your environment, you might have to deploy an optional remote collector node, or additional master, data, and replica nodes.

The vRealize Operations Manager deployment process includes the following steps:

1. Ensure that all installation prerequisites have been met.

   Prerequisites are detailed in the [vRealize Operations Manager vApp Deployment Guide](https://vmware.com).
2. Download and install the VMware vRealize Operations Manager .ova file (OVF) for each vRealize Operations Manager node you want to deploy.

3. Connect to the vApp through a supported web browser to begin node configuration.

4. Select **New Installation** and follow the wizard to complete configuration of the master node.

5. Configure additional nodes such as data and replica.

6. Start vRealize Operations Manager and log in.

For detailed configuration information, see the [vRealize Operations Manager](#) Configuration Guide.

## Deploying ESA

### Introduction

Dell EMC Enterprise Storage Analytics (ESA) for vRealize Operations Manager is a management pack for VMware vRealize Operations Manager that enables the collection of analytical data from Dell EMC resources. ESA complies with VMware management pack certification requirements and has received the VMware Ready certification.

### Install the Dell EMC adapter

The ESA installation procedure installs the Dell EMC adapter and the dashboards. Before you begin, obtain the PAK file for the Dell EMC adapter from Dell EMC Online Support.

**Note:** If you use Microsoft Internet Explorer, the installation file downloads as a ZIP file but functions the same way as the PAK file.

**Caution:** When you upgrade ESA, the standard Dell EMC dashboards are overwritten. To customize a standard Dell EMC dashboard, clone it, rename it, and then customize it.

Install the adapter as follows:

1. Save the PAK file in a temporary folder.

2. In your web browser, start the vRealize Operations Manager administrative UI. For example, enter `https://vROPs_<ip_address>`.

3. Log in as an administrator.

4. Select **Administration > Solutions** and then click **Add (+)** to upload the PAK file.

5. When a UI message indicates that the PAK file is ready to install, complete the wizard.

   Depending on your system's performance, the installation can take from 5 to 15 minutes.

6. When the installation is complete, click **Finish**.

   The adapter appears in the list of installed solutions.

After ESA has been installed, configure it for vCenter and for the PowerMax array, as described in the [ESA product documentation](#) on Dell EMC Online Support.
Chapter 8: Management Software and Data Protection Deployment

Deploying VSI

Introduction

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

Deploy the VSI appliance

To deploy the VSI appliance:

1. Download the latest Solutions Integration Service OVA file from the following location:
   https://support.emc.com/products/32161_VSI-Series
2. Log in to the vSphere Web Client.
3. On the Home page, go to Hosts and Clusters.
4. Right-click the vCenter cluster and 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. At Select source, enter the location of the Solutions Integration Service OVA file, and then click Next.
7. On the Review details page, verify that the information is correct, and then click Next.
8. Accept the End User License Agreement (EULA), and then click Next.
9. At Select name and folder, enter a name for the destination folder if you want to change it from the default location.
10. Select the folder or datacenter location where you want to save the Solutions Integration Service OVA file, and then click Next.
11. At Select a resource, select the compute resource, and then click Next.
12. At Select storage, select a disk format and datastore, and then click Next.
13. At Setup network:

   a. Select a network.

   b. Select the IP address format IPV4 for the Solutions Integration Service.

14. For the 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 box, verify the details, and then click Finish.
16. Right-click the name of the VM with the newly deployed Solutions Integration Service, and then select **Power On**. Wait for the deployment to finish, and for the Solutions Integration Service to be operational.

17. Verify the REST web service deployment:
   a. Open a web browser, and go to:
      
      https://<Solutions_Integration_Service_IP Address>:8443/vsi_usm/
      
      For example: https://192.168.0.3:8443/vsi_usm/
   
   b. Accept all certificates or add them to exceptions.

18. Change the root password:
   a. Log in to the vSphere console with the default username **root** and password **root**.
   b. At the prompt, set a new, secure password for the root user.

19. Enable SSH:
   a. Log in to vSphere.
   b. Run the following commands:
      
      # systemctl enable sshd
      # systemctl start sshd
      
      The SSH service is now enabled.

Register the VSI plug-in

Register the VSI plug-in so that you can download and enable the VSI plug-in extensions:

1. Open a web browser and go to the Solutions Integration Service Administrator web page, logging in with the Solutions Integration Service credentials as follows:
   
   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** and enter values for the following parameters:
   - **vCenter IP/Hostname**—IP address that contains the VSI plug-in package
   - **vCenter Username**—Username that has administrative privileges
   - **vCenter Password**—Administrator’s password
   - **Admin Email (Optional)**—Email address to which notifications are to be sent

3. Click **Register**.

4. Browse to the **vSphere Web Client** address.

5. In the **vSphere Web Client** window, select **vCenter** in the navigation pane to verify that EMC VSI is listed.
Deploying IDPA

IDPA DP4400 is a converged appliance that combines backup, replication, deduplication, search, analytics, and instant access and restore, as well as disaster recovery and long-term retention in the cloud.

IDPA DP4400 provides comprehensive data protection that is simple to manage, deploy, and upgrade. It enables you to protect large application ecosystems, simplify data protection monitoring and management with the IDPA System Manager, and grow capacity from 24 TB to 96 TB without any additional hardware. DP4400 delivers an average data deduplication rate of 55:1 and shortens backup windows by up to two times. Compared to similar solutions, DP4400 provides protection at up to 80 percent less cost and protects up to four times more data in a single 2U appliance.

To deploy IDPA 4400, follow the instructions in the *Dell EMC Integrated Data Protection Appliance: Getting Started*. 
This chapter presents the following topics:

**Dell EMC documentation** ................................................................. 81

**VMware documentation** ............................................................... 81
Dell EMC documentation

The following Dell EMC documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell EMC representative.

- Dell EMC PowerEdge R640 Installation and Service Manual
- Dell EMC PowerEdge MX7000 Spec Sheet
- Integrated Dell Remote Access Controller 9 User Guide
- Knowledge Base: iDRAC9
- PowerMax Technical Documentation
- Using the Dell EMC VMAX and PowerMax Content Pack for VMware vRealize Log Insight
- OS10 Enterprise Edition User Guide
- Support for Dell Networking S3048-ON: Manuals & documents
- Support for Dell Networking S5248F-ON: Manuals & documents
- Connectrix DS-6510B: Documentation
- VSI for VMware vSphere Web Client: Documentation
- OpenManage Integration for VMware vCenter Knowledge Base
- Dell EMC Integrated Data Protection Appliance: Getting Started
- Enterprise Storage Analytics product documentation

VMware documentation

The following VMware resources provide additional and relevant information:

- VMware vSphere 6.5 Documentation Center
- Installing and Upgrading vRealize Automation
- Getting Started: vRealize Log Insight 4.7
- Dell - IDRAC
- vRealize Operations Manager vApp Deployment Guide
- vRealize Operations Manager Configuration Guide
This appendix presents the following topic:

**Site survey tables**........................................................................................................83
Appendix A: Site Survey

Site survey tables

Before you begin the Ready Stack deployment, gather site information as outlined in the following tables.

Table 11. Network topology

<table>
<thead>
<tr>
<th>Switch</th>
<th>Hostname</th>
<th>Management IP address</th>
<th>VLT ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3048-ON</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5248-ON-Top</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5248-ON-Bottom</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional configuration notes (Spanning Tree Protocol, routing protocols, and so on, as applicable):

Table 12. VLAN information

<table>
<thead>
<tr>
<th>Network type</th>
<th>VLAN ID</th>
<th>S5248F-ON-Top IP CIDR</th>
<th>S5248F-ON-Bottom IP CIDR</th>
<th>VRRP IP address</th>
<th>VRRP group</th>
<th>S3048 IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOB</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>
<tr>
<td>vMotion</td>
<td>120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute VM</td>
<td>210</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 13. Network services

<table>
<thead>
<tr>
<th>Next hop/default gateway</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS [1, 2]:</td>
<td></td>
</tr>
<tr>
<td>NTP [1, 2]:</td>
<td></td>
</tr>
</tbody>
</table>

Table 14. Switch port mappings

<table>
<thead>
<tr>
<th>S5248F-ON-Top</th>
<th>S5248F-ON-Bottom</th>
<th>S3048-ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>NIC port 1</td>
<td>NIC port 2</td>
</tr>
<tr>
<td>Mgmt1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 15. 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>S5248F-ON-Top</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S5248F-ON-Bottom</td>
<td></td>
</tr>
<tr>
<td>OOB</td>
<td>Standard</td>
<td>101</td>
<td>S5248F-ON-Top</td>
<td>S5248F-ON-Bottom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S3048-ON-OOB</td>
<td></td>
</tr>
</tbody>
</table>

### Table 16. FC port mapping

<table>
<thead>
<tr>
<th>FC port</th>
<th>WWN</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-A P0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-A P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-A P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-A P3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-B P0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-B P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-B P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-B P3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt1 P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt1 P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt2 P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt2 P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp1 P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp1 P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2 P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2 P2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3 P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3 P2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 17. Host information

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Gateway</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 18. Management virtual machines

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Gateway</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server Appliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OMIVV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDPA 4400</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 19. vSphere HA cluster information

<table>
<thead>
<tr>
<th>Cluster details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management cluster name</td>
<td>MgmtPod</td>
</tr>
<tr>
<td>Virtual datacenter name</td>
<td>Site A</td>
</tr>
<tr>
<td>Management cluster hosts</td>
<td>Mgmt1, Mgmt2</td>
</tr>
<tr>
<td>Compute cluster name</td>
<td>ComputePod</td>
</tr>
<tr>
<td>Cluster hosts</td>
<td>Comp1, Comp2, Comp3</td>
</tr>
</tbody>
</table>