Abstract
This deployment guide describes the requirements, configuration, and deployment of a converged infrastructure that is based on VMware Cloud Foundation and Dell EMC PowerEdge servers, Unity All Flash storage, and integrated data protection.
Copyright

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 08/19 Deployment Guide H17834.

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

Chapter 2 Predeployment Requirements
Introduction .......................................................................................................................................9
Data center requirements ..................................................................................................................9
Site survey information ....................................................................................................................9
Validated components ......................................................................................................................9

Chapter 3 Physical Layout
Introduction .......................................................................................................................................12
Rack layout ......................................................................................................................................12
Cabling............................................................................................................................................14
Hardware installation checklist ........................................................................................................15

Chapter 4 Network Configuration
Introduction .......................................................................................................................................17
Configuring Dell EMC PowerSwitch S5248F-ON switches ................................................................18
Configuring the Dell EMC PowerSwitch S4148T-ON switch ................................................................24
Preparing switches for NSX Edge routing .......................................................................................27
Networking configuration checklist ..................................................................................................29

Chapter 5 SAN Storage Deployment and Configuration
Introduction .......................................................................................................................................31
Deploying Unity XT x80 storage .......................................................................................................31
Deploying Connectrix DS-6620B switches .........................................................................................33
Site survey example: FC port mappings ............................................................................................33
Zoning host servers to storage controllers ........................................................................................34
Adding cluster hosts to the storage array ..........................................................................................36
Creating a LUN ................................................................................................................................37

Chapter 6 VMware Cloud Foundation Deployment
Introduction .......................................................................................................................................40
General deployment guidelines ........................................................................................................40
Installing ESXi on the management hosts .........................................................................................41
Configuring the ESXi management network .......................................................... 44
Installing VMware Cloud Foundation Builder ....................................................... 47
Completing the deployment parameter sheet ...................................................... 48
Creating the management domain ..................................................................... 49

Chapter 7  Compute Cluster Deployment 50
Prerequisites ....................................................................................................... 51
Installing ESXi on the compute hosts ................................................................. 51
Configuring the ESXi management network on the compute cluster .......... 51
Configuring NFS resources in SDDC Manager .................................................... 53
Configuring NFS on Unity XT x80 ..................................................................... 55
Deploying the VI workload domain ................................................................... 56
Creating VI workload domain datastores ......................................................... 57

Chapter 8  Management Software and Data Protection Deployment 58
Introduction ........................................................................................................ 59
Deploying OMIVV ............................................................................................. 59
vRealize Suite product deployment overview ................................................... 69
Deploying vRealize Lifecycle Manager .............................................................. 69
Deploying vRealize Automation ........................................................................ 70
Deploying vRealize Log Insight ........................................................................ 71
Deploying vRealize Operations ......................................................................... 72
Connecting vRealize Suite to workload domains ............................................. 73
Enabling vRealize Log Insight connection to workload domains ................... 74
Deploying ESA .................................................................................................. 74
Deploying VSI .................................................................................................... 75
Deploying IDPA .................................................................................................. 77

Chapter 9  References 78
Dell EMC documentation .................................................................................. 79
VMware documentation ..................................................................................... 79

Appendix A  Site Survey 80
Site survey tables ............................................................................................... 81
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 data center 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 Unity XT x80 storage
- Dell EMC PowerEdge servers
- Dell EMC S-Series switches
- Dell EMC Connectrix DS-6600 Series Fibre Channel (FC) switches
- VMware data center virtualization and management product suites that support the VMware Cloud Foundation integrated hybrid cloud platform
- 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
- A reference architecture that incorporates physical topology diagrams and general connectivity guidelines
- Design guidance that focuses on scale, flexibility, and high availability
- Design and deployment guidance that incorporates validation, interoperability testing, and best practices
- Software-designed data center (SDDC) integration that enables intelligent operations, automation, and analysis through VMware vRealize Automation, VMware vRealize Log Insight, and VMware vRealize Operations
- Unified management and system monitoring through VMware vCenter and VMware Cloud Foundation SDDC 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. VMware validated the PowerEdge server configurations as vSAN Ready Nodes, which form the basis for the compute and storage components in a VMware Cloud Foundation deployment.

In addition to Ready Stack, Dell EMC offers other SDDC platforms that are enabled by VMware Cloud Foundation, including Dell EMC VxRail SDDC.

Document purpose and scope

This guide provides basic guidance for deploying Dell EMC Ready Stack for VMware Cloud Foundation. For links to related product installation guides, see Chapter 9, References.
This guide provides deployment guidance only. Information about any modifications to the configuration and their potential impact on configuration availability is outside the scope of this document. For detailed information about the Ready Stack architecture, see the *Dell EMC Ready Stack: VMware Cloud Foundation on PowerEdge Servers and Unity Storage Design Guide*.

This document does not include information about existing infrastructure components beyond those in 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 prerequisites and a knowledge of data center 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 author 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

**Note:** For links to additional documentation for this solution, see the [Ready Stack Info Hub](#).
Chapter 2 Predeployment Requirements

This chapter presents the following topics:

- **Introduction** ................................................................. 9
- **Data center 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. This chapter describes the predeployment requirements for proceeding with the deployment.

Data center requirements

To support the solution, the environment must include:

- An existing Ethernet infrastructure with which to integrate. Dell EMC PowerSwitch S5248F-ON switches support 10/25 GB and 40/100 GB uplinks to the network core switches. Additional components, such as Dell EMC network cables and transceivers, are needed. Ensure that you have all necessary components to facilitate connecting to the existing network before beginning deployment.
- Microsoft Active Directory, DNS, and NTP services on the management network. A DHCP server is recommended but not required.
- An enterprise Certificate Authority or third-party service.
- Sufficient power and cooling to support all components. To determine accurate power and cooling needs, see the component product documentation.

Site survey information

Appendix A on page 80 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.

VMware Cloud Foundation has an extensive checklist to help ensure that customers have all the necessary information to plan and prepare for a successful deployment. When deploying VMware Cloud Foundation, completing the requirements before beginning deployment is critical. See the VMware Cloud Foundation documentation and sign up for the VMware Cloud Foundation Planner well ahead of your planned deployment.

Validated components

The following table lists the software and firmware versions that we have 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>Virtualization hosts</td>
<td>Dell EMC PowerEdge R640/R740/740xd (vSAN Ready Node models that are required for management domain)</td>
<td>• BIOS 1.6.13&lt;br&gt;• iDRAC 3.30.30</td>
</tr>
<tr>
<td></td>
<td>Intel X710 quad-port 10 Gb direct attach, small form-factor pluggable plus (SFP+), converged network adapter, low-profile</td>
<td>• Firmware 18.8.9&lt;br&gt;• Driver 18.8.0</td>
</tr>
<tr>
<td></td>
<td>QLogic 2692 dual-port FC host bus adapter (HBA) (workload domain)</td>
<td>• Firmware 14.10.05&lt;br&gt;• Driver 3.1.16.0-1</td>
</tr>
<tr>
<td></td>
<td>Dell EMC PERC H330 minicard</td>
<td>• Firmware 16.17.00.03&lt;br&gt;• Driver 2.51.25.01</td>
</tr>
<tr>
<td></td>
<td>Dell EMC BOSS controller card+ with 2 x M.2 sticks 120 GB (RAID 1) FH, or Internal SD Module with 2 x 16 GB SD Card</td>
<td>• Firmware 2.5.13.3016&lt;br&gt;• Driver 1.2.0.1048</td>
</tr>
<tr>
<td></td>
<td>2 X 400 GB SSD SAS write-intensive 12 Gb/s 512n 2.5 in. hot-plug drive, PX05SM, 10 DWPD, 7,300 TBW (optional vSAN caching tier)</td>
<td>Firmware AS0E, A00</td>
</tr>
<tr>
<td></td>
<td>8 x 1.8 TB 10K RPM SAS 12 Gb/s 512e 2.5 in. hot-plug hard drive (optional vSAN capacity tier)</td>
<td>Firmware 2T51</td>
</tr>
<tr>
<td>Network</td>
<td>Out-of-band (OOB)—Dell EMC PowerSwitch S4148T-ON switch (S3048-ON may also be used)</td>
<td>• Firmware 3.33.5.1-19, A00&lt;br&gt;• OS 10.4.3.0</td>
</tr>
<tr>
<td></td>
<td>Top-of-rack (ToR)—Dell EMC PowerSwitch S5248F-ON switch (leaf)</td>
<td>• Firmware 3.40.5.1-11, A00&lt;br&gt;• OS 10.4.3.0</td>
</tr>
<tr>
<td></td>
<td>Dell EMC PowerSwitch Z9264F-ON switch (for spine, if needed)</td>
<td></td>
</tr>
<tr>
<td>Storage (workload domain)</td>
<td>Dell EMC Unity XT x80 all-flash unified storage</td>
<td>Unity OE 4.5.1.0.5.001</td>
</tr>
<tr>
<td></td>
<td>2 x Dell EMC Connectrix DS-6620B switches</td>
<td>Fabric OS 8.2.1a</td>
</tr>
<tr>
<td>Software</td>
<td>VMware Cloud Foundation</td>
<td>3.5.1 [VMware Cloud Foundation Bill of Materials]</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Virtual Storage Integrator (VSI)</td>
<td>8.0</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>4.2</td>
</tr>
<tr>
<td></td>
<td>Dell EMC Integrated Data Protection Appliance (IDPA) DP4400</td>
<td>2.3</td>
</tr>
</tbody>
</table>
Chapter 3: Physical Layout

This chapter presents the following topics:

Introduction...............................................................................................................12
Rack layout................................................................................................................12
Cabling......................................................................................................................14
Hardware installation checklist..............................................................................15
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 Ready Stack physical rack layout is flexible and depends on many data center elements such as power, thermals, and weight restrictions. 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.

The Dell EMC Unity XT x80 storage arrays are the latest release in the Unity family of unified storage products that offers integrated block, file, and advanced data services. New features include: More memory, more processing power, 25 GbE I/O support, larger capacity drives with non-volatile memory express (NVMe) support, data services including inline data reduction, and enhanced replication. These features contribute to performance and efficiency increases from the previous generation of up to two and three times, respectively.

Unity XT x80 storage can require fewer or additional disk enclosures, depending on the storage capacity and solid-state drive (SSD) type. Additional items such as Dell EMC Integrated Data Appliance (IDPA) can also be included within the same rack, space permitting. Ready Stacks are sized in Enterprise Small, Medium, and Large configurations. The following figure is an example of the Enterprise Medium configuration:
Figure 1. Ready Stack components in Enterprise Medium configuration—front rack view
Cabling

The following figure shows the required cabling for the Ready Stack workload domain components. The management domain servers use vSAN storage so do not require connectivity to the Connectrix switches.

![Dell EMC Ready Stack cabling diagram](image)

Figure 2. Dell EMC Ready Stack cabling

Networking technology of 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-6620B switches are prepopulated with the required FC optics. Unity XT x80 storage and PowerEdge servers require additional 16 GB small form-factor pluggable (SFP) FC adapters. Dell EMC Multimode LC/LC fiber optic cables are required between the PowerEdge server and Unity XT x80 storage array and the Connectrix FC switches. Cat 5e or Cat 6 Ethernet cabling is required for Dell EMC iDRAC, Connectrix, and Unity XT x80 management connectivity. For small configurations, you can connect 1 GbE devices to ToR switches by using a 1000Base-T SFP transceiver, which eliminates the need for the Dell EMC S4148T-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 and fabric connections from switches to servers have been made, as shown in Figure 2 on page 14.
- Power has been connected to each component.
Chapter 4 Network Configuration

This chapter presents the following topics:

- Introduction ....................................................................................................... 17
- Configuring Dell EMC PowerSwitch S5248F-ON switches ............................. 18
- Configuring the Dell EMC PowerSwitch S4148T-ON switch ......................... 24
- Preparing switches for NSX Edge routing ....................................................... 27
- Networking configuration checklist ................................................................. 29
Chapter 4: Network Configuration

Introduction

This chapter describes how to configure the Ready Stack for PowerSwitch S4148T-ON out-of-band (OOB) management and S5248F-ON top-of-rack (ToR) switches. The configuration reflects a standard VMware Cloud Foundation deployment configuration, with discrete management and workload domains. These procedures are an example of a working configuration. Ensure that you review the procedures with your site networking team before performing them.

Networking site survey information

The networking site survey tables in this section are examples only. Appendix A on page 80 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>S4148T-ON</td>
<td>SWOOOB</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>S5248F-ON-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-ON-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>SS5248F-ON-Top IP CIDR</th>
<th>SS5248F-ON-Bottom IP CIDR</th>
<th>VRRP IP address</th>
<th>VRRP group</th>
<th>S4148T-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>Not applicable</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>Not applicable</td>
</tr>
<tr>
<td>vSAN</td>
<td>130</td>
<td>172.90.130.252/24</td>
<td>172.90.130.253/24</td>
<td>172.90.130.254</td>
<td>4</td>
<td>Not applicable</td>
</tr>
<tr>
<td>NFS</td>
<td>140</td>
<td>172.90.140.252/24</td>
<td>172.90.140.253/24</td>
<td>172.90.140.254</td>
<td>5</td>
<td>Not applicable</td>
</tr>
<tr>
<td>vRealize Suite (optional)</td>
<td>220</td>
<td>172.90.220.252/24</td>
<td>172.90.220.253/24</td>
<td>172.90.220.254</td>
<td>7</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Uplink01</td>
<td>230</td>
<td>172.90.230.252/24</td>
<td>172.90.230.253/24</td>
<td>172.90.230.254</td>
<td>230</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Uplink02</td>
<td>240</td>
<td>192.90.240.252/24</td>
<td>172.90.240.253/24</td>
<td>172.90.240.254</td>
<td>240</td>
<td>Not applicable</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>172.90.110.250</td>
</tr>
<tr>
<td>Component</td>
<td>S5248F-ON-Top</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>Server</td>
<td>NIC Port 1</td>
</tr>
<tr>
<td>Mgmt1</td>
<td>Ethernet 1/1/1</td>
</tr>
<tr>
<td>Mgmt2</td>
<td>Ethernet 1/2/1</td>
</tr>
<tr>
<td>Comp1</td>
<td>Ethernet 1/3/1</td>
</tr>
<tr>
<td>Comp2</td>
<td>Ethernet 1/4/1</td>
</tr>
<tr>
<td>Comp3</td>
<td>Ethernet 1/5/1</td>
</tr>
</tbody>
</table>

**Prerequisites**

You need a laptop with a serial connection and terminal emulation software such as PuTTY.

**Typographical conventions**

Configuration instructions use certain typographical conventions to designate commands and screen output.

The Courier font identifies command syntax. Information that is specific to your environment or site survey is in <> 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 that 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 in **bold** type. Optional commands are in *italicized bold* type.

**Configuring Dell EMC PowerSwitch S5248F-ON switches**

This section describes a minimal configuration for your Dell EMC PowerSwitch S5248F-ON switches to support Ready Stack. Additional configuration might be necessary for your environment and to configure communication to your core data center network.

If you are not familiar with configuring the Dell EMC PowerSwitch S5248F-ON switch, see [Support for PowerSwitch S5248F-ON](https://www.dell.com) on Dell EMC Online Support.
Perform the following tasks on each of the S5248F-ON switches:

1. Using the RJ45-to-serial-port cable included with your switch, connect one end of the cable 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 on the back of the switch. The console port is on the upper right near the fans and power supplies.

   ![RS-232 Console Port](image)

   ![Management Port](image)

   **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:

   ```text
   OS10# configure terminal
   ```

4. Configure the hostname and time zone, and set a username and password for EXEC mode by running the following commands:

   ```text
   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:

   ```text
   SW1(config)# ip route 0.0.0.0/0 <core network gateway>
   SW1(config)# do write memory
   ```
Chapter 4: Network Configuration

Configure the management interface

The Virtual Link Trunking interconnect (VLTi) heartbeat uses the management interface on the back of the Dell EMC PowerSwitch S5248F-ON switch. The S5248F-ON switch is connected to the S4148T-ON switch with a Cat 5e Ethernet network cable. To configure the management interface, enter 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
   SW1(conf-if-ma-1/1/1)# ip address 172.90.100.252/24
   SW2(config-if-ma-1/1/1)# no ip address dhcp
   SW2(config-if-ma-1/1/1)# ip address 172.90.100.253/24
   SW1(conf-if-ma-1/1/1)# exit

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 might cause network issues. The values that are provided here are examples only.

   SW1(config)# spanning-tree mode rstp
   SW1(config)# spanning-tree rstp priority 16384
   SW2(config)# spanning-tree mode rstp
   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 to be 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(config-if-vl-100)# ip address 172.90.100.252/24
   SW1(config-if-vl-100)# mtu 9000
   SW1(config-if-vl-100)# vrrp-group 1
   SW1(config-if-vl-100-vrid-1)# virtual-address 172.90.100.254
   SW1(config-if-vl-100-vrid-1)# exit
   SW1(config-if-vl-100)# no shutdown
   SW1(config-if-vl-100)# exit
   SW1(config)# do write
2. Configure the management VLAN:

```plaintext
SW1(config)# interface vlan 110
SW1(config-if-vl-110)# description "Management VLAN"
SW1(config-if-vl-110)# ip address 172.90.110.252/24
SW1(config-if-vl-110)# mtu 9000
SW1(config-if-vl-110)# vrrp-group 2
SW1(config-if-vlan110-vrid-2)# virtual-address 172.90.110.254
SW1(config-if-vlan110-vrid-2)# exit
SW1(config-if-vl-110)# no shutdown
SW1(config-if-vl-110)# exit
SW1(config)# do write
```

3. Configure the VM migration VLAN:

```plaintext
SW1(config)# interface vlan 120
SW1(config-if-vl-120)# description "VM migration VLAN"
SW1(config-if-vl-120)# ip address 172.90.120.252/24
SW1(config-if-vl-120)# mtu 9000
SW1(config-if-vl-120)# vrrp-group 3
SW1(config-if-vlan120-vrid-3)# virtual-address 172.90.120.254
SW1(config-if-vlan120-vrid-3)# exit
SW1(config-if-vl-120)# no shutdown
SW1(config-if-vl-120)# exit
SW1(config)# do write
```

4. Configure the vSAN VLAN:

```plaintext
SW1(config)# interface vlan 130
SW1(config-if-vl-130)# description "VM migration VLAN"
SW1(config-if-vl-130)# ip address 172.90.130.252/24
SW1(config-if-vl-130)# mtu 9000
SW1(config-if-vl-130)# vrrp-group 4
SW1(config-if-vlan130-vrid-4)# virtual-address 172.90.130.254
SW1(config-if-vlan130-vrid-4)# exit
SW1(config-if-vl-130)# no shutdown
SW1(config-if-vl-130)# exit
SW1(config)# do write
```

5. Configure the NFS VLAN:

```plaintext
SW1(config)# interface vlan 140
SW1(config-if-vl-140)# description "VI Workload NFS"
SW1(config-if-vl-140)# ip address 172.90.140.252/24
SW1(config-if-vl-140)# mtu 9000
SW1(config-if-vl-140)# vrrp-group 5
SW1(config-if-vlan140-vrid-5)# virtual-address 172.90.140.254
SW1(config-if-vlan140-vrid-5)# exit
SW1(config-if-vl-140)# no shutdown
SW1(config-if-vl-140)# exit
SW1(config)# do write
```
6. Configure the VXLAN VLAN:

```plaintext
SW1(config)# interface vlan 210
SW1(conf-if-vl-210)# description "VXLAN VLAN"
SW1(conf-if-vl-210)# ip address 172.90.210.252/24
SW1(conf-if-vl-210)# mtu 9000
SW1(conf-if-vl-210)# vrrp-group 6
SW1(conf-if-vlan210-vrid-6)# virtual-address 172.90.210.254
SW1(conf-if-vlan210-vrid-6)# exit
SW1(conf-if-vl-210)# no shutdown
SW1(config)# do write
```

7. Configure the vRealize VLAN:

```plaintext
SW1(config)# interface vlan 210
SW1(conf-if-vl-210)# description "vRealize VLAN"
SW1(conf-if-vl-210)# ip address 172.90.220.252/24
SW1(conf-if-vl-210)# mtu 9000
SW1(conf-if-vl-210)# vrrp-group 7
SW1(conf-if-vlan210-vrid-7)# virtual-address 172.90.220.254
SW1(conf-if-vlan210-vrid-7)# exit
SW1(conf-if-vl-210)# no shutdown
SW1(config)# do write
```

8. To verify that all the settings have been recorded, review the configuration from enable mode by running the following command:

```plaintext
SW1# show running-config
```

9. Repeat the preceding steps to configure the bottom S5248F-ON switch in the configuration.

Configure the VLTi ports

Configure the ports to be used for VLTi traffic on each switch:

1. Run the following commands:

```plaintext
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:

```plaintext
SW1(config)# vlt-domain 1
SW1(conf-vlt-1)# backup destination 192.168.1.253
SW1(conf-vlt-1)# backup destination 192.168.1.252
SW1(conf-vlt-1)# discovery-interface ethernet 1/1/53-1/1/54
SW1(config)# 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 is displayed:

```
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 9000
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 110,120,130,140,210,220
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 is as follows:

```
interface ethernet1/1/1
   no shutdown
   switchport mode trunk
   switchport access vlan 100
   switchport trunk allowed vlan 110,120,130,140,210,220
   mtu 9000
   flowcontrol receive off
   spanning-tree guard root
   spanning-tree port type edge
```

...
Chapter 4: Network Configuration

Configure the port channel

The Dell EMC PowerSwitch S4148T-ON switch connects to the network through the S5248F-ON switches using a port channel consisting of one interface on each S5248F-ON switch. Configure the port channel and port:

1. Configure the port channel by running the following commands:

   `SW1(config)# interface port-channel 101`
   `SW1(conf-if-po-101)# description “OOB uplink”`
   `SW1(conf-if-po-101)# no shutdown`
   `SW1(conf-if-po-101)# switchport mode trunk`
   `SW1(conf-if-po-101)# switchport trunk allowed vlan 100,110,120,130,140,210,220`
   `SW1(conf-if-po-101)# mtu 9000`
   `SW1(conf-if-po-101)# vlt-port-channel 101`
   `SW1(conf-if-po-101)# exit`

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

   `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)# description “OOB uplink”`
   `SW1(conf-if-eth1/1/48:1)# channel-group 101 mode active`
   `SW1(conf-if-eth1/1/48:1)# mtu 9000`
   `SW1(conf-if-eth1/1/48:1)# exit`

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

Configuring the Dell EMC PowerSwitch S4148T-ON switch

The S4148T-ON switch serves as the OOB management switch for the Ready Stack. You can use a single switch because this connectivity is not considered critical for workload operations.

Configure the S4148T-ON switch

Configure the Dell EMC PowerSwitch S4148T-ON switch:

1. Using the RJ45-to-serial-port cable included with your switch, connect one end of the cable to your workstation and the other end to the RS-232 console port of the switch, as shown in the following figure:

   ![Figure 4. Serial port](image-url)
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 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 S4148T-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 9000
   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 recorded, review the configuration by running the following command from enable mode:
   ```
   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 9000

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 9000
   flowcontrol receive on
   spanning-tree port type edge
   

Configure the port channel

The Dell EMC PowerSwitch S4148T-ON switch connects to the network through the Dell EMC PowerSwitch S5248F-ON VLT domain using a port channel consisting of two 10 GbE ports on the S4148T-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 9000
   SWOOB(conf-if-vl-100)# exit
   SWOOB(config)# do write

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 9000
   SWOOB(conf-if-po-101)# exit
Chapter 4: Network Configuration

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 9000
   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) Eth 1/1/50 (Up)</td>
</tr>
</tbody>
</table>

Preparation switches for NSX Edge routing

The S5248F-ON switches must be configured to allow north/south NSX VXLAN traffic to be routed to the core network. Dell EMC recommends deploying the switching fabric in a traditional leaf/spine architecture, with the S5248F-ON (leaf) switches connecting to upstream Z9264-F-ON (spine) switches, which then connect to the core data center fabric. Optionally, you can connect the S5248F-ON switches directly to core data center fabric.

VMware NSX Edge Services Gateways (ESGs) are specialized virtual machines that provide networking services such as gateway routing to VXLAN overlay networks. The ESGs connect to the leaf/spine switches to enable processing of VXLAN north/south traffic. Two VLANs (uplink01, and uplink02) connect the ESGs, and Border Gateway Protocol (BGP) is used to exchange routing information. These VLANs are only configured on leaf switches that are connected to hosts where the ESGs are configured to run. One VLAN is configured on each leaf switch, and redundancy is provided by having an ESG peer for each IP address.

Note: In larger configurations, create VMware host affinity rules to ensure that the ESG VMs are always confined to physical hosts that are connected to configured leaf switches.

For detailed ESG configuration details, which are outside the scope of this document, see Deploy NSX Edges in Cloud Foundation Version 3.7.1.
The following steps detail how to configure the S5248F-ON switches with the hostnames SW1 and SW2:

1. Create VLAN 2711 and assign an IP address:

```
SW1(config)# interface vlan2711
SW1(config-if-vl-2711)# description esg-uplink01
SW1(config-if-vl-2711)# no shutdown
SW1(config-if-vl-2711)# mtu 9216
SW1(config-if-vl-2711)# ip address 172.90.230.1/24
SW1(config-if-vl-2711)# exit
```

2. Configure the management node ports as VLAN members for the two uplink VLANs:

```
SW1(config)# interface range ethernet1/1/17-1/1/18
SW1(conf-range-eth1/1/17-1/1/18)# switchport trunk allowed vlan 230-240
SW1(conf-range-eth1/1/17-1/1/18)# exit
```

3. Configure eBGP for peering with the ESGs:

```
SW1(config)# router bgp 65101
SW1(config-router-bgp-65101)# neighbor 172.90.230.2
SW1(config-router-neighbor)# advertisement-interval 5
SW1(config-router-neighbor)# bfd
SW1(config-router-neighbor)# fall-over
SW1(config-router-neighbor)# password <bgp-password>
SW1(config-router-neighbor)# remote-as 65003
SW1(config-router-neighbor)# no shutdown
SW1(config-router-neighbor)# exit
SW1(config-router-bgp-65101)# neighbor 172.90.230.3
SW1(config-router-neighbor)# advertisement-interval 5
SW1(config-router-neighbor)# bfd
SW1(config-router-neighbor)# fall-over
SW1(config-router-neighbor)# password <bgp-password>
SW1(config-router-neighbor)# remote-as 65003
SW1(config-router-neighbor)# no shutdown
SW1(config-router-neighbor)# end
```

4. Update the existing route map:

```
SW1(config)# ip prefix-list spine-leaf seq 60 permit 172.90.230.0/24
SW1(config)# ip prefix-list spine-leaf seq 70 permit 172.27.240.0/24
```

Note: Add other networks to the IP prefix list based on the tenant workload networks that are used in the environment.
Verify peering and BGP

The NSX Edge devices must establish a connection to each of the leaf switches before BGP updates can be exchanged. Confirm the successful peering of the NSX Edge devices and confirm that BGP routing has been established: From switch SW1, run the `show ip bgp summary` command to show a summary of the neighbor adjacencies.

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.
- S4148T-ON switch is configured.
- S4148T-ON switch is connected to the S5248F-ON switches.
This chapter presents the following topics:

**Introduction** ....................................................................................................... 31
**Deploying Unity XT x80 storage** ....................................................................... 31
**Deploying Connectrix DS-6620B switches** ...................................................... 33
**Site survey example: FC port mappings** ......................................................... 33
**Zoning host servers to storage controllers** ..................................................... 34
**Adding cluster hosts to the storage array** ....................................................... 36
**Creating a LUN** .................................................................................................. 37
Introduction

The VMware Cloud Foundation software-defined data center (SDDC) architecture uses vSAN for management domain storage. However, workload domain storage can be implemented using vSAN or NFS (file) and supports auxiliary storage using block protocols. In this deployment, we use FC storage that is backed by the Unity XT x80 Series all-flash array as auxiliary storage. The FC storage complements the NFS storage, which is provisioned later and is also backed by the Unity XT x80.

Note: Although the design guide for this Ready Stack depicts Unity storage and this deployment guide depicts the latest Unity XT storage, the setup and deployment procedures in this guide are applicable to both Unity and Unity XT storage arrays.

Also, while vSAN and NFS storage can be managed from within the SDDC Manager interface, all FC datastores must be managed independently from the workload-domain VMware vCenter instance.

Note: Present only FC datastores to workload domains. Presenting FC datastores to the management domain is not supported.

This chapter describes the procedures for deploying and configuring the Unity XT x80 storage array to support the workload domain. It assumes that all storage equipment has been powered and connected to the appropriate networks. For enclosure cabling guidelines, see the Dell EMC Unity All Flash and Unity Hybrid Installation Guide or consult with your Dell EMC Sales representative.

Note: Preprovision virtual infrastructure (VI) workload domain storage before bringing up VMware Cloud Foundation.

Deploying Unity XT x80 storage

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

Deploy the Unity XT x80 storage:

1. Connect the Unity XT x80 system to the network.

   The management IP address for the Unity XT x80 system can be assigned dynamically or statically:

   - **Dynamic**—If your network supports DHCP, the Unity XT x80 system automatically obtains a network address when you power on the system.

   - **Static**—If you are not running the storage system in a network that supports DHCP or if you prefer to assign a static IP address manually, you must install and run the Connection Utility on the Microsoft Windows based computer.

2. Connect to Dell EMC Unisphere storage management:

   a. Launch a web browser and enter the management IP address as the destination.
b. 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 do so, open the Settings page, and click the gear icon in the upper left.

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

Unity XT x80 arrays can communicate with the Customer Support Center through a network connection to the Secure Remote Services gateway.

Two remote service options are available by which to send storage system information to Dell EMC for remote troubleshooting:

- Integrated Secure Remote Services (physical deployments only)
- Centralized Secure Remote Services Virtual Edition (VE)

Integrated Secure Remote Services runs directly on the storage system. When you select this option, you set up the storage system to use a secure connection between the system and Dell EMC servers. You can choose either:

- Two-way connectivity (the default) from Unity XT x80 to Dell EMC and from Dell EMC to Unity XT x80 for remote access
- One-way connectivity from Unity XT x80 to Dell EMC through HTTP

Centralized Secure Remote Services VE runs on a gateway server. When you select this option, you add the storage system to other storage systems in a Secure Remote Services cluster. The cluster resides behind a single common (centralized) secure connection between Dell EMC servers and an external Secure Remote Services gateway. The gateway is the single point of entry and exit for all IP-based Dell EMC remote support activities for the storage systems that are associated with the gateway.

For setup procedures, see Dell EMC Unity Family Technical Documentation.
Deploying Connectrix DS-6620B switches

Before deploying the FC switches, connect all power cables and management cables. For cabling guidelines for the storage array and hosts, see Connectrix DS-6620B on Dell EMC Online Support.

To deploy the Connectrix DS-6620B 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 by 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 subnet mask 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>
</tbody>
</table>
Zoning host servers to storage controllers

Zone the 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.

   b. In the Create New Alias dialog box, enter a name for the new alias—Unity_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 Unity XT x80 system in Unisphere storage management.

![Figure 5. Unity XT x80 ports with WWNs](image)

4. Create aliases for the WWNs of the compute hosts:
   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—**CMPT_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.

   ![Figure 5. Unity XT x80 ports with WWNs](image)

f. Repeat the preceding steps to create aliases for all compute host 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**.
   c. In the **Create New Zone** dialog box, enter a name for the new zone, and click **OK**.
   d. Under **Member Selection List**, expand **Aliases** to view the nested elements.
Select all aliases of the Unity XT x80 storage ports and the alias of the server WWN to be included in the zone.

6. Enable configuration:
   a. Click the Zone Config tab.
   b. Under Member Selection List, expand Zones to view the nested elements.
   c. Select all the zones that you created for the compute hosts.
   d. Click the right arrow to move the selected zones in Member Selection List to Zone Config Members.
   e. Click Save Config.
      This process takes a few seconds.
   f. Click Enable Config and select the name of the zone configuration.
   g. 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:

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

      The port WWNs are displayed, as shown in the following figure:

      ![Figure 6. WWN in ESXi shell](image)

2. Log in to Unisphere storage management.
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 compute servers to be added to the storage array.

Creating a LUN

This procedure describes how to create LUNs and present them to the compute cluster. The LUNs are used as datastores for compute cluster VMs. You can also use this procedure to create additional LUNs for the compute cluster.

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. In the upper left of the LUNs pane, click the plus sign (+).
   The Create LUNs wizard opens.

5. On the Configure LUN(s) page:
   a. In the Number of LUNs field, select 1, or select another number if you want to create multiple LUNs with the same properties.
   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.
   e. To create a thin LUN, select Thin.
      If Thin is not selected, a thick LUN is created.
   f. 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 compute hosts that require access to the LUN, and then click OK.

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 to be created automatically, and then click Obtain the HBA's WWNs.
10. On the Replication page, if configuration is 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 you require additional LUNs with unique properties for the VI workload domain, repeat steps 4 through 12 to create the LUNs and assign them to hosts.

You can also add LUNs from the Hosts Properties window.

Storage sizing for the VI workload domain is deployment-specific, based on the number of VMs being deployed and their storage I/O requirements.

For additional sizing information, see the VMware Cloud Foundation Capacity Planner.
Chapter 6 VMware Cloud Foundation Deployment

This chapter presents the following topics:

Introduction ....................................................................................................... 40
General deployment guidelines ....................................................................... 40
Installing ESXi on the management hosts ...................................................... 41
Configuring the ESXi management network ................................................... 44
Installing VMware Cloud Foundation Builder ................................................. 47
Completing the deployment parameter sheet ................................................. 48
Creating the management domain ................................................................... 49
Introduction

The deployment process for VMware Cloud Foundation greatly simplifies the complex process of standing up an end-to-end software-defined data center (SDDC) environment. VMware Cloud Foundation uses a structured stand-up process that provides the following features and services:

- An imaging platform that can be used for initial and subsequent deployment of all VMware Cloud Foundation component software, including management and workload domains
- A configuration process that captures all required environment settings
- A validation process that validates configuration data before attempting deployment
- Deployment tooling, automation, logging, and troubleshooting
- Post-installation management and configuration through the SDDC Manager tool

While VMware Cloud Foundation abstracts much of the installation and integration of the various underlying SDDC components, you must still invest significant time, thought, and effort into the predeployment and planning processes; these areas are critical to a successful VMware Cloud Foundation deployment.

While a detailed walkthrough of a VMware Cloud Foundation deployment is outside the scope of this document, this chapter covers the high-level procedural steps for deploying VMware Cloud Foundation on Ready Stack.

While Ready Stack supports both the standard and consolidated VMware Cloud Foundation architecture models, this deployment is based on the former. If you do not require discrete isolation of management and workload domains, you can choose the latter model.

For detailed VMware Cloud Foundation planning, sizing, deployment, and troubleshooting guidance, see VMware Cloud Foundation Documentation.

General deployment guidelines

Before you begin to deploy VMware Cloud Foundation, complete the following deployment configuration options:

- Identify and create within Active Directory all required service accounts with the correct roles and privileges.
- Identify and validate all networking vLANs and IP subnets. If NSX Edge gateways will be deployed for upstream routing, also identify and validate the peer autonomous system (AS) number or numbers and routing credentials.
- Identify and validate all networking services (DHCP, DNS, NTP), and ensure that they are reachable.
- Ensure that all hosts and VMware Cloud Foundation VMs are fully resolvable within DNS (forward and reverse).
Chapter 6: VMware Cloud Foundation Deployment

- Ensure that any upstream firewalls have appropriate ports open for management access to Ready Stack and VMware Cloud Foundation networks, services, and components.

- Ensure that correct licenses are available for all VMware Cloud Foundation software products.

- Ensure that signed certificates are available for all VMware Cloud Foundation software products. Never use embedded self-signed certificates in a production VMware Cloud Foundation deployment.

- For VI workload domains, configure FC storage and assign it to hosts.

- Install and configure Microsoft SQL Server 2016 if you will be deploying VMware vRealize Automation, or use an existing installation.

For details, see the VMware Cloud Foundation Planning and Preparation Guide.

Installing ESXi on the management hosts

Install VMware ESXi on the PowerEdge management hosts that will be part of the management cluster. For convenience, you can order PowerEdge servers with VMware ESXi 6.7 preinstalled; otherwise, you can install ESXi remotely through the iDRAC web interface or locally. Alternatively, you can use the VMware Imaging Appliance (VIA) that is part of the VMware Cloud Foundation Builder VM.

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.

Requirements

To complete the procedures in this section, you need:

- iDRAC IP addresses or FQDNs

- iDRAC credentials

- iDRAC Enterprise license applied on all nodes

- Dell EMC-customized ESXi 6.7 image

  For download instructions, see VMware vSphere ESXi 6.7.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

- DNS server records for hostnames

**Note:** The iDRAC User Guide provides instructions for setting up the iDRAC, including configuring the IP address.
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:
      
      ```bash
      racadm set bios.sysprofilesettings.WorkloadProfile VtOptimizedProfile
      ```
   d. Run the following command to process the change:
      
      ```bash
      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.
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 6.7, 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 is displayed.

---

**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 that you have mapped will be available throughout the 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

Install ESXi on the management cluster:

1. In the iDRAC Virtual Console, at the **Welcome to the VMware ESXi 6.7 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 is displayed:

   ![ESXi Found message]

   **Figure 8. ESXi Found message**

   4. If the **ESXi Found** message is displayed:
      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 6.7.
   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 (DCUI).
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 14 of the site survey.
12. Press Enter.
13. Select DNS Configuration and press Enter.
14. Enter the IP address of the DNS servers and the FQDN of the host. See Table 10 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.
Chapter 6: VMware Cloud Foundation Deployment

Test 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:

   ![Test Management Network](image)

   **Figure 9. Test Management Network**

2. Press Enter to continue.

   When the test is complete, results that are similar to those in the following figure are displayed:

   ![Test network results](image)

   **Figure 10. Test network results**

Configuration settings specific to VMware Cloud Foundation

VMware Cloud Foundation requires the following ESXi configuration:

- Enable TSM-SSH service and set the policy to **Start and Stop with Host**.
- Enable and configure NTP service and set the policy to **Start and Stop with Host**.

Numerous methods exist for setting TSM-SSH service policy and NTP settings. For information, see the following VMware Knowledge Base articles:

- [Enabling or disabling Lockdown mode on an ESXi host](https://kb.vmware.com/s/article/1008077) (1008077)
- [Configuring Network Time Protocol (NTP) on an ESXi host using the vSphere Web Client](https://kb.vmware.com/s/article/57147) (57147)
Installing VMware Cloud Foundation Builder

The VMware Cloud Foundation Builder VM provides VMware Cloud Foundation staging, imaging, configuration, and deployment services. It is responsible for the entire SDDC bring-up process. Installation of this component is the first of a multistep bring-up process for VMware Cloud Foundation.

Although VMware Cloud Foundation Builder includes VIA, we do not use it because we have installed ESXi remotely through the iDRAC.

VMware Cloud Foundation Builder does require a host outside of the Ready Stack environment to perform the VMware Cloud Foundation bring-up process. You can perform the process on a laptop running VMware Workstation or VMware Fusion, or on an ESXi host. The VMware Cloud Foundation Builder VM must have network access to all hosts on the management network. Deployment of the VMware Cloud Foundation Builder VM requires approximately 350 GB of storage.

For this deployment guide, we installed VMware Cloud Foundation Builder on a PowerEdge R640 server that was connected to S5248F-ON switches and running ESXi 6.7.

To install the VMware Cloud Foundation Builder VM:

1. Download the VMware Cloud Foundation Builder OVA to a network location that is accessible to the ESXi host.
   
   You must have an authorized VMware account to access the download file.

2. Log in to the ESXi host with the VMware Host Client, and deploy the OVA using the default options.

3. In the Select Networks dialog box, select the port group that is associated with the VLAN ID that is used by the ESXi hosts where VMware Cloud Foundation will be deployed.

4. Enter the configuration that is specific to your environment.
   
   Do not change the Default Deployment Architecture (vcf).

5. Connect to the VM through SSH, using the administrator credentials that you specified during the ESXi installation, and verify:
   
   - Network connectivity to all network services such as NTP, DHCP, and so on
   - Network connectivity to Ready Stack management hosts
   - Forward and reverse DNS lookups of the Ready Stack management hosts

>Note: DNS configuration errors are one of the leading causes of VMware Cloud Foundation deployment failures.
Completing the deployment parameter sheet

The deployment parameter sheet is an XLS file that contains all the configuration details that are required to install the components of the VMware Cloud Foundation stack. The XLS file is later converted to JSON and used as a configuration source for the bring-up process.

To download the deployment parameter spreadsheet:

2. On the VMware Cloud Foundation page, enter the administrator credentials that you provided when you deployed the VMware Cloud Foundation Builder VM.
3. Verify that the environment meets the criteria in the pre-bring-up checklist and select the check boxes. Correct any issues before proceeding.
4. Accept the End-User License Agreement, and then click Download Deployment Parameter Sheet.

The deployment parameter spreadsheet contains important configuration data that is necessary for installing and configuring all the interconnected VMware Cloud Foundation components. While you can obtain many of the core parameters from Appendix A: Site Survey Site Survey, numerous other configuration settings are required. An exhaustive explanation of all required input parameters is out of scope for this document. For detailed guidance about populating the deployment parameter spreadsheet, see the Cloud Builder Deployment Parameter Guide (requires My VMware account credentials).

The deployment parameter guide also provides basic sizing guidance for your environment. Ensure that you have all the required environment information including:

- Host and VM names (FQDN, and short names)
- Host and VM IP addresses, subnet masks, and gateways
- Host security thumbprints (if required)
- Networking information including CIDR, VLAN, inclusion ranges, and so on
- Service accounts and credential information
- VMware Cloud Foundation product license keys
- Infrastructure details that were specified previously (NTP, DNS, and so on)
Creating the management domain

After the deployment parameter sheet configuration details have been populated, the next step is to create the management domain through the bring-up process. During this phase, the deployment parameter spreadsheet is uploaded to VMware Cloud Foundation Builder, where it is converted to JSON and validated. If errors are found, they must be corrected before configuration can begin.

Upload and validate the parameter spreadsheet to initiate the bring-up process and create the management domain as follows:

1. Log in to the VMware Cloud Foundation Builder VM with your administrator credentials by navigating to https://<Cloud_Builder_VM_IP>.
2. Click Upload Config File, select the completed parameter spreadsheet, and click Upload.
3. After the file is uploaded, click Validate to validate the uploaded file.
   Any errors prevent the bring-up process from starting. Correct any errors by clicking Re-try or by updating the deployment parameter spreadsheet and uploading it again.
4. Acknowledge any warning messages, and then click Next.
5. Click Begin Bring-up.
   After the bring-up process is initiated, the management domain is created with all required components: SDDC Manager, vCenter servers, and the NSX Manager and NSX Controllers.
6. Click the link that is provided for SDDC Manager and review the management domain details for accuracy.
7. Log in to vCenter Server and verify the health status and configuration details of the management cluster, vSAN cluster, and deployed VMs.
8. Optionally, power off and remove the VMware Cloud Foundation Builder VM.
This chapter presents the following topics:

**Prerequisites** ..................................................................................................................51
**Installing ESXi on the compute hosts** .................................................................51
**Configuring the ESXi management network on the compute cluster** ..........53
**Configuring NFS resources in SDDC Manager** ..............................................53
**Configuring NFS on Unity XT x80** .................................................................55
**Deploying the VI workload domain** .................................................................56
**Creating VI workload domain datastores** ..................................................57
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 6.7 image
  
  For download instructions, see [VMware vSphere ESXi 6.7.x on Dell EMC PowerEdge Systems Image Customization Information](https://www.dell.com/support) on Dell EMC Online Support. Make a note of the image location on your system because you will need it to mount virtual media.
- Hostnames, management VLAN ID, and IP address information
- vSphere credentials
- Static IP addresses for each of the management servers
- DNS server records for hostnames (forward and reverse)

**Note:** The [iDRAC User Guide](https://www.dell.com/support) provides instructions for setting up the iDRAC, including configuring the IP address. For a link to the guide, see the [iDRAC page](https://www.dell.com/support) 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 remote installation.

**Caution:** When you upgrade VMware ESXi hosts within the VMware Cloud Foundation VI workload domain, hosts requiring custom FC vSphere Installation Bundles (VIBs) might be overwritten, potentially causing an outage. For more information, see the VMware KB article [How to upgrade ESXi hosts in VMware Cloud Foundation 3.5 with a vendor-specific ISO image](https://kb.vmware.com/s/article/65047).

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, and then log in.

      The default credentials are:
      
      - **User**—root
      - **Password**—calvin
Chapter 7: Compute Cluster Deployment

b. At the /admin1-> prompt, run the following command:
   
   racadm set bios.sysprofilesettings.WorkloadProfile VtOptimizedProfile

c. Create a job for processing the change by running the following command:
   
   racadm jobqueue create BIOS.Setup.1-1

d. Reboot the compute host.

e. 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
   - 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 6.7.

7. Click Browse to go to the location of the Dell EMC ISO file for VMware ESXi 6.7, select the file, and then 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 44.
Configuring the ESXi management network on the compute cluster

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

1. Follow the steps in Configure the management network on page 45.
2. Follow the steps in Test the management network on page 46.

Configuring NFS resources in SDDC Manager

To be provisioned through SDDC Manager, the VI workload domains require file-backed (NFS or vSAN) primary storage. Secondary storage can be NFS or block storage, but it is not managed through SDDC Manager. In this section, we configure the Unity XT x80 NFS services, which SDDC Manager uses during the VI workload domain bring-up process. We also describe how to configure vSAN, which may be used if you are deploying Dell EMC vSAN Ready Nodes as VI workload domain hosts. The following figure details the storage configuration that is used in this guide, along with an optional second workload domain:

In SDDC Manager, create an IP resource pool for NFS or vSAN:

1. In a browser, enter one of the following URLs:
   - https://<FQDN>, where <FQDN> is the hostname of SDDC Manager
   - https://<IP_address>, where <IP_address> is the IP address of SDDC Manager
2. Log in as user vcf, using the password that you provided on the deployment parameter spreadsheet before beginning the bring-up process.

3. From the SDDC Manager Dashboard, in the left pane, expand Administration, and then select Network Settings.

4. In the upper right, click Create Network Pool.

5. Create the network pool:
   a. At Network Pool Name, specify a pool name.
   b. At Network Type, select NFS or vSAN.
   c. Under NFS Network Information or vSAN Network Information, enter the IP storage network information.
   d. Click Save.
   e. If configuring NFS, record the Included IP Address Ranges, as shown in the following figure.

You will need this information when you assign host access permissions on the Unity XT x80 NFS share.

![SDDC Manager NFS network pool](image)

Figure 12. SDDC Manager NFS network pool

f. If configuring vSAN, skip to Deploying the VI workload domain.
Chapter 7: Compute Cluster Deployment

Configuring NFS on Unity XT x80

After you configure the IP resources in SDDC Manager, configure NFS resources on the Unity XT x80 storage array. SDDC Manager consumes the NFS resources during the workload domain bring-up process. First configure the NAS server and then create the NFS share.

Configure the NAS server

The NAS server manages file resources on the Unity XT x80. To create the NAS server, follow these steps:

1. In the Unity Unisphere UI:
   a. Under Storage, click File.
   b. Click NAS Servers, and then click the plus sign (+).

2. Continue through the wizard, specifying the settings that are unique to your environment, and pay attention to the following items:
   - On the Interface page, specify an IP address within the VLAN of the NFS network pool that you created earlier in SDDC Manager, as shown in the following figure:

   ![Figure 13. Configuring the NAS server address](image)


Configure the shared file system

Create the shared file system as follows:

1. In the Unity Unisphere UI, click File Systems and click the plus sign (+).

2. On the Protocol page, select Linux/Unix Shares (NFS), select the NAS Server that you previously created, and then click Next.

3. Specify the options for Name and click Next.
4. On the Shares page, select **NFS Share (Linux/Unix)**, specify a share name, and then click **Next**.

Make note of the NFS share path for later use in configuring the NFS share from within SDDC Manager.

5. On the Access page:
   a. Set Default Access to Read/Write, allow Root.
   b. Click the plus sign (+) to configure access.
   c. Under **Configure Access**, at **customize access for the following hosts**, add the IP addresses that you previously assigned to the NFS network pool in **Create the IP resource pool**.

6. Continue with the wizard and specify the options for the **Snapshot** and **Replication** pages.

7. At the Summary page, click **Finish**.

---

### Deploying the VI workload domain

After you create both the NFS and FC storage resources on the Unity XT x80 system, deploy the VI workload domain. If you are using vSAN, only the FC storage resources on the Unity XT 80 are used.

Deploy the VI workload domain as follows:

1. On the SDDC Manager Dashboard, click **+ Workload Domain**, and then click **VI – Virtual Infrastructure**.
2. Under **Storage Selection**, select **NFS** or **vSAN**, and then click **Next**.
3. When the **VI Configuration** wizard begins, enter the environment-specific details on the **Name, Compute**, and **NSX** pages.
4. On the **NFS Storage** page, enter the NFS share path that you specified in **Configure the shared file system**.

   For vSAN, on the **vSAN Storage** page, specify the level of availability required. A value of 1 is the recommended minimum.

5. Continue with the wizard to specify details for the **Hosts, Licenses**, and **Object Names** pages.
6. On the **Review** page, click **Finish** to begin the workload domain deployment. When the deployment is complete, SDDC Manager displays the NFS share information, as shown in the following figure:

![Figure 14. SDDC Manager summary (NFS storage)](image)

**Creating VI workload domain datastores**

After you create the NFS- or vSAN-backed VI workload domain, present the FC storage service as ancillary storage.

**Present storage to vCenter**

Present the FC storage to the VI workload domain vCenter:

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 VI workload domain cluster object, and select **Storage > Rescan storage**.
5. Right-click the VI workload domain cluster object and select **Storage > New Datastore**.
6. Complete the **New Datastore** wizard to create the datastore for the VI workload domain.
Chapter 8 Management Software and Data Protection Deployment

This chapter presents the following topics:

- **Introduction**: 59
- **Deploying OMIVV**: 59
- **vRealize Suite product deployment overview**: 69
- **Deploying vRealize Lifecycle Manager**: 69
- **Deploying vRealize Automation**: 70
- **Deploying vRealize Log Insight**: 71
- **Deploying vRealize Operations**: 72
- **Connecting vRealize Suite to workload domains**: 73
- **Enabling vRealize Log Insight connection to workload domains**: 74
- **Deploying ESA**: 74
- **Deploying VSI**: 75
- **Deploying IDPA**: 77
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 see the relevant product documentation for detailed deployment instructions and to review advanced configuration options.

Deploying OMIVV

OMIVV is a virtual appliance that is designed to streamline the management processes in your data center environment. It enables 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</td>
</tr>
<tr>
<td>Medium</td>
<td>Up to 500</td>
<td>4</td>
<td>16</td>
<td>44</td>
</tr>
<tr>
<td>Large</td>
<td>Up to 1000</td>
<td>8</td>
<td>32</td>
<td>44</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

Install OMIVV in each VI workload domain vCenter instance by repeating the procedures in this section for each VI workload domain vCenter instance.

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 of the downloaded ZIP file and extract the contents of the file.
Deploy the OVF file

Deploy the Open Virtualization Format (OVF) file that contains the OMIVV VM 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 End User License Agreement 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 Zerored) 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. On the Setup Networks page, select the network configuration settings, and then click Next. Dell EMC recommends that the OMIVV VM and the vCenter server be on the same network—Management VLAN 110 in this example.
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

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

![OMIVV setup](image)

Figure 15. OMIVV setup

9. On the **Date and Time** tab, select **Synchronize date and time over the network**.
10. Add valid NTP server details (ideally, use the same NTP servers to which your vCenter is synchronized).
11. Click **Time Zone**, select the applicable time zone, and then click **OK**.
12. To configure a static IP address to the OMIVV appliance:
   a. Click Network Configuration.
   b. Select **Auto eth0**, and then click **Edit**.
   c. Click 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**.
13. To change the hostname of the OMIVV appliance:
   a. Click Change Hostname.
   b. Enter a valid hostname and click **Update hostname**.
14. Ensure that the OMIVV VM is restarted.
15. In a web browser, go to https://<OMIVV Appliance IP or Hostname>.

16. At the login prompt, enter the password.

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

![OMIVV Administration Console](image)

**Figure 16. OMIVV Administration Console**

**Register the management domain 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 an 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 in one of the following formats:
   - domain\user
   - domain/user
   - user@domain

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 **Administration** section of vSphere Web Client displays the OMIVV icon.
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 OMIVV in each VI workload domain vCenter instance by repeating the procedures in this section for each VI workload domain vCenter instance.
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:

![Figure 17. vSphere Web Client: Home page](image)

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**.

Create 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.
Create a connection profile as follows:

1. In the Initial Configuration Wizard, 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:

![Figure 18. Initial Configuration Wizard: Name and Credentials page](image)

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.
To download and store the host certificate and validate it during all future connections, select **Enable Certificate Check**.

Skip to step 5.

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 the **Host Root** section.
      The username is **root**, which is the default and cannot be changed.
   f. In the **Password** field, enter the password.
      The password is limited to 127 characters.
   g. In the **Verify Password** field, reenter the password.
   h. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.

5. Click **Next**.

6. In the **Connection Profile Associated Hosts** dialog box, select the hosts for the connection profile, and then click **OK**.

7. To test the connection profile, select one or more hosts and click **Test Connection**.

8. 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:

---

**Figure 19. vSphere host compliance**
3. If no hosts are listed and the page is disabled, proceed to the next section, Validate OMIVV functionality.

4. If any hosts are listed as noncompliant:
   a. Click Fix non-compliant vSphere Hosts.
   b. Review the text and click Next.
   c. Select the listed hosts, and then click Finish.
      Wait for OMIVV to process the necessary changes to the hosts.
   d. Refresh the page to confirm that there are no longer any noncompliant hosts.

Validate OMIVV functionality

Validate OMIVV functionality by running an inventory job:

1. In OMIVV, go to Monitor > Job Queue > Inventory History > Hosts Inventory.
2. In the vCenters list, select the vCenter server.
3. Click Run Now and wait for the inventory jobs to be completed.
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 > Manage Settings > Appliance 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 EMC 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**.

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

### vRealize Suite product deployment overview

You can use SDDC Manager to deploy vRealize Suite Lifecycle Manager, vRealize Operations, and vRealize Automation. You can also enable vRealize Log Insight for all VI workload domains.

**Note:** vRealize products are licensed separately from VMware Cloud Foundation.

You must deploy vRealize Suite Lifecycle Manager before you deploy vRealize Operations or vRealize Automation. SDDC Manager automates the deployment of both vRealize Automation and vRealize Operations in VMware Cloud Foundation. You can connect these deployments to your VI workload domains.

For detailed information about the requirements for installing vRealize Suite products, see the [VMware Cloud Foundation Planning and Preparation Guide](#).

For detailed installation information, see the [VMware Cloud Foundation Operations and Administration Guide](#).

### Deploying vRealize Lifecycle Manager

#### Introduction

vRealize Suite Lifecycle Manager provides complete life cycle and content management capabilities for vRealize Suite products. It helps customers accelerate time to value by automating deployment, upgrades, and configuration, while bringing DevOps principles to the management of vRealize Suite content.

#### Prerequisites

Before you install vRealize Lifecycle Manager, ensure that:

- The vRealize Lifecycle Manager installation package has been downloaded from the VMware Depot and copied to the local repository.
- The vRealize VLAN is configured on the switches and the vRealize subnet is routable to the management network.
- IP allocation and forward/reverse DNS records are prepared for the vRealize Suite Lifecycle Manager virtual appliance.

#### Deploy vRealize Lifecycle Manager

Deploy vRealize Lifecycle Manager from SDDC Manager as follows:

1. From the SDDC Manager Dashboard, select **Administration > vRealize Suite**.

   The **vRealize Suite** navigation bar is displayed. It shows the vRealize Suite products that are available for your VMware Cloud Foundation system deployment.

2. Click **vRealize Suite Lifecycle Manager**.
3. Click **Deploy**.

The **vRealize Lifecycle Manager Installation Prerequisites** page displays the prerequisites for the installation.

4. Review the prerequisites and select each checkbox to confirm that the prerequisite has been met.

5. Click **Begin** to launch the vRealize Lifecycle Manager Installation wizard.

6. On the **Network Settings** page, enter a valid VLAN ID, subnet mask, and gateway address.

7. Click **Next**.

8. On the **Virtual Appliance Settings** page, enter the following information:
   - FQDN of the vRealize Suite Lifecycle Manager virtual appliance
   - Password for the System Administrator account
   - Password for the Root account

9. Click **Next**.

10. On the **Review Summary** page, review the installation configuration settings.

11. Click **Finish**.

   SDDC Manager validates the inputs and reports any errors or warnings.

12. Address any validation issues, and then click **Finish**.

   A message indicates that the deployment is in progress.

   If the deployment fails, the page displays a deployment status of **Failed**. Click **Restart Task** or **Uninstall**.

   To view the details of the deployment in progress or a deployment failure, click **View Status in Tasks**. The **Tasks** panel opens at the bottom page. Open individual tasks to view details.

After the successful deployment of vRealize Suite Lifecycle Manager, you can open the UI by clicking the vRealize Suite Lifecycle Manager link below the page title. The vRealize Suite Lifecycle Manager UI opens in a new browser tab.

**Deploying vRealize Automation**

**Introduction**

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.

**Prerequisites**

Before deploying vRealize Automation for use with VMware Cloud Foundation, install a license and ensure that all additional prerequisites, as described in this section, are met.
Install vRealize Automation license

Before deploying vRealize Automation for use with VMware Cloud Foundation, add a license:

1. From the SDDC Manager Dashboard, select **Administration > Licensing**.
2. Click **+ License Key**.
3. Select **VMware vRealize Automation** as the product name.
4. Enter the license key.
   
   You can enter a license key for either vRealize Automation or a suite license for a product that includes vRealize Automation—vCloud Suite or vRealize Suite, for example.

5. Enter a description for the license.
   
   If you have multiple license keys for a product, the description helps to identify the license.

6. Click **Add**.

Additional prerequisites

Before you install vRealize Automation, ensure that the following prerequisites are met:

- You have downloaded the vRealize Suite bundles from the VMware Depot.
- IP allocation and forward/reverse DNS records are prepared for the vRealize Automation components.
- You have created the required Active Directory service account for vRealize Automation.
- You have configured a certificate authority in SDDC Manager.
- The multi-SAN certificate and private key, generated by a trusted Certificate Authority, are available for vRealize Automation.
- Microsoft SQL Server is properly deployed and configured for vRealize Automation.
- You have created and exported a Microsoft Windows Server OVA template for the vRealize Automation IaaS components.

Deploy vRealize Automation

As with vRealize Lifecycle Manager, deploy vRealize Automation in VMware Cloud Foundation by using SDDC Manager. For detailed installation procedures, see the *VMware Cloud Foundation Operations and Administration Guide*.

Deploying vRealize Log Insight

**Introduction**

vRealize Log Insight provides scalable log management with native vSphere support and third-party extensibility. Its intuitive UI enables simple interactive searches and deep analytical queries.

During VMware Cloud Foundation bring-up, SDDC Manager deploys and configures the vRealize Log Insight virtual appliance. From your deployed vRealize Log Insight instance,
you can view and analyze logs to help with diagnostics, troubleshooting, and trend analysis.

The bring-up process also installs and configures content packs in the vRealize Log Insight instance. Content packs provide dashboards, extracted fields, predefined queries, and alerts that are related to the content pack’s product or set of logs. When you launch the vRealize Log Insight Web interface, the installed content packs are ready for use.

vRealize Log Insight content packs are available on the VMware Solutions Exchange.

Access vRealize Log Insight

Access vRealize Log Insight as follows.

Caution: Do not change the password of the admin account within the vRealize Log Insight Web interface. Unpredictable results can occur.

1. From the SDDC Manager Dashboard, open the vRealize Log Insight Web interface.
2. If the vRealize Log Insight login screen is displayed, log in with the appropriate credentials:
   - If you are using an account that was set up for you in vRealize Log Insight, use those credentials to log in.
   - If you are launching the interface for the first time after the initial bring-up process, use the username admin and the randomized password that was set when the passwords were rotated at the end of the bring-up process. Then use the vRealize Log Insight Web interface to assign permissions to your superuser account and other user accounts.

Deploying vRealize Operations

Introduction

vRealize Operations provides end-to-end visibility across physical, virtual, and cloud infrastructures, enabling comprehensive IT operations management. vRealize Operations enables you to automate key processes and improve efficiency based on real-time events.

Prerequisites

Before deploying vRealize Operations for use with VMware Cloud Foundation, install a license and ensure that all additional prerequisites, as described in this section, are met.

Install the vRealize Operations license

1. From the SDDC Manager Dashboard, go to Administration > Licensing.
2. Click + License Key.
3. Select VMware vRealize Operations as the product name.
4. Enter the license key.

The license key can be for vRealize Operations or a suite license for a product that includes vRealize Operations—vCloud Suite or vRealize Suite, for example.
Chapter 8: Management Software and Data Protection Deployment

5. Enter a description for the license.
   If you have multiple license keys for a product, the description helps to identify the license.

6. Click Add.

Additional prerequisites
Before deploying vRealize Operations, ensure that the following prerequisites are met:

- You have downloaded the vRealize Suite bundles from the VMware Depot. The bundle is obtained separately from the VMware Cloud Foundation installation download.
- IP allocation and forward/reverse DNS records are prepared for the vRealize Operations components.
- You have determined the size of the vRealize Operations deployment to provide enough resources to accommodate the analytics operations for monitoring the expected number of workloads and SDDC management packs in the VMware Cloud Foundation system. For more information, see the Introducing the vRealize Operations Sizing Tool.

Deploy vRealize Operations
vRealize Operations is deployed from SDDC Manager. For detailed installation guidance, see the VMware Cloud Foundation Operations and Administration Guide.

Connecting vRealize Suite to workload domains

Introduction
You can use the SDDC Manager UI to connect workload domains to vRealize Operations and vRealize Automation product deployments in VMware Cloud Foundation.

Note: VMware Cloud Foundation does not support vRealize Automation or vRealize Operations for NSX-T workload domains. Only NSX for vSphere workload domains are supported.

Connect vRealize Suite to a workload domain
Connect vRealize Suite products to a workload domain as follows.

Note: If you enable a connection between vRealize Automation and a workload domain, and then complete the Connect to Workload Domains wizard, you cannot disable the connection.

1. From the SDDC Manager Dashboard, go to Inventory > Workload Domains.
   The Workload Domains page displays information for all workload domains.

2. Click the Security tab.

3. Click Connect to vRealize Products.
   The Connect to vRealize Products wizard opens to the Modify Connection page. This page lists all currently configured workload domains and enables you to connect workload domains to your vRealize Operations and vRealize Automation deployments.

4. Select Enable for the desired workload domain.
5. If prompted, provide the Active Directory credentials that you used during the deployment of vRealize Automation, and then click Next.

6. Review the connection and click Finish.

### Enabling vRealize Log Insight connection to workload domains

**Introduction**
You can connect vRealize Log Insight in VMware Cloud Foundation to all workload domains in the SDDC Manager UI. After you have enabled the connection to vRealize Log Insight, you cannot disable it. All subsequently created workload domains are connected automatically and send logs to the vRealize Log Insight cluster.

**Enable the vRealize Log Insight connection**
You must have a valid license key for vRealize Log Insight, which is licensed separately from VMware Cloud Foundation. You can view your license in the vRealize Log Insight UI by going to Management > License.

To enable the vRealize Log Insight connection to workload domains:

1. Verify that the vRealize Log Insight cluster is online and operational.
2. From the SDDC Manager Dashboard, click Administration > vRealize Suite.
   
   The vRealize Suite navigation bar is displayed. It shows the vRealize Suite products that are available for your VMware Cloud Foundation system deployment.

3. Click vRealize Log Insight.
   
   The vRealize Log Insight page is displayed. The top portion of the page includes an Enable button, which is used to enable log collection for all workload domains. If log collection is not enabled, the Enable button is active. The lower portion of the page displays the configuration details, including load balancer hostname, node size, and node count.

4. Click Enable.
   
   After a moment, the following message is displayed:
   
   Connect Workload Domains to vRealize Log Insight in Progress

5. In Tasks, monitor the status of the Connect Workload Domains to vRealize Log Insight action.

   After the connection is successful, vRealize Log Insight collects logs from the management workload domain and all additional workload domains.

### Deploying ESA

**Introduction**
Dell EMC Enterprise Storage Analytics (ESA) 4.6 for vRealize Operations is a management pack for VMware vRealize Operations 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.
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 Enterprise Storage Analytics for vRealize Operations on 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 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 is included in the list of installed solutions.

After ESA has been installed, configure it for vCenter and for the Unity XT x80 array, as described in the documentation at Enterprise Storage Analytics for vRealize Operations on Dell EMC Online Support.

**Deploying VSI**

**Introduction**

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 virtual appliance:

1. Download the current VSI for VMware vSphere Client OVA from Dell EMC Online Support.
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 is displayed:
   
   This site is using the VMware Client integration Plug-In. Do you want to allow it to access your operating system?

5. Click **Allow** to launch the Deploy OVF Template wizard.

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, 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 data center 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
   ```

**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 to send notifications

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 Dell EMC VSI is listed.

**Deploying IDPA**

IDPA DP4400 is a converged virtual appliance that combines backup, replication, deduplication, search, analytics, and instant access and restore capabilities. It also provides for disaster recovery and long-term data 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 for 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 Guide*. 
Chapter 9: References

This chapter presents the following topics:

- Dell EMC documentation ................................................................. 79
- VMware documentation ................................................................. 79
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.

- Ready Stack Info Hub
- Dell EMC Ready Stack: VMware Cloud Foundation on PowerEdge Servers and Unity Storage Design Guide
- Dell EMC PowerEdge R640 Installation and Service Manual
- Dell EMC PowerEdge R740 Installation and Service Manual
- Integrated Dell Remote Access Controller 9 User Guide
- Knowledge Base: iDRAC9
- Dell EMC Unity XT All-Flash Unified Storage
- OS10 Enterprise Edition User Guide
- PowerSwitch S4148T-ON: Manuals & documents
- PowerSwitch S5248F-ON: Manuals & documents
- Connectrix DS-6620B: Documentation
- Dell EMC Virtual Storage Integrator (VSI) for VMware vSphere Client Product Guide
- OpenManage Integration for VMware vCenter Knowledge Base
- Dell EMC Integrated Data Protection Appliance 2.4: Getting Started
- Enterprise Storage Analytics 4.6 product documentation
- Dell EMC Unity: Dynamic Pools White Paper
- Dell EMC Storage with VMware Cloud Foundation
- Dell EMC vSAN Ready Nodes
- Dell EMC Validated System for Virtualization - NSX Reference Architecture
- VCF on VxRail multirack deployment using BGP EVPN

VMware documentation

The following VMware resources provide additional and relevant information:

- VMware vSphere 6.7 Documentation Center
- VMware Cloud Foundation Documentation Center
- Installing and Upgrading vRealize Automation 7.6
- Getting Started: vRealize Log Insight 4.7
- Dell - IDRAC Content Pack for VMware Log Insight
- vRealize Operations Manager vApp Deployment Guide
- vRealize Operations Manager Configuration Guide
Appendix A Site Survey

This appendix presents the following topic:

Site survey tables...........................................................................................................81
Site survey tables

Before you begin the Ready Stack deployment, gather site information as outlined in the following tables. You can use this data to help populate the VMware Cloud Foundation deployment parameter worksheet that is described in Chapter 6, VMware Cloud Foundation Deployment. For detailed planning and deployment guidance, see *VMware Cloud Foundation Planning and Preparation Guide*.

Table 8. 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>S4148T-ON</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5248F-ON-Top</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5248F-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 9. 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>S4148T-ON 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 domain</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>vSAN</td>
<td>130</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td>140</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VXLAN</td>
<td>210</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRealize</td>
<td>220</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uplink01</td>
<td>230</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uplink02</td>
<td>240</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 10. Network services

<table>
<thead>
<tr>
<th>IP address/FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS [1, 2]:</td>
</tr>
<tr>
<td>NTP [1, 2]:</td>
</tr>
<tr>
<td>DHCP [1, 2]:</td>
</tr>
<tr>
<td>Active Directory [DC1, DC2]</td>
</tr>
</tbody>
</table>

### Table 11. Switch port mappings

<table>
<thead>
<tr>
<th>Server</th>
<th>S5248F-ON-Top</th>
<th>S5248F-ON-Bottom</th>
<th>S4148T-ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt1</td>
<td>NIC port 1</td>
<td>NIC port 2</td>
<td>iDRAC</td>
</tr>
<tr>
<td>Mgmt2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comp3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 12. 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>S5248F-ON-Bottom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></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></td>
<td>S4148T-ON-OOB</td>
</tr>
</tbody>
</table>

### Table 13. Fibre Channel 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>
</tbody>
</table>
## Appendix A: Site Survey

### Table 14. 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 15. 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>SDDC Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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 16. 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 data center name</td>
<td>Site A</td>
</tr>
<tr>
<td>Management cluster hosts</td>
<td>Mgmt1, Mgmt2, Mgmt3, Mgmt4 (optional)</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>