

Dell EMC Integrated Data Protection Appliance

Version 2.4.1

Installation Guide

REV. 02

December 2019

Copyright © 2019 Dell Inc. or its subsidiaries. All rights reserved.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Chapter 1	Introduction	5
	Document scope and audience.....	6
	Product features.....	6
Chapter 2	Preinstallation requirements	9
	Install Network Validation Tool.....	10
	Prepare the site and unpack the system	10
	Prepare the network environment.....	11
	Network connectivity overview.....	12
	Online Support.....	14
Chapter 3	Install the IDPA Appliance	15
	Installation overview.....	16
	Install the rails.....	16
	Secure the rails to the cabinet.....	17
	Install the system in the cabinet.....	18
	Install the bezel.....	20
	Connect the system to the network.....	21
	DP4400 ports.....	22
	Connect the power cables and power on.....	22
	Configure iDRAC.....	23
Chapter 4	Install IDPA	25
	Connect to the ACM.....	26
	DP4400 ports.....	27
	Installing the DataProtection-ACM pre-installation patch.....	27
	Install the IDPA pre-installation patch on the DataProtection-ACM	28
	Secure Remote Services (SRS).....	30
	Prepare the IDPA environment for SRS registration.....	30
	Network Configuration wizard.....	33
	Install and deploy IDPA.....	35
	Retry installation.....	39
	Rollback installation.....	40
	Troubleshoot Health monitoring.....	40
	Troubleshooting.....	41
	Configure the DataProtection-ACM for separate management networks by using the configuration wizard.....	41
	Configure the ACM settings manually for separate management networks.....	42
	IDPA post installation tasks.....	43
	Configure crontab for DP Advisor database backup.....	43
Chapter 5	License activation	45
	In-product activation.....	46
	Manual activation.....	46
Chapter 6	Storage expansion	47
	Remove the front bezel to access front panel hard drives.....	48

	Install the expansion hard drives.....	48
	Install the front bezel.....	50
	Storage expansion and upgrade.....	51
Chapter 7	Install the IDPA post-installation patch on DataProtection-ACM	53
Chapter 8	Update the IDPA Firmware (DP4400)	57
	Overview.....	58
	Prerequisites.....	58
	Prepare the Environment.....	58
	Update the iDRAC Firmware.....	59
	Update the iDRAC Service Module (ISM).....	59
	Perform the Required Checks on IDPA Point Products.....	60
	Checks on Avamar Virtual Edition (AVE).....	61
	Checks on Data Domain Virtual Edition (DDVE).....	62
	Set the VMs to enter Service Mode through ACM.....	62
	Update the Firmware.....	62
Chapter 9	Upgrade the IDPA software (DP4400)	63
	Upgrade components.....	64
	Upgrade Prerequisites (DP4400).....	64
	Upgrade the appliance software (DP4400).....	65
	Upgrade Postrequisites	68
Chapter 10	Additional resources	69
	Document references for IDPA.....	70
	IDPA training resources.....	70
Index		71

CHAPTER 1

Introduction

This section contains the following topics.

- [Document scope and audience](#)..... 6
- [Product features](#)..... 6

Document scope and audience

This document describes IDPA and explains how to install the hardware and perform the initial software configuration after the appliance hardware is set up.

The target audience for this document includes field personnel, partners, and customers responsible for managing and operating IDPA.

Product features

IDPA provides a simplified configuration and integration of data protection components in a consolidated solution.

Integrated solution

IDPA DP4400 model is a hyperconverged, 2U system that a user can install and configure onsite.

The DP4400 includes a virtual edition of Avamar server (AVE) as a Backup Server node with an optional NDMP Accelerator, a virtual edition of Data Domain system (DDVE) as the Protection Storage node, Cloud Disaster Recovery, IDPA System Manager as a centralized system management, an Appliance Configuration Manager (ACM) for simplified configuration and upgrades, Search, Reporting and Analytics, and a compute node that hosts the virtual components and the software.

The Search, Reporting and Analytics, and CDRA components are optional. Also, you can also perform the Search, Reporting and Analytics, and CDRA functions in a central corporate implementation.

If your organization enables communication through the Internet, as part of the initial configuration of the system, you can register the IDPA Appliance, Avamar, Data Domain and Reporting and Analytics components with Secure Remote Services (formerly ESRS). The Secure Remote Services is a secure, IP-based, distributed customer service support system that provides Dell EMC customers with command, control, and visibility of support-related activities.

Centralized management

IDPA System Manager provides advanced monitoring and management capabilities of the IDPA from a single pane of glass and includes the following features.

- A comprehensive dashboard that includes information about Avamar, IDPA Appliance, Data Domain, Search, and Data Protection Advisor.
 - Backup activities
 - Replication activities
 - Assets
 - Capacity
 - Health
 - Alerts
- A comprehensive dashboard to manage Avamar, Data Domain, Data Protection Advisor, and Search components.
- Advanced search and recover operations through integration with Search.
- Comprehensive reporting capabilities
- Cloud backups.

Appliance administration

The ACM provides a graphical, web-based interface for configuring, monitoring, and upgrading the appliance.

The ACM dashboard displays a summary of the configuration of the individual components. It also enables the administrators to monitor the appliance, change configuration details such as changing the Data Domain disk capacity, changing the common password for the appliance, change LDAP settings, update customer information, and change the values in the General Settings panel. The ACM dashboard enables you to upgrade the system and its components. It also displays the health information of the Appliance Server and VMware components.

Backup administration

The IDPA uses Avamar Virtual Edition (AVE) servers to perform backup operations, with the data being stored in a Data Domain system. Generally, when using the Avamar Administrator Management Console, all Avamar servers look and behave the same. The main differences among the Avamar server configurations are the number of nodes and disk drives that are reported in the server monitor.

You can also add an Avamar NDMP Accelerator (one NDMP Accelerator node is supported in DP4400) to enable backup and recovery of NAS systems. The Avamar NDMP Accelerator uses the network data management protocol (NDMP) to enable backup and recovery of network-attached storage (NAS) systems. The accelerator performs NDMP processing and then sends the data directly to the Data Domain Server (DDVE Storage).

Reporting and Analytics

The Reporting and Analytics feature offers a robust reporting functionality with dedicated sections for various features. These reports help you retrieve information about the Data Domain (DDVE) and Avamar (AVE). Using these reports, you can identify outages in the environment, diagnose problems, plan to mitigate risks, and forecast future trends. You can also run system and customized reports, dashboard templates, and schedule the reports generation as per your requirements.

Search

The Search feature provides a powerful way to search backup data within the IDPA and then restore the backup data based on the results of the Search. Scheduled collection activities are used to gather and index the metadata (such as keyword, name, type, location, size, and backup server/client, or indexed content) of the backup, which is then stored within the IDPA.

Disaster recovery

The CDRA is a solution, which enables disaster recovery of one or more on-premises virtual machines (VMs) to the cloud. CDRA integrates with the existing on-premises backup software and a Data Domain system to copy the VM backups to the cloud. It can then run a disaster recovery test or a failover, which converts a VM to an Amazon Web Services Elastic Compute Cloud (EC2) instance, and then runs this instance in the cloud.

Note:

Installing CDRA components, Search, and Reporting and Analytics (based on Data Protection Advisor) is optional. Also, if these components are already configured in your environment, then the appliance can be configured to use the central implementation in your environment. You do not need to configure the optional components that are bundled in IDPA again.

However, the IDPA dashboard does not display any data that is associated with external CDRA, Search, and Data Protection Advisor. Moreover, you must manage and configure any such external instances. Also, IDPA does not support local Search and Analytics (not part of IDPA but are centrally implemented at the customer environment) when these functions are performed by external implementations.

Scalability

The DP4400 is designed to be scalable so it can scale up with ever-changing needs. See the *Expanding storage capacity* section in the *Dell EMC Integrated Data Protection Appliance Product Guide* for more information about how to add storage capacity.

- For the DP4400 model with a capacity from 8 TB to 24 TB, you can expand the storage capacity in multiples of 4 TB increments up to 24 TB. You can now expand the capacity beyond 24 TB in 12 TB increments.
- For the DP4400 model with a capacity from 24 TB to 96 TB, you can expand the storage capacity in 12 TB increments, and you can expand the capacity up to a maximum of 96 TB.

The following table details the configuration for the DP4400 models.

Table 1 Configuration for IDPA DP4400 Models

Model	Configuration Details
DP4400	From 8 TB up to 24 TB
	From 24 TB up to 96 TB

Unified support

The same Customer Support team supports both the hardware and the software that is used in the appliance.

CHAPTER 2

Preinstallation requirements

Before you install IDPA follow the preinstallation requirements in the following topics.

• Install Network Validation Tool	10
• Prepare the site and unpack the system	10
• Prepare the network environment	11
• Network connectivity overview	12
• Online Support	14

Install Network Validation Tool

The Network Validation Tool (NVT) for IDPA runs multiple automated tests to validate the network configuration. You must run the NVT for IDPA from a system on the management network.

Before you install IDPA, network configuration must be completed for the datacenter. After the network requirements are met for the appliance, you must install and run the Network Validation Tool to validate the network requirements for a successful deployment of IDPA in the datacenter. To download the NVT, and for more information about NVT, see <https://help.psapps.emc.com/display/HELP/Network+Validation+Tool+for+IDPA>.

Prepare the site and unpack the system

Before you begin

Verify that you have the following components:

- 2U DP4400 system
- Rail kit, including:
 - Two sliding rails
 - Two velcro straps
 - Four screws
 - Four washers
- Two power cables
- Bezel
- Phillips-head screwdriver with magnetic tip (not provided)
- Qualified Ethernet cables:

Type of switch	NIC Type	Speed	Cable Required
10 Gb SFP+	SFP+ (optical)	10 Gb	LC-to-LC with SR optical GBICs or twinax
1 Gb or 10 Gb RJ45	SFP+ with 1GbBASE-T GBIC	1 Gb	UTP with RJ45 (Cat5e or Cat6)
1 Gb or 10 Gb RJ45	10 GbBASE-T (RJ45)	1 Gb or 10 Gb (depending on the switch)	UTP/STP with RJ45 (Cat6a or Cat7)


- Anti-static wrist strap and conductive foam pad

Prepare the network environment

Before you begin

You must have a computer at the install location with:

- A power adapter, C13 to NEMA 5–15 (if based in North America or country-specific cord in other geographical locations), or a power cable for your laptop power adapter with a C13 plug, to power your laptop from a rack PDU
- An Ethernet port
- Latest version of Google Chrome or Mozilla Firefox


 **Note:** Ensure that ICMP (ping) is enabled in the customer environment during IDPA installation.


About this task


The following steps must be completed before starting initial configuration with the Appliance Configuration Manager:

Procedure


1. Identify 13 unassigned IP addresses for the IDPA components. To simplify configuration, select a range of 13 contiguous addresses.
2. Register the 13 IP addresses in DNS with forward and reverse lookup entries for each address. Ensure that the router for the 13 IP addresses can be pinged.

 **Note:** When you reserve the IP addresses, you must assign the IP addresses to hostnames in the DNS server. Ensure that the hostnames that are assigned to the point products are in lower case and do not have an underscore (_) or the at (@) characters. If the hostnames have an underscore (_) or the at (@) characters, the configuration fails.

 **Note:** When you configure the DNS server settings during appliance configuration ensure that you configure the settings properly. After, you configure the hostname and domain name of the point products you cannot modify the settings. You can modify the DNS server IP address on the point products after the appliance is configured. Ensure that the new DNS server has the same hostname and domain names that are associated with the corresponding point product IP addresses. For more information about modifying the DNS server IP address, see [KB 537628](#).

 **Note:** Ensure that **ICMP** is enabled in your network environment. If **ICMP** is disabled, the deployment of the appliance fails.

3. Download the license files for Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE), and Data Protection Advisor (DP Advisor) from the Dell EMC Software Licensing Central.

 **Note:** For DP4400, only during the initial activation, the license keys are automatically downloaded from the ELMS server if the appliance is connected to the network with Internet access. If the licenses are not activated automatically, you must manually activate the licenses. For more information about activating the licenses manually, see [Manual activation](#) on page 46

The contact person who is mentioned on your sales order should have received the License Authorization Code (LAC) letter through an email during the order fulfillment process. The

LAC letter includes the license authorization code that is associated with your order, instructions for downloading software binaries, and instructions for activating the entitlements online through Dell EMC Software Licensing Central.

Follow the steps mentioned in the LAC letter to activate the software and download the license keys. For additional information, see the Standard Activation Process section in the *License Activation Guide*.

Note: The LAC letter has the link <https://licensing.emc.com/deeplink/<LAC>> which directs you to Dell EMC Software Licensing Central. <LAC> is a unique alphanumeric value that is mentioned in your LAC letter.

After the activation is complete, download the license keys that are generated for Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE), and Data Protection Advisor (DP Advisor). Use these license keys during the IDPA configuration. For more information License activation, see [License activation](#) on page 45

Network connectivity overview

During the initial configuration, IP addresses are assigned to various functional components of IDPA, typically by allocating a range of IP addresses. IDPA requires 13 IP addresses for the various components. Using a range is the preferred method as it simplifies the assignment and reduces the chance for errors while entering the IP addresses. When a range of IP addresses is used during the IDPA configuration, the IP addresses are assigned in a standard order. Optionally, discrete IP addresses can be assigned manually to each functional component.

Of these 13 IP addresses, two are required for the initial network configuration; one for the ACM and the other for the ESXi server. After the initial network configuration is successful, the IPs for the other components can be configured using a range of 11 IP addresses. If a range of IPs is not available, users can also set random IPs of the same subnet to the components.

Use the following table to determine which IP address is allocated to a component. The *IP Range Allocation* (first column in the table) is the value that you should add to the first IP address in the range.

Table 2 IP address range assignments for DP4400

IP Range Allocation	Example	Component	Assigned Field
+0	192.0.2.1	vCenter	VMware vCenter Server VM
+1	192.0.2.2	Protection storage	DDVE Management IP
+2	192.0.2.3	Protection storage	DDVE Backup IP 1
+3	192.0.2.4	Protection storage	DDVE Backup IP 2
+4	192.0.2.5	Backup application	Avamar Virtual Edition Server IP
+5	192.0.2.6	Backup application	Avamar Proxy VM
+6	192.0.2.7	IDPA System Manager	IDPA System Manager VM
+7	192.0.2.8	Reporting and Analytics	Application Server Host VM
+8	192.0.2.9	Reporting and Analytics	Datastore Server Host VM
+9	192.0.2.10	Search	Index Master Node Host VM

Table 2 IP address range assignments for DP4400 (continued)

IP Range Allocation	Example	Component	Assigned Field
+10	192 . 0 . 2 . 11	DD Cloud DR CDRA (optional)	Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance

Note: IDPA is compatible with IPv4 enabled networks and does not support pure IPv6 or dual-stack networks.

Note: For more information on the network and firewall ports that are used in IDPA, see *Network ports* in the *IDPA Security Configuration Guide*.

Separate management network

DP4400 models support separating the backup network traffic from the management network traffic. For configuring separate management network you need two IP addresses one for the management network and one for the backup settings on the ACM, and one for the ESXi server.

Use the following table to determine which IP address is allocated to a component when you configure a separate management network. The *IP Range Allocation* (first column in the table) is the value that you should add to the first IP address in the range.

Table 3 Management IP address range assignments for the DP4400 with Dedicated Backup Network

Management IP Range Allocation	Component	Assigned Field
+0	vCenter	VMware vCenter Server VM
+1	Protection storage	Management IP
+2	Backup application	Avamar Virtual Edition Server IP
+3	Backup application	Avamar Proxy VM
+4	IDPA System Manager	IDPA System Manager VM
+5	Reporting and Analytics	Application Server Host VM
+6	Reporting and Analytics	Datastore Server Host VM
+7	Search	Index Master Node Host VM
+8	DD Cloud DR CDRA (optional)	Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance

Table 4 Backup IP address range assignments for the DP4400 with Dedicated Backup Network

Backup IP Range Allocation	Component	Assigned Field
+0	Protection storage	DDVE Backup IP 1
+1	Protection storage	DDVE Backup IP 2
+2	Backup application	Avamar Proxy VM

Online Support

Record the following information related to your Online Support account:


Online Support credentials

To create an Online Support account, go to <https://www.dell.com/support>. Your username and password is required for Secure Remote Services (formerly ESRS) configuration.

Site ID

A Site ID is created in Support systems for each location within your organization where Dell EMC products are installed. Your Site ID is required during initial configuration. Verify your Site ID number on Online Support:

1. Log in to Online Support with your credentials.
2. Hover over your username and select **Manage Company Information**.
3. Click **View Sites**.

 **Note:** You can also search for a site and add it to the My Sites list. If a site ID is not available or the correct site ID is not listed, you must notify your local field representative to request one.

CHAPTER 3

Install the IDPA Appliance

The following topics describe how to install the IDPA Appliance.

• Installation overview	16
• Install the rails	16
• Secure the rails to the cabinet	17
• Install the system in the cabinet	18
• Install the bezel	20
• Connect the system to the network	21
• Connect the power cables and power on	22
• Configure iDRAC	23

Installation overview

This guide is designed for personnel who install, configure, and maintain the Integrated Data Protection Appliance DP4400. To use this hardware publication, you should be familiar with digital storage equipment and cabling.

Before you begin

Gather the required materials and configure your network environment as specified in [Prepare the site and unpack the system](#) on page 10.

About this task

Use the following sequence of actions as a guide to install the system.

Procedure

1. [Install](#) and [secure](#) the rails.
2. [Install the system in the cabinet](#) and [attach the bezel](#).
3. [Connect the system to the network](#).
4. [Connect the power cables and power on](#).

Results

The system is ready for initial configuration. For additional help and resources, review the information in [Additional resources](#) on page 69.

Install the rails

About this task

The rails are labeled left and right, and cannot be interchanged. The front side of each rail is labeled **Left Front** or **Right Front** when the rail faces the cabinet front.

Procedure


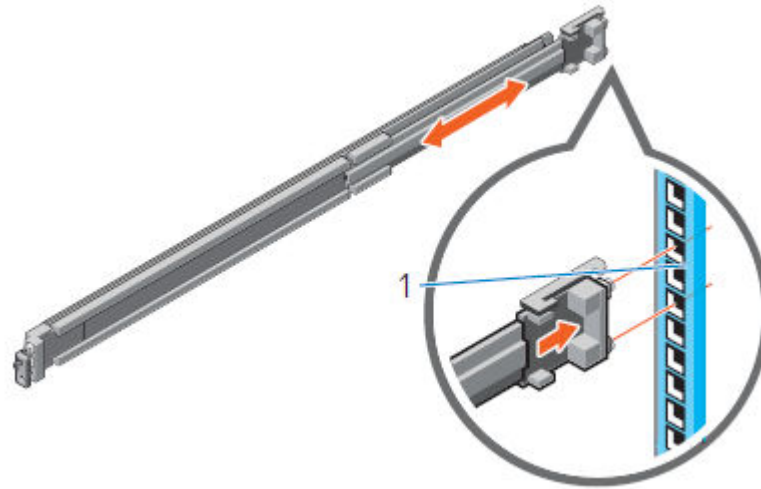
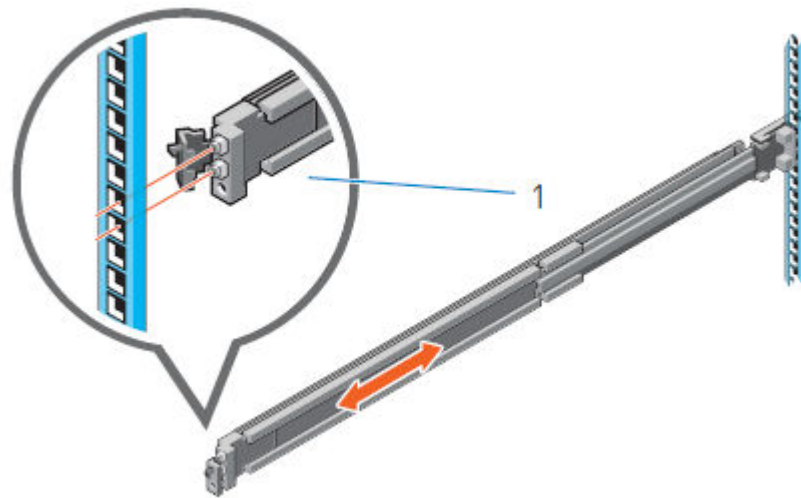
1. Determine where to mount the system, and mark the location at the front and back of the cabinet.
 **Note:** Install the left rail assembly first.
2. Fully extend the rear sliding bracket of the rail.
3. Position the rail end piece labeled **Left Front** facing inward and orient the rear end piece to align with the holes on the rear cabinet flanges.
4. Push the rail straight toward the rear of the rack until the latch locks in place.

Figure 1 Installing the rear end of the rail

5. For the front end piece, rotate the latch outward and pull the rail forward until the pins slide into the flange, and release the latch to secure the rail in place.

Figure 2 Installing the front end of the rail

6. Repeat the preceding steps to install the right rail assembly.

Secure the rails to the cabinet

The supplied screws and washers are used to secure the rail assemblies to the front and rear of the cabinet.

About this task

- Note:** For square hole cabinets, install the supplied conical washer before installing the screw.
For unthreaded round hole cabinets, install only the screw without the conical washer.

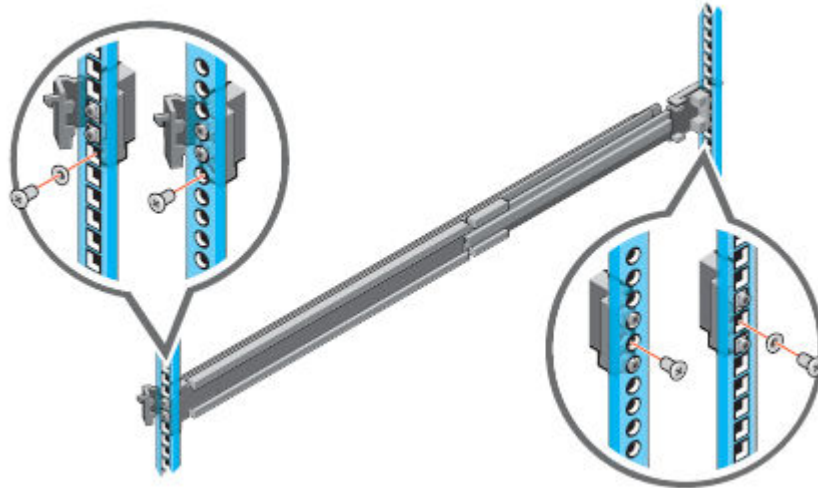
Procedure

1. Align the screws with the designated U spaces on the front and rear rack flanges.

Ensure that the screw holes on the tab of the system retention bracket are seated on the designated U spaces.

2. Insert and tighten the two screws using the Phillips #2 screwdriver.

Figure 3 Installing screws



Install the system in the cabinet

About this task

⚠ WARNING The system is heavy. To avoid personal injury and/or damage to the equipment, do not attempt to install the system in a cabinet without a mechanical lift and/or help from another person.

Procedure

1. At front of the cabinet, pull the inner slide rails out of the cabinet until they lock into place.

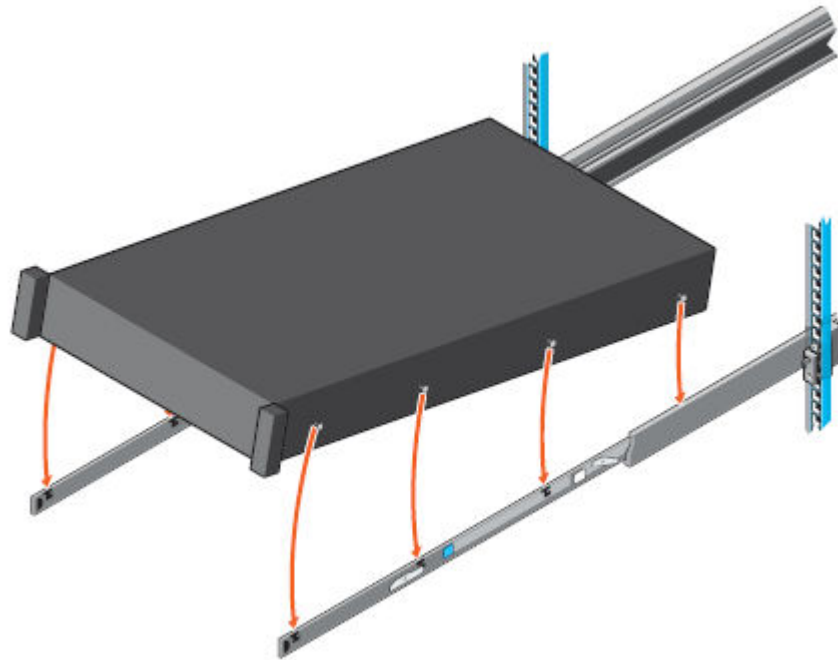
Figure 4 Pull the inner rails out of the cabinet



2. Locate the rear rail standoff on each side of the system. Position the system above the rails and lower the rear rail standoffs into the rear J-slots on the slide assemblies.

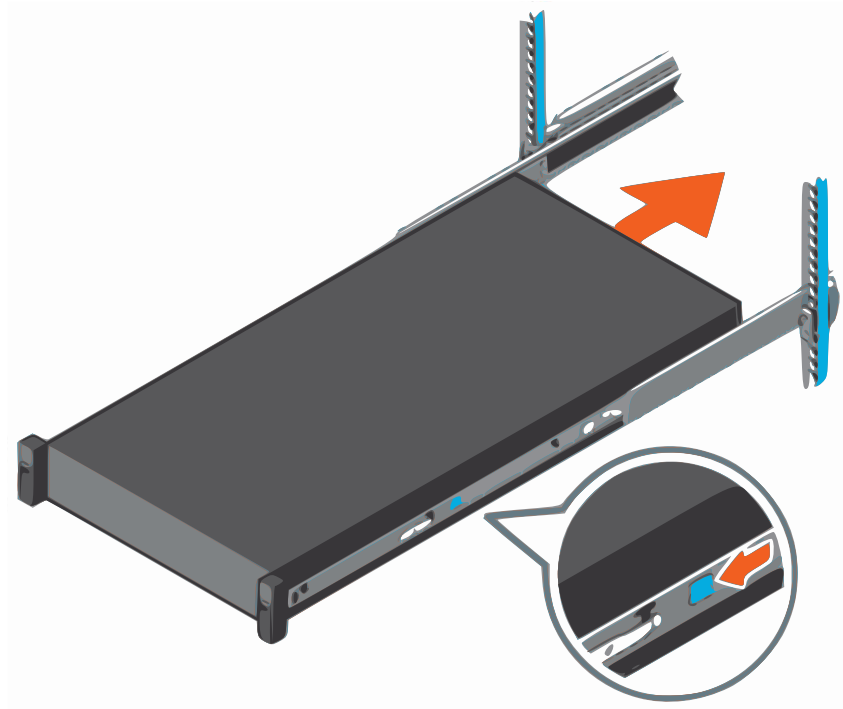
3. Rotate the system downward until all the rail standoffs are seated in the J-slots.

Figure 5 Install the system in the rails



4. Push the system inward until the lock levers click into place.
 5. Pull the blue slide release lock tabs forward on both rails and slide the system into the cabinet. The slam latches will engage to secure the system in the cabinet.
- Note:** Ensure that the inner rail slides completely into the middle rail. The middle rail locks if the inner rail is not fully engaged.

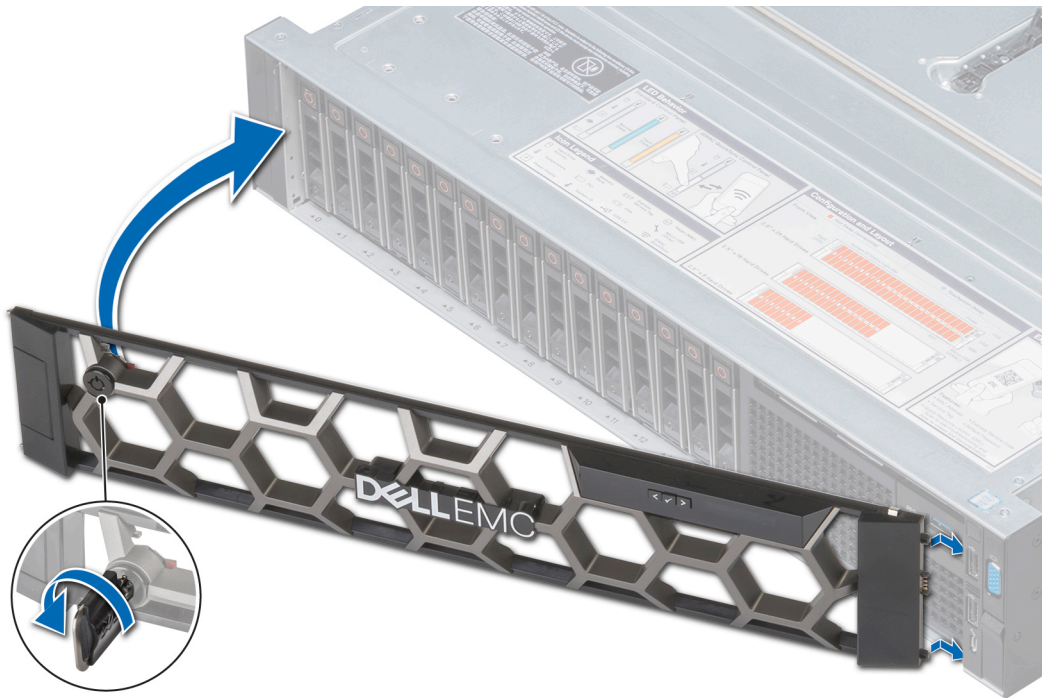
Figure 6 Slide the system into the cabinet



Install the bezel

Procedure

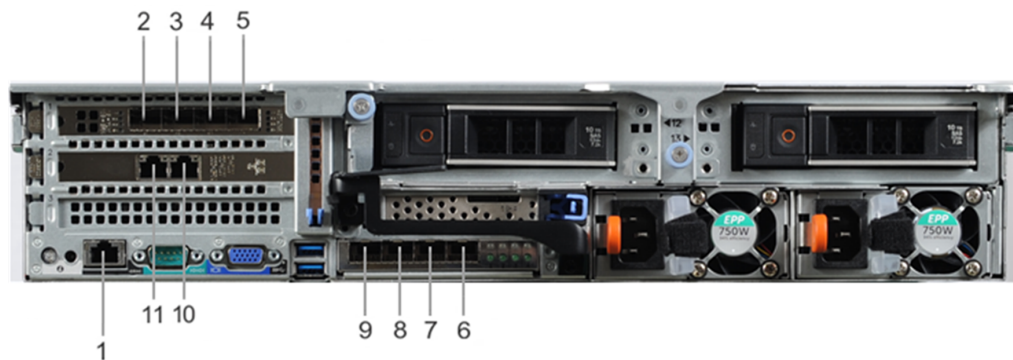
1. Align and insert the right end of the bezel onto the system.
2. Press the release button and fit the left end of the bezel onto the system.
3. Lock the bezel by using the key.

Figure 7 Installing the front bezel

Connect the system to the network

The following figure shows the location of the DP4400 network ports and iDRAC port.

About this task

Figure 8 DP4400 network and iDRAC connections

Procedure

1. Use a Cat5e or Cat6 UTP copper Ethernet cable to connect a 1 GbE port (10) to the service computer.
2. If the DP4400 contains 10 Gb SFP network cards, use fiber cables with a 10 Gb optical SFP to connect the four required 10 GbE ports (2, 3, 8, 9) to access ports on the switch in your network.
3. If the DP4400 contains 10 Gb BASE-T network cards, use Cat6a UTP or Cat7 copper cables to connect the four required 10 GbE ports (2, 3, 8, 9) to access ports on the switch in your network.




4. Use a Cat5e or Cat6 copper Ethernet cable to connect the iDRAC port (1) in the lower left of the system chassis to the network.

DP4400 ports

About this task

Table 5 DP4400 port types


Callout number	Port type
1	iDRAC
2	10 GbE (required)
3	10 GbE (required)
4	10 GbE (unused)
5	10 GbE (unused)
6	10 GbE (unused)
7	10 GbE (unused)
8	10 GbE (required)
9	10 GbE (required)
10	1 GbE
11	1 GbE (unused)

-  **Note:** Ports 2 and 9 are a vSwitch0 network team. Ports 3 and 8 are a vSwitch1 network team and are used during appliance configuration.
-  **Note:** Ensure that the four required 10 GbE ports (2, 3, 8, and 9) are connected to the access ports on the switch in your network.
-  **Note:** If you select the **Separate Management Network** check box, ensure that you connect port 2 and 9 to the management VLAN and ports 3 and 8 to backup VLAN.

Connect the power cables and power on

Procedure

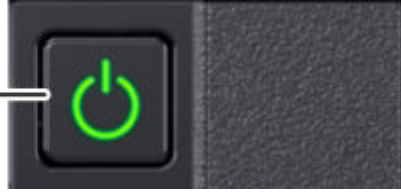
1. Connect the power supply units to the rack.

-  **Note:** Connect each PSU to a redundant AC power source. Redundant power sources allow one AC source to fail or be serviced without impacting system operation. Connect PSU 0 to one AC source, and PSU 1 to the other AC source.

The system may not power on automatically after plugging in the AC power cords. The system identification button located on the rear of the chassis, on the lower left-hand side illuminates blue when power is on.

2. If the system does not power on automatically after connecting the power cables, press the power button on the right control panel at the front of the chassis to power on the system .

1



Configure iDRAC

You must configure the Integrated Dell Remote Access Controller (iDRAC) for system upgrade and maintenance operations. Additionally, IDPA supports the use of iDRAC to change security settings and enables you to remotely power the system on.

Before you begin

Connect to the unit using a VGA monitor with a keyboard or a serial port, power on the appliance, and perform the following steps:

Note: Do not use iDRAC to change the storage configuration, system settings, or BIOS settings, as making changes to these will impact the system functionality. Contact Support if changes are required in any of these areas.

Procedure

1. During the system boot process, press **F2** to access the BIOS menu.
2. In the **System Setup Main Menu** page, click **iDRAC Settings**.
The iDRAC Settings page is displayed.
3. Click **Network**.
The Network page is displayed.
4. Under **IPv4 Settings**, specify static IP address details.
5. Press **Esc** to return to the previous menu.
6. Select **User Configuration**.
 - a. Enable the root user.
 - b. Change the root user password.

Note that the default password is *Idpa_1234*.

CHAPTER 4

Install IDPA

The following topics describe how to install and configure IDPA.

• Connect to the ACM	26
• Installing the DataProtection-ACM pre-installation patch	27
• Secure Remote Services (SRS)	30
• Network Configuration wizard	33
• Install and deploy IDPA	35
• Troubleshooting	41
• Configure the DataProtection-ACM for separate management networks by using the configuration wizard	41
• Configure the ACM settings manually for separate management networks	42
• IDPA post installation tasks	43

Connect to the ACM

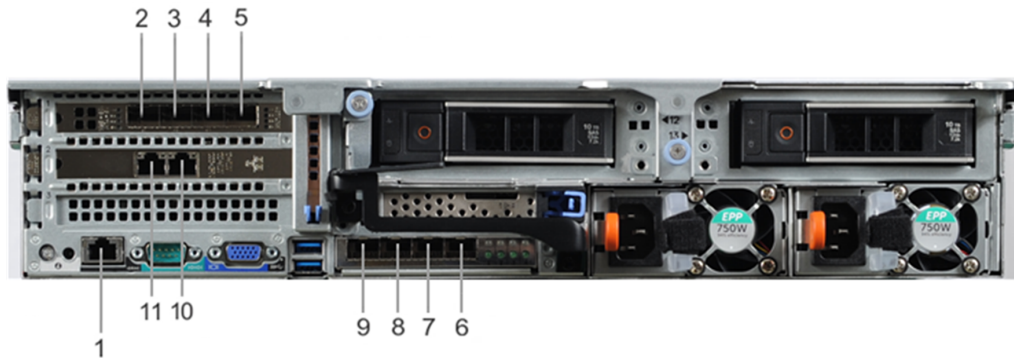
Connect to the ACM user interface and begin the configuration process. For a seamless experience, enable both private and public network connections to your service computer.

Before you begin

- After powering on the appliance, wait 5 minutes for startup to complete.
- Verify that the service computer is connected to the 1 GbE port that is identified as (10) in [Figure 9](#) on page 26.
- On the service computer, record the IP address settings for the Ethernet interface that is connected to the DP4400.

Note: IDPA uses the 192.168.100.xxx IP addresses for the internal components. Ensure that the 192.168.100 network is not used in your environment. If the network addresses are in use, contact Customer Support for assistance.

Figure 9 DP4400 network and iDRAC connections



Procedure

1. On the service computer, assign the static IP address 192.168.100.98 and the subnet mask 255.255.255.0 for the Ethernet interface that is connected to the DP4400.
A default gateway is not required.
2. Verify that the ACM responds to a ping on the default ACM IP address, 192.168.100.100.
3. To connect to the ACM user interface, type `https://192.168.100.100:8543/` in a browser window.
4. Log in to the ACM with the default system account username and password:
 - **User Name:** root
 - **Password:** Idpa_1234
5. Provide a new password when prompted.

Note: This password is assigned to all appliance components. It must contain 9–20 characters and include at least one of each type of supported characters. The following types of characters are supported:

- Uppercase letters (A–Z)
- Lowercase letters (a–z)

- Numbers (0–9)
- Special characters: Period (.), hyphen (-), and underscore (_)

The password must not include common names or usernames such as `root` or `admin`. Also, the password must not start with a hyphen (-) and end with a period (.).

The system logs you out after changing the password. Log back in with the new password.

6. On the **End User License Agreement** screen, accept the EULA.

Results

The **Network Configuration** screen appears.

DP4400 ports

About this task

Table 6 DP4400 port types

Callout number	Port type
1	iDRAC
2	10 GbE (required)
3	10 GbE (required)
4	10 GbE (unused)
5	10 GbE (unused)
6	10 GbE (unused)
7	10 GbE (unused)
8	10 GbE (required)
9	10 GbE (required)
10	1 GbE
11	1 GbE (unused)

- Note:** Ports 2 and 9 are a vSwitch0 network team. Ports 3 and 8 are a vSwitch1 network team and are used during appliance configuration.
- Note:** Ensure that the four required 10 GbE ports (2, 3, 8, and 9) are connected to the access ports on the switch in your network.
- Note:** If you select the **Separate Management Network** check box, ensure that you connect port 2 and 9 to the management VLAN and ports 3 and 8 to backup VLAN.

Installing the DataProtection-ACM pre-installation patch

Before you configure the DataProtection-ACM virtual machine, install the latest IDPA pre-installation patch if it is available.

For example:

`Idpa_pre_update_N.N.N-nnnnnn.zip`

Where *N.N.N* is the latest pre-installation patch version and *nnnnnn* is the build number.

You can install the pre-installation patch before you connect to the DataProtection-ACM using a browser for the initial configuration.

Install the IDPA pre-installation patch on the DataProtection-ACM

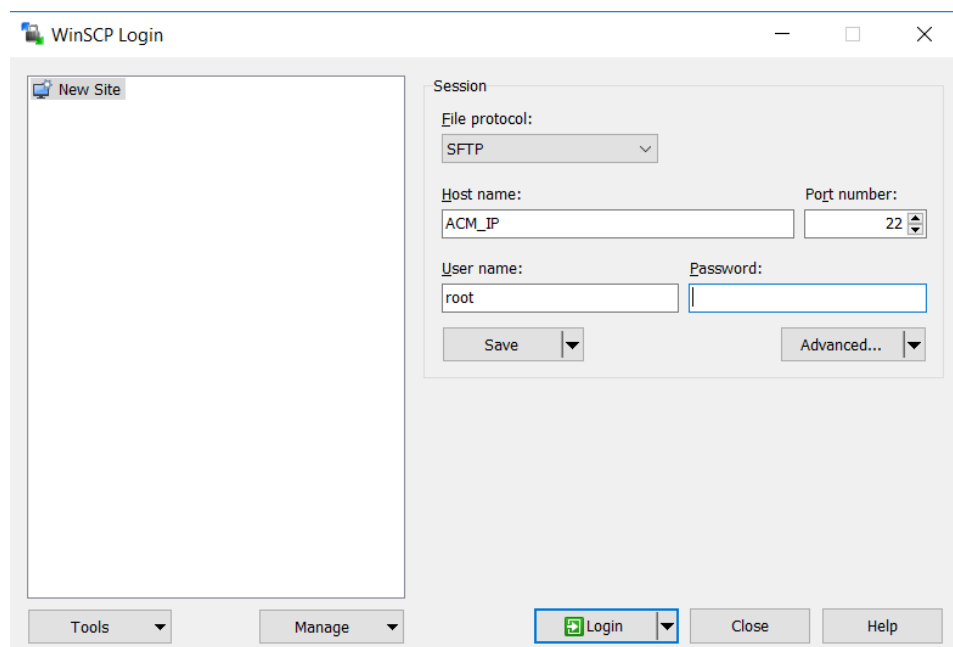
This section provides information about how to install the pre-installation patch on the DataProtection-ACM.

Procedure

1. Check https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance to see if a pre-installation patch is available for your version of IDPA. If a pre-installation patch is available, download it to a folder on your laptop.
2. Extract the contents of the `Idpa_pre_update_N.N.N.nnnnnn.zip` file.
The zip file contains the `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` file and the `ReadMe.txt` file.
Note: For additional information about installing the pre-installation patch, see the `ReadMe.txt` file.
3. Open the WinSCP or SCP application on the service laptop, and then connect to the DataProtection-ACM by performing the following actions:
 - a. In the **File protocol** field, select **SFTP**.
 - b. In the **Hostname** field, enter `192.168.100.100` as the IP address of the DataProtection-ACM.
 - c. In the **Port number** field, specify the default port number **22**.
 - d. In the **User name** field, enter `root`.
 - e. In the **Password** field, enter `Idpa_1234`.
 - f. Click **Login**.

The following figure shows a sample WinSCP session configuration window.

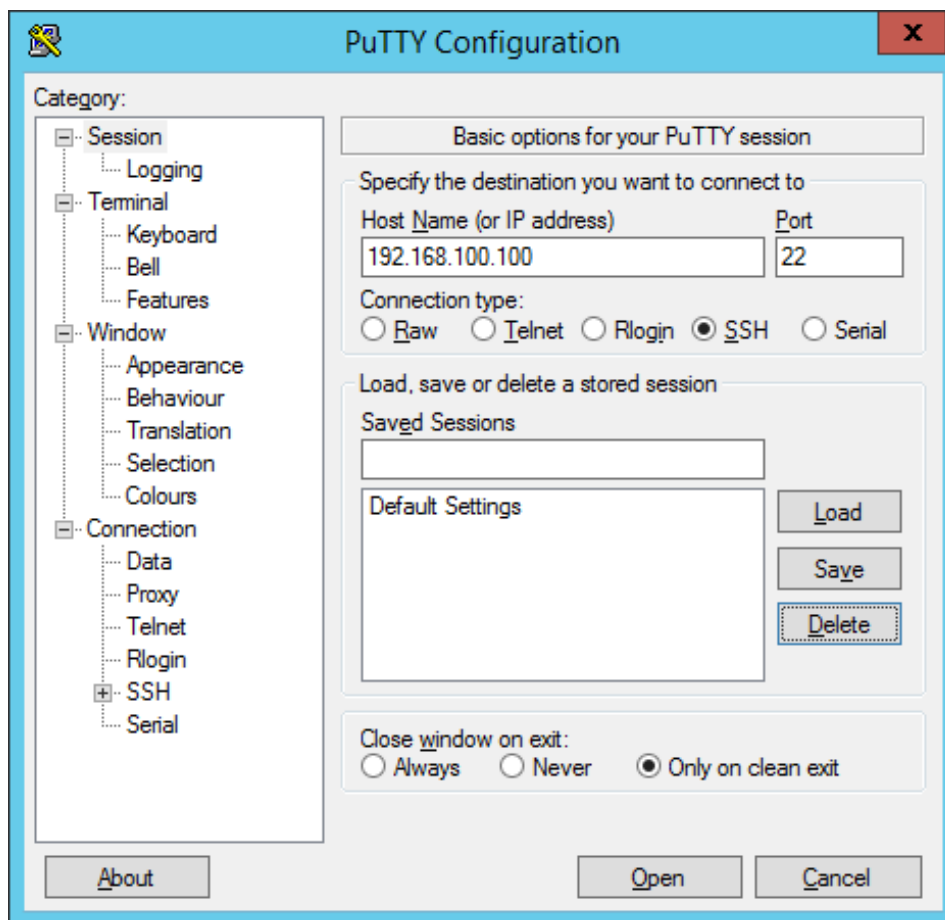
Figure 10 WinSCP session configuration window



4. Create a temporary folder `/tmp/patch`.
5. Copy the `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` file to the `/tmp/patch` directory.
6. Connect to the DataProtection-ACM by using Putty from the service laptop.

The following figure shows the Putty configuration screen.

Figure 11 Putty Configuration screen for DataProtection-ACM



7. At the login as prompt, type `root`.
8. At the Password prompt, type the password for the root user.
The default password for the root user is `Idpa_1234`.
9. Determine the DataProtection-ACM version by typing the following command:

```
rpm -qa | grep dataprotection
```

Ensure that the DataProtection-ACM version is earlier than `dataprotection-N.N.N-nnnnn.x86_64`. For more information, see the `ReadMe.txt` file available in the `Idpa_pre_update_N.N.N.nnnnnn.zip` file.

where *n.n.n* is the latest IDPA version and *nnnnn* is the build number.

10. Change to the directory that contains the pre-installation patch file by typing the following command:

```
cd /tmp/patch
```
11. Extract the contents of the `.tar.gz` file by typing the following command:

```
tar -xvf Idpa_pre_update_N.N.N.nnnnnn.tar.gz
```

The contents are extracted to a subdirectory named `Idpa_pre_update_N.N.N.nnnnnn`.

12. Change directory to `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` directory by typing the following command:

```
cd /tmp/patch/Idpa_pre_update_N.N.N.nnnnnn/
```

13. Change permission of `install.sh` file by typing the following command:

```
chmod +x install.sh
```

14. Run the installation script file by typing the following command:

```
./install.sh
```

Messages are displayed on the screen during the installation process. The following message might be displayed, which you can ignore:

```
"warning: file /usr/local/dataprotection/var/configmgr/server_data/
config/InfrastructureComponents_Template.xml: remove failed: No
such file or directory"
"warning: file /usr/local/dataprotection/customscripts/
Config.properties: remove failed: No such file or directory"
```

15. Verify that the pre-installation patch installation completed successfully by typing the following command:

```
rpm -qa | grep dataprotection
```

Ensure that the DataProtection-ACM version is the latest version.

16. Delete the `Idpa_pre_update_N.N.N.nnnnnn.zip` file, and then delete the `/tmp/patch/Idpa_pre_update_N.N.N.nnnnnn` directory.

Secure Remote Services (SRS)

Secure Remote Services (SRS) delivers a secure, IP-based, distributed remote service support solution that provides command, control, and visibility of remote services access.

Dell EMC strongly recommends that you complete the SRS registration process, so that it enables you to have the following advantages:

- Dell EMC delivers product event reports such as error alerts, thereby greatly increasing the availability of your information infrastructure.
- Dell EMC provides rapid remote services either through automated recognition and notification or through interpretation and response when a support event occurs, eliminating the need for on-site support visits.
- Provides increased protection of your information.
- Reduced risk.
- Improved time-to-repair.

Complete information on SRS is available from the Online Support site at <https://support.emc.com>.

Prepare the IDPA environment for SRS registration

To prepare the IDPA environment for SRS registration, add the customer site IDs to the SRS gateway, and then register DataProtection-ACM with SRS.

Before configuring SRS, ensure that you have installed the hotfix as described in [#unique_30](#).

For more information about Configuring SRS, see [#unique_31](#).

Add customer site IDs to SRS

Add all customer site IDs to the SRSgateway host.

Before you begin

Obtain the list of customer site IDs, and ensure that the SRS gateway host runs a minimum version of 3.20.00.08.

Procedure

1. To connect to the SRS gateway, open a browser window and type the following URL:

`https://SRS_Gateway_IP_Address:9443`

where *SRS_Gateway_IP_Address* is the IP address of the SRS gateway host.

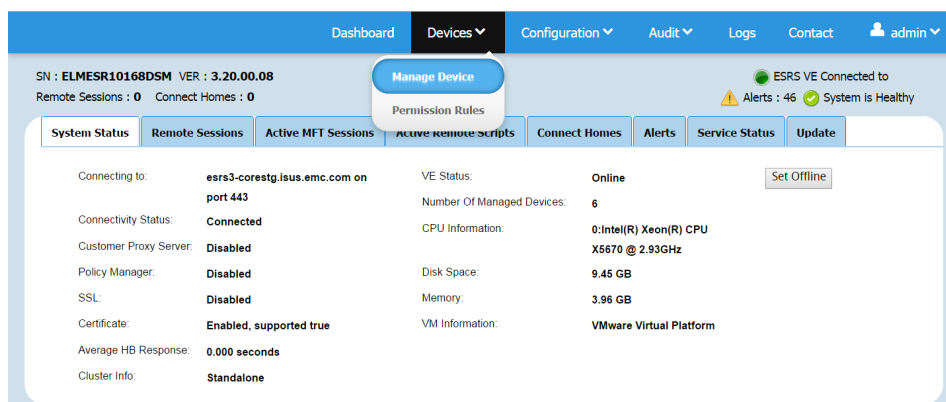
2. When prompted, type the SRS username and password, and then click **Login**.

The SRS console appears.

3. From the **Devices** menu, select **Manage Device**.

The following figure shows the SRS console and the **Devices** menu.

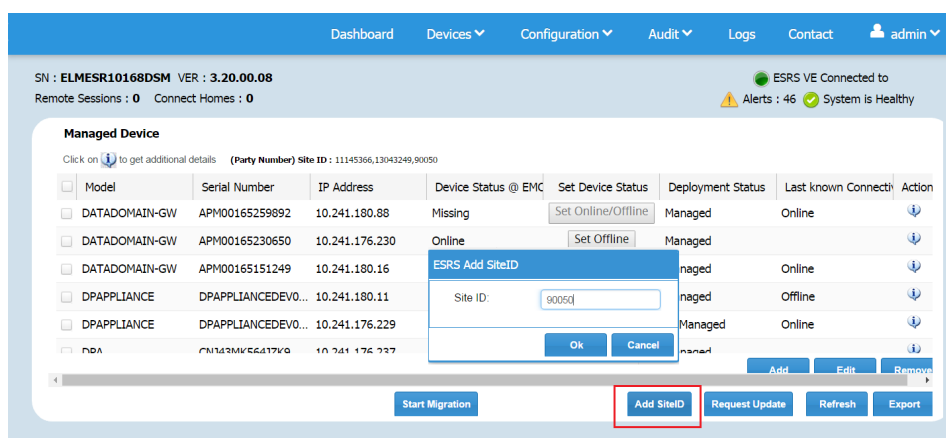
Figure 12 SRS Devices menu



4. Click the **Add SiteID** button. In the **SRS Add SiteID** window, type the site ID, and then click **OK**.

The following figure shows the **SRS Add SiteID** window.

Figure 13 SRS Add SiteID window



- From the **SN** field in the upper-left corner of the SRS console, retrieve and record the SRS gateway serial number, and then close the web page.

Verifying the SRS gateway site ID addition

After you add the customer site IDs to the SRS gateway, confirm that the site IDs appear on the SRS staging server.

Before you begin

Ensure that you have the SRS gateway serial number and the customer site IDs.

About this task

To verify that the site IDs were added successfully, perform the following steps.

Procedure

- Connect to the SRS server. In a browser window, type the following URL:

<http://servicelink.emc.com>

The **RSA Access Manager** page appears.

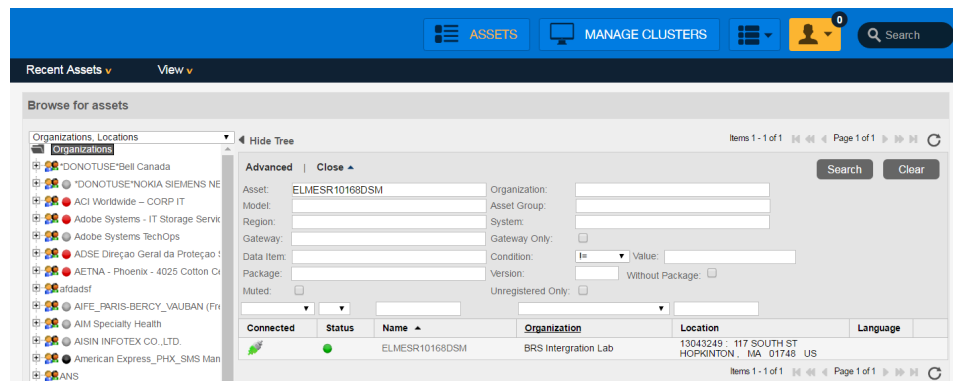
- In the **User ID** field, type your user ID. In the **Password** field, type your SecureID passcode, and then click **Go**.

The SRS staging console appears with the **Assets** view selected.

- In the **Asset** field, type the serial number of the customer SRS gateway, and then click **Search**

The following figure shows the **Assets** view.

Figure 14 SRS Assets view



- In the **Search Results** table, click the SRS gateway serial number.

The following figure shows the **Search Results** table, with the SRS gateway serial number highlighted.

Figure 15 Search Results table with serial number highlighted

Advanced | Close ▲

Search Clear

Asset: ELMESR10168DSM Organization:

Model: Asset Group:

Region: System:

Gateway: Gateway Only: ☐

Data Item: Condition: I= Value:

Package: Version: Without Package: ☐

Muted: ☐ Unregistered Only: ☐

Connected	Status	Name	Organization	Location	Language
		ELMESR10168DSM	BRS Intergration Lab	13043249 - 117 SOUTH ST HOPKINTON, MA 01748 US	

Items 1 - 1 of 1 Page 1 of 1

The **Device Information** window appears.

- In the **Additional Info** area, click **Managed Devices**.

The following figure shows the **Device Information** window with the **Managed Devices** option selected.

Figure 16 SRS device information with Managed Devices selected

Assets : ELMESR10168DSM Jump to: Dashboard

Device Additional Info

Last SR Number: 3.20.00.08

ESRS Version: 3.20.00.08

Managed Devices

Add Device To WatchList

Location

Organization: BRS Intergration Lab

Region: 54000 CS Region-52721 AM CS District

Location: 13043249 117 SOUTH ST HOPKINTON, MA 01748 US

Language:

Contacts View all | Manage

ELMESR10168DSM

Serial number: ELMESR10168DSM

Model: ESRS-VE

Asset Group(s): /Root Asset Group/Default Model Group/ESRS-VE Default Group

Status: Good

Registration: 10/4/16 2:21 PM

Last contact: 3/29/17 2:23 AM (7 seconds ago)

Agent Version: 6.9.0

Ping rate: 30 seconds

Time zone: Eastern Daylight Time

Muted: No

Data

3/27/17 11:51 AM AvailableGASList: <https://esrs3-corestg.isus.emc.com:443/images/testBandwidth.gif>; <https://esr3gdstg01-dbi.isus.emc.com:443/images/testBandwidth.gif>; <https://esr3gdstg02-dbi.isus.emc.com:443/images/testBandwidth.gif>; <https://esr3gdstg03-dbi.isus.emc.com:443/images/testBandwidth.gif>

3/27/17 2:24 PM CHCEMFileAge: 0

3/27/17 2:24 PM CHCEMFileCount: 0

Recent Actions

3/29/17 2:10 AM Delivered to Agent Package Deployed [Gateway Sync Package]

ESRS Remote Session

CLViaSSH

WebUI

View All Active

Actions View all

Restart Connectivity Service

Set Device Online/Offline (1 - Online, 0 - Offline)

Scripts View all

ESRS Diagnostics - Run

The **HA Gateway Cluster** window appears.

- Confirm that all site IDs appear in the **HA Gateway Cluster** window, and then close the web page.

Network Configuration wizard

After accepting the EULA, configure initial connectivity to the DP4400 appliance.

About this task

Provide the information required in the steps below to configure the network.

Note: The IDPA is compatible with IPv4 enabled networks and does not support pure IPv6 or dual stack networks.

Procedure

- Provide the following information to configure the network settings.

Subnet mask

IP address mask that identifies the range of IP addresses in the subnet where the appliance is connected.

Gateway IP address

Default gateway IP address of the appliance.

Primary DNS server IP address

The primary DNS server for your network environment.

Secondary DNS server IP address

The secondary DNS server for your network environment.

Domain name

The domain name for your network environment.

Appliance Configuration Manager IP Address/Hostname

The IP address to assign to the ACM. This is the first IP address of the 13 IPs that is reserved for the ACM.

ESXi IP Address/Hostname

The IP address to assign to the ESXi server. This is the second IP address of the 13 IPs that is reserved for ESXi.

NTP server IP Address/Hostname

The NTP server IP address for your network environment.

If you want to configure the separate management and backup network, perform the following actions.

2. Click **Separate Management Network** check box to configure the separate management and backup network settings.
 - a. Provide the following information to configure the **Management network settings**.

Subnet mask

IP address mask that identifies the range of IP addresses in the subnet where the appliance is connected.

Gateway IP address

Default gateway IP address of the appliance.

Primary DNS server IP address

The primary DNS server for your network environment.

Secondary DNS server IP address

The secondary DNS server for your network environment.

Domain name

The domain name for your network environment.

Appliance Configuration Manager IP Address/Hostname

The IP address to assign to the ACM. This is the first IP address of the 13 IPs that is reserved for the ACM.

ESXi IP Address/Hostname

The IP address to assign to the ESXi server. This is the second IP address of the 13 IPs that is reserved for ESXi.

NTP server IP Address/Hostname

The NTP server IP address for your network environment.

- b. Provide the following information to configure the **Backup network settings**.

Subnet mask

IP address mask that identifies the range of IP addresses in the subnet where the appliance is connected.

Gateway IP address

Default gateway IP address of the appliance.

Primary DNS server IP address

The primary DNS server for your network environment.

Secondary DNS server IP address

The secondary DNS server for your network environment.

Domain name


The domain name for your network environment.

Appliance Configuration Manager IP Address/Hostname

The IP address to assign to the ACM. This is the first IP address of the 13 IPs that is reserved for the ACM.

3. Click **Submit**.

Results


- After you configure basic networking, your web browser automatically redirects to the ACM IP address assigned during network configuration.
-  **Note:** For automatic forwarding to work correctly, the computer you use to complete the configuration must be connected to the same network as the configured ACM IP address.
- If you cannot have connections to both public and private networks simultaneously, disconnect from the private appliance configuration network and then connect to the network that the ACM IP address is on to complete the rest of the configuration.
- Once the network configuration is complete, revert the network adapter IP address settings on the service computer to their previous state.
- If the network configuration fails, you can click **Rollback** to revert all the settings. You must review the settings, make any changes if required, and then configure the network settings again.

Install and deploy IDPA

This procedure provides you information about how to install and deploy the DP4400 appliance. The GUI helps you in setting up IDPA and prepares the appliance for use.

About this task

To install and deploy the IDPA Appliance, complete the following actions.


-  **Note:** Ensure that you install and run the Network Validation Tool before you install IDPA. For more information about NVT, see [Install Network Validation Tool](#)


Procedure

- Open a browser and enter `https://192.168.100.100:8543` to access the ACM UI.
- Enter **Username** and **Password** in the respective fields and click **Login**.
The **Change Appliance password** page is displayed.

3. Enter the current password, new password, and confirm the new password in the **Current Password**, **New Password**, and **Confirm Password** fields in the **Change Appliance Password** page and click **Submit**.

The **Change Appliance Password** dialog box is displayed.

 **Note:** After you successfully change the password, the system automatically logs out and prompts you to log in with the new password.

 **Note:** This password applies to all the components of the IDPA Appliance.

4. Read the **End User License Agreement** and click **I agree** in the page to continue the deployment.

The **Network Configuration** page is displayed.

5. In the **Network Configuration** page, if you want to configure the separate management network, click the **Seperate Management Network** check box to enter the IP addresses for the separate management and backup network settings. For more information about the IP range for the separate management network, see [Configure the DataProtection-ACM for separate backup networks by using the configuration wizard](#).


After you configure the **Seperate Management Network** continue from step 8 on page 37

6. In the **Network Configuration** page, under **Network settings** section enter the IP addresses in the following field and click **Submit** if you have not selected the **Seperate Management Network** check box.

 **Note:** Ensure that you read the prerequisites before you configure the network settings.

- Subnet mask
- Gateway IP address
- Primary DNS server IP address
- Secondary DNS server IP address
- Domain Name
- Appliance Configuration Manager IP Address/Hostname
- ESXi IP Address/Hostname
- NTP server IP Address/Hostname


After you enter the IP addresses, you must confirm the changes that you have made. To confirm the changes, perform the following actions.

 **Note:** Network configuration is a one-time activity, and once configured you cannot modify the configuration. To modify the configuration, you must contact the Customer Support team.

- a. In the **Network Configuration** dialog box, click **Yes** to apply the settings.

The Network Configuration progress page is displayed.

- b. Click **No** to discard the changes.

 **Note:** If the network configuration fails, click **Retry** to revert the changes.

After the configuration is completed the system logs out, and you are redirected to the newly configured ACM IP Address. You must log in to the ACM UI using your username and password.

 **Note:** If the PS team is installing or configuring the appliance skip steps 7 through 14.

7. In the Dell EMC Secure Remote Services configuration for Integrated Data Protection Appliance page, perform the following actions.
 - a. Enter the **SRS Gateway IP**.
 - b. Enter the online support credentials in the **Username** and **Password** fields.
 - c. Click **Configure**.

The IDPA Appliance configuration page is displayed.

Note: If you want, you can skip the Secure Remote Services configuration and configure it from the ACM dashboard later.

8. In the IDPA Appliance configuration page, perform the following actions.

Note: Ensure that you click the prerequisites link available on the **Welcome** page and read them before you continue.

- a. In the **Welcome** page, select the **Optional components** that you want to install in the configuration and click **Next**.

Note: The system automatically downloads the licenses for **Protection Storage**, **Backup Server**, and **Reporting and Analytics** point products if you are connected to the network with an Internet connection. For more information about In-product activation, see [In-product activation](#) on page 46

Note: If you are not connected to the network or the licenses are not downloaded from the ELMS server, click **Browse** to locate and upload the licenses manually. For more information about manually activating the licenses, see [Manual activation](#) on page 46

Note: The system validates the license file with the following checks.

- The maximum storage capacity for the appliance cannot be more than 24 TB (appliance with 8 TB to 24 TB capacity) and 96 TB (appliance with capacity of 24 TB to 96 TB) based on the appliance you have.
- The license file should not have the hash (#) character.
- The license must be in multiples of 4 TB.

- b. Click **Next**.

- c. In the **General settings** page, perform the following actions.

- a. Select the **Time zone** from the list.


- b. Enter the IP address in the **SMTP server** and **SNMP server** fields.

- c. Select and enter the IP address in the **Separate Management Network IP address range (11)** field.

Note: If you have configured the , enter the IP addresses in the **IP address range (9)** and **IP address range (3)** fields in the **Management network settings** and **Backup network settings** sections respectively. For more information about manually configuring the ACM, see [Configure the ACM manually for Separate management networks](#).

Note: The system automatically assigns 11 IP addresses in chronological order that is based on the IP address that you enter to configure the other components of the

appliance. For example, if you enter 10.200.1.10 the system automatically generates a range of IP address from 10.200.1.10 to 20.

 **Note:** If you do not select the **IP address range** check box, you must manually configure and enter the IP addresses in the other sections. See, Step 9.


d. Click **Validate**.

The system validates the availability of the IP addresses and allocates them to the IDPA components. To view the list of IP addresses allocated to the individual components, hover on the green check mark.


e. Click **Next**.

The **Customer information** settings page is displayed.

9. You can configure the settings manually if you have not selected the **Separate Management Network** check box. To configure the settings manually, perform the following actions.
 - a. In the **Protection storage configuration** page, under the **Data network** section, enter valid IP addresses for **Backup IP 1 address** and **Backup IP 2 address**.
 - b. In the **Backup server** page, enter valid IP addresses in the following.
 - **Avamar server IP address** in the **Backup node** section
 - **Image Proxy IP address** in the **Integrated Data Protection Appliance backup**
 - c. In the **IDPA System Manager** page, enter the IP address in the **Server IP Address** field.
 - d. In the **Reporting and Analytics** page, enter the IP addresses in the **Application server IP address** and **Datastore server IP address** fields.
 - e. In the **Search** page, enter the IP address in the **Index Master Node IP address**.
 - f. In the **Cloud Disaster Recovery** page, enter the IP address in the **Cloud DR Add On IP address**.

 **Note:** The Reporting and Analytics, Search, and Cloud Disaster Recovery pages are displayed if you select the optional components in the **Welcome** page.

The Configuration progress page is displayed. You can view the configuration progress for each component along with the configuration progress for the appliance.


 **Note:** For more information about manually configuring the ACM after you have configured the separate management networks, see [Configure the ACM manually for Separate management networks](#).

10. In the **Customer information** settings page, enter information in the mandatory fields.
 - **Administrator email**
 - **Company name**
 - **Admin contact name**
 - **Admin contact number**
 - **Location**
 - **Site ID**
11. Click **Next**.
12. In the **Summary** page, review the information that you entered and click **Submit** to start the configuration.

13. In the **Configuration progress** page, you can perform the following actions.

 **Note:** You can perform these actions after the installation is complete.


- a. Click **Download Solution ID** to download the solution ID.
- b. Click **Download Configuration** to download the configuration.
- c. Click **Download configuration XML** to download the configuration XML file.

 **Note:** You can perform the above actions when IDPA is configured successfully.


- d. View the **Errors**, **Warnings**, and **Diagnostic report** only if the configuration fails.

14. Click **Finish**.

The IDPA Appliance is installed and deployed. You are prompted to login to the ACM dashboard. In case it take longer, refresh the browser and login to ACM dashboard.

 **Note:** If the installation fails, you can perform the following actions.

- Click **Download log bundle** to download the logs of the installation and then click **Retry** to install the critical components that have failed to install from the point the installation failed. For more information about retry installation, see [Retry installation](#) on page 39
- Click **Download log bundle** to download the logs of the installation and then click **Rollback** to review the settings, make any changes if required on the **Welcome** page and then configure the settings. Ensure that you download the logs before you rollback the installation. For more information about rolling back the installation, see [Rollback installation](#) on page 40

 **Note:** If you have selected **Optional components** such as Search, DPA, or CDRA, and if any of these components fail during installation, the configuration of the other components continues until it finishes. After the configuration process for the required components is completed, you must log in to the ACM dashboard to configure the failed components.

Retry installation

If the installation fails, you can continue from the point where the installation failed.


About this task

During the appliance deployment, if any of the critical components fail to install you can retry the installation of the component from the point where the installation failed. To retry the installation, perform the following actions.

Procedure


1. Click **Retry** on the **Configuration progress** page.

The **Retry Configuration** dialog box is displayed.

 **Note:** The ACM reverts the changes that are made to the component that failed during installation and resumes the appliance configuration.

2. Click **Yes** to continue the installation.

The **Configuration progress** page is displayed. The installation continues from the point where the installation failed.

 **Note:** If the ACM is rebooting or the ACM web service is restarting during IDPA deployment the **Retry** option is not available, you can only **Rollback** the installation.

Rollback installation

If the installation fails, you can rollback the installation and follow the wizard to set up and deploy the IDPA appliance.

Before you begin

Ensure that you click **Download log bundle** to download the logs before you start the rollback.

About this task


The rollback feature reverts the changes that are made to the appliance configuration. You can review the settings and start the appliance installation and configuration again.

To rollback the appliance configuration, perform the following actions.

Procedure


1. Click **Rollback** on the **Configuration progress** page.

The **Rollback Configuration** page is displayed.

 **Note:** The ACM reverts the changes that are made to the appliance configuration.

2. Click **Yes** to continue the installation.

The **Configuration progress** page is displayed. The system reverts all the changes that are made to the appliance.

 **Note:** You can see the details of the rollback progress of all the components on the **Configuration progress** page.

Results

After the rollback is successful, the **Configuration Welcome** page is displayed. Configure the appliance from the **Configuration Welcome** page. To configure and deploy the appliance follow Step 8 through Step 13 in the [Install and deploy](#) section.

Troubleshoot Health monitoring

After installing the IDPA Appliance if you access the Health tab and see a **Service Down - Message broker** error message, then you need to run commands on the ACM to resolve the error.

About this task

To resolve the **Service Down - Message broker** error on the Health tab, perform the following actions on the ACM.

Procedure

1. Log in to the ACM using SSH.
2. Run the following command to restart the RabbitMQ service.
3. Run the following command to check if the RabbitMQ service is running.

```
#service rabbitmq-server restart
```

```
#service rabbitmq-server status
```

4. Run the following command to restart the Data Protection web application after the RabbitMQ service starts.

```
#service dataprotection_webapp restart
```


5. Refresh the browser and verify that there are no errors on the Health tab.

Troubleshooting

This section provides information on how to troubleshoot some of the issues in IDPA.

Creating and downloading a log bundle

You can create and download a log bundle that can be analyzed or sent to customer support.

1. In the ACM dashboard, click the log bundle icon in the upper right and select **Create log bundle**.
2. On the Create log bundle dialog, select the components you want included in the log bundle and click OK.
3. When the log bundle is created, reselect the log bundle icon and select **Download log bundle**. Then specify the download location and click **OK**.

Accessing vCenter

If you need to log in to vCenter to troubleshoot an issue encountered during installation, use the user *idpauser@localos* and the common password for the IDPA. This user account has limited privileges, but has access to information that can help identify and address problems.

System Manager service status for msm-monitor and rabbitmq-server is down.

If the IDPA System Manager services **msm-monitor** and **rabbitmq-server** are reported as failed in the ACM dashboard after a fresh installation, reinstall the IDPA System Manager packages. This retains the existing configuration of IDPA System Manager. Reinstallation of IDPA System Manager is done with the same set of steps used to upgrade the System Manager, only in this case you must upgrade to the same version (18.2.0-13). For detailed steps to upgrade IDPA System Manager, refer to the topic Upgrading System Manager in the **IDPA System Manager 18.2 Administration Guide**.

Configure the DataProtection-ACM for separate management networks by using the configuration wizard

This section summarizes the configuration differences in the configuration wizard when you configure the separate management network from the backup network.

Procedure

1. In the **Network Configuration** page, select **Separate Management Network** check box, and under the **Management network settings** and **Backup network settings** section enter the IP addresses in the following fields and click **Submit**.

 **Note:** Ensure that you read the prerequisites before you configure the network settings.

- **Subnet mask**
- **Gateway IP address**
- **Primary DNS server IP address**
- **Secondary DNS server IP address**
- **Domain Name**
- **Appliance Configuration Manager IP Address/Hostname**
- **ESXi IP Address/Hostname** (only for Management network settings)

- **NTP server IP Address/Hostname** (only for Management network settings)
2. In the **General Settings** page, perform the following actions:
 - a. Select the **IP address range** in the **Management network settings** and **Backup network settings** section.
 - b. Click **Validate**.

The system validates the availability of the IP addresses and allocates them to the IDPA components. To view the list of IP addresses allocated to the individual components, hover on the green check mark.


Results

DP Advisor communicates with the Avamar storage nodes and Data Domain system over the management network. As a result, the wizard automatically assigns IP addresses from the management network, if you enabled a management network IP address range.

Configure the ACM settings manually for separate management networks

This section provides information about the configuration differences in configuring ACM manually after you have configured the separate management network from the network configuration wizard.

About this task

 **Note:** The options in the following procedure are available after you have configured the separate management network during network configuration. For more information, see [Network configuration wizard](#).

Procedure

1. In the **General Settings** page, ensure that you do not select the **IP address range** check box in the **Management network settings** and **Backup network settings** sections.
2. Click **Next**.
The **vCenter configuration** page is displayed.
3. In the **vCenter configuration** page, enter the unique IP address in the **IP address** field to configure the internal **vCenter**.
4. Click **Next**.
The **Protection Storage configuration** page is displayed.
5. In the **Protection Storage configuration** page, enter unique IP addresses under the **Protection Storage** and **Backup Network** sections for the following fields.
 - **Management Network IP address**
 - **Backup IP address1**
 - **Backup IP address 2**
6. Click **Next**.
The **Backup Server configuration** page is displayed.
7. In the **Backup Server configuration** page, enter unique IP addresses under the **Backup node** and **Integrated Data Protection Appliance backup** section for the following fields.
 - **Backup Node IP**

- **Image Proxy IP address**
 - **Backup Proxy IP address**
8. Click **Next**.
The IDPA System Manager page is displayed.
 9. In the **IDPA System Manager** page, enter the unique IP address in the **Management Network IP** field.

IDPA post installation tasks

After you install the IDPA software in your appliance, you need to complete the following tasks. This section includes the following topics.

Configure crontab for DP Advisor database backup

Create a job to backup the DP Advisor database in the crontab of the DP Advisor database VM.

About this task

Perform the following steps from the ACM.

Procedure

1. Log in to the DP Advisor database VM by using SSH.
2. Create **dbbkp** folder under **/data01**.
`mkdir -p /data01/dbbkp`
3. Create a shell script with the name **vi dbbkp.sh** with the following:

```
#!/bin/sh
#Take backup of DPA database
/opt/emc/dpa/services/bin/dpa.sh datastore export /data01/dbbkp
#Delete the files older than 3 days
find /data01/dbbkp/datastore* -type d -ctime +2 | xargs rm -rf
```

4. Run the following command to make the executable script:

```
chmod +x /data01/dbbkp/dbbkp.sh
```

5. Edit the crontab by typing the following command:

```
crontab -e
```

6. Add a line in the crontab file for the backup job.

For example, to create a job that runs daily at 7 P.M, type the following:

```
00 19 * * * /usr/bin/sh /data01/dbbkp/dbbkp.sh >> /tmp/dpabkp.log 2>&1
```

7. Save the change and exit crontab by typing the following command:

```
:wq
```

Results

The cron job creates a subfolder in the **/data01/dbbkp** directory for each backup on the DPA datastore virtual machine, which contains the backup data. For example: **data01/dbbkp/datastore-6_3_0_7-2017-04-25-1155/**

CHAPTER 5

License activation

You need a license to use IDPA. To use all the features of IDPA you need to activate the license that you have received. To activate the licenses you need to be connected to a network with an internet connection for In-product activation or you must have received the License Activation Code (LAC) letter through email during the fulfillment process to manually activate the licenses. The LAC letter includes the license authorization code that is associated with your order, instructions for downloading software binaries, and instructions for activating the entitlements online through Dell EMC Software Licensing Central.

This section provides information on the various ways in which you can activate your license.

- [In-product activation](#).....46
- [Manual activation](#).....46

In-product activation

The In-product license activation feature is available only on the DP4400 appliance. The ACM automatically downloads the licenses for **Protection Storage**, **Backup Server**, and **Reporting and Analytics** point products from the ELMS server.

Note: Ensure that the appliance is connected to a network with a working Internet connection to automatically download the licenses.

After the licenses are successfully downloaded, the **License** tab on the IDPA Configuration page is not displayed. If the licenses are not downloaded successfully during network configuration, the **License** tab is displayed on the IDPA Configuration page with a **Check online for licenses** button. You can click **Check online for licenses** to download the licenses from the ELMS server.

Note: If the system is unable to download the licenses automatically from the ELMS server, an error message is displayed, and you need to manually activate the licenses. For more information about how to manually activate the licenses, see [Manual activation](#) on page 46.

Manual activation

The manual license activation feature enables you to upload and activate the licenses that you have downloaded from the ELMS server.

Before you begin

- Ensure that you have the email with the License Authorization Code (LAC) letter that you have received during the order fulfillment process.
- The LAC letter (for initial activations, this is the serial number of the appliance) includes the license authorization code (for initial activations, this is the serial number of the appliance) that is associated with your order, instructions for downloading software binaries, and instructions for activating the entitlements online through Dell EMC Software Licensing Central. For more information, see the *Software Licensing Central Activation, Entitlements, Rehost and Regeneration Guide* on <https://community.emc.com/community/labs/tes>.

About this task

To manually activate the licenses on the IDPA configuration page, complete the following actions.

Procedure

1. In the **Welcome** page, select the optional components that you want to install in the configuration and click **Next**.
2. In the **License** page, click **Browse** on the **Protection Storage**, **Backup Server**, and **Reporting and Analytics** sections.

The **Open** dialog box is displayed.

3. Locate and select the licenses for the respective point products and click **Open**.

The licenses are activated, and a green tick appears beside **Browse**.

Results

The licenses are activated for the point products. To continue with the configuration, follow the steps from [Step 8d](#) in *Install and deploy IDPA* on page 35.

CHAPTER 6

Storage expansion

You can upgrade the storage capacity of the DP4400 appliance to 96 TB. You can expand the storage capacity in multiples of 4 TB (for the appliance with 8 TB to 24 TB capacity) up to 24 TB and multiples of 12 TB (for the appliance with capacity of 24 TB and above) up to a maximum of 96 TB.

- [Remove the front bezel to access front panel hard drives](#).....48
- [Install the expansion hard drives](#).....48
- [Install the front bezel](#)..... 50
- [Storage expansion and upgrade](#)..... 51

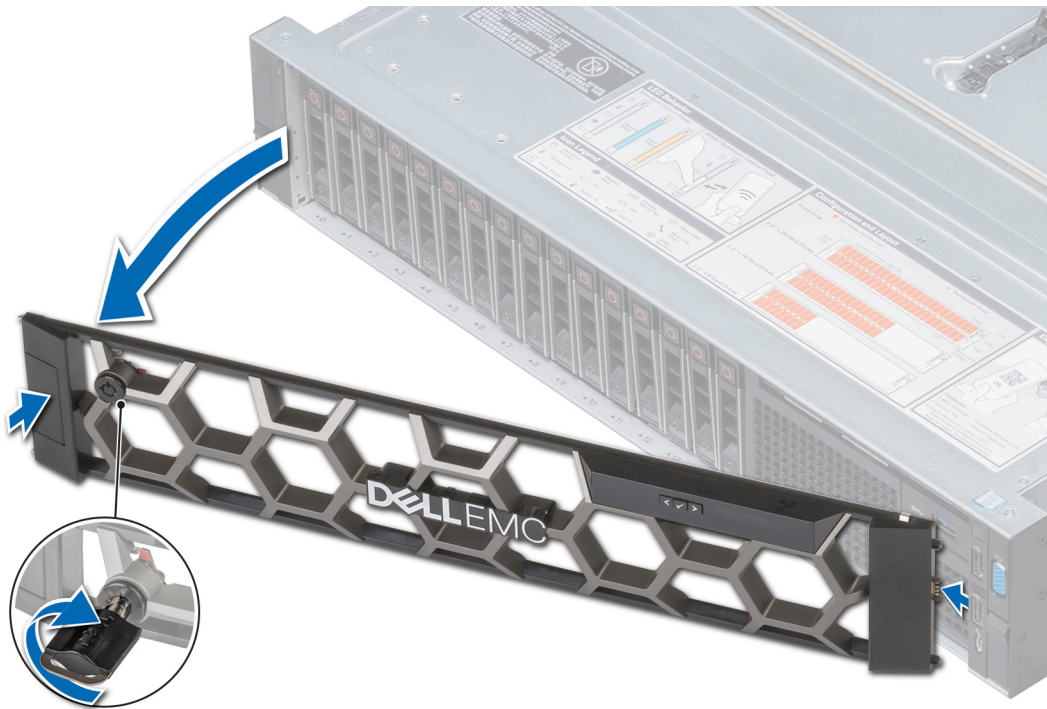
Remove the front bezel to access front panel hard drives

The procedure to remove the front bezel with the LCD panel and the front bezel without the LCD panel is the same.

Procedure

1. Unlock the bezel by using the bezel key.
2. Press the release button, and pull the left end of the bezel.
3. Unhook the right end, and remove the bezel.

Figure 17 Removing the front bezel



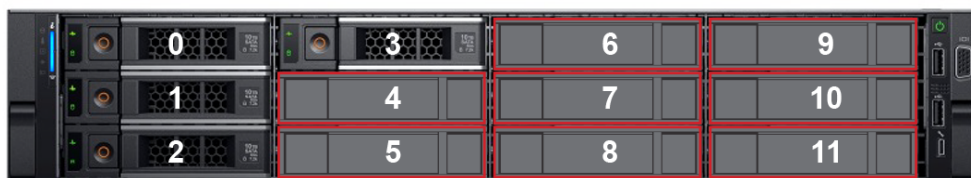
Install the expansion hard drives

About this task

Install the expansion hard drives into slots 4-11 on the front of the system.

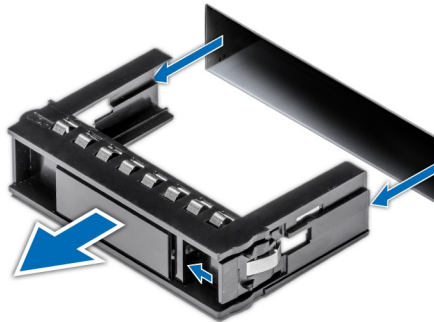
CAUTION Dell recommends that you install only the hard drives provided by Dell in the disk expansion kit.

Figure 18 Hard drive slots



Procedure

1. Remove the hard drive blank.

Figure 19 Removing a drive blank

2. Press the release button on the front of the hard drive to open the release handle.

Figure 20 Opening the release handle

3. Insert the hard drive into the hard drive slot and slide until the hard drive connects with the backplane.
4. Close the hard drive release handle to lock the hard drive in place.

Figure 21 Installing a hard drive

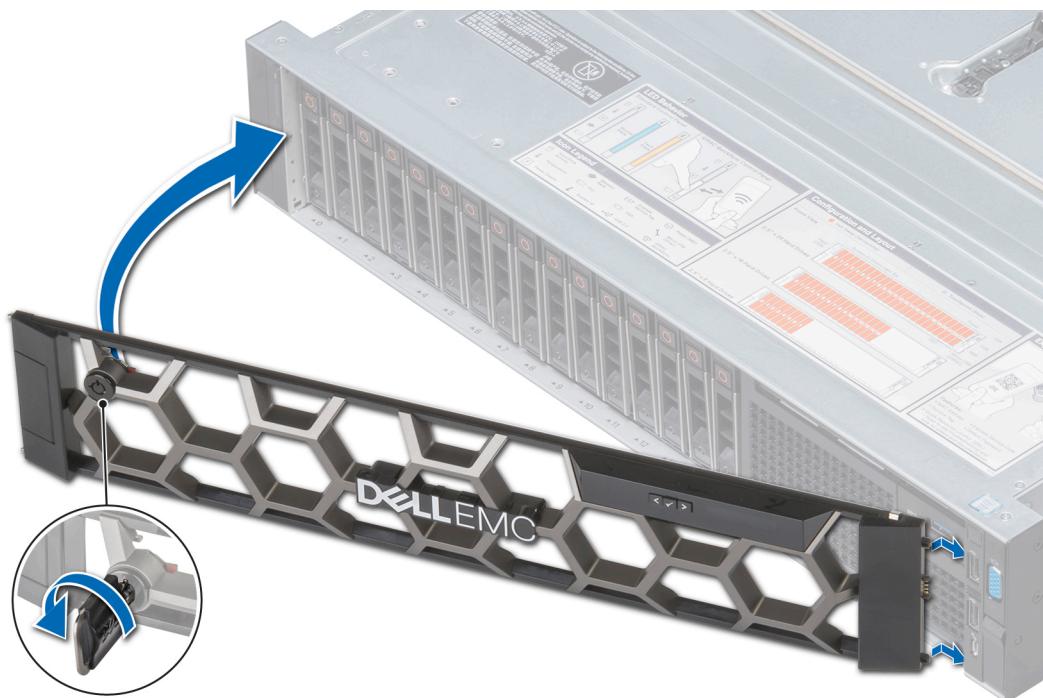


Install the front bezel

The procedure to install the front bezel with the LCD panel and the front bezel without the LCD panel is the same.

Procedure

1. Align and insert the right end of the bezel onto the system.
2. Press the release button and fit the left end of the bezel onto the system.
3. Lock the bezel by using the key.

Figure 22 Installing the front bezel

Storage expansion and upgrade

You can expand the storage capacity by obtaining the required additional licenses through ELMS (an electronic license management system). The storage capacity of the DP4400 appliance with a capacity of 8 TB to 24 TB can be expanded beyond 24 TB by adding disk drives to the appliance using the disk expansion kit. Upgrade the appliance to version 2.4.1 using the ACM and then install the disk drives. If you have an appliance with 8 TB to 24 TB capacity which is on version 2.4.1, you can expand the storage capacity using the disk expansion kit.

Before you begin

The following prerequisites are required when expanding the DP4400 (8 TB to 24 TB) model beyond 24 TB using the disk expansion kit:

- Ensure that you have IDPA version 2.4.1.
- Ensure that the storage capacity in the new license is not less than the capacity in your current license.
- If the original DDVE license includes license for cloud tier, then the new storage expansion license must include the license for the cloud tier.

About this task

To expand the storage capacity of the appliance, perform the following actions.

Procedure

1. Log in to the ACM UI.
The ACM dashboard **Home** page is displayed.
2. Click the **Gear** icon and select **Expand storage** in the **Protection Storage** panel.
The **Storage expansion** window is displayed.

3. Click **Browse** on the **License file** field in the **Protection Storage** section.
The **Open** dialog box is displayed.
4. Select the Data Domain Virtual Edition (DDVE) license file for disk expansion that you have downloaded.
Note: If the license is valid, a green tick is displayed.
5. Select the **I agree that the expansion operation overwrites data on the additional 8 drives** check box to overwrite the existing data on the new drives.
Note: This check box is available only when you are expanding your storage capacity from the 8 TB - 24 TB appliance beyond 24 TB.
6. Select the **I agree to restart Protection Storage server** or **I agree to restart Protection Storage file system** check box to restart the protection storage server for adding the SCSI controller and restart file system service to enable the cloud feature during the storage expansion.
Note: This option is applicable only when you are expanding your storage capacity from the 8 TB - 24 TB appliance beyond 24 TB.
Note: The **I agree to restart Protection Storage server** or **I agree to restart Protection Storage file system** check box is not displayed when the SCSI controller was added previously and if there is no change in the cloud tier enabled status.
Note: The **I agree to restart Protection Storage file system** check box enables the cloud feature on the protection storage server during storage expansion.
Note: The **I agree to restart Protection Storage server** check box adds the SCSI controller to the protection storage server and to change the cloud tier enabled status (if applicable) during the storage expansion.
Note: Ensure that there is no active I/O operation running on **Protection Storage** server.
7. Click **Expand**.
The **Storage expansion** window displays the progress bar. You can see the details of the storage expansion.
8. Click **Finish**.
The ACM dashboard **Home** page is displayed.

Results

The storage capacities are updated in the **Total backup storage**, **Available backup storage**, and the **Cloud Storage** fields in the **Protection Storage** panel.

- Note:** The **Cloud Storage** field is updated if you have added the cloud feature during storage expansion.
- Note:** The check boxes in [Step 5](#) and [Step 6](#) are displayed if you are expanding the storage capacity of the appliance beyond 24 TB.

CHAPTER 7

Install the IDPA post-installation patch on DataProtection-ACM

Perform the following steps to install a postinstallation patch:

Before you begin

You must go through the readme file available along with this postinstallation patch to verify if there are any preinstallation tasks that you must perform before applying this postinstallation patch.

Procedure

1. Go to https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance website to verify if any postinstallation patches are available for your version of IDPA. If any postinstallation patch is available, download it to your local folder.


Information similar to the following is displayed when you go to the https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance website to download the postinstallation patch:

`Idpa_post_update_N.N.N.nnnnnn.tar.gz`

Where:

- *N.N.N* is the latest postinstallation patch version.
- *nnnnnn* is the build number.

2. Copy the `Idpa_post_update_N.N.N.nnnnnn.tar.gz` file to `/data01/upgrade` location on the ACM.

 **Note:** Ensure that only the postinstallation patch file exists in this folder and no other packages exist. If there are any other install files in this folder, you must delete them before installing the patch.


3. Ensure that you have the executable permission for the install package that you copied to the `/data01/upgrade` directory. If you do not have the executable permission, run the `chmod 644 Idpa_post_update_<version.build number>.tar.gz` command to obtain the permission.

4. Log in to the ACM and click the **Upgrade** tab.


The latest upgrade package file is automatically detected and is displayed in **Upgrade Binary Location**.

5. Click **Extract**.

The browser redirects to `https://<acm_configured_public_ip>:9443` with a changed port number.

 **Note:** The validation process takes approximately 15 minutes, and the ACM can time out while waiting. To resume the session, you must login in once again.

The system validates the following:


- VLAN status
 - Validates if it can connect to all 3 ESXi servers (Applicable for DP5300, DP5800, DP8300, and DP8800 models only).
 - Validates the number of vSAN clusters (Applicable for DP5300, DP5800, DP8300, and DP8800 models only).
 - Validate if the vSAN datastore is greater than 16.2 TB (Applicable for DP5300, DP5800, DP8300, and DP8800 models only).
 - Validates the connection to all components.
 - Validates the license status.
 - Validates if Avamar services are running.
 - Validates to ensure that no backup jobs are running on Avamar.
 - Validates if the DD capacity used is less than 85%.
 - Avamar checkpoint validation
 - vSAN requirements (Applicable for DP5300, DP5800, DP8300, and DP8800 models only):
 - Checks for inaccessible vSAN objects or virtual machines.
 - Checks if the vSAN cluster requires a disk data rebalance.
 - Checks if a component rebuilding task is currently in progress in the vSAN cluster.
 - Checks for sufficient disk space requirements (30%).
 - ESX upgrade prerequisites:
 - Requires valid connection points to all the required ESXi servers.
 - Requires that the applicable ESXi servers are in maintenance mode.
 - Requires that the VCSA version is higher than ESXi version. In case, there is a major upgrade to VCSA, then the private IP address of the VCSA, 192.168.100.108 should not be in use.
-  **Note:** The private IP address of the VCSA, 192.168.100.108, is only required temporarily during the upgrade process.


A table displays the current version, new version, and type (for example, major, patch) of each component for which an upgrade is available.

If the validation is not successful, check the errors that are displayed when you hover over the exclamation mark. Resolve all the errors and then click **Extract**.

6. Click **Upgrade**, type the ACM password, and click **Authenticate**.
7. To start the upgrade, click **Yes**.

The upgrade process starts.

 **Note:** The upgrade process can take five to six hours, during which all activity on the IDPA must be quiesced. The system is not accessible during parts of the upgrade.

 **WARNING** If the upgrade process is still running, do not shut down/reboot the ACM or restart the *dataprotection_webapp* service. For some reason, if you have shut down/rebooted the ACM or restarted the *dataprotection_webapp* service while the upgrade process is still running, and if you are unable to see the progress of the upgrade after the ACM is rebooted, then contact a technical support professional.

The **Upgrade Progress** displays the following:

- The ACM upgrade progress bar with the progress percentage and description of the upgrade step in progress
 - Individual component upgrade progress bar with progress percentage and description of the upgrade step in progress
8. After all the components are upgraded successfully and the overall IDPA upgrade progress bar shows 100%, click **Finish**.
 9. Click **OK** on the **Upgrade Finish** window.
 - Note:** After the upgrade is complete, there can be a scenario where Avamar is in maintenance mode and the jobs cannot be executed at that time. After Avamar comes out of the maintenance mode, the jobs are executed.
 - Note:** After the upgrade is complete, acknowledge the notification `Event ConnectEMC notification failed on the Avamar Administrator`. This notification is generated during upgrade when the MC service is disconnected.
 - Note:** After the upgrade is complete, there is a warning on vCenter about a potential vulnerable issue that is described in CVE-2018-3646. IDPA uses the ESXi version which has the fix for this vulnerability, however this fix is not enabled by default as it has severe performance impact. Refer to the *IDPA Security Configuration Guide* for more information.
 - Note:** If you have NDMP Accelerator nodes added to IDPA, you must manually upgrade the NDMP accelerator nodes. To upgrade NDMP accelerator nodes, see the *Upgrading the accelerator software* section in the *Dell EMC Avamar NDMP Accelerator for Dell EMC NAS Systems User Guide*.

The dashboard with all the products and their upgraded versions are displayed along with the newly configured ACM. If the upgrade process does not complete as expected, see [#unique_51](#).

If the upgrade for any component fails, then the upgrade process is stopped until you troubleshoot and resolve the failure. However, if there are any noncritical warnings, the upgrade process continues. These warnings must be resolved once the upgrade process is completed.

Install the IDPA post-installation patch on DataProtection-ACM

CHAPTER 8

Update the IDPA Firmware (DP4400)

This chapter describes how to update the IDPA firmware on DP4400 models.

Topics include:

• Overview	58
• Prerequisites	58
• Prepare the Environment	58
• Update the iDRAC Firmware	59
• Update the iDRAC Service Module (ISM)	59
• Perform the Required Checks on IDPA Point Products	60
• Set the VMs to enter Service Mode through ACM	62
• Update the Firmware	62


Overview

Before upgrading the IDPA software, the IDPA system must have its firmware updated to *DP4400_Firmware_Update_June2019_Package*.

The topics below describe how to update the IDPA firmware on DP4400 models for all the required IDPA hardware components, so that you can seamlessly upgrade from IDPA version 2.4 to IDPA version 2.4.1.

The DP4400 firmware update is three-stage process, which consists of the following:

- Updating the Integrated Dell Remote Access Controller (iDRAC) firmware and iDRAC Service Module (ISM).
- Performing the required checks on the IDPA point products to ensure that all activity on the IDPA is quiesced, all the services on ACM have green checkmarks, and so on.
- Updating the firmware.

 **Note:** The firmware update process takes more than two and a half hours to complete, it is recommended that you keep a four hour window to complete the process.

Prerequisites

The following are required to successfully complete the firmware update procedure, so that you can upgrade to the latest versions of IDPA:

- Obtain the latest upgrade package - Download the *DP4400_Firmware_Update_June2019_Package* zip file from the Online Support website (https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance) to your local folder, use the sha256 checksum validation process to verify its integrity, and keep it ready.
- iDRAC - Ensure that you are connected and have configured iDRAC. For information about how to connect and configure iDRAC, see the latest *Integrated Data Protection Appliance DP4400 Installation Guide* available on the Online Support website.
- ACM – Ensure that the ACM is up and running.
- ESXi server – Ensure that you have valid connection points to the required ESXi server.

Prepare the Environment

Before you begin

- Ensure that you have full administrator privileges or be a root user to perform these tasks.
- To connect to Appliance Configuration Manager (ACM) and other components, you must have an SSH client.

Procedure

1. Using an SSH client, connect to the ACM as a root user.
2. Under root, create a new directory and name the directory as *Firmware Update*.
3. From the *IDPA_R640_Firmware_Update_June2019_Package* update package that you downloaded from the Online Support website, copy the latest `dpatools-2.0.0-<xx>.rpm` file to the newly created directory (*Firmware Update*).
4. Run the following command:

```
dpatools-2.0.0-<xx>.rpm
```

5. Go to the newly created directory `/usr/local/dpatools/bin/payload`, and extract the firmware package with `tar -xvzf IDPA-2.303-2.303.tar.gz`.
6. Copy the `/usr/local/dpatools/bin/payload/VIBS/cross_oem-dell-dcism-esxi_3.4.0.1.ESX6i-live.vib` to a temporary directory on the ESXi host using root credentials and the required IP address.

For example, `scp cross_oem-dell-dcism-esxi_3.4.0.1.ESX6i-live.vib root@192.168.100.101:/tmp`.

Update the iDRAC Firmware

You must complete updating the iDRAC Firmware and ISM on all the three iDRACs and their associated ESXi hosts.

Before you begin

Ensure that you are connected to iDRAC and it is configured.

Procedure

1. In a supported web browser, type `https://[iDRAC-IP-address]` and press **Enter** to login to iDRAC.
To obtain the iDRAC IP address, connect to the ESXi host by using an SSH client and run the `enum_instances OMC_IPMIIPProtocolEndpoint root/cimv2 | grep IPv4Address` command.
The iDRAC homepage is displayed.
2. On the iDRAC **Dashboard**, verify if the latest firmware update (version 3.34.34.34) is applied. If not, you must update the iDRAC to the latest firmware version.
3. To update the iDRAC to the latest firmware version, select **Maintenance > System Update**. The **Firmware Update** page is displayed.
4. On the **Manual Update** tab, select **Local** as the file location as you will be uploading the firmware file from your local system.
5. Click **Browse** and select the **iDRAC-with-Lifecycle Controller_Firmware_3HT97_WN64_3.34.34.34_A00.EXE** file from the latest update package that you downloaded from Online Support website.
6. Click **Upload**.
After the upload is complete, the **Update Details** section displays the firmware file uploaded to iDRAC and its status.
7. Select the uploaded firmware file and click **Install** to successfully update the iDRAC firmware.

Update the iDRAC Service Module (ISM)

The latest ISM required for IDPA is 3.4.0.1.

About this task

This section provides information on how to verify and update the iDRAC Service Module. To verify and update the ISM, perform the following:

- On the ESXi host, run the following command to get the installed version of ISM.
`esxcli software version vib | grep dci`

- If the ISM is not on version 3.4.0.1, run the following command to update the ISM:

```
esxcli software vib update -v /tmp/cross_oem-dell-dcism-esxi_3.4.0.1.ESX6i-live.vib
```
- To verify that you have successfully updated the ISM and it is up and running, go to **iDRAC homepage > iDRAC Settings > Settings > iDRAC Service Module Setup**.

If the iDRAC reports that the ISM is not up and running, perform the following steps to reinstall the ISM:

Procedure

1. Stop the ISM service by running the following command:

```
/etc/init.d/dcism-netmon-watchdog stop
```

2. Wait for 30 seconds to a minute for this command to execute successfully.
3. Reinstall the ISM by running the following command.

```
/etc/init.d/dcism-netmon-watchdog start install
```


4. Verify the status of the ISM by running the following command:

```
/etc/init.d/dcism-netmon-watchdog status
```

Refresh the iDRAC settings and wait for up to 20 minutes for a successful communication between iDRAC and ISM to take place.

5. After 20 minutes, if the iDRAC reports that the ISM is not running, you must uninstall and reinstall the ISM.
 - a. To uninstall the ISM, run the `esxcli software vib -n remove dcism` command.
 - b. To re-install the ISM, run the `esxcli software vib install -v /tmp/cross_oem-dell-dcism-esxi_3.4.0.1.ESX6i-live.vib` command.
6. After you have verified that the required ISM is installed on the system and it is up and running, on the ESXi host, check if `/scratch/dell/appliance` directory exists. If it does, delete the folder by running following command:

```
cd /scratch/dell/ && rm -rf appliance
```

 **Note:** Be careful while deleting the `/scratch/dell/appliance` folder. If you are uncertain, delete this folder manually or contact Technical Support.

7. Restart the PTAgent by running the following command:

```
/etc/init.d/DellPTAgent restart.
```

Perform the Required Checks on IDPA Point Products

Perform the following checks:

- Ensure that all activity on IDPA is quiesced including the VMs.
- Make sure that all the services on ACM have green checkmarks indicating that they are all healthy, up and running, and properly configured. If any of the services are not in green, you must log on to that particular service and restart it.

Checks on Avamar Virtual Edition (AVE)

You must perform these required checks on Avamar Virtual Edition (AVE) by running the commands that are listed here.

Procedure

1. Using an SSH client, connect to the AVE.
2. Extend SSH session timeout and allow commands to survive beyond the SSH session closure, by running the following command:


```
unset TMOUT
```

3. Ensure that AVE services are up and running, by running the following command:

```
status.dpn
```

4. Ensure that no maintenance, backup, or replication activities are occurring on AVE, by running the following command:

```
mccli activity show -active
```

 **Note:** If there are any maintenance, backup, or replication activities running on AVE, then you must log in to the Avamar UI and cancel them.

5. Verify if all the AVE services are up and running by running the following command:

```
dpnctl status
```

Once this command successfully executes, an output similar to the following is displayed:

```
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up.
dpnctl: INFO: emt status: up.
dpnctl: INFO: Backup scheduler status: up.
dpnctl: INFO: Maintenance windows scheduler status: enabled.
dpnctl: INFO: Unattended startup status: disabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: ConnectEMC status: up.
dpnctl: INFO: ddrmaint-service status: up.
```

Other Recommended Checks on AVE

The following are some of the recommended checks that you can perform on AVE:

About this task

- `ddrmaint cplist` - Displays a list of checkpoints.
- `cplist -lscp` - Queries the checkpoint information from the running gsan processes on the data nodes.
- `mccli dd show-prot` - View the Data Domain system information, such as hostname, capacity, usage, stream limits, DDOS version, monitor status, cloud tier settings, and so on.
- `mccli dd show-prop` - Displays information such as, hostname, total capacity, server utilization, user name, and so on.
- `dpnctl start sched` - Starts the MCS and the scheduler.

Checks on Data Domain Virtual Edition (DDVE)

You must perform the following checks on DDVE by running the commands that are listed here.

Procedure

1. Using an SSH client, connect to DDVE.
2. Ensure that the file system is up and running, file system cleaning is not happening, and there are no critical alerts by running the following commands respectively:
 - `filesys status`
 - `filesys clean status`
 - `alerts show current`

Set the VMs to enter Service Mode through ACM

You must make the virtual machines enter the service mode through ACM before proceeding with the firmware update.

Procedure

1. Using an SSH client, connect to the ACM.
2. Set the IDPA DP4400 model into service mode through the ACM, by running the following command:

```
dpaccli -servicemode
```

Note: Once you have successfully set the VMs to enter the service mode, ensure that all the VMs are in the Service Mode by logging in to vSphere and verifying them. All the VMs except the ESXi host and the ACM will be powered off.

Update the Firmware

Procedure

1. Using an SSH client, connect to the ACM.
2. Tail the `dpaccli` log file by running the following command:

```
tail -f /usr/local/dpatools/logs/dpaccli.log
```
3. Start the firmware update process, by running the following command:

```
dpaccli -fwupdate /usr/local/dpatools/bin/payload/  
IDPA-2.300-2.300.tar.gz
```

Results

- After a system restart, you lose connectivity to the ACM.
- The firmware update packages will be scheduled and will start getting installed once the reboot is complete.
- After some time, ACM displays the services coming back online and vSphere displays all the VMs coming back online.

CHAPTER 9

Upgrade the IDPA software (DP4400)

This chapter describes how to upgrade the IDPA software on DP4400 models.

Topics include:

• Upgrade components	64
• Upgrade Prerequisites (DP4400)	64
• Upgrade the appliance software (DP4400)	65
• Upgrade Postrequisites	68

Upgrade components

This topic describes the list of core components that are required for the upgrade process.

Upgrade of the software for various core components of IDPA happens in this sequence:


1. Backup Server (Avamar), IDPA System Manager, Reporting and Analytics (Data Protection Advisor), Search, CDRA, and ACM.
2. Protection Storage (Data Domain).
3. VCSA (vCenter Server Appliance) and Compute node (ESXi).

Upgrade components:

- Backup Server (Avamar).
- IDPA System Manager.
- Reporting and Analytics (Data Protection Advisor).
- Search.
- Protection Storage (Data Domain).
- CDRA.
- ACM.
- VCSA.
- Compute node (ESXi).

Upgrade Prerequisites (DP4400)

This section provides you information about the prerequisites that you need to complete before you begin the upgrade procedure.

 **Note:** All the existing Avamar packages and the snapshots are deleted before the upgrade.

- Before proceeding with this upgrade, you must apply the Proxy Deployment Manager (PDM) Hotfix 305717 to avoid VCenter host/cluster tree returning empty during discovery. To apply the Hotfix 305717, SSH to the Avamar client with root credentials and run the following command:

```
cd /usr/local/avamar/src mv <PDM HF > /data01/avamar/repo/packages  
[Avamar GUI] Apply PDM HF.
```

For more information, see the *KB Article 529640*.

- Review the *Integrated Data Protection Appliance Release Notes* for information specific to the current release.
- If you have NDMP Accelerator nodes added to IDPA, you must manually upgrade the NDMP accelerator nodes. To upgrade NDMP accelerator nodes, see the *Upgrading the accelerator software* section in the *Dell EMC Avamar NDMP Accelerator for Dell EMC NAS Systems User Guide*.
- An upgrade should be started only during a software upgrade maintenance window. Ensure that no other maintenance or backup activity is occurring on Avamar or Avamar Virtual Edition during the upgrade process (Avamar jobs should not be running and Avamar Server status should be idle). You can check the server status by running the following command on the Avamar server:


```
admin@vdppunvm140:~/>: opstatus.dpn
```

- Ensure that you note down the Search settings before starting the upgrade procedure because as part of the upgrade, Search is also upgraded. Search upgrade comprises of deleting the old Search VM and adding the new Search VM, which will delete all the Search settings such as the custom user permissions and email notifications after the upgrade. Similarly, the LDAP settings are stored on ACM, and ACM restores the previous LDAP settings on the new Search VM after the upgrade.
- Ensure that all the ESXi passwords are synchronized with ACM. If you have changed the ESXi passwords, see *ESXi settings* under *Change passwords and synchronize components* section in the *IDPA Product Guide* to synchronize them.
- Make sure that the ACM Dashboard is not displaying any `Password out of sync` for any of the components.
- Ensure that the VCenter passwords are synchronized with ACM. If you have changed the VCenter password, see under *Change passwords and synchronize components* section in the *IDPA Product Guide*.
- Ensure that the ESXi server is up and running, by verifying on the vCenter UI.
- Ensure that Avamar and Data Domain storage consumption is less than 85 percent. Refer to *Monitoring the system with the Avamar Administrator Dashboard* and *Monitoring Data Domain system capacity* sections in the *Dell EMC Avamar Data Domain System Integration Guide* for more information.
- Disable all the backup policies through the Avamar UI. Refer to the section *Enabling and disabling a backup policy* in the *Dell EMC Avamar Administration Guide*.
- Restart MCS on Avamar before starting the upgrade process to ensure Avamar is quiesced, so that the upgrade does not fail due to Avamar being busy. To restart MCS on Avamar, login to the Avamar Utility node with SSH (ssh login credential is `admin` and the password is the common appliance password that you would have provided) by using the Avamar IP address and run the `dpnctl stop mcs` command to stop and then run the `dpnctl start mcs` command to restart the Avamar server.
- Make sure that you check the health of the vCenter before the upgrade procedure. To check the health of the vCenter, login to the vCenter Web interface. If there are any critical alerts requiring user action, you must first fix those critical alerts before starting the IDPA upgrade procedure.

Upgrade the appliance software (DP4400)


Upgrade the software for the components of IDPA from the **Upgrade** tab of the ACM.

Procedure

1. Download the upgrade package file from Online Support and use the md5sum validation process to verify its integrity.

The name of the file is in the format `IDPA_Upgrade_<version>.tar.gz`.

2. Copy the file to `/data01/upgrade` on the ACM.


 **Note:** Ensure that only the upgrade file exists in this folder and no other post or prepatch packages exist.

3. Ensure that you have the executable permission for the upgrade package that you copied to the `/data01/upgrade` directory. If you do not have the executable permission, type the `chmod 644 Idpa_Upgrade_<version>.tar.gz` command to obtain the permission.
4. Log in to the ACM and click the **Upgrade** tab.

The latest upgrade package file is automatically detected and is displayed in **Upgrade Binary Location**.


5. Click **Extract**.

After the tar.gz file is extracted a new window opens and the validations are performed.

 **Note:** The validation process takes approximately 15 minutes, and the ACM can time out while waiting. To resume the session, you must log in once again.

The system validates the following:

- VLAN status
- Validates the connection to all components.
- Validates the license status.
- Validates if Avamar services are running.
- Validates to ensure that no backup jobs are running on Avamar.
- Validates if the DD capacity used is less than 85%.
- Avamar Checkpoint validation
- Validates if the vCSA root account password is expired.
- Validates if the vCSA administrator and root user account passwords are synchronized.
- ESX upgrade prerequisites:
 - Requires valid connection points to the required ESXi servers.
 - Verify that the ESXi Server can enter and exit maintenance mode successfully before the upgrade.
 - Requires that the VCSA version is higher than ESXi version.
 - In case, there is a major upgrade to VCSA, then the private IP address of the VCSA, 192.168.100.108 should not be in use in the customer environment as it will be temporarily used by IDPA.

 **Note:** The private IP address of the VCSA, 192.168.100.108, is only required temporarily during the upgrade process.


A table displays the current version, new version, and type (for example, major, patch) of each component for which an upgrade is available.


If the validation is not successful, check the errors that are displayed when you hover on the exclamation mark. Resolve all the errors and then click **Revalidate**. If you want to cancel the upgrade and return to the ACM dashboard, click **Cancel**.

6. Click **Upgrade**, type the ACM password, and click **Authenticate**.

7. To start the upgrade, click **Yes**. To cancel the upgrade, click **No**.

The upgrade process starts. The ACM also undergoes an upgrade which results in users getting logged out of ACM.

 **Note:** The upgrade process can take five to six hours, during which all jobs on the IDPA must be quiesced. The system is not accessible during parts of the upgrade.

 **Note:** If the upgrade process is still running, do not shut down/reboot the ACM or restart the *dataprotection_webapp* service. For some reason, if you have shut down/rebooted the ACM or restarted the *dataprotection_webapp* service while the upgrade process is still running, and if you are unable to see the progress of the upgrade after the ACM is rebooted, then contact Customer Support.

8. Relogin to the ACM.

The **Upgrade Progress** displays the following:

- The ACM upgrade progress bar with the progress percentage and description of the upgrade step in progress.
 - Individual component upgrade progress bar with progress percentage and description of the upgrade step in progress.
9. After all the components are upgraded successfully and the overall IDPA upgrade progress bar shows 100%, click **Finish**.
10. Click **OK** on the **Upgrade Finish** window to reboot the IDPA system.

- Note:** After the upgrade is complete, there can be a scenario where Avamar is in maintenance mode and the jobs cannot be executed at that time. After Avamar comes out of the maintenance mode, the jobs are executed.
- Note:** After the upgrade is complete, acknowledge the notification `Event ConnectEMC notification failed on the Avamar Administrator GUI`. This notification is generated during upgrade when the Avamar service is disconnected.
- Note:** After the upgrade is complete, there is a warning on vCenter about a potential vulnerability issue that is described in CVE-2018-3646. See <https://kb.vmware.com/s/article/57374> and <https://kb.vmware.com/s/article/55806> for more information. IDPA uses the ESXi version which has the fix for this vulnerability, however this fix is not enabled by default as it has severe performance impact. See the *Security updates and patching* section on the *IDPA Security Configuration Guide* for more information.

Results

The following components are updated:


- Backup Server (Avamar)
- IDPA System Manager (Data Protection Central)
- Reporting and Analytics (Data Protection Advisor)
- Search
- Protection Storage (Data Domain)
- ACM
- VCSA (vCenter Server Appliance)
- Compute nodes (ESXi)

The dashboard with all the products and their upgraded versions are displayed along with the newly configured ACM. If the upgrade process does not complete as expected, see *Troubleshooting component software upgrades* in the *IDPA Product Guide*.

If the upgrade for any component fails, then the upgrade process is stopped until you troubleshoot and resolve the failure. However, if there are any noncritical warnings, the upgrade process continues. These warnings must be resolved once the upgrade process is completed to ensure a trouble-free operation of IDPA.

Upgrade Postrequisites

After you have successfully completed the upgrade procedure, ensure that you are aware/perform the following:

- To save the log files from the upgrade process, click **Download logs** when the upgrade is complete. When you have finished, click **Finish**.
- After the upgrade process is complete, you must close the browser and start a new browser session before you relogin to ACM.
- The *Upgrading proxies* section of the *Avamar for VMware User Guide* provides instructions for upgrading the Avamar proxies. The upgrade must be performed on each Avamar proxy in the environment.
 -  **Note:** Verify if the old Avamar proxy VMs still exist in your vCenter, and if they do, delete them from your vCenter after they are successfully replaced by the upgraded Avamar proxy VMs. To completely delete the old Avamar proxy VMs, click the **Delete from disk** option.
- If the upgrade operation fails and if you attempt to upgrade again after two or three days using the **Retry** button, the upgrade operation fails with a message `No validated checkpoint found`. For more information on this, see the Knowledge Base article [535533](#).

CHAPTER 10

Additional resources

- [Document references for IDPA](#).....70
- [IDPA training resources](#).....70

Document references for IDPA

The IDPA documentation set includes the following publications:

- *Integrated Data Protection Appliance DP4400 Installation Guide*
Instruction for installing the IDPA DP4400 hardware and software.
- *Integrated Data Protection Appliance Getting Started Guide*
Explains how to perform initial IDPA configuration tasks and how to get started with basic functionality like backup and restore.
- *Integrated Data Protection Appliance Product Guide*
Provides the overview and administration information about the IDPA system.
- *Integrated Data Protection Appliance Release Notes*
Product information about the current IDPA release.
- *Integrated Data Protection Appliance DP4400 Service Procedure Guide*
Procedures for replacing or upgrading hardware components of the IDPA.
- *Integrated Data Protection Appliance Security Configuration Guide*
Information about the security features that are used to control user and network access, monitor system access and use, and support the transmission of storage data.
- *Integrated Data Protection Appliance Software Compatibility Guide*
Information about software components and versions that are used in the IDPA product.

IDPA training resources

Video walkthroughs, demonstrations, and explanations of product features are available online.

You can obtain additional IDPA training and information at <https://education.emc.com>.

INDEX

A

ACM manual settings 42
audience 6

C

Capacity 47, 51
Crontab 43

D

Deploy IDPA 35
Deploy IDPA Appliances 35
DP Advisor 43

E

Expansion 47, 51

H

Health error 40
Health tab 40

I

Install IDPA 25, 35
Introduction 5

L

License activation 45, 46

N

Network configuration 33
Network Validation Tool 10
NVT 10

P

postinstallation 53
Postrequisites 68
Preinstall IDPA 21, 27, 28
Preinstallation 9
Prerequisites 64

R

requirements 9
Retry installation 39
Rollback installation 40

S

Scope 6
Secure Remote Services 30
separate backup network 41
Separate management network 42

Storage 47, 51

Storage expansion 47, 51

T

Troubleshoot 40
Troubleshoot health 40

U

Upgrade 64, 68
 critical components 64
 non-critical components 64
Upgrade DP4400 64

