White Paper

Dell EMC PowerProtect DP Series Appliance: Configuration Best Practices

PowerProtect DP Series Appliance version 2.7

Abstract

This guide provides best practices for deploying and configuring the PowerProtect DP Series Appliance.

January 2022

H18637.1

Revisions

Date	Description
January 2021	Initial release for IDPA version 2.6
January 2022	Updated release for PowerProtect DP Series Appliance version 2.7

Acknowledgments

Author: Sandeep Rajagopal

Table of contents

Executive summary

This guide provides best practices for deploying and configuring the PowerProtect DP Series Appliance (formerly IDPA).

As part of an effort to improve its product lines, Dell Technologies periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware that are currently in use. The product release notes provide the most up-to-date information about product features.

Contact a technical support professional for assistance with product functionality.

Audience

The information in this publication is intended for customers who are responsible for planning, implementing, administering, or auditing security controls in environments that contain PowerProtect DP Series Appliance solutions. The primary audience is Customer Service (CS) and remote Professional Services (PS) engineers.

Product naming conventions and terminology changes

The following table describes the recent name and terminology changes to IDPA or the PowerProtect DP Series Appliance starting with version 2.7.

Table 1 Product naming conventions and terminology changes

Existing product or component name	New name or terminology
Virtual Machines	Services
ESXi	Hypervisor
vSphere	Hypervisor Platform
vCenter/vCSA (VM)	Hypervisor Manager
vCenter service daemon	Hypervisor Manager Service Daemon
vSAN	Storage Pool
ACM (VM)	Appliance Configuration Manager (Service)
dpatools	Infrastructure Management Service
PT-Agent	Node Event Service
Avamar (VM)	Protection Software (Service)
Avamar Proxy / vProxy (VM)	VM Proxy (Service)
DD / DDVE	Protection Storage
DPC (VM)	Data Protection Central (Service)
DPA	Reporting & Analytics
(DP) Search	Search
CDRA (VM)	Cloud DR (Service)

CDRS	Cloud DR Server
Cyber Recovery (VM)	Cyber Recovery (Service)
Integrated Dell Remote Access Controller (iDRAC)	iDRAC
iDRAC Service Module (iSM) / iSM Service	iDRAC Service Module

1 Introduction

The PowerProtect DP Series Appliance (formerly IDPA) is an all-in-one, prebuilt backup appliance. It reduces the complexity of managing multiple data silos, point solutions, and vendor relationships by simplifying deployment and management. The PowerProtect DP series appliance delivers powerful, enterprise-grade data protection capabilities for small, midsize, and enterprise organizations at a low cost to protect your data.

The PowerProtect DP Series Appliance provides a solution for data protection administrators who are challenged to manage independent and disconnected applications to configure and manage data protection and storage devices.

The PowerProtect DP Series Appliance combines multiple hardware and software solutions into a single product. To help you manage the infrastructure, Data Protection Central for the PowerProtect DP Series Appliance enables administrators to efficiently manage the PowerProtect DP Series Appliance components from a single user interface. These capabilities include monitoring, reporting, analytics, and search, which help you simplify the data protection experience.

The PowerProtect DP Series Appliance provides easy configuration and integration of data protection components in a consolidated solution and offers the following:

- Simplified deployment and configuration
- Backup administration
- Deduplication
- Native cloud disaster recovery (DR) and long-term retention (LTR)
- Instant access and restore
- Monitoring and analytics
- Search
- Scalability
- Unified support

Figure 1 PowerProtect DP Series Appliance

During manufacturing, each internal component in the PowerProtect DP Series Appliance is assigned an IP address for internal connectivity and communications. During deployment, the Customer Service (CS) or Dell EMC Professional Service (PS) members configure the PowerProtect DP Series Appliance components and the Dell switch to communicate on a public network in the customer environment. This process requires configuring the management interface of each component with a customer-supplied public IP address.

The configured PowerProtect DP Series Appliance includes the following services in a storage pool:

- One virtual hypervisor manager server appliance
- One appliance configuration manager (ACM) server
- Three hypervisor hosts
- Protection Software (AVE) for DP4400 and DP5900 models only
- VM proxy
- Data Protection Central (DPC)
- Search servers (optional component):

  - Three servers for DP8400 and DP8900 models, which include two secondary index data servers and one primary index server
  - One server for the DP5900 model, which acts as both secondary index data server and primary index server.

- Reporting & Analytics servers (optional component):
  - Reporting & Analytics application server
  - Reporting & Analytics data collection agent
  - Reporting & Analytics datastore server
- Cloud DR (optional component)
- Cyber Recovery (optional component)

The Cyber Recovery (CR) solution is supported for only new installations of DP4400 and DP5900 models.

The storage pool provides the following benefits:

- Redundancy
- Failover and high availability
- Load balancing: Services are moved between hypervisor hosts automatically

2 PowerProtect DP Series appliance deployment preparation checklist

Before you begin the deployment, the CS engineer goes to the customer site, and the Solution Architect (SA) and Project Manager (PM) must complete the following requirements:

Table 2 Preparation checklist

Completed (check)	Deployment prerequisites
❑	Complete tasks in the Enterprise Delivery Platform (EDP) portal. The EDP replaces the Pre-Engagement Questionnaire (PEQ) spreadsheet. You can access the EDP portal at https://ctm.dell.com/pde/user.html while connected to the Dell network. You must have a project assigned to you to view it in the portal. After importing the services sales order and project information from FinancialForce, EDP facilitates the online planning, customer readiness checks, post-deployment verification, and customer acknowledgment through TechDirect. You must perform the following tasks in the EDP portal: • Complete site survey and site design • Verify site readiness • Perform a pre-deployment call to the customer • Generate and finalize a verification report Procedures for these tasks are described in the ProDeploy Enterprise User's Guide which is available on the EDP training site: https://dell.sharepoint.com/sites/Enable-EnterpriseDeliveryPortal/SitePages/EnterpriseDelivery-Portal.aspx
❑	When you reserve the IP addresses for the PowerProtect DP Series Appliance components, 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.
❑	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 Integrated Data Protection Appliance: How to change DNS entries in a deployed IDPA (537628).

❑	Ensure that you have a valid NTP IP address which is reachable from the appliance.
❑	If you do not have a valid IP address for DNS, NTP, and Gateway, the appliance can be configured using the ACM IP address. See Self-contained deployment (optional) section for more information.
❑	Install the network validation tool (NVT). Ensure the NVT runs successfully without errors before the onsite visit of the CS Field Engineer is scheduled.
❑	Required cables and SFP/QSFP are available according to customer uplink requirement.
❑	Engineer is aware of PowerProtect DP Series Appliance Dell switch uplink-related configuration according to customer environment. The created switch configuration file must be provided to the CS Field engineer before onsite visit.
❑	All required licenses (Protection Storage, Reporting & Analytics, and Protection Software) are present with the customer. The SA and PM must ensure that the licenses are provided to Implementation Specialist before implementation schedule.
❑	PM and SA must verify if the customer has a secure remote services gateway, and if it is on the correct version.
❑	Ensure the power requirements for PowerProtect DP Series Appliance rack are in place.
❑	Ensure that you have the following cables: ❑ USB (male) to serial (male) ❑ RJ45 (male) to serial (female) ❑ Optional, Null modem/serial: Required if you encounter a problem that requires a serial connection to the Protection Storage system. ❑ CAT6 Ethernet cable
❑	Install the Putty application on the CS Engineer laptop.

❑	Install the WinSCP application on the PS Engineer laptop.
❑	❑ Ensure you can generate an RSA Secure ID soft or hard token while you are at the customer site. ❑ Ensure you can create a Webex session for remote PS access while you are at the customer site, or ensure that the customer can set up Webex access with the remote PS engineer.
❑	Ensure that the required network and firewall ports for installing PowerProtect DP Series Appliance are open on the customer network. For more information see, *Network ports* in the *PowerProtect DP Series Appliance Security configuration guide.*
❑	If the uplink switches are Cisco, ensure that you disable the port security.

2.1 Install the network validation tool

The network validation tool (NVT) for PowerProtect DP Series Appliance runs multiple automated tests to validate the network configuration. You must run the NVT for PowerProtect DP Series Appliance from a system on the management network.

Before you install PowerProtect DP Series Appliance, network configuration must be completed for the data center. After completing all network configurations required for PowerProtect DP Series Appliance installation, install and run the Network Validation Tool to validate the network requirements for a successful deployment of PowerProtect DP Series Appliance in the data center. To download the NVT, and for more information about NVT, see https://central.dell.com/solutions/NVT-PP.

2.2 Default username and passwords on the PowerProtect DP Series Appliance

The following table summarizes the default usernames and passwords that a remote PS engineer requires to log in to and to configure the PowerProtect DP Series Appliance.

Table 3 Default usernames and passwords on the PowerProtect DP Series Appliance

Components	Username	Passwords
VMware Hypervisor hosts	root	Idpa_1234
Hypervisor Manager	vsphere.local\Administrator root	Idpa_1234
Network switch	admin	Idpa_1234

Components	Username	Passwords
Initial ACM password	root	Idpa_1234
Protection Storage system	sysadmin	Idpa_1234
Hypervisor iDRAC	root	Idpa_1234
Protection Software / NDMP accelerator	root	changeme
Protection Storage iDRAC	root	<Protection Software PSNT>
Cyber Recovery	crso	Appliance common password

Use English characters when changing any of the default passwords.

Ensure the password meets the following criteria:

- Maximum of 20 characters
- Minimum of nine characters
- Must not start with a hyphen (-)
- Contains at least one uppercase and one lowercase letter
- Contains at least one number
- Must not include common names and usernames like root or admin
- Contains at least one special character, such as:
  - Period (.)
  - Hyphen (-)
  - Underscore (_)

2.3 License activation

You must have a license to use the PowerProtect DP Series Appliance. To use all features of PowerProtect DP Series Appliance, you must activate the license that you have received.

To activate the licenses, you must 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.

2.3.1 In-product activation

The in-product license activation enables the ACM to automatically download the licenses for **Protection Storage**, **Protection Software (Backup Server)**, and **Reporting and Analytics** products from the ELMS server.

Note: Ensure 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 **PowerProtect DP Series Appliance Configuration** page is not displayed. If the licenses are not downloaded successfully during the network configuration, the License tab is displayed on the **PowerProtect DP Series Appliance** Configuration page with a **Check online for licenses** button. Click **Check online for licenses** to download the licenses from the ELMS server.

Note: In-product license activation is not supported in the following cases:

- On a IPv6 enabled network
- When ACM is being used as DNS

Note: If the system is unable to download the licenses automatically from the ELMS server, an error message displays, and you must manually activate the licenses.

2.3.2 Manual activation

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

The following are the prerequisites:

- Ensure that you have the email with the License Authorization Code (LAC) letter that you received during the order-fulfillment process.
- The LAC letter includes the license authorization code (for initial activations, this letter is the serial number of the appliance) that is associated with your order. The letter also includes 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://www.dell.com/support/contents/en-us/article/product-support/self-support-knowledgebase/software-and-downloads/software-licensing-central-documentation

To manually activate the licenses on the **PowerProtect DP Series Appliance configuration** page, complete the following actions.

1. In the **Welcome** page, select the optional components that you must install in the configuration, and click **Next**.

Note: If you have selected IPv6 as your network, the optional components Search and Cloud DR are not available to install as they do not support IPv6-enabled networks.

2. In the License page, complete the following steps for each section (Browse on the **Protection Storage, Protection Software, and Reporting and Analytics**).

    a. Click the license section. The **Open** dialog box is displayed.
    b. Select the license for the respective product and click **Open**.

The licenses are activated, and a green checkmark appears next to **Browse**.

3 Network connectivity overview

The following tables detail the IP addresses required by PowerProtect DP Series Appliance for various components. These addresses can be assigned either as a range of addresses or as individual, noncontiguous addresses. Using a range is the preferred method because it simplifies the assignment and reduces the chance for errors while you enter the IP addresses. When you use a range of IP addresses during the PowerProtect DP Series Appliance configuration, the IP addresses are assigned in a standard order.

The following tables are separated to provide model-specific information about the IP addresses that must be allocated to a component.

3.1 IP address requirements for DP4400

The following table provides the list of IP addresses required for DP4400.

Note: The number of IP addresses required in the IP address range assignments table may vary based on the optional components you have selected.

Table 4 IP address requirements.

Number of IP addresses required	Component	DNS entry required
1	Appliance Configuration Manager	Yes
1	PowerProtect DP Series Appliance Hypervisor	Yes
1	PowerProtect DP Series Appliance Hypervisor Manager	Yes
1	Protection Storage (management)	Yes
2	Protection Storage (backup)	No
1	Protection Software	Yes
1	Protection Software internal proxy	Yes
1	Data Protection Central	Yes
2	Reporting & Analytics (optional)	Yes
1	Search (optional)	Yes
1	Cloud DR (optional)	Yes
1	Cyber Recovery (optional)	Yes

Table 5 IP address assignments

Components	Number of IPs			Description
	Single network	Separate networks (optional)		
		Management	Backup	
Appliance Configuration Manager	1	1	0	Appliance Configuration Manager (Service)
Hypervisor	1	1	0	Hypervisor
Hypervisor Manager	1	1	0	Hypervisor Manager
Protection Software	1	1	0	Protection Software (AVE)
Protection Software internal proxy	1	1	1	Protection Software internal proxy
Protection Storage	1	1	0	Protection Storage (Management)
Protection Storage	2	0	2	Protection Storage (backup)
Data Protection Central	1	1	0	Data Protection Central
Reporting & Analytics (Optional)	2	2	0	Reporting & Analytics (Application/ Datastore Service)
Search (optional)	1	1	0	Search (Index Primary Node Service)
Cloud DR (optional)	1	1	0	CDRA (Service)
Cyber recovery (optional)	1	1	0	Cyber recovery (Service)

3.2 IP address requirement for DP5900

The following table provides the list of IP addresses required for DP5900.

Note: The number of IP addresses required in the IP address range assignments table may vary based on the optional components you have selected.

Table 6 IP address requirements.

Number of IP addresses required	Component	DNS entry required
1	Appliance Configuration Manager	Yes
3	PowerProtect DP Series Appliance Hypervisor	Yes
1	PowerProtect DP Series Appliance Hypervisor Manager	Yes
1	Protection Storage (management)	Yes
4	Protection Storage (backup)	No
1	Protection Software	Yes
1	Protection Software internal proxy	Yes
1	Data Protection Central	Yes
3	Reporting & Analytics (optional)	Yes
1	Search (optional)	Yes
1	Cloud DR (optional)	Yes
1	Cyber Recovery (optional)	Yes

Table 7 IP address assignments

Components	Number of IPs			Description
	Single network	Separate networks (optional)		
		Management	Backup	
Appliance Configuration Manager	1	1	0	Appliance Configuration Manager (Service)
Hypervisor Host 1	1	1	0	Hypervisor
Hypervisor Host 2	1	1	0	Hypervisor
Hypervisor Host 3	1	1	0	Hypervisor
Hypervisor Manager	1	1	0	Hypervisor Manager
Protection Software	1	1	0	Protection Software (AVE)

Protection Software internal proxy	1	1	1	Protection Software internal proxy
Protection Storage	1	1	0	Protection Storage (Management)
Protection Storage	4	0	4	Protection Storage (backup)
Data Protection Central	1	1	0	Data Protection Central
Reporting & Analytics (Optional)	1	1	0	Reporting & Analytics (Application Service)
Reporting & Analytics (Optional)	1	1	0	Reporting & Analytics (Datastore Service)
Reporting & Analytics (Optional)	1	1	0	Reporting & Analytics (Agent Service)
Search (optional)	1	1	0	Search (Index Primary Node Service)
Cloud DR (optional)	1	1	0	CDRA (Service)
Cyber recovery (optional)	1	1	0	Cyber recovery (Service)

3.3 IP address requirement for DP8400 and DP8900

The DP8400 requires a total of 13 IP addresses which includes one management IP and five backup IP addresses for Protection Storage.

The DP8900 requires a total of 14 IP addresses which includes one management IP and six backup IP addresses for Protection Storage.

For more information about the network and firewall ports that are used in PowerProtect DP Series Appliance, see *Network ports section* in the *PowerProtect DP Series Appliance Security Configuration Guide*.

Table 8 IP address requirements.

Number of IP addresses required	Component	DNS entry required
1	Appliance Configuration Manager	Yes
3	PowerProtect DP Series Appliance Hypervisor	Yes
1	PowerProtect DP Series Appliance Hypervisor Manager	Yes
1	Protection Storage (management)	Yes
6	Protection Storage (backup)	No
1	Protection Software	Yes
1	Protection Software internal proxy	Yes
1	Data Protection Central	Yes
3	Reporting & Analytics (optional)	Yes
3	Search (optional)	Yes
1	Cloud DR (optional)	Yes

Table 9 IP address assignments.

Components	Number of IPs			Description
	Single network	Separate networks (optional)		
		Management	Backup IP	
Appliance Configuration Manager	1	1	0	Appliance Configuration Manager (Service)
Hypervisor Host 1	1	1	0	Hypervisor
Hypervisor Host 2	1	1	0	Hypervisor
Hypervisor Host 3	1	1	0	Hypervisor
Hypervisor Manager	1	1	0	Hypervisor Manager
Protection Software	1	1	0	Protection Software
Protection Software internal proxy	1	1	1	Protection Software internal proxy
Protection Storage	1	1	0	Protection Storage (Management)
Protection Storage	6	0	6	Protection Storage (backup)

Data Protection Central	1	1	0	Data Protection Central
Reporting & Analytics (optional)	1	1	0	Reporting & Analytics (Application Service)
Reporting & Analytics (optional)	1	1	0	Reporting & Analytics (Datastore Service)
Reporting & Analytics (optional)	1	1	0	Reporting & Analytics (Agent Service)
Search (optional)	1	1	0	Search (Index Primary Node Service)
Search (optional)	1	1	0	Index Data Node 1
Search (optional)	1	1	0	Index Data Node 2
Cloud DR (optional)	1	1	0	CDRA (Service)

4 Sizing overview

Sizing the PowerProtect DP Series Appliance is the most important activity to complete before the installation process. Sizing the appliance provides the system administrator with a holistic view of the compute, bandwidth, and storage consumption for the workloads that the customer wants to protect using PowerProtect DP Series Appliance.

To facilitate the sizing process, the Customer Support (CS) and Professional Service (PS) team members can use the Solution Builder tool (Dell Technologies internal access only). This tool can generate the sizing report for the PowerProtect DP Series Appliance based on customer inputs and workloads that would be protected using PowerProtect DP Series Appliance.

4.1 Scalability overview

The PowerProtect DP Series Appliance models are designed to be scalable so it can scale up with ever-changing needs. See the section "*Expanding storage capacity"* in the *Dell EMC PowerProtect DP Series Appliance Installation Guide* for more information about how to add storage capacity.

- For the DP4400S 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. By adding the disk expansion kit, you can also 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. You can expand the capacity up to a maximum of 96 TB.
- You can also expand the storage capacity of the DP5xxx and DP8xxxx models. For more information related to storage capacity expansion, see the section *"Storage capacity"* in the *Dell EMC PowerProtect DP Series Product Guide.* The following table details the configuration for PowerProtect DP Series Appliance models.

Table 10 Configuration for PowerProtect DP Series appliance model

Model	Minimum capacity	Maximum capacity
DP4400	8 TB	24 TB
	24 TB	96 TB
DP5900	96 TB	288 TB
DP8400	192 TB	768 TB
DP8900	576 TB	1056 TB

5 Installation overview

This white paper is designed for personnel who install, configure, and maintain the PowerProtect DP Series Appliance DP4400. It is assumed that the DP4400 appliance is already racked and stacked in the customer's data center before you proceed with the steps in this section.

Note: This procedure is applicable for **the PowerProtect DP Series Appliance DP4400 model**. All other models are preconfigured and installed by the Professional Services (PS) team.

5.1 Connect the system to the network

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

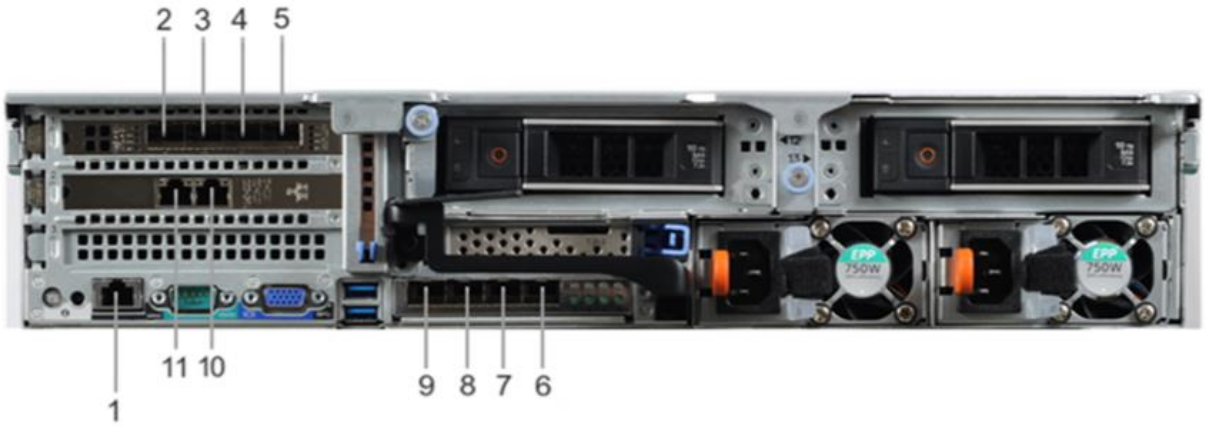

Figure 2 DP4400 network and iDRAC connections

Steps:

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.

5.1.1 DP4400 ports

Based on the above diagram, the following table details each type of port and its associated callout number.

Table 11 DP4400 ports

Callout number	Type of port
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 (required)
11	1 GbE (unused)

Notes:

- Ports 2 and 9 are for vSwitch0 network team. Ports 3 and 8 are for vSwitch1 network team and are used during appliance configuration.
- 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.
- Switch MTU should be 1528 or higher. Jumbo frames are not supported. PowerProtect DP4400 sometimes may fail with the following error message:

  ```
  Adding back-end storage. Exception occurred while executing Avamar
  integration task. Failed to add Data Domain as Avamar back-end storage.
  ```

- To resolve this problem, you must either remove the MTU or increase it to 1518 or higher. See KB Article https://www.dell.com/support/kbdoc/en-us/000053472/dp4400-deployment-failed-at-66-exception-in-adding-data-domain-as-backend-storage-for-avamar-timeout-adding-back-end-storage-exception-occurred-while-executing-avamar-integration-task-failed-to-add-data-domain-as-avamar-back-end-storage for more information.

5.1.2 Connect power cables and power on system

This topic describes how to connect the power cables and power on the system.

Note: Use an uninterruptible power supply (UPS) to protect against data loss caused by unplanned power outages.

Steps:

1. Connect the power supply units to the rack.

   The system may not power on automatically after plugging in the AC power cables. The system identification button is on the back of the chassis, and the lower-left 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-side control panel at the front of the chassis to power on the system.

Figure 3 Power button

5.1.3 Configure iDRAC

You must configure the iDRAC for system upgrade and maintenance operations. Also, the PowerProtect DP Series Appliance supports the use of iDRAC to change security settings and enables you to remotely power the system on.

Prerequisites: 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. Making changes to these will impact the system functionality. Contact Dell Support if changes are required in any of these areas.

Steps:

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: The default password is **Idpa_1234**.

5.2 IP address requirements

Now that the PowerProtect DP Series Appliance is all powered up, there is one last step that we would need to complete before we install the PowerProtect DP4400 software. This step ensures we have all IP addresses required by PowerProtect for the various components for a seamless deployment experience.

About this task: When you reserve the IP addresses, you must assign the IP addresses to a fully qualified domain name (FQDN) in the DNS server. The following is the supported format for a FQDN:

Supported characters:

- Upper- or lower-case letters (A-z, a-z)
- Numbers (0-9)
- Hyphen (-)
- Must not exceed the 255-character limit.
- Must not include any special characters, symbols, spaces, or punctuation other than a hyphen (-).

Labels are the strings in the FQDN which are separated by a period (.). Use a period only as a separator between labels. The following is the supported format for labels:

- Each label must start with a letter or number.
- Must not exceed the 63-character limit.
- Each label must have at least one letter.
- A label must not start or end with a hyphen (-)

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 hostnames for the point products. However, 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 the KB Article https://www.dell.com/support/kbdoc/en-us/000021476/integrated-data-protection-appliance-how-to-change-dns-entries-in-a-deployed-idpa

Ensure you have a valid NTP IP address which is reachable from the appliance.

Note: Ensure that the time difference between the NTP and Hypervisor server is no more than 10 minutes. If the time difference between the two servers is more than 10 minutes, the appliance network configuration may fail.

If there is no valid IP address for the DNS, NTP, or Gateway, the appliance can be configured using the ACM IP address. See the *Self Contained Deployment (optional)* section for more information.

When a range of IP addresses is used during the configuration, the IP addresses are assigned in a standard order. Once assigned, each IP should be registered in DNS with forward and reverse lookup entries.

A total of 13 unused IP addresses are needed **(Hint: use ping to validate)** for all components and one each for Hypervisor and ACM. Total number of IP address requirement varies according to optional component selection. iDRAC also needs an IP address.

5.3 Configure DP4400 Software

This section describes how to configure the DP4400 Software.

5.3.1 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.

Prerequisites:

- After powering on the appliance, wait 5 minutes for the startup to finish.
- Verify that the service computer is connected to the 1 GbE port (item 10 in Figure 2).
- On the service computer, record the IP address settings for the Ethernet interface that is connected to the DP4400.

Steps:

1. On the service computer, assign the static IP address **192.168.100.98** and the subnet mask **255.255.255.224** 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:

   - Username: **root**
   - Password: **Idpa_1234**

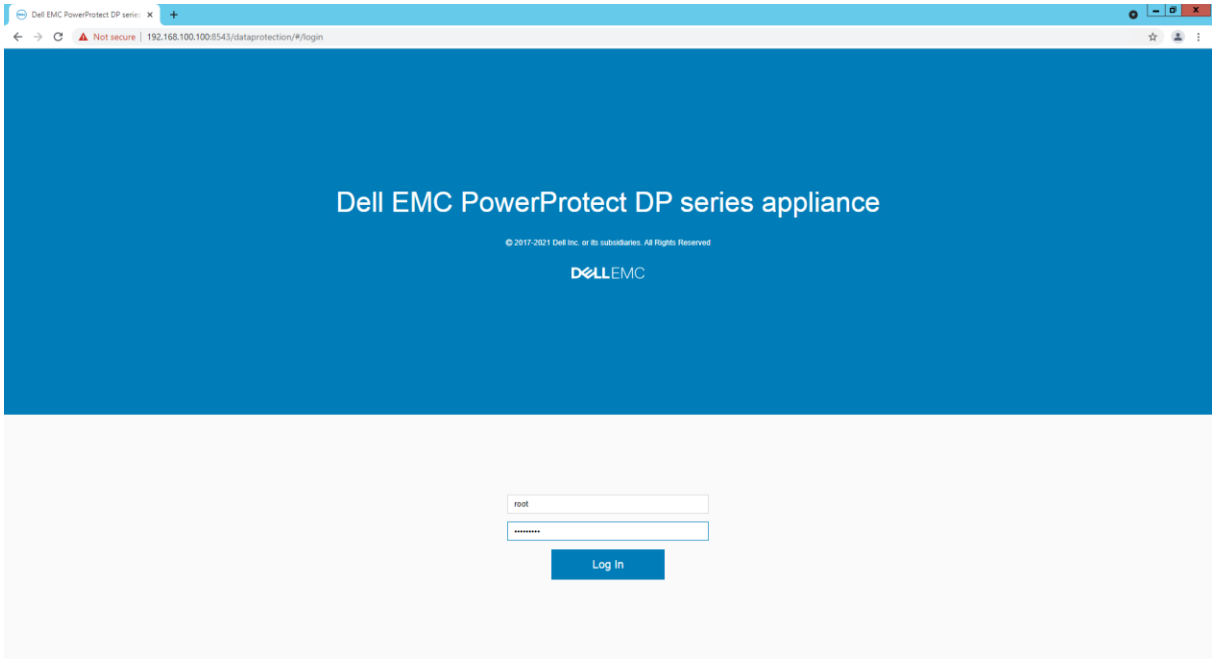

Figure 4 PowerProtect DP Series Appliance login screen.

5. After a successful login, the **Change Appliance Password** screen is displayed.
   The **Change Appliance Password** page consists of *Update Appliance Password*.

   Update Appliance Password

   This password will be assigned to all components of the appliance. It must contain 9–20 characters and include at least one of each type of supported character.

   - 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 (.).

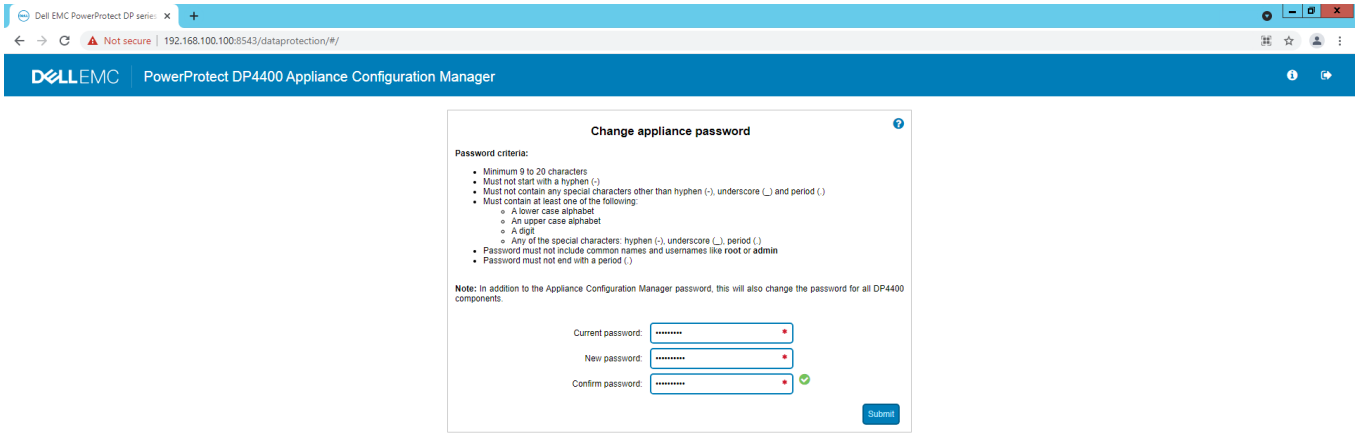

Figure 5 Change appliance password

6. Once you successfully change the passwords, the system logs you out. You must log in again with your new credentials.

7. On the End User License Agreement screen, accept the EULA.

   The Network Configuration screen is displayed.

5.4 Network configuration wizard

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

The PowerProtect DP Series Appliance supports both IPv4 and IPv6-enabled networks. Network configuration wizard will configure public network for the Appliance Configuration Manager and the Hypervisor Server.

1. Depending on the type of network you have selected (IPv4 or IPv6), provide the following information to configure the network settings:

Note: For this white paper, the PowerProtect DP Series Appliance would be configured using IPv4 Network using a single network topology.

   - **IPv4 network Subnet mask**: IP address mask that identifies the range of IP addresses in the subnet where the appliance is connected.

- **IPv6 network Prefix Length:** IP address length that identifies the range of IP addresses where the appliance is connected.
- **Appliance Configuration Manager IP Address/Hostname:** The IP address to assign to the ACM. This address is the first of the 13 IP addresses, and it is reserved for the ACM.
- **ESXi IP Address/Hostname:** The IP address to assign to the ESXi server. This address is the second of the 13 IP addresses, and it is reserved for ESXi.
- **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.
- **NTP server IP Address/Hostname:** The NTP server IP address for your network environment.

Note: If you want to configure the separate management and backup network, perform the following actions. Click **Separate Management Network** check box to configure the separate management and backup network settings.

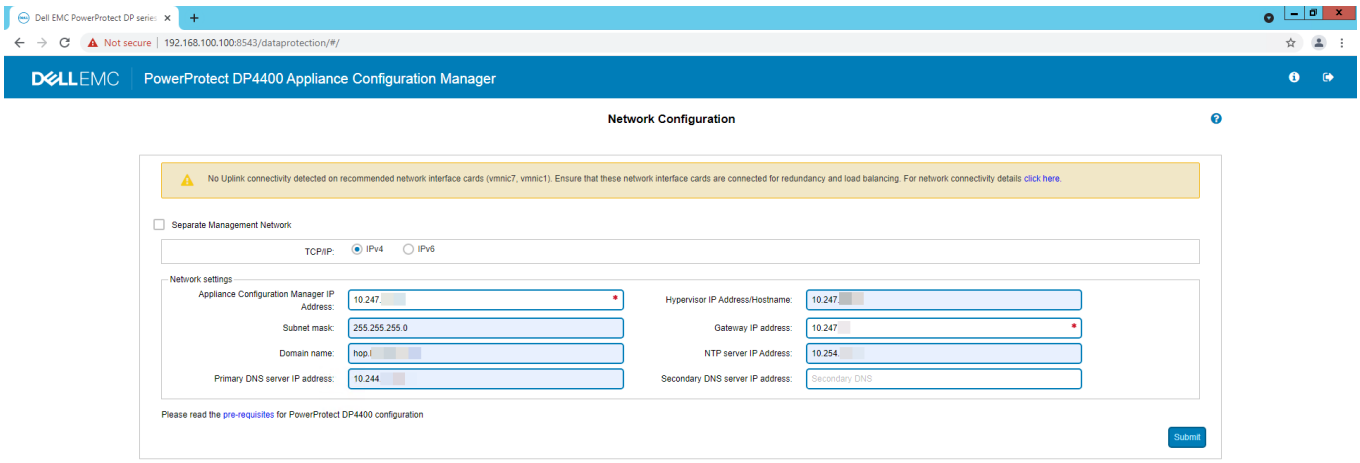

Figure 6 Initial Network configuration.

2. Click **Submit** to continue.

After you complete the previous steps, note the following:

- After you configure basic networking, the web browser automatically redirects to the ACM IP address assigned during network configuration.

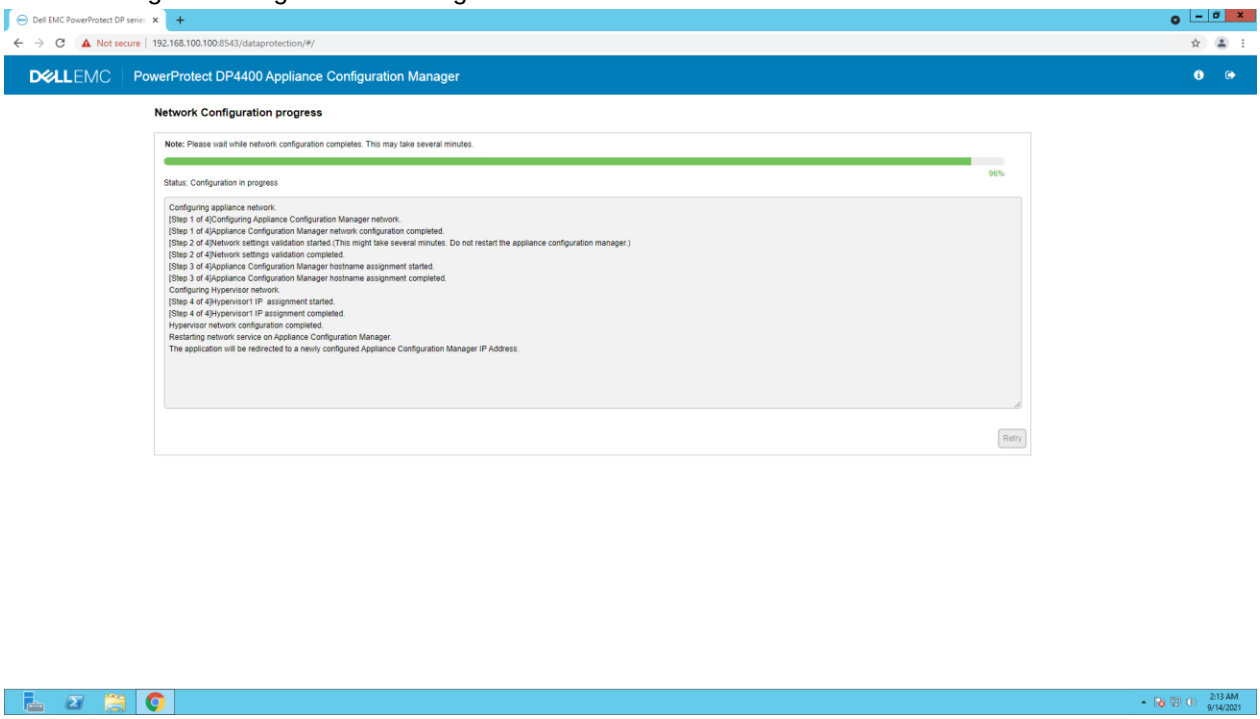

Figure 7 Network configuration progress.

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. 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, click **Rollback** to revert all the settings. You must review the settings, make changes if required, and configure the network settings again.

3. Log in to the ACM using the public IP Address.
   - Username: **root**
   - Password: **< Newly updated Password>**

The SRS page appears

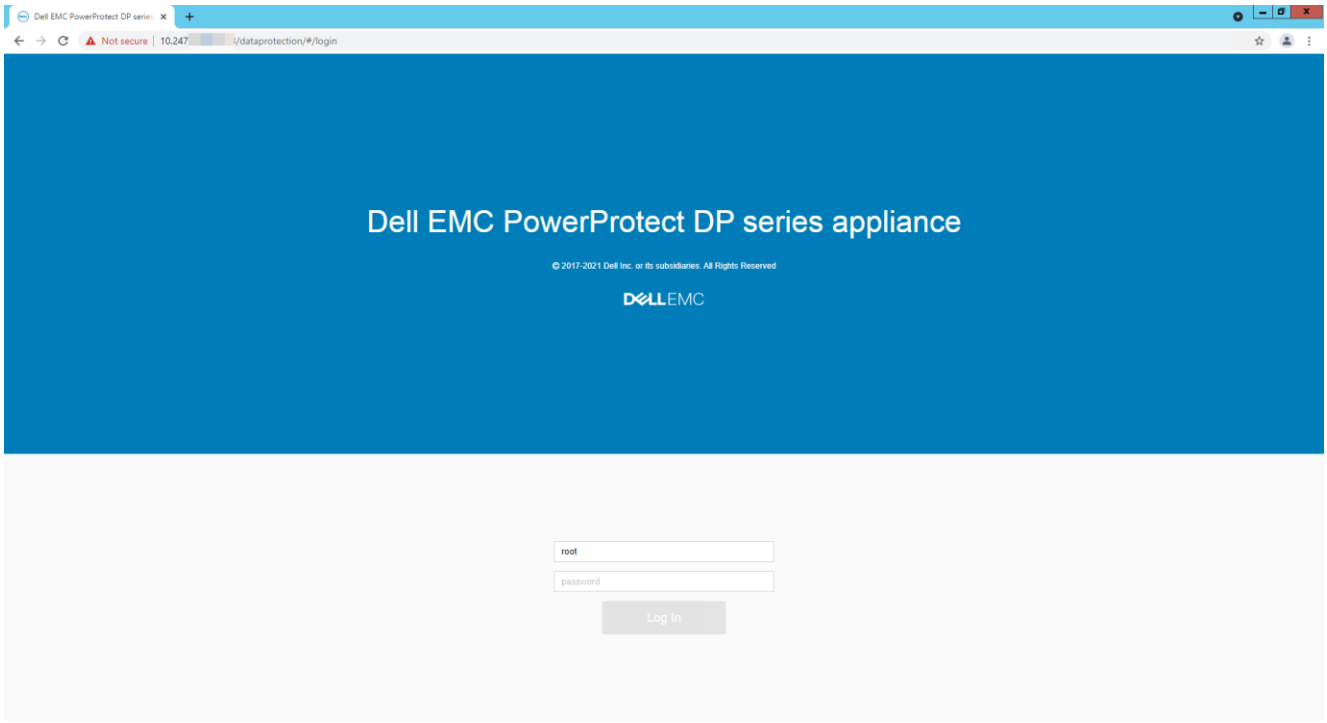

Figure 8 ACM Login page using public IP

4. We recommend skipping the SRS configuration and configuring it from the ACM dashboard later.

5. The PowerProtect DP Series Appliance configuration page appears. On the PowerProtect DP Series Appliance configuration page, perform the following steps.

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

On the Welcome page, select the optional components that you want to install in the configuration and click **Next**.

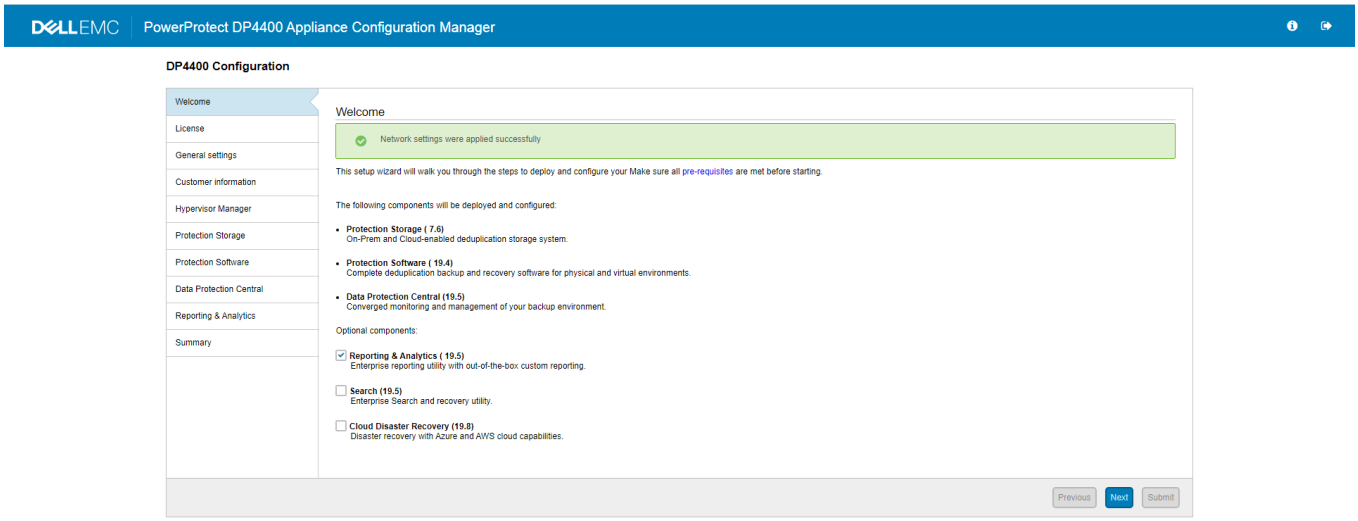

Figure 9 DP4400 Configuration page

6. If you are connected to the network with an Internet connection, the system automatically downloads the licenses for Protection Storage, Protection Software, and Reporting and Analytics point products.

In-product activation is not supported on IPv6-enabled network and dark side appliance. 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 license files manually. The system validates the license files 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. Depending on the appliance you have, you can upgrade the storage capacity from 8 TB to 24 TB in increments of 4 TB or 24 TB to 96 TB in increments of 12 TB.
- The license file should not have the hash (#) character.
- The license must be in multiples of 4 TB.

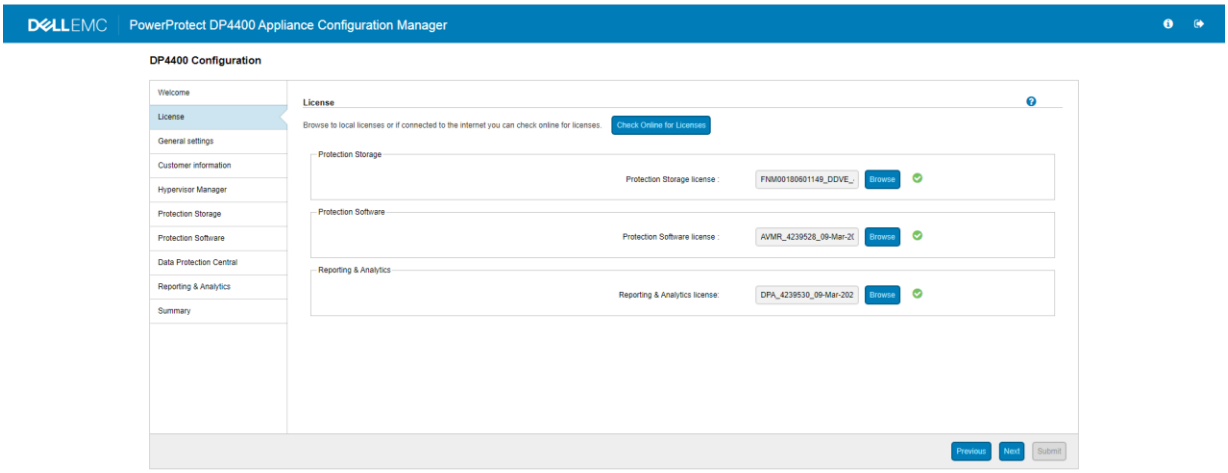

Figure 10 Licensing the DP4400 Server.

7. Click **Next.** The General setting page is displayed.

8. On the **General settings page**, perform the following actions:

a. Verify the number in the Serial Number field, which is the Locking ID mentioned in the *Dell EMC software license activation notification email.*
b. Select the **Time zone** from the list.
c. Select and enter the IP address in the **IP address range (11)** field.

The system automatically assigns 11 IP addresses in a chronological order, which is based on the IP address that you specify to configure the other components of the appliance. For example, if you specify 10.200.1.10, the system automatically generates a range of IP address from 10.200.1.10 to 20.

Note: If any of the optional components such as Reporting & Analytics, Search, and CDR is not selected **Welcome page**, the IP address range will be reduced here.

If you have configured separate management network, specify 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.

Note: If any of the optional components such as Reporting & Analytics, Search, and CDR is not selected on **Welcome page**, the IP address range will be reduced here.

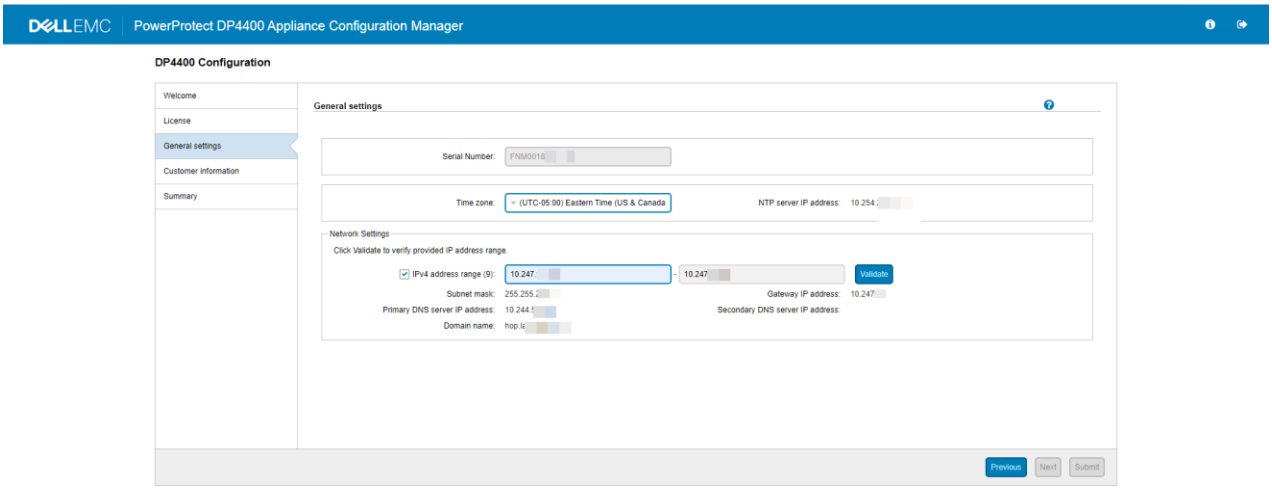

Figure 11 Network settings

9. Click **Validate**.

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

Note: If you do not select the IP address range checkbox, you must manually configure and specify the IP addresses for each component.

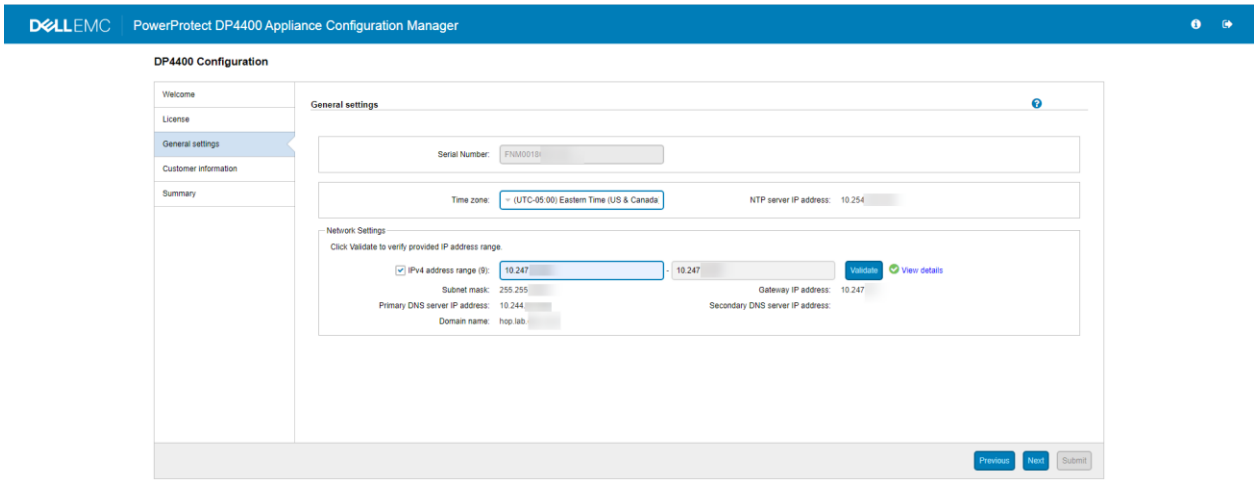

Figure 12 Network setting validation.

10. Click **Next**.

The **Customer Information Settings** page is displayed.

11. On the **Customer information settings** page, perform the following actions:

a**.** On the **Customer information** section, enter information in the mandatory fields.

> Enter the name of the company in the **Company name** field.
> Enter the name of the administrator in the **Admin contact name** field.
> Enter the contact number of the administrator in the **Admin contact number** field.
> Enter the location in the **Location** field.
> Enter the site ID in the **Site ID** field.

Note: If you select the **Email notification** checkbox, the **Email Configuration** section is displayed.

b. In the **Email Configuration** section, enter information in the mandatory fields.

Note: If you select the **Email notification** check box, the **Email Configuration** section is displayed.

> Enter the SMTP server IP address in the **SMTP server** field.
> Enter the port number in the **Port** field.

Note: The **Port** field is auto populated and is the default SMTP port.

> Enter the email address of the administrator in the **Administrator email** field.
> Click **Test Email** to send a test email to the administrator's email address.

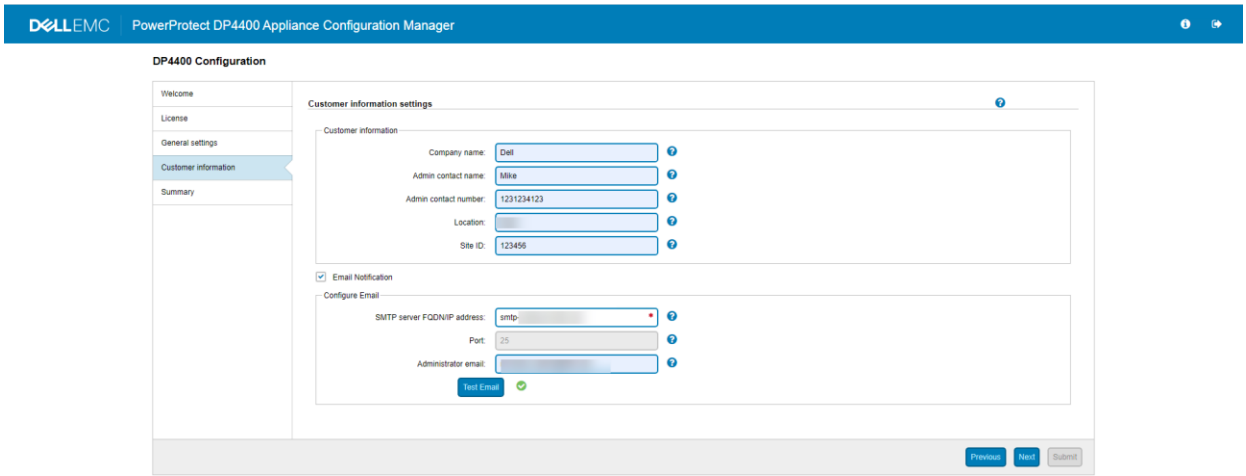

Figure 13 Customer information.

12. Click **Next**.

13. In the **Summary** page, review the information that you entered and click **Submit** to start the configuration.

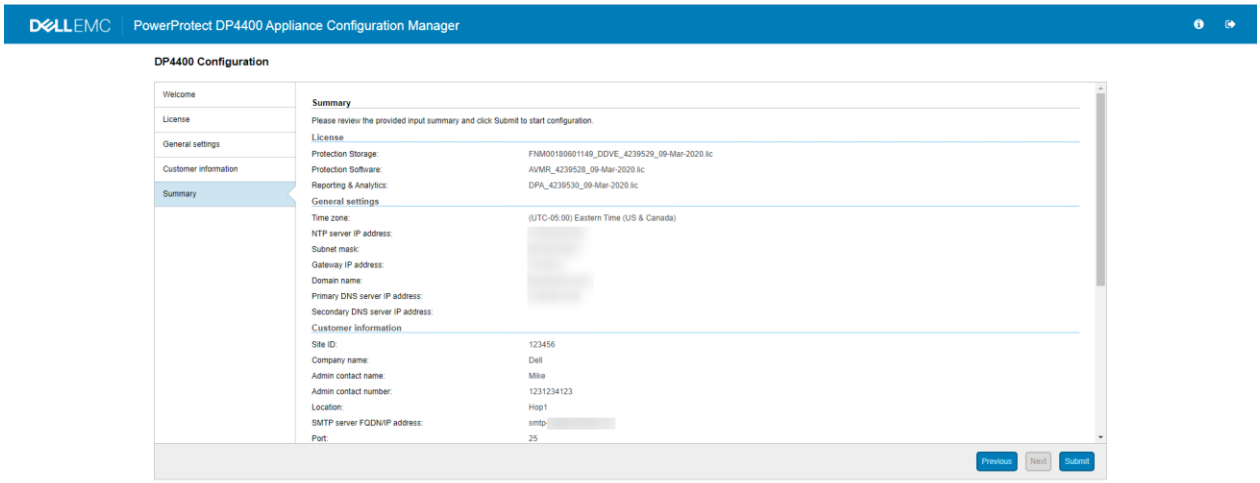

Figure 14 Configuration summary

14. Click the **Submit** button. A confirmation message is displayed.

15. Click **Yes** to continue to configure the Appliance.

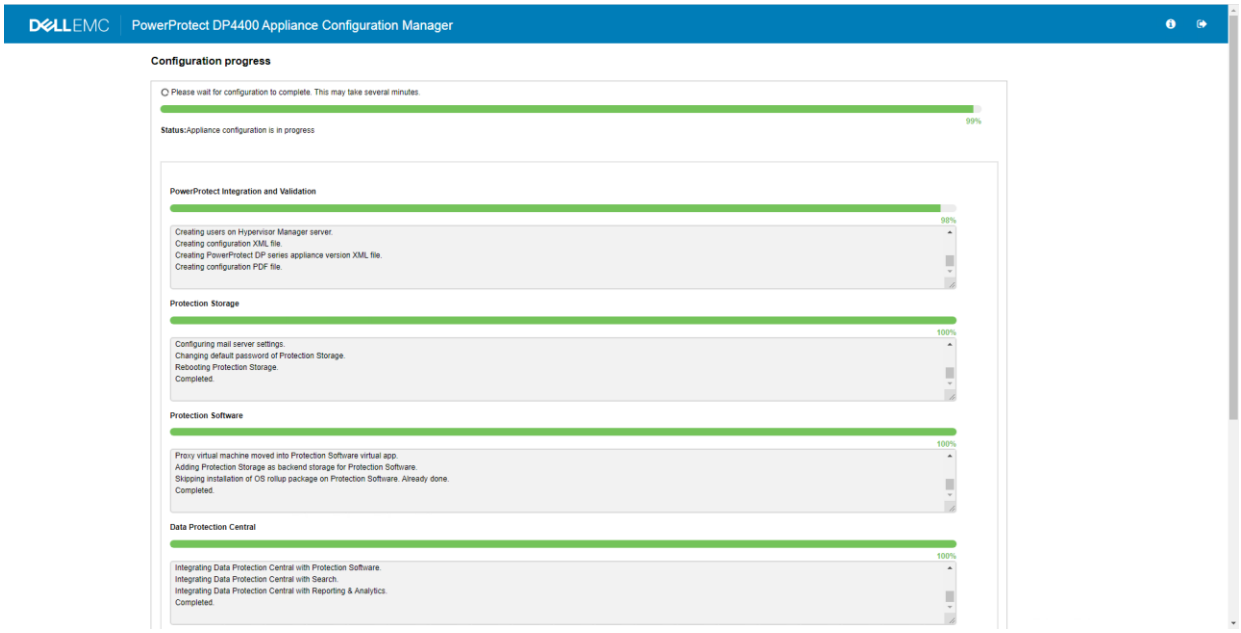

Figure 15 Figure 14: Appliance configuration In Progress.

16. Click **Finish.**

Note: Once the appliance is configured successfully, you can download the **Solution ID, configuration file configuration XML file** for your reference.

The PowerProtect DP Series Appliance has been successfully deployed and configured.

5.4.1 Self-contained deployment (optional)

Self-contained deployment refers to configuring the appliance network using the ACM IP for DNS, NTP, and Gateway. This is an optional task.

Perform this task only if you do not have a valid IP address for DNS, NTP, and Gateway. After the appliance is deployed and configured successfully, you can change the DNS, NTP, and Gateway from the ACM dashboard.

Prerequisites

1. Self-contained deployment is supported only on IPv4 network.

Note: You cannot configure the ACM as DNS and NTP on a IPv6 network.

2. In a single network configuration, there should be at least two uplinks that are connected to the switch.

Perform the following temporary workaround if you do not have two uplinks:

Assign two temporary IPs in different subnets (subnet should be different than Protection Storage management IP) to Protection Storage backup IPs. These IPs do not require DNS entries. After the deployment, change the Protection Storage IPs assigned to these NICs and update the Protection Storage `ifgroup`. This workaround prevents the Protection Storage configuration failure.

About this task:

Perform the following steps when you are on the **Network Configuration page** on ACM.

1. Open an SSH session as a **root** user on ACM using a private IP.
2. Run the command:

   ```
   cd /usr/local/dataprotection/var/configmgr/server_data/config/
   ```

3. Open the file commonconfig.xml using vi editor: vi commonconfig.xml
4. Find the following tags:
   - <ConfigureAcmDNS>false</ConfigureAcmDNS>
   - <ConfigureAcmNTP>false</ConfigureAcmNTP>
5. Change the values of the tags based on the mode of deployment:
   - To configure DNS, set the value of tag `ConfigureAcmDNS` as `True`.
   - To configure NTP, set the value of tag `ConfigureAcmNTP` as `True`.
6. Save the `commonconfig.xml` file.

7. Perform these steps to configure DNS:

   a. Run the command: `cd /usr/local/dataprotection/customscripts/`
   b. Open the file `dns_ip_hostname_mappings.properties` using vi editor:

   `dns_ip_hostname_mappings.properties`

   The content of the file depends on the appliance model. Verify if the required keys are present in the file, or you can add them manually.

   c.

   Enter the required IPs, hostname mapping, and other details as per the keys present in the file. See the
   guidelines for updating the file:

- To use the IP range for assigning IP addresses and host names to the respective components, see IP address requirements section on page 25.

  Note: IP range validation is not supported in self-contained deployment

- For a single network, leave the separate backup network fields blank.

  Note: Enter the short hostname and not the FQDN.

- Hostname entries must not contain underscore (_).

- Enter the IP address or hostname for the optional components (Reporting and Analytics, Search, and Cloud DR). If the corresponding IP addresses or hostnames are not added in the file during deployment, the optional components cannot be deployed from the ACM dashboard later while ACM is being used as DNS.

  d. Save the dns_ip_hostname_mappings.properties file.
  e. Go to the ACM **Network Configuration page** on the Internet browser and refresh the page.

  The Network Configuration page should be automatically populated if the _ip_hostname_mappings.properties file is updated with all the required fields.

8. Enter the ACM IP in **NTP server IP Address** field.
9. 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.

- If the network configuration fails, you can click **Rollback** to revert all the settings. Review the settings, modify if required, and then configure the network settings again.

Next steps:

- After the network configuration is complete, revert the network adapter IP address settings on the service computer to their previous state.
- After completing the network configuration, see *Configure the DP4400 Software* for the steps to install and deploy the appliance.

5.5 Troubleshooting

This section provides information about troubleshoot the installation failures using the following actions.

- Click **Download log bundle** to download the logs of the installation that can be analyzed or sent to Technical Support.
- Click **Retry** to install the critical components that have failed to install from the point the installation failed.
- Click **Rollback** to review or modify the settings if required on the **Welcome** page and then configure the settings.

5.5.1 Retry installation

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.

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

If the **Retry** operation is done after 5 days of configuration failure, `Note that the user can retry without destroying file system` warning message is displayed.

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 PowerProtect DP Series Appliance the **Retry** option is not available, you can only **Rollback** the installation.

5.5.2 Roll back Installation

If the installation fails, you can roll back the installation when the **Retry** functionality does not resolve the issue, follow the wizard to set up and deploy the PowerProtect DP Series Appliance.

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.

Prerequisite:

Click **Download log bundle** to download the logs before you start the **Rollback**.

To roll back the appliance configuration, perform the following actions.

1. Click Rollback on the Configuration progress page.
2. The Rollback Configuration page is displayed.

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

3. If the **Retry** operation is done after 5 days of configuration failure, Note that without destroying the file system on Protection Storage, next configuration cannot be submitted warning message is displayed.
4. Click **Yes** to continue the installation.
5. 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** page.

6. After the **Rollback** is successful, the **Configuration Welcome** page is displayed. Configure the appliance from the **Configuration Welcome** page.

5.5.3 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.

6 Use cases

PowerProtect DP Series Appliance supports many ecosystems. The following table depicts the workloads that PowerProtect DP Series Appliance supports out of the factory and other workloads that require RPQ approval.

Table 12 Supported use cases with PowerProtect DP Series Appliance

Use case	DP4400S and DP4400	DP5900	DP8400	DP8900
Single vLAN	Yes	Yes	Yes	Yes
Flat network or no vLAN	Yes	Yes	Yes	Yes
Separated backup or management (< 2.5)	RPQ	RPQ	RPQ	RPQ
Separated backup or management (> 2.5)	Yes	Yes	Yes	Yes
Separated replication	RPQ	RPQ	RPQ	RPQ
Multiple backup networks using separate NICs	RPQ	RPQ	RPQ	RPQ
Multiple backup networks using vLAN tagging	RPQ	RPQ	RPQ	RPQ
Re-IP of IDPA components	RPQ	RPQ	RPQ	RPQ
Direct backups to DD Series with DD Boost	Yes	Yes	Yes	Yes
Client-side NAT	RPQ	RPQ	RPQ	RPQ
VTL support (filed upgrade FC SLIC)	No	RPQ	RPQ	RPQ
DDBEA support	Yes	Yes	Yes	Yes
BoostFS support	Yes	Yes	Yes	Yes
Third-party CIFS, NIFS direct to embedded DD Series	RPQ	RPQ	RPQ	RPQ
Rerack IDPA into customer rack (all models)	Yes	RPQ	RPQ	RPQ
Manage multiple IDPAs from external DPC	Yes	Yes	Yes	Yes
Monitor/report multiple IDPAs from external DPA	Yes	Yes	Yes	Yes

Use case	DP4400S and DP4400	DP5900	DP8400	DP8900
Re-IP of IDPA system by Professional Services	Yes	Yes	Yes	Yes
Physical NDMP accelerator node (with initial setup)	Yes	Yes	Yes	Yes

7 Upgrade PowerProtect DP Series Appliance software (DP4400)

This section describes how to upgrade the PowerProtect DP Series Appliance software for a DP4400 model. The software, firmware, and infrastructure components are upgraded in the appliance upgrade.

The following components are upgraded:

- ACM
- Hypervisor Manager
- Hypervisor and server firmware
- Protection Software
- Protection Storage
- Data Protection Central
- Reporting and Analytics (optional)
- Search (optional)
- Cloud DR (optional)

The components are upgraded in the following sequence:

1. Protection Software, Protection Storage, Data Protection Central, Reporting and Analytics, Search, Cloud DR, and ACM.
2. Hypervisor Manager, Hypervisor, and server firmware.

7.1 Supported upgrade paths

The following table details the supported upgrade paths for PowerProtect DP Series Appliance 2.7 on DP4400 models.

Note: To verify if you are upgrading the appliance from a supported version, click the **About** icon on the top-left corner of the ACM Dashboard.

Table 13 Supported upgrade paths

Current Version	Supported Upgrade path	Additional Information
PowerProtect DP Series Appliance version 2.6	Upgrade to PowerProtect DP Series Appliance version 2.7	You can directly upgrade to PowerProtect DP Series Appliance Version 2.7
PowerProtect DP Series Appliance version 2.6.1	Upgrade to PowerProtect DP Series Appliance version 2.7	You can directly upgrade to PowerProtect DP Series Appliance Version 2.7

Note: For information on the supported upgrade paths for appliance versions 2.5 and below, see the https://elabnavigator.emc.com/eln/modernHomeDataProtection.

7.1.2 Upgrade prerequisites

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

ACM

1. Ensure that the upgrade binary idpa-hw-upgrade_.tar.gz is downloaded from Dell EMC Support, and copied on the /data01/upgrade folder in the ACM.

Note: The `/data01/upgrade` folder must not contain any other post or pre-patch packages

Note: If you are upgrading both the software as well as the infrastructure components, you may delete the upgrade binary, which is approximately 50 GB, from the source location after the file is transferred to the ACM. However, if you are upgrading only the software components (from version 2.4.x and 2.5), you must retain the upgrade binary as you will have to copy the same file again to the ACM for the Infrastructure upgrade.

2. Log in to the ACM Service IP using SSH. and then run the following command to validate the upgrade package using the SHA256 checksum process: `sha256sum -c < *tar.gz.sha256 file name>`

3. Ensure that you have executable permission for the downloaded upgrade package. To get the executable permission, run the following command: `chmod 644 idpa-hw-upgrade_<version>.tar.gz.`

7.1.1 Protection Software

1. The PowerProtect DP Series Appliance upgrade must be performed during a maintenance window when no other maintenance activities or backup replication jobs are in progress.

2. Ensure that the replication policies are disabled and that there are no replication jobs that are triggered from the source Protection Software Server while the upgrade is in progress, either on the source or on the destination Protection Software servers. See **Stop Backup and Replication jobs section** if you are unable to cancel the replication or backup job.

7.1.2 Cloud DR

This section is applicable **only** if the Cloud DR deployed on the PowerProtect DP Series Appliance is configured with the Cloud DR Server.

The following are the Cloud DR and Cloud DR Server requirements before upgrading the appliance:

- The Cloud DR (Service) must be manually upgraded to version 19.5.x or 19.6.x
- The Cloud DR Server must be manually upgraded to version 19.8.x

The Cloud DR is automatically upgraded to its 19.8.x version with the appliance upgrade.

Note: If the Cloud DR Server is not configured with the Cloud DR, you can proceed directly with the appliance upgrade as the Cloud DR is upgraded with the appliance upgrade.

The versions of the Cloud DR Server and Cloud DR do not have to be identical, and you are not required to upgrade them simultaneously (unless otherwise instructed). When uploading an upgrade package, if the upgrade package version is not supported, you receive a notification.

When upgrading from Cloud DR Server/Cloud DR version after 18.3, you can directly upgrade to a version that is four times later than the current version (for example, 18.3 > 19.3 > 19.5).

7.1.3 Sequence of manual Cloud DR or Cloud DR Server Upgrade

The table below describes the upgrade paths and the sequence in which the Cloud DR and Cloud DR Server must be upgraded.

Table 14 Sequence of Cloud DR or Cloud DR Server upgrade.

Appliance version	Corresponding CDR version	Cloud DR Server and Cloud DR upgrade steps
PowerProtect DP Series Appliance 2.6	19.5	Upgrade Cloud DR Server from version 19.5 to 19.8.
PowerProtect DP Series Appliance 2.6.1	19.6	Upgrade Cloud DR Server from version 19.6 to 19.8

7.1.4 Upload Upgrade Packages

About this task:
Perform the following steps to download the upgrade packages and upload them from the Cloud DR system:

Steps:

1. Download the **Cloud Disaster Recovery Upgrade** `multi_package` from the Dell Support site.
2. From the Cloud DR Server **System** menu, select **Upgrades.**
3. To upload the upgrade package that you just downloaded, click **Upload Package**.
4. To replace the currently uploaded package with another Cloud DR package, click **Upload Different Package.**

Note: After you upload an upgrade package for Cloud DR Server, the **Upgrade Cloud DR Server** button is displayed.

Note: After uploading an upgrade package for the Cloud DR, a message indicates that the CDRA upgrade is pending. If the upgrade package includes both Cloud DR Server and Cloud DR, then the Cloud DR upgrade starts after the Cloud DR Server has been upgraded. The **Cloud DR restore ova package** is upgraded as part of the Cloud DR upgrade process.

Note: Do not upgrade the Cloud DR Server while the rapid recovery process is running. If you upgrade the Cloud DR Server while the rapid recovery process is running, the process is not monitored after the upgrade and the machine image is lost.

For detailed information about how to upgrade Cloud DR/Cloud DR Server, see *Upgrading the CDRS and CDRAs chapter in the Dell EMC Cloud Disaster Recovery Installation and Administration Guide*, which can be obtained from the Dell EMC Support site.

7.1.5 Upgrade the Cloud DR Server

To upgrade the Cloud DR Server, perform the following steps.

Prerequisites
Download the upgrade package (Cloud DR Server or Cloud DR, or both) from the Dell EMC Support site.

Ensure that there is no rapid recovery process running.

Steps:

1. From the Cloud DR Server **System** menu option, select **Upgrades**.

Note: If a disaster recovery operation is in progress, the upgrade process is disabled.

2. Click **Upgrade Cloud DR Server**.

3. In the **Cloud DR Server Upgrade** dialog box, click **Upgrade**.

   Expect a short downtime during the upgrade while the Cloud DR Server restarts. You cannot perform disaster recovery operations until the upgrade completes, and you restart the browser.

4. Restart the browser and log in to the Cloud DR Server interface.

Results:

After the Cloud DR Server upgrade is successful, it may take about 10 to 15 minutes for the changes to reflect in the Cloud DR UI. The time taken for the changes to reflect depends on network connection between the Cloud DR and Cloud DR Server. Wait for the Cloud DR Server upgrade to reflect in the Cloud DR UI, and then continue with the Cloud DR upgrade if required.

7.1.6 Upgrading Cloud DR

To upgrade the Cloud DR, perform the following steps.

Steps

1. From the Cloud DR **System** menu option, select **Upgrades**.
   The **Upgrades** page displays and provides information about the current version and upgrade status of the Cloud DR.

2. If an upgrade package is available for the Cloud DR, click **Upgrade Cloud DR Add-on.**

   The Cloud DR is upgraded to the new version. A short downtime may occur during the upgrade while the Cloud DR restarts.

   At the end of the upgrade process, the Cloud DR login page is displayed.

3. Restart the browser and log in to the Cloud DR interface.

7.1.3 Upgrading the PowerProtect DP Series Appliance

About this task

This section describes how to upgrade the appliance to its 2.7 version. Both the software and infrastructure components are upgraded in this upgrade process.

- **Software Upgrade:** Upgrades Protection Storage, Protection Software, Data Protection Central, Reporting & Analytics, Search, Cloud DR, and ACM.
- **Infrastructure Upgrade:** Upgrades Hypervisor Manager and Hypervisor, and the PowerEdge server firmware.

Steps

1. Log in to the ACM UI using `https://< ACM Hostname>:8543`
   It is recommended to use ACM hostname to connect to the ACM UI instead of using the IP address.

Note: Ensure that there are no errors or operations in progress in the ACM dashboard before moving to the next step.

If you are unable to connect to the ACM UI using the hostname, add the following entry in the host's file: , and restart the browser.

- For Windows computers, the hosts file is located at `C:\Windows\System32\drivers\etc\hosts`
- For Linux computers, the hosts file is located at `/etc/hosts`

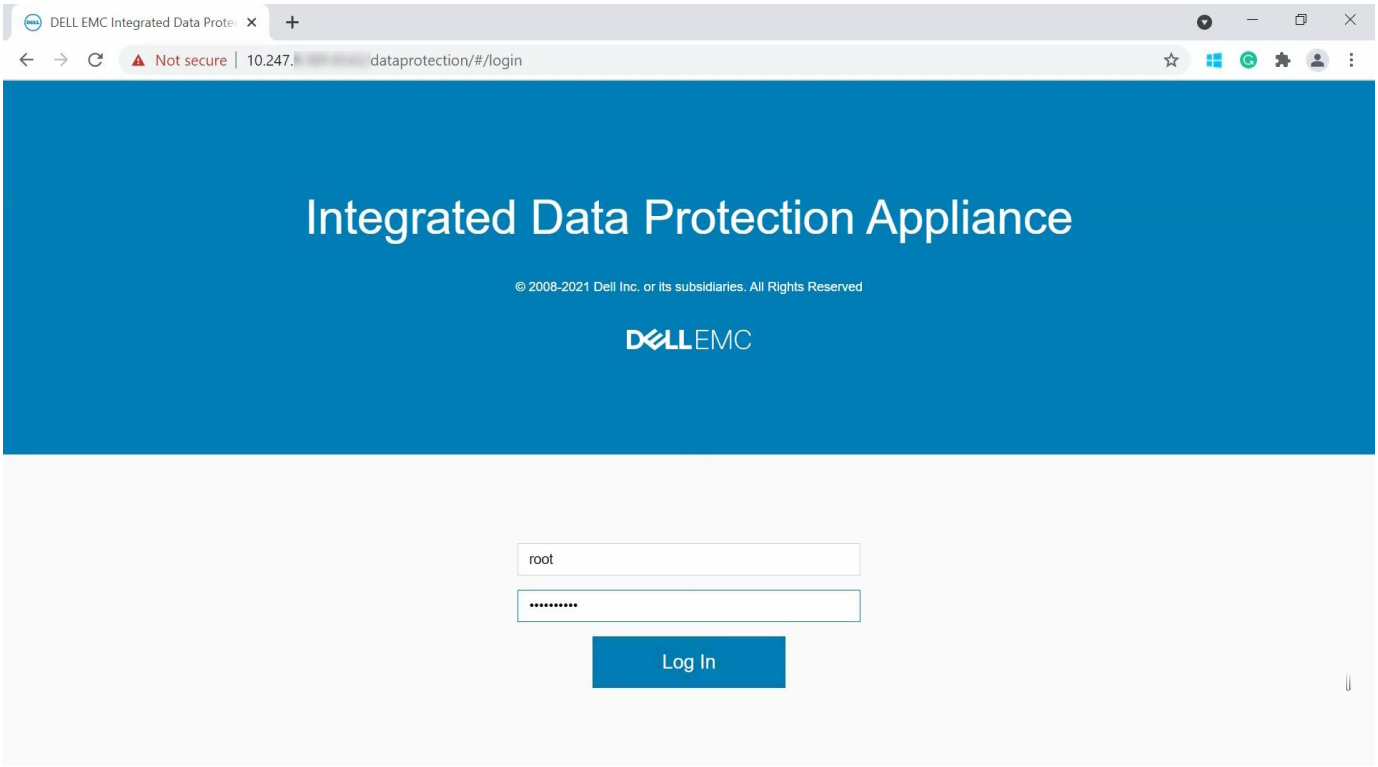

Figure 16 ACM login screen

2. Verify that the tar.gz file is automatically populated in the **Upgrade File Location** field of the **Upgrade tab.**

   If the tar.gz file is not automatically populated, then type the path in the Upgrade File Location field.

Note: Ensure that the upgrade tar.gz file name begins with idpa.

If the path or the file name is incorrect, an error message is displayed.

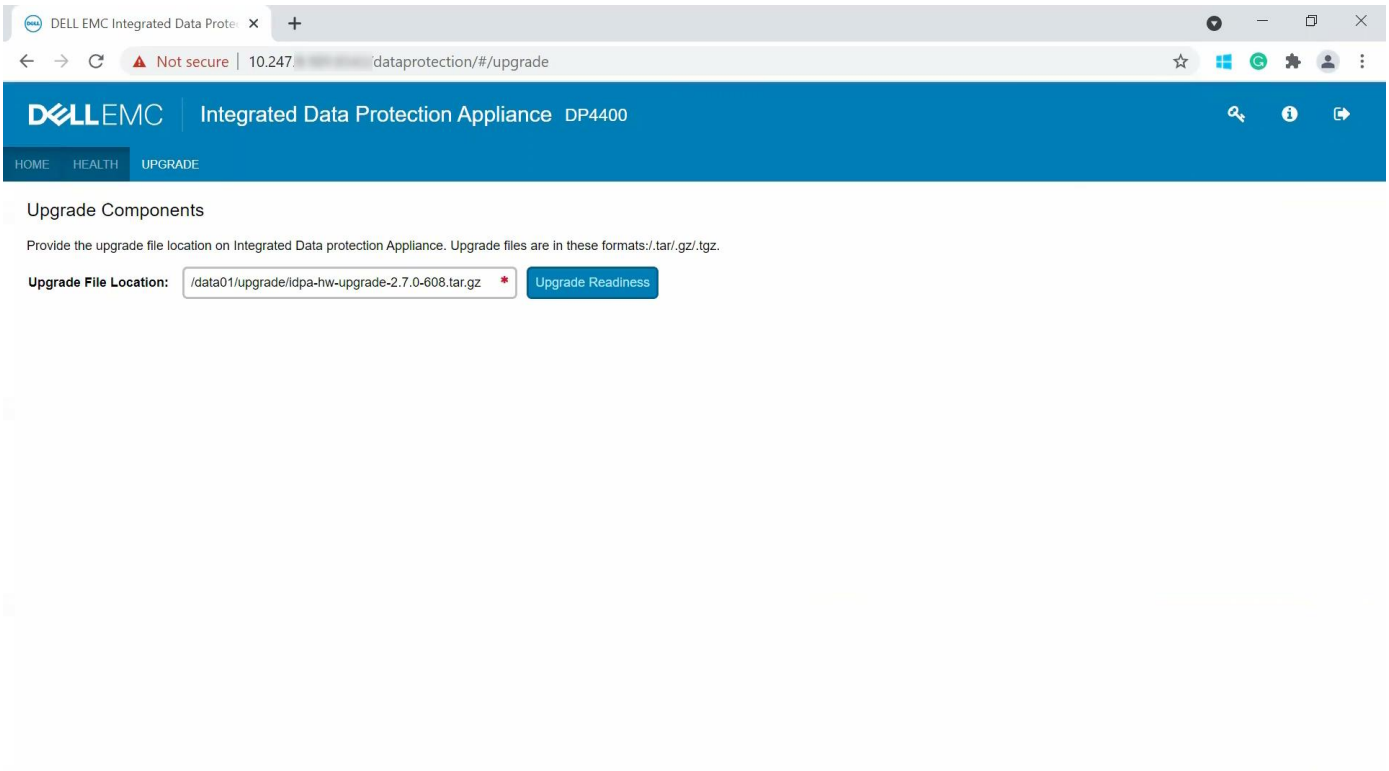

Figure 17 Upgrade tab

3. Click **Upgrade Readiness.**

   Once the upgrade readiness completes successfully, the upgrade **End User License Agreement** page is displayed.

Note: If the End User License Agreement page is not displayed, ensure that the port 9443 is open in your network firewall, and then access the upgrade UI from the following link: `https:// <ACM FQDN or IP>:9443/ dataprotection-upgrade`

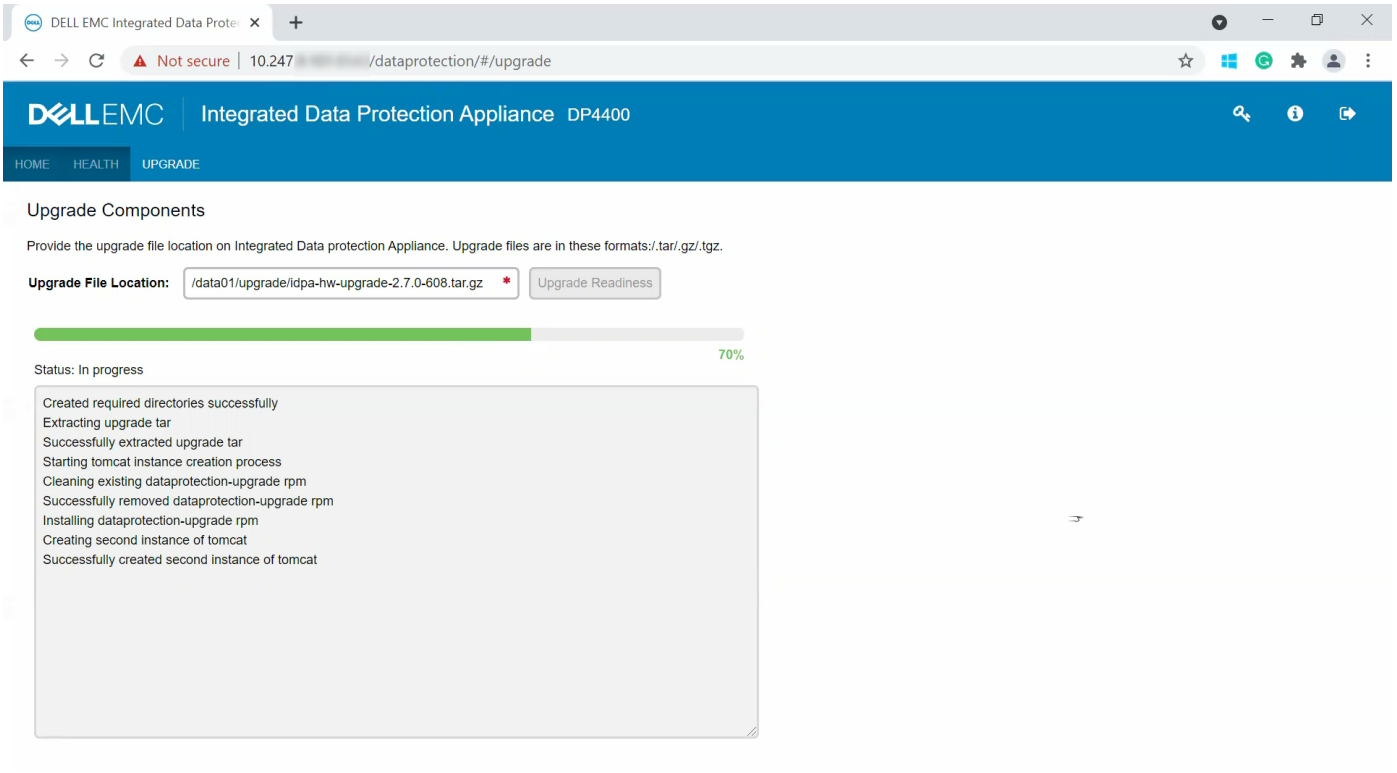

Figure 18 Upgrade readiness in progress

4. Read the **Dell EMC End User License Agreement** and click **Agree** to continue with the upgrade validations.

   If you click **Disagree**, and then **Cancel**, you will be directed back to the ACM dashboard.

5. Check the upgrade options, and then click **Validate** to perform validation checks on the components to be upgraded.

   Software Upgrade and **Infrastructure Upgrade** are selected by default. Go with either the default **Software Upgrade** and **Infrastructure Upgrade**, or just **Software Upgrade.**

Note: If you unselect **Infrastructure Upgrade,** then you must upgrade the infrastructure components later. You will not be allowed to upgrade to future versions of PowerProtect DP Series Appliance without upgrading the corresponding infrastructure components. It is recommended to only use this method if you can afford two comparatively shorter upgrade windows instead of one long upgrade window.

Note: When upgrading only the software components from versions PowerProtect DP Series Appliance 2.5 and older, the upgrade `tar.gz` bundle is not preserved in the ACM. When you perform the infrastructure, components upgrade you will have to manually copy the upgrade tar bundle to the ACM `/data01/upgrade` folder again.

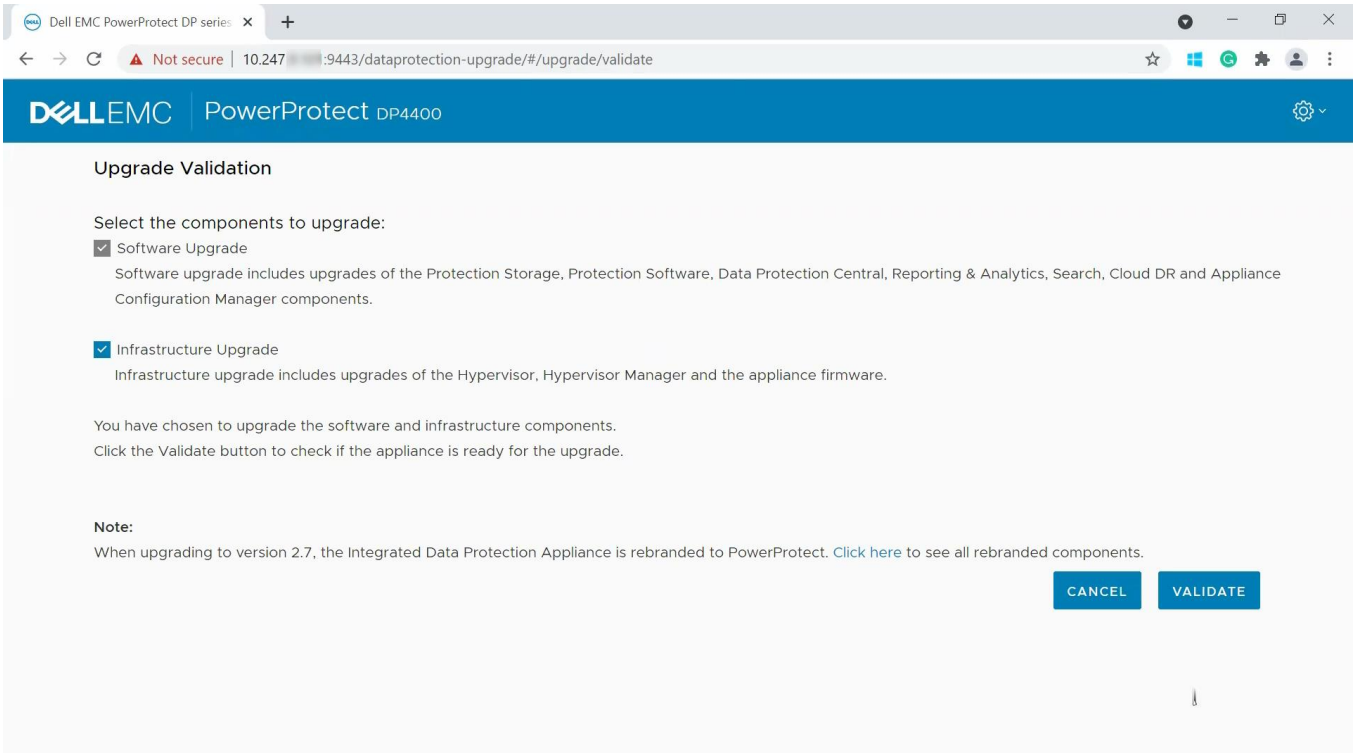

Figure 19 Upgrade Validation page for upgrade component selection.

6. Wait for the **validation** checks to complete.

   The software verifies the requirements for performing the upgrade based on the options selected in the **Upgrade Validation** page.

Note: If you selected the Infrastructure Upgrade option, the **Current Version** of the **Server Firmware** row may be displayed as **N/A** or **Unknown**.

N/A is displayed when the upgrade validation process is unable to retrieve the firmware block version, which may be an exception or may be due to a run time error. **Unknown** is displayed when the upgrade validation process is unable to identify the firmware block version from the retrieved information as the hardware components on the server node have different firmware versions from the known firmware block.
Proceed with the next step as this does not impact the upgrade process.

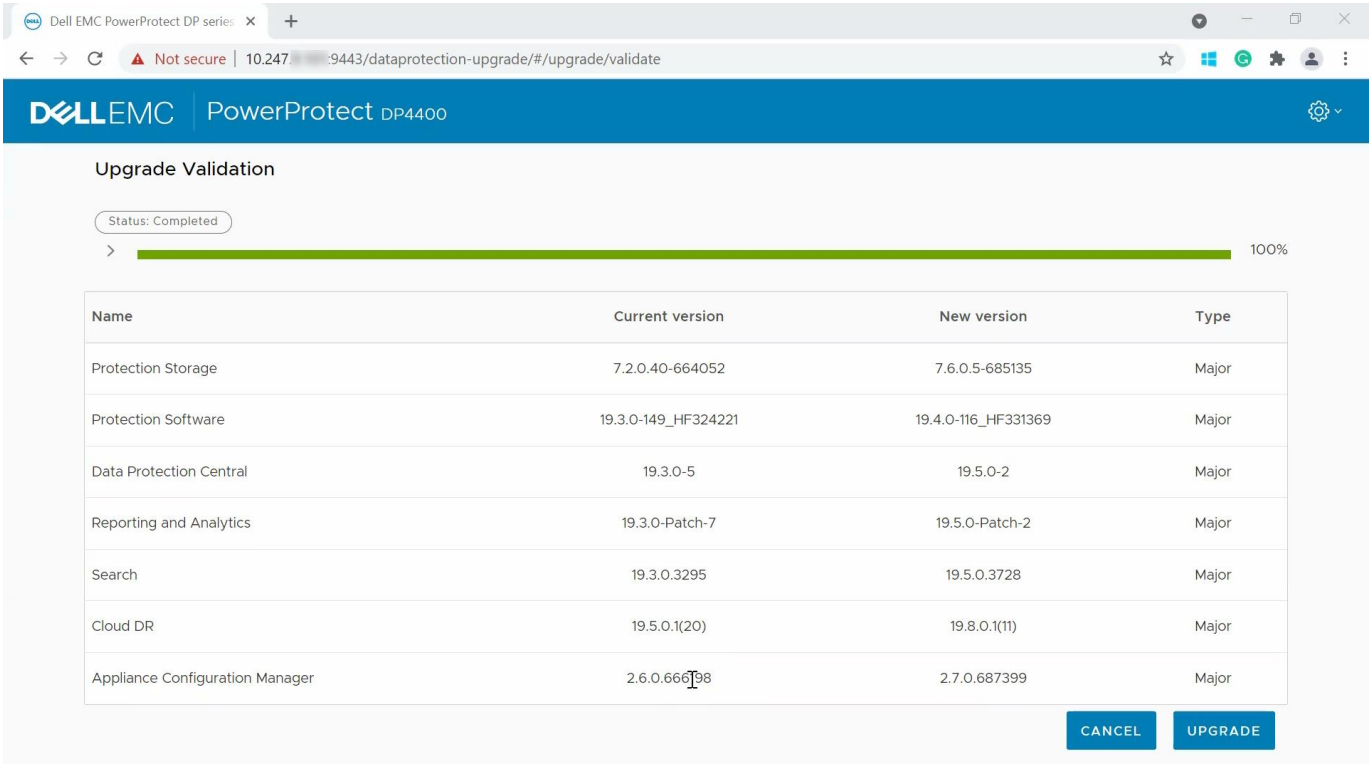

Figure 20 Upgrade validation page to initiate the upgrade task.

7. Click **Upgrade**, and then click **Ok** after all the validations are complete.

   The **Upgrade Progress** page displays the details of the upgrade progress. This process may take a few hours to complete based on the upgrade options selected in the **Upgrade Validation** page. If the upgrade for any component fails, then the upgrade process is stopped until you troubleshoot and resolve the failure.

Note: The browser session may time out if the **Upgrade Progress** page is idle for some time. Refresh the browser and log in to the ACM again to reconnect to the **Upgrade Progress** page.

Note: If you click **Cancel** instead of **Upgrade**, then you are redirected to the ACM dashboard. When you proceed with upgrade process again, the **End User License Agreement page** is not displayed as the **End User License Agreement** is already accepted.

Note: During the upgrade, the upgrade workflow performs some operations on the individual components such as renaming or restarting the components, which generates alerts. You can ignore these alerts as they are part of the upgrade process workflow. However, if there are any critical hardware-related alerts, contact Dell EMC Technical Support personnel.

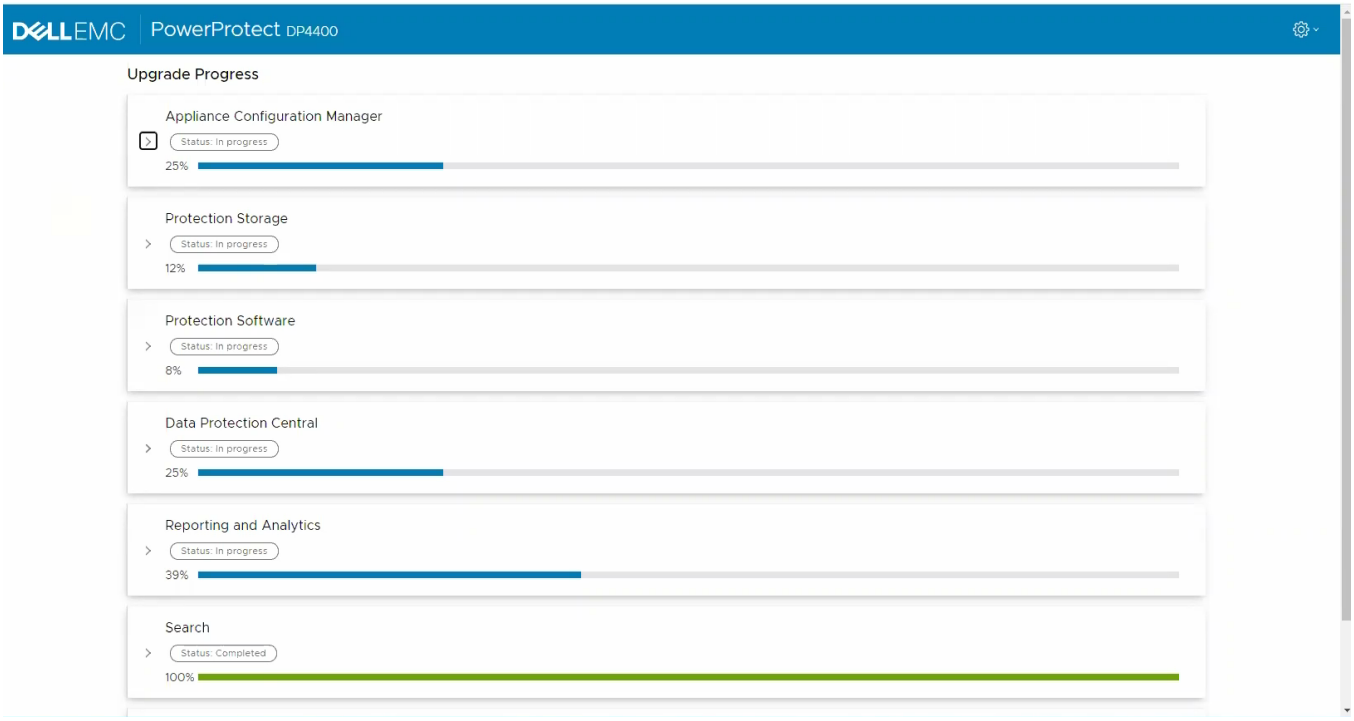

Figure 21 Upgrade in progress

8. Optional: **Click Download Logs** to collect the logs after the upgrade process completes.

9. Click **Finish**, and then **Ok** to finish the upgrade operation.

   Wait for the time displayed in the pop-up window, after which you are redirected to the ACM dashboard. Do not move to another screen when the timer is displayed in the pop-up window.

Note: If you close the pop-up window before the specified time, you must open ACM dashboard manually in browser. However, the ACM dashboard may be inaccessible, or the status of some components may be displayed incorrectly due to post upgrade startup which is in progress. You need to wait for at least 30 minutes after you click finish until the ACM and other appliance services restart.

Note: If the appliance was upgraded from version 2.4.x or version 2.5, then it will take longer for the ACM dashboard to be displayed. During this time, do not attempt to delete or power on any of the ACM services (especially the ACM-old service).

The Hypervisor server restarts along with all the server appliance services hosted on it. The DP4400 appliance takes between 5 to 45 minutes to start up depending on the upgrade paths

Figure 22 Upgrade completed successfully

10. Verify that all the components started up, and that there are no errors in ACM dashboard.

    If you went with the default software and infrastructure upgrade in Step 5, then the appliance is successfully upgraded to its 2.7 version.

Note: If errors are displayed in the ACM dashboard, then close the existing browser window and open the ACM UI in a new browser window

Note: If you enabled FIPS when upgrading to the PowerProtect DP Series Appliance 2.7, the Protection Software internal VM proxy will not be upgraded. During the upgrade, the Protection Software internal VM proxy is powered off because it does not meet FIPS compliance. After the upgrade, the Protection Software internal VM proxy will remain at 19.3 (not 19.4.x.x).

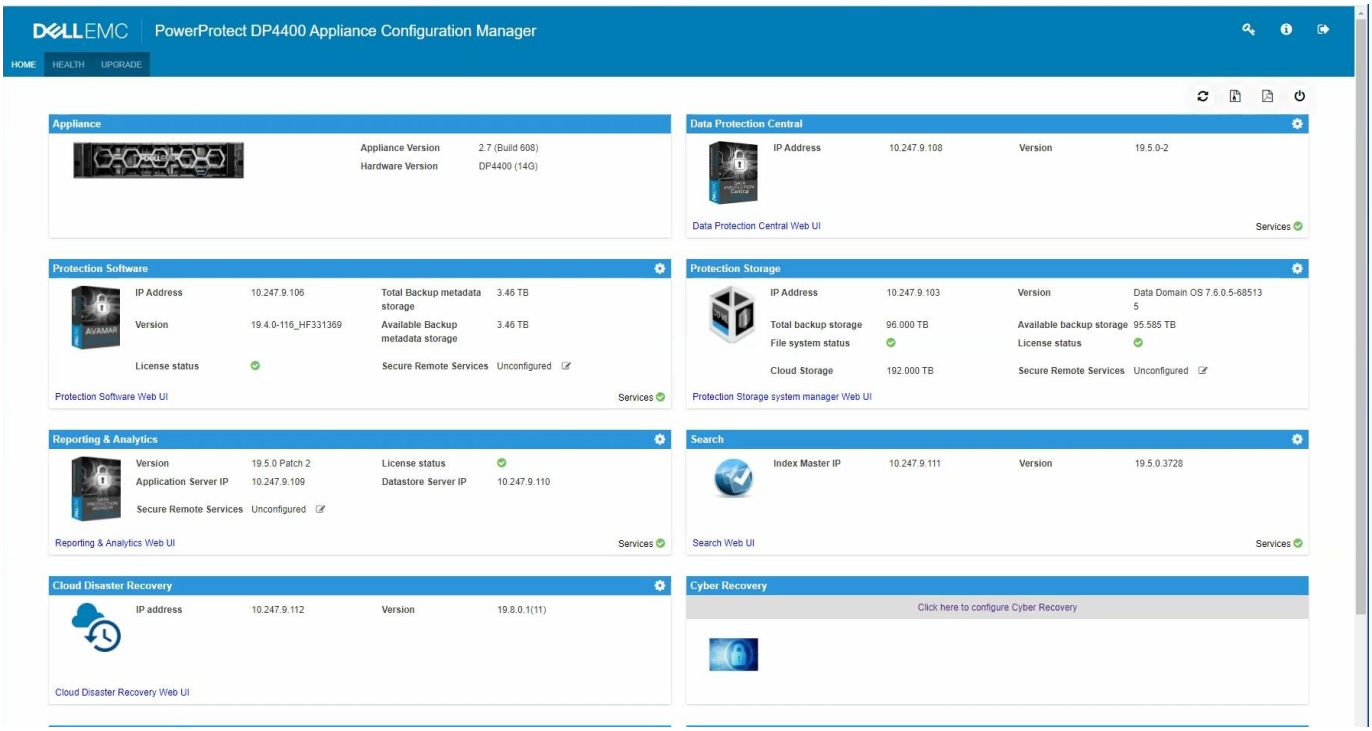

Figure 23 Appliance is upgraded to version 2.7

11. If you had cleared the **Infrastructure Upgrade** check box in step 5, then the ACM dashboard displays a notification that the infrastructure components upgrade is pending. Go to the **Upgrade** tab and repeat all the upgrade steps again to upgrade the infrastructure components.

Note: When upgrading only the software components from versions PowerProtect DP Series Appliance 2.5 and older, the upgrade `tar.gz` bundle is not preserved in the ACM. When you perform the infrastructure, components upgrade you will have to manually copy the upgrade tar bundle to the ACM `/data01/upgrade` folder again.

Note: The upgrade `tar.gz` bundle is the same as the one used for the software upgrade.

7.2 Troubleshoot upgrade validation and upgrade failure

This section describes some of the possible issues encountered during validation checks and appliance upgrade process.

7.2.1 Troubleshoot Upgrade Validation failures

This section describes some of the possible upgrade validation failures and their workaround.

7.2.1.1 Unable to access the ACM UI during appliance upgrade

About this task:

If you are unable to access the ACM UI from `https://<ACM FQDN or IP Address>:9443/dataprotection-upgrade`, then perform the following steps to cancel the upgrade process manually.

Steps:

1. Stop the ACM tomcat service using the following command: `service dataprotection_webapp stop`
2. Stop the ACM upgrade tomcat service if it is running, using the following command: `service dataprotection_webapp_upgrade stop`
3. Check if the ACM tomcat service is running using the following command: `service dataprotection_webapp status`
4. Check if the appliance status is `ESRS_AV_CONFIGURED` in the `applianceStatus.xml` file using the following command: `Cat /usr/local/dataprotection/var/configmgr/server_data/status/applianceStatus.xml | grep applianceState`
5. Copy the upgrade Tomcat logs from the `/usr/local/dataprotection/upgrade-tomcat/logs/` folder using the following command: `cp -R /usr/local/dataprotection/upgrade-tomcat/logs/ /data01/upgradetomcat-logs-backup/`
6. Delete the upgrade-tomcat folder from the `/usr/local/dataprotection/` folder using the following command: `rm -rf /usr/local/dataprotection/upgrade-tomcat`
7. Copy upgrade logs from `/data01/tmp/patch/logs` and then delete patch folder from path `/data01/tmp/`
8. Run the following command to start the ACM Tomcat service: `service dataprotection_webapp start`
9. Retry the appliance upgrade operation. If you are unable to access the URL, then contact Dell Support.

7.2.2 Protection Storage

This section describes the possible solutions for Protection Storage upgrade validation failures. You must perform the steps given in this chapter using an SSH client and connect to the Protection Storage with the sysadmin user account.

Perform the following to fix the possible upgrade validation failures:

- Check that the Protection Storage consumption is less than 99% by running the following command: `filesys show space`

  If the storage consumption is above 99%, then contact Dell Support.

- Check the file system status by running the following command: `filesys status`

  If the file system status is in a healthy state but busy, then wait for the task to complete and then retry the upgrade validation.

- Check if any cleanup operations are in progress by running the following command: `filesys clean status.`

  Wait for the cleanup task to complete, and then retry the upgrade validation.

- Check for any critical alerts using the following command: `alerts show current`

  Fix the issues to clear the alerts, and then retry the upgrade validation.

7.2.3 Used capacity of the / partition on search exceeds 55 percent

About this task:

The upgrade validation may fail if the used capacity of the / partition on Search exceeds 55 percent.

Perform the following steps:

1. Using an SSH connection, with root credentials, connect to Search.
2. Verify the used space on Search by running the following command: `df -h`
3. Verify that the used space of the `/` partition is 55 percent and above.
4. Change the directory to the `/var/log/` folder.
5. Delete all the files with the extension `.xz`. The following command provides an example: `rm *.xz`
6. Clear the large log files if required. For example, you can clear the messages files.
7. Verify that the used space of the `/` partition is below 55 percent.

8. If the used space of the / partition is still 55 percent or above, then follow the steps mentioned in the KB Article https://www.dell.com/support/kbdoc/en-us/000186645/data-protection-search-unable-to-login-to search-web-administrator-system-drive-full

7.2.4 Used capacity of the partitions other than the / partition on Search exceeds 90 percent

About this task:

The upgrade validation may fail if the used capacity of the partitions other than the / on Search exceeds 90 percent.

Perform the following steps:

1. Using an SSH connection, with root credentials, connect to the Search.
2. Verify the used space on Search by running the following command: `df -h`
3. Identify the partitions that are using 90 percent and above of the storage space.
4. For the partition mounted on `/mnt/es_data`, you can reduce the used space by deleting the indices from the **Search Web UI.**
5. For the partition mounted on `/mnt/search`, you can reduce the used space by deleting the older or unwanted log files.
6. Ensure the Search services are running.
   - Verify the status of Search services.
     - service elasticsearch status
     - service search-cis-core status
   - If the services are in a stopped state, then start the service.
     - service elasticsearch start
     - service search-cis-core start
   - If the services fail to start, restart the Search VM, and then check the status of the services again.
     - reboot

7.2.5 Protection Software

This section describes the possible solutions for Protection Software (Service) upgrade validation failures. You must perform the steps given in this chapter on Protection Software using an SSH client.

Perform the following to fix the possible upgrade validation failures:

- Check if there is at least 38 GB of free space in the /space directory on the Protection Software Server by running the following command `df -h`. If the free space in the directory is lower than 38GB, then delete unwanted files from the directory.

  If the total size of `/space` partition is less than 96 GB, then see the KB Article https://www.dell.com/support/kbdoc/en-us/000190523/how-to-increase-space-partition-size-in-ave-vm on how to increase partition size in the Protection Software (service).

- Check if any policies are enabled. All policies must be disabled before an appliance upgrade.

- Check if a replication server is configured. The upgrade validations may fail if a replication server is configured.

  Contact Dell Support to validate the configuration using the latest AV Proactive check and continue with the upgrade.

- Check if any Protection Software Backup clients and agents were manually upgraded before the Protection Software Server upgrade.

  Contact Dell Support to validate the configuration using the latest AV Proactive check and continue with the upgrade.

7.2.6 Create a validated checkpoint

Prerequisites:

Check if you have a validated checkpoint which is not older than 24 hours with an `HFScheck` by running the following command: `status.dpn`

About this task:

The upgrade validation may fail if you do not have a validated checkpoint on the Protection Software. The validated checkpoint must not be older than 24 hours, with a `HFScheck` which is not older than 36 hours. To create a new validated checkpoint perform the following steps:

1. Log in to the Protection Software Server using the `admin` user account.

2. Run the following command to create a checkpoint: `mccli checkpoint create --override_maintenance_scheduler=true --wait=0`

3. Run the following command to view the created checkpoint: `cplist -lscp`

4. Run the following command to validate the checkpoint: `mccli checkpoint validate --cptag=CheckpointTagFromPreviousCommand --override_maintenance_scheduler=true --wait=0`

7.2.7 Terminate Unavailable Sessions

About this task:

The upgrade validation may fail if there are any unavailable sessions running on the VM Proxy (Service). To terminate these unavailable sessions, perform the following steps:

1. Log in to the Protection Software system as an Admin user, using putty.

2. Run the following command to see the active sessions in the system: `avmaint sessions | grep "path\| sessionid\|starttime"`

   - path: Displays the path for the client.
   - sessionid: Displays the unique identifier of the session.
   - starttime: Displays the UNIX time stamp of when the session began.

3. Translate the value from the start time parameter to a readable format by running the following command: `t.pl < Start time>`

4. Compare the value with the backup scheduler to confirm if the session is running. If the session started several days ago and is not configured as **overtime**, then it may be an unavailable session.

5. Run the following command to remove the unavailable sessions: `avmaint kill`

6. After you have removed all of the unavailable sessions, run the following command to see the list of sessions running on the Protection Software server: `avmaint sessions –full`

Note: You may have to stop the stale entries on the proxy server as needed.

7.2.8 Stop backup and replication jobs

About this task:

The PowerProtect DP Series Appliance upgrade must be performed during a maintenance window when no other Protection Software maintenance activities, backup or replication jobs are running.

To ensure this, perform the following steps.

1. Connect to the utility node using SSH and log in as an admin user.

2. Run the following command to verify if the server status is idle: `opstatus.dpn`

3. Run the following commands:

   - `avmaint sessions | grep path`: To check if any backup jobs are in progress.
   - `mccli activity show --active | grep Replication` : To check if any replication jobs are in progress.

   Sample Output:

```
admin@dp5900-08-10:~/>: avmaint sessions | grep path
path="/AVI_BACKUPS"
path="/"
admin@dp5900-08-10:~/>: mccli activity show --active | grep Replication
9163194680374209 Running 0 2021-09-18 02:33 EDT 00h:02m:10s 2021-09-19 02:33 EDT
```

```
Replication Source 133.4 MB 83%  dp5900-08-10.datadomain.com /MC_SYSTEM
1631946917158146 Running 0 2021-09-18 02:35 EDT 00h:00m:14s 2021-09-19 02:33 EDT
Replication Source 140.2 MB 2.1% EM_BACKUPS                  /
admin@dp5900-08-10:~/>:
```

   If any backup or replication jobs are running, you can either wait for these jobs to complete or you can terminate these jobs. You can also contact Dell Support to terminate these backup jobs.

4. Run the following command to terminate the backup or replication jobs: `mccli activity cancel --id= <job_id>`

5. Run the following commands to confirm that the jobs are no longer in progress.

   - `avmaint sessions | grep path`: To check if any backup jobs are in progress.
   - `mccli activity show --active | grep Replication` : To check if any replication jobs are in progress.

7.2.9 Reporting and Analytics

About this task:

The size of the `/data01` partition on the Reporting and Analytics DataStore service must not exceed 60 GB. If the size of the `/data01` partition is over 60 GB, then the upgrade validation will fail.

To verify the size of `/data01 partition`, perform the following steps:

1. Connect to the Reporting and Analytics DataStore service using SSH with root credentials.

2. Verify the size of the `/data01` partition using the following command: `df -h`

3. Verify the value in size column of the `/data01` partition.

4. If the size is over 60GB, then contact Dell support to upgrade the Reporting and Analytics components.

7.2.10 Data Protection Central

If you have configured an external LDAP server, ensure that it is configured from the ACM Dashboard.

Prerequisites:

If you have configured an external LDAP server in the Data Protection Central manually (not through the ACM Dashboard), then the upgrade validation for the Reporting & Analytics component upgrade will fail.

Note: Configuring an external LDAP from the Data Protection Central is not supported.

About this task

Perform the following steps to check if the LDAP settings are configured through the ACM Dashboard:

1. Log in to the ACM Dashboard.

2. Click the icon on the left of the **Shutdown Appliance** and download the current configuration to view the Appliance Configuration PDF file with the current appliance configuration details.

3. To connect to the Data Protection Central, specify the username mentioned in the LDAP settings of the PowerProtect DP Series Appliance Configuration PDF. If you successfully log in using the provided username, it indicates that the LDAP configuration is in sync.

   If you are unable to log in using the username mentioned in the LDAP settings of the PowerProtect DP Series Appliance Configuration PDF, then reconfigure the Data Protection Central LDAP configuration using the ACM hostname (usually idpauser) as LDAP server. See *Revert to internal LDAP environment section in the PowerProtect DP Series Appliance Product Guide* for more information

4. Reconfigure the external LDAP from the ACM Dashboard. See *Configure external LDAP environment section in the PowerProtect DP Series Appliance Product Guide* for more information.

7.2.11 ACM, Hypervisor Manager, and Hypervisor

This section describes the possible solutions for ACM, Hypervisor Manager, and Hypervisor upgrade validation failures.

Perform the following to fix the possible upgrade validation failures:

- Check if the private IP addresses `192.168.100.108` used by the Hypervisor Manager component, and `192.168.100.113` used by the ACM component are available for the upgrade validation. If the IP addresses are not available then the upgrade validation will fail. Ensure that these IP addresses are available, and then retry the upgrade validation.

If a custom internal IP address range is used, then update the ACM's temporary IP address and the gateway in the `/ data01/tmp/patch/ip_details.properties` file.

- Check if you have created or copied any VMs, folders, or files on the Hypervisor or Hypervisor Manager servers of the appliance. Ensure the following, and then retry the upgrade validation:
  - No non-PowerProtect DP Series Appliance-VMs, vApps, Resource pools, or any custom settings are deployed or configured on the appliance.
  - No custom files and folders exist on the Hypervisor and Hypervisor Manager (Service) servers.
  - No files are copied to the Hypervisor or Hypervisor Manager (Service) Server partitions. These include ISO, VIB, or other binary files manually copied to the Hypervisor or Hypervisor Manager (Service) Server storage partitions.

7.2.12 Set correct hostname in Hypervisor server

About this task:

The upgrade validation may fail if the hostname (short and FQDN) is not set correctly on the Hypervisor server. To ensure you have the correct hostname for the Hypervisor server which reflects on iDRAC, perform the following steps:

1. Connect to the ACM Server using an SSH connection
2. Run the following command to view the hostname of the IP addresses associated with the Hypervisor Server: `nslookup`
3. Connect to the Hypervisor server using an SSH connection.
4. Run the following commands to verify if the hostname matches the one retrieved from the `nslookup` command:
   - `hostname -s`
   - `hostname -f`
5. If the hostname on the Hypervisor is incorrect, then run the following commands:
   - `esxcli system hostname set --host=hostname`
   - `esxcli system hostname set --fqdn=fqdn`
6. Log in to the iDRAC console.
7. Go to **System Panel** in the **iDRAC** dashboard and verify the value in the **Host Name** field. If you are unable to access the iDRAC console for any of the Hypervisor servers, follow the steps listed in KB article

https://www.dell.com/support/kbdoc/en-us/000021500/idpa-how-to-perform-firmware-upgrades-using-idrac-remotely

8. If the hostname does not reflect correctly on the **iDRAC** Dashboard, then refresh the console and then verify the hostname.
9. If the hostname does not reflect correctly even after refreshing the console, then stop and restart the iDRAC service:

a. Run the following command: `esxcli system wbem set -e=true`
b. Run the following command to stop the service: `/etc/init.d/sfcbd-watchdog stop`
c. Run the following command to start the service again: `/etc/init.d/sfcbd-watchdog start`

7.2.13 Reduce storage space in Hypervisor Manager partition

About this task

The validation for the Hypervisor Manager may fail with if the used storage space for the `/storage/log` partition is more than 90%. To reduce the used storage space in the `/storage/log` perform the following steps:

1. Using an SSH client, connect to the Hypervisor Manager Server service as a `root` user.
2. Switch to the Shell prompt: `shell`
3. Run the following command to ensure that the Hypervisor Manager services are running: `service-control --all -status`
4. Run the following command to verify the size of the /storage/log partition: `df -h`

Note: This partition is over 90% in use. Delete unwanted files and bring this percentage value below 90% to ensure the upgrade validations are successful.

5. Run the following command to identify the top 20 files with high disk usage: `du -a /storage/log | sort -n -r | head -n 20`
6. Delete the files listed in the output of the above command.
7. Run the following command to verify that the `%` Use value for the `/storage/log` partition is below 90%: `df -h`
8. Repeat the steps 5 to 7 until the `/storage/log` partition is below 90%.
9. Run the following command to restart all of the Hypervisor Manager services and Platform Services Controller services: `service-control --start -all`
10. Run the following command to ensure that all the Hypervisor Manager services are running before the start of the update procedure: `service-control --all --status`

7.2.14 Troubleshoot Upgrade failures

This section describes the possible issues you may encounter when upgrading the appliance to its 2.7 version

7.2.14.1 Unable to start the appliance after upgrade

About this task:

If the appliance fails to start up after you click **Finish**, connect to the Hypervisor UI and perform the following tasks:

1. Check if the Hypervisor server is in maintenance mode.
2. Exit the maintenance mode.
3. Power on the Data-Protection-ACM VM.

Note: Do not power on any of the other VMs (especially the ACM-old VM). Once the **Data-Protection-ACM** VM powers on, you can monitor the progress of the appliance startup from the ACM UI.

7.2.15 Protection Software

This section describes the possible upgrade errors you may encounter with Protection Software and their possible workaround.

7.2.15.1 Protection Software unable to start after upgrade

The Protection Software may fail to start or may have functionality issues if you have installed unsupported custom SSL certificates on the Protection Software. Contact Dell Support to resolve the issue.

7.2.15.2 Search is disconnected from the Protection Software after PowerProtect DP Series Appliance upgrade

About this task:

After you upgrade the PowerProtect DP Series Appliance, Search may be disconnected from the Protection Software. If this is the case, there will be a red broken link icon over the **idpa-backupServer** listed in the **Search UI > Manage: Avamar > Administration > Sources page**. To connect Search to the Protection Software, perform the following steps.

1. In the upper right corner of the Search UI, in the **Manage**: field, select **Avamar** from the drop-down menu
2. In the left navigation pane, click **Administration > Sources.**
   A list of Protection Software Search sources appears.
3. Click within the row that contains **idpa-backupServer.**
4. Click the **Repair Agent** button (hammer and wrench icon) in the right vertical toolbar.

   This runs a repair agent job to connect Search to the Protection Software.

Note: For more troubleshooting related information's please refer to *"Dell EMC PowerProtect DP series*

appliance Installation and Upgrade Guide"

7.2.16 Upgrade log files

If the upgrade readiness or the upgrade task fails, please collect the log files in the following locations and contact Dell Support:

- Log files for the most recent upgrade process are in **/data01/tmp/patch/logs** and include the following:
  - ACM: `acm_upgrade.log`
  - Protection Storage: `dd_precheck.log, dd_upgrade.log`
  - DP Advisor: `dpa_upgrade.log`
  - Search: `dps_upgrade.log`
  - Protection Software: `AvamarServerUpgrade.log, av_upgrade.log`
  - Data Protection Central: `dpc_deploy_config.log`
  - Common logs for all components: `appLevelUpgrade.log, detailed_upgrade_logs.log`
- Log files for past upgrades are archived in **/data01/upgradeLogs,** in the format **idpa_upgradeLogs<date>_<*time*>.tgz.**

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

A.1 Document references for PowerProtect DP Series Appliance

PowerProtect DP Series Appliance documentation set includes the following publications:

- *PowerProtect DP Series Appliance Installation and Upgrade Guide*

  Instructions for installing the PowerProtect DP Series Appliance DP4400 hardware and software. The guide also contains instructions for upgrading DP5900.

- *PowerProtect DP Series Appliance Field and Professional Services Deployment Guide for DP5xxx and DP8xxx*

  Instructions for installing and setting up PowerProtect DP Series Appliance DP5xxx and DP8xxx

- *PowerProtect DP Series Appliance Product Guide*

  Provides the overview and administration information about the PowerProtect DP Series Appliance system.

- *PowerProtect DP Series Appliance Release Notes*

  Product information about the current PowerProtect DP Series Appliance release

- *PowerProtect DP Series 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.

- *PowerProtect DP Series Appliance Software Compatibility Guide*

  Information about software components and versions that are used in the PowerProtect DP Series Appliance product

- *PowerProtect DP Series Appliance DP4400 Service Procedure Guide*

  Procedures for replacing or upgrading hardware components of the PowerProtect DP Series Appliance.

- *PowerProtect DP Series Appliance Field Replacement Guide for DP5xxx and DP8xx*

  Instructions for adding, replacing, and servicing DP5xxx and DP8xxx hardware components

A.2 PowerProtect DP Series Appliance training resources

See more IDPA training and information at https://education.emc.com including video walkthroughs, demonstrations, and explanations of product features.