Dell EMC Integrated Data Protection Appliance

Version 2.3

Product Guide

302-005-524

REV. 01

DELL EMC

Published January 2019

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

CONTENTS

Revision history

Table 1 IDPA Product Guide Revision History

Revision	Date	Description
01	January 2019	First release of this document for IDPA 2.3

CHAPTER 1

Introduction

This chapter provides a general overview of the Integrated Data Protection Appliance 2.3 features and hardware configurations.

Topics include:

Document scope and audience

The scope of this document is to describe the administrative details of the Integrated Data Protection Appliance (IDPA).

The target audience for this document includes field personnel, partners, and customers responsible for managing and operating the IDPA. This document is designed for people familiar with Dell EMC Data Protection solutions.

Product features

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

Simplified deployment and configuration
The IDPA DP4400 model is a hyper-converged, 2U system that a user can install and configure onsite.

Other models of IDPA (DP5300, DP5800, DP8300, and DP8800) are shipped as a complete unit, with all hardware components racked and cabled in the factory. Installation and initial configuration are completed by Customer Support. The solution includes an Avamar server as the Backup Server node with optional NDMP Accelerators, a Data Domain system as the Protection Storage node, Compute nodes for virtual components and software, a networking switch for improved setup speed, and Cloud Disaster Recovery.

Note

This is applicable for the DP5300, 5800, 8300, and 8800 appliances. The Cloud Disaster Recovery node is applicable for DP4400.

The system software for each component is installed and configured to the greatest extent possible before the appliance is shipped. A backup application, target storage, reporting and analytics, search, cloud disaster recovery, system manager, and the appliance configuration manager (ACM) come embedded in the appliance.

It also includes the IDPA System Manager. The Search, Reporting and Analytics, and CDRA are all optional to set up. Additionally, the Search, Reporting and Analytics, and CDRA functions can also be performed by a central corporate implementation of these functions.

After the unit is on site, it is connected to the existing infrastructure, powered on, and registered with Secure Remote Services (formerly ESRS). After successful Secure Remote Services registration, the ACM licenses the individual components and completes onsite network configuration.

Centralized management
The ACM provides a graphical, web-based interface for configuring, monitoring, and upgrading the appliance. IDPA System Manager provides advanced monitoring and management capabilities of the IDPA from a single pane of glass and includes the following features:

- Comprehensive dashboards that include the following Avamar and IDPA system information:
  - Backup activities
  - Replication activities

  - Capacity
  - Health
  - Alerts
- Monitoring multiple systems capabilities including system health and activities.
- Management capabilities for the backup application.
- Advanced search and recover operations through integration with Search.
- Reporting capabilities.
- Cloud backups.

Backup administration

You can also add Avamar NDMP Accelerators to enable backup and recovery of NAS systems. The IDPA uses Avamar servers to perform backup operations. Depending on various IDPA models, it uses either an Avamar Virtual Edition (AVE) or a scalable multi-node configuration, with the data being stored in a Data Domain system. For the most part, when using the Avamar Administrator Management Console, all Avamar servers look and behave the same. The main differences among the Avamar server configurations are the number of nodes and disk drives reported in the server monitor.

The Avamar NDMP Accelerator uses the network data management protocol (NDMP) to enable backup and recovery of network-attached storage (NAS) systems. The accelerator performs NDMP processing and real-time data deduplication and then sends the data directly to the Avamar server.

Reporting and Analytics

The reporting and analytics feature offers robust reporting functionality with dedicated sections for various features. The reports help you retrieve information about the environment so that you can review and analyze the activities in the environment. Using these reports, you can identify outages in the environment, diagnose problems, plan to mitigate risks, and forecast future trends. You can run system and customized reports, dashboard templates on demand, and schedule the reports generation as per your enterprise requirements.

TheACM dashboard displays a summary of the configuration of the individual components and allows the administrator to monitor the appliance, change configuration details, or upgrade the system and its components. The dashboard also displays appliance health alert information for the server and VMware components.

Installing Data Protection Advisor is optional. Also, if DPA is already configured in your environment, then the appliance can be configured to use central implementation of DPA with IDPA. You do not need to configure DPA component that is bundled in DPA once again.

If you are running a corporate deployment of the Data Protection Advisor instance, IDPA supports it externally to analyze the system. However, IDPA dashboard will not display any data associated with the external IDPA. Moreover, you must manage and configure any such external DPA instances. Also, IDPA does not support local analytics.

Search

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

Installing Search is optional. Also, if Search is already configured in your environment, then the appliance can be configured to use the central implementation of Search with

IDPA. You do not need to configure the Search component that is bundled in IDPA once again.

If you are running a corporate deployment of Search instance, IDPA supports it externally to index the system. However, the IDPA dashboard will not display any data associated with external Search. Moreover, you must manage and configure any such external Search instances. Also, IDPA does not support local search.

Disaster recovery

CDRA is an optional solution that facilitates the recovery of on-premises virtual machines by providing the capability to recover those VMs in the cloud. CDRA integrates with the backup application inside the IDPA to copy backups of virtual machine data to the public cloud. It can then perform DR tests or failover of production environments by orchestrating a complete conversion of the VM to an Amazon Web Services Elastic Compute Cloud (EC2) instance, and by running this instance in the cloud.

The CDRA is a built-in application that manages deployment of the necessary infrastructure to the cloud, copying of virtual machine backups to the cloud, and orchestrates the compression, encryption and copying of the backed-up VM data to the cloud.

Installing CDRA is optional. Also, if CDRA is already configured in your environment, then the appliance can be configured to use the previously configured CDRA with IDPA. You do not need to configure the CDRA component that is bundled in IDPA once again.

Note

If you have configured an external CDRA, the **Cloud Disaster Recovery** panel does not display any events or data associated with the external CDRA. Moreover, you must manage and configure any such external CDRAs

---

Scalability

The IDPA is designed to be scalable so it can grow with changing needs. The following table details the base configuration for all the IDPA models, which can be expanded by licensing additional capacity in increments.

Table 2 Capacity Specification for all IDPA Models

Model	Capacity
DP4400	From 24 TB up to 96 TB
DP5300	From 34 TB up to 130 TB
DP5800	From 96 TB up to 288 TB
DP8300	From 192 TB up to 720 TB
DP8800	From 624 TB to 1 PB

Unified support

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

System architecture and components

The IDPA integrates multiple data protection solutions into a single product.

Detailed configuration

The IDPA is available in the following models:

Table 3 Configuration options for each model

Model	Protection Storage model	Protection Storage configuration options (usable TB)	Backup Server	Avamar Accelerator Node for NDMP/NAS Backup (optional)
DP4400	Data Domain Virtual Edition	24, 36, 48, 60, 72, 84, or 96 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5300	Data Domain 6300	34, 82, or 130 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5800	Data Domain 6800	96, 144, 192, 240, or 288 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1–3)
DP8300	Data Domain 9300	192, 240, 288, 336, 384, 432, 480, 528, 576, 624, 672, or 720 TB	Avamar Grid: • One utility node • Three M1200 storage nodes (12 TB) • Two switches	NDMP Accelerator (1–4)
DP8800	Data Domain 9800	624, 672, 720 768, 816, 864, 912, 960, or 1008 TB	Avamar Grid: • One utility node • Four M1200 storage nodes (16 TB) • Two switches	NDMP Accelerator (1–4)

Base hardware

The following hardware is included with the IDPA models, DP4400, DP5300, DP5800, DP8300, and DP8800:

- Supported shelf type: DS60 with 4 TB
- Titan-P rack
  - Single Phase
  - 3-Phase Delta
  - 3-Phase WYE
- Three Dell R640 servers
- Dell S4048 48-port switch

Note

Ports Fo 1/13, Fo 1/14, Fo 1/51, Fo 1/52, Fo 1/53, and Fo 1/54 are reserved for uplinks to the network environment.

- Internal cabling

Embedded software

After initial configuration, the following software is deployed and configured:

- Data Domain
- VMware vCenter Server (internal architecture platform on which the appliance runs)
- Avamar
- Integrated Data Protection Appliance System Manager
- Data Protection Advisor (optional)
  - Data Collection Agent Host VM
  - Data Processor Tool Host VM
- Data Protection Search (optional)
  - Search Index VM
  - Search Index 2 VM (DP5300 and DP5800 models)
  - Search Index 3 VM (DP8300 and DP8800 models)
- DD Cloud DR CDRA (optional)
- Appliance Configuration Manager

System self-protection

The IDPA is configured to protect itself from data loss with the backup and storage applications included in the system. The system is protected with self-defined and self-initiated backup jobs that are scheduled daily and have a 30-day retention period. The system metadata is protected using checkpoint backup to the internal target storage.

The below table is applicable for DP5300, DP5800, DP8300, and DP8800 models only

Table 4 Component VM backup jobs

Virtual machine	Backup job
ACM	Management_VM_Backup
vCenter	vCenter_Backup
DP Advisor	DataProtectionAdvisor_Backup
Search	DataProtectionSearch_Backup
IDPA System Manager	DataProtectionCentral_Backup

Note

(Applicable for DP5300, DP5800, DP8300, and DP8800 models only) If one of the servers in the IDPA vSAN cluster fails, you must immediately log in to the **Avamar Administrator** GUI and disable the backup jobs in *Component VM backup jobs* table. For disabling the Avamar backup jobs, refer to the *Avamar Administration Guide*. After disabling the backup jobs, refer to Monitor the vSAN cluster on page 45.

Note

Backup jobs are related to virtual machines hosted on the IDPA appliance. If one of the servers in the cluster fails, it may not be possible to take a snapshot of the VM, which leads to backup failure. Once all the three servers in the cluster are up and running, you must re-enable the backup jobs from the Avamar UI. For more information on re-enabling the backup jobs through the Avamar UI, refer to the *Avamar Administration Guide*.

Network connectivity overview

When a range of IP addresses is used during the IDPA configuration, the IP addresses are assigned in a standard order. Use the table below to determine which IP address is allocated to a component.

The first column in each table, IP Range Allocation, is the value to add to the first IP address in the range.

Table 5 IP address range assignments for the DP4400

IP Range Allocation	Example	Component	Assigned Field
+0	`192.0.2.1`	vCenter	VMware vCenter Server VM
+1	`192.0.2.2`	Target storage	Management IP 1
+2	`192.0.2.3`	Target storage	Backup IP 2
+3	`192.0.2.4`	Target storage	Backup IP 3
+4	`192.0.2.5`	Backup application	Server IP
+5	`192.0.2.6`	Backup application	Avamar Proxy VM
+6	`192.0.2.7`	IDPA System Manager	IDPA System Manager VM
+7	`192.0.2.8`	Analytics and reporting	Application Server Host VM
+8	`192.0.2.9`	Analytics and reporting	Datastore Server Host VM
+9	`192.0.2.10`	Search	Index Master Node Host VM
+10	`192.0.2.11`	DD Cloud DR CDRA (optional)	Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance

Table 6 IP address range assignments for the DP5300 and DP5800

IP Range Allocation	Component	Assigned Field
+0	Data Domain	Management IP 1

Table 6 IP address range assignments for the DP5300 and DP5800 (continued)

IP Range Allocation	Component	Assigned Field
+1	Data Domain	Backup IP 2
+2	Data Domain	Backup IP 3
+3	Data Domain	Backup IP 4
+4	Avamar	Server IP
+5	Avamar	Proxy IP
+6	DP Advisor	Application Server IP
+7	DP Advisor	Data Store Server IP
+8	DP Advisor	Agent IP
+9	Search	Index Master Node 1
+10	IDPA System Manager	IDPA System Manager

Table 7 IP address range assignments for the DP8300 and DP8800

IP Range Allocation	Component	Assigned Field
+0	Data Domain	Management IP 1
+1	Data Domain	Backup IP 2
+2	Data Domain	Backup IP 3
+3	Data Domain	Backup IP 4
+4	Data Domain	Backup IP 5
+5	Data Domain	Backup IP 6
+6	Avamar	Proxy IP
+7	DP Advisor	Application Server IP
+8	DP Advisor	Data Store Server IP
+9	DP Advisor	Agent IP
+10	Search	Index Master Node 1
+11	Search	Index Data Node 1
+12	Search	Index Data Node 2
+13	IDPA System Manager	IDPA System Manager

Table 8 Management IP address range assignments for the DP8300 and DP8800 with Dedicated Backup Network

Management IP Range Allocation	Component	Assigned Field
+0	Avamar	Management IP
+1	DP Advisor	Application Server IP

Table 8 Management IP address range assignments for the DP8300 and DP8800 with Dedicated Backup Network (continued)

Management IP Range Allocation	Component	Assigned Field
+2	DP Advisor	Data Store Server IP
+3	DP Advisor	Agent IP
+4	DP Advisor	Data Processor Tool
+5	IDPA System Manager	IDPA System Manager

Table 9 Backup IP address range assignments for the DP8300 and DP8800 with Dedicated Backup Network

Backup IP Range Allocation	Component	Assigned Field
+0	Data Domain	Management IP 1
+1	Data Domain	Backup IP 2
+2	Data Domain	Backup IP 3
+3	Data Domain	Backup IP 4
+4	Data Domain	Backup IP 5
+5	Data Domain	Backup IP 6
+6	Avamar	Proxy IP
+7	Search	Index Master Node 1
+8	Search	Index Data Node 1
+9	Search	Index Data Node 2
+10	Search	Index Data Node 3
+11	Search	Index Data Node 4
+12	IDPA System Manager	IDPA System Manager

Example 1 Sample configuration

For a DP5300 system with the specified range `192.0.2.1/13`, the IP assignments are:

Assigned IP Address	Component	Assigned Field
`192.0.2.1`	Data Domain	Management IP 1
`192.0.2.2`	Data Domain	Backup IP 2
`192.0.2.3`	Data Domain	Backup IP 3
`192.0.2.4`	Data Domain	Backup IP 4
`192.0.2.5`	Avamar	Server IP
`192.0.2.6`	Avamar	Proxy IP
`192.0.2.7`	DP Advisor	Application Server IP

Example 1 Sample configuration (continued)

Assigned IP Address	Component	Assigned Field
192.0.2.8	DP Advisor	Data Store Server IP
192.0.2.9	DP Advisor	Agent IP
192.0.2.10	DP Advisor	Data Processor Tool
192.0.2.11	Search	Index Master Node 1
192.0.2.12	Search	Index Data Node 1
192.0.2.13	IDPA System Manager	IDPA System Manager

Note

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

Customer Support tasks

This section describes IDPA components that require Customer Support for additional assistance.

Table 10 Customer Support tasks

Task	Description	Applicable IDPA models
Licensing	• If you are unable to find the right license keys for any of the components. • To obtain licensing for increased storage capacity.	All models.
Secure Remote Services (SRS)	To register customer site IDs to the SRS gateway.	All models.
Physical NDMP server	During fresh installation, configuration, and upgrade.	All models.
Physical Avamar Server	During fresh installation and upgrade.	• DP8300 • DP8800
Latest firmware, BIOS, and driver updates on all Dell Servers	For upgrading IDPA models on Generation 13 (Gen 13) servers.	• DP5300 • DP5800 • DP8300 • DP8800

Table 10 Customer Support tasks (continued)

Gen 13 Dell Servers must have two additional drives added per server, amounting to 7 SAS drives per ESX Server	For upgrading IDPA models on Generation 13 (Gen 13) servers.	• DP5300 • DP5800 • DP8300 • DP8800

CHAPTER 2

Monitor and manage the appliance

This chapter introduces the features and functionality of the ACM dashboard.

Topics include:

About the dashboard

The ACM dashboard enables you to manage settings for the appliance and individual components, update customer support information, and upgrade software for the appliance and its components. The ACM dashboard also performs system health monitoring for the appliance hardware.

To access the dashboard, type `https://<ACM IP address>:8543/` in a web browser and log in. The dashboard requires Google Chrome 64.0.3282.140 and later or Mozilla Firefox 47.2 and later.

Note

The dashboard is enabled only after configuring IDPA.

Note

The first time you log in to the dashboard, you must review and accept the terms of the End User License Agreement (EULA). After accepting the EULA, you must set the ACM password.

The initial view displays the **Home** page and tabs for **Health** and **Upgrade**.

Basic management tasks

The ACM dashboard enables you to view system details, change the password of appliance components, and log out from the dashboard.

Changing the appliance password

The appliance password is common for all IDPA point products/components.

1. Click the **Change Password** icon.
2. Type the **Current Password**.
3. Type and confirm the **New Password**.

   Note

   The password must contain 9 through 20 characters and include at least one of each type of supported character. The following types of characters are supported:

   - Uppercase letters (`A–Z`)
   - Lowercase letters (`a–z`)
   - Numbers (`0–9`)
   - Special characters: Period (`.`), hyphen (`-`), and underscore (`_`)
   - Must not start with a hyphen (`-`)

   The password must not include common names or usernames such as `root` or `admin`.

4. Click **Change Password**.
   The password change process for ACM and all the other IDPA components is initiated. The **Password change progress** shows the progress bar with status descriptions.

Note

The password change process takes approximately 40 minutes to complete.

The password gets changed for the users in the following sequence:

1. ACM internal LDAP user `idpauser`.
2. Storage (DDVE) `sysadmin` user.
3. Backup Server (Avamar) users:
   a. Operating system `admin` and operating system `root`.
   b. Avamar server users – `root`, `mcuser`, `repulser`, and `viewuser`.
4. Backup server proxy operating system `root` user.
5. IDPA System Manager(DPC) users: Operating system `admin` and operating system `root`.
6. Reporting and analytics (DPA) users: Application Server operating system `root`, Datastore operating system `root`, Application server `administrator`.
7. Search(DPS) operating system `root` and search default LDAP `root` and `admin`.
8. Cloud disaster recovery(CDRA) `admin` password.
9. VCenter and ESXi `idpauser` password.
10. ACM root password.

Note

After changing the password, ACM users will be logged out and they need to login again using the updated password.

Viewing version and build details
Click the **Information** (**i**) icon. The **About** page displays details about the IDPA version and build number.

Logging out
Click the **Log Out** button.

Appliance Configuration Manager dashboard Home

The **Home** tab provides an overview of the status and settings for the IDPA and each component.

On the dashboard **Home** tab, you can view the network configuration and product details, manage the password, time zone, SMTP, SNMP, and NTP settings, and modify customer support information.

You can also configure LDAP, create and download log bundles, download the current appliance configuration, shutdown the appliance, register components with Secure Remote Services (formerly ESRS), and install optional components such as Reporting and Analytics, Search, Data Protection Advisor, and Cloud Disaster Recovery (CDRA) if not already installed.

Note

The Secure Remote Services configuration link is present under gear icon menu for the relevant components. Mouse over on the gear icon to see a list of all the menu options.

Downloading the configuration details
To download a PDF containing the current details of the IDPA configuration, click the Adobe PDF icon.

Managing system components
The **Home** tab contains panels for each of the following:

- **IDPA System Manager**
- **Backup Server**
- **Protection Storage**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery**
- **Virtualization**
- **Customer Information panel**
- **General Settings**

Note

If a component cannot be reached on the network or has an incorrect stored credential, the corresponding panel prompts the user to resolve the issue.

IDPA System Manager panel

The **IDPA System Manager** panel displays the IDPA System Manager version and component IP address. To launch the web interface, click **IDPA System Manager Web UI** and log in.

Note

If external LDAP has not been configured then use `idpauser` as username. If external LDAP has been configured then use the LDAP username of the user.

Hover over **Services** to view the status information for **IDPA System Manager** services.

For more information about **IDPA System Manager** workflows and capabilities, refer to the *IDPA System Manager Administration Guide*.

Backup Server panel

The **Backup Server** panel displays the component IP address, Avamar version, total and available backup metadata storage, number of NDMP servers, license status of the Backup Server node, and whether the installation of agents is in progress. To launch the web interface, click **Backup Server Web UI** and log in. You can download the Avamar agents from the web interface.

For more information about the role of backup agents and how to install them, refer to the *Avamar Administration Guide*. Hover over **Services** to view the status information for Avamar services.

Enabling certificate verification

By default, vCenter certificate checking is disabled on the IDPA.

The IDPA uses a modified version of the Avamar `MCServer.xml` file. During configuration, this modification causes vCenter certificates to be ignored when adding vCenter servers. To enable certificate checking:

1. In the `MCServer.xml` file, change the `ignore_vc_cert` value to `false`. The `MCServer.xml` file is located in `/space/avamar/var/mc/server_data/prefs/mcserver.xml`.
2. Restart the MC service using `dpnctl`,
3. Stop `mcs` and `dpctl`, and
4. Start `mcs` commands on Avamar server.

Protection Storage panel

The **Protection Storage** panel displays the DD OS version, component IP address, total and available backup storage, the file system and license status of the Protection Storage node, and any alerts that require your action. To access additional functionality of the component, click the **Protection Storage System Manager** link.

Expanding storage capacity

You can add storage for Data Domain to expand the capacity of the Protection Storage node. Increasing the attached storage requires additional licensing.

Before you begin

- Obtain licensing for the increased storage capacity through ELMS (an electronic license management system, managing electronic software licenses enablement.)

Once the system detects the hardware, the **Expand storage** option is available in the gear icon menu.

Procedure

1. In the **Protection Storage** panel, mouse over the gear icon on the top right and click the **Expand storage**.

   The **Storage expansion and license upgrade** wizard appears.
2. Click **Browse** and select the required license files for the additional storage.
3. Click **Expand**.

Results

After several minutes, the dashboard reflects the increased storage capacity.

Configuring cloud long-term retention feature on IDPA

DD Cloud Tier is configured through ACM configuration. Follow the below procedures to create DD cloud units and configure Avamar back policies for cloud LTR.

Before you begin

Note

For detailed information on creating DD cloud units, refer *Data Domain Operating System Administration Guide*.

This process refers to the procedures in the following documents:

- *Data Domain Operating System Administration Guide* for DD OS 6.0 or higher
- *Avamar and Data Domain System Integration Guide* for Avamar 7.4 or higher

Procedure

1. On the **ACM** home tab, click the **Protection Storage System Manager** link.

   The **Data Domain System Manager** GUI is displayed.

2. Follow the "Importing CA certificates" procedure in the *Data Domain Operating System Administration Guide*.

   After importing the certificate, close the **Data Domain System Manager**.
3. Connect to the Avamar user interface through IDPA System Manager.

   The **Avamar Administrator** GUI is displayed.
4. Follow the "Adding or editing a Data Domain system with cloud tier support" procedure in the *Avamar and Data Domain System Integration Guide*.

   Note

   The ACM makes the step that refers to "Adding a Data Domain system" unnecessary. To learn how to access the **Edit Data Domain System** dialog box, refer to "Editing a Data Domain system."
5. Follow the "Creating a new tier group" procedure in the *Avamar and Data Domain System Integration Guide*.
6. To verify your configuration, click the **Activity** launcher button in **Avamar Administrator** and review the list of session on the **Activity Monitor** tab.

Reporting and Analytics panel

The **Reporting and Analytics** panel displays the Data Protection Advisor version, IP addresses for the Application Server and Datastore Server, the license status of the Reporting and Analytics node, and any alerts that require your action. To load the Reporting and Analytics console, click the **Reporting and Analytics Web UI** link. Hover over the **Services** to view the status information for Data Protection Advisor services.

If Data Protection Advisor is not configured during the initial configuration process, the panel displays a message indicating Reporting and Analytics is not configured. To configure the Reporting and Analytics node, click the message. The Reporting and Analytics Configuration screen is displayed. On the **Reporting and Analytics Configuration** screen, provide the required license information and IP addresses and click **Configure**.

IDPA also supports external Data Protection Advisor to analyze the system if you are running a corporate deployment of the Data Protection Advisor instance. However, IDPA dashboard does not display any data associated with the external Data Protection Advisor separately from the IDPA . Moreover, if you are using an external Data Protection Advisor instance, you must manage and configure any such external Data Protection Advisor instances. Also, IDPA does not support local analytics.

Search panel

The **Search** panel displays the Search version, LDAP host name, administrator group IP address for the Index Master node, and any alerts that require your action. To load the Search console, click the **Search** link. Hover over **Services** to view the status information for Search services.

If Search is not configured during the initial configuration process, the panel displays a message indicating Search is not configured. To configure the Search node, click the message. The Search Configuration screen appears. On the **Search Configuration** screen, provide the required IP address and click **Configure**.

Configuring clients in Search

To enable indexing for backup clients, additional configuration in Search is required. Refer to the procedures in the "Collections" chapter of the *Data Protection Search*

Installation and Administration Guide. In the **Sources** section of the **Collections** wizard, select the clients that are connected to the appliance.

All the domains under Avamar get indexed automatically. Only those client domains that are added post deployment of Search, are added manually.

Cloud Disaster Recovery panel

The **Cloud Disaster Recovery** panel displays the CDRA version, and alerts that require any action. To load the Cloud Disaster Recovery console, click the **Cloud Disaster Recovery Web UI** link.

Note

If you have configured an external CDRA, the **Cloud Disaster Recovery** panel does not display any events or data associated with the external CDRA. Moreover, you must manage and configure any such external CDRAs.

If CDRA is not configured during the initial configuration process, the panel displays **Click here to configure Cloud Disaster Recovery**, indicating that Cloud Disaster Recovery is not configured. To configure the Cloud Disaster Recovery node, click the message. The Cloud Disaster Recovery Configuration screen is displayed. On the **Cloud Disaster Recovery Configuration** screen, provide the IP address and click **Configure**.

Note

- Do not change Avamar root user password before configuring CDRA from the dashboard.
- Do not change Data Domain boost user password before configuring CDRA from the Dashboard.
- If a cloud account and email address are not configured during theCDRA configuration, the CDRA login page does not work. You have to configure cloud account and email address manually in CDRA.

Connect to the cloud account and add Cloud DR targets

Connect the CDRA to the Amazon Web Services account and add targets to the account.

Before you begin

- You have logged in to CDRA as administrator.
- You have an AWS account that is already configured before connecting to the cloud account.

Note

IDPA does the CDRA configuration automatically.

Procedure

1. Click **Cloud Account** on the menu bar.

   The **Connect to Cloud Account** page appears.
2. Click **Add Cloud Account**.
3. In the **Connecting to AWS Cloud account** dialog box, enter the access key and the secret key for the AWS account. http://docs.aws.amazon.com/IAM/

latest/UserGuide/id_credentials_access-keys.html provides information about obtaining the access and secret keys.

4. To copy the IAM policy, click **Copy IAM Policy**.

   This action copies to the buffer a JSON version of the minimum AWS user account permissions that are required for Cloud DR implementation, which can then be applied to AWS to set the permissions policy for the AWS user.

5. To view the Identity and Access Management (IAM) policy that represents the minimum AWS user account permissions that are required for Cloud DR implementation, click **Show IAM Policy**.

6. To save the AWS cloud account, click **Verify & Save**.

   The CDRA verifies that the account exists before saving the cloud account information and closing the **Connecting to AWS Cloud account** dialog box.

Note

When you have provided credentials to an AWS account, you cannot change to another AWS account.

Add cloud targets

You can add one or more cloud targets to the cloud account that includes selecting an Amazon S3 bucket and an encryption method.

Procedure

1. Click **Cloud Account** on the menu bar.

   The **Connect to Cloud Account** page appears.

2. Click **Add Cloud DR Target** to set up one or more Cloud DR targets on the cloud account.

   The Cloud DR target is the S3 bucket on AWS where data is written when VMs are backed up to the cloud. The Cloud DR Server is deployed on one of the targets.

   The **Add Cloud DR Target** dialog box opens.

3. Enter a name for the Cloud DR target.

   The name entered here appears in the Avamar Administrator when creating a Cloud DR backup policy.

4. Select an Amazon S3 bucket for the Cloud DR target.

5. Click **Advance security option** and select an encryption method:

Option	Description
SSE-S3	Default encryption (no cost)
SSE-KMS	Key management service encryption (incurs a cost)

Note

If you select the SSE-KMS encryption method, only the default customer managed key is supported. Changing the encryption key might cause errors with the files in the Amazon S3 bucket.

For more information about these encryption methods, see:

- SSE-S3 - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html
- SSE-KMS - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

6. Click **Add**.

Deploy the Cloud DR Server

Deploy the CDRS on a on a specific Cloud DR target.

Before you begin

- Cloud DR targets are required in the AWS account before performing this task. Connect to the cloud account and add Cloud DR targets on page 25 contains information about adding Cloud DR targets to the AWS account.
- AWS Marketplace terms must be accepted before deploying the Cloud DR Server.

Procedure

1. Click Cloud DR Server on the menu bar.
   - If no CDRS has been deployed, the **Deploy Cloud DR Server** page appears.
   - If the CDRS has already been deployed, the **Cloud DR Server** page appears. You cannot deploy additional CDRS instances.
2. In the **Cloud DR Server Configuration** section, select the Cloud DR target on which to deploy the **Cloud DR Server**.
3. To allocate IP addresses for the Cloud DR solution, provide the **IPV4 CIDR Range**.
4. In the **User Configuration** section, enter and confirm passwords for the CDRS Admin and CDRS Monitor users.

   The passwords must:

   - Be at least eight characters in length
   - Contain characters of a minimum of three of the following types:
     - English uppercase: A-Z
     - English lowercase: a-z
     - Numeric character: 0–9
     - Special (non-alphanumeric) characters

   a. Enter and confirm passwords for the CDRS Admin and CDRS Monitor users.

   b. Enter an email address for DD Cloud DR password reset requests.

   When the Cloud DR Server is successfully deployed, AWS sends an email to this address for verification. Follow the instructions in the email within 24 hours of deployment.
5. To confirm that you accept the marketplace terms, click the **I have accepted the AWS Marketplace terms** checkbox.
6. Click **Deploy** Cloud DR Server.

The CDRA begins deployment of the CDRS to the Cloud DR target. If an error occurs during deployment, click **Cleanup** to delete the cloud resources that CDRS creates, and then retry deployment.

Deploying the CDRS may take up to 30 minutes.

If the deployment is successful, the Cloud DR Server page appears, listing the hostname of the CDRS host, and the region. Also deployed are:

- A Virtual Private Cloud (VPC).
- An Amazon Relational Database Services (RDS) catalog, to maintain persistent data.
- A private subnet for communication between the RDS and CDRS.
- A public subnet (Standard Mode) or private subnet (Professional Mode) with internet access to be used by CDRS.
- The CDRS EC2 instance.

The M4.Large instance type is used for the CDRS instance. To reduce deployment costs, you may want to purchase reserved instances from AWS; otherwise an on-demand instance is used. An elastic IP address is automatically assigned to the CDRS instance. You cannot change this IP address.

Note

Multiple Cloud DR Add-on appliances can connect to a single Cloud DR Server instance. However, one Cloud DR Add-on appliance cannot connect to multiple Cloud DR Server instances.

Results

When the CDRS is deployed, connect to the Cloud DR Server by clicking the CDRS hostname.

Create rapid recovery images for protected VMs

You can accelerate the recovery process ahead of time by creating rapid recovery images for protected VMs.

Creating a rapid recovery image starts the rehydration process and converts the VMDK files to an Amazon Machine Image (AMI). The recovery process then launches the recovered instance from the AMI.

Perform this procedure when a new backup copy is available in the Amazon S3 bucket.

Procedure

1. In the CDRS user interface, select **Protection > VM Protection** in the navigation pane.

   The existing protected VMs appear in the right pane. The **Rapid recovery image** column indicates whether the VM is enabled for rapid recovery.

2. Select one or more VMs and click **Create Rapid Recovery Image**.

Results

- The CDRS creates the AMI and removes any previous AMI for an earlier copy.
- You can verify the results by reviewing the **Rapid recovery image** column.
- You can disable rapid recovery for a VM by selecting it and clicking **Disable Rapid Recovery Image**.

- You can monitor the protection status and its progress by reviewing the **Protection status** column.

Note

Ensure that when you set up Disaster Recovery for client VMs that need to be restored on the cloud using CDRA, the OS version on the client VMs must be supported by AWS at the time of restore. While performing a recovery to AWS, if the kernel version of the OS on the client VMs is not an AWS supported kernel version, then the recovery activities fail with an error message.

Perform a DR test or failover of a single VM

This procedure describes how to perform a DR test or failover on a single VM by using the Cloud DR Server interface.

Before you begin

To perform a DR test or failover of a VM by using the Cloud DR Server interface, you must have instances of virtual machines that are backed up by the on-premises backup software and copied to the cloud.

To ensure a successful failover, and better prepare for a disaster, best practices recommend testing various disaster recovery scenarios. After performing a DR test, you can promote the test to a failover.

When an operational error or disaster occurs on premises, you can fail over a VM to the public cloud. When the on-premise issue is resolved, you may fail the VM back to the on-premises environment.

Note

When performing failovers, you must fail over VMs in the correct order to ensure the continued operation of servers and applications.

Procedure

1. In the Cloud DR Server user interface, select **Recovery > VM Recovery**

   You can also open the **VM Recovery** page from the dashboard by clicking **See All** in the **Recovery** pane.

   The **VM Recovery** page appears.
2. Select the VM you want to recover and click **DR Test** or **Failover**.

   If you click **Failover** and the VM has never been tested, a message prompts you about this condition. Running a DR test is recommended before implementing a failover. The message also recommends that you shut down the production VM to avoid a possible data loss that is caused by accidental user access.

   Click **Select Copy** to continue.
3. On the **Copy and Network** window, select the VM copy and the network where you want to launch the EC2 instance.

   The **Advanced Options** section at the bottom of the window indicates the auto-selected EC2 instance type and security group to use for the recovery process.
4. If you do not want to use the auto-selected EC2 instance type or security group, expand **Advanced Options** and select an alternate EC2 instance type and one or more security groups.

5. Click **Start DR Test** or **Start Failover**.

Results

The recovery process begins and you can monitor progress on the **DR Activities** page. During the recovery process:

1. If the VM is not enabled for rapid recovery, a temporary Restore Service instance is launched in each region where recovery is needed. This instance performs hydration during recovery, and is automatically terminated after 10 minutes of idle time.
2. The Cloud DR Server then converts the VMDK to an AMI and launches an EC2 instance that is based on the AMI.
3. When the EC2 instance is running, the Cloud DR Server deletes the VMDK and AMI.

Virtualization panel

The **Virtualization** panel displays information about the internal virtual environment on the appliance, including the IP address and version of the vCenter server and ESXi host.

Customer information panel

The **Customer Information** panel displays the administrator contact and site information. To view the full value of an item, hover over the item.
Perform the following actions to change the customer information:

Procedure

1. In the **Customer Information** panel, click the **Edit** icon next to the value you want to change.
2. Type a new value:
   - **Admin Name**—Type the name of the administrator and click **Save**.
   - **Admin Number**—Type the phone number of the administrator and click **Save**.
   - **Admin Email**—Type the email address of the administrator and click **Save**.
   - **Company Name**—Type the name of the company and click **Save**.
   - **Location**—Type the location of the IDPA and click **Save**.
   - **Site ID**—Type the Site ID of the IDPA and click **Save**.

   You can verify your Site ID number on the Online Support website:

   a. Log in to the Online Support website with your credentials.
   b. Select **Service Center**.
   c. On the Service Center page, below the Sites and Contracts area, click **Administer a Site**.
   d. Ensure that the site where the storage system is installed is listed in the My Sites area.

Note

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

Results

Any new information that is provided is updated for the Backup Server node.

General Settings panel

The **General Settings** panel displays basic settings including time and network configuration. To view the full value of an item, hover over the item.
Perform the following actions to change the general settings information:

Procedure

1. In the **General Settings** panel, click the **Edit** icon next to the value you want to change.
2. Select or type a new value:
   - **Time Zone**—Select the time zone from the list and click **Save**. The time zone is updated for the Avamar, Data Domain, DP Advisor nodes, and Search nodes, the ACM, and the vCenter host server.

     NOTICE

     If this setting is changed, the Data Domain node restarts automatically.
   - **SMTP**—Type the SMTP server IP address and click **Save**. The SMTP server IP address is updated for the Avamar and Data Domain nodes and the vCenter host server.

     NOTICE

     If this setting is changed, the Avamar MCS and Backup Scheduler services restart automatically. Ensure that there is no backup running on the Avamar node before changing this setting.
   - **SNMP**—Type the SNMP server IP address and click **Save**. The SNMP server IP address is updated for the Avamar and Data Domain nodes and the vCenter host server.
   - **NTP**—Type the NTP server IP address and click **Save**. The NTP server IP address is updated for the Avamar, Data Domain, DP Advisor, and Search nodes, the ACM, and the vCenter host server.

     Note

     The NTP server must be specified by IP address. Do not use a server name in this field.
3. To change ACM DNS, perform the following step:
   a. Edit the `etc/resolv.conf` file, and then specify the IP address of the customer DNS server and the domain name.

      For example, when the customer environment has a public DNS server with an IP address of 10.254.66.23 and the domain name is mycompany.com, the `/etc/resolv.conf` file contains the following entries:

      Note

      The following output is an example, not the actual domain name and nameserver addresses. These values must be provided by the customer.

```
search mycompany.com
nameserver 10.254.66.23
nameserver 192.168.100.100
```

Note

Ensure that the entry for the public DNS server appears before the private DNS server. If the private DNS server appears first, the DPA integration with the Data Domain system will fail.

Configure external LDAP environment

You can change the default configuration to an external LDAP environment. By default, the application has the internal LDAP configuration.

The LDAP settings page on the ACM dashboard enables you to configure the existing LDAP settings. You cannot view the existing LDAP settings from the Configure LDAP settings page. Also, the LDAP account is used to login to IDPA System Manager and Search components only.

Note

If you want to view the LDAP settings, click the **Download current configuration** icon beside the **Shutdown appliance** icon on the ACM dashboard. The application generates a PDF file with the details of all the settings of the configuration.

To configure the LDAP settings, perform the following actions.

Note

Ensure that you meet the following LDAP password requirements while configuring the external LDAP environment:

- Use only the following characters:
  - Letters (`A–Z`, `a–z`)
  - Numbers (`0–9`)
  - Period (`.`)
  - Hyphen (`-`)
  - Underscore (`_`)
- Contain at least one supported special character
- Be no longer than 20 characters

Procedure

1. Select **LDAP type**.
2. Check **Secure LDAP** to specify if the LDAP is secure.
3. Enter **Server hostname**.
4. Enter **Domain name**.

Note

- The domain to which the **Server hostname** belongs should be the same as the **Domain name** specified.
- The domain name can be alphanumeric characters and special characters (-, _, ., =, and ,).

5. Enter **Query username**.

Note

The query username can be alphanumeric characters and special characters (-, _, ., =, ,, and @).

6. Enter **Query password**.

Note

The query password should be minimum 9 to 20 characters, contains at least lower case alphabet, upper case alphabet, digit and any of these special characters—-, _, and ..

7. Enter **Admin group name**.

Note

The **Admin group name** is case sensitive and must be identical to the group name entered in the LDAP server. If there is a mismatch in the names the configuration fails.

8. Enter **Port number**.
9. Click **Validate** to check the validation of your LDAP details.
10. Click **Submit**., and then **Close**.

    The settings have been updated to external LDAP environment.
11. Click **Close**.

Revert to internal LDAP environment

By default, the application has the internal LDAP configuration. However, if you have changed this default configuration to an external LDAP environment and if you need to revert it to internal LDAP environment, it consists of a three-stage procedure that you must follow.

Before you begin

If you know your internal LDAP password, note it down and keep it ready.

If you have changed the common appliance password after configuring the external LDAP, then your internal LDAP password is set to the old common appliance password when the internal LDAP was last used.

Verify Internal LDAP password

If you already know internal LDAP password, then perform the following steps to verify the password:

Procedure

1. Connect to the ACM by using an SSH client.
2. To validate your existing password, run the `ldapsearch` command with your password. An example is given below.

```
# ldapsearch -h ldaps:/<ACM_IP> -p 636 -D
uid=idpauser,ou=People,dc=idpa,dc=com -b dc=idpa,dc=com -w
<IDPAUSER_PWD>
```

Create internal LDAP password

If you do not remember the internal LDAP password, you must first set the internal LDAP password, by performing the following steps:

Procedure

1. Connect to the ACM by using an SSH client.
2. Generate a `hash` for the new password. An example input is given below.

```
vdppunvm340:/etc/openldap # slappasswd -s <NEW_PASSWORD>
```

3. Create a file with the modified `hash` file. An example is given below.

```
# vi /etc/openldap/update_idpauserpwd.ldif

dn: uid=idpauser,ou=People,dc=idpa,dc=com
changetype: modify
replace: userPassword
userPassword: <COMMAND_OUPUT_IN_FIRSTSTEP>
```

4. Execute the following command to update the password using the LDAP root password.

```
# ldapmodify -x -D cn=Manager,dc=idpa,dc=com -w
"<LDAP_ROOT_PASSWORD>" -f /etc/openldap/
update_idpauserpwd.ldif
```

   Where the *<LDAP_ROOT_PASSWORD>* is the same as the common appliance password.

5. Execute the `ldapsearch` command on the ACM with the new password to validate. An example is given below.

```
# ldapsearch -h ldaps:/<ACM_IP> -p 636 -D
uid=idpauser,ou=People,dc=idpa,dc=com -b dc=idpa,dc=com -w
<NEW_IDPAUSER_PWD>
```

Revert to internal LDAP environment

To revert to internal LDAP environment, perform the following steps:

Procedure

1. Update the LDAP settings from the ACM dashboard using the following values:
   - LDAP type: *OPENLDAP*
   - Secure LDAP: *Checked/selected*
   - Server hostname: *<ACM_HOSTNAME_FQDN>*
   - Domain name: *dc=idpa,dc=com*
   - Query username: *uid=idpauser,ou=People,dc=idpa,dc=com*
   - Query password: *<Internal LDAP user account password>*
   - Admin groupname: *dp_admin*
   - Port number: *636*
2. Connect to the ACM by using an SSH client.
3. Modify the following settings in the `/usr/local/dataprotection/var/configmgr/server_data/config/commonconfig.xml file`:

   <useExternalLdapSettings>true</useExternalLdapSettings> to *<useExternalLdapSettings>false</useExternalLdapSettings>*

Shut down the IDPA

You can shut down the IDPA appliance from the ACM console.

Before you begin

- Ensure that there are no backup jobs running on Avamar.

  Note

  - If there are backup jobs running on Avamar when the IDPA appliance shutdown operation is in progress, the shutdown operation waits for the Avamar jobs to complete with the status `Waiting for shutdown of Backup Server`.
  - It is recommended that you wait for the backup jobs to complete. However, if you must shut down the appliance immediately, and then you must log in to the Avamar UI and cancel the backup jobs that are in progress.
- Ensure that a validated checkpoint was taken in the last 36 hours on Avamar.
- Ensure that you have taken a backup of the MCS in the last 12 hours.
- Shutting down the IDPA appliance requires physical intervention, or use of IDPA, to restart the system. If you are remotely shutting down the IDPA appliances, ensure that you have physical access to the system, or have configured iDRAC on the system to power it back on.

To shut down IDPA, perform the following actions.

Procedure

1. On the ACM dashboard **Home** tab, click the **Shutdown Appliance** icon.
2. Enter the ACM root password, and click **Yes**.

   The appliance shut down progress is displayed.

Note

The IDPA appliance shuts down the components in the following order.

- Backup Server
- Search
- Reporting and Analytics
- System Manager
- Cloud Disaster Recovery Agent
- Protection Storage
- Appliance Configuration Manager
- vCenter Server
- Compute Node

Note

If the ACM initiated shutdown fails to shut down the **Backup Server**, **Protection Storage** or both components, the ACM displays a message that the ACM continues to shut down the other components.

Note

If any components fail to shut down, you must manually shut down the components. For more information about manual shut down of IDPA components, see Troubleshoot shutdown

Advanced backup configuration

The **Advanced Backup Configuration** tab allows an administrator to add, delete, or edit a NAS system on the IDPA.

Configuring NAS servers with NDMP Accelerators

Before you begin

Adding a NAS system requires at least one NDMP Accelerator.

From the **Advanced Backup Configuration** tab of the dashboard, an administrator can add the following supported NAS systems:

- EMC Celerra, EMC Unity, or EMC VNX
- EMC Isilon
- NetApp filer
- Oracle ZFS

This view also allows an administrator to edit or delete an existing connected NAS system.

Procedure

1. From **Advanced Backup Configuration** > **NAS** page, click **Add**.
2. Select the **NAS Type**, **Encoding Scheme**, and **NDMP Accelerator**.

3. Type the **NDMP Account Name**, **NDMP Account Password**, and **Avamar Account Name**.

   Note

   Only the following characters may be used in the NDMP account name: `a-z` (lowercase), '`.`', '`-`', and '`_`'.

   A green check mark indicates that the **NDMP Account Password** and **Confirm Password** field match.

4. Click **Save**.

Results

After adding a NAS system, you can create a protection job for the new system with the Avamar Administrator GUI.

Health

The **Health** tab displays status information and alerts for the hardware components of the IDPA and the vSphere alerts from the IDPA ESXi servers.

The IDPA uses Secure Remote Services to automatically send critical and fatal events to Customer Support for troubleshooting. A support ticket is opened based on the events that are received. Critical and fatal events are sent to Customer Support either after 30 min have elapsed, or when 30 events have accumulated, whichever occurs first.

By default, all events are deleted after 30 days. If no events have occurred in the selected time period, the **Event Summary** and **Event Details** panel indicate that there is no data available.

Event Summary

The **Event Summary** panel displays a summary of the status events on the appliance, grouped by **Device** and **Severity**.

To refresh the data displayed on the **Health** page, click the **Refresh** icon beside the **Event filter** list.

Note

The application refreshes the data based on the filters that you have selected.

To change the time period for which events are displayed, select an option from the **Event filter** list. Selecting **Today** lists events that have occurred from midnight to the present.

To show only events for a specific device or of a specific severity in the **Event Details** panel, click the corresponding wedge in the chart.

Event Details

The **Event Details** panel displays a list of the status events on the appliance. Use the **Component**, **Component Name** and **Severity** lists and click **Search** to filter the events and display the details of each event. To read more detailed information about an event, click its table entry. To export the list as a CSV file, click the **CSV** icon.

To clear the options selected in the filters, click **Reset**.

Troubleshooting

If a critical component of the health monitoring function is not working, the panels indicate that the service is down and an error message is displayed at the top of the

page. For more information about how to resolve issues with the **Health** tab, see Troubleshooting health monitoring on page 63.

Upgrade

The **Upgrade** tab allows an administrator to update the IDPA software. Refer to Upgrade the IDPA software (DP4400) on page 47 for more information.

Start up the IDPA

The following procedure is applicable only for DP5300, DP5800, DP8300, and DP8800 models. IDPA DP4400 model has only one ESXi Server and powering that ESXi Server ensures powering of all IDPA point products in the required sequence.

Powering on IDPA requires starting individual components in the correct order.

Procedure

1. Power on Data Domain system.
2. Power on the NDMP accelerator or accelerators if they are included in the configuration.

   Note

   Do not continue until both Data Domain and all NDMP accelerators are fully initialized. To verify that the Data Domain system is fully initialized, log in to the Data Domain system using `sysadmin` as the *username*, and for *password*, use the IDPA common password. Check the file system status using the `filesys status` command. The file system should be up and running. To verify that the NDMP accelerators are fully initialized, connect to the accelerator node using **SSH**.

3. For configurations with a physical Avamar implementation, power on the utility node and storage nodes.

   This step is not necessary for configurations with AVE.

   Note

   Do not continue until Avamar is fully initialized.

4. On IDPA DP5300, DP5800, DP8300, and DP8800 models, power on each of the ESXi servers, moving from the bottom ESXi server to the top.

Results

The remaining process finishes automatically. Once the ESXi servers are powered on, IDPA automatically starts all other components.
For issues during startup, see Troubleshooting startup on page 59.

Note

After IDPA starts successfully, you can connect to the ACM dashboard and monitor the progress of the Startup. If there is a failure in the Startup, the application displays an error message with an option to access the ACM dashboard page.

Access components with a browser

In addition to clicking the links in the ACM panels, you can access the user interface for individual components by browsing to the corresponding network location and typing the username and password.

In each of the following sections, *<component_ip>* refers to the IP address of the component. The credentials for Search and IDPA System Manager are determined by your LDAP setup.

Note

Ensure you are using Flash version 27.0.0.183 or later to access the vCenter web client.

Table 11 Access Components

Component	Location	Username
Avamar client manager	`https://<component_ip>/aam`	`MCUser`
Avamar user interface	`https://<component_ip>/mcui`	`MCUser`
Avamar SSH login		`admin`
Data Domain user interface	`https://<component_ip>`	`sysadmin`
IDPA System Manager user interface	`https://<component_ip>`	`<username>@<domain>` **Note** If external LDAP has not been configured, then the username is `idpauser`, by default.
DP Advisor user interface	`https://<component_ip>:90502/dpaui/jsp`	`administrator`
Search user interface	`https://<component_ip>/admin/#/login`	`<username>@<domain>` **Note** If external LDAP has not been configured, then the username is `idpauser`, by default.
vCenter web client	`https://<component_ip>`	`idpauser`

User accounts for components

The IDPA configuration uses the user accounts in Table 12 on page 40. By default, these accounts use the common IDPA password that is set from the **General settings**

page of the ACM UI. For information on how to change component passwords, refer to Change passwords and synchronize components on page 40.

Table 12 Component and user account mapping

Component	Using SSO	Username	Password
ACM	No	root	Common password provided during IDPA Appliance configuration.
IDPA System Manager (If external LDAP is not configured)	No	idpauser	Common password provided during IDPA Appliance configuration.
IDPA System Manager (If external LDAP is configured)	No	Respective LDAP credentials	External LDAP password as applicable.
Avamar	Yes	NA	SSO will take care of this logging in automatically.
Data Domain	No	sysadmin	Common password provided during IDPA Appliance configuration.
Data Protection Advisor	No	administrator	Common password provided during IDPA Appliance configuration.
Search	Yes	NA	SSO will take care of this logging in automatically.
CDRA	No	admin	Common password provided during IDPA Appliance configuration.
CDRS	No	admin or monitor	Password set during CDRS deployment.
vCenter	No	idpauser	Common password provided during IDPA Appliance configuration.
ESXi	No	idpauser	Common password provided during IDPA Appliance configuration.

Change passwords and synchronize components

Single-click user password change is one of the new features of IDPA. It is recommended that you use this feature for changing the password as it changes passwords for all the components in the IDPA.

Note

Changing passwords of individual components is not recommended. Due to any unforeseen circumstances, if you have to change passwords of individual components, refer the following section.

Changing passwords for individual components

Some changes to component passwords and settings require updating the settings of other components.

Changing a password for a component causes the ACM UI to display the `password out of sync` error message. To allow the ACM to gather health information for the component, you must update the stored password in the ACM UI to match. To update an unsynchronized password, click the error text.

Note

All passwords for the individual components must adhere to the IDPA requirements, even when they are changed on individual components.

Note

If you modify the password manually on Avamar and do not use the change password option on IDPA Appliance the system displays an error message when you try to update the password using the ACM dashboard. For more information about resolving the Avamar password being out of sync, see Credential mismatch

Data Domain settings

Updating the Data Domain password

For information about how to change the Data Domain `sysadmin` account password, refer to the *Data Domain Operating System Administration Guide*. After changing the password for the `sysadmin` account, log in to DP Advisor and update the Data Domain SSH credentials to match.

NOTICE

Update the Data Domain SSH credentials in DP Advisor immediately. Failure to do so can cause account lockout as DP Advisor repeatedly tries to connect with the old password.

After updating the password in DP Advisor, log in to the ACM and update the **Protection Storage** password to match.

Note

Do not change DD boost user password before configuring CDRA from Dashboard.

Avamar settings

Updating Avamar passwords

Avamar uses multiple user accounts, including `MCUser`, `viewuser`, server `root`, OS `admin`, and OS `root`. The IDPA requires that the OS `admin` and OS `root` accounts use the same password. The `MCUser`, `viewuser`, and server `root` accounts must also share a password, which can be different than the OS `admin` and OS `root` password. For more information about how to change an Avamar password, refer to the *Avamar Administration Guide*.

After changing the password for any Avamar account, log in to the ACM and update the **Backup Server** password to match.

If you change the `MCUser` account password, update it in the Search Admin UI. For more information about how to change the Avamar password for Search, refer to the *Data Protection Search Installation and Administration Guide*.

If you change the `viewuser` account password, update it in the DP Advisor UI. For more information about how to change the Avamar password in DP Advisor, refer to the *Data Protection Advisor Installation and Administration Guide*.

Updating the DD Boost user password

After changing the password for the Data Domain `DDBoostUser` account, log in to the **Avamar Administrator** GUI. Edit the Data Domain system settings and update the DD Boost user password to match. For more information, refer to the "Editing a Data Domain system" procedure in the *Avamar Administration Guide*.

Note

Do not change DD boost user password before configuring CDRA from Dashboard.

DP Advisor settings

Updating DP Advisor passwords

To change the DP Advisor `administrator` account password or `root` password, you must log in and change that password for each DP Advisor node. For more information about how to change a password in DP Advisor, refer to the *Data Protection Advisor Installation and Administration Guide*.

After changing the password on all nodes, log in to the ACM and update the **Reporting and Analytics** password to match.

Updating the Data Domain SNMP community string

If the community string is changed from its default value of *public*, DP Advisor must be updated to reflect the change.

1. Log in to Data Domain and change the community string with the following command, where *<community_string>* is the new string and *<Dpa_DC_Agent_IP>* is the IP address of the Data Collection Agent VM.

   ```
   snmp add rw-community
   <community_string> hosts
   <Dpa_DC_Agent_IP>
   ```

2. In the **Reporting and Analytics** panel of the ACM, click the **Reporting and Analytics Web UI** link.
3. Click **Manage Credentials** on the **Admin** > **System** page.
4. Select the **EMC Data Domain Credential** and update the community string to match.

Search settings

Updating the Search password

To change the Search OS `root` password, you must log in and change the OS `root` password for each Search node. For more information about how to change the OS `root` password, refer to the *Data Protection Search Installation and Administration Guide*.

After changing the password for the Search OS `root` account, log in to the ACM and update the **Search** password to match.

Note

`#`, `?`, `/`, and `\` are illegal characters for new passwords.

Updating the LDAP configuration for Search

If the LDAP query user password is changed, it may not be possible to log in to the Search Admin UI. To update this password, refer to the referenced procedures in the *Data Protection Search Installation and Administration Guide*.

1. The first time you log in to a Search node with SSH, you must accept the EULA. For more information, refer to the "Initializing the Data Protection Search environment" procedure in the *Data Protection Search Installation and Administration Guide*.
2. After accepting the EULA, select the option `[2] Configure Network Settings` and then press **F9** to quit.
3. When the system displays `Do you want to reboot now? y(es) or n(o):`, type **no**.
4. To update the LDAP configuration, complete the "Updating LDAP configuration in the Data Protection Search Admin installation script" procedure in the *Data Protection Search Installation and Administration Guide*.
5. Repeat steps 1–4 for each Search node.
6. Log in to each Search Index Data Node with SSH and run the command **service unicorn restart**.
7. Log in to the Search Index Master Node with SSH and run the command **service unicorn restart**.

vCenter settings

Updating the vCenter password for the ACM

For information about how to change the vCenter `root` password, refer to the documentation on the vCenter Support website. After changing the password:

Note

If you are manually changing the password for the vCenter Server, the password you set for the `vsphere.local\Administrator` and the `root user` accounts must be the same.

---

1. Log in to the ACM with SSH.
2. Change directory to `/usr/local/dataprotection/customscripts/tools`
3. Run the script `sync_vcenter_password.sh`
4. Modify the permissions on the script by running the command `chmod +x sync_vcenter_password.sh`

For more information about the `sync_vcenter_passwords.sh` script, run `sync_vcenter_passwords.sh -h`

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.

Updating the vCenter password for Avamar

1. Connect to the Avamar user interface with an SSH client as a user with the Administrator role.
   The **Avamar Administrator** GUI is displayed.

2. Locate the vCenter client in the vCenter domain.
3. Edit the vCenter client and update the `root` password to match.

Updating the vsphere.local\Administrator password
For information about how to change the `vsphere.local\Administrator` password, refer to the documentation on the vCenter Support website. The domain is `vsphere.local`.

ESXi settings

Updating the ESXi password
For information about how to change the ESXi password, refer to the documentation on the ESXi Support website. After changing the password:

1. Log in to the ACM with SSH.
2. Change directory to `/usr/local/dataprotection/customscripts/tools`
3. Run the script `sync_Switch_Server_ESX_Passwords.sh`
4. Modify the permissions on the script by running the command `chmod +x sync_Switch_Server_ESX_Passwords.sh`

For more information about the `sync_Switch_Server_ESX_Passwords.sh` script, run `sync_Switch_Server_ESX_Passwords.sh -h`

Note

The script `sync_Switch_Server_ESX_Passwords.sh` is named as `sync_ESX_Passwords.sh` for IDPA systems that shipped with version 2.0, although they have been updated to a newer version of the software.

LDAP settings

LDAP password requirements
The LDAP password must:

- Use only the following characters:
  - Letters (`A–Z`, `a–z`)
  - Numbers (`0–9`)
  - Period (`.`)
  - Hyphen (`-`)
  - Underscore (`_`)
- Contain at least one supported special character
- Be no longer than 20 characters

Switch Settings

If you have changed the password for the switch, you must follow the below procedure to synchronize the password with ACM. If the switch password is not synchronized with ACM, then the health monitoring of the switch may not work in ACM.

Before you begin

The *Administrator*

password and the *Enable Password* on the switch should be the same.

Procedure

1. After you have changed the switch password, login to ACM with SSH.
2. Open the *InfrastructureComponents.xml* file. The *InfrastructureComponents.xml* file contains passwords in an encrypted format.
3. To update the switch password, change the `isEncrypted` flag to `false` and type the password in plain text format between the password tag as shown below:

```
<Switch>
   <ipAddress>192.168.100.97</ipAddress>
  <username>admin</username>
<password isEncrypted="false">Idpa_12345 </password>
</Switch>
```

4. Stop and restart the data protection service on ACM using the below commands:

```
service dataprotection_webapp stop
service dataprotection_webapp start
```

   Your new switch password gets encrypted after restarting the ACM service.

Monitor the vSAN cluster

vSAN cluster is applicable for DP5300, DP5800, DP8300, and DP8800 models only. The IDPA hosts the component VMs on a three-node vSAN cluster. The cluster tolerates single-node or single-disk failure.

To ensure the vSAN cluster is operating without issue, monitor the cluster nodes daily using vCenter. If one of the nodes fails, a red circle with an exclamation point is displayed on its icon. Its state is marked **Not responding** and its disk group is not mounted. For information on connecting to vCenter, refer to Access components with a browser on page 39 and the documentation on the vCenter Support website.

Note

If one of the servers in the IDPA vSAN cluster fails, you must immediately log in to the **Avamar Administrator** GUI and disable the backup jobs in Table 4 on page 12 . For more information about disabling Avamar backup jobs, refer to the *Avamar Administration Guide*. To continue the IDPA working with two servers, contact Customer Support.

Note

Backup jobs are related to virtual machines hosted on the IDPA appliance. If one of the servers in the cluster fails, it may not be possible to take a snapshot of the VM, which leads to backup failure. Once all the three servers in the cluster are up and running, you must re-enable the backup jobs from the Avamar UI. For more information on re-enabling the backup jobs through the Avamar UI, refer to the *Avamar Administration Guide*.

CHAPTER 3

Upgrade the IDPA software (DP4400)

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

Topics include:

Upgrade components

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

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

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

Upgrade components:

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

Upgrade Prerequisites (DP4400)

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

Note

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

- Review the *Integrated Data Protection Appliance Release Notes* for information specific to the current release.
- Ensure that no file system cleaning activity is in progress on the Data Domain system by running the following command:
  `filesys clean status`
- If you have NDMP Accelerator nodes added to IDPA, you must manually upgrade the NDMP accelerator nodes. To upgrade NDMP accelerator nodes, see the *Upgrading the accelerator software* section in the *Dell EMC Avamar NDMP Accelerator for Dell EMC NAS Systems User Guide*.
- Ensure that at least one validated checkpoint is present on Avamar. If a validated checkpoint does not exist, ensure that you create one checkpoint before upgrading. To create a checkpoint, perform the following actions:
  1. Login to the Avamar utility node using SSH.
  2. Execute following commands as a root user:
     - `mccli checkpoint show`

This command displays all the Avamar checkpoints.

- `mccli checkpoint create --override_maintenance_scheduler=true –wait`
  This command returns the tag of the checkpoint created.
- `mccli checkpoint validate --cptag=CheckpointTagFromPreviousCommand --override_maintenance_scheduler=true –wait`
  This command validates the checkpoint

- An upgrade should be started only during a software upgrade maintenance window. Ensure that no other maintenance or backup activity is occurring on Avamar or Avamar Virtual Edition during the upgrade process. You can check the server status by running the following command on the Avamar server:

  `admin@vdppunvm140:~/>: opstatus.dpn`
- Ensure that all the ESXi passwords are synchronized with ACM. If you have changed the ESXi passwords, seeESXi settings on page 44 under the section Change passwords and synchronize components to synchronize them.
- Make sure that the ACM Dashboard is not displaying any `Password out of sync` for any of the components.
- Ensure that the VCenter passwords are synchronized with ACM. If you have changed the VCenter password, seevCenter settings on page 43 under the sectionChange passwords and synchronize components on page 40.
- If the upgrade process is still running, do not shut down/reboot the ACM or restart the *dataprotection_webapp* service. For some reason, if you have shut down/rebooted the ACM or restarted the *dataprotection_webapp* service while the upgrade process is still running, and if you are unable to see the progress of the upgrade after the ACM is rebooted, then contact Customer Support
- Ensure that the ESXi server is up and running, by verifying on the vCenter UI.
- Ensure that Avamar and Data Domain storage consumption is less than 85 percent. Refer to *Monitoring the system with the Avamar Administrator Dashboard* and *Monitoring Data Domain system capacity* sections in the *Dell EMC Avamar Data Domain System Integration Guide* for more information.
- Disable all the backup policies through the Avamar UI. Refer to the section *Enabling and disabling a backup policy* in the *Dell EMC Avamar Administration Guide*.
- Restart MCS on Avamar before starting the upgrade process to ensure Avamar is quiesced, so that the upgrade does not fail due to Avamar being busy. To restart MCS on Avamar , login to the Avamar Utility node with SSH (ssh login credential is `admin` and the password is the common appliance password that you would have provided) by using the Avamar IP address and run the `dpnctl stop mcs` command to stop and then run the `dpnctl start mcs` command to restart the Avamar server.
- Make sure that you check the health of the vCenter before the upgrade procedure. To check the health of the vCenter, login to the vCenter Web interface. If there are any critical alerts requiring user action, you must first fix those critical alerts before starting the IDPA upgrade procedure.

Upgrade the appliance software (DP400)

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

You can upgrade from IDPA version 2.2 to IDPA version 2.3 (on DP4400 models).

Procedure

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

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

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

   Note

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

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

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

5. Click **Validate**.

   Note

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

   The system validates the following:

   - VLAN status
   - Validates the connection to all components.
   - Validates the license status.
   - Validates if Avamar services are running.
   - Validates to ensure that no backup jobs are running on Avamar.
   - Validates if the DD capacity used is less than 85%.
   - Avamar checkpoint validation
   - ESX upgrade prerequisites:
     - Requires valid connection points to the required ESXi servers.
     - Requires that the applicable ESXi server is in maintenance mode.
     - Requires that the VCSA version is higher than ESXi version. In case, there is a major upgrade to VCSA, then the private IP address of the VCSA, `192.168.100.108` should not be in use.

     Note

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

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

6. Click **Upgrade**, type the ACM password, and click **Authenticate**.
7. To start the upgrade, click **Yes**. To cancel the upgrade, click **No**.

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

Note

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

Note

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

8. Relogin to the ACM.

   The **Upgrade Progress** displays:

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

Note

After the upgrade is complete, there can be a scenario where Avamar is in maintenance mode and the jobs cannot be executed at that time. After Avamar comes out of the maintenance mode, the jobs are executed

Note

After the upgrade is complete, acknowledge the notification `Event ConnectEMC notification failed` on the Avamar Administrator GUI. This notification is generated during upgrade when the Avamar service is disconnected.

Note

After the upgrade is complete, there is a warning on vCenter about a potential vulnerable issue that is described in CVE-2018-3646. IDPA uses the ESXi version which has the fix for this vulnerability, however this fix is not enabled by default as it has severe performance impact. Refer to the *IDPA Security Configuration Guide* for more information.

Results

The following components are updated:

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

The dashboard with all the products and their upgraded versions are displayed along with the newly configured ACM. If the upgrade process does not complete as expected, see Troubleshooting component software upgrades on page 69.
If the upgrade for any component fails, then the upgrade process is stopped until you troubleshoot and resolve the failure. However, if there are any noncritical warnings, the upgrade process continues. These warnings must be resolved once the upgrade process is completed.

Upgrade Postrequisites

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

- To save the log files from the upgrade process, click **Download logs** when the upgrade is complete. When you have finished, click **Finish**.
- After the upgrade process is complete, you must close the browser and start a new browser session before you relogin to ACM.
- The *Upgrading proxies* section of the *Avamar for VMware User Guide* provides instructions for upgrading the Avamar proxies. The upgrade must be performed on each Avamar proxy in the environment.

  Note

  Verify if the old Avamar proxy VMs still exist in your vCenter, and if they do, delete them from your vCenter after they are successfully replaced by the upgraded Avamar proxy VMs. To completely delete the old Avamar proxy VMs, click the **Delete from disk** option.

Upgrade CDRA manually

If your existing CDRA is not configured with CDRS, then your CDRA instance is replaced with the CDRA that is bundled within the IDPA release package. However, if your existing CDRA is configured with CDRS, then the IDPA release package does not upgrade your CDRA. You must manually upgrade it after the IDPA is upgraded from version 2.2 to version 2.3, using the IDPA user interface by first upgrading the CDRS, which in turn notifies you to upgrade the appropriate CDRA version.

For more information about Cloud Disaster Recovery Add-on (CDRA) compatibility for various IDPA versions, see the *Integrated Data Protection Appliance Software Compatibility Guide*.

IDPA version 2.2 is bundled with CDRA version 17.4. However, IDPA 2.3 is compatible with CDRA version 18.3 P2.

To upgrade from CDRA version 17.4 to 18.3 P2, first you must manually upgrade the CDRA from 17.4 to 18.1. Once you complete the upgrade from 17.4 to 18.1, then you must manually upgrade from 18.1 to 18.2. Once this upgrade is also complete, you must upgrade from 18.2 to 18.3 P2, which is compatible with IDPA 2.3.

Note

For detailed information about how to upgrade CDRA/CDRS, see the *Upgrade the Cloud DR Add-on*, *Upload upgrade packages for the CDRS and CDRA*, and *Upgrade the Cloud DR Server* procedures in the *Dell EMC Data Domain Cloud Disaster Recovery Installation and Administration Guide*, which can be obtained from Online Support website.

To upgrade the CDRA/CDRS from IDPA 2.2 to IDPA 2.3:

Procedure

1. Download the following Data Domain Cloud Disaster Recovery Upgrade Packages from the Online Support website at https://support.emc.com:
   - Data Domain Cloud Disaster Recovery 18.1 Upgrade Package.
   - Data Domain Cloud Disaster Recovery 18.2 Upgrade Package.
   - Data Domain Cloud Disaster Recovery 18.3 P2 Upgrade Package.
2. Upload the Data Domain Cloud Disaster Recovery 18.1 Upgrade Package to CDRS and upgrade the CDRS to 18.1.
3. Upgrade the CDRA to 18.1.
4. Upload the Data Domain Cloud Disaster Recovery 18.2 Upgrade Package to CDRS and upgrade the CDRS to 18.2.
5. Upgrade CDRA to 18.2.
6. Upload the Data Domain Cloud Disaster Recovery 18.3 P2 Upgrade Package to CDRS and upgrade the CDRS to 18.3 P2.
7. Upgrade the CDRA to 18.3 P2.

CHAPTER 4

Troubleshooting

This chapter contains basic troubleshooting information to help resolve possible issues.

Topics include:

System log files

To help troubleshoot issues, download bundled log files for the IDPA from the **Home** tab page directly. Select the **Download log bundle** option from the log bundle icon available on the **Home** tab page to download the log files. The log files for the specified components are saved in the folder `/Downloads/` on the system in a compressed format.
During an upgrade, additional log files are generated in a different location. For more information, refer to Upgrade log files on page 72.

Note

The user should not create or copy their logs in `/data01/log_bundle` folder as this functionality deletes all existing log while creating log bundle.

Troubleshoot shutdown

During the shut down process, if the appliance or any of the components fail to shut down automatically, you can manually shut down the IDPA appliance and its individual components.

Note

Since Avamar and Data Domain are still running on IDPA the infrastructure components like the vCenter and ESX are also running. To shut down the Avamar and Data Domain you must also shut down the vCenter and ESX components manually.

Shut down Avamar manually

This section provides you information about how to shut down the Avamar component manually for the various IDPA Appliances.

DP8300 and DP8800

This section provides you information about how to shut down the Avamar component manually in the DP8300 and DP8800 appliances.

To manually shut down the Avamar component, perform the following actions.

Procedure

1. Login to the Avamar server with SSH by using the Avamar IP address.
   a. Load the SSH keys by running the following commands.

      ```
      ssh-agent bash
      ```

      ```
      ssh-add ~admin/.ssh/admin_key
      ```

   b. Verify that no maintenance jobs are running on the Avamar server by running the following command.

      ```
      status.dpn
      ```

   c. Create a checkpoint by running the following command:

      ```
      mccli checkpoint create --override_maintenance_scheduler
      ```

d. Backup the MCS data by running the following command:

```
mcserver.sh --flush
```

e. Stop all Avamar services by running the following command.

```
dpnctl stop all
```

f. Answer `yes` to the EMS question.

g. Verify that the Avamar services stop when you run the following command.

```
dpnctl status
```

h. Prepare the Avamar nodes for shut down by running the following commands

```
mapall --user=root --all 'touch /fastboot' mapall --user=root
--all 'halt'
```

i. Power off all nodes in the grid.

DP5300, DP5800, and DP4400

This section provides you information about how to shut down the Avamar component manually in the DP5300, DP5800, and DP4400 appliances.

To manually shut down the Avamar virtual edition component, perform the following actions.

Procedure

1. Login to the Avamar Virtual Edition (AVE) server with SSH by using the Avamar IP address.
   a. Create a checkpoint by running the following command.

   ```
   mccli checkpoint create --override_maintenance_scheduler
   ```

   b. Backup the MCS data by running the following command:

   ```
   mcserver.sh --flush
   ```

   c. Stop all Avamar services by running the following command.

   ```
   dpnctl stop all
   ```

   d. Power off the AVE from vCenter.

Note

If you have the DP4400 appliance, then you must shutdown ESX. For more information about manual shut down of ESX, see Shut down ESX manually.

Shut down Data Domain manually

This section provides you information about how to shut down the Data Domain component manually.

To manually shut down the Data Domain component or the DDVE, perform the following actions.

Note

The manual shut down for Data Domain system is applicable for the DP5300, DP5800, DP8300, and DP8800 appliances.

Note

The manual shut down for DDVE is applicable for the DP4400 appliance.

Procedure

1. Open a new SSH session to login to the Data Domain system and DDVE.
2. Shut down the Data Domain or DDVE system by running the following command.

   ```
   system poweroff
   ```

   Note

   If you have the DP4400 appliance, then you must shutdown ESX. For more information about manual shut down of ESX, see Shut down ESX manually.

Shut down vCenter manually

This section provides you information about how to shut down the vCenter manually.

This procedure to shut down vCenter manually is applicable for all models of IDPA. To manually shut down the vCenter, perform the following actions.

Procedure

1. Open a browser and enter the IP address to access vCenter.

   The login page is displayed.
2. Enter your username and password on the vCenter login page.
3. Shut down the Data Protection virtual application.

   Note

   All virtual machines and virtual applications under Data Protection virtual application are automatically shut down.
4. Shut down the IDPA Virtual Machine Guest operating system and the virtual machine.

Shut down ESX manually

This section provides you information about how to shut down the ESX manually.

This procedure to shut down ESX manually is applicable for all models of IDPA. To manually shut down the ESX, perform the following actions.

Procedure

1. Login to the ESXi server on which the vCenter is installed.
2. Login to each ESXi host.

3. Set all ESXi hosts into maintenance mode by running the following command on each host

   ```
   esxcli system maintenanceMode set -e true -m noAction
   ```

4. Shut down all ESXi host using the vSphere client or the ESXi host.

Troubleshooting startup

If one part of the startup process fails to complete automatically, the problem can be resolved manually to allow startup to continue.

Avamar does not start
If Avamar does not complete startup, connect to the Avamar server. If Avamar reports that GSAN did not shut down cleanly, select the option to roll back to the last checkpoint.

The ACM does not start
If the ACM service does not start within 2 hours and 15 minutes of powering on the appliance, one or more of the following components are not powered on or are not accessible on the network:

- Data Domain
- AVE

The Data Domain component must be powered on and accessible before the ESXi host is powered on.

1. Verify that the components that are required for the configuration are powered on.
2. Verify that the required components are accessible on the network. Resolve any connectivity issues that are encountered.
   - If the ACM loads successfully, skip the rest of this procedure. The Search nodes, DP Advisor nodes, IDPA System Manager, AVE, and Avamar Proxy start automatically.
   - If all required components are powered on and accessible, but the ACM does not load, restart the ACM service:
3. Stop the `dataprotection_webapp` service:
   ```
   service dataprotection_webapp stop
   ```
4. Start the `dataprotection_webapp` service:
   ```
   service dataprotection_webapp start
   ```

The Search nodes, DP Advisor nodes, IDPA System Manager, AVE, and Avamar Proxy start automatically.

The VMs do not start
Switch on the power button present on the Dell Server. The ACM internally executes `local.sh (/etc/init.d/local.sh)` and the VMs start automatically. To start the VMs manually:

1. Move ESXi out of maintenance mode manually.

   Note

   To do this, log in to ESX using `idpauser` and select **Exit maintenance mode**.

2. Start the DataProtection-VCSA by running the `/etc/init.d/local.sh` script on ESXi or power on the VM from the ESXi.
   DataProtection-ACM VM starts five minutes after the VCSA VM starts.
3. If DDVE VM is not up, click the **Power on** button to start the DDVE VM.
   Code waits filesystem status to show up and running.
4. If AVE is not started, start AVE VM from ESX UI.
5. login to AVE using admin credentials.
   ACM executes `dpnctl status all`, `dpnctl start all`, and `dpnctl start maint` commands.
6. If something goes wrong, execute the following in sequence and click the **Power on** button:
   - DataProtectionSearch Vapp
   - DPADatastoreServer VM
   - DPAApplicationServer VM
   - DataDomainCloudDR VApp
   - DataProtectionCentral VApp
   - AVProxy VM
7. Login to the DPA Application Server VM using SSH.
8. Stop all DPA Application Services by executing the following command:
   `/opt/emc/dpa/services/bin/dpa.sh service stop`

   Continue to ignore if there are any errors.
9. Login to the DPA Application Server VM using SSH.
10. Stop all DPA Datastore Server services by executing the following command:
    `/opt/emc/dpa/services/bin/dpa.sh service stop`
11. Verify if all the services are stopped on the DPA Application Server and on the DPA Datastore Server by executing the following command:

    `/opt/emc/dpa/services/bin/dpa.sh service status`
12. Once all the services on both the DPA Application and the DPA Datastore servers are stopped, restart the services on the DPA Datastore Server by executing the following command:

    `/opt/emc/dpa/services/bin/dpa.sh service start`
13. Once all the services on the DPA Datastore servers are started, restart the services on the DPA Application Server by executing the following command:

    `/opt/emc/dpa/services/bin/dpa.sh service start`
14. You must wait for sometime until all the services are started on DPA Datastore Server. You can verify the status by executing the following command:
    `/opt/emc/dpa/services/bin/dpa.sh service status`
15. You must wait for sometime until all the services are started on DPA Application Server. You can verify the status by executing the following command:

    `/opt/emc/dpa/services/bin/dpa.sh service status`
16. If DPS vApp does not get started, start the vApp.
17. Start the services of Search by logging in to index master IP using OS root credentials and execute following commands:

    a. `service elasticsearch start`

b. `service search-cis-core start`
c. `service search-cis-schedule start`
d. `service search-networker-worker start`
e. `service search-networker-action start`
f. `service search-avamar-worker start`
g. `service search-avamar-action start`
h. `service search-worker start`
i. `service search-adminapi start`
j. `service search-api start`

18. Login to VCSA using **`idpauser`** credentials, select **AVProxy** VM and click the **Power on** button.
19. After IDPA starts, start two services of Avamar using `dpnctl start emt`.

Adding a CA-signed certificate

The ACM includes a self-signed certificate, which may cause the browser to report an unsecured connection. To resolve this issue, replace the default certificate with a CA-signed certificate.

Before you begin

- Access the IDPA command line using one of the following procedures:
  - Log in to vCenter, right-click the DataProtection-ACM VM, and select **Open Console**. Type the ACM credentials.
  - Connect to the ACM by using an SSH client to access its IP address. Type the ACM credentials.
- Change the directory to `/root`

Procedure

1. Stop the Tomcat server.

   `service dataprotection_webapp stop`

2. Back up the existing keystore file.

   `cp /root/.keystore /root/.keystore.bkp`
   Use the backup if you encounter any errors in this process.

3. Delete the existing self-signed certificate from the keystore.

   `/usr/java/latest/bin/keytool -delete -alias tomcat -storepass changeit`

4. Create a new certificate.

   `/usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -keyalg RSA -sigalg SHA256withRSA -keystore /root/.keystore -storepass changeit -keypass changeit -validity 3650 -dname "CN=idpa.companyname, OU=Idpa, O=CompanyName, L=Hopkinton, S=Massachusetts , C=US"`

5. Generate a CSR file for the keystore.

   `/usr/java/latest/bin/keytool -certreq -alias tomcat -keyalg RSA -file /root/ACM_Host.csr -keystore /root/.keystore`

6. Get the CA-signed certificate in the .p7b format by using the CSR content and save the certificate.
7. Import the new certificate into the keystore.

   /usr/java/latest/bin/keytool -import -alias tomcat -file /root/certnew.p7b -keystore /root/.keystore
8. To ensure `/usr/local/dataprotection/tomcat/conf/server.xml` is using the `/root/.keystore` file, check the value of the `keystoreFile` attribute for the HTTP Connector.
9. Verify the certificates in the keystore.

   /usr/java/latest/bin/keytool -list -keystore /root/.keystore -alias tomcat
10. Start the Tomcat server.

    service dataprotection_webapp start

Configure secure AD having self-signed Certificates on IDPA

If you are using secure AD with self-signed Certificates, search fails to configure if the self-signed certificate is not present on search VM.

Procedure

1. Export root CA certificate.

   Refer https://support.microsoft.com/en-us/help/555252 to know how to export the root CA certificate.
2. Log into the Root Certification Authority server or Active Directory Server with administrator account.
3. Go to **Start** > **Run**, type **cmd**, and press **Enter**.
4. To export the Root Certification Authority server into a new file name `ca_name.cer`, run `certutil -ca.cert ca_name.cer`.
5. Convert certificate as PEM format as follows:
   a. Cy `ca_name.cer` to Search Master.
   b. Run `openssl x509 -in ca_ name.cer -inform der -out ca_name.pem -outform pem`.
   c. Copy this `ca_name.pem` to `/etc/pki/trust/anchors/` on Search Node.
6. Do LDAP Configuration from Dashboard.

Troubleshoot Avamar

If there is a problem with Avamar, the **Backup Server** panel in the ACM dashboard displays the following status:

`Backup Agents Installation in progress...`

Possible causes for this issue include:

- The Avamar service, Avamar, or AVE is down.
- Avamar cannot be pinged.
- There is a mismatch between the Avamar administrator password and the password stored in the ACM.

The Avamar service is down
To start the Avamar service:

1. Using an SSH client, connect to the Avamar Utility node as the admin user.
2. Type the command `dpnctl start all`

Avamar or AVE is down
Power on the Avamar or AVE server.

Avamar cannot be pinged
If Avamar cannot be pinged, find and resolve the source of the issue. Possible causes include:

- The Avamar server is down.
- There is a network connectivity issue.
- The Avamar server has a hardware issue.

Credential mismatch

This section provides information about how to resolve the password mismatch scenario for Avamar. If you modify the password manually on Avamar and do not use the change password option on IDPA Appliance the system displays an error message when you try to update the password using the ACM dashboard.

To resolve a password mismatch, perform the following actions.

Procedure

1. Click the warning message in the **Backup Server** panel and enter a new password.

   The system displays a **Failed to update Backup Server info search** error message.
2. Click the **Refresh** button on the ACM dashboard.
3. Click **Update Password** in the **Backup Server** panel and enter a new password.

   The system displays a **Avamar MCUser test connection failed** error message.
4. Click the **Refresh** button on the ACM dashboard.
5. Click **Update Password** in the **Backup Server** panel and enter a new password.

   The system updates the new password.

Troubleshooting health monitoring

If there is an issue with SNMP or one of the health monitor processes, the **Health** tab cannot display data.

SNMP validation errors
By default, the ACM validates the SNMP configuration of the switch and Dell servers every 4 hours. If the ACM detects that the SNMP configuration for a component is disabled or missing, it automatically corrects the configuration.

If the ACM cannot reach one of the components on its internal IP, the following message is displayed on the **Health** tab: `Failed to validate SNMP configuration on component(s) <unreachable-component>`

To resolve this issue:

1. Verify that the internal IP addresses of IDPA Appliance server is reachable on the network.
2. If the component is reachable on the network, verify SSH connectivity by attempting to connect with the default SSH password. If an SSH connection cannot be established, revert the SSH password on the component to the default password.

Note

Refer Changing passwords and synchronizing components to know how to change passwords and synchronize components.

Health monitor processes errors

If the SNMP Receiver port, Message Broker service, or Database service is down, the following message is displayed on the **Health** tab: `Health monitor processes are down : <process>`

To resolve this issue, connect to the ACM using SSH and follow the procedure that corresponds to the error message:

- If the SNMP Receiver port is down, verify that port 161 is enabled. If the port is enabled and the problem persists, restart the Tomcat service with the following command:

  ```
  service dataprotection_webapp restart
  ```

- If the Message Broker service is down, verify that the RabbitMQ service is running with the following command:

  ```
  service rabbitmq-server status
  ```

  If the service is not running, start it with the following command:

  ```
  service rabbitmq-server start
  ```

- If the Database service is down, verify that the PostgreSQL service is running with the following command:

  ```
  service dataprotection_database status
  ```

  If the service is not running, start it with the following command:

  ```
  service dataprotection_database start
  ```

Verifying the switch configuration

If the internal IP for the switch is not set, configured as default, or disabled, a critical error occurs.

Before beginning a system upgrade, verify that the switch configuration is correct, and correct it if necessary. The same process can also be used to resolve the error that occurs when the switch configuration is not correct.

Establish a physical connection to the Dell switch

Establish a connection between the USB port on your laptop and the serial port on the Dell switch.

This connection requires two cables:

- RJ45 to serial cable. The following figure shows a RJ45 to serial cable.

  Figure 1 RJ45 to serial cable

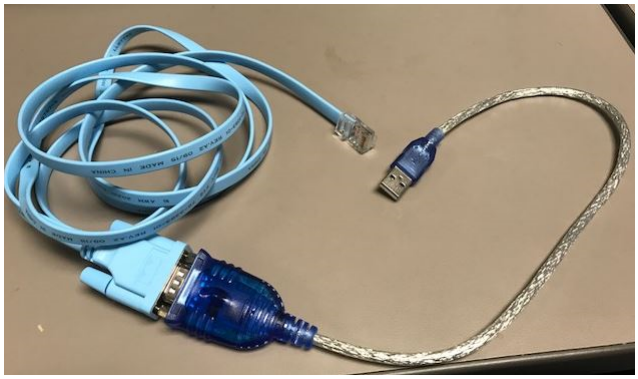
- USB to serial cable. The following figure shows a USB to serial cable.

  Figure 2 USB to serial cable

The following figure shows the two cables connected together. Connect these two cables and plug the RJ45 end into the switch and the USB end into your laptop.

Figure 3 RJ45 cable connected to the USB cable



The following figure shows the serial port circled in red, on the back of the Dell switch while looking at the front of the cabinet. Above the serial port is the switch management port that is connected to the network.

Figure 4 Serial port on the Dell switch

Note

You must order the necessary cables for the switch. They are not included with IDPA.

Configure a serial connection to the Dell switch

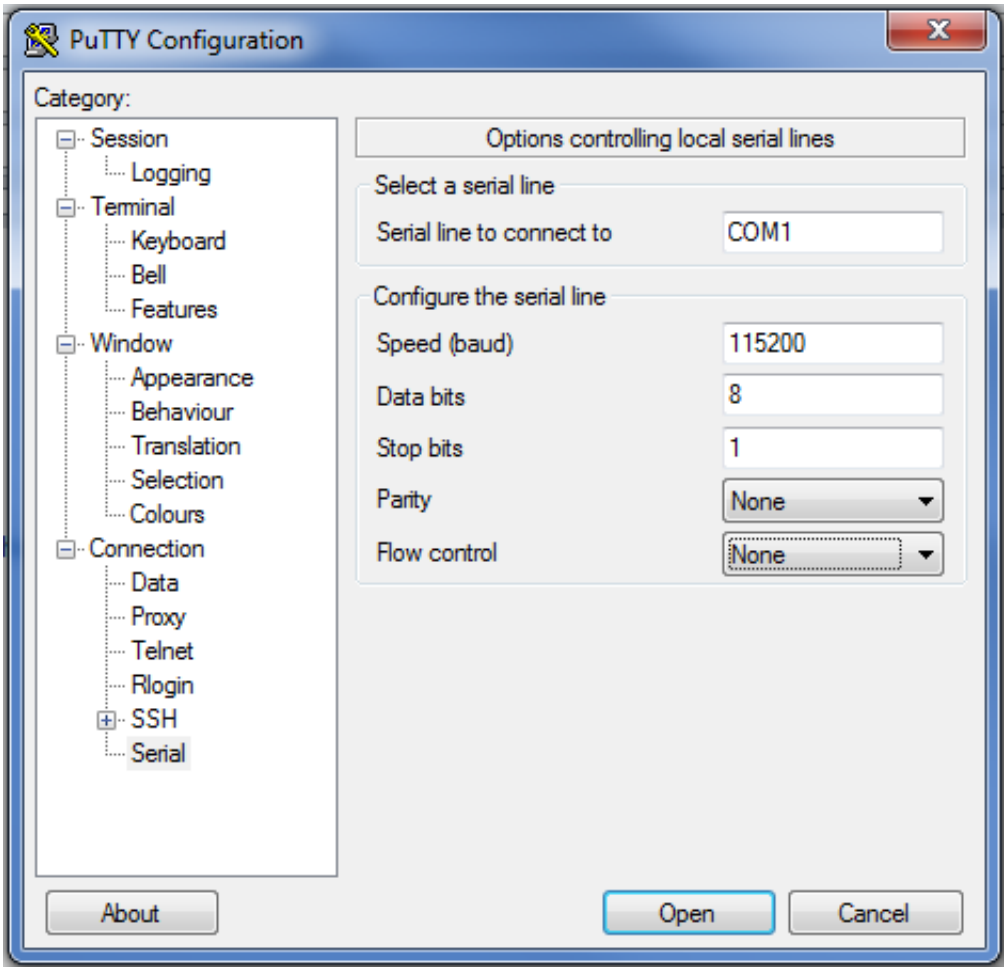
Perform the following steps on your laptop to establish a connection to the switch:

Procedure

1. Start the Putty application, from the **Category** navigation tree, select **Serial**, and then configure the following options:
   - Speed (baud): 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: none
   - Flow control: none

   The following figure shows the **Serial Connection Configuration** window.

Figure 5 Serial Connection Configuration window



2. Click **Open**.

Verify VLAN 121 is configured on the switch

Connect to the Dell switch and verify that the VLAN ID and internal IP address required by IDPA is configured on the switch.

Before you begin

The following values are required:

- VLAN ID: 121
- IP address: 192.168.100.97
- Netmask: 255.255.255.224

Perform the following steps through the Putty connection over the serial connection to the switch:

Procedure

1. Start the EXEC privilege mode by typing the `enable` command.

   The Password prompt appears and displays output similar to the following:

   ```
   DPappliance-switch>enable
   Password:
   ```

2. At the **Password** prompt, type the password for the admin account.

   Output similar to the following appears:

   ```
   The SupportAssist EULA acceptance option has not been
   selected. SupportAssist
   can be enabled once the SupportAssist EULA has been
   accepted. Use the:
   'support-assist activate' command to accept EULA and
   enable SupportAssist.

   DPappliance-switch#
   ```

3. Verify the status of VLAN 121 by typing the **`show interface Vlan 121`** command.

   - The following output appears if VLAN 121 is configured:

     ```
     Vlan 121 is up, line protocol is up
     Vlan alias name is: dpa_esx_mgmt
     Address is 14:18:77:23:ef:7b, Current address is
     14:18:77:23:ef:7b
     Interface index is 1275130368
     Internet address is 192.168.100.97/27
     Mode of IPv4 Address Assignment : MANUAL
     DHCP Client-ID(61): 14187723ef7b
     MTU 1554 bytes, IP MTU 1500 bytes
     LineSpeed 1000 Mbit
     ARP type: ARPA, ARP Timeout 04:00:00
     Last clearing of "show interface" counters 15w6d5h
     Queueing strategy: fifo
     Time since last interface status change: 6w5d16h
     Input Statistics:
     290706216 packets, 335648042970 bytes
     Output Statistics:
     295834439 packets, 336248091631 bytes
     ```

   - The following output appears if VLAN 121 is not configured:

     ```
     Error: No such interface Vl 121.
     ```

4. If necessary, configure VLAN 121 with the required IP address and netmask:

   a. Start the configuration mode by typing the following command:

      `configure`

      Output similar to the following appears:

      ```
      DPappliance-switch#configure
      DPappliance-switch(conf)#
      ```

   b. Start the interface mode for VLAN 121 by typing the **`interface vlan 121`** command.

      Output similar to the following appears:

      ```
      DPappliance-switch(conf)#interface vlan 121
      DPappliance-switch(conf-if-vl-121)#
      ```

   c. Assign the IP address to the management NIC by typing the **`ip address 192.168.100.97 255.255.255.224`** command.

      `ip address 192.168.100.97 255.255.255.224`

      Output similar to the following appears:

```
DPappliance-switch(conf-if-vl-121)#ip address
192.168.100.97 255.255.255.224
```

d. Type the **exit** command twice to return to the top level of the Dell switch interface.

Troubleshooting component software upgrades

You can troubleshoot the upgrade failures using the different options available.

Retry upgrade process

When there is an upgrade failure for a component, the progress bar is displayed in red and you can see the **RETRY** and **DOWNLOAD LOGS** buttons. Click **RETRY** to retry the upgrade again.

Alternatively, you can click **DOWNLOAD LOGS** to download the log files.

If the Avamar upgrade fails while upgrading the IDPA appliance software, and if you are retrying the Avamar upgrade even after 24 hours of failure, then you must manually upgrade the Avamar server.

If the Avamar upgrade fails during the **RETRY** operation, with a message `Validated checkpoint not found`, then you must manually upgrade the Avamar server and click the **Sync** button which is displayed for the failed component, in this case, Avamar.

Advanced troubleshooting (support only)

When there is an upgrade failure even after using the Retry option, the technical support professional can use the Rollback and Sync options to troubleshoot the upgrade failure.

Using rollback

The Rollback option reverts the component to its previous state using the snapshots taken. The upgrade process uses vSphere snapshot technology to preserve the preupgrade configuration of the IDPA. Before a component is upgraded, a snapshot of the component VM is created. When the upgrade is completed successfully, the snapshots are deleted. If the upgrade fails, the snapshots are used to revert the components to their previous state. If the upgrade fails and any of the VMs are not restored, review the information in Upgrade log files on page 72 and contact Customer Support.

Note

If upgrading DD OS is not successful, contact Customer Support.

---

1. In the **Upgrade progress** window, select **Troubleshooting (Support only)** checkbox at the top.
   The **ROLLBACK** button is displayed for the component with upgrade failure.
2. Click **ROLLBACK**.
   The component reverts to the previous version. Refer to the section Rollback is Successful on page 70.

   If rollback is unsuccessful, see the section Rollback Failed on page 70.

Using Sync

When there is an upgrade failure, the support personnel can manually update the specific component in the background. However, when the upgrade of a particular point product fails, and if a manual upgrade is performed on the failed point product, then the **Sync** functionality does not verify the operating system version of the point product. The customer/CS performing the manual upgrade must ensure that the appropriate operating system rollup is applied to the point product before manually upgrading it.

For more information about operating system rollup versions and their associated patches if applicable, see the *Integrated Data Protection Appliance Software Compatibility Guide*.

After the manual update, follow these steps:

1. In the **Upgrade progress** window, select **Troubleshooting (Support only)** checkbox at the top.
   The **SYNC** button is displayed for the component with upgrade failure.
2. Click **SYNC**. The **SYNC** validates the manually upgraded component version and reflects the upgrade progress bar in green and status to completed.

Rollback is Successful

IDPA is rolled back to its previous state.

No manual action is required from your side. You can login to dashboard to ensure that all the services are up and running.

Optionally, after analyzing the logs, if you find any issues with the upgrade, you can go to upgrade once again.

You can download the logs from the upgrade progress user interface. Alternatively, you can also retrieve the logs from `/data01/upgradeLogs` directory on the **Appliance Configuration Manager**.

Rollback Failed

If the IDPA rollback fails during the upgrade procedure, you need to perform the following manual steps.

Many of these steps are most like completed by the IDPA upgrade workflow as IDPA upgrade does not stop operations if an error is encountered.

Procedure

1. Check for all the products in VMware vCenter to ensure there is no snapshot by the name *BeforeUpgrade*. If the *BeforeUpgrade* snapshot exists, you must delete that snapshot. To delete the *BeforeUpgrade* VMware vCenter snapshots from all the components, perform the following steps on each of the component where *BeforeUpgrade* snapshot exists:
   - Avamar Proxy:
     a. Revert to the snapshot and then delete the snapshot.
   - AVE Server:
     a. Shutdown the AVE VM.
     b. Revert to the snapshot and delete the snapshot.
     c. Change all the data disks to independent-persistent.

d. Power on the AVE VM to verify if all the AVE services are up and running.

- DPA VMs:

a. Revert to snapshots of all DPA VMs such as DPA Datastore Server, DPA Application Server, DPA Agent, DPA DD Processor Tool, and so on.

b. Delete the snapshots.

c. Login using putty to the DPA Datastore Server and note down the datastore directory in `/data01` with the name *datastore-xxxx*

d. Execute following command:

```
/opt/emc/dpa/services/bin/dpa.sh datastore import /
data01/datastore-*/
```

e. Login to the DPA Application Server using putty and execute the following command:

```
/opt/emc/dpa/services/bin/dpa.sh service start
```

f. Verify that the services are correctly starting by navigating to *https://dpaAppServerIp:9002*

- DPS VMs:

a. Stop the DPS Services.

b. Shutdown or power off the DPS Vapp.

c. Revert to the snapshot *BeforeUpgrade*.

d. Delete the snapshot *BeforeUpgrade* from all DPS VMs.

e. Change hard disk 3 mode to independent-persistent for all the DPS VMs.

f. Power on the DPS VApp.

g. Ensure that all DPS Services are up and running.

- DPS Index Master Node Services:

a. Login to DPS Master Index Node using putty.

b. Execute the following commands:

  - `service dpworker status`
  - `service unicorn status`
  - `service elasticsearch status`

- Data Domain: If there is a failure in the Data Domain upgrade, contact Customer Support.

2. Start the Avamar scheduler service by logging in to Avamar using putty and executing the `dpnctl start scheduler` command:
3. Uninstall the dataprotection-upgrade RPM from ACM

   To uninstall the dataprotection-upgrade RPM, on ACM, execute the `rpm -qa | grep dataprotection-upgrade` command to check if any dataprotection-upgrade RPM is present. If it is present, note down its name and uninstall it by using the `-e dataprotection-upgrade-rpm-name` command.

4. Use `create tar` command to create a tarball of `/data01/tmp/patch/logs` folder and save it to the `/data01/upgradeLogs` folder.

5. Restart the tomcat service on ACM using following commands:
   - `service dataprotection_webapp stop`
   - `service dataprotection_webapp start`

Upgrade log files

If both the upgrade process and snapshot recovery fail, collect the log files in the following locations and contact Customer Support:

- Log files for the most recent upgrade process are located in `/data01/tmp/patch/logs` and include the following:
  - ACM—`acm_upgrade.log`
  - Data Domain—`dd_precheck.log`, `dd_upgrade.log`
  - DP Advisor—`dpa_upgrade.log`
  - Search—`dps_upgrade.log`
  - AVE—`AvamarServerUpgrade.log`, `av_upgrade.log`
  - IDPA System Manager—`dpc_deploy_config.log`
  - Common logs for all components—`appLevelUpgrade.log`, `detailed_upgrade_logs.log`
  - Internal service call logs — `Upgrade-utility.log`
  - Validation logs — `Validate.log`
- Log files for past upgrades are archived in `/data01/upgradeLogs`, in the format `idpa_upgradeLogs<date>_<time>.tgz`.

Log file details

The following log file content is extraneous and can be ignored:

In the log file `/data01/tmp/patch/logs/appLevelUpgrade.log`

```
RUNNING,26,Please Contact Dell/EMC Support to upgrade Physical
Backup server and NDMP
RUNNING,74,Performing post upgrade operations
RUNNING,74,Please login again to Appliance Management deployment
and configuration page
```

In the log file `/data01/tmp/patch/logs/detailed_upgrade_logs.log`

```
ERROR : Couldn't upgrade avi-cli to 0.2.1-44.
Performing post upgrade operations
Check if the dataprotection-upgrade package deployed successfully
on tomcat.
Dataprotection-upgrade package deployed successfully.

Old Version , New Version
Updateing Appliance status for Old Version .., New Version ..
Input oldVersion .., newVersion ..
No implementation for given version ..
Appliance status updated Failed.
```

In the log file `/data01/tmp/patch/logs/acm_upgrade.log`

```
Error: Could not open input file: /usr/java/jdk1.8.0_131/lib/
tools.pack
```

```
    plugin.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
plugin.pack
    javaws.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
javaws.pack
    deploy.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
deploy.pack
    rt.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
rt.pack
    jsse.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
jsse.pack
    charsets.jar...
Error: Could not open input file: /usr/java/jdk1.8.0_131/jre/lib/
charsets.pack
    localedata.jar...
Error: Could not open input file: /usr/java/
jdk1.8.0_131/jre/lib/ext/localedata.pack

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

CHAPTER 5

Additional resources

This chapter provides references to other materials related to the IDPA and individual components.

Topics include:

Document references for the IDPA

The IDPA documentation set includes the following publications:

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

Document references for individual components

The documentation for these components can be obtained from Online Support at https://support.emc.com.

Protection Storage node

The following document contains information that is related to Data Domain:

- *Data Domain Operating System Administration Guide*
  This publication explains how to manage Data Domain systems with an emphasis on procedures using the Data Domain System Manager.

Backup Server node

The following documents contain information that is related to Avamar:

- *Avamar Administration Guide*
  This publication describes how to configure, administer, monitor, and maintain an Avamar server.
- *Avamar and Data Domain System Integration Guide*
  This guide includes procedures for configuring the Avamar server to perform cloud tier operations on the Data Domain system.
- *Avamar for VMware User Guide*
  This publication describes various methods and strategies for protecting VMware virtual machines.
- *Avamar NDMP Accelerator for Oracle ZFS User Guide*
  This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported Oracle ZFS storage appliances.

- *Avamar NDMP Accelerator for NetApp Filers User Guide*
  This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported NetApp filers.
- *Avamar NDMP Accelerator for EMC NAS Systems User Guide*
  This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported EMC Isilon, Unity, VNX, VNXe, and Celerra systems.
- *Avamar for VMware User Guide*
  This publication describes various methods and strategies for protecting VMware virtual machines.

IDPA System Manager node

The following documents contain information that is related to Integrated Data Protection Appliance System Manager:

- *IDPA System Manager Release Notes*
  Contains the most up-to-date information about the current release.
- *IDPA System Manager Getting Started Guide*
  This document includes information about how to deploy Integrated Data Protection Appliance System Manager, and then get started with Integrated Data Protection Appliance System Manager administration.
- *IDPA System Manager Administration Guide*
  This document includes information about how to administer Integrated Data Protection Appliance System Manager.
- *IDPA System Manager Security Configuration Guide*
  This document includes information about security features and capabilities of Integrated Data Protection Appliance System Manager.

Reporting and Analytics node

The following documents contain information that is related to Data Protection Advisor:

- *Data Protection Advisor Installation and Administration Guide*
  This publication describes how to install, maintain and configure DP Advisor.
- *Data Protection Advisor Product Guide*
  This document provides information on how to use the DP Advisor web console to run and create reports, view alerts, and view the status of replication operations.

Search Storage

The following document contains information that is related to Data Protection Search:

- *Data Protection Search Installation and Administration Guide*
  This publication describes how to install, maintain and configure Search.

Cloud Disaster Recovery

The following documents contain information that is related to DD Cloud DR and CDRA.

- *Data Domain Cloud Disaster Recovery Release Notes*
  Contains supplemental information about DD Cloud DR and the most up-to-date information about the current release.
- *Data Domain Cloud Disaster Recovery Installation and Administration Guide*
  This document describes how to install, deploy, and use the DD Cloud DR product.

IDPA training resources

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

You can obtain additional IDPA training and information at https://education.emc.com, such as:

- Integrated Data Protection Appliance 2.2 DP4400 Overview
- Integrated Data Protection Appliance 2.2 DP4400 Getting Started
- Integrated Data Protection Appliance 2.2 DP4400 CRU Maintenance
- Integrated Data Protection Appliance 2.2 System Manager Overview
- Integrated Data Protection Appliance 2.2 Alert Monitoring

INDEX