

# Dell EMC Integrated Data Protection Appliance

Version 2.2

## Getting Started Guide

302-004-953

Rev. 03

December 2019

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

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

Dell EMC  
Hopkinton, Massachusetts 01748-9103  
1-508-435-1000 In North America 1-866-464-7381  
[www.DellEMC.com](http://www.DellEMC.com)

# CONTENTS

<b>Chapter 1</b>	<b>Introduction</b>	<b>5</b>
	Document scope and audience.....	6
	Product features.....	6
	System self-protection.....	7
	Network connectivity overview.....	7
	Install Network Validation Tool.....	8
<b>Chapter 2</b>	<b>Setting up the DP4400</b>	<b>9</b>
	Prepare the network environment.....	10
	Configuration worksheet.....	11
	Online Support.....	11
	Connect to the ACM.....	11
	Network Configuration wizard.....	12
	Appliance Configuration Manager.....	15
	Welcome.....	15
	License.....	15
	General settings.....	15
	Customer information.....	15
	Manual configuration of component IP addresses.....	15
	Summary.....	16
	Configuration progress.....	16
	Secure Remote Services configuration for components .....	16
	Next steps.....	16
	Troubleshooting.....	16
<b>Chapter 3</b>	<b>About the dashboard</b>	<b>19</b>
	ACM dashboard Home.....	20
	IDPA System Manager panel.....	21
	Backup Server panel.....	22
	Protection Storage panel.....	22
	Reporting and Analytics panel.....	22
	Search panel.....	23
	Cloud Disaster Recovery panel.....	23
	Virtualization panel.....	24
	Customer Support and General Settings panels.....	24
	User accounts for components.....	25
	Change passwords and synchronize components.....	26
<b>Chapter 4</b>	<b>Performing a VM backup</b>	<b>27</b>
	VM backups overview.....	28
	Define vCenter and VMware clients.....	28
	Deploy the Avamar proxy.....	32
	Install the Avamar proxy hotfix.....	33
	Create and run the backup policy.....	34
<b>Chapter 5</b>	<b>Restoring a VM backup</b>	<b>37</b>
	Restore a Virtual Machine .....	38

	Restore using Instant Access.....	41
	Restore specific files.....	43
<b>Chapter 6</b>	<b>Generating reports</b>	<b>45</b>
	Generate a report.....	46
<b>Index</b>		<b>47</b>

# CHAPTER 1

## Introduction

This section contains the following topics:

- [Document scope and audience](#)..... 6
- [Product features](#)..... 6
- [System self-protection](#)..... 7
- [Network connectivity overview](#)..... 7
- [Install Network Validation Tool](#)..... 8

## Document scope and audience

This document describes IDPA and explains how to perform the initial software configuration after the appliance hardware is set up. It also describes a number of procedures that you can use to get IDPA up and running in a relatively short time.

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

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

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, appliance configuration manager (ACM) come embedded on the appliance.

This release includes the IDPA System Manager and adds the optional Cloud Disaster Recovery (CDRA) to the software stack.

### 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.

### Backup administration

The IDPA protects virtual and physical clients, different types of file systems, applications, and databases.

### Monitoring 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 custom and system report and dashboard templates on demand or on a schedule at defined time intervals, per the enterprise requirements.

The ACM 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.

### 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, which is then stored within the IDPA.

### Disaster recovery

DD Cloud DR is an optional solution that facilitates the recovery of on-premises virtual machines by providing the capability to recover those VMs in the cloud. DD Cloud DR 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.


 **Note:** CDRA is optional.

### Scalability

The IDPA is designed to be scalable so it can grow with changing needs. The base DP4400 configuration includes 24TB of storage space, which can be expanded by licencing additional capacity in increments of 12TB up to a maximum of 96TB.

### Unified support

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

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

## 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.

## 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 1** 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	Data IP 1
+2	192.0.2.3	Target storage	Data IP 2
+3	192.0.2.4	Target storage	Data 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

## Install Network Validation Tool

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

Before you install IDPA, it is recommended that you run the Network Validation Tool to validate the network settings for a successful deployment of IDPA in the datacenter. You must review the network configuration before starting the IDPA installation. To download the NVT and for more information about the tool, see <https://help.psapps.emc.com/display/HELP/Network+Validation+Tool+for+IDPA>.



# CHAPTER 2

## Setting up the DP4400

- [Prepare the network environment](#)..... 10
- [Configuration worksheet](#)..... 11
- [Appliance Configuration Manager](#)..... 15
- [Troubleshooting](#)..... 16

# Prepare the network environment

## Before you begin

You must have a computer at the install location with:

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

**Note:** The DP4400 supports only one network. Separate management, backup, or replication network configurations (such as VLAN tagging) are not supported.

## About this task

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

## Procedure

1. Identify 14 unassigned IP addresses for the IDPA components. To simplify configuration, you must select 14 contiguous addresses.

Note that all components must run on a single VLAN or subnet with the exception of the iDRAC interface, which can be on a separate subnet or VLAN. For further information about IP addresses, see [Network connectivity overview](#) on page 7.

2. Register the 14 IP addresses in DNS with forward and reverse lookup entries for each address. Ensure that the router for the 14 IP addresses can be pinged.

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

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

The contact person mentioned on your sales order should have received the License Authorization Code (LAC) letter through an email during the order fulfillment process. The LAC letter includes the license authorization code associated with your order, instructions for downloading software binaries, and instructions for activating the entitlements online through Dell EMC Software Licensing Central.

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

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

After the activation is complete, download the license keys that are generated for Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE), and Data Protection Advisor (DP Advisor). Use these license keys during the IDPA configuration.

## Configuration worksheet

Use this worksheet to collect and record information to start setting up your appliance using the following:

- Online Support
- Network Configuration wizard
- *Appliance Configuration Manager* ACM

### Online Support

Record the following information related to your Online Support account:


#### Online Support credentials

Your username and password is required for Secure Remote Services (formerly ESRS) configuration. To create an Online Support account, go to [support.emc.com](http://support.emc.com).

#### Site ID

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

1. Log in to Online Support with your credentials.
2. Select **Service Center**.
3. In the **Administration** section of the Service Center page, click **View and manage company information**.
4. Click **View Sites** and ensure that the site where the IDPA 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.

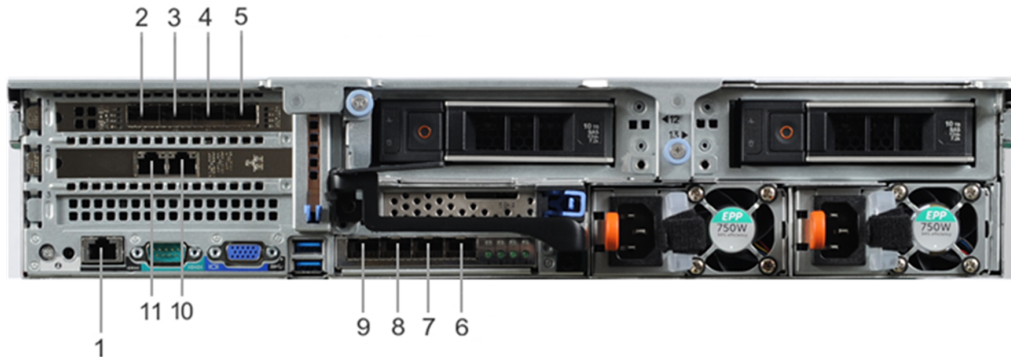
### Connect to the ACM

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

#### Before you begin

- After powering on the appliance, wait 5 minutes for startup to finish.
- Verify that the service computer is connected to the 1 GbE port identified as (10) in [Figure 1](#) on page 12.
- On the service computer, record the IP address settings for the Ethernet interface that is connected to the DP4400.

**Figure 1** DP4400 network and iDRAC connections



### Procedure

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

**Note:** This password will be assigned to all appliance components. It must contain 9–20 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 (\_)

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

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

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

### Results

The **Network Configuration** screen appears.

## Network Configuration wizard

After accepting the EULA, establish initial connectivity to the DP4400 components.

### About this task

The information that is required for this section is recorded in the *Integrated Data Protection Appliance Pre-Engagement Questionnaire*.

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

### Procedure

1. Provide the following information to configure the basic network settings:

#### Subnet mask

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

- Note:** The DP4400 supports only one network. Separate management, backup, or replication network configurations (such as VLAN tagging) are not supported.

#### Gateway

Default gateway IP address of the appliance.

#### Primary DNS server

The primary DNS server for your network environment.

#### Secondary DNS server

The secondary DNS server for your network environment.

#### Domain name

The domain name for your network environment.

#### Appliance Configuration Manager IP

The IP address to assign to the ACM.

#### ESXi IP

The IP address to assign to the ESXi server.

2. Click **Submit**.

### After you finish

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

- Note:** You need to force sync the time on the hardware with the host time and ESXi with the NTP server. To force sync the time, perform the following steps.

1. Login to the **ESXi**.
2. Run the following command to force a time sync on **ESXi**. against a functioning NTP server.  

```
# sntp -S <NTP server>
```
3. Run the following command to sync the hardware time with the host time.  

```
# ipmitool sel time set "`date +%m/%d/%Y %H:%M:%S`"
```

- Note:** For automatic forwarding to work correctly, the computer you use to complete the configuration must be attached to the same network as the configured set ACM IP address.

- If you cannot have connections to both public and private networks at the same time, disconnect from the private appliance configuration network and then connect to the network that the ACM IP address is on to complete the rest of the configuration.

- Once the network configuration is complete, revert the network adapter IP address settings on the service computer to their previous state.

## Appliance Configuration Manager

The ACM walks you through the initial set up of the IDPA and prepares the appliance for use. Use the following list of screens and related actions as a guide to the initial configuration process.

To access the ACM UI, type the IP address you assigned to the ACM in a browser as follows:

`https://<configured ACM IP address>:8543/dataprotection`

### Welcome

Read the prerequisite information and select the checkbox to accept.

(optional) Select **Cloud Disaster Recovery**.

**Note:** If you choose to configure **Cloud Disaster Recovery**, you cannot remove it from the IDPA later.

### License

Upload the Data Domain, Avamar, and Data Protection Advisor license files you obtained from Online Support.

### General settings

Select your time zone and type the SMTP, SNMP, and NTP server IP addresses.

**Note:** The SNMP server IP is the address of an external trap host. Although this is a mandatory value, you can enter the IP address of any reachable server if no SNMP server is available.

Select **IP address range (11)** and, in the associated field, type the first IP address in the sequential range of 11 IP addresses for the IDPA to use. The ACM assigns one IP address in the range to each virtual machine in the configuration.

**Note:** It is recommended that you specify an IP range. IP ranges are not required, but they do reduce the number of IP addresses that have to be typed manually during later wizard steps.

(optional) To specify non-sequential IP addresses for each virtual machine in the configuration, do not select **IP address range**.

### Customer information

Enter your customer contact information, including the name, email address, and contact number of the administrator, and also the location name, company name, and Site ID. Customer Support will use this information to contact you when needed.

### Manual configuration of component IP addresses

If you selected **IP address range** on the **General settings** screen, go to [Summary](#) on page 16.

(manual configuration) If you did not select **IP address range** on the **General settings** screen, type an IP address in each field on the following screens:

- **vCenter**
- **Protection Storage**
- **Backup Server**

- **IDPA System Manager**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery** (if selected on the **Welcome** screen)

## Summary

Review the configuration summary. To make changes, return to the previous screens.

When the configuration is correct, click **Submit**. The process continues automatically.

**Note:** The configuration process takes several hours to complete, and continues on its own if you disconnect from the DP4400. If your session is interrupted during configuration, verify that you are connected to the network and type the ACM IP address in your browser as follows:  
`https://<configured ACM IP address>:8543/dataprotection`  
If prompted, log in with the ACM credentials to view the current state of the configuration progress.

## Configuration progress

When the configuration process is complete, you can download the configuration information as a PDF or XML file.

When you are finished, click **Finish**.

## Secure Remote Services configuration for components

(optional) Enter the Secure Remote Services gateway IP address and your Online Support credentials to send component system information to Customer Support and expedite issue resolution.

**Note:** This step repeats for each component that can be registered with Secure Remote Services.

## Next steps

### Results

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

Refer to [About the dashboard](#) on page 19 for more information about using the ACM dashboard to monitor and manage the components of the IDPA.

## Troubleshooting

### Creating and downloading a log bundle

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

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



### Accessing vCenter

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



# CHAPTER 3

## About the dashboard

The ACM dashboard allows you to manage settings for the appliance and individual components, update customer support information, and upgrade software for the appliance and its components.

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.

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


• <a href="#">ACM dashboard Home</a> .....	20
• <a href="#">IDPA System Manager panel</a> .....	21
• <a href="#">Backup Server panel</a> .....	22
• <a href="#">Protection Storage panel</a> .....	22
• <a href="#">Reporting and Analytics panel</a> .....	22
• <a href="#">Search panel</a> .....	23
• <a href="#">Cloud Disaster Recovery panel</a> .....	23
• <a href="#">Virtualization panel</a> .....	24
• <a href="#">Customer Support and General Settings panels</a> .....	24
• <a href="#">User accounts for components</a> .....	25
• <a href="#">Change passwords and synchronize components</a> .....	26

## ACM 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, update the common password across all components, register components with Secure Remote Services (formerly ESRS), and install optional components (CDRA).

 **Note:** Secure Remote Services configuration link is present under gear icon menu. Do mouse hover on the gear icon to list all the menu options.

If DPS or DPA failed during configuration, ACM does not stop whole configuration. The configuration process still continues until it finishes. After the configuration process is finished, ACM dashboard provides an option to configure the failed component (DPS or DPA).


### Downloading the configuration details

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

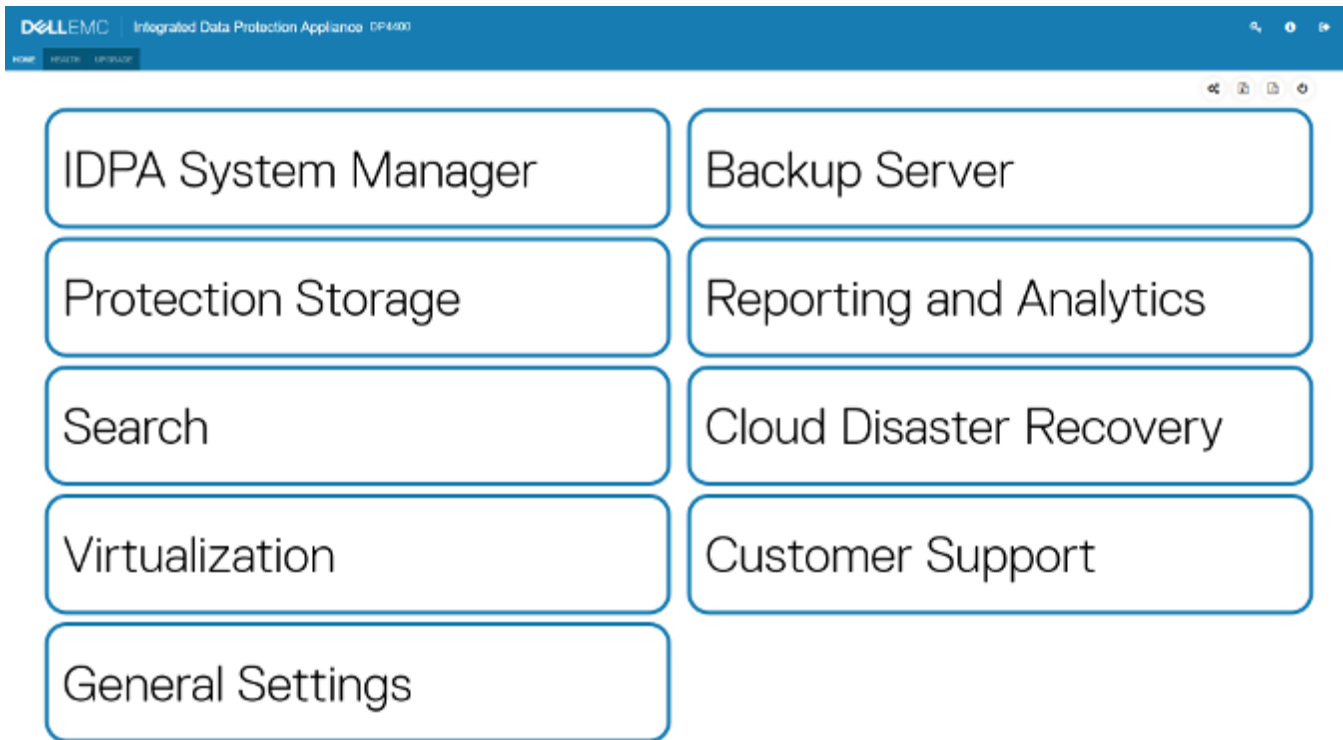
### Managing system components

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 Support**
- **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.

**Figure 2** ACM dashboard home layout without individual panel details



**Note:** When ACM restarts, it tries to start each component. This may impact the speed with which the ACM UI is up and running.

## IDPA System Manager panel

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

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

Move the cursor to **Services** to view status information for IDPA System Manager services.

**Figure 3** The **IDPA System Manager** panel on the ACM **Home** page



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, license status of the Backup Server node, and whether the installation of agents is in progress. Click the **Download Agents** link that appears after the agent installation finishes to load the Avamar Web Restore GUI, from which the Avamar agents can be downloaded.

Figure 4 The **Backup Server** panel on the ACM Home page

Property	Value
IP Address	10.241.189.137
Version	7.5.1-101_HF293433_13
License status	✓
Total Backup metadata storage	3.46 TB
Available Backup metadata storage	3.46 TB

Download backup agents Services ✓

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

## 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 requiring user action. To access additional functionality of the component, click the **Protection Storage System Manager** link.

Figure 5 The **Protection Storage** panel on the ACM Home page

Property	Value
IP Address	10.241.189.134
Version	Data Domain OS 6.1.1.10-590811
Total backup storage	48.407 TB
Available backup storage	48.240 TB
File system status	✓
License status	✓
Cloud Storage	192.000 TB

Protection Storage system manager

## Reporting and Analytics panel

The **Reporting and Analytics** panel displays the DP Advisor version, IP addresses for the Application Server and Datastore Server, the license status of the Reporting and Analytics node, and any alerts requiring user action. To load the Reporting and Analytics console, click the **Reporting and Analytics Web UI** link. Move the cursor to **Services** to view status information for DP Advisor services.

Figure 6 The Reporting and Analytics panel on the ACM Home page

Version	6.5.0.103022	License status	✓
Application Server IP	10.241.189.140	Datastore Server IP	10.241.189.141

Reporting and Analytics Web UI Services ✓

If DP Advisor was 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 appears. On the **Reporting and Analytics Configuration** screen, provide the required license information and IP addresses and then click **Configure**.

## Search panel

The **Search** panel displays the Search version, IP address for the Index Master node, and any alerts requiring user action. To load the Search console, click the **Search** link. Move the cursor to **Services** to view status information for Search services.

Figure 7 The Search panel on the ACM Home page

Index Master IP	10.241.189.142	Version	18.0.0.1041
[Search Icon]			

Search Services ✓

If Search was 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**.

## Cloud Disaster Recovery panel

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

**Figure 8** The **Cloud Disaster Recovery** panel on the ACM **Home** page



If CDRA was 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 appears. On the **Cloud Disaster Recovery Configuration** screen, provide IP address and click **Configure**.

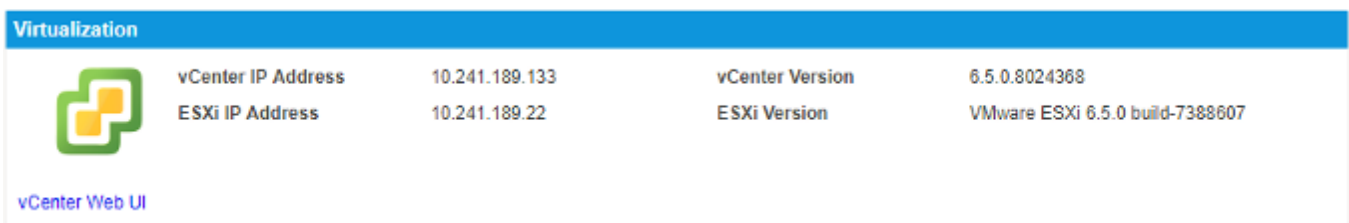
**Note:**

- Do not change Avamar root user password before configuring CDRA from dashboard.
- Do not change DD boost user password before configuring CDRA from Dashboard.
- If cloud account and email address are not configured in CDRA configuration, the CDRA login page does not work. User has to configure cloud account and email address manually in CDRA.

## 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.

**Figure 9** The **Virtualization** panel on the ACM **Home** page



## Customer Support and General Settings panels

The **Customer Support** panel displays the administrator contact and site information. To view the full value of an item, hover over the item.



**Figure 10** The **Customer Support** panel on the ACM Home page

The **General Settings** panel displays basic settings including time and network configuration. To view the full value of an item, hover over the item.

**Figure 11** The **General Settings** panel on the ACM Home page

## User accounts for components

The IDPA configuration uses the user accounts in [Table 2](#) on page 25. By default, these accounts use the common IDPA password . For information on how to change component passwords, refer to [Change passwords and synchronize components](#) on page 26.

**Table 2** Component and user account mapping

Component	Using SSO	Username	Password
ACM	No	root	Common password provided during DP4400 configuration.
IDPA System Manager (If external LDAP is not configured)	No	idpauser	Common password provided during DP4400 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 DP4400 configuration.
Data Protection Advisor	No	administrator	Common password provided during DP4400 configuration.
Search	Yes	NA	SSO will take care of this logging in automatically.
CDRA	No	admin	Common password provided during DP4400 configuration.
CDRS	No	admin or monitor	Password set during CDRS deployment.

**Table 2** Component and user account mapping (continued)

Component	Using SSO	Username	Password
vCenter	No	idpauser	Common password provided during DP4400 configuration.
ESXi	No	idpauser	Common password provided during DP4400 configuration.

## Change passwords and synchronize components

Single click user password change is one of the new features introduced in DP4400. It is recommended that you use the 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.

# CHAPTER 4

## Performing a VM backup

This section contains the following topics:

- [VM backups overview](#) .....28
- [Define vCenter and VMware clients](#) ..... 28
- [Deploy the Avamar proxy](#) ..... 32
- [Install the Avamar proxy hotfix](#) ..... 33
- [Create and run the backup policy](#) ..... 34

## VM backups overview

As soon as your environment is up and running, you can follow the steps in this section to backup a VMware client.

In case you are using Avamar for the first time, the section includes preparatory tasks, such as defining vCenter and VMware clients and deploying an Avamar proxy.

The entire process is organized into the following procedures:

- [Define vCenter and VMware clients.](#)
- [Deploy the Avamar proxy.](#)
- [Install the Avamar proxy hotfix.](#)
- [Create and run the backup policy](#)

Further information about Avamar backups is available in the Avamar documentation, including the *Avamar Administration Guide* and the *Avamar Backup Clients User Guide*.

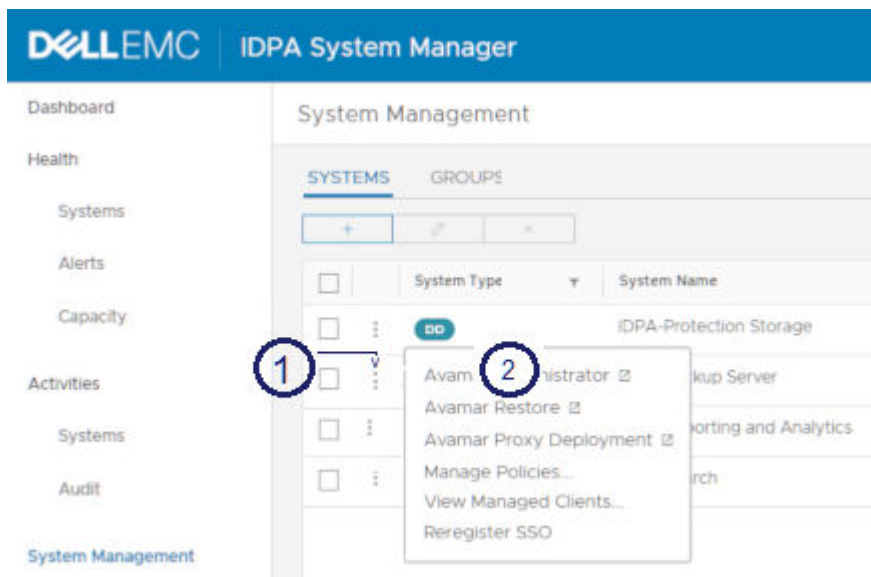
## Define vCenter and VMware clients

### About this task

This procedure shows you how to create the vCenter and VM clients and add a dataset to the VM client.

### Procedure

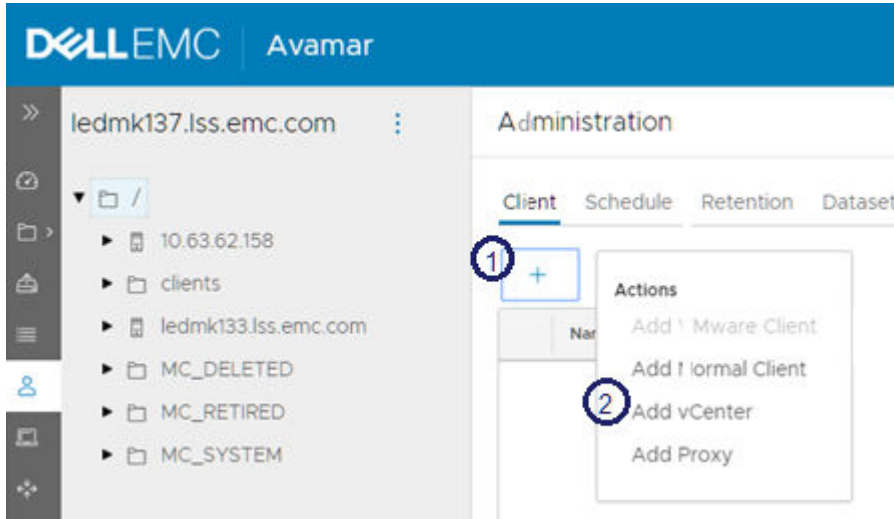
1. Using a browser, log into the ACM dashboard at *https://<ACM IP address>:8543*.
2. Click **IDPA System Manager Web UI** and log in to the System Manager.
3. Click **System Management** in the navigation pane to display the **System Management** pane.
4. Click the vertical ellipsis for the IDPA-Backup Server and select **Avamar Restore** to launch the Avamar UI.



1. Click vertical ellipsis.

2. Select **Avamar Restore**.

5. In the Avamar navigation pane, click **Administration**.
6. To add the vCenter client:
  - a. Click the plus sign (+) and select **Add vCenter** to launch the wizard.



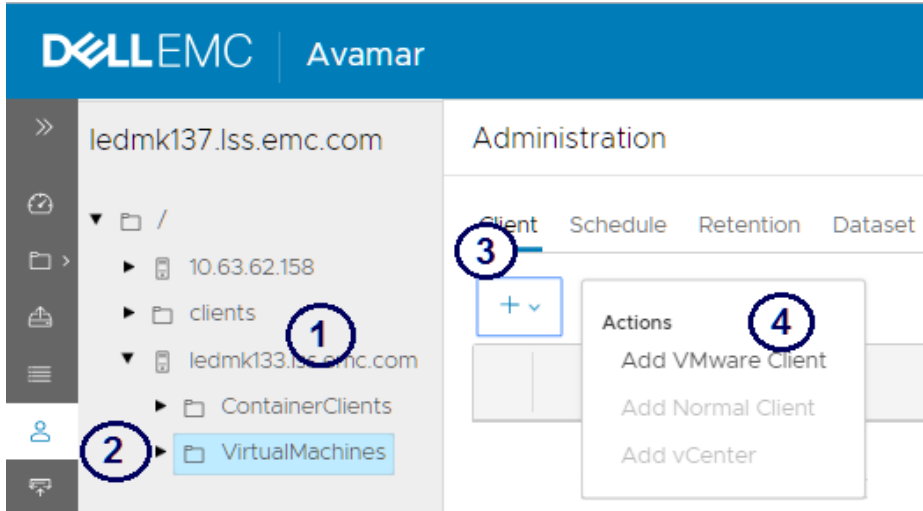
1. Click plus sign.
2. Select **Add vCenter**

- b. Use the following table to complete the fields on each page, clicking **Next** to proceed to the next page.

**Table 3** Adding vCenter Clients

Page	Field	Description
Client Information	Client Type	Select VMware vCenter.
	New Client Name or IP	Client name or IP address.
	Client Domain	Domain name.
vCenter Information	User Name	The user name of the vCenter server administrator.
	Password	The administrator password.
	Port	The vCenter HTTPS port number.
Advanced	All fields are optional for this task.	
Optional Information	All fields are optional for this task.	

- c. Click **ADD** to complete the wizard. Then refresh the screen to verify the new vCenter client.
7. To add the VMware client:
  - a. In the middle pane, expand the new vCenter client and click **VirtualMachines**.
  - b. In the right pane, click the plus sign (+) and select **Add VMware Client**.



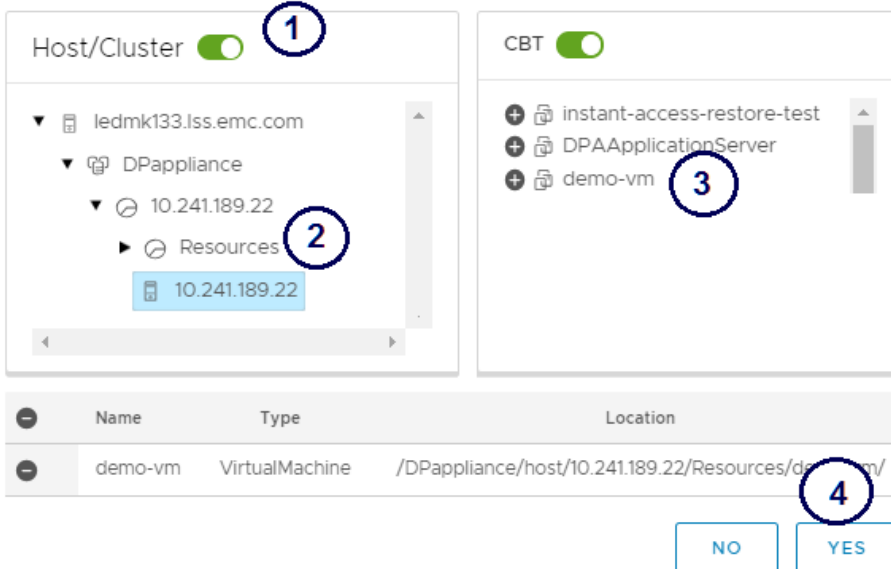
1. Expand vCenter.
2. Click **VirtualMachines**.
3. Click plus sign.
4. Select **Add VMware Client**.

c. On the **Select VMware Entity** window, enable the **Host/Cluster** button. Then expand the host/cluster tree and select the cluster hosting the VM that you want to back up.

The VMs assigned to the cluster display in the right panel.

d. In the right panel, select the VM you want to back up and click **YES**.

### Select VMware Entity



1. Enable **Host/Cluster** button.
2. Select cluster.
3. Select VM.
4. Click **YES**.

8. To add the dataset:

- a. Click **Administration** in the Avamar navigation pane and select the root domain folder in the middle pane.
- b. Select **Dataset** in the right pane and then click the plus sign (+) to display the **Create DataSet** window.
- c. In the Dataset Name field, type the dataset name.
- d. Click **Windows VMware Image** in the **Plugins** list to display the **Windows VMware Image** page.
- e. Select the **Index VMware Image Backups** checkbox and click **Submit**.

NOTE: Indexing is used for restoring specific files and is optional for backing up entire VMs. Selecting it here will allow you to restore specific files as described in [Restore specific files](#).

### Create DataSet

DataSet Name:

The screenshot shows the 'Create DataSet' window with the following elements:

- 1**: A circled '1' points to the 'DataSet Name' input field containing 'vm\_dataset'.
- 2**: A circled '2' points to the 'Windows VMware Image' plugin in the 'Plugins' list on the left.
- 3**: A circled '3' points to the 'Index VMware Image Backups' checkbox, which is checked.
- 4**: A circled '4' points to the 'SUBMIT' button at the bottom right.

The 'Windows VMware Image' plugin configuration page includes the following options:

- Use Changed Block Tracking (CBT) to increase performance
- set annotation tag LastBackupStatus and LastSuccessfulBackup
- Index VMware Image Backups

Buttons at the bottom: CLOSE (disabled), SUBMIT (active).

1. Enter the dataset name.
2. Select **Windows VMware Image**.
3. Select **Index VMware Image Backups**.
4. Click **Submit**.

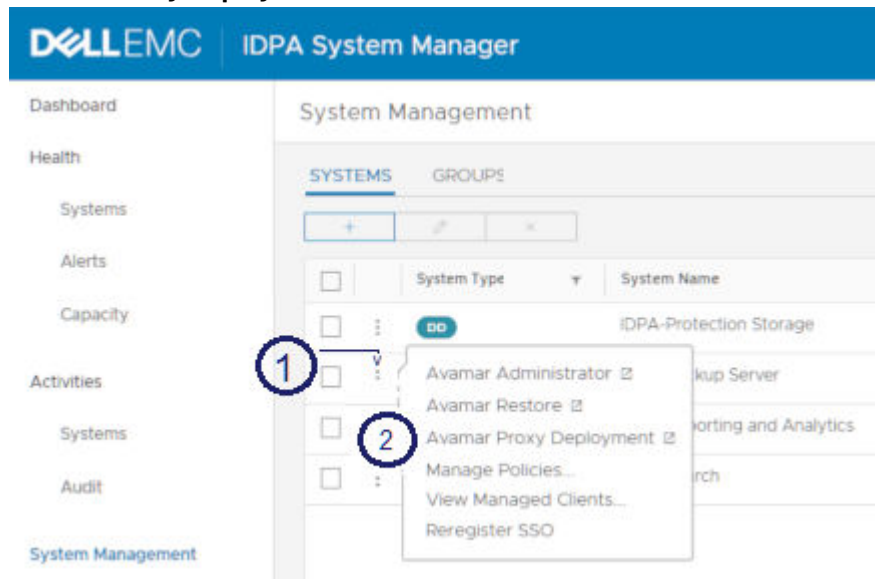
## Deploy the Avamar proxy


### About this task

Deploy the Avamar proxy on each vCenter that you intend to protect.

### Procedure

1. Launch the **IDPA System Manager Web UI** and click **System Management** in the navigation pane.
2. In the right pane, click the vertical ellipsis in front of the IDPA Backup Server and select **Avamar Proxy Deployment**.



1. Click vertical ellipsis.
2. Select **Avamar Proxy Deployment**.
3. On the **Config** window, specify the **vCenter**, **Data Change Rate**, and **Backup Window**. Then select the **Protect Virtual Machines on Local Storage** checkbox.
4. Click **CREATE RECOMMENDATION**.  
The **Recommendations** pane shows the proposed new proxies under each ESXi host.
5. Expand the listings in the **Recommendations** pane and select **New proxy** under the ESXi server host.
6. Click  to display the **New Proxy** dialog.
  - a. Type the proxy hostname in the **Name** field.
  - b. Select an Avamar server **Domain** where this proxy will reside.
  - c. Type the IP address in the **IP** field.
  - d. Select a datastore from the **Datastore** list.
  - e. Select **VM Network** from the **Network** list.
  - f. Type the fully-qualified server name or IP address in the **DNS** field.
  - g. Type the network gateway IP address in the **Gateway** field.



- h. Type the network mask in the **Netmask** field.
  - i. Click **SAVE**.
7. Click ✓ to deploy the proxy.

The proxy deployment displays in the lower panel.

## Install the Avamar proxy hotfix

To use Virtual Machine indexing at the time of the image backup you must install Avamar Hotfix 298624 on all Avamar proxies. If you do not apply the Avamar hotfix, the proxies may run out of storage space due to debug logging being enabled by default.

### Before you begin

Download Avamar Hotfix 298624 from the following location:

[ftp://avamar\\_ftp:anonymous@ftp.avamar.com/software/hotfixes/298624/SLES12SP1\\_64/AvamarVMwareCombined-linux-sles12sp1-x86\\_64-7.5.101-101.rpm](ftp://avamar_ftp:anonymous@ftp.avamar.com/software/hotfixes/298624/SLES12SP1_64/AvamarVMwareCombined-linux-sles12sp1-x86_64-7.5.101-101.rpm)

### About this task

Repeat this procedure for each Avamar proxy. The following default credentials are required to authenticate on or connect to an Avamar proxy:

Username: `root`  
 Password: `avam@r`

### Procedure

1. Using the `scp` command or WinSCP, copy the hotfix file to `/space/avamar/var` on the proxy.
2. Connect with SSH to the proxy using the default credentials.
3. Type the command `rm -f /tmp/*.SQL`
4. Go to the directory in which the hotfix file is located:

```
cd /space/avamar/var
```

5. Install the hotfix:

```
rpm -Uvh AvamarVMwareCombined-linux-sles12sp1-x86_64-7.5.101.101.rpm --force
```

### Results

To verify successful RPM installation, check the version with the following command:

```
avtar --version
```

If the RPM is installed, the output is:

```
version:      7.5.101-101_HF298624
```

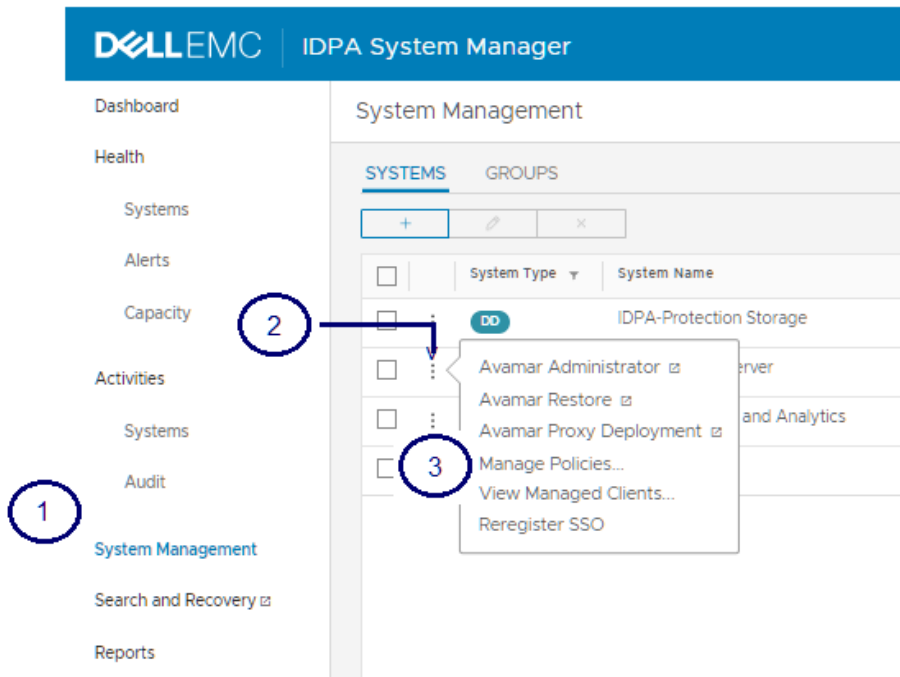
# Create and run the backup policy

## About this task

These steps show how to create the policy to protect the VMware client and then run the policy.

## Procedure

1. In the IDPA System Manager, click **System Management** in the navigation pane.
2. In the right pane, click the vertical ellipsis for the IDPA backup server and select **Manage Policies**.



1. Click **System Management**.
2. Click vertical ellipsis.
3. Select **Manage Policies**.

The **Manage Policies** pane displays.

3. In the **Manage Policies** pane, click the plus sign (+) to launch the **Add Policy** wizard.
4. Use the following table to complete the wizard pages, clicking **Next** to proceed to the next page.

**Table 4** Adding Policies

Page	Field	Description
Information	Name	The policy name.
	Domain	Accept the default entry.
	Enable	Click to enable the policy.
	Dataset	Select <b>VMware Image Dataset</b> .

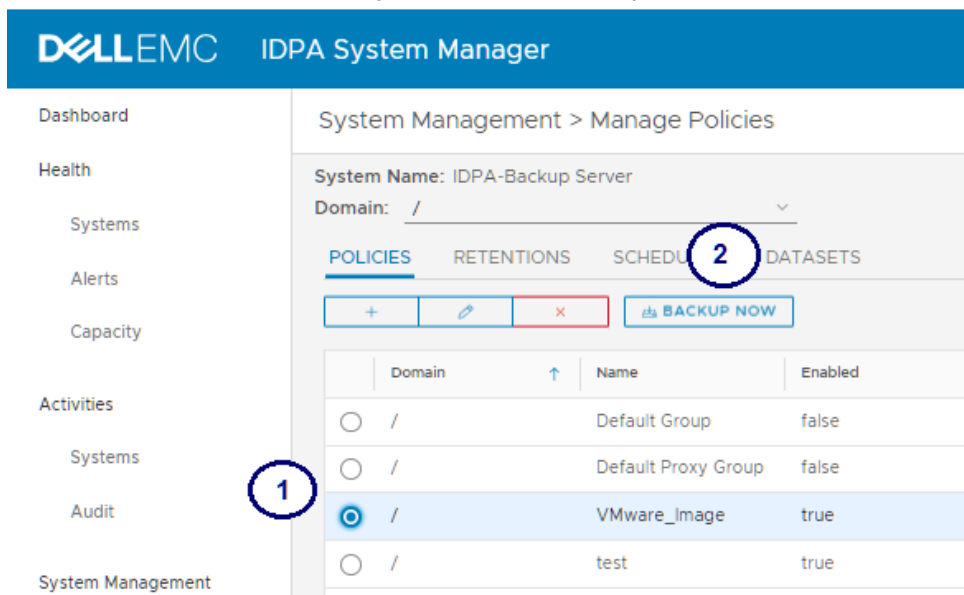
**Table 4** Adding Policies (continued)

Page	Field	Description
	Schedule	Select <b>Daily Schedule</b> .
	Retention	Select <b>Default Retention</b> .
Clients	Available Clients	Select the VM client defined earlier in this guide.
Proxies (Optional)	Available Proxies	Select the proxy defined earlier in this guide.

5. Click **Finish**.

The new policy displays in the policy list.

6. To run the policy, select it in the policy list and click **BACKUP NOW**.



1. Select the policy.

2. Click **BACKUP NOW**.

7. Monitor the policy run by clicking **Systems** under **Activities** in the navigation pane.



# CHAPTER 5

## Restoring a VM backup

This section describes three different methods of restoring the VM backup that was created in the previous chapter:

- [Restore a Virtual Machine](#) ..... 38
- [Restore using Instant Access](#)..... 41
- [Restore specific files](#)..... 43

## Restore a Virtual Machine

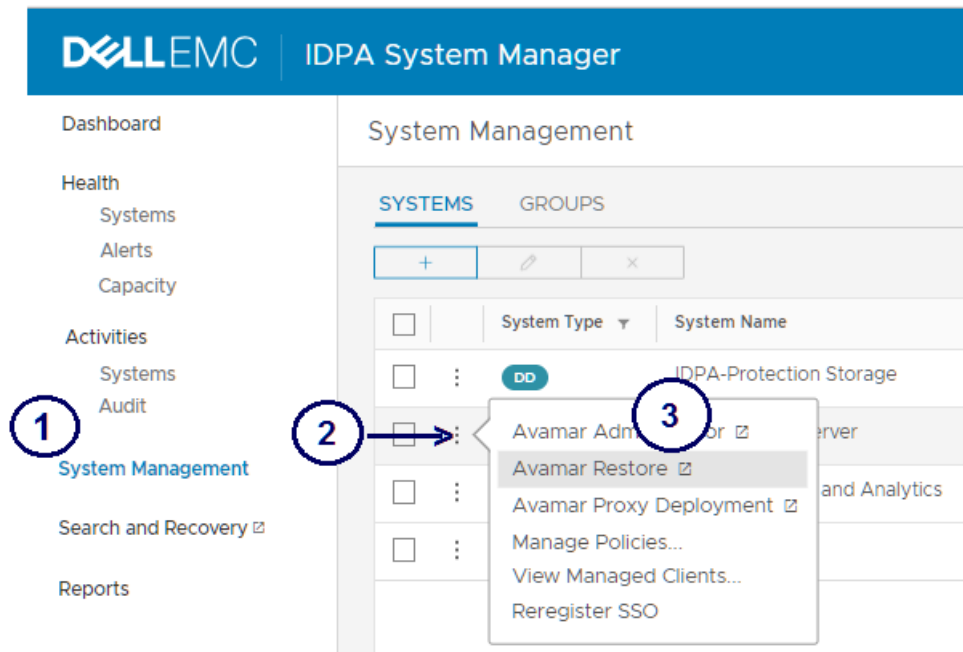
These steps illustrate the basic VM restore procedure.

### Before you begin

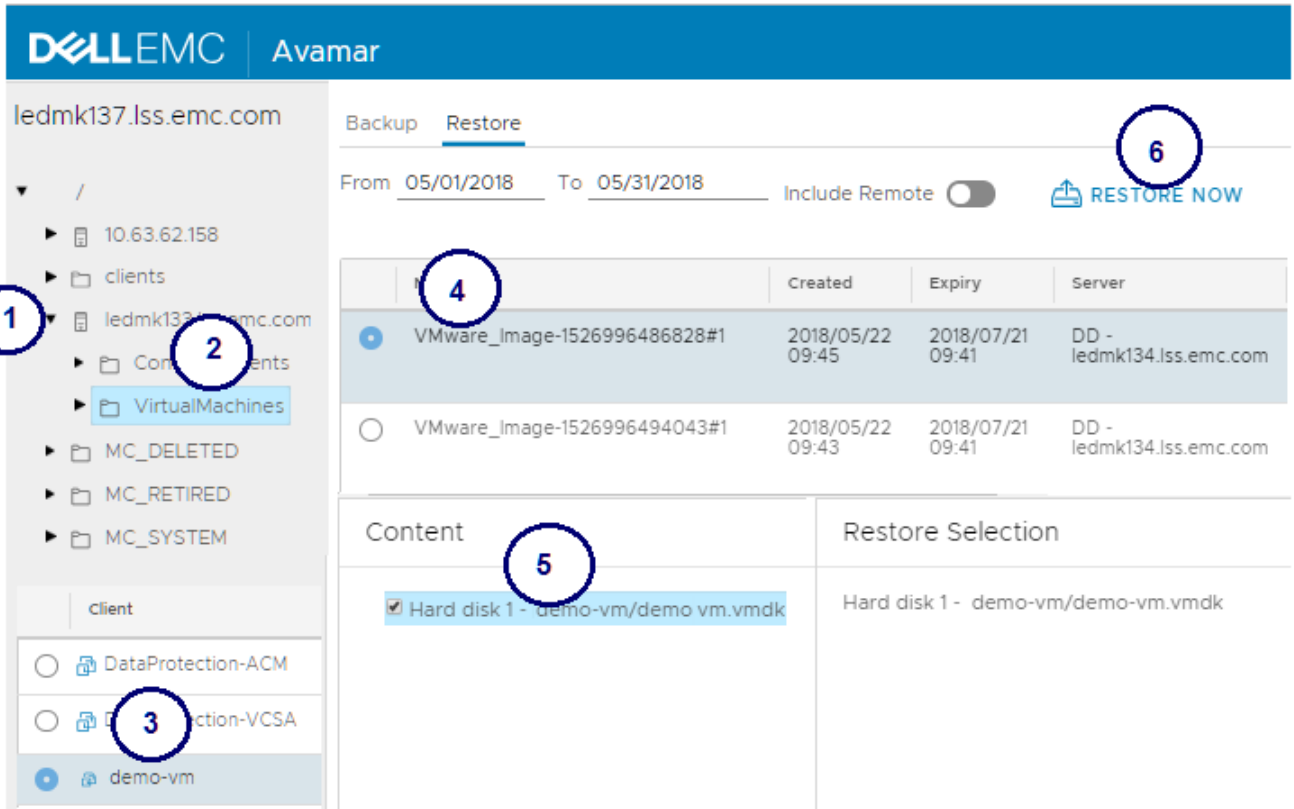
A backup of the VM must exist in order to perform a restore.

### Procedure

1. Access the IDPA System Manager and select **System Management** in the navigation pane.
2. In the right pane, click the vertical ellipsis to the left of the IDPA backup server and select **Avamar Restore**.



1. Select **System Management**.
2. Click vertical ellipsis.
3. Select **Avamar Restore**.
3. Expand the vCenter in the middle pane and select **VirtualMachines** to display the VM clients belonging to that vCenter.
4. In the client list, select the VM client that you want to restore.
5. In the right pane, select the backup that you want to restore and then select the restore content in the **Content** area.
6. To start the restore wizard, select the content that you want to restore and click **RESTORE NOW**.



1. Expand vCenter.
2. Click **VirtualMachines**.
3. Select client.
4. Select latest backup.
5. Select content.
6. Click **Restore Now**.
7. Use the following table to complete each wizard page, clicking **NEXT** to proceed to the next page.

**Table 5** Restoring from a VM

Wizard page	Field	Description
Basic Config	Destination	Select <b>Restore to new Virtual Machine</b> .
	Post Restore Options	Select <b>Do not power on VM after restore</b> .
	Proxy	Select <b>Automatic</b> .
Advanced Config	vCenter	Select the IP address of the vCenter to manage the restored VM.
	VM Name	Enter a name for the restored VM.
Location		Expand the tree and select the VM where you want to perform the restore.
Host/Cluster		Expand the tree and select the ESXi host/cluster.
Resource Pool		Expand the tree and select the resource pool.
Datstore		Select the destination ESX datstore.

8. On the **Summary** page, review your entries and click **FINISH** to perform the restore.
9. To monitor the results, select **Activity** in the Avamar navigation tree and view the processing results in the right pane.



## Restore using Instant Access

### About this task

You can use the instant access feature to perform near real-time recovery of a VM. It mounts a VM backup image on a NFS share in your backup environment and powers on the VM so that it can be managed in vCenter.

After you complete these steps, you should move the VM from your backup environment to the production system.

### Procedure

1. Launch the IDPA System Manager and click **System Management** in the navigation pane.
2. In the right pane, click the vertical ellipsis to the left of the IDPA backup server and select **Avamar Restore**.
3. Expand the vCenter tree and select **VirtualMachines** to display the **Client** list.
4. Select the client in the **Client** list to display the recent backups of that client in right pane.
5. Select the backup that you want to restore. Then select the content in the **Content** area and click **Restore Now** in the upper right to launch the Restore wizard.

The screenshot shows the Dell EMC Avamar interface. The top bar displays the Dell EMC logo and the word 'Avamar'. Below the bar, the navigation pane on the left shows a tree structure with 'VirtualMachines' selected (callout 1). The main area is split into two panes. The left pane shows a 'Client' list with 'demo-vm' selected (callout 2). The right pane shows a table of backup clients (callout 3) with columns for Name, Label, Created, fPlugin, and Size. The first row is selected. Below the table, the 'Content' area shows 'demo-vm/demo-vm.vmdk' selected (callout 4). The 'Restore Selection' area shows 'demo-vm/demo-vm.vmdk'. In the top right corner, there is a 'RESTORE NOW' button (callout 5).

Name	Label	Created	fPlugin	Size
MOD-1526564097797#1	6	2018/05/17 09:39	Windows VMware I	80 GB
MOD-1525888167605#1	5	2018/05/09 13:52	Windows VMware I	80 GB
MOD-1525888160592#1	4	2018/05/09 13:50	Windows VMware I	80 GB
MOD-1525871082323#1	3	2018/05/09 09:05	Windows VMware I	80 GB
MOD-1525869725749#1	2	2018/05/09 08:45	Windows VMware I	80 GB

1. Select **VirtualMachines**.
2. Select client.
3. Select latest backup.
4. Select content.
5. Click **Restore Now**.

- Use following table to complete each wizard page, clicking **NEXT** to proceed to the next page.

**Table 6** Restore Using Instant Access

Wizard page	Field	Description
Basic Config	Destination	Select <b>Instant Access</b> .
	Post Restore Options	Select a restore option.
	Proxy	Select <b>Automatic</b> .
Advanced Config	vCenter	Select the IP address of the vCenter to manage the restored VM.
	VM Name	Enter a name for the restored VM.
Location		Expand the tree and select the VM where you want to perform the restore.
Host/Cluster		Expand the tree and select the ESXi host/cluster.
Resource Pool		Expand the tree and select the resource pool.

- On the **Summary** page, review your entries and click **FINISH** to perform the restore.
- To monitor the results, select **Activity** in the Avamar navigation tree and view the processing results in the right pane.

## Restore specific files

You can restore specific files directly from search results.

### Before you begin

Ensure that Avamar is indexing your backed-up VM images. For instructions, see the *Dell EMC Search Administration Guide*.

### About this task

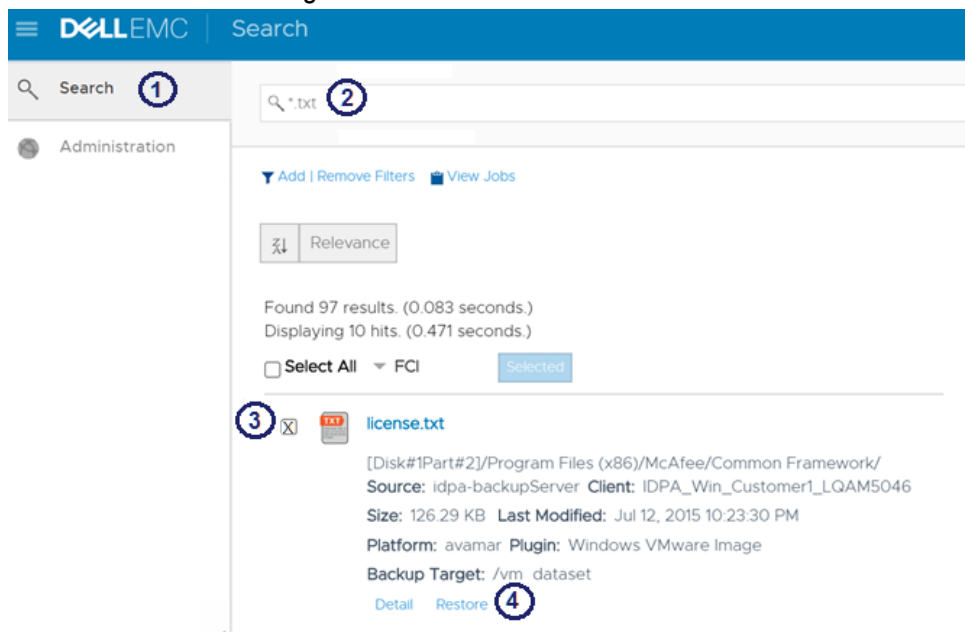
In this procedure, the Search application is used to search for and restore specific files in a VM backup.

### Procedure

1. Access the IDPA System Manager and select **Search and Recovery** in the navigation pane.
2. Log in to the Search application.
3. In the **Search** field, enter a query to retrieve specific files and click **Search**. (You can also use filter options to refine the search results.)

The retrieved files display.

4. Select one or more files that you want to restore and click **Restore** to display the **Restore** dialog.



1. Click **Search**.
  2. Enter search query.
  3. Select one or more files.
  4. Click **Restore**.
5. Use the following table to complete the **Restore** dialog.

**Table 7** Restore Specific Files

Field	Description
Original path / Destination path	Select the restore location. When applicable, click <b>Overwrite</b> and select <b>Restore Access Control List</b> to protect the file with the same access control list settings
Client	When <b>Destination Path</b> is selected, select the client where you want to save the file.
Restore to	Specify the path where you want to save the file.
Username / Password	Specify the VM user name and password.

6. Click **Restore** to initiate the restore process.
7. To monitor the results, click **View Jobs** under the **Search** field, refreshing the screen to view ongoing actions.

# CHAPTER 6

## Generating reports

This section contains the following topics:

- [Generate a report](#).....46

## Generate a report

### About this task

Out of the box, you can run 11 pre-built reports for Avamar and Data Domain systems.

For more information about these reports, see the *Dell EMC Data Protection Advisor Product Guide*.

If you want to generate your own reports, see the *Dell EMC Data Protection Custom Report Guide*.

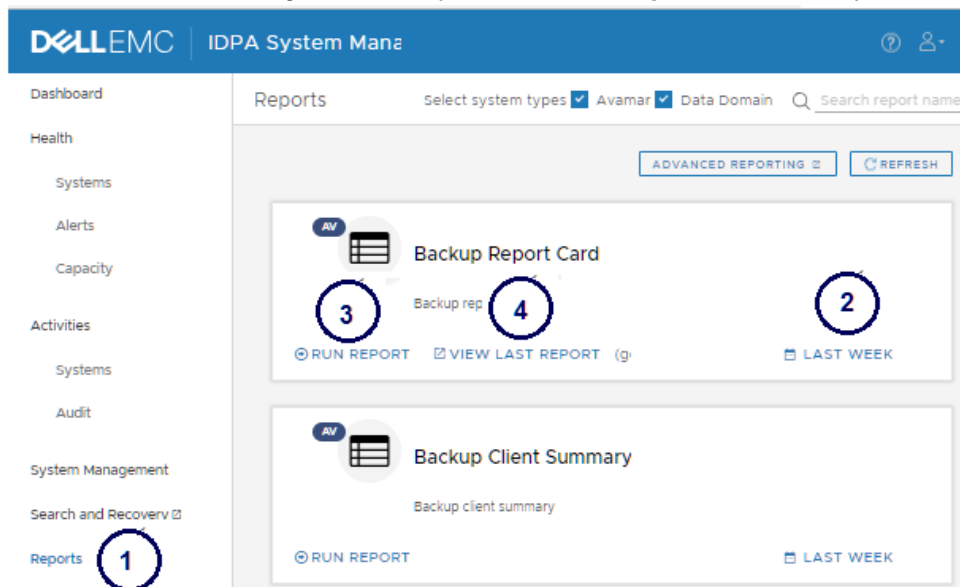
### Procedure

1. Access the *IDPA System Manager* and select **Reports** in the navigation pane.

In the right pane, each report type is displayed in a separate card. The pane displays both Avamar and Data Domain reports, but you can use the checkboxes in the upper right to filter the reports shown.

The report period for each report displays in the lower right. The default report period is the previous week, but you can change this by clicking **Last Week** and selecting a different period.

2. To generate a report, click **Run Report** under the report name.



1. Select **Reports**.
2. (Optional) Change time period.
3. Click **RUN REPORT**.
4. Click **VIEW LAST REPORT**.

IDPA generates the report and displays **View Last Report** when it is ready to display.

3. Click **View Last Report** to display the report in a new window.

# INDEX

## N

Network Validation Tool 8

NVT 8

