# Dell EMC Integrated Data Protection Appliance

Version 2.4

## Getting Started Guide

302-005-675
REV. 05
December 2019

DELL EMC

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

# CONTENTS

# CHAPTER 1

# Introduction

This section contains the following topics:

# 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 like performing backups, restores, and generating reports that you can use to get the IDPA appliance 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

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

### Integrated solution

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

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

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

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

### Centralized management

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

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

### Appliance administration

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

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

### Backup administration

The IDPA uses Avamar Virtual Edition (AVE) servers to perform backup operations, with the data being stored in a Data Domain system. 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 that are reported in the server monitor.

You can also add Avamar NDMP Accelerators to enable backup and recovery of NAS systems. The Avamar NDMP Accelerator uses the network data management protocol (NDMP) to enable backup and recovery of network-attached storage (NAS) systems. The accelerator performs NDMP processing and then sends the data directly to the Data Domain Server.

### Reporting and Analytics

The Reporting and Analytics feature offers a robust reporting functionality with dedicated sections for various features. These reports help you retrieve information about the 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 also run system and customized reports, dashboard templates, and schedule the reports generation as per your requirements.

### Search

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

### Disaster recovery

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

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

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

### Scalability

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

- For the DP4400 model with a capacity from 8 TB to 24 TB, you can expand the storage capacity in 4 TB increments, but you cannot expand the capacity beyond 24 TB.
- For the DP4400 model with a capacity from 24 TB to 96 TB, you can expand the storage capacity in 12 TB increments, but you cannot expand the capacity beyond 96 TB.

The following table details the base configuration for the DP4400 models.

**Table 1** Base Configuration for IDPA DP4400 Models

| Model | Base Configuration |
|---|---|
| DP4400 | From 8 TB up to 24 TB |
| | From 24 TB up to 96 TB |

### Unified support

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

## System self-protection

The IDPA is configured to protect itself from data loss with the backup and storage applications included in the system

It is protected with a pre-defined backup job policy that is scheduled daily and has a 30-day retention period. The metadata is protected through a backup to the Protection Storage (Data Domain) using checkpoints.

**Table 2** 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 |

## Network connectivity overview

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

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

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

**Table 3** IP address range assignments for DP4400

| IP Range Allocation | Example | Component | Assigned Field |
|---|---|---|---|
| +0 | `192.0.2.1` | vCenter | VMware vCenter Server VM |
| +1 | `192.0.2.2` | 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` | Reporting and Analytics | Application Server Host VM |
| +8 | `192.0.2.9` | Reporting and Analytics | Datastore Server Host VM |
| +9 | `192.0.2.10` | Search | Index Master Node Host VM |
| +10 | `192.0.2.11` | DD Cloud DR CDRA (optional) | Data Domain Cloud Disaster Recovery (DD Cloud DR) Cloud DR Add-on (CDRA) virtual appliance |

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

# 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 IDPA Appliance

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

**About this task**

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

**Procedure**

1. Identify 13 unassigned IP addresses for the IDPA components. To simplify configuration, select a range of 13 contiguous addresses.

   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 8.

   **Note:**
   The DP4400 installation requires IP addresses strictly from a single subnet having a single gateway.

2. Register the 13 IP addresses in DNS with forward and reverse lookup entries for each address. Ensure that the router for the 13 IP addresses can be pinged.

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

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

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

   **Note:** For DP4400, only during the initial activation, the license keys are automatically downloaded from the ELMS server if the appliance is connected to the internet.

   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
- Appliance Configuration Manager (ACM)
- Network Configuration wizard

## Online Support

Record the following information related to your Online Support account:

### Online Support credentials

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

### Site ID

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

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

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

## Connect to the ACM

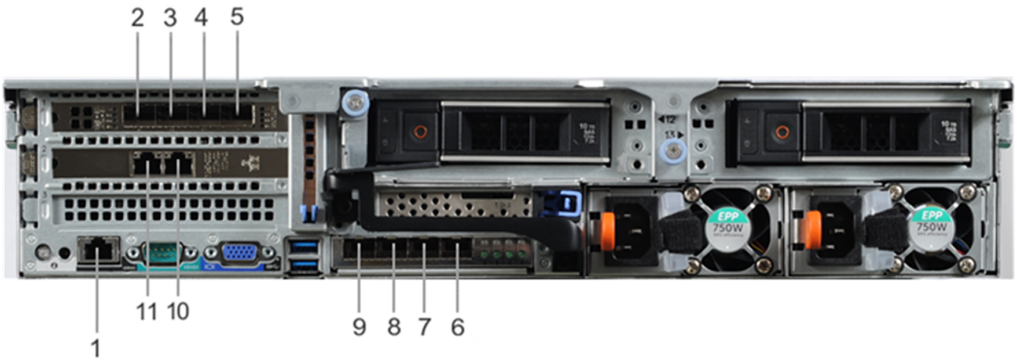
Connect to the ACM user interface and begin the configuration process. For a seamless experience, enable both private and public network connections to your service computer.

**Before you begin**

- After powering on the appliance, wait 5 minutes for startup to complete.
- Verify that the service computer is connected to the 1 GbE port identified as (10) in Figure 1 on page 15.
- On the service computer, record the IP address settings for the Ethernet interface that is connected to the DP4400.

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

**Figure 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`. Also, the password must not start with a hyphen (`-`) and end with a period (`.`).

   The system logs you out after changing the password. Log back in with the new password.
6. On the **End User License Agreement** screen, accept the EULA.

### Results

The **Network Configuration** screen appears.

## DP4400 ports

### About this task

The following table provides the callout number and the type of port for the DP4400 ports in *Figure 1 DP4400 network and iDRAC connections*.

**Table 4** DP4400 port types

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

**Note:** Ports 2 and 9 are a vSwitch0 network team. Ports 3 and 8 are a vSwitch1 network team and are used during appliance configuration.

**Note:** Ensure that the four required 10 GbE ports (2, 3, 8, and 9) are connected to the access ports on the switch in your network.

# Network Configuration wizard

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

### 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. This is the first IP address of the 13 IPs that is reserved for the ACM.

**ESXi IP**

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

**NTP server IP**

The NTP server IP address for your network environment.

2. Click **Submit**.

**Results**

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

  **Note:** For automatic forwarding to work correctly, the computer you use to complete the configuration must be connected to the same network as the configured ACM IP address.
- If you cannot have connections to both public and private networks 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 setup 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 `https://<configured ACM IP address>:8543` URL in a browser.

## Secure Remote Services (SRS)

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

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

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

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

### Secure Remote Services configuration for IDPA

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

## Welcome

Read the prerequisites on the prerequisites link available on the welcome page before you continue.

You can select **Cloud Disaster Recovery**, **Data Protection Advisor**, and **Data Protection Search** from the list of optional components to deploy and configure on the IDPA appliance.

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

## License

The DP4400 uses the In-Product license activation feature which automatically downloads and activates the licenses for the components if the appliance is connected to the internet.

If you are not connected to the internet you must upload the Data Domain, Avamar, and Data Protection Advisor licenses obtained from Dell EMC Software Licensing Central.

## General settings

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

Do not select the **Select IP address range (11)** check box if you are specifying non-sequential IP addresses for each component in the configuration.

## 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 19.

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`

If prompted, log in with the ACM credentials to view the current state of the configuration progress.

## Download configuration information

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, SNMP, and NTP settings, and modify customer support information.
Refer to About the ACM dashboard on page 35 for more information about using the ACM dashboard to monitor and manage the components of the IDPA.

# Installing the DataProtection-ACM pre-installation patch

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

For example:

`Idpa_pre_update_N.N.N-nnnnnn.zip`

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

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

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

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

**Procedure**

1. Check https://support.emc.com/downloads/41849_Integrated-Data-Protection-Appliance to see if a pre-installation patch is available for your version of IDPA. If a pre-installation patch is available, download it to a folder on your laptop.
2. Extract the contents of the `Idpa_pre_update_N.N.N.nnnnnn.zip` file.

   The zip file contains the `Idpa_pre_update_N.N.N.nnnnnn.tar.gz` file and the `ReadMe.txt` file.

   **Note:** For additional information about installing the pre-installation patch, see the `ReadMe.txt` file.
3. Open the WinSCP or SCP application on the service laptop, and then connect to the DataProtection-ACM by performing the following actions:
   a. In the **File protocol** field, select **SFTP**.
   b. In the **Hostname** field, enter `192.168.100.100` as the IP address of the DataProtection-ACM.
   c. In the **Port number** field, specify the default port number **22**.

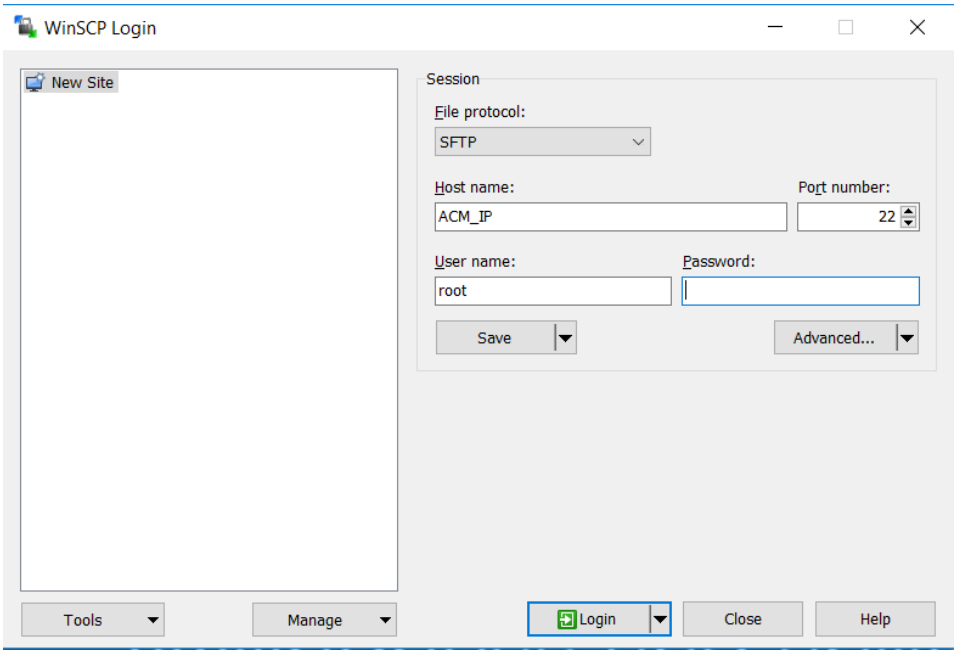
d. In the **User name** field, enter `root`.

e. In the **Password** field, enter `Idpa_1234`.

f. Click **Login**.

The following figure shows a sample WinSCP session configuration window.

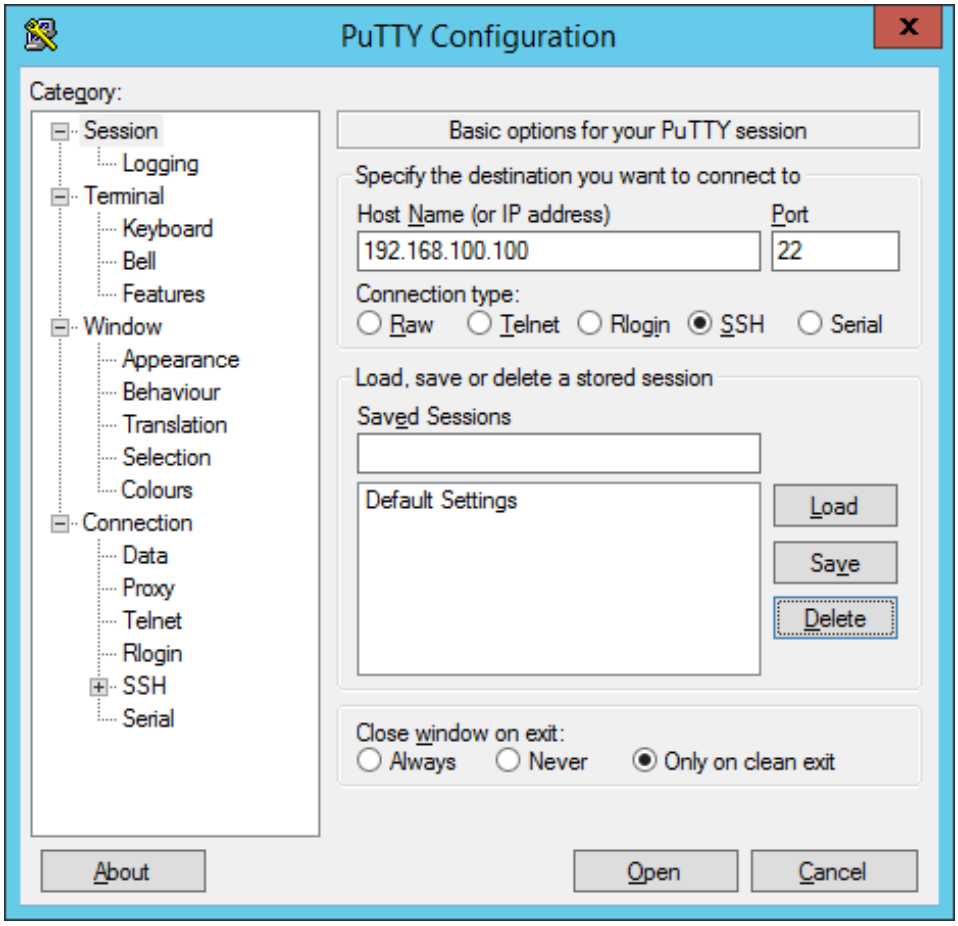
**Figure 2** WinSCP session configuration window




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

   The following figure shows the Putty configuration screen.

**Figure 3** Putty Configuration screen for DataProtection-ACM




7. At the login as prompt, type **root**.
8. At the Password prompt, type the password for the root user.

   The default password for the root user is Idpa_1234.
9. Determine the DataProtection-ACM version by typing the following command:

   **rpm -qa | grep dataprotection**

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

   where *n.n.n* is the latest IDPA version and *nnnnnn* is the build number.
10. Change to the directory that contains the pre-installation patch file by typing the following command:

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

    **tar -xvf** Idpa_pre_update_*N.N.N.nnnnnn*.tar.gz

    The contents are extracted to a subdirectory named Idpa_pre_update_*N.N.N.nnnnnn*.
12. Change directory to Idpa_pre_update_*N.N.N.nnnnnn*.tar.gz directory by typing the following command:

    **cd /tmp/patch/Idpa_pre_update_*N.N.N.nnnnnn*/**

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

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

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

    **`./install.sh`**

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

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

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

    **`rpm -qa | grep dataprotection`**
    Ensure that the DataProtection-ACM version is the latest version.

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

# Secure Remote Services (SRS)

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

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

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

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

## Prepare the IDPA environment for SRS registration

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

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

Fore more information about Configuring SRS, see #unique_31.

## Add customer site IDs to SRS

Add all customer site IDs to the SRSgateway host.

### Before you begin

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

### Procedure

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

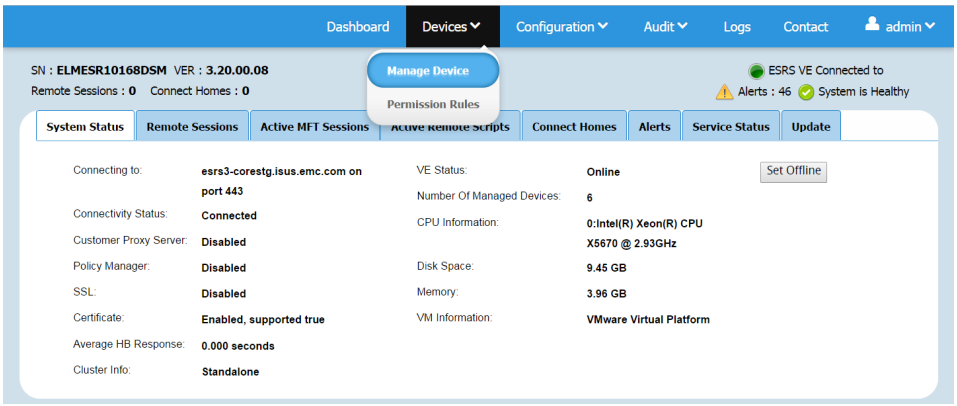
   `https://SRS_Gateway_IP_Address:9443`
   where *SRS_Gateway_IP_Address* is the IP address of the SRS gateway host.

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

   The SRS console appears.

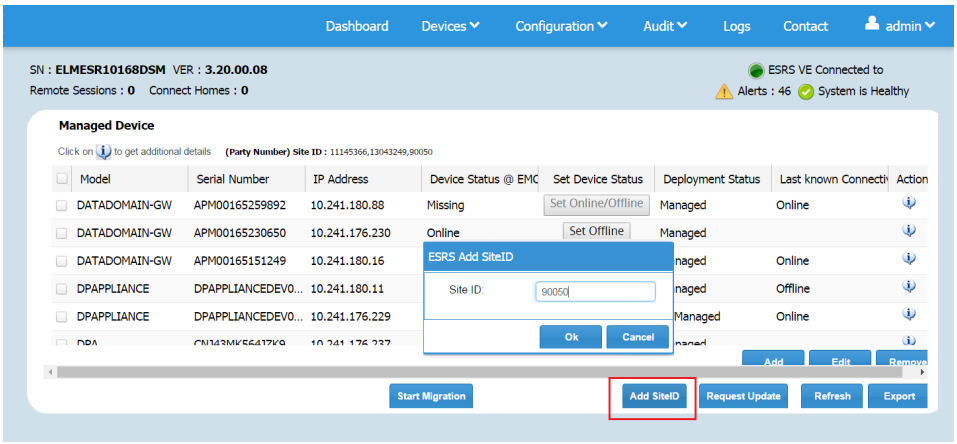
3. From the **Devices** menu, select **Manage Device**.

   The following figure shows the SRS console and the **Devices** menu.
   **Figure 4** SRS Devices menu




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

   The following figure shows the **SRS Add SiteID** window.
   **Figure 5** SRS Add SiteID window



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

## Verifying the SRS gateway site ID addition

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

### Before you begin

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

### About this task

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

### Procedure

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

   http://servicelink.emc.com

   The **RSA Access Manager** page appears.

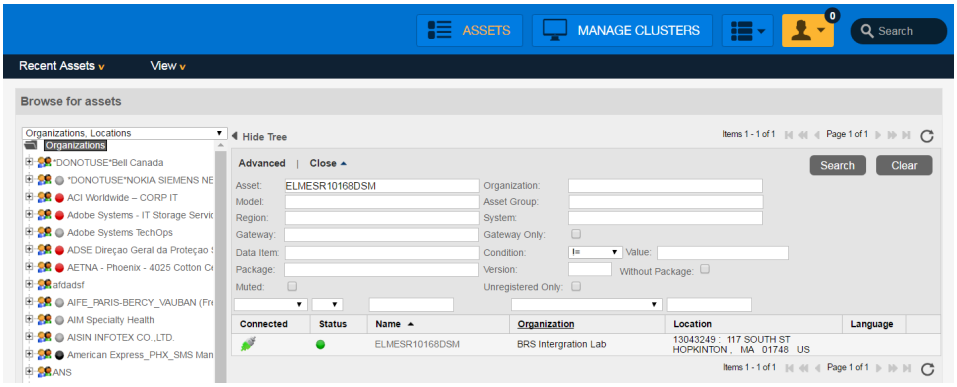
2. In the **User ID** field, type your user ID. In the **Password** field, type your SecureID passcode, and then click **Go**.

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

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

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

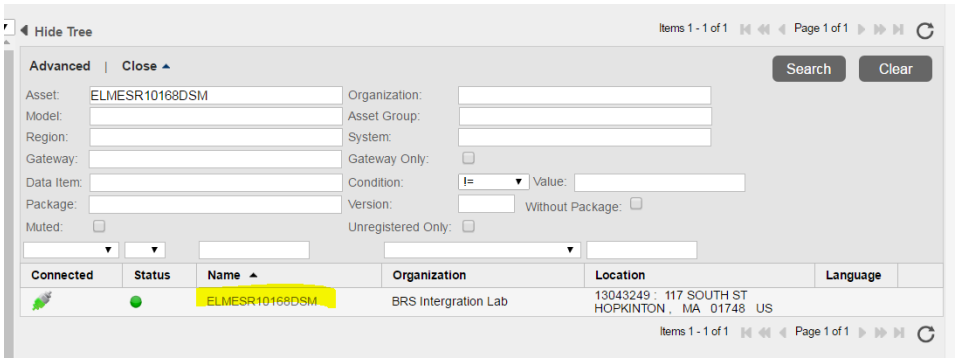
   **Figure 6** SRS Assets view




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

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

**Figure 7** Search Results table with serial number highlighted

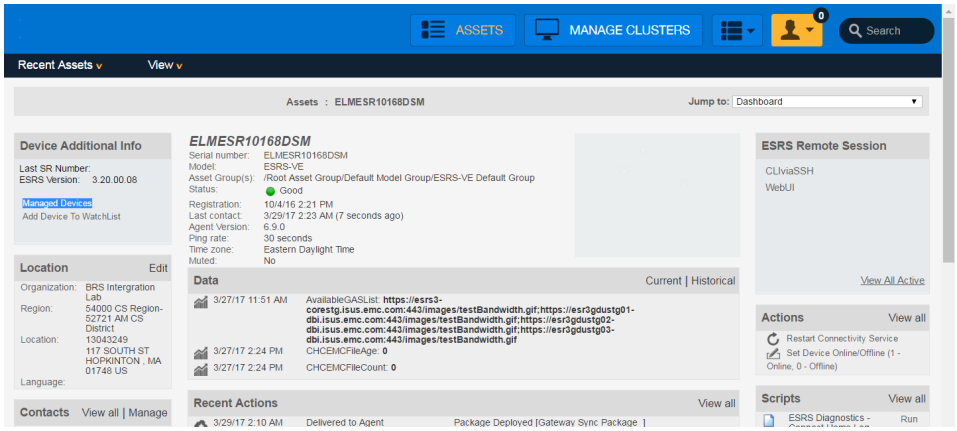



The **Device Information** window appears.

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

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

   **Figure 8** SRS device information with Managed Devices selected




The **HA Gateway Cluster** window appears.

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

# Install and deploy IDPA

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

### About this task

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

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

### Procedure

1. Open a browser and enter `https://192.168.100.100:8543` to access the ACM UI.
2. Enter **Username** and **Password** in the respective fields and click **Login**.

   The **Change Appliance Password** page is displayed.

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

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

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

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

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

   The **Network Configuration** page is displayed.

5. In the **Network Configuration** page, under **Network Settings** section enter the IP addresses in the following field and click **Submit**.

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

   - **Subnet Mask**
   - **Gateway**
   - **Primary DNS server**
   - **Secondary DNS server**
   - **Domain Name**
   - **Appliance Configuration Manager IP Address**
   - **ESXi IP Address**
   - **NTP server**

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

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

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

      The Network Configuration progress page is displayed.

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

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

6. In the Dell EMC Secure Remote Services for Integrated Data Protection Appliance page, perform the following actions.

   a. Enter the **SRS Gateway IP**.

   b. Enter the online support credentials in the **Username** and **Password** fields.

   c. Click **Configure**.

   The IDPA Appliance configuration page is displayed.

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

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

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

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

b. In the **License** page, the system automatically downloads the licenses for **Protection Storage**, **Backup Server**, and **Reporting and Analytics** if you are connected to the network.

c. Click **Next**.

**Note:** If you are not connected to the network, click **Browse** to locate and upload the licenses.

d. In the **General Settings** page, perform the following actions.

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

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

c. Select and enter the IP address in the **IP address range (11)** field.

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

**Note:** If you do not select the **IP address range (11)** checkbox you must manually configure and enter the IP addresses in the other sections. See Step 8 through Step 9

e. Click **Validate.**

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

f. Click **Next**.

The **Customer information** page is displayed.

8. You can configure the settings manually. To configure the settings manually, perform the following actions.

a. In the **Protection storage configuration** page, under the **Data network** section, enter valid IP addresses for **Backup IP 1 address** and **Backup IP 2 address**.

b. In the **Backup server** page, enter valid IP addresses in the following.

- **Avamar server IP address** in the **Backup node** section.
- **Image Proxy IP address** in the **Integrated Data Protection Appliance backup**.

c. In the **IDPA System Manager** page, enter the IP address in the **Server IP Address** field.

d. In the **Reporting and Analytics** page, enter the IP addresses in the **Application server IP address** and **Datastore server IP address** fields.

e. In the **Search** page, enter the IP address in the **Index Master Node IP address**.

f. In the **Cloud Disaster Recovery** page, enter the IP address in the **Cloud DR Add On IP address**.

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

The Configuration progress page is displayed. You can view the configuration progress for each component in addition to the configuration progress for the appliance.

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

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

    a. View the **Errors**, **Warnings**, and **Diagnostic report**.

    b. Click **Download PDF** to download a PDF of the configuration progress.

    c. Click **Download Solution ID** to download the solution ID.

    d. Click **Download Configuration** to download the configuration.

    e. Click **Download configuration XML** to download the configuration XML file.
13. Click **Finish**.

    The IDPA Appliance is installed and deployed.

    **Note:** If the installation fails, click **Download Log Bundle** to download the logs of the installation and then click **Retry** to re-start the installation. Ensure that you download the logs before you retry the installation, else the system deletes the logs.

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

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

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

**Procedure**

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

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

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

2. In the **General Settings** page, perform the following actions:
   a. Select the **IP address range** in the **Management network settings** and **Backup network settings** section.
   b. Click **Validate**.

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

### Results

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

## Configure the ACM settings manually for separate management networks

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

### About this task

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

### Procedure

1. In the **General Settings** page, ensure that you do not select the **IP address range** check box in the **Management network settings** and **Backup network settings** sections.
2. Click **Next**.

   The **vCenter configuration** page is displayed.
3. In the **vCenter configuration** page, enter the unique IP address in the **IP address** field to configure the internal **vCenter**.
4. Click **Next**.

   The **Protection Storage configuration** page is displayed.
5. In the **Protection Storage configuration** page, enter unique IP addresses under the **Protection Stoarge** and **Backup Network** sections for the following fields.
   - **Management Network IP address**
   - **Backup IP address1**
   - **Backup IP address 2**

6. Click **Next**.

   The **Backup Server configuration** page is displayed.

7. in the **Backup Server configuration** page, enter unique IP addresses under the **Backup node** and **Integrated Data Protection Appliance backup** section for the following fields.
   - **Backup Node IP**
   - **Image Proxy IP address**
   - **Backup Proxy IP address**

8. Click **Next**.

   The IDPA System Manager page is displayed.

9. In the **IDPA System Manager** page, enter the unique IP address in the **Management Network IP** field.

## Retry installation

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

**About this task**

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

**Procedure**

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

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

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

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

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

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

## Rollback installation

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

**Before you begin**

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

**About this task**

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

**Procedure**

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

   The **Rollback Configuration** page is displayed.

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

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

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

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

**Results**

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

## Troubleshoot Health monitoring

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

**About this task**

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

**Procedure**

1. Log in to the ACM using SSH.
2. Run the following command to restart the RabbitMQ service.

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

3. Run the following command to check if the RabbitMQ service is running.

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

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

   ```
   #service dataprotection_webapp restart
   ```

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

# Troubleshooting

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

### Creating and downloading a log bundle

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

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

### Accessing vCenter

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

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

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

# CHAPTER 3

# About the ACM 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 version 64 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**.

# Appliance Configuration Manager dashboard home

The **Home** tab provides an overview of the status and settings for the IDPA components and also displays the general settings and customer information of the IDPA appliance.

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 the LDAP settings, 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:** You can configure the Secure Remote Services present under the **General Settings** panel. If the Secure Remote Services is not configured, you can configure it by clicking the **Edit** icon.

### 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**
- **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.

You can hover over the **Services** to view the status information for **IDPA System Manager** services.

To launch the web interface, click **IDPA System Manager Web UI** and log in.

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

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, metadata of the total and available backup storage, license status of the Backup Server node, and whether the installation of agents is in progress.

You can hover over the **Services** to view the status information for Avamar services.

Click **Backup Server Web UI** to launch the Avamar Web Interface 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*.

# 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.

**Note:** Protection Storage (Data Domain) cannot be managed by the Data Domain Management Center (DDMC) instance.

# Reporting and Analytics panel

The **Reporting and Analytics** panel displays the Data Protection Advisor (DPA) version, IP addresses for the Application Server and the Datastore Server, the license status of the Reporting and Analytics node, and any alerts that require your action.

You can hover over the **Services** to view the status information for Data Protection Advisor services.

To load the Reporting and Analytics console, click the **Reporting and Analytics Web UI** link.

If Reporting and Analytics 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 supports use of an external DPA implementation to analyze the system if you are running a corporate deployment of the DPA instance. However, IDPA dashboard (ACM) does not display any data that is associated with the external DPA separately. IDPA does not support local analytics and search functions when an external instance of DPA or Search is used. Moreover, if you are using an external DPA instance, you must configure and manage any such external DPA instances as external instances cannot be configured or managed through the ACM.

# Search panel

The **Search** panel displays the Search version, 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**.

IDPA supports the use of an external Search node if you are running a corporate deployment of the Search instance. However, the Search panel on the IDPA dashboard (ACM) does not display any data that is associated with the external Search separately. IDPA does not support local analytics and search functions when external instances of Search are used. Moreover, if you are using an external Search instance, you must configure and manage any such external instances as external instances cannot be configured and managed through the ACM.

# 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.

IDPA supports the use of an external CDRA if you are running a corporate deployment of the CDRA instance. However, the Cloud Disaster Recovery panel on the IDPA dashboard (ACM) does not display any events or data that is associated with the external CDRA separately. Moreover, if you are using an external CDRA instance, you must configure and manage any such external CDRA instances as external instances cannot be configured and managed through the ACM.

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

# Customer Information and General Settings panels

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

Hover over the gear icon on the **Customer Information** panel and click on **Enable remote support** to configure ESRS for the IDPA Appliance.

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

# User accounts for components

The IDPA configuration uses the user accounts in Table 5 on page 39. By default, these accounts use the common IDPA password .
The LDAP references in the below table apply to IDPA System Manager and Search components only. The appliance and other components do not use LDAP.

For information about how to change component passwords, see Change passwords and synchronize components on page 39.

**Table 5** Component and user account mapping

| Component | Username | Password |
|---|---|---|
| ACM | root | Common password provided during IDPA Appliance configuration. |
| IDPA System Manager (If external LDAP is not configured) | idpauser | Common password provided during IDPA Appliance configuration. |
| IDPA System Manager (If external LDAP is configured) | Respective LDAP credentials | External LDAP password as applicable. |
| Avamar | admin | Common password provided during the IDPA Appliance configuration |
| Data Domain | sysadmin | Common password provided during the IDPA Appliance configuration. |
| Data Protection Advisor | administrator | Common password provided during IDPA Appliance configuration. |
| Search | Respective LDAP credentials. If external LDAP is not configured, then idpauser | Common password provided during IDPA Appliance configuration. |
| CDRA | admin | Common password provided during IDPA Appliance configuration. |
| CDRS | admin or monitor | Password set during CDRS deployment. |
| vCenter | idpauser | Common password provided during IDPA Appliance configuration. |
| ESXi | idpauser | Common password provided during IDPA Appliance configuration. |

# Change passwords and synchronize components

Single-click user password change is one of the features, which simplifies the password maintenance of IDPA.

It is recommended that you use this feature for changing the password as it changes passwords for all the components in IDPA.

**WARNING** Changing passwords of individual components is not recommended. Due to any unforeseen circumstances, if you have to change passwords of individual components, see 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 an IDPA component causes the ACM UI to display the `password out of sync` error message. To enable the ACM to gather health information for the component, you must update the stored password (old password) in the ACM UI with the respective component's updated password. 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 the Avamar server and do not use the change password option on the 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 the Credential mismatch section.

## Credential mismatch

This section provides information about how to resolve the password mismatch scenario for the IDPA point products. If you manually modify the password on the point products 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.

**About this task**

To resolve a password mismatch, perform the following actions.

**Procedure**

1. Click the warning message in the point products panel and enter a new password.
2. Click **Update Password** in the point products panel and enter a new password.
3. Click the **Refresh** button on the ACM dashboard.

   The system updates the new password for all the relevant accounts.

## Credential mismatch for Backup Server

This section provides information about how to resolve the password mismatch scenario for the Backup Server . If you manually modify the password on the Backup Server 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.

**About this task**

To resolve a password mismatch on the Backup Server, 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 for all the relevant accounts.

# CHAPTER 4

# Performing a VM backup

This section contains the following topics:

# 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.

If 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

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

**About this task**

To create the vCenter and VM clients and add a dataset to the VM client, perform the following actions.

**Procedure**

1. Open a browser and enter `https://<ACM IP address>:8543` to access the ACM UI.
2. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
3. Click **System Management** on the left pane to display the System Managerpage.
4. Click the vertical ellipsis for the Avamar-Backup Server and select **Avamar Restore**.

   The **Asset Management** page on the Avamar UI is displayed.
5. To add the vCenter client, perform the following actions.
   a. Click the vertical ellipsis beside **ADD CLIENT** and select **Add VMware vCenter**.

      **Note:** Ensure that you are on the **root** domain.

      The **New vCenter Client** window is displayed.
   b. Select or enter the details that are required in the fields to create a vCenter client using the following table. Click **Next** to continue to the next page.

**Table 6** Adding vCenter Clients

| Page | Field | Description |
|---|---|---|
| Client Information | Client Type | Select VMware vCenter. |
| | New Client Name or IP | Client name or IP address. |

**Table 6** Adding vCenter Clients (continued)

| Page | Field | Description |
|---|---|---|
| | Client Domain | Domain name. |
| vCenter Information | User Name | The user name of the vCenter server administrator. |
| | Password | The administrator password. |
| | Verify Password | Enter the same password to verify if they are identical. |
| | Port | The vCenter HTTPS port number. |
| Advanced | Auto Discovery<br>• Enable Dynamic VM import by rule<br>• Enable Changed Block Tracking | Select the check box to enable the options. This an optional field.<br>**Note:** The **Enable Changed Block Tracking** checkbox is enable only when you select **Enable Dynamic VM import by rule**. |
| Optional Information | Optional Information<br>• Contact<br>• Phone<br>• Email<br>• Location | Enter the relevant information in the fields. All fields are optional for this task. |

c. Click **ADD** on the **Summary** page. Then refresh the screen to verify the new vCenter client.

d. Click **OK** on the **Finish** page.

The vCenter client is added and the **Asset Management** page is displayed

**Note:** Refresh the page to verify if the vCenter client is added.

6. To add the VMware client, perform the following actions.

a. In the **Domain** pane, expand the new vCenter client and click **VirtualMachines**.

b. In the **Asset Management** pane, click **ADD CLIENT**.

The **Select VMware Entity** page is displayed.

c. On the **Select VMware Entity** window, expand the host or cluster tree and select the cluster hosting the VM that you want to back up.

**Note:** To view the host or cluster details toggle the **Host/Cluster** button.

The VMs assigned to the cluster are displayed in the right panel.

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

7. To add the dataset perform the following actions.

a. Click **Setting** under the **Adminstration** section on the left pane.

**Note:** Ensure that you are on the **root** domain.

b. Click the **Dataset** tab in the **Setting** pane. and then click the plus sign (**+**) to display the **Create DataSet** window.

c. Click **+ ADD**.

The **Create DataSet** window is displayed.

d. In the **Dataset Name** field, enter the dataset name.

e. Select **Windows VMware Image** from the list of **Plugins** available.

**Note:** You can select a different plugin from the list of plugins available. The setting options and source data are different for the different plugins.

The **Windows VMware Image** options are displayed under the **Options** tab.

f. Select the **Index VMware Image Backups** checkbox.

g. Click **Source Data** tab to view the setting options.

The options available in the source data tab allows you to backup the source data based on your selection.

h. Click **Submit**.

The application displays **Dataset created successfully** message on the Avamar dashboard page.

**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.

# Deploy an Avamar proxy

This section provides you information about how to deploy the Avamar proxy.

**About this task**

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

**Procedure**

1. Open a browser and enter `https://<ACM IP address>:8543` to access the ACM UI.
2. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
3. Click **System Management** on the left pane to display the System Managerpage.
4. Click the vertical ellipsis for the Avamar-Backup Server and select **Avamar Proxy Deployment**.

   The **Proxy Management** page on the Avamar UI is displayed.
5. In the right pane, click the vertical ellipsis in front of the IDPA Backup Server and select **Avamar Proxy Deployment**.
6. In the **Config** section, perform the following actions. **Data Change Rate**, and **Backup Window**. Then select the checkbox.
   a. Select the vCenter that you added. For more information about adding a vCenter, see Define vCenter and VMware clients
   b. Enter the data change rate in the **Data Change Rate (%)** field.
   c. Enter the number of minutes in the **Backup Window (minutes)** field.
   d. Select the **Protect Virtual Machines on Local Storage** checkbox.
7. Click **CREATE RECOMMENDATION**.

   The **Recommendations** section displays the proposed new proxies under each host.
8. Expand the listings in the **Recommendations** section and select **New proxy** under the ESXi server host.
9. Click  .

   The **Proxy** window is displayed.
   a. Enter the proxy hostname in the **Name** field.
   b. Select an Avamar server **Domain** where this proxy resides.
   c. Enter the IP address in the **IP** field.
   d. Select a datastore from the **Datastore** list.
   e. Select a network from the **Network** list.
   f. Enter the server name or IP address in the **DNS** field.
   g. Enter the network gateway IP address in the **Gateway** field.
   h. Enter the network mask in the **Netmask** field.
   i. Enter the IP address in the **NTP** field.
   j. Click **SAVE**.

10. Click ✓ on the **Recommendations** section to deploy the proxy.

    The proxy deployment is displayed in the lower panel.

# Create and run the backup policy

This section provides you information about how to create a backup policy. The backup policy is created to protect the VMware client.

### About this task

To create the policy, perform the following actions.

### Procedure

1. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
2. Click **System Management** on the left pane to display the System Managerpage.
3. Click the vertical ellipsis for the Avamar-Backup Server and select **Manage Policies**.

   The **System Management > Manage Policies** page is displayed.
4. In the **Manage Policies** page, click plus (**+**).

   The **Add policy** window is displayed.
5. Select or enter the details that are required in the fields to create a new backup policy using the following table. Click **Next** to continue to the next page.

   **Table 7** Adding Policies

| Page | Field | Description |
|---|---|---|
| Information | Name | The policy name. |
| | Domain | Accept the default entry. |
| | Enabled | Click to enable the policy. |
| | Dataset | Select **VMware Image Dataset**. |
| | Schedule | Select **Daily Schedule**. |
| | Retention | Select **Default Retention**. |
| Clients (Optional) | Available clients | Select the VM client defined earlier in this guide. |
| Proxies (Optional) | Available proxies | Select the proxy defined earlier in this guide. |

6. Click **Finish**.

   The new policy is displayed in the policy list.
7. To run the policy, select the policy from the list and click **BACKUP NOW**.
8. Monitor the policy by clicking **Systems** under **Job Activities** in the left 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

This section provides you information about the basic VM restore procedure.

**Before you begin**

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

**About this task**

To restore a virtual machine, perform the following actions.

**Procedure**

1. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
2. Click **System Management** on the left pane to display the System Managerpage.
3. Click the vertical ellipsis for the Avamar-Backup Server and select **Avamar Restore**.

   The **Asset Management** page on the Avamar UI is displayed.
4. Expand the vCenter that you added in the **Domain** pane and select **Virtual Machines** to display the VM clients belonging to that vCenter.
5. In the client list, select the VM client that you want to restore.
6. Click **VIEW MORE** to view the list of all the backups.
7. Select the latest backup from the list and click **RESTORE**.

   The **Select Restore Content** window is displayed.
8. Select the content that you want to restore and click **NEXT**.

   The **Restore** window is displayed.
9. Select or enter the details that are required in the fields to restore from a virtual machine using the following table. Click **Next** to continue to the next page.

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

**Table 8** Restoring from a VM

| Wizard page | Field | Description |
|---|---|---|
| Basic Config | Destination | Select **Restore to new Virtual Machine**. |
| | Post Restore Options | Select **Do not power on VM after restore**. |
| | Proxy | Select **Automatic**. |
| | Use CBT to increase performance | Select the checkbox to increase the performance using CBT. |
| 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. |

**Table 8** Restoring from a VM (continued)

| Wizard page | Field | Description |
|---|---|---|
| Resource Pool | | Expand the tree and select the resource pool. |
| Datastore | | Select the destination ESX datastore. |

**Note:** The options in the **Restore** wizard change based on the options you select during the restore procedure.

10. On the **Summary** page, review your entries and click **FINISH** to perform the restore.

**Note:** To monitor the results, click **Activity** in the Avamar UI navigation tree and view the processing results on the right **Activity** pane.

# Restore using Instant Access

You can use the instant access feature to perform near real-time recovery of a VM. Avamar 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.

**About this task**

To restore a virtual machine using the instant access feature, perform the following actions.

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

.

**Procedure**

1. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
2. Click **System Management** on the left pane to display the System Managerpage.
3. Click the vertical ellipsis for the Avamar-Backup Server and select **Avamar Restore**.

   The **Asset Management** page on the Avamar UI is displayed.
4. Expand the vCenter that you added in the **Domain** pane and select **Virtual Machines** to display the VM clients belonging to that vCenter.
5. In the client list, select the VM client that you want to restore.
6. Click **RESTORE**.

   The **Qucik Restore** dialog box is displayed.

   **Note:** The quick restore feature restores the latest backup.
7. Click **OK**.

   The **Select Restore Content** window is displayed.
8. Select the content that you want to restore and click **NEXT**.

   The **Restore** window is displayed.
9. Select or enter the details that are required in the fields to restore from a virtual machine using the following table. Click **Next** to continue to the next page.

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

**Table 9** Restore Using Instant Access

| Wizard page | Field | Description |
|---|---|---|
| Basic Config | Destination | Select **Instant Access**. |
| | Proxy | Select **Automatic**. |
| 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. |

**Table 9** Restore Using Instant Access (continued)

| Wizard page | Field | Description |
|---|---|---|
| Host/Cluster | | Expand the tree and select the ESXi host/cluster. |
| Resource Pool | | Expand the tree and select the resource pool. |

**Note:** The options in the **Restore** wizard change based on the options you select during the restore procedure.

10. On the **Summary** page, review your entries and click **FINISH** to perform the restore.

**Note:** To monitor the results, click **Activity** in the Avamar UI navigation tree and view the processing results on the right **Activity** 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. To restore specific files, perform the following actions.

### Procedure

1. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
2. Click **Search and Recovery** on the left pane.

   The application opens the **Search** page.
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 application displays the list of files based on your query.
4. Select one or more files that you want to restore and click **Restore** to display the **Restore** dialog.
5. Select or enter the details that are required in the fields to restore from the search results using the following table. Click **Next** to continue to the next page.

**Table 10** Restore Specific Files

| Field | Description |
|---|---|
| Original path / Destination path | Select the restore location. When applicable, click **Overwrite** and select **Restore Access Control List** to protect the file with the same access control list settings |
| Client | When **Destination Path** 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

This feature enables you to generate reports for Avamar and Data Domain systems. There are 11 preconfigured reports that you can generate.

### About this task

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. Click **IDPA System Manager Web UI** and log in to the System Manager.

   The IDPA System Manager dashboard page is displayed.
2. Click **Reports** on the left pane.

   On the right pane, each type of report is displayed. The pane displays both Avamar and Data Domain reports. You can select the Avamar and Data Domain, or both check boxes in the upper right to filter the reports shown.

   The report period for each report is displayed in the lower right. The default report period is the previous week, but you can change the time period by clicking **LAST WEEK** list and selecting a different period.
3. To generate a report, click **RUN REPORT** under the report name.

   IDPA generates the report and displays the **View Last Report** with the timestamp on completion.
4. Click **View Last Report** to display the report in a new window.

# INDEX