

Dell EMC IDPA System Manager

Version 18.2

Administration Guide

302-005-309

REV 02

October 2019

Copyright © 2017-2019 Dell Inc. or its subsidiaries. All rights reserved.

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

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

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

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

CONTENTS

	Preface	7
Chapter 1	Overview	11
	IDPA System Manager overview.....	12
	Environment and system requirements	13
	Monitoring systems	14
	Managing Avamar systems	14
	Systems data refresh times	14
	Search and recover capabilities.....	15
	Report capabilities.....	15
	User Interface.....	16
	Header.....	16
	View version information.....	16
	User menu.....	16
	Left menu.....	17
	Pages.....	18
	Master and Detail panes.....	18
	Changing dashboards.....	18
	Filtering.....	18
	Sort information that is displayed in tables.....	20
	Dialog boxes.....	20
	Notification bar.....	20
	Overflow button.....	20
Chapter 2	Using Dashboards	21
	Dashboards overview.....	22
	Dashboard widgets	22
	Activity Counts widget.....	22
	Activity Trend widget.....	23
	Assets Summary widget.....	23
	Assets Top Offenders widget	23
	Alerts Summary widget.....	23
	Storage Capacity Top Utilization widget.....	24
	Storage capacity summary widget	24
	Health summary widget.....	24
	Drill down pages.....	25
	Managing dashboards.....	25
	Add a dashboard.....	25
	Editing a dashboard.....	25
	Delete a dashboard.....	26
	Editing widgets	27
	Change the widget type.....	27
	Edit the reporting time range.....	27
	Edit the activity view.....	28
	Edit the activity type	28
	Refresh the dashboard.....	29
	Filter systems or assets in a dashboard widget.....	29

Chapter 3	Monitoring System Health	31
	Monitoring health status.....	32
	Reading the Health page.....	32
	Reading the detailed health summary pane.....	33
	Data Protection Advisor and Search system health information.....	34
	Managing alerts.....	35
	Reading alerts	35
	Dismissing alerts.....	36
	Monitoring system capacity.....	37
	Reading the system capacity table.....	37
	Reading the detailed system capacity pane.....	37
Chapter 4	Monitoring Activities	39
	Activities overview.....	40
	Monitoring job activities	40
	Reading the Job Activities page.....	40
	Reading the detailed job activity pane.....	41
	Rerun an Avamar job activity.....	42
	View job activities for a specific system.....	42
	Monitoring asset activities.....	42
	Reading the Asset Activities page.....	42
	Reading the detailed asset activity pane.....	43
	Rerun an Avamar asset activity.....	44
	View asset activities for a specific system.....	44
	View activities for a specific asset.....	44
	View asset activities within a job.....	45
Chapter 5	Managing Systems	47
	System management overview.....	48
	Adding a system.....	48
	Add an Avamar system.....	48
	Add a Data Domain System.....	49
	Add a Data Protection Advisor system.....	50
	Add a Search system.....	50
	Edit a system.....	51
	Delete a system.....	51
	Managing system groups.....	52
	Add a group.....	52
	Edit a group.....	53
	Delete a group.....	54
Chapter 6	Monitoring Assets	55
	Assets overview.....	56
	Monitoring assets.....	56
	Reading the Assets Inventory page.....	56
	Reading the detailed asset pane.....	56
	View assets for a specific system.....	57
	Tag assets	58
	Filter assets.....	58
Chapter 7	Managing Avamar Protection Policies	59
	Overview of Avamar policies.....	60
	Managing data protection policies for Avamar systems.....	60


	View policies.....	60
	Adding an Avamar policy.....	60
	Editing an Avamar policy.....	64
	Delete a policy.....	66
	Run a backup policy.....	66
Chapter 8	Launching System Management Applications	69
	Launching Avamar Administrator.....	70
	Launch Avamar Administrator from the overflow button.....	70
	Launch Avamar Administrator from the Detail pane.....	70
	Launching Avamar AUI.....	71
	Launch Avamar Restore from the overflow button.....	71
	Launch Avamar Proxy Deployment from the overflow button.....	71
	Launching Data Domain System Manager.....	72
	Launch System Manager from the overflow button.....	72
	Launch System Manager from the Detail pane.....	72
	Launching Search.....	73
	Launching Data Protection Advisor.....	73
Chapter 9	Running Reports	75
	Reports overview.....	76
	Run a report.....	76
	View the last report.....	77
	Backup Report Card.....	77
	Backup Client Summary.....	77
	Strike Summary.....	78
	Backup Data Backed Up Daily.....	78
	Backup Number of Jobs Backed Up Daily.....	79
	Data Domain Utilization.....	79
	Data Domain Tier Utilization.....	79
	Data Domain Daily Compression Statistics.....	79
	Data Domain Filesystem Utilization	80
	Data Domain DeDuplication Ratio.....	80
	Data Domain Active Streams.....	80
Chapter 10	Auditing IDPA System Manager Activities	81
	IDPA System Manager audit overview.....	82
	Activities audit information.....	82
Chapter 11	Server Administration	83
	Backing up IDPA System Manager.....	84
	Restoring a backup of IDPA System Manager.....	84
	Change the IDPA System Manager IP address.....	84
	Change the network configuration for OVA deployments of IDPA System Manager.....	85
	Upgrading IDPA System Manager.....	86
	Upgrade IDPA System Manager to version 18.2 on standalone server or virtual machine.....	86
	IDPA System Manager OS update.....	88
	Migrating from Multiple Systems Management to IDPA System Manager.....	88

Chapter 12	Troubleshooting	89
	Directory structure and log information.....	90
	Deployment of IDPA System Manager fails due to "No space left on device" ...	90
	Troubleshooting LDAP.....	91
	Check the LDAP status in the log file.....	91
	Diagnosing LDAP authentication failure.....	92
	Restore access to IDPA System Manager after LDAP misconfiguration ..	92
	Remove LDAP from IDPA System Manager.....	93
	Systems fail to activate.....	93
	Avamar systems fail to activate.....	94
	Lockbox.....	94
	Lockbox password requirements.....	95
	Reset the lockbox.....	95
	Remove the lockbox.....	95
	Create the lockbox.....	96
	Unlock a IDPA System Manager user account.....	96
	The SSO service fails to start on IDPA System Manager.....	96
	Disabling SSO	97
	Reregister SSO for a system.....	98
	Resolve error notifications.....	98
Glossary		99

Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

 **Note:** This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

Purpose

This document includes information about how to administer IDPA System Manager.

Audience

This document is intended for IDPA System Manager administrators.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
02	October 7, 2019	Editorial updates.
01	January 31, 2019	First release of the <i>IDPA System Manager 18.2 Administration Guide</i> .

Related Documentation

For information about IDPA System Manager compatibility, refer to the IDPA System Manager Release Notes.

The IDPA System Manager documentation set includes the following publications:


- *IDPA System Manager Getting Started Guide*
- *IDPA System Manager Security Configuration Guide*
- *IDPA System Manager Release Notes*
- *IDPA System Manager Administration Guide*


The documentation for the following products includes more information:

- Avamar
- Data Domain
- Search
- Data Protection Advisor

Special notice conventions that are used in this document

The following conventions are used for special notices:

 **NOTICE** Identifies content that warns of potential business or data loss.

 **Note:** Contains information that is incidental, but not essential, to the topic.

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.

i **Note:** To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://community.emc.com>. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Overview

Learn about IDPA System Manager.

This chapter contains the following sections:

• IDPA System Manager overview	12
• Environment and system requirements	13
• Monitoring systems	14
• Managing Avamar systems	14
• Systems data refresh times	14
• Search and recover capabilities	15
• Report capabilities	15
• User Interface	16

IDPA System Manager overview

IDPA System Manager provides a solution for data protection administrators who manage multiple independent data protection applications and storage devices.

When you work with multiple data protection applications, operational monitoring and management can be a complex, time consuming effort.

IDPA System Manager enables administrators to efficiently and effectively monitor and manage the software products within the Data Protection Suite family from a single user interface, simplifying the entire data protection experience.

IDPA System Manager includes the following features:

Comprehensive dashboards

IDPA System Manager has a comprehensive and customizable dashboard for at-a-glance monitoring of systems and activities. IDPA System Manager supports up to 20 dashboards per user.

Avamar system monitoring and management

IDPA System Manager supports a maximum combination of 200 Avamar systems.

When you add an Avamar system to IDPA System Manager, you can perform the following tasks:

- Launch Avamar Administrator or the AUI, using Single-Sign On (SSO) for supported versions.
- Monitor system health status and any alerts from the system.
- Monitor storage capacity usage.
- Monitor backup and replication activities at the Avamar job level.
- Monitor backup and replication activities at the Avamar asset level. Assets are virtual machines or plugins on the Avamar system.
- Rerun failed backup and replication activities at the job or asset level.
- Manage and run Avamar protection policies.

Data Domain system monitoring

IDPA System Manager supports adding up to 80 Data Domain systems.

When you add a Data Domain system to IDPA System Manager, you can perform the following tasks:

- Launch Data Domain System Manager.
- Monitor system health status and any alerts from the system.
- Monitor storage capacity usage.

Search integration

IDPA System Manager supports adding a single Search system.

When you integrate Search with IDPA System Manager, you can perform the following tasks:

- Launch Search Web User Interface, using Single-Sign On (SSO) for supported versions.
- Perform complex search and recover operations.

Data Protection Advisor integration

IDPA System Manager supports adding a single Data Protection Advisor system.

When you integrate Data Protection Advisor with IDPA System Manager, you can perform the following tasks:

- Launch DPA Web Console, using Single-Sign On (SSO) for supported versions.
- Run 11 of the most used Data Protection Advisor reports on Avamar and Data Domain systems.

Environment and system requirements

The following list includes information about environment and system requirements:

- To deploy the IDPA System Manager OVA, you must use VMware vCenter with VMware ESX 5.5 or later. The IDPA System Manager OVA does not deploy directly to the ESXi server.
- The IDPA System Manager host must have a minimum of 4 CPUs, 8 GB of RAM, and 550 GB of disk space available.
- The FQDN, IP, Netmask, NTP, Gateway, DNS, and time zone must be configured. The FQDN must resolve to the IP address.
- The environment must use static network settings.
- IDPA System Manager requires a minimum browser window size of 1366x768.
- Ensure that the DNS is set up correctly. The correct DNS setup ensures that systems can resolve the IDPA System Manager hostname and FQDN name.
- IDPA System Manager is compatible with VMware vSphere Fault Tolerance (FT), VMware vSphere High Availability (HA), and VMware vSphere vMotion.
- It is highly recommended that the ESXi server for the VMware environment where IDPA System Manager is deployed is protected from unexpected power outages with an uninterrupted power supply device.

Note: If you must power off the IDPA System Manager virtual machine, do not use the **Power off the virtual machine** feature in vCenter. Instead, shut down the machine gracefully with the **Shut Down Guest OS** button or the `shutdown -h now bash shell` command.

The following table includes information about the minimum versions of products that are supported with IDPA System Manager:

Table 3 Compatibility

Product	Supported versions
Avamar	7.5.0-183_HF300003 hotfix
	7.5.1-101_HF298709_27 hotfix
	18.1
	18.2
Data Domain	6.0
	6.1
	6.1.1
	6.1.2
	6.2
Data Protection Advisor	6.5
	18.1
	18.2

Table 3 Compatibility (continued)

Product	Supported versions
Search	1.1 SP3
	18.1
	18.2
Mozilla Firefox	Latest version
Google Chrome	Latest version

Monitoring systems

IDPA System Manager includes system monitoring features.

The systems monitoring features include:

- **Job Activities:** Monitor backup and replication activities at the job-level for Avamar systems.
- **Asset Activities:** Monitor backup and replication activities at the asset-level within jobs for Avamar systems.
- **Health:** Monitor the health status for Avamar and Data Domain systems.
- **Alerts:** Monitor alerts originating from Avamar and Data Domain systems.
- **Capacity:** Monitor capacity usage for Avamar and Data Domain systems.

Note: If a Data Domain system is configured in a monitored Avamar system, the Data Domain system is automatically added as a monitored system. However, you must add the Data Domain system credentials to IDPA System Manager to enable the full system monitoring features.

Managing Avamar systems

For Avamar systems, IDPA System Manager includes policy management and client management capabilities.

IDPA System Manager includes the following Policy Management capabilities:

- View, add, edit, and delete policies, retentions, schedules, and datasets.
- Add clients and proxies to policies.
- Perform a backup of a policy.
- Rerun a backup or replication activity.

IDPA System Manager includes the capability for you to view existing clients that are associated with an Avamar system.

Systems data refresh times

Every 90 seconds, IDPA System Manager refreshes system monitoring information based on data that has been fetched from systems within that 90 seconds.

Refresh the page to see the updated information.

Certain types of system information have different data refresh times. The following table describes the frequency that IDPA System Manager fetches information from systems being monitored.

Table 4 Systems monitoring data fetch times

Monitoring information type	Approximate data fetch times
Data Domain system health status and alerts	Every 5 minutes
Data Domain system capacity	Every 40 minutes
Avamar system health status	Every 1 minute
Avamar system capacity, checkpoint, and garbage collection	Every 15 minutes

Search and recover capabilities


IDPA System Manager integrates with Search to provide you with the ability to perform complex search and recover operations.

IDPA System Manager launches Search in a new browser tab.

After launching Search, you can perform the following tasks:

- Perform a targeted full content index (FCI) search.
- Search for files by name, location, size, owner, file type, and date.
- Perform advanced search queries including symbols, wildcards, filters, and operators.
- From the **Search Results** page:
 - View a preview of the content.
 - Download content.
 - Recover content.
 - Review the size of files or directories.

For comprehensive information about Search, refer to the Search documentation set.


 **Note:** To take full advantage of IDPA System Manager capabilities, it is recommended that all systems that are configured in Search also be configured in IDPA System Manager.

Report capabilities

IDPA System Manager provides the capability for you to run 11 of the most used Data Protection Advisor reports for Avamar and Data Domain systems.

IDPA System Manager reporting features require you to have Data Protection Advisor in the environment. For more information about Data Protection Advisor, refer to the Data Protection Advisor documentation set.

You can run, and then view these reports directly in the IDPA System Manager user interface. You can also specify the reporting period for these reports within the IDPA System Manager interface.

 **Note:** To take full advantage of IDPA System Manager capabilities, it is recommended that all systems that are configured in Data Protection Advisor also be configured in IDPA System Manager.

User Interface

Learn about the components of the IDPA System Manager user interface.

Header

The header includes the following components:

- **Active Filter** button: This button enables you to filter the information that appears on a page by one or more systems, groups, or tags. The **Active Filter** button appears only on pages where you can filter information.
- **User** menu: This menu enables you to change the password or log out of IDPA System Manager.
- **About** button: This button enables you to view IDPA System Manager version information.

Figure 1 Header



View version information

About this task

Click the following button to see details about the IDPA System Manager version:

Figure 2 About button



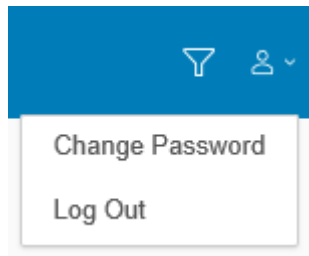
A dialog box appears and displays IDPA System Manager version information.

User menu

The **User** menu provides the capability for you to perform user tasks.

To perform the following user tasks, use the **User** menu:

- Change a password.
 - ① **Note:** If an external LDAP or AD user is logged in to the IDPA System Manager environment, change password is not supported.
- Log out of the user interface.

Figure 3 User menu

Change password

IDPA System Manager provides the capability for you to change a user password.

About this task

The password must meet the following requirements:

- A minimum length of 9 characters.
- A maximum length of 15 characters.
- At least one lowercase character.
- At least one uppercase character.
- At least one number.
- At least one of the following special characters:
! @ # \$ % ^ & * () - _

Procedure

1. In the **User** menu, click the down-arrow.
2. Select **Change Password**.
The **Change Password** dialog box appears.
3. Type the current password.
4. Type the new password.
5. To confirm that the new password was typed correctly, type the new password again.
6. Click **CHANGE PASSWORD**.

Log out of IDPA System Manager

When you are not using IDPA System Manager, it is recommended that you log out.

Procedure

1. In the **User** menu, click the down-arrow.
2. Select **Log out**.
The **Confirm** dialog box appears.
3. Click **LOG OUT**.

Left menu

The left menu provides the capability for you to browse the user interface.

From the left menu, you can access the following IDPA System Manager features:

- **Dashboard**
- **Health**
- **Alerts**
- **Capacity**
- **Asset Activities**
- **Job Activities**
- **System Management**
- **Asset Inventory**
- **Audit**
- **Search and Recovery**
- **Reports**

Pages

IDPA System Manager presents information in dashboards and detail pages.

Dashboard pages provide at a glance insight into operational behavior.

Detail pages display focused information and provide the capability for you to perform IDPA System Manager tasks.

Master and Detail panes

Most IDPA System Manager pages are composed of a **Master** and **Detail** pane.

The **Master** pane appears on the left side of a page and displays information in a table format. The **Detail** pane appears on the right side of a page and displays additional information for a selected row in a table. The **Detail** pane may also include buttons that you can use to perform tasks that are specific to the selected row in the table.

Changing dashboards

Click the **Dashboard** drop-down list to select a different dashboard.

Filtering

IDPA System Manager includes filtering capabilities. Filtering allows you to customize the information that appears.

The following filter types are available for you to use:

- **Column filters:** Appear in table headers.
- **Domain Filter:** Appears in the **Policies**, **Retentions**, **Schedules**, and **Datasets** pages for Avamar only.
- **Active Filter:** Appears in the user interface header.
- **Asset Filter:** Appears as a search bar on the **Asset Inventory** page.
- **Widget Filter:** Appears in widgets on the dashboard.

Column filters

Column filters can be used to filter the information that appears in tables.

Domain Filter

The **Domain Filter** can be used to select the domains that you want to view in the **Policies**, **Retentions**, **Schedules**, and **Datasets** pages for Avamar only.

Asset Filter

The **Asset Filter** can be used to filter assets listed on the **Asset Inventory** page. The **Asset Filter** search bar enables you to filter assets using a search phrase such as an asset tag, operating system, plugin, or asset name.

Active Filter

The **Active Filter** can be used to filter by one or more systems, system groups, or, on the **Asset Inventory** page only, by asset tags.

The **Active Filter** appears in on the following pages:

- **Health**
- **Alerts**
- **Capacity**
- **Job Activities**
- **Asset Activities**
- **Asset Inventory**

To filter certain items with the **Active Filter**, move one or more systems or system groups to the **Filtered By** pane.

When the **Active Filter** is enabled, a white filter icon appears enclosed in a circle in the header

Widget Filter

The **Widget Filter** can be used to refine the information that appears in a widget.

All types of widgets include a **Widget Filter** that enables you to filter the information reported in that widget by time range, system, system groups, or, for asset specific widgets, by asset tags.

Several widgets allow you to filter by time range. You can specify one of the following options:

- Last Hour
- Last 24 hours
- Last 7 days
- All Available

The **Activities Trend** widget also allows you to select whether to include the present day in the data for the past week.

The **Activities Count** and **Activities Trend** widgets allow you to choose to view activities information at the job or asset level. Also, these widgets allow you to pick whether to display backup activities, replication activities, or both.

When you use a dashboard widget to access a page, the information that is displayed is automatically filtered based on the widget filter settings.

Any active filters that are applied to a page, are listed in the filtered by section that appears at the top of the table.

Monitoring data is stored for 90 days. The **All Available** option is limited to data stored within the last 90 days.

Sort information that is displayed in tables

Information that is displayed in tables can be sorted in ascending or descending order.

About this task

To sort information, click a column heading.

After you click the column heading, an arrow appears. An up-arrow indicates that the column data is sorted in ascending order. A down-arrow indicates that the column data is sorted in descending order.

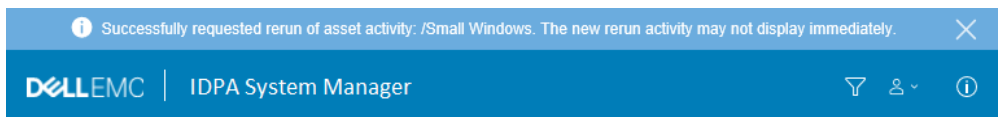
Dialog boxes

Dialog boxes can appear with information about a specific task. Dialog boxes can also appear for questions that require a decision.

Notification bar

To inform you of completed events or to alert you of issues that may require attention, notifications may appear in a bar across the top of the IDPA System Manager interface.

Figure 4 Example notification



Overflow button

Overflow buttons can appear within the user interface. When you click an **Overflow** button, a menu of available operations appears.

Figure 5 Overflow button



CHAPTER 2

Using Dashboards

Learn about using IDPA System Manager dashboards.

This chapter contains the following sections:

- [Dashboards overview](#) 22
- [Dashboard widgets](#) 22
- [Drill down pages](#) 25
- [Managing dashboards](#) 25
- [Editing widgets](#) 27

Dashboards overview

IDPA System Manager dashboards provide at-a-glance insight into systems and activities.

Dashboard widgets include key performance indicators that display the following types of system information:

- Backup Activities
- Replication Activities
- Trends
- Assets
- Capacity
- Health
- Alerts

From dashboard widgets, you can drill down into specific areas of interest.

All dashboard widgets have customizable settings. The customizable settings vary based on each widget. Certain widgets allow you to change the view, activity type, and time range. All widgets include a widget filter that you can use to filter by systems and groups. The widget filter also can filter by assets when available for a widget .

You can customize the dashboard layout to your preference by changing the widget type. Individualized dashboard settings are stored for each user. You can add, edit, and delete custom dashboards. Each user can create and store up to 20 dashboards.

Dashboard widgets

IDPA System Manager dashboards are composed of widgets that include a key performance indicator (KPI) or multiple KPIs. KPIs provide the capability for you to measure the objectives and performance of the systems that are configured in IDPA System Manager.

Activity Counts widget

The Activity Counts widget lists the number of recent activities and their status.

By default, there are two Activity Counts widgets on the dashboard: the **Assets | Backups & Replications** widget and the **Jobs | Backups & Replications** widget.

The Activity Counts widget shows the following information:

- The total percentage of activities that completed successfully.
- A donut chart comparing the activity status counts.
- A list of the status counts:
 - The number of activities that successfully completed.
 - The number of activities that failed.
 - The number of activities that completed with exceptions.
 - The number of running activities.
 - The number of pending activities.

You can use the overflow menu to customize the Activity Counts widget, including changing the view, activity type, and time period being reported.

Activity Trend widget

The Activity Trend widget shows trends in activity status over a period of the past seven days.

The Activity Trend widget shows a line graph that measures the completion status of activities over the past week.

The default Activity Trend widget is the **Asset | Backups & Replications Trend** widget. You can choose to include today in the trend and you can also customize the widget with a number of other options using the overflow menu.

Click **View All** to visit the **Asset Activities** or **Job Activities** page depending upon the set or chosen view.

Click **View All** to visit the **Asset Activities** or **Job Activities** page, according to the view that the widget is set to.

Assets Summary widget

The **Assets | Summary** widget reports the completed asset activities for any protection type.

The **Assets | Summary** widget is divided into two panes:

- The top portion of the left pane displays the total number of virtual machine assets. The bottom portion displays the number of assets that had recent successful backup and replication activities within the configured time range.
- The top portion of the right pane displays the total number of other assets. The bottom portion displays the number of assets that had recent successful backup and replication activities within the configured time range.

Click **View All** to view all assets on the **Asset Inventory** page.

Assets Top Offenders widget

The **Assets | Top Offenders** widget lists the total number of assets with three or more consecutive backup or replication failures.

This widget lists the top three systems using the with the most consecutive failures. The widget lists the following information for each of these systems:

- The system name.
- A bar representing the number of failed and successful activities.

This widget also lists the following information for the top three systems with the most failures:

- The name of the system.
- The date of the most recent failed activity.
- The number of consecutive failures.

The **Assets | Top Offenders** widget lists the total number of assets with three or more consecutive backup or replication failures.

Click **View All** to visit the **Asset Inventory** page.

Click an asset in the list to view the **Asset Activities** page filtered by that asset.

Alerts Summary widget

The **Alerts | Summary** widget shows a summary of active alerts for systems configured in IDPA System Manager.

The **Alerts | Summary** widget lists the following summary information:

- Number of error alerts
- Number of warn alerts
- Number of info alerts

The **Alerts | Summary** widget also lists the three most recent alerts.

Click **View All** to visit the **Alerts** page.

Storage Capacity Top Utilization widget

The **Storage Capacity | Top Utilization** widget shows a summary of the systems using the most storage.

The **Storage Capacity | Top Utilization** widget lists the top three systems using the highest percentage of their capacity. The widget lists the following information for each of these systems:

- The system name.
- A bar representing the storage usage.
- The percentage of available storage used.
- The amount of storage used and the amount of storage available.

The **Exceeded Threshold** count shows the total number of systems exceeding 80% or more of their storage capacity.

Click **View All** to visit the **Capacity** page.

Storage capacity summary widget

The **Storage Capacity | Summary** widget shows a summary of the storage capacity usage for Data Domain and Avamar systems configured in IDPA System Manager.

The **Storage Capacity | Summary** widget lists the following information:

- **Used:** Amount of storage used.
- **Available:** Amount of storage available.
- **Total:** Total amount of storage, including both used and available.

The **Storage Capacity | Summary** widget also shows a capacity bar that represents the total storage usage.

Click **View All** to visit the **Capacity** page.

Health summary widget

The **Health | Summary** widget shows a health status summary of systems configured in IDPA System Manager.

The **Health | Summary** widget lists the following summary information:

- Number of systems that are not reporting
- Number of unhealthy systems
- Number of healthy systems

The **Health | Summary** widget also lists the three most unhealthy systems with a health bar that compares the number of healthy and unhealthy key performance indicators (KPIs).

Click **View All** to visit the **Health** page.

Drill down pages

Drill down pages cover a specific area of interest, for example, alerts, capacity, health, and activities.

To access a specific drill down page, click inside a dashboard widget. The drill down page is filtered by the widget settings. Each drill down page Master pane displays information in a table. You can view additional information about a specific row in a table in the Detail pane that appears on the right side of the user interface. In the Detail pane, you may be able to perform additional actions.

Managing dashboards

Each user can have up to 20 dashboards in IDPA System Manager.

Add a dashboard

IDPA System Manager provides the capability for you to add a dashboard.

Procedure

1. In the **Dashboard**, click:



The **Add Dashboard** dialog box appears.

2. Type a name for the dashboard.
3. (Optional) To set this dashboard as the default dashboard, select **Set as default dashboard**.
4. Click **ADD DASHBOARD**.

Editing a dashboard

IDPA System Manager provides the capability for you to edit a dashboard.


To accomplish the following tasks, edit a dashboard:

- Rename a dashboard.
- Set a dashboard to be the default dashboard.
- Reset widgets to the default settings.

Rename a dashboard

You can specify a new name for a dashboard.

Procedure

1. Select the dashboard that you want to rename.
2. Click .


The **Edit Dashboard** dialog box appears.

3. In the **Dashboard Name** field, type a new name.
4. Click **SAVE**.

Set a dashboard to be the default dashboard

To set a dashboard to be the initial dashboard that is displayed when you log in to IDPA System Manager, set the dashboard to be the default dashboard.


Procedure

1. Select the dashboard that you want to be the default dashboard.
2. Click  .
The **Edit Dashboard** dialog box appears.
3. Select **Set as default dashboard**.
4. Click **SAVE**.

Reset dashboard widgets to default settings

Resetting widgets eliminates any filtering selections and reverts the widget to the default setting.

Procedure


1. Select the dashboard that you want to edit.
2. Click  .
The **Edit Dashboard** dialog box appears.
3. Select **Reset widgets back to defaults**.
4. Click **SAVE**.

The dashboard is reset to the default settings.

Delete a dashboard

If a dashboard is no longer required, you can delete the dashboard.

About this task

 **Note:** You cannot delete a dashboard that has been set as the default dashboard. However, you can set another dashboard to be the default dashboard, and then return to the former default dashboard and delete it.

Procedure

1. Open the dashboard that you want to delete, and then click:



A dialog box appears and displays the following message:

Are you sure you want to delete "<dashboard_name>" dashboard?

2. Click **DELETE**.

The dashboard is deleted and the default dashboard is displayed.

Editing widgets

To customize the dashboard, you can edit and filter widgets to show the information you want.

Change the widget type

Change widget types to customize or rearrange the dashboard.

Procedure

1. In the upper right corner of the widget, click the overflow button:



2. Select **Widget Type**.

A menu appears that displays all of the available widget type options.

3. Select one of the following widget types:

- **Assets | Backups & Replications**
- **Assets | Backups & Replications Trend**
- **Alerts | Summary**
- **Assets | Top Offenders**
- **Assets | Summary**
- **Jobs | Backups & Replications**
- **Jobs | Backups & Replications Trend**
- **Health | Summary**
- **Storage Capacity | Summary**
- **Storage Capacity | Top Utilization**

Results

The widget changes to the new type.

Edit the reporting time range

About this task

Note: The reporting period data only reflects the data that exists in IDPA System Manager. Any alerts or activities that occurred before the system was added to IDPA System Manager do not appear.

Procedure

1. In the upper right corner of the widget, click the overflow button:



2. Select **Time Range**.

A menu appears that displays all of the available reporting period options.

3. Select one of the following reporting period options:

- **Last Hour**

- **Last 24 Hours**
- **Last 7 Days**
- **All Available**

Results

The widget updates with the new reporting period setting.

Edit the activity view

Certain widgets enable you to change the activity view being reported to either jobs or assets.

About this task

You can change the activity view for the following widgets:

- Activity Counts
- Activity Trends

Procedure

1. In the upper right corner of the widget, click the overflow button:



2. Select **View**.

A menu appears that displays all of the available activity level view options.

3. Select one of the following activity level options:

- **Assets**
- **Jobs**

Results

The widget updates with the new activity view setting.

Edit the activity type

Certain widgets enable you to change the activity type being reported to either backups or replications.

About this task

You can change the activity type for the following widgets:

- Activity Counts
- Activity Trends

Procedure

1. In the upper right corner of the widget, click the overflow button:



2. Select **Activity Type**.

A menu appears that displays all of the available activity type options.

3. Select one of the following activity type options:

- **Backups**

- Replications
- Backups & Replications

Results

The widget updates with the new activity type setting.

Refresh the dashboard

About this task

To manually refresh the dashboard, click the  button.

Filter systems or assets in a dashboard widget

The default widget scope setting is to display information for all systems and assets. To reduce the scope to a system, system group, or asset tag level, perform the following procedure.

Procedure

1. In the upper right corner of the widget, click the overflow button:



2. Select **Filter**.

The **Widget Filter** dialog box appears.

3. To add systems, system groups, or asset tags to the filter, perform the following steps:
 - a. Select one or more options on the **Available** pane.
To narrow the amount of options listed in the **Available** pane, use the search bar.
 - b. Click:



The groups or systems are added to the filter.

4. To remove groups or systems from the filter, perform one of the following action sequences:
 - To clear all groups or systems from the filter, click:



- To remove certain groups or systems from the filter, perform the following steps:
 - Select one or more groups or systems in the **Filtered By** pane.
 - Click:



The groups or systems are removed from the filter

5. Click **APPLY**.

The widget refreshes and displays only information for the selected systems, system groups, or asset tags.

CHAPTER 3

Monitoring System Health

Learn how to monitor system health in IDPA System Manager.

This chapter contains the following sections:

- [Monitoring health status](#)..... 32
- [Managing alerts](#)..... 35
- [Monitoring system capacity](#)..... 37

Monitoring health status

To view the health status of systems that are configured in IDPA System Manager, visit the **Health** page.

The **Health** page lists all of the systems in a table with basic health summary information.

To view additional details about the health of a system, select a system in the table. The additional information for the selected system appears in the Detail pane.

Reading the Health page

The table on the **Health** page lists the following basic system health status information.

System Name

The name that was specified to identify the system when it was added to IDPA System Manager.

Version

The system version.

Health

A status that indicates the health of the system in IDPA System Manager. The status types that can be displayed are as follows:

- **Good:** IDPA System Manager tracks criteria to determine the health of each system. [Criteria that determine system health status](#) on page 32 provides the criteria used for each type of system.
- **NotReporting:** A system health status is updated to **NotReporting** when IDPA System Manager cannot communicate with the system.
- **Unhealthy:** If any of the criteria that are used to determine the health of a system are not successful, the system health status is updated to **Unhealthy**.

Criteria that determine system health status

IDPA System Manager tracks criteria to determine the health of each system.

Avamar health status criteria

If an Avamar system meets the following criteria the health status for the system is updated to **Good**:

- The communication between IDPA System Manager and the Avamar system is active and the Avamar system is able to report information to IDPA System Manager.
- The system is able to report activities information to IDPA System Manager.
- The capacity of the storage system is less than or equal to 80%.
- The system has no errors or warning alerts.
- A successful garbage collection for the system has occurred in the last 24 hours.
- A successful checkpoint was taken in the last 24 hours.
- A successful HFS checkpoint validation has occurred in the last 24 hours.
- The license for the system is valid.
- The SSO connection status is good.
- The system information configured on the **System Management** page is completed with all of the required connection details.

Data Domain health status criteria

If a Data Domain system meets the following criteria the health status for the system is updated to **Good**:

- The communication between IDPA System Manager and the Data Domain system is active and the Data Domain system is able to report information to IDPA System Manager.
- The capacity of the storage system is less than or equal to 80%.
- The system has no errors or warning alerts.
- The system information configured on the **System Management** page is completed with all of the required connection details.

Reading the detailed health summary pane

To view more detailed health information for a system, select the system in the **Health** table. The Detail pane lists detailed health summary information for the system.

Avamar health information on the Detail pane

Select a row in the **Master** pane to display additional information about the health of a system. The following information is listed in the **Detail** pane for Avamar system health.

Health Summary

A summary checklist of the components that are used to determine the health of the Avamar system in IDPA System Manager. Above the checklist, the **Last Update** field lists the date and time of the most recent communication with the Avamar system. The components include:

- Reporting
If the Reporting component shows an X, to reactivate reporting, click **Reporting**, and then click **REACTIVATE**.
- Capacity
- Alerts
- Garbage Collection
- Checkpoint
- Checkpoint Validation
- License
- SSO

Note: The SSO health status reflects the IDPA System Manager SSO connection status rather than the status of the remote system. Therefore, the SSO health may be reported as healthy when the monitored system is out of sync.

The *IDPA System Manager Security Configuration Guide* provides information on which versions of Avamar are supported with SSO.

If the SSO component is broken, to reregister single sign on, click **SSO** and then click **REREGISTER**.

- Connection Information

A check mark represents success. An X represents failure.

Click a component for more information about the status.

Capacity

A summary of the storage availability and usage, including the following components:

- **Used:** The amount of storage that is used, shown in GB and as a percentage.
- **Available:** The amount of storage that is available in GB.
- **Total Capacity:** The total amount of used and available storage.

System Details

A summary of the following information:

- **Last Garbage Collection:** Reports whether garbage collection was successful in the last 24 hours.
- **Last HFS Checkpoint:** Reports whether there was an HFS checkpoint in the last 24 hours.
- **Last HFS Checkpoint Validation:** Reports whether HFS checkpoint validation occurred in the last 24 hours.

License Information

A summary of the licensing information, including the following components:

- **License Status:** Reports whether the license status is valid or invalid.
- **License Expiration:** Reports when the license expires.

Data Domain health information on the Detail pane

Select a row in the **Master** pane to display additional information about the health of a system.

The following information is listed in the **Detail** pane for Data Domain system health.

Health Summary

A summary checklist of the components that are used to determine the health of the system in IDPA System Manager. Above the checklist, the **Last Update** field lists the date and time of the most recent communication with the Data Domain system. The components include:

- Reporting
- Capacity
- Alerts
- Connection Information

Storage

A summary of the storage availability and usage, including the following components:

- **Used:** The amount of storage that is used, shown in GB and as a percentage.
- **Available:** The amount of storage that is available in GB.
- **Total Capacity:** The total amount of used and available storage.

Data Protection Advisor and Search system health information

IDPA System Manager does not collect health attribute information or generate a health status for Search and Data Protection Advisor systems.

As a result, IDPA System Manager reports Search and Data Protection Advisor system health status as **None**.

The system version for Search and Data Protection Advisor is retrieved only when you add the systems to IDPA System Manager. If you upgrade either software, IDPA System Manager does not

update the version number. As a workaround, to update the version number displayed in IDPA System Manager, edit the Search or Data Protection Advisor system on the **System Management** page.

Managing alerts

To view and manage alerts for IDPA System Manager and all systems, visit the **Alerts** page.

To update the alerts table, click **Refresh**.

Note: Alerts that have been acknowledged in a system management console, such as Avamar Administrator or Data Domain Management Console, are removed from IDPA System Manager.

Reading alerts

Alerts are listed in a table on the **Alerts** page.

The following information is listed for each alert.

System Name

The name that was specified when the system was added to IDPA System Manager.

Level

The type of alert in IDPA System Manager. The level types that can be displayed are as follows:

- Error
- Warn
- Informational

To learn how IDPA System Manager maps alert levels from different systems, refer to [Mapping system alert levels](#) on page 35.

Category

The category of the alert.

Created Date

The date on which the alert was created.

Message

A description for the alert.

Mapping system alert levels

IDPA System Manager maps alerts from systems to three alert levels: Error, Warning, or Informational.

Mapping Avamar alert levels to IDPA System Manager

The following table shows what level Avamar alerts are reported as in IDPA System Manager.

Table 5 Avamar alert levels in IDPA System Manager

Avamar alert level	IDPA System Manager alert level
Warning	Error

Table 5 Avamar alert levels in IDPA System Manager (continued)

Avamar alert level	IDPA System Manager alert level
Error	Error

Mapping Data Domain alert levels to IDPA System Manager

The following table shows what level Data Domain alerts are reported as in IDPA System Manager.


Table 6 Data Domain alert levels in IDPA System Manager

Data Domain alert level	IDPA System Manager alert level
Alert	Error
Critical	Error
Emergency	Error
Error	Error
Warning	Warn
Debug	Informational
Info	Informational
Notice	Informational

Dismissing alerts

Dismiss health alerts to clear the alerts from IDPA System Manager and change the system **Alerts** health component status to **Good**.

Dismissing alerts will only remove the alerts from being displayed in IDPA System Manager and does not acknowledge or remove the alerts from the monitored systems. If the underlying issue still exists on the monitored system, the alert may reappear in IDPA System Manager.

 **Note:** Fixing the underlying issue or acknowledging the alerts on the monitored system will remove the alert from IDPA System Manager.

Dismiss alerts

Procedure

1. In the **Left** menu, select **Alerts**.
2. Select the alerts that you want to dismiss:
 - To dismiss individual alerts, click the box beside one or more alerts.
 - To dismiss all alerts, click the box in the header row.
3. Click **DISMISS**.

Results

The selected alerts are removed from IDPA System Manager. A **Dismiss alerts** action appears on the **Audit** page.

Monitoring system capacity

To view the capacity state of all Avamar and Data Domain systems that are configured in IDPA System Manager, visit the **Capacity** page.

Capacity monitoring can keep you aware of unexpected data growth that may cause downstream failures.

To view additional information about a system, select a system in the **Capacity** table. The additional information for the selected system appears in the **Detail** pane.

Reading the system capacity table

The table on the **Capacity** page lists the following basic system capacity information.

System Name

A name that was manually specified to help identify the system.

Utilization

The percentage of the system storage that is used.

Usage

The amount of the storage that is used.

Available

The amount of storage that is available.

Total Capacity

The total amount of storage.

Reading the detailed system capacity pane

To view more detailed capacity information for a system, select the system in the **Capacity** table. The Detail pane lists detailed capacity information for the system.

Avamar detailed capacity pane

When you select an Avamar system on the **Capacity** page, the Detail pane lists the following Avamar system capacity information.

Health Summary

Displays the last date and time the database was updated or displays **Not Reporting** if the system is not reporting. Note that capacity data might be outdated if the system is in the **Not Reporting** state.

Capacity

A summary of the capacity usage, including the following components:

- **Used:** The amount of the storage that is used and the percentage of storage used.
- **Available:** The amount of storage that is available.
- **Total Capacity:** The total amount of used and available storage.
- **Metadata Used:** The percentage of the storage that is used for metadata.

Forecast

The forecasted number of days until the system storage becomes full.

Data Domain detailed capacity pane

When you select a Data Domain system on the **Capacity** page, the Detail pane lists the following Data Domain system capacity information.

Health Summary

Displays the last date and time the database was updated or displays **Not Reporting** if the system is not reporting. Note that capacity data might be outdated if the system is in the **Not Reporting** state.

Capacity

A summary of the capacity usage, including the following components:

- **Usage:** The amount of the storage that is used.
- **Available:** The amount of storage that is available.
- **Total Capacity:** The total amount of used and available storage.

MTrees

The status and usage of each MTree. The following components are reported for each MTree in the Data Domain system:

- The name of the MTree.
- **Usage:** The amount of storage that is used on the MTree.
- **Status:** The status of the MTree.

CHAPTER 4

Monitoring Activities

This chapter contains the following sections:

- [Activities overview](#) 40
- [Monitoring job activities](#) 40
- [Monitoring asset activities](#) 42

Activities overview

IDPA System Manager Activities include system activities at the job and asset level.

System activity includes information about backup and replication activities for Avamar systems connected to IDPA System Manager.

Monitoring job activities

To monitor backup and replication activities at the job level from all systems, visit the **Job Activities** page.

By default, the Master pane on the **Job Activities** page displays activities that started in the last 24 hours. Use the filter icon in the **Started** column to filter for jobs, as required. To view additional information about an activity, select the activity from the table on the Master pane. Additional details for the activity appears in the Detail pane.

For Avamar systems, you can view a list of clients that are associated with any activity.

For Avamar systems only, you can rerun backup and replication jobs.

Reading the Job Activities page

The table on the **Job Activities** page lists basic job information.

The following information is listed on the **Job Activities** page.

Activity Name

The name of the policy that the activity is associated with.

Type

The type of activity. The activity types that can be displayed are as follows:

- Backup
- Replication

Status

The status of the activity. The statuses that can be displayed are as follows:

- Pending
- Completed
- Failed
- Completed with exceptions
- Running

System Name

The name that is defined in IDPA System Manager.

Started

The date and time that the activity started.

Reading the detailed job activity pane

To view more detailed information about a job, select the job in the **Job Activities** table. The Detail pane lists detailed information for the job activity.

Avamar activity information on the Detail pane

Select a row in the **Master** pane to display additional information about an activity. The following information is listed in the **Detail** pane table for Avamar system activities.

Status

The activity status information. The following components are reported:

- **Activity Name:** The name of the activity.
- **System Name:** The name of the system.
- **System Type:** The type of system.
- **Policy Type:** The type of policy.

Asset Activities

A summary of asset information. The following components are reported:

- **Completed:** The number of assets that completed.
- **Failed:** The number of assets that failed.
- **With Exceptions:** The number of assets that have exceptions.
- **Running:** The number of assets that are actively running.
- **Pending:** The number of assets that have a status of pending.
- **Total:** The total number of assets that are associated with the activity.

Target

A summary of the target information for the activity. The following components are reported:

- **Type:** The storage target type for the activity.
For backups, the target type is either Avamar or Data Domain.
For replication, the target type is Avamar replication.
- **Hostname:** The storage target hostname where the backup is stored.
This column is reported for backup activities only.
- **Total Size:** The total size of all of the assets within the job.

Time

A summary of the time information for the activity. The following components are reported:

- **Started:** The date and time that the activity started.
- **Ended:** The date and time that the activity ended.
- **Duration:** The length of time the activity took to complete.

Rerun an Avamar job activity

IDPA System Manager provides the capability for you to rerun an Avamar activity from the **Job Activities** page.

About this task

You can rerun a failed activity from the top of the Detail pane by clicking **Rerun Activity**. To rerun any activity, including successful activities, perform the following procedure.

Procedure

1. In the **Left** menu, select **Job Activities**.
2. On the **Master** pane, select the row for the Avamar activity that you want to rerun.
3. Click the overflow menu:




4. Click **Rerun Activity**.

The activity runs and is added to a new row in the table.

View job activities for a specific system

Learn how to view job activities for a specific system.

Procedure

1. From the left menu, click **System Management**.
The **System Management** page appears.
2. In the row for the system, click the Overflow menu ().
3. Click **View Job Activities**.

Results

The **Job Activities** page appears, listing only the activities for the selected system.

Monitoring asset activities

To monitor backup and replication activities at the asset level from all systems, visit the **Asset Activities** page.

By default, the Master pane on the **Asset Activities** page displays activities that started in the last 24 hours. Use the filter icon in the Started column to filter the activities, as required.

To view additional information about an activity, select the activity from the table on the Master pane. Additional details for the activity appears in the Detail pane.

Reading the Asset Activities page

The table on the **Asset Activities** page lists basic job information.

The following information is listed on the **Asset Activities** page.

Asset Name

The name of the asset.

Type

The type of activity.

For Avamar, IDPA System Manager reports backup and replication activities.

Status

The status of the activity. The statuses that can be displayed are as follows:

- Pending
- Completed
- Failed
- Completed with exceptions
- Running

Protection Type

The type of plugin that the asset is associated with.

Started

The date and time that the activity started.

Reading the detailed asset activity pane

To view more detailed asset activity information, select the activity in the **Asset Activities** table. The Detail pane lists detailed information for the asset activity.

Avamar asset activity information on the Detail pane

Select an activity on the **Asset Activities** page to view more details in the Detail pane.

The Detail pane lists the following information for Avamar asset activities:

Status

The status of the activity.

If the status is failed, to run the activity for the asset only, click **RERUN ACTIVITY**.

Status Message

The error message or code for the failure, if applicable.

This field appears only when the activity failed and an error message is available.

Activity Name

The name of the job activity that the asset activity is part of.

System Name

The name of the system that protects the asset.

System Type

The type of protection system.

Policy Type

The type of policy.

Time

A summary of the time information for the activity. The following components are reported:

- **Started:** The date and time that the activity started.

- **Ended:** The date and time that the activity ended.

Details

Additional details for the asset activity. The following components are reported:

- **Backup Label:** The Avamar backup label.
- **Backup Number:** The Avamar backup sequence number.
- **Bytes Modified:** The number of modified bytes in the activity.
- **Bytes Processed:** The number of bytes processed during the activity.
- **Bytes Modified Sent:** The number of bytes modified that are sent to storage during the backup or replication activity.
- **Expiration:** The expiration date for the backup.


Rerun an Avamar asset activity

When an Avamar backup or replication activity fails for an asset, IDPA System Manager provides the capability for you to rerun the activity at the asset level.

About this task

You can rerun a failed activity from the top of the Detail pane by clicking **Rerun Activity**. To rerun any activity, including successful activities, perform the following procedure.

Procedure


1. From the left menu, select **Asset Activities**.
2. On the **Asset Activities** page, select the row for the Avamar activity that you want to rerun.
3. Click , and then click **Rerun Asset Activity**.

The activity runs for the asset and is added to a new row in the table.

View asset activities for a specific system

Learn how to view asset activities for a specific system.

Procedure

1. From the left menu, click **System Management**.
The **System Management** page appears.
2. In the row for the system, click the Overflow menu ().
3. Click **View Asset Activities**.

Results

The **Asset Activities** page appears, listing only the activities for the selected system.

View activities for a specific asset

Learn how to view activities for a specific asset.

Procedure

1. From the left menu, click **Asset Inventory**.

The **Asset Inventory** page appears.

2. Select the asset that you want to view activities for.
3. In the Detail pane, click **VIEW ACTIVITIES**.

Results

The **Asset Activities** page appears, listing only the activities for the selected asset.

View asset activities within a job

Learn how to view activities within a job at the asset level.

Procedure

1. From the left menu, click **Job Activities**.
The **Job Activities** page appears.
2. Select the job that you want to view asset activities for.
3. In the Detail pane, beside **Asset Activities**, click **VIEW**.

Results

The **Asset Activities** page appears, listing only the asset activities within the job.

CHAPTER 5

Managing Systems

Learn about managing systems and groups in IDPA System Manager.

This chapter contains the following sections:

• System management overview	48
• Adding a system	48
• Edit a system	51
• Delete a system	51
• Managing system groups	52

System management overview


The **System Management** page provides the capability for you to add, edit, remove, and manage systems and groups in IDPA System Manager.

The following list includes the system management capabilities that are available in IDPA System Manager:

- Add, edit, and delete Avamar, Data Domain, Data Protection Advisor, and Search systems.
- Organize systems into groups, including the ability to add, edit, and delete groups.
- View system information.
- Launch the native management application for the system.
- For Avamar systems:
 - View, add, edit, and delete policies, retentions, schedules, and datasets.
 - Add clients and proxies to policies.
 - Perform a backup of a policy.
- When an Avamar system is not reporting, you can reactivate messaging.

Adding a system

Learn how to add a system to IDPA System Manager.

 **Note:** You can configure only one Search and Data Protection Advisor system with IDPA System Manager at a time.

Add an Avamar system

To use IDPA System Manager to monitor and manage Avamar systems, add one or more Avamar systems.

Procedure


1. In the **Left** menu, select **System Management**.

2. Click .

The **Add System** window appears.

3. On the **Select System Type** page, select **Avamar**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that helps identify the system.
 - **Hostname:** Specify the fully qualified domain name (FQDN) of the Avamar system.
 - **Avamar Username:** Specify the username of the Avamar system. For Avamar Administrator, the username is MCUser.
 - **Avamar Password:** Specify the password for the Avamar system user interface.
 - **OS Root password:** Specify the OS root password.
5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:

- **Port:** Specify the Avamar MCS port. The default value is 9443. To specify the default value, leave this field blank.

 **Note:** When you add a system to IDPA System Manager that uses a non-standard port, you must modify the IDPA System Manager firewall to allow communication with that port. The *IDPA System Manager Security Configuration Guide* provides instructions.

- **Override MCGUI URL:** Specify an alternate URL destination for the **AVAMAR ADMINISTRATOR** button.
To override the **AVAMAR ADMINISTRATOR** link to direct to the AUI, type `https://<avamar_fqdn>/aui`.


6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the exact certificate on the Avamar system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.

IDPA System Manager does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system's certificate changes, IDPA System Manager will refuse to connect with the system.

In this scenario, edit the system on the IDPA System Manager **System Management** page to verify the new certificate details.

Add a Data Domain System

Procedure

1. In the **Left** menu, select **System Management**.
2. Click .
The **Add System** window appears.
3. On the **Select System Type** page, select **Data Domain**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that helps identify the system.
 - **Hostname:** Specify the Fully Qualified Domain Name (FQDN) of the Data Domain system.
 - **Username:** Specify the Data Domain administrator username.
 - **Password:** Specify the Data Domain administrator password.
5. Click **Next**.
6. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the Data Domain system.
7. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.


IDPA System Manager does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system's certificate changes, IDPA System Manager will refuse to connect with the system.

In this scenario, edit the system on the IDPA System Manager **System Management** page to verify the new certificate details.


Add a Data Protection Advisor system

To use the IDPA System Manager reporting features, you must add a Data Protection Advisor system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Click .

The **Add System** dialog box appears.
3. On the **Select System Type** page, select **Data Protection Advisor**, and then click **Next**.
4. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that helps identify the system.
 - **Hostname:** Specify the fully qualified domain name (FQDN) of the Data Protection Advisor system.
 - **Username:** Specify the Data Protection Advisor Administrator username.
 - **Password:** Specify the Data Protection Advisor Administrator password.
5. (Optional) To specify a non-default Data Protection Advisor port number, click **Show optional fields**, and then type the port number in the **Port** field.

 **Note:** When you add a system to IDPA System Manager that uses a non-standard port, you must modify the IDPA System Manager firewall to allow communication with that port. The *IDPA System Manager Security Configuration Guide* provides instructions.

6. Click **Next**.
7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the Data Protection Advisor system.
8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.


IDPA System Manager does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system's certificate changes, IDPA System Manager will refuse to connect with the system.

In this scenario, edit the system on the IDPA System Manager **System Management** page to verify the new certificate details.

Add a Search system

To perform advanced search and recover operations, you must add a Search system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Click .

The **Add System** window appears.

3. On the **Select System Type** page, select **Data Protection Search**, and then click **Next**.
 4. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that helps identify the Search system.
 - **Hostname:** Specify the fully qualified domain name (FQDN) of the Search system.
 - **Username:** Specify the Search Administrator username.
 - **Password:** Specify the Search Administrator password.
 5. (Optional) To specify optional fields, click **Show optional fields**, and then specify the following information, as required:
 - **Admin Rest API Port:** Specify the Search REST API port. The default value is 448.
 - **Search UI Port:** Specify the Search UI port. The default value is 443.
- Note:** When you add a system to IDPA System Manager that uses a non-standard port, you must modify the IDPA System Manager firewall to allow communication with that port. The *IDPA System Manager Security Configuration Guide* provides instructions.
6. Click **Next**.
 7. On the **Certificate Verification** page, to ensure that you are adding the correct system, verify that the certificate information being displayed matches the certificate on the Search system.
 8. Once you have confirmed that the certificate information is correct, select **Accept Certificate**, and then click **SAVE**.


IDPA System Manager does not validate the certificate and uses the certificate that you verify to connect with the system. If the remote system's certificate changes, IDPA System Manager will refuse to connect with the system.

In this scenario, edit the system on the IDPA System Manager **System Management** page to verify the new certificate details.

Edit a system

After a system is added, you can edit the system details.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the system that you want to edit.
3. Click .

The **Edit System** dialog box appears.
4. Edit the details for the selected system.
5. Click **SAVE**.

Delete a system

If a system is no longer required, you can delete the system.

Procedure

1. In the **Left** menu, select **System Management**.

2. Select the system that you want to delete.
If required, you can select multiple systems.

3. Click .

The **Confirm Delete** dialog box appears.

4. Click **DELETE**.
The system is removed.

After you delete a system, a deactivation activity message appears on the **Audit** page.

Managing system groups

IDPA System Manager includes capabilities to organize systems into groups.

You can use groups in IDPA System Manager filters.

After a group is created, you can edit the group. When a group is no longer required, you can delete the group.

Add a group

To organize systems, you can use groups.

Procedure

1. In the **Left** menu, select **System Management**.
2. Click **GROUPS**.

The **GROUPS** page appears.

3. Click .

The **Add Group** dialog box appears.

4. In the **Group Name** field, type a name for the group.
5. To add systems to the group, perform the following steps:

- a. Select one or more systems in the **Available** pane.

To narrow the amount of group or systems listed in the **Available** pane, use the search bar.

- b. Click:



The systems are added to the group.

6. To remove systems from the group, perform one of the following action sequences:

- To clear all systems from the group, click:



- To remove certain systems from the group, perform the following steps:

- Select one or more systems in the **Selected** pane.
- Click:



The systems are removed from the group.

7. Click **SAVE**.

Edit a group

If changes are required to a group, you can edit the group.

Procedure

1. In the **Left** menu, select **System Management**.
2. Click **GROUPS**.

The **GROUPS** page appears.

3. Select the group that you want to edit.

- 4.



The **Edit Group** window appears.

5. (Optional) Edit the **Group Name**.
6. To add systems to the group, perform the following steps:
 - a. Select one or more systems in the **Available** pane.

To narrow the amount of systems listed in the **Available** pane, use the search bar.

- b. Click:



The systems are added to the group.

7. To remove systems from the group, perform one of the following action sequences:
 - To clear all systems from the group, click:



- To remove certain systems from the group, perform the following steps:

- Select one or more systems in the **Selected** pane.
- Click:



The systems are removed from the group.

8. Click **SAVE**.

Delete a group

If a group is no longer required, you can delete the group.

Procedure

1. In the **Left** menu, select **System Management**.
2. Click **GROUPS**.

The **GROUPS** page appears.

3. Select the group that you want to delete.

- 4.

Click 

The **Confirm Delete** dialog box appears.

5. Click **DELETE**.

CHAPTER 6

Monitoring Assets

This chapter contains the following sections:

- [Assets overview](#) 56
- [Monitoring assets](#) 56
- [View assets for a specific system](#) 57
- [Tag assets](#) 58
- [Filter assets](#) 58

Assets overview

View and manage protected assets on the **Asset Inventory** page.

Assets are resources that are configured in an Avamar system. IDPA System Manager discovers assets when you add an Avamar system.

The following list describes the different types of assets that IDPA System Manager monitors:

- Hosts with a backup agent installed, including application, database, and file system agents.
- Hosts with Network Data Management Protocol (NDMP) data module installed.
- Hosts that are located on a virtual machine protected by VM image backups.

Monitoring assets

To view the discovered assets, visit the **Asset Inventory** page.

The **Asset Inventory** page lists all of the system assets in a table with basic summary information. To view additional details, select an asset in the table. The additional information for the selected asset appears in the Detail pane.

Reading the Assets Inventory page

The table on the **Asset Inventory** page lists the following basic asset information.

Name

The name of the asset.

System Name

The name of the system that protects the asset.

Type

The type of asset. There are two asset types that IDPA System Manager displays:

- **Virtual Machine:** An asset that is hosted on a virtual machine.
- **Other:** Any other type of asset, including filesystems, databases, and NDMP.

Last Backup

The timestamp of the most recent backup.

Recent Failures

The number of recent activities for the asset that failed. Once an activity successfully completes, this column is cleared.

Reading the detailed asset pane

To view more detailed information for an asset, select the asset in the **Asset Inventory** table. The Detail pane lists detailed information for the asset.

Avamar detailed asset pane

When you select an Avamar asset on the **Asset Inventory** page, the Detail pane lists the following Avamar asset information.

System Name

The name of system that protects the asset.

System Type

The type of system that protects the asset.

OS

The operating system that is installed on the asset.

Agent Version

The version of the agent on the asset. This field appears only for non-virtual machine type assets.

Domain

The domain that the asset is part of.

Recent Failures

The number of recent failures of backup or replication activities for the asset.

Under **Recent Failures**, the **Last Failure** component lists the date of the most recent failed activity.

The **Recent Failures** and **Last Failure** components are only listed when there are recent failures.

Tags

The tags that are applied to the asset.

Plugins


The plugins that are installed on the asset. The following information is reported:

- **Last Backup:** The date and time of the most recent backup.
- **Protected By:** The name of the policy that backs up the asset.
- **Last Replication:** The date and time of the most recent replication.
- **Replicated By:** The name of the policy that replicates the asset.

View assets for a specific system

Learn how to view asset activities for a specific system.

Procedure

1. From the left menu, click **System Management**.
The **System Management** page appears.
2. In the row for the system, click the Overflow menu ().
3. Click **View Assets**.

Results

The **Asset Inventory** page appears, listing only the assets for the selected system.

Tag assets

Add asset tags to organize assets and enable custom filtering.

Procedure

1. From the left menu, click **Asset Inventory**.
The **Asset Inventory** page appears.
2. Select one or more assets that you want to tag.
To select all assets, click the checkbox in the table header.
The Detail pane lists the selected assets and the set of tags that are applied to the assets.
3. In the Detail pane, under **Tags**, type the tag name, and then press Enter.
The tag is added to all of the selected assets.
4. To delete a tag, click **X**.

Results

When you add an asset tag, the tag is added as an option to use in filtering information on certain pages and dashboard widgets.

Filter assets

Use the search bar on the **Asset Inventory** page to quickly filter assets.

Procedure

1. From the left menu, click **Asset Inventory**.
The **Asset Inventory** page appears.
2. In the search bar, type a search keyword.
Some types of keywords that you can use include a tag, asset name, system type, operating system, and Avamar plugin name.
The **Assets Inventory** page refreshes and lists only the assets that match the search keyword.
3. To clear the search filter, in the search bar, click **x**.

CHAPTER 7

Managing Avamar Protection Policies

This chapter contains the following sections:

- [Overview of Avamar policies](#)..... 60
- [Managing data protection policies for Avamar systems](#)..... 60
- [Run a backup policy](#)..... 66

Overview of Avamar policies

Policies in IDPA System Manager are rules for client backups that can be specified, named and then applied to one or more groups.

IDPA System Manager policies include information about all policies, not just policies that were initiated or configured in IDPA System Manager.

Policies include the following components:

- **Retentions**—Retentions in IDPA System Manager are the policies that define the amount of time in which a set of data remains available for restore. Retention is a persistent and reusable policy that can be named and attached to multiple groups.
- **Schedules**—Schedules in IDPA System Manager provide the ability to control the frequency and the start and end time of backups of clients in a group. A schedule is a persistent and reusable policy that can be named and attached to multiple groups.
- **Datasets**—Datasets in IDPA System Manager are a policy that define a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable policy that can be named and attached to multiple groups.

Managing data protection policies for Avamar systems


For Avamar systems, IDPA System Manager provides the capability for you to view, add, edit, and delete data protection policies.

You can also start an immediate backup using a policy.

View policies

IDPA System Manager provides the capability for you to view policies for an Avamar system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3.  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab where a list of policies for the selected Avamar system are displayed.


Adding an Avamar policy

Learn how to add an Avamar backup policy with IDPA System Manager.

Add a backup policy

IDPA System Manager provides the capability for you to add a policy for an Avamar system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3.  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. (Optional) To change the domain where the policy will be created, select a different domain from the **Domain** drop-down list.

When you add a policy, the policy is created in the domain selected in the **Domain** drop-down list. By default, the root "/" directory is selected as the **Domain**.

5. Click **ADD**.

The **Add Policy** dialog box appears.

6. In the **Information** panel, specify information for the following fields, and then click **NEXT**:

- **Name**—You can specify any name that helps identify the policy.
- **Enabled**—Specify whether to enable the policy. The default is disabled.
- **Dataset**—The dataset that is to be associated with the policy.
- **Schedule**—The schedule that is to be associated with the policy.
- **Retention**—The retention that is to be associated with the policy.


In the **Add Policy** dialog box, the **Domain** field is read-only and maps to the domain specified on the **System Management > Manage Policies** page.

7. (Optional) In the **Clients** panel, select one or more clients to be associated with the policy.

To perform a search for clients and filter by the client domain and name, in the **Search for clients...** field, type search criteria.

8. Click **NEXT**.

9. (Optional) In the **Proxies** panel, select one or more proxies to be associated with the policy.

 **Note:** The **Auto Proxy Enabled** checkbox is automatically selected. When this checkbox is selected, all proxies are automatically added to policies.


10. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the policy was successfully added, and in the list of policies, the new policy is displayed.

Add a retention

IDPA System Manager provides the capability for you to add a retention for an Avamar system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3.  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **RETENTIONS** tab, click **RETENTIONS**.

5. (Optional) To change the domain where the retention will be created, select a different domain from the **Domain** drop-down list.

When you add a retention, the retention is created in the domain selected in the **Domain** drop-down list. By default, the root "/" directory is selected as the **Domain**.

6. Click **ADD**.

The **Add Retention** dialog box appears.

7. Specify the following information:

- **Name**—You can specify any name that helps identify the retention.
- **Expiration Type**

In the **Add Retention** dialog box, the **Domain** field is read-only and maps to the domain specified on the **System Management > Manage Policies** page.

If required, specify information for additional fields depending on the **Expiration Type**.

8. Click **FINISH**.


The page refreshes, a notification appears in the **Notification** bar that indicates the retention was successfully added, and in the list of retentions, the new retention is displayed.

Add a schedule

IDPA System Manager provides the capability for you to add a schedule for an Avamar system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.

3. Click , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **SCHEDULES** tab, click **SCHEDULES**.
5. (Optional) To change the domain where the schedule will be created, select a different domain from the **Domain** drop-down list.

When you add a schedule, the schedule is created in the domain selected in the **Domain** drop-down list. By default, the root "/" directory is selected as the **Domain**.

6. Click **ADD**.

The **Add Schedule** dialog box appears.

7. Specify the following fields:

- **Name**—You can specify any name that helps identify the schedule.
- **Type**

In the **Add Schedule** dialog box, the **Domain** field is read-only and maps to the domain specified on the **System Management > Manage Policies** page.

The **Timezone** field is read-only. The default for this field is the local time zone of the user.

If required, specify information for additional fields depending on the selected **Type**.

8. If you did not specify **On Demand** for the **Type** field, specify a date for the following fields:
 - **Delay Until**
 - **End After**


9. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the schedule was successfully added, and in the list of schedules, the new schedule is displayed.

Add a dataset

IDPA System Manager provides the capability for you to add a dataset for an Avamar system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3. Click  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **DATASETS** tab, click **DATASETS**.
5. (Optional) To change the domain where the dataset will be created, select a different domain from the **Domain** drop-down list.

When you add a dataset, the dataset is created in the domain selected in the **Domain** drop-down list. By default, the root "/" directory is selected as the **Domain**.

6. Click **ADD**.

The **Add Dataset** dialog box appears.

7. Specify a Name.

You can specify any name that helps identify the dataset.

In the **Add Dataset** dialog box, the **Domain** field is read-only and maps to the domain specified on the **System Management > Manage Policies** page.

8. Select a Plug-in type, and then select one of the following:

- **All**
- **Select Files and/or Folders**
For the selected Plug-in type, to add a specific file or folder, type the name of the file or folder, and then click **ADD**. After you click **ADD**, the specific file or folder is added to the **Plug-in** list.

9. From the **Plug-in** list, delete any plug-in entries that you do not want to be included.

The following is the default list of plug-in options:

- AIX File System
- FreeBSD File System
- HP-UX File System
- Linux File System
- Macintosh File System
- NetWare File System
- SCO OpenServer File System
- Solaris File System
- UnixWare File System
- Windows File System

To delete a Plug-in, in the **Remove Plug-In** column, click the **X** that is associated with the Plug-in that you want to delete.

10. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the dataset was successfully added, and in the list of datasets, the new dataset is displayed.


Editing an Avamar policy

Learn how to edit an Avamar backup policy with IDPA System Manager.


Edit a policy

IDPA System Manager provides the capability for you to edit a policy for an Avamar system.

About this task

 **Note:** You cannot edit Avamar reserved items. For Avamar reserved items, the **EDIT** button is disabled.

Procedure


1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3.  , and then click **Manage Policies**.
The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.
4. Select the policy that you want to edit, and then click **EDIT**.
The **Edit Policy** dialog box appears.
5. (Optional) In the **Information** panel, edit the fields.
6. Click **NEXT**.
7. (Optional) In the **Clients** panel, select, or clear the checkboxes for the available clients.
8. Click **NEXT**.
9. (Optional) In the **Proxies** panel, select, or clear the checkboxes for Auto Proxy Enabled and available proxies.
10. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the policy was successfully updated, and in the list of policies, the updated policy is displayed.


Edit a retention

IDPA System Manager provides the capability for you to edit a retention for an Avamar system.

About this task

 **Note:** You cannot edit Avamar reserved items. For Avamar reserved items, the **EDIT** button is disabled.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3.  , and then click **Manage Policies**.
The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **RETENTIONS** tab, click **RETENTIONS**.
5. From the list, select the retention that you want to edit.
6. Click **EDIT**.

The **Edit Retention** dialog box appears.

7. In the **Edit Retention** dialog box, edit the following:
 - Name
 - Expiration Type
 - Retention Period

If required, edit information for additional fields depending on the **Expiration Type**.


8. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the retention was successfully updated, and in the list of retentions, the updated retention is displayed.


Edit a schedule

IDPA System Manager provides the capability for you to edit a schedule for an Avamar system.

About this task

 **Note:** You cannot edit Avamar reserved items. For Avamar reserved items, the **EDIT** button is disabled.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3. Click  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **SCHEDULES** tab, click **SCHEDULES**.
5. From the list, select the schedule that you want to edit.
6. Click **EDIT**.

The **Edit Schedule** dialog box appears.


7. Edit the fields.
8. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the schedule was edited, and in the list of schedules, the updated schedule is displayed.


Edit a dataset

IDPA System Manager provides the capability for you to edit a dataset for an Avamar system.

About this task

 **Note:** You cannot edit Avamar reserved items. For Avamar reserved items, the **EDIT** button is disabled.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3. Click  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. To open the **DATASETS** tab, click **DATASETS**.
5. From the list, select the dataset that you want to edit.
6. Click **EDIT**.

The **Edit Dataset** dialog box appears.


7. Edit the fields.
8. Click **FINISH**.

The page refreshes, a notification appears in the **Notification** bar that indicates the dataset was successfully updated, and in the list of datasets, the updated dataset is displayed.


Delete a policy

IDPA System Manager provides the capability for you to delete a policy for an Avamar system.

About this task

 **Note:** You cannot delete Avamar reserved items. For Avamar reserved items, the **DELETE** button is disabled.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select an Avamar system.
3. Click  , and then click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

4. Select the policy that you want to delete, and then click **DELETE**.

The **Confirm Delete** dialog box appears.

5. Click **DELETE**.

The page refreshes, a notification appears in the **Notification** bar that indicates the policy was successfully deleted, and the policy is no longer displayed in the list of policies.

Run a backup policy

IDPA System Manager provides the capability for you to run a backup policy.

About this task

If the policy is enabled and has clients, the **BACKUP NOW** button is enabled, otherwise the button is disabled.

Procedure

1. In the **Left** menu, select **System Management**.

2. Select an Avamar system.
3. Click:



4. Click **Manage Policies**.

The **System Management > Manage Policies** page appears, open to the **POLICIES** tab.

5. Select a policy, and then click **BACKUP NOW**.

A message appears in the **Notification** bar that indicates the backup has started for the selected policy.

You can track the backup progress on the **Audit** page or the **Job Activities** page.

CHAPTER 8

Launching System Management Applications

IDPA System Manager allows you to launch native system management applications.

This chapter includes the following topics:

- [Launching Avamar Administrator](#) 70
- [Launching Avamar AUI](#) 71
- [Launching Data Domain System Manager](#) 72
- [Launching Search](#) 73
- [Launching Data Protection Advisor](#) 73

Launching Avamar Administrator

IDPA System Manager provides the capability for you to launch Avamar Administrator.

For instructions about how to use Avamar Administrator, refer to the Avamar documentation.

Launch Avamar Administrator from the overflow button

Before you begin

IDPA System Manager must be open to one of the following pages:

- **Health**
- **Alerts**
- **Capacity**
- **Job Activities**
- **Asset Activities**
- **Asset Inventory**
- **System Management**

Procedure

1. Click the overflow button beside the Avamar system:



2. Click **Avamar Administrator**.

A prompt appears to download a .jnlp file for Avamar Administrator. Based on the browser settings, you can either open or save the file.

3. Execute the .jnlp file to launch Avamar Administrator.

Due to system security settings, there may be security prompts when you execute the .jnlp file. Accept the security prompts to continue launching Avamar Administrator.

Results

Avamar Administrator launches.

Launch Avamar Administrator from the Detail pane

Before you begin

IDPA System Manager must be open to one of the following pages:

- **Health**
- **Capacity**
- **Job Activities**
- **Asset Activities**
- **Asset Inventory**

Procedure

1. Select the Avamar system from the list of systems on the **Master** pane.
2. In the **Detail** pane, click **AVAMAR ADMINISTRATOR**.

A prompt appears to download a .jnlp file for Avamar Administrator. Based on the browser settings, you can either open or save the file.

3. Execute the .jnlp file to launch Avamar Administrator.


Due to system security settings, there may be security prompts when you execute the .jnlp file. Accept the security prompts to continue launching Avamar Administrator.

Results

Avamar Administrator launches.

Launching Avamar AUI

IDPA System Manager provides the capability for you to launch Avamar AUI to either the **Avamar Restore** or **Avamar Proxy Deployment** pages.

 **Note:** To launch the AUI from IDPA System Manager, the Avamar system must be version 7.5.1 or later.

For instructions about how to use Avamar AUI, refer to the Avamar documentation.

Launch Avamar Restore from the overflow button

Before you begin

You can launch the AUI **Avamar Restore** page when IDPA System Manager is open to one of the following pages:

- **Asset Activities**
- **Job Activities**
- **Asset Inventory**
- **System Management**

Procedure

1. Click the overflow button beside the Avamar system:



2. Click **Avamar Restore**.

Results

The Avamar AUI launches to the **Avamar Restore** page.

Launch Avamar Proxy Deployment from the overflow button

Before you begin

You can launch the AUI **Avamar Proxy Deployment** page when IDPA System Manager is open to one of the following pages:

- **Job Activities**
- **Asset Activities**
- **System Management**

Procedure

1. Click the overflow button beside the Avamar system:



2. Click **Avamar Proxy Deployment**.

Results

The Avamar AUI launches to the **Avamar Proxy Deployment** page.

Launching Data Domain System Manager

IDPA System Manager provides the capability for you to launch the Data Domain System Manager.

For instructions about how to log into and use Data Domain System Manager, refer to the Data Domain documentation.

Launch System Manager from the overflow button

Before you begin

IDPA System Manager must be open to one of the following pages:

- **Health**
- **Alerts**
- **Capacity**
- **System Management**

Procedure

1. Click the overflow button beside the Data Domain system:



2. Click **System Manager**.

Results

Data Domain System Manager launches.

Launch System Manager from the Detail pane

Before you begin

IDPA System Manager must be open to one of the following pages:

- **Health**
- **Capacity**

Procedure

1. Select the Data Domain system from the list of systems on the **Master** pane.
2. In the **Detail** pane, click **SYSTEM MANAGER**.


Results

Data Domain System Manager launches.

Launching Search

IDPA System Manager provides the capability for you to launch Search.


Procedure

1. In the **Left** menu, select **System Management**.
The **System Management** page appears.
2. In the row for the Search system, click the Overflow menu ().
3. Click **DATA PROTECTION SEARCH**.
Search launches in a new browser tab.
4. For further instructions about how to log in to Search, refer to the Search documentation.

Launching Data Protection Advisor

IDPA System Manager provides the capability for you to launch Data Protection Advisor.

Procedure

1. In the **Left** menu, select **System Management**.
The **System Management** page appears.
2. In the row for the Data Protection Advisor system, click the Overflow menu ().
3. Click **DATA PROTECTION ADVISOR**.
Data Protection Advisor launches in a new browser tab.
4. For further instructions about how to log in to Data Protection Advisor, refer to the Data Protection Advisor documentation.

CHAPTER 9

Running Reports

Learn about IDPA System Manager reports.

This chapter contains the following sections:

• Reports overview	76
• Run a report	76
• View the last report	77
• Backup Report Card	77
• Backup Client Summary	77
• Strike Summary	78
• Backup Data Backed Up Daily	78
• Backup Number of Jobs Backed Up Daily	79
• Data Domain Utilization	79
• Data Domain Tier Utilization	79
• Data Domain Daily Compression Statistics	79
• Data Domain Filesystem Utilization	80
• Data Domain DeDuplication Ratio	80
• Data Domain Active Streams	80

Reports overview


IDPA System Manager provides the capability for you to run 11 of the most used Data Protection Advisor reports for Avamar and Data Domain systems.

IDPA System Manager reporting features require you to have Data Protection Advisor system configured with IDPA System Manager.

[Add a Data Protection Advisor system](#) on page 50 provides instructions for adding a Data Protection Advisor system to IDPA System Manager.

For more information about Data Protection Advisor, refer to the Data Protection Advisor documentation set.

You can run, and then view these reports directly in the IDPA System Manager user interface. You can also specify the reporting period for these reports within the IDPA System Manager interface.

 **Note:** To take full advantage of IDPA System Manager capabilities, it is recommended that all systems that are configured in Data Protection Advisor also be configured in IDPA System Manager.

Run a report

In the IDPA System Manager user interface, you can run 11 of the most used Data Protection Advisor reports for Avamar and Data Domain systems.

Procedure

1. In the **Left** menu, select **Reports**.
2. (Optional) To filter the list of reports on system type, select one or more of the following options:
 - **Avamar**
 - **Data Domain**
3. (Optional) To search for a specific report, type the report name in the search box.
4. (Optional) To specify a reporting period other than the default of last week for the report that you want to run, click **LAST WEEK**.

A menu appears and displays a list of the reporting periods that are available.

From the list, select a reporting period.

5. On the report that you want to run, click **RUN REPORT**.

While the report is generating, the **RUN REPORT** button displays `PROCESSING`.

When the report is available for viewing, a notification appears at the top of the user interface.

6. After the report generation is complete, to view the report, click **VIEW LAST REPORT**.

The report opens in a new window.

View the last report

IDPA System Manager provides the capability for you to view the last report that was run.

About this task

Data Protection Advisor retains reports for a period of 24 hours. The **View Report** link will not be visible if the last report was generated more than 24 hours ago.

Procedure

1. In the **Left** menu, select **Reports**.
2. (Optional) To filter the list of reports on system type, select one or more of the following options:
 - **Avamar**
 - **Data Domain**
3. (Optional) To search for a specific report, type the report name in the search box.
4. On the report that you want to view, click **VIEW LAST REPORT**.

The report opens in a new window.

Backup Report Card

The **Backup Report Card** reports information about each client that was backed up over the reporting period and the number of successful and unsuccessful jobs on a daily basis in a report card.

The **Backup Report Card** identifies clients that have repetitive failures, or more importantly, clients that have not been backed up at all. For each day in the specified reporting period, a cell displays the backup status of each client:

- If the cell for a client is completely green, all backups were successful for that client on that day.
- If the cell is completely red, all backups failed for that client on that day.
- If there is a mix of red and green, the proportion represents the percentage of backups that failed on that client on that day.
- If a cell is white, no backups occurred for that client on that day.

Backup Client Summary

The **Backup Client Summary** report provides of summary of the backup client in a table report.

The report includes the following information:

- **Completed**—Count of the total number of clients on the backup server that has at least one job on it.
- **Successful**—Indicates that all jobs that were processed on the client during the reporting period were successful.
- **Partial**—Indicates that some jobs were successful and that some jobs were unsuccessful during the reporting period. The statuses of jobs could be **Successful**, **Failure**, or **Missed**. The **Backup Client Summary** report lists a client as a **Partial** client when it has a mix of failed, successful, and missed jobs within the period.

- **Failed**—Count of the total number of clients after deduplication with only failed jobs on them.
- **Missed**—Count of the number of clients with all missed jobs on them.
- **Active**—Count of the number of clients with active jobs running.
- **Success Rate**—Success rate of clients on the backup server over the reporting period.

Strike Summary

The **Strike Summary** report returns the number of clients that have not been backed up for one or more days consecutively in a table report.

The report includes the following information:

- **One Strike**—Count of the number of clients that have at least one failure in the last 24 hours, which is the last day.
- **Two Strikes**—Count of the number of clients that have at least one failure in the last 24 hour to 48 hour period and last 24 hour period, which is the last 2 days.
- **Three Strikes**—Count of the number of clients that have at least one failure in the last 3 days.

The following list includes information about strikes and other elements of this report:

- Strikes are based on clients.
- If deduplication is enabled in **Configure Report Settings** in the Data Protection Advisor web console, the jobs on the client are deduplicated to discount earlier failures where a job later succeeded.
- A partial success where some jobs are successful and some fail for a client, counts as strike.
- If a client has a combination of missed/failed or missed/successful jobs, it is considered a partial client and is included in the strike count. Alternatively, a client with all missed jobs is included in the count.
- Full or incremental Backup level does not make a difference. Reports do not filter based on job level.
- If you run a report with a period of last day, the report only returns a one strike failed client count because you only ran it for the last day. If you run the report for last 2 days, if any exist, it returns the count for one and two strike failures. If you run it for last week or last 3 days, the report returns any failures in last 3 days.
- The report is hard-coded to return failure counts only for consecutive failed clients for the last 3 days, maximum. It does not matter if you configure the report to run with a period that is longer than 3 days. For example, if you specify the period of last month, the report does not report on any three strikes within the last month.

Backup Data Backed Up Daily

The **Backup Data Backed Up Daily** report returns the total data by server that is backed up daily in a column chart.

The report includes the following information:

- **Total Size**—Total amount of data backed up (in GB).
- **Server**—Name of the server on which the backup occurred.

Backup Number of Jobs Backed Up Daily

The **Backup Number of Jobs Backed Up Daily** report returns the total number of jobs that are backed up daily in a column chart.

Num Jobs represents the number of jobs that have completed.

Data Domain Utilization

The **Data Domain Utilization** report returns information about Data Domain utilization in a table.

The report includes the following information:

- **Hostname**—Name of the host on which the file system is mounted.
- **Utilization**—Average utilization for all hosts as a percentage.
- **Capacity**—Total capacity on the host in GB.
- **Used Capacity**—Amount of space that is used on the file system in MB.
- **Cleanable Space**—Amount of space that can be cleaned in MB.
- **Free Capacity**—Amount of free space on the file system in MB.
- **Last Day Change**—The amount of space that is used in MB per Data Domain in the 24 hours.
- **Dedup Ratio**—The de-duplication ratio that Data Domain is achieving.

Data Domain Tier Utilization

The **Data Domain Tier Utilization** report returns information about Data Domain system tier capacity and utilization in a table report.

The report includes the following information:

- **Hostname**—Name of the Data Domain.
- **Tier**—Name of the tier.
- **Utilization**—Capacity utilization on the tier as a percentage.
- **Capacity**—Total storage space in MB.
- **Used Capacity**—Post compression size in MB.
- **Available Capacity**—Available storage space in MB.
- **Pre Compression Size**—Pre compression size in MB.
- **Cleanable Space**—Amount of cleanable space in MB.

Data Domain Daily Compression Statistics

Returns Data Domain daily compression statistics in a line chart. Uses data from the Daily Compression Statistics data source.

- **Hostname**—Name or IP address of the Data Domain server.
- **Total Compression Factor**—Difference between the Pre Compression Size and the Post Local Compression Size (in MB).

- Dedupe Ratio—Difference between the Deduplication Ratio and the Total Compression Factor, displayed as a percentage.
- Global Compression Factor—Size after deduplication (in MB).
- Local Compression Factor—Size after deduplication + local compression (in MB).
- Reduction—Displayed as a percentage.

Data Domain Filesystem Utilization

The **Data Domain Filesystem Utilization** report returns Data Domain utilization trend values over time in a line chart.

Utilization represents Data Domain file system utilization value as a percentage.

Data Domain DeDuplication Ratio

The **Data Domain DeDuplication Ratio** report returns the ratio for the size of data that is deduplicated against the original data size over time in a line chart.

The report includes the following information:

- Hostname—Name or IP address of Data Domain.
- Dedupe Ratio—Difference between the Deduplication Ratio and the Total Compression Factor as a percentage.

Data Domain Active Streams

The **Data Domain Active Streams** report returns the Data Domain active streams in a line chart.

The report includes the following information:

- Hostname—Name or IP address of the Data Domain server.
- Active Read Streams—Number of active read file streams.
- Active Write Streams—Number of active write file streams.
- Re Opened Read Streams—Re-opened read file streams in the past 30 seconds.
- Re Opened Write Streams—Re-opened write file streams in the past 30 seconds.

CHAPTER 10

Auditing IDPA System Manager Activities

This chapter includes the following sections:

- [IDPA System Manager audit overview](#) 82
- [Activities audit information](#) 82

IDPA System Manager audit overview

On the **Audit** page, you can view audit information about activities in IDPA System Manager.

Audit information includes actions and tasks that IDPA System Manager users have performed.

The audit information can also be used to track the status of long running tasks.

Activities audit information

The **Audit** page displays audit information about activities in IDPA System Manager.

Basic audit information

The following list includes the basic types of audit information for activities that are displayed in the table on the **Audit** page.

Title

The title of the activity.

Status

The state of the activity.

Progress

The percentage of the activity that is complete.

Last Updated

The date and time the activity was last updated.

User

The user that initiated the activity.

Additional audit information

The following list includes additional details that are only displayed when you click the drop-down arrow for an activity.

Description

The description of the activity.

Comments

The comments for the activity, if applicable.

Sub Tasks

Sub tasks for the activity, if applicable. The following information is listed for each sub task:

- Title
- Status
- Progress
- Last Updated

Click the drop-down arrow for a sub task to display additional details.

CHAPTER 11

Server Administration

Learn about IDPA System Manager server administration.

This chapter contains the following sections:

- [Backing up IDPA System Manager](#) 84
- [Restoring a backup of IDPA System Manager](#) 84
- [Change the IDPA System Manager IP address](#) 84
- [Change the network configuration for OVA deployments of IDPA System Manager](#) 85
- [Upgrading IDPA System Manager](#) 86

Backing up IDPA System Manager

If IDPA System Manager is deployed as virtual machine, a virtual machine backup application can be used to back up the IDPA System Manager.

IDPA System Manager can also be backed up using a file system based backup application.

When using a file system based backup application, ensure that no IDPA System Manager administrator activities occur when performing the backup. Include the following directories in the file system backup:

- /data01
- /usr/local/dpc
- /var/log/dpc
- /var/lib/dpc

Restoring a backup of IDPA System Manager

To restore IDPA System Manager from a file system backup, perform the following procedure:

1. Deploy the IDPA System Manager OVA.
The *IDPA System Manager Getting Started Guide* provides information.
2. Stop the IDPA System Manager services using the following command:

```
/usr/local/dpc/bin/dpc stop
```

3. Restore the IDPA System Manager directories to the original locations.
4. To activate the changes, restart IDPA System Manager using the following command:

```
/usr/local/dpc/bin/dpc start
```

Change the IDPA System Manager IP address

IDPA System Manager supports changing the IP address of the IDPA System Manager system.

Procedure

1. Launch a command prompt.
2. Log in as the root user.
3. Launch YaST, and then browse to **System > Network Settings**.

The YaST **Network Settings** dialog box appears with four tabs:

- Global Options
- Overview
- Hostname/DNS
- Routing

4. Click **Overview**.

The **Overview** tab contains information about installed network interfaces and configurations.

One Network card is listed.

5. Use the Tab key to select **Edit**, and then press Enter.
The **Network Card Setup** page appears.
6. On the **Network Card Setup** page, make the following changes:
 - Change **IP Address** to the new IP address.
 - Change **Subnet Mask**, if required.
 - Ensure that the **Statically Assigned IP Address** is selected.

Note: Do not change the **Hostname** from the value that was set when IDPA System Manager was deployed. IDPA System Manager uses the hostname to generate certificates and changing the hostname will invalidate the certificates.

7. Use the Tab key to select **Next**, and then press Enter.
8. Use the Tab key to select **OK**, and then press Enter.
The IP address changes are applied.
9. Use the Tab key to select **Quit**, and then press Enter.
10. Run the following commands to restart the IDPA System Manager services:

```
/usr/local/dpc/bin/dpc stop
```

```
/usr/local/dpc/bin/dpc start
```

Change the network configuration for OVA deployments of IDPA System Manager

For OVA deployments of IDPA System Manager, use the `dpc-network` command to update network configuration settings.

Procedure

1. Log in to vCenter using the vSphere client where the IDPA System Manager OVA is deployed.
2. Launch a command prompt.
3. Run the `dpc-network` command with the following syntax, as required:

```
usr/local/dpc/bin/dpc-network {-i<ip_address> | -n<netmask> | -g<gateway> | -d<dns>}
```

where:

- i**
Updates the IDPA System Manager IP address.
- n**
Updates the IDPA System Manager netmask.
- g**
Updates the IDPA System Manager gateway.
- d**

Updates the IDPA System Manager domain system name (DNS).

Consider the following examples:

- The following command updates the IDPA System Manager OVA IP address:

```
usr/local/dpc/bin/dpc-network -i 192.168.2.150
```

- The following command updates all of the IDPA System Manager OVA network settings:

```
usr/local/dpc/bin/dpc-network -i 192.168.2.150 -n 255.255.255.0 -g 192.168.2.1 -d 192.168.1.100
```

- i **Note:** Do not change the IDPA System Manager hostname. The hostname set up during deployment is used to create the lockbox. If you change the hostname, IDPA System Manager cannot access the lockbox.

Results

The network settings are updated.

Upgrading IDPA System Manager

Learn about upgrading from a previous release to IDPA System Manager 18.2.

This chapter includes the following topics:

Upgrade IDPA System Manager to version 18.2 on standalone server or virtual machine

IDPA System Manager supports a direct upgrade to the latest version.

Before you begin

- i **NOTICE** Before you upgrade IDPA System Manager, it is highly recommended that you back up the IDPA System Manager system. [Backing up IDPA System Manager](#) on page 84 provides information on how to back up IDPA System Manager.

Ensure that the system being upgraded meets the following requirements:

- Standalone server deployments require 1.5GHz processor.
- Virtual machine deployments require 4 CPUs with 1 core each.
- 8GB of RAM.
- 550 GB of disk space available.
- The environment is running SuSE Linux Enterprise Server 12 SP2.
It is recommended that you disable AppArmor. If you must enable AppArmor, then the AppArmor profiles should not block the applications used by IDPA System Manager.
- Java Platform Standard Edition Development Kit (JDK) version 8u181 or greater is installed, including the following packages:
 - javapackages-tools-2.0.1-8.1.x86_64
 - java-1_8_0-openjdk-headless-1.8.0.181-27.26.2.x86_64
 - java-1_8_0-openjdk-1.8.0.181-27.26.2.x86_64

- i **Note:** Java may require additional packages to be installed.

- The Linux socat package is installed.
- The DNS is set up correctly. The correct DNS set up ensures that systems monitored by IDPA System Manager can resolve the IDPA System Manager hostname and Fully Qualified Domain Name (FQDN).
- The FQDN, IP, Netmask, Gateway, DNS, NTP, and time zone are configured.
- The environment is using static network settings.

About this task

- Note:** It is highly recommended that the VMware environment where IDPA System Manager is deployed is backed up by UPS (Uninterrupted Power Supply). To shutdown DPC, do not use the "Power off the virtual machine" feature on vCenter. Instead, shutdown the Operating System gracefully in DPC using 'shutdown -h now' in the bash shell

Procedure

1. To access the IDPA System Manager system, type the following command:

```
ssh -l <USERNAME> <DPC_FQDN>
```

2. To switch to the root user, type the following command:

```
su -
```

3. Copy the IDPA System Manager software update file to the IDPA System Manager host.

- Note:** Depending on the method that you use to copy the update file, you may be required to disable the firewall to allow the file to be copied to the IDPA System Manager host. To disable the firewall, run the following command:

```
systemctl stop SuSEfirewall2
```

Once you have copied the file, to restart the firewall, run the following command:

```
systemctl start SuSEfirewall2
```

4. To initiate the upgrade to version 18.2, type the following command:

```
java -jar emc-dpc-18.2.0-<buildnumber>.jar
```

After you finish

After upgrading IDPA System Manager, for OVA deployments only, you must upgrade the IDPA System Manager operating system, which will install security updates and adjust firewall settings.

- Note:** During a IDPA System Manager upgrade to version 18.2, data is migrated from the old version to the new version. Depending on the amount of data, this migration could take up to several minutes. After the upgrade, when the IDPA System Manager 18.2 system starts up, the database is re-indexed. This operation could also take several minutes, depending on the amount of data. You cannot log in to the IDPA System Manager web user interface until the re-indexing operation is complete.

IDPA System Manager OS update

Periodically, security patches and fixes are released for the IDPA System Manager OS.

About this task

These fixes must be installed on OVA deployments of IDPA System Manager. When available, it is highly recommended that you install these security patches and fixes on the IDPA System Manager server.

The *Data Protection Central OS Update Release Notes* provides information about the security patches and fixes included in the IDPA System Manager OS update. The Support KB article <https://support.emc.com/kb/522157> provides instructions for installing the OS update.

Migrating from Multiple Systems Management to IDPA System Manager

About this task

IDPA System Manager does not support a direct upgrade from Multiple Systems Management (MSM) due to significant architectural changes that give IDPA System Manager better stability and scalability.

Procedure

1. Identify the Avamar systems being monitored with MSM that are supported with IDPA System Manager.

Avamar versions 7.5.0-183_HF300003 hotfix and later are supported with IDPA System Manager.
2. Using the MSM user interface, remove the Avamar systems identified in step 1 from MSM.
3. Deploy the IDPA System Manager OVA.


The *IDPA System Manager Getting Started Guide* provides instructions.

4. Log into the IDPA System Manager OVA, and then use **System Management** to add the Avamar systems.

Each Avamar system remains in the **NotReporting** state for several minutes until adaptor activation is complete.

Results

Once the adaptor activation is complete, the migrated Avamar systems begin logging activities to IDPA System Manager and are no longer monitored by MSM.

 **Note:** Historical Avamar monitoring data is not transferred to IDPA System Manager.

IDPA System Manager will attempt to automatically add any Data Domain systems configured with monitored Avamar systems. If required, Data Domain systems can also be added manually through IDPA System Manager **System Management**.

CHAPTER 12

Troubleshooting

The following sections may assist with troubleshooting issues with IDPA System Manager.

Topics include:

• Directory structure and log information	90
• Deployment of IDPA System Manager fails due to "No space left on device"	90
• Troubleshooting LDAP	91
• Systems fail to activate	93
• Avamar systems fail to activate	94
• Lockbox	94
• Unlock a IDPA System Manager user account	96
• The SSO service fails to start on IDPA System Manager	96
• Disabling SSO	97
• Reregister SSO for a system	98
• Resolve error notifications	98

Directory structure and log information

The following list includes information about the IDPA System Manager directory structure and log information:

- All IDPA System Manager specific packages are under:
`/usr/local/dpc/lib`
- Each package has its own subdirectory. For example, `setup` and `monitor`.
- Each package has similar structures. For example, `bin` and `conf`.
- The `/usr/local/dpc/bin` directory includes scripts to start or stop IDPA System Manager services. To start or stop an individual IDPA System Manager service, use the `service` command.
- The `/var/log/dpc` directory hosts all IDPA System Manager related logs including NGINX, MongoDB, and RabbitMQ.
- The `/var/lib/dpc` directory hosts all IDPA System Manager generated data which consists of MongoDB and RabbitMQ.
- All IDPA System Manager related logs are under:
`/var/log/dpc/[module name]`
`[module name].out` files contain console logging from starting and running the module process.
`[module name].log` files contain logging from the module.
- All Elemental Gateway (ELG) logs are under:
`/var/log/dpc/elg/`
- The IDPA System Manager user interface (`msm-ui-main` service) log is under:
`/var/log/dpc/msm-ui-main`
This log file is small and contains information from starting the Node.js server.
- The IDPA System Manager Monitoring (`dpc-monitor` service) logs are under:
`/var/log/dpc/monitor`
This directory contains the rolling log files from the monitoring process.

Deployment of IDPA System Manager fails due to "No space left on device"

If deployment of IDPA System Manager fails with an error message similar to the following in the `/var/log/dpc/install/install.log` file, delete the IDPA System Manager virtual machine and re-attempt installation.

```
error: unpacking of archive failed on file /usr/lib64/erlang/lib/os_mon-2.4.3/priv/mibs/OTP-OS-MON-MIB.bin: cpio: rename failed - No space left on device
```

Troubleshooting LDAP

Learn how to diagnose and resolve common LDAP configuration issues.

Check the LDAP status in the log file

Check the `/var/log/dpc/elg/elg.log` log file for messages about the LDAP connection status.

Messages that appear during LDAP connection failure

If the following message appears, the LDAP client did not make a successful connection to the LDAP server:

```
2018-04-03 11:00:26,929 INFO localhost-startStop-1 c.e.c.c.SecurityConfig LDAP or AD Directory Service providers are not available
```

There are multiple issues that can prevent the LDAP client from connecting to the LDAP server. Look for error messages in the log file that provide more information.

The following table describes various error messages that appear during LDAP connection failures and their causes.

Table 7 LDAP communication messages

Message	Cause
INFO localhost-startStop-1 c.e.c.c.SecurityConfig LDAP or AD Directory Service providers are not available	No LDAP or AD setting are provided or they are provided with incorrect information.
.ADLdapAuthenticationProvider Ignoring AD authentication. Verification of ldap settings failed. Failed to connect	Invalid AD configuration information.
.LdapAuthenticationProvider Ignoring LDAP authentication. Verification of ldap settings failed. Failed to connect	Invalid LDAP configuration information.
PKIX path building failed: java.security.cert.CertPathBuilderException: Could not build a validated path	Validation of the LDAP server certificate could not be completed. One possible solution for this issue is to add the LDAP server certificate to the IDPA System Manager Java keystore.

Messages that appear during LDAP connection success

Messages similar to the following appear when the LDAP client successfully connects to the LDAP server:

```
c.e.c.s.a.l.LDAPSecureStorage LDAP admin credentials are secured
c.e.c.s.a.l.ExternalAuthenticationProvider Type: LDAP
c.e.c.s.a.l.ExternalAuthenticationProvider Base DN: dc=mydomain,dc=com
```

```
c.e.c.s.a.l.ExternalAuthenticationProvider Admin user DN:
cn=Administrator,dc=my-domain,dc=com
c.e.c.s.a.l.ExternalAuthenticationProvider User Base: ou=people
c.e.c.s.a.l.ExternalAuthenticationProvider User Search DN: (|(uid={0})(cn={0}))
c.e.c.s.a.l.ExternalAuthenticationProvider User Pattern DN: []
c.e.c.s.a.l.ExternalAuthenticationProvider Group Name: dp_admin
c.e.c.s.a.l.ExternalAuthenticationProvider Group Search Base: ou=group
c.e.c.s.a.l.ExternalAuthenticationProvider Group Search Filter: (&(member={0})
(cn=dp_admin))
o.s.s.l.DefaultSpringSecurityContextSource URL 'ldap://12.3.104.150:546/dc=my-
domain,dc=com', root DN is 'dc=mydomain,dc=com'
12.3.104.150:546/dc=my-domain,dc=com', root DN is 'dc=mydomain,dc=com'
```

Diagnosing LDAP authentication failure

LDAP user authentication fails when the LDAP lookup matches more than one record for the user in the LDAP server.

Issue

If IDPA System Manager is configured to use LDAP authentication, and the authentication lookup of a user returns more than one record, IDPA System Manager displays the following message:

```
We didn't recognize the username or password you entered. Please try again
```

Also, the `/var/log/dpc/elg/elg.log` log file will contain the following message:

```
2018-04-04 08:23:04,834 ERROR http-nio-9002-exec-8 o.a.c.c.C.[.[.[.
[dispatcherServlet] Servlet.service() for servlet[dispatcherServlet] in context
with path [/elg] threw exception
org.springframework.dao.IncorrectResultSizeDataAccessException: Incorrect
result size: expected 1, actual 2
```

Solution

Ensure that each user that is registered for LDAP authentication matches only one LDAP record.

Restore access to IDPA System Manager after LDAP misconfiguration

When LDAP is configured incorrectly, you can be locked out of the IDPA System Manager OVA.

About this task

If you cannot log into IDPA System Manager after configuring LDAP, perform the following steps.

Procedure

1. To disable the `ldap.properties` file, rename it using the following command:

```
mv ldap.properties ldap.properties.old
```

2. To restart IDPA System Manager and activate the change, type the following commands:

```
/usr/local/dpc/bin/dpc stop
/usr/local/dpc/bin/dpc start
```

Results

After IDPA System Manager is restarted, LDAP is disabled and access to IDPA System Manager is restored.

Remove LDAP from IDPA System Manager

If required, you can remove LDAP from IDPA System Manager.

Procedure

1. To access the IDPA System Manager system, type the following command:

```
ssh -l <USERNAME> <DPC_FQDN>
```

2. To switch to the root user, type the following command:

```
su -
```

3. To remove the `ldap.properties` file, type the following command:

```
rm /var/lib/dpc/elg/ldap.properties
```

4. To restart IDPA System Manager and activate the change, type the following command:

```
/usr/local/dpc/bin/dpc start
```

5. Once IDPA System Manager is started, type the following command to confirm that all of the services are active:

```
/usr/local/dpc/bin/dpc status
```

6. Log in to the IDPA System Manager user interface with the username and password for the non-LDAP user account.

For example:

```
https://DPC_fqdn
```

where *DPC_fqdn* is the IDPA System Manager fully qualified domain name.

Systems fail to activate

If a system is in a `NotReporting` health state for more than 5 minutes after the system is added or after a refresh is performed on the **Systems Management** page, reactivate messaging.

To reactivate messaging, perform the following steps:

1. Browse to the **Systems Management** page.
2. Select the system that is not reporting.

3. Click **Reactivate**.
4. Browse to the **Audit** screen, and then monitor the progress.

Avamar systems fail to activate

The following error messages may appear on the **Activities > Audit** page when an Avamar system fails to activate.

Failed - ERROR: Unable to get signed client certificate from lava81105.dev.local

Verify the network settings are correct.

The *IDPA System Manager Security Configuration Guide* provides information on the network settings that are required for successful communication.

Failed - unable to create root session to process msgborkerctl task

This message can appear after an Avamar system is upgraded.

Perform the following steps to resolve this issue:

1. Login to the Avamar system using SSH.
2. Switch to the root user.
3. Open the `/etc/ssh/sshd_config` file for editing.
4. Check for duplicate entries after the `Match all` text near the bottom of the file.
5. Comment out any duplicate entries that do not apply to the Avamar system.
6. Save and close the file.
7. Restart the sshd service by running the following command:

```
service sshd restart
```

8. In IDPA System Manager, on the **Systems Management** page, select the Avamar system, and then click **Reactivate**.

Lockbox

IDPA System Manager uses a secure storage lockbox to encrypt and store both internal system credentials and credentials for external systems that IDPA System Manager monitors and manages.

The lockbox is created when you deploy IDPA System Manager. During deployment, you must specify a lockbox password. The password is encrypted and stored in the lockbox along with Stable System Values (SSVs), which uniquely identify the IDPA System Manager host. The lockbox uses the SSVs to generate an encryption key to encrypt the system credentials.

Lockbox password requirements

The lockbox password must be between 8 and 256 characters in length.

Reset the lockbox

In certain situations, for example, when a virtual machine is moved, you may have to reset the lockbox.

Procedure

1. Open an SSH session with an SSH tool, such as PuTTY.
2. As the Linux OS user admin, log in to the IDPA System Manager host.
3. Type the following commands:

```
cd /usr/local/dpc/lib/elg
sudo service msm-monitor stop
bin/elgcli -reset -lockbox -password {original_password}
sudo service msm-monitor start
```

where *original_password* is the password that was specified when the lockbox was created.

If resetting the lockbox is unsuccessful, remove the existing lockbox, and then create the lockbox again.

Remove the lockbox

In certain situations, you may need to remove the lockbox, for example, when resetting the lockbox is unsuccessful.

Procedure

1. Open an SSH session with an SSH tool, such as PuTTY.
2. As the Linux OS user admin, log in to the IDPA System Manager host.
3. Type the following command:

```
cd /var/lib/dpc/security/
```

4. To remove the lockbox, remove the following files with the `rm -rf` command:
 - `clp_lb.lb`
 - `clp_lb.lb.FCD`


After you finish

If you are re-creating the lockbox, each system must be edited to enter the login credentials and store them in the lockbox.

Create the lockbox

If for some reason you are required to remove the lockbox that was automatically created during the initial OVA deployment, you can manually create a lockbox.

About this task

 **Note:** Each system must be edited to enter the login credentials and store them in the lockbox.

Procedure

1. Open an SSH session with an SSH tool, such as PuTTY.
2. As the Linux OS user admin, log in to the IDPA System Manager host.
3. Type the following commands:

```
cd /usr/local/dpc/lib/elg
sudo service msm-monitor stop
sudo service msm-elg stop
bin/elgcli -create -lockbox -password <secure_storage_password>
cd /var/lib/dpc/security/
chown dpc:dpc clp_lb.lb*
sudo service msm-monitor start
sudo service msm-elg start
```

The lockbox password must be between 8 and 256 characters in length.

Unlock a IDPA System Manager user account

When too many failed login attempts through SSH are made on a IDPA System Manager user account, the account is locked. You can reset the account to unlock it and regain access.

Procedure

1. Connect to the console of the IDPA System Manager server, and log in to the "admin" account.
2. To change to the root user, run the following command:

```
su -
```

3. To reset SSH access to the user account, run the following command:

```
pam_tally2 --user=admin --reset
```

The SSO service fails to start on IDPA System Manager

About this task

If the IDPA System Manager SSO service fails to start, perform the following procedure to resolve the issue.

Procedure

1. Connect to the console of the IDPA System Manager server, and log in to the "admin" account.

2. Change to the root user by running the following command:

```
su -
```

3. Open the `dpc-ssoservice` file for editing by running the following command:

```
vi /usr/local/dpc/lib/sso/setup/dpc-ssoservice
```

4. Add `TimeoutStartSec=` to the `[Service]` section.

For example:

```
[Service]
Type=forking
ExecStart=/usr/local/dpc/lib/sso/bin/dpc-ssos start
ExecStop=/usr/local/dpc/lib/sso/bin/dpc-ssos stop
User=admin
TimeoutStartSec=
```

5. Save and close the `dpc-ssoservice` file.
6. Copy the updated file to the `/usr/lib/systemd/system/` folder by running the following command:

```
cp /usr/local/dpc/lib/sso/setup/dpc-ssoservice /usr/lib/systemd/system/
```

7. Run the following commands to restart the IDPA System Manager services:

```
/usr/local/dpc/bin/dpc stop
```

```
/usr/local/dpc/bin/dpc start
```

Disabling SSO

If single sign on (SSO) to IDPA System Manager is not working, disable it to log in to IDPA System Manager using the credentials stored in secure storage.

Procedure

1. Open the `application.properties` file located in `/usr/local/dpc/lib/dpc/elg/` for editing.
2. Add the following entry to the `application.properties` file:

```
elg.sso.enabled=false
```

3. Save and close the `application.properties` file.

- Restart the ELG service using the following command:

```
service msm-elg restart
```

Results

You can now log in to IDPA System Manager using the credentials stored in secure storage.

Reregister SSO for a system

When single sign on (SSO) is not working, you can reregister the SSO client.

Procedure

- On the **System Management** page, select the system that you want to reregister SSO for.
- Click the overflow button:



- Click **Reregister SSO**.

The reregister operation may take several minutes to complete. You can track the status of the operation in the **Audit** page.

Resolve error notifications

There are several ways that you can resolve error notifications that appear in a red bar at the top of the browser window.

About this task

The following list includes the different ways that you can resolve error notifications:

- On the right side of the bar, click the red **X** button.
- If the page is not displaying or not functioning correctly, it is recommended that you refresh the browser.
- If refreshing the browser is not working, log out of the IDPA System Manager user interface, and then log back in.

GLOSSARY

A

- administrator** Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.
- Avamar Administrator** A graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.
- Avamar client** A computer or workstation that runs Avamar software and accesses the Avamar server over a network connection. Avamar client software comprises a *client agent* and one or more *plug-ins*.
- Avamar server** The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

E

- Element managers** Applications that are used to configure and manage one or more data protection and storage devices.

H

- HFS check** An Avamar Hash File System check (HFS check) is an internal operation that validates the integrity of a specific checkpoint. Once a checkpoint has passed an HFS check, it can be considered reliable enough to be used for a server rollback.
- host** Computer on a network.
- hostname** Name or address of a physical or virtual host computer that is connected to a network.

I

- IDPA System Manager server** The IDPA System Manager server contains the business logic and supporting databases, hosts the web application, and communicates with all managed servers for management and monitoring purposes. The IDPA System Manager server collects event data from adapters that run on the managed Avamar server.

L

Lightweight Directory Access Protocol (LDAP) Set of protocols for accessing information directories.

O

OVA Open Virtual Appliance (OVA) is a single file distribution of a package that follows the packaging format standard called Open Virtualization Format (OVF). The application server is deployed as an OVA virtual machine.

S

SSH Secure Shell. A remote login utility that authenticates by way of encrypted security keys instead of prompting for passwords. This prevents passwords from traveling across networks in an unprotected manner.