

Dell EMC IDPA System Manager

Version 18.1

Administration Guide

302-004-612

REV 04

Copyright © 2017-2018 Dell Inc. or its subsidiaries. All rights reserved.

Published December 2018

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	IDPA System Manager Overview	11
	Product overview.....	12
	Environment and system requirements	12
	Single Sign-On overview.....	13
	Monitoring systems	13
	Managing Avamar systems	14
	Systems data refresh times	14
	Search and recover capabilities.....	14
	Report capabilities.....	15
	Backing up IDPA System Manager.....	15
	Restoring a backup of IDPA System Manager.....	16
Chapter 2	User Interface	17
	Header.....	18
	View version information.....	18
	User menu.....	18
	Change password.....	19
	Log out of IDPA System Manager.....	19
	Left menu.....	19
	Pages.....	21
	Master and Detail panes.....	21
	Choose another Dashboard menu.....	22
	Filtering.....	22
	Sort information that is displayed in tables.....	23
	Dialog boxes.....	24
	Notification bar.....	24
	Overflow button.....	24
Chapter 3	Dashboards	25
	Dashboards overview.....	26
	Drill down pages.....	26
	Widgets and key performance indicators.....	26
	Change the reporting period for a widget.....	28
	Refresh the dashboard.....	28
	Filter systems for a dashboard widget.....	29
	Add a dashboard.....	29
	Editing a dashboard.....	30
	Rename a dashboard.....	30
	Set a dashboard to be the default dashboard.....	30
	Reset widgets to a selected dashboard template.....	31
	Delete a dashboard.....	31
	Toggle between full screen and normal screen.....	31
Chapter 4	Health	33
	Health overview.....	34

	Health > Systems page.....	34
	Avamar system health information.....	34
	Data Domain system health information.....	36
	Data Protection Advisor and Search system health information....	37
	Health > Alerts page.....	38
	Avamar health alerts information.....	38
	Data Domain health alerts information.....	38
	IDPA System Manager alerts information.....	39
	Dismissing alerts.....	40
	Health > Capacity page.....	40
	Avamar health capacity information.....	41
	Data Domain health capacity information.....	41
Chapter 5	Activities	43
	Activities overview.....	44
	Activities > Systems page.....	44
	Avamar activities systems information.....	44
	Rerun an Avamar activity.....	46
	View the list of clients that are associated with an activity.....	46
	Activities > Clients page.....	46
	Activities > Audit page.....	47
	Activities audit information.....	48
Chapter 6	System Management	49
	System Management overview.....	50
	Avamar system management.....	50
	Add an Avamar system.....	50
	Edit an Avamar system.....	51
	Reactivate messaging for an Avamar system.....	51
	Policies.....	51
	Managing policies for Avamar systems.....	52
	View clients for Avamar systems.....	61
	Delete an Avamar system.....	62
	Data Domain system management.....	62
	Add a Data Domain System.....	62
	Edit a Data Domain system.....	62
	Delete a Data Domain system.....	63
	Data Protection Advisor system management.....	63
	Add a Data Protection Advisor system.....	63
	Edit an Data Protection Advisor system.....	64
	Delete an Data Protection Advisor system.....	64
	Search system management.....	65
	Add a Search system.....	65
	Edit a Search system.....	66
	Delete a Search system.....	66
	Reregister SSO for a system.....	66
	Group Management.....	67
	Add a group.....	67
	Edit a group.....	68
	Delete a group.....	68
Chapter 7	Launching System Management Applications	71
	Launching Avamar Administrator.....	72
	Launch Avamar Administrator from the overflow button.....	72

	Launch Avamar Administrator from the Detail pane.....	72
	Launching Avamar AUI.....	73
	Launch Avamar Restore from the overflow button.....	73
	Launch Avamar Proxy Deployment from the overflow button.....	73
	Launching Data Domain System Manager.....	74
	Launch System Manager from the overflow button.....	74
	Launch System Manager from the Detail pane.....	74
	Launching Search.....	75
	Launching Data Protection Advisor.....	75
Chapter 8	Reports	77
	Reports overview.....	78
	Run a report.....	78
	View the last report.....	79
	Backup Report Card.....	79
	Backup Client Summary.....	79
	Strike Summary.....	80
	Backup Data Backed Up Daily.....	80
	Backup Number of Jobs Backed Up Daily.....	81
	Data Domain Utilization.....	81
	Data Domain Tier Utilization.....	81
	Data Domain Daily Compression Statistics.....	81
	Data Domain Filesystem Utilization	82
	Data Domain DeDuplication Ratio.....	82
	Data Domain Active Streams.....	82
Chapter 9	Server Administration	83
	Change the IDPA System Manager IP address.....	84
Chapter 10	Upgrading IDPA System Manager	85
	Upgrade IDPA System Manager to version 18.1 on standalone server or virtual machine.....	86
	Install the IDPA System Manager OS update.....	87
	Migrating from Multiple Systems Management to IDPA System Manager.... 87	
Chapter 11	Troubleshooting	89
	Directory structure and log information.....	90
	Troubleshooting LDAP.....	90
	Checking the LDAP connection status	90
	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
	Secure storage.....	94
	Secure storage password requirements.....	95
	Reset the secure storage.....	95
	Remove the secure storage.....	95
	Create the secure storage.....	96
	Unlock a IDPA System Manager user account.....	96
	The SSO service fails to start on IDPA System Manager.....	96

CONTENTS

Disabling SSO 97
Number of activities listed in IDPA System Manager does not match Avamar
Administrator98
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 at <https://support.emc.com>.

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
04	December 18, 2018	The following updates are included in this revision: <ul style="list-style-type: none">• Updated the "System Management" chapter to add information about adding systems that use non-standard ports.• Updated the "Add an Avamar system" section to add instructions to override the Avamar Administrator link with a link to the the AUJ.• Updated step 3 in "Upgrade IDPA System Manager to version 18.1 on standalone server or virtual machine."
03	September 12, 2018	Added information about updating system versions to "Search and Data Protection Advisor system health information"
02	July 23, 2018	This revision includes the following changes: <ul style="list-style-type: none">• Updated "The SSO service fails to start on IDPA System Manager" to add step 7.• Updated "Install the IDPA System Manager OS update" to add information and link to KB article.
01	June 22, 2018	First release of the <i>IDPA System Manager 18.1 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.

Table 2 Style conventions (continued)

{ }	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://support.emc.com>
- <https://community.emc.com>

Where to get support

The Support website at <https://support.emc.com> provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact Support.


To access a product specific Support page:

1. Go to <https://support.emc.com/products>.
2. In the **Find a Product by Name** box, type a product name, and then select the product from the list that appears.
3. Click .
4. (Optional) To add the product to **My Saved Products**, in the product specific page, click **Add to My Saved Products**.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for by solution number, for example, 123456, or by keyword.

To search the Knowledgebase:

1. Go to <https://support.emc.com>.
2. Click **Advanced Search**.
The screen refreshes and filter options appear.
3. In the **Search Support or Find Service Request by Number** box, type a solution number or keywords.
4. (Optional) To limit the search to specific products, type a product name in the **Scope by product** box, and then select the product from the list that appears.
5. In the **Scope by resource** list box, select **Knowledgebase**.
The **Knowledgebase Advanced Search** panel appears.
6. (Optional) Specify other filters or advanced options.
7. Click .

Live chat

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

1. Go to <https://support.emc.com>.
2. Click **Chat with Support**.

Service requests

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

1. Go to <https://support.emc.com>.
 2. Click **Create a Service Request**.
-

Note

To create a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request:

1. Go to <https://support.emc.com>.
2. Click **Manage service requests**.

Online communities

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

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

IDPA System Manager Overview

Learn about IDPA System Manager.

Topics include:

- [Product overview](#) 12
- [Environment and system requirements](#) 12
- [Single Sign-On overview](#) 13
- [Monitoring systems](#) 13
- [Managing Avamar systems](#) 14
- [Systems data refresh times](#) 14
- [Search and recover capabilities](#) 14
- [Report capabilities](#) 15
- [Backing up IDPA System Manager](#) 15
- [Restoring a backup of IDPA System Manager](#) 16

Product overview

IDPA System Manager provides a solution for data protection administrators who are challenged by having to manage independent and disconnected applications that are used to configure and manage one or more data protection and storage devices.

Working with multiple applications in this manner causes daily operational monitoring and management to 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:

- Ability to launch the following software from a central location:
 - Avamar
 - Data Domain
 - Search
 - Data Protection Advisor
- Comprehensive dashboards that include the following system information:
 - The following information for Avamar and Data Domain systems:
 - Backup and replication activities
 - Health
 - Alerts
 - Capacity information for Avamar and Data Domain systems.
- Ability to monitor multiple systems capabilities including system health and activities.
- Ability to manage Avamar systems.
- Complex search and recover operations through integration with Search.
- Reporting capabilities through integration with Data Protection Advisor.

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 2 CPUs, 6 GB of RAM, and 550 GB of disk space available.
- The FQDN, IP, Netmask, 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.

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	7.4.1-58_HF299182_48 hotfix
	7.5.0-183_HF284113_2 hotfix
	7.5.1-101_HF298709_27 hotfix
Data Domain	6.0
	6.1
	6.1.1
Data Protection Advisor	6.4
	6.5
Search	1.1 SP3
	18.0
Mozilla Firefox	Latest version
Google Chrome	Latest version

Single Sign-On overview

IDPA System Manager supports Single Sign-On (SSO) authentication for certain systems.

SSO streamlines the process of managing systems by logging you into system management applications directly when you launch them from IDPA System Manager.

Systems must meet the following version requirements to have SSO enabled:

- Search systems must be version 18.1 or later.
- Avamar systems must be version 7.5.0-183_HF284113_2 hotfix or later.

If systems do not meet these version requirements, SSO is not available. You can monitor the SSO health status on the **Health > Systems** page.

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.

Monitoring systems

IDPA System Manager includes system monitoring features at the activity, system, and alert level.

The systems monitoring features include:

- **Activities**—Displays backup and replication (clone) activity information for Avamar systems.

- Alerts—Displays alerts information originating from Avamar and Data Domain systems.
- Capacity—Displays capacity information at a system level for Avamar and Data Domain systems.

If a Data Domain system is configured in a monitored Avamar system, the Data Domain system is automatically added as a monitored system.

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.

Different 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 alerts	Every 5 minutes
Data Domain system health status	Every 2 minutes
Data Domain system capacity	Every 60 minutes
Avamar system alerts	Every 90 seconds
Avamar system health status	Every 1 minute
Avamar system capacity, checkpoint, and garbage collection	Every 15 minutes
Avamar system activities	Every 15 seconds

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.

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

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
```


CHAPTER 2

User Interface

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

Topics include:

• Header	18
• View version information	18
• User menu	18
• Left menu	19
• Pages	21
• Master and Detail panes	21
• Choose another Dashboard menu	22
• Filtering	22
• Sort information that is displayed in tables	23
• Dialog boxes	24
• Notification bar	24
• Overflow button	24

Header

The header includes the following components:

- **System Filter** button—This button provides you with the ability to filter the information that appears on a page by one or more systems or groups. The **System Filter** button appears only on the **Health** information pages and the **Activities > Systems** page.
- **User** menu—This menu provides the ability to change the password or log out of IDPA System Manager.
- **About** button—This button provides the ability to view IDPA System Manager version information.

Figure 1 Header



View version information

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:

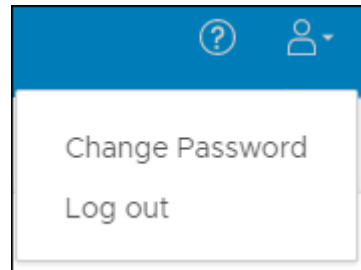
- Change a password.

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.

The password must meet the following requirements:

- A minimum length of 9 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:

- **Dashboards**
 - **Health**
 - Systems
 - Alerts
 - Capacity
 - **Activities**
 - Systems
 - Audit
 - **System Management**
 - **Search and Recovery**
-

Note

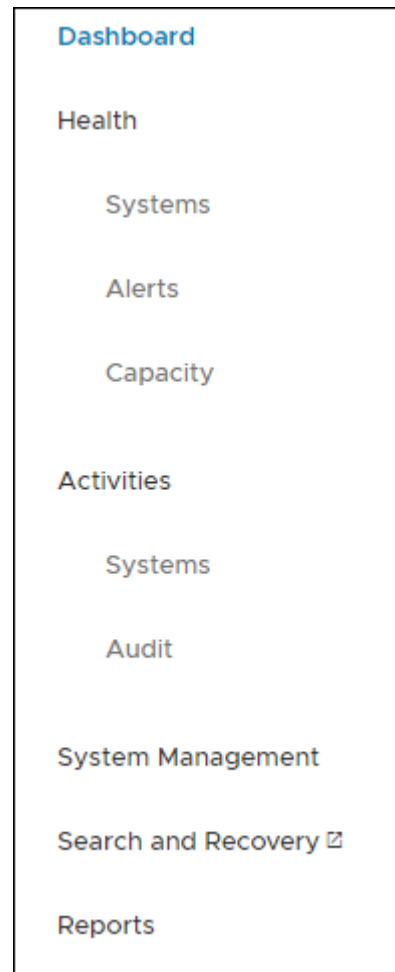
The **Search and Recovery** link is disabled when a Search system is not successfully configured in IDPA System Manager.

- **Reports**
-

Note

The **Reports** link is disabled when an Data Protection Advisor system is not successfully configured in IDPA System Manager.

Figure 4 Left menu



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.

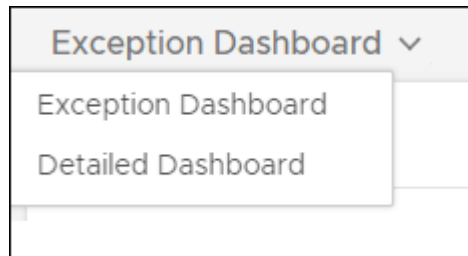
Choose another Dashboard menu

The **Choose another Dashboard** menu provides the capability for you to select a different dashboard to view.

Note

The **Choose another Dashboard** menu name is always the name of the dashboard that is selected.

Figure 5 Choose another Dashboard menu



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.
- **System Filter**—Appears in the user interface header.
- **Widget filters**—Appear in widgets.

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.

System Filter

The **System Filter** can be used to filter by one or more groups and systems.

[Group Management](#) on page 67 provides information on organizing systems into groups.

The **System Filter** appears in widgets and in the header on the following pages:

- **Health > Systems**
- **Health > Alerts**
- **Health > Capacity**
- **Activities > Systems**

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

When the **System Filter** is enabled, the icon appears blue and enclosed in a circle.

Widget filters

Widget filters can be used to filter the information that appears in a widget.

All widgets include a **System Filter**.

Some widgets provide the ability for you to filter by reporting period. You can specify one of the following options:

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

When you use a dashboard widget to access a page, the information that is displayed is automatically filtered based on the widget settings. In contrast, when you use the **Left** menu to access a page, the information that is displayed is unfiltered or is filtered based on a previously set **System Filter**.

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

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.

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.

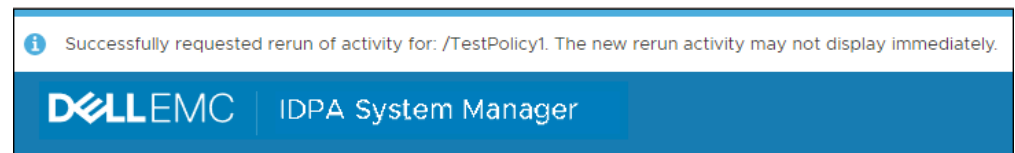
Dialog boxes

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 6 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 7 Overflow button



CHAPTER 3

Dashboards

Learn about IDPA System Manager Dashboards.

Topics include:

- [Dashboards overview](#)..... 26
- [Drill down pages](#)..... 26
- [Widgets and key performance indicators](#)..... 26
- [Change the reporting period for a widget](#)..... 28
- [Refresh the dashboard](#)..... 28
- [Filter systems for a dashboard widget](#)..... 29
- [Add a dashboard](#)..... 29
- [Editing a dashboard](#)..... 30
- [Delete a dashboard](#)..... 31
- [Toggle between full screen and normal screen](#)..... 31

Dashboards overview

IDPA System Manager dashboards provide at a glance insight into operational behavior.

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

- Backup Activities
- Replication Activities
- Capacity
- Health
- Alerts

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

Dashboard widgets include a **System Filter** that provides the capability for you to filter by one or more systems or groups. Some widgets allow you to change the reporting period.

There are two default dashboards:

- **Exception Dashboard**
- **Detailed Dashboard**

You can add, edit, and delete dashboards as required.

A maximum of 20 dashboards are supported.

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. 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.

Widgets and key performance indicators

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. There are also IDPA System Manager specific KPIs.

The following table lists the KPIs that are available for each widget type in the default dashboards.

Table 5 Widget KPIs in the default dashboards

Widget	KPIs
Backup activities	The following KPIs are available in the Exception Dashboard : <ul style="list-style-type: none"> • Failed

Table 5 Widget KPIs in the default dashboards (continued)

Widget	KPIs
	<ul style="list-style-type: none"> • Completed with exceptions <p>The following KPIs are available in the Detailed Dashboard:</p> <ul style="list-style-type: none"> • Success Percent • Failed • Completed with exceptions • Running • Completed • Total
Replication activities	<p>The following KPIs are available in the Exception Dashboard:</p> <ul style="list-style-type: none"> • Failed • Completed with exceptions <p>The following KPIs are available in the Detailed Dashboard:</p> <ul style="list-style-type: none"> • Success Percent • Failed • Completed with exceptions • Running • Completed • Total
Alerts	<p>The following KPIs are available in the Exception Dashboard:</p> <ul style="list-style-type: none"> • Errors • Warnings <p>The following KPIs are available in the Detailed Dashboard:</p> <ul style="list-style-type: none"> • Warnings • Errors • Informational
Capacity	<p>The following KPIs are available in the Exception Dashboard and Detailed Dashboard:</p> <ul style="list-style-type: none"> • Percentage of capacity utilized • Systems crossed capacity threshold • Capacity of the top 3 highest utilized systems <p>For each of the top 3 highest utilized systems, the following are displayed:</p> <ul style="list-style-type: none"> ▪ Total used ▪ Total capacity ▪ Percentage of capacity utilized

Table 5 Widget KPIs in the default dashboards (continued)

Widget	KPIs
Health	<p>The following KPIs are available in the Exception Dashboard:</p> <ul style="list-style-type: none"> • Number of unhealthy systems • Number of systems not reporting <p>The following KPIs are available in the Detailed Dashboard:</p> <ul style="list-style-type: none"> • Number of unhealthy systems • Number of systems not reporting • Number of good systems

Note

In IDPA System Manager, the activity status information is based on the Policy rather than the individual client. As a result, the number of activities listed in IDPA System Manager does not match the number of activities reported in Avamar Administrator. To compare activity status in IDPA System Manager to Avamar Administrator, add up the number of clients in each Policy for the particular activity status and time frame. The Troubleshooting chapter provides more information.

Change the reporting period for a widget

The reporting period for a widget is displayed in the bottom left corner of the widget. To change the reporting period for a widget, perform the following procedure.

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. Click the reporting period.
A menu appears that displays all of the available reporting period options.
2. Select one of the reporting period options.
The widget updates with the selected reporting period information.

Refresh the dashboard

Dashboard widgets are automatically refreshed every five minutes.


To manually refresh the dashboard, click the  button.

Filter systems for a dashboard widget

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

Procedure

1.

In the dashboard widget that you want to filter the systems for, click the  button.

The **System Filter** dialog box appears.

2. To add groups or systems to the filter, perform the following steps:

a. Select one or more groups or 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 groups or systems are added to the filter.

3. 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

4. Click **APPLY**.

The widget refreshes and displays only information for the selected groups or systems.

Add a dashboard

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

A total of 20 dashboards are supported.

Procedure

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



The **Add Dashboard** dialog box appears.

2. Type a name for the dashboard.
3. Select one of the following dashboard templates:
 - **Exception Dashboard**
 - **Detailed Dashboard**
4. (Optional) To set this dashboard as the default dashboard, select **Set as default dashboard**.
5. 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 widgets to a selected dashboard template

IDPA System Manager provides the capability for you to reset the widget settings to a selected dashboard template.

Resetting the widget eliminates any filtering that was specified.

Procedure

1. Select the dashboard that you want to edit.

2. Click .

The **Edit Dashboard** dialog box appears.

3. Select **Reset widgets to selected dashboard templates**.

The **Edit Dashboard** dialog box refreshes and displays the **Exception Dashboard** and **Detailed Dashboard** templates.

4. Select the **Exception Dashboard** template or the **Detailed Dashboard** template.
5. In the **Type RESET to confirm** field, type **RESET**.
6. Click **SAVE**.

Delete a dashboard

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

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.

Toggle between full screen and normal screen.

In the **Dashboard**, you can toggle the display between full and normal screen mode.

When you are in normal screen mode, to enter full screen mode, click .

Note

Full screen mode hides the header and **Left** menu.

When you are in full screen mode, to return to normal screen mode, click .



CHAPTER 4

Health

Learn about IDPA System Manager Health.

Topics include:

- [Health overview](#) 34
- [Health > Systems page](#) 34
- [Health > Alerts page](#) 38
- [Health > Capacity page](#) 40

Health overview

IDPA System Manager health includes information about system status, alerts, and capacity for systems that are configured in IDPA System Manager.

This information is used to determine the health state of the system.

Capacity information appears for Avamar and Data Domain systems only.

Health > Systems page

On the **Health > Systems** page, you can view the health state of all systems that are configured in IDPA System Manager.

To view additional information about the health of a system, in the list of systems, select the row that the system appears in. The additional information for the selected system appears in the **Detail** pane.

Dismiss health alerts to clear the alerts from IDPA System Manager and change the system **Alerts** health component status to **Good**. [Dismiss alerts](#) on page 40 provides instructions.

Avamar system health information

The **Health > Systems** page displays information about the health of an Avamar system.

Note

Alerts that have been acknowledged in Avamar Administrator are removed from IDPA System Manager.

System health information on the Master pane

The following information is listed in the **Master** pane for Avamar system health.

System Type

The type of system.

System Name

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

Version

The Avamar 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 seven data points to determine the health of an Avamar system. 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 capacity of the system that is used 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.
- **NotReporting**—An Avamar system health status is updated to **NotReporting** when the connection between IDPA System Manager and the Avamar system is offline for an interval of equal to or greater than five minutes. IDPA System Manager checks whether the Avamar system is back online each minute.
- **Unhealthy**—If any of the data points that are used to determine the health of an Avamar system are not successful, the Avamar system health status is updated to **Unhealthy**.

System 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 Verification
- License
- SSO

Note

The SSO health status reflects the Data Protection Central 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.

If the SSO component shows an X, to reregister single sign on, click **SSO**, and then click **REREGISTER**.

A check mark represents success. An X represents failure.

Click on a component for more information about the status.

System Information

A summary of the following information:

Last Garbage Collection—Reports whether garbage collection was successful in the last 24 hours.

HFS Verified Status

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

- **Last Checkpoint**—Reports whether there was an HFS checkpoint in the last 24 hours.
- **Last Checkpoint Validation**—Reports whether HFS checkpoint validation occurred in the last 24 hours.

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.
- **Capacity**—The total amount of used and available storage.

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 system health information

The **Health > Systems** page displays information about Data Domain system health.

Note

Alerts that have been acknowledged in Data Domain System Manager are removed from IDPA System Manager.

System health information on the Master pane

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

System Type

The type of system.

System Name

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

Version

The Data Domain 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 three data points to determine the health of a Data Domain system. 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 system that is used is less than or equal to 80%.
 - The system has no errors or warning alerts.
- **NotReporting**—A Data Domain system is updated to the **NotReporting** status when a IDPA System Manager Data Domain activity cannot communicate with the Data Domain system. IDPA System Manager checks whether the Data Domain system is back online each minute.
- **Unhealthy**—If any of the three data points that are used to determine the health of a Data Domain system are not successful, the Data Domain system health status is updated to **Unhealthy**.

System 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

A check mark represents success. An X represents failure.

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.
- **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.

Health > Alerts page

On the **Health > Alerts** page, alerts from all systems that are configured in IDPA System Manager are reported in a table.

Avamar health alerts information

The **Health > Alerts** page displays information about Avamar system alerts.

Note

Alerts that have been acknowledged in Avamar Administrator are removed from IDPA System Manager.

The following list displays the types of information that are available for Avamar system alerts.

System Type

The type of system.

System Name

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

Level

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

- Error
- Warn

Avamar types of Warning and Error are displayed in IDPA System Manager with the Level of Error.

Category

The category of the alert.

Created Date

The date on which the alert was created.

Message

A description for the alert.

Data Domain health alerts information

The **Health > Alerts** page displays information about Data Domain system alerts.

Note

Alerts that have been acknowledged in Data Domain System Manager are removed from IDPA System Manager.

The following list displays the types of information that are available for Data Domain system alerts.

System Type

The type of system.

System Name

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

Level

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

- Error
- Informational
- Warn

IDPA System Manager maps Data Domain alerts as follows:

- Alert—Error
- Critical—Error
- Debug—Informational
- Emergency—Error
- Error—Error
- Info—Informational
- Notice—Informational
- Warning—Warn

Category

The category of the alert.

Created Date

The date in which the alert was created.

Message

A description for the alert.

IDPA System Manager alerts information

The **Health > Alerts** page displays information about IDPA System Manager system alerts.

The following list displays the types of information that are available for IDPA System Manager system alerts.

System Type

The type of system.

System Name

This field shows **DPC Server** for IDPA System Manager alerts information.

Level

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

- Error

- Informational
- Warn

Category

The category of the alert.

Created Date

The date on which the alert was created.

Message

A description for the alert.

Dismissing alerts

You can dismiss alerts from IDPA System Manager.

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 **Health > 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 **Activities > Audit** page.

Health > Capacity page

On the **Health > Capacity** page, you can view the capacity state of all Avamar and Data Domain systems that are configured in IDPA System Manager. Capacity monitoring can keep you apprised of unexpected data growth that may cause downstream failures.

To view additional information about a system, in the list of systems, select the row that the system appears in. The additional information for the selected system appears in the **Detail** pane.

Avamar health capacity information

The **Health > Capacity** page displays information about Avamar system capacity.

Health capacity information on the Master pane

The following information is listed on the **Master** pane for Avamar system capacity.

System

The type of system.

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 in GB.

Available

The amount of storage that is available in GB.

Total Capacity

The total amount of used and available storage.

Health capacity information on the Detail pane

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

Health Summary

Displays the last date and time the database was updated.

Capacity

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

- **Total Capacity**—The total amount of used and available storage.
- **Usage**—The amount of the storage that is used in GB.
- **Metadata**—The percentage of the storage that is used for metadata.
- **Available**—The amount of storage that is available in GB.

Forecast

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

Data Domain health capacity information

The **Health > Capacity** page displays information about Data Domain system capacity.

Health capacity information on the Master pane

The following information is listed on the **Master** pane for Data Domain system capacity.

System

The type of system.

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 in GB.

Available

The amount of storage that is available in GB.

Total Capacity

The total amount of used and available storage.

Health capacity information on the Detail pane

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

Health Summary

Displays the last date and time the database was updated.

Capacity

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

- **Total Capacity**—The total amount of used and available storage.
- **Usage**—The amount of the storage that is used in GB.
- **Metadata**—The percentage of the storage that is used for metadata.
- **Available**—The amount of storage that is available in GB.

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 in GB.
- **Status**—The status of the MTree.

CHAPTER 5

Activities

Learn about IDPA System Manager Activities.

Topics include:

- [Activities overview](#) 44
- [Activities > Systems page](#) 44
- [Activities > Audit page](#) 47

Activities overview

IDPA System Manager Activities include system activity and audit information.

System activity includes information about backup and replication activities for Avamar systems connected to 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 > Systems page

On the **Activities > Systems** page, activities from all systems that are monitored in IDPA System Manager can be viewed in the **Master** pane, in a table.

To view additional information about an activity, in the **Master** pane, select the row that the activity appears in. The additional information for the selected activity appears in the **Detail** pane.

For Avamar systems, you can view a list of clients that are associated with an activity. For Avamar systems only, you can rerun backup and replication activities.

Avamar activities systems information

The **Activities > Systems** page displays information about Avamar system activities.

Consider the following when reading Avamar information on the **Activities > Systems** page.

Number of activities may not match Avamar Administration

In IDPA System Manager, the activity status information is based on the Policy rather than the individual client. As a result, the number of activities listed in IDPA System Manager does not match what is reported in the Avamar Administrator user interface.

To compare activity status in IDPA System Manager to Avamar Administrator, add up the number of clients in each Policy for the particular activity status and time frame. The Troubleshooting chapter provides more information.

Avamar activity information on the Master pane

The following information is listed in the **Master** pane table for Avamar system activities.

System Type

The type of system.

System Name

The name that is defined in IDPA System Manager.

Activity 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:

- Completed
- Failed
- Completed with exceptions
- Running

Activity Name

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

Started

The date and time that the activity started.

Ended

The date and time that the activity ended.

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 Type**—The type of system.
- **Policy Type**—The type of policy.
- **Schedule**—The schedule that is associated with the policy.

Clients

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

- **Clients Failed**—The number of clients that failed.
- **Clients Active**—The number of clients that are active.
- **Clients Completed**—The number of clients that completed.
- **Clients with Exceptions**—The number of clients that have exceptions.
- **Clients Pending**—The number of clients that have a status of pending.
- **Number of Clients**—The number of clients that are associated with the activity.

Targets

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

- **Target Type**—The target type for the activity.
- **Target Name**—The target name for the activity.
- **Total Size**—The total size of the activity.

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 activity

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

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 **Activities > Systems**.
2. On the **Master** pane, select the row for the Avamar activity that you want to rerun.
3. Click , and then click **Rerun Activity**.

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

View the list of clients that are associated with an activity

IDPA System Manager provides the capability for you to view the list of clients that are associated with an activity.

Procedure

1. In the **Left** menu, select **Activities > Systems**.
2. Filter the list of activities, and then select a row in the table.
The **Detail** pane displays additional information about the selected activity.
3. Click **VIEW CLIENTS**.

The **Clients** page appears. The **Clients** page includes in the **Master** pane a table that displays information about the selected activity for each client.

Activities > Clients page

On the **Activities > Clients** page, activities from clients that are associated with an Avamar activity are listed in the **Master** pane.

To view additional information about an activity, in the **Master** pane, select the row that the activity appears in. The additional information for the selected activity appears in the **Detail** pane.

Avamar clients information

The **Activities > Clients** page displays information about Avamar clients.

Activity information on the Master pane

The following information is listed on the **Clients** page in the **Master** pane.

Client Name

The name that is associated with the client.

Status

The status of the activity.

Started

The date and time that the activity started.

Ended

The date and time that the activity ended.

Activity information on the Detail pane

Select a row in the **Master** pane to display additional information about a client. The following information is listed in the **Detail** pane table for clients.

System Type

The type of system that the client is protected by.

Activity Type

The type of activity that the client is associated with.

Status

The activity status information.

Status Message

If applicable, a status message associated with the activity.

Started

The date and time that the activity started.

Ended

The date and time that the activity ended.

Bytes Processed

The total number of bytes processed.

Bytes Modified

The total number of bytes modified.

Files Modified

For file system backups, the total number of files modified.

Files Processed

For file system backups, the total number of files processed.

Activities > Audit page

On the **Activities > 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 **Activities > 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 **Activities > 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 6

System Management

Learn about IDPA System Manager **System Management**.

Topics include:

- [System Management overview](#)..... 50
- [Avamar system management](#)..... 50
- [Data Domain system management](#)..... 62
- [Data Protection Advisor system management](#)..... 63
- [Search system management](#)..... 65
- [Reregister SSO for a system](#)..... 66
- [Group Management](#)..... 67

System Management overview

System Management provides the capability for you to add, edit, remove, and manage systems 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 in to 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.
 - View existing clients that are associated with an Avamar system.
 - View client backups.
- When an Avamar system is not reporting, you can reactivate messaging.

Avamar system management

IDPA System Manager includes capabilities to manage Avamar systems.

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** dialog box appears.

The **Add System** dialog box appears.

3. In the **Type** list box, select **Avamar**.
4. Specify the following connection information:
 - **Name**—You can specify any name that helps identify the system.
 - **Hostname**—Specify the fully qualified domain name (FQDN) of the Avamar system.
 - **Avamar Username**—The username is MCUser.
 - **Avamar Password**—The password is the MCUser password.
 - **OS Root password**—The password is 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 **SAVE**.

The **System Management** page refreshes and displays the new system.

Edit an Avamar system

After an Avamar system is added, if required, you can edit the system details.

Procedure

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

Reactivate messaging for an Avamar system

If an Avamar system is displaying the health status of `NotReporting`, reactivating messaging may be required.

Procedure

1. On the **System Management** page, select the Avamar system that you want to reactivate messaging for.

2. Click , and then click **Reactivate**.

The health status changes to `Activating`.

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

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 policies for Avamar systems



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

You can also select a policy, and then perform a backup now.

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.  Click , 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.

Add a 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.  Click , 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.



Edit a policy

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

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. 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.


Delete a policy

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

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.

Perform a backup now

IDPA System Manager provides the capability for you to select a backup, and then perform a backup immediately.

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 , and then click **Manage Policies**.

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

4. 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 **Activities > Audit** or the **Activities > Systems** page.

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.  Click , 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.



Edit a retention

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

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 **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.



Delete a retention

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

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

The **Confirm Delete** dialog box appears.

7. Click **DELETE**.


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

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.

Edit a schedule



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

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.

Delete a schedule



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

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

The **Confirm Delete** dialog box appears.

7. Click **DELETE**.

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

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.



Edit a dataset

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

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 dataset

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

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

The **Confirm Delete** dialog box appears.



7. Click **DELETE**.

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

View clients for Avamar systems

IDPA System Manager provides the capability for you to view clients for Avamar systems.

Procedure



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

The **Managed Clients** page appears.

View client backups

IDPA System Manager includes the capability to view client backups.

Procedure

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

The **Managed Clients** page appears.

4. From the list of clients, select the client for which you want to view the list of backups.

In the **Detail** pane, the **BACKUPS** button appears.

5. Click **BACKUPS**.

The **Managed Clients > Backups** page appears.

6. (Optional) To view additional information about a backup, select a row.

Delete an Avamar system

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

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Avamar 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 an Avamar system, a message deactivation activity appears on the **Activities > Audit** page.

Data Domain system management

IDPA System Manager includes capabilities to manage Data Domain systems.

Add a Data Domain System

Procedure

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

2. Click .

The **Add System** dialog box appears.

3. In the **Type** list box, select **Data Domain**.
4. Specify the following connection information:
 - **Name**—You can specify any 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 **SAVE**.

The **System Management** page refreshes and displays the new system.

Edit a Data Domain system

After a Data Domain system is added, if required, you can edit the system details.

Procedure

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

3. Click .

The **Edit System** dialog box appears.

4. Edit the system details.
5. Click **SAVE**.

Delete a Data Domain system

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

Note

If you delete a Data Domain that is still attached to an Avamar system that IDPA System Manager is monitoring, the Data Domain is automatically added back to IDPA System Manager.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Data Domain 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.

Data Protection Advisor system management

IDPA System Manager includes capabilities to manage Data Protection Advisor systems.

Note

You can configure only one Data Protection Advisor system with IDPA System Manager at a time.

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. In the **Type** list box, select **Data Protection Advisor**.
4. Specify the following connection information:

- **Name**—You can specify any name that helps identify the system.
 - **Hostname**—Specify the Fully Qualified Domain Name (FQDN) of the Data Protection Advisor system.
 - **Username**—The username that is used to log in to the Data Protection Advisor user interface.
 - **Password**—The password that is used to log in to the Data Protection Advisor user interface.
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 **SAVE**.

The **System Management** page refreshes and displays the new system.

Successfully adding a Data Protection Advisor system enables the **Reports** link in the **Left** menu. The **Reports** link can be used to launch Data Protection Advisor in a new browser tab.

Edit an Data Protection Advisor system

After an Data Protection Advisor system is added, if required, you can edit the system details.

Note

If you must change the hostname of an existing Data Protection Advisor system, you must delete the system and re-add it with the new hostname.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Data Protection Advisor system.

3. Click .

The **Edit System** dialog box appears.

4. Edit the system details.
5. Click **SAVE**.

Delete an Data Protection Advisor system

If an Data Protection Advisor system is no longer required, you can delete the system.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Data Protection Advisor system.

3. Click .
The **Confirm Delete** dialog box appears.
4. Click **DELETE**.
The system is removed.

Search system management

IDPA System Manager includes capabilities to manage Search systems.


Note

You can configure only one Search system with IDPA System Manager at a time.

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** dialog box appears.
3. In the **Type** list box, select **Data Protection Search**.
4. Specify the following connection information:
 - **Name**—Specify any name that identifies the Search system.
 - **Hostname**—Specify the fully qualified domain name (FQDN) of the Search system.
 - **Username**—The username that is used to log in to the Search user interface.
 - **Password**—The password that is used to log in to the Search user interface.
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 **SAVE**.
The **System Management** page refreshes and displays the new system.

Successfully adding a Search system enables the **Search and Recovery** link in the **Left** menu. The **Search and Recovery** link can be used to launch Search in a new browser tab.


Edit a Search system

After a Search system is created, if required, you can edit the system details.

Note

If you must change the hostname of an existing Search system, you must delete the system and re-add it with the new hostname.

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Search system.
3. Click .


The **Edit System** dialog box appears.

4. Edit the system details.
5. Click **SAVE**.

Delete a Search system

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

Procedure

1. In the **Left** menu, select **System Management**.
2. Select the Search system.
3. Click .

The **Confirm Delete** dialog box appears.

4. Click **DELETE**.

The system is removed.

Reregister SSO for a system

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

Procedure

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



3. Click **Reregister SSO**.

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

Group Management

IDPA System Manager includes capabilities to organize systems into groups. Groups are useful to apply 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 filter.

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

- To clear all systems from the filter, click:



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

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

- Click:



The systems are removed from the filter

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. Click 

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 group or systems listed in the **Available** pane, use the search bar.

- b. Click:



The systems are added to the filter.

7. To remove systems from the filter, perform one of the following action sequences:

- To clear all systems from the filter, click:



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

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

- Click:



The systems are removed from the filter

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 7

Launching System Management Applications

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

This chapter includes the following topics:

- [Launching Avamar Administrator](#) 72
- [Launching Avamar AUI](#) 73
- [Launching Data Domain System Manager](#) 74
- [Launching Search](#) 75
- [Launching Data Protection Advisor](#) 75

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 > Systems**
- **Health > Alerts**
- **Health > Capacity**
- **Activities > Systems**
- **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 > Systems**
- **Health > Capacity**
- **Activities > Systems**

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:

- **Activities > Systems**
- **Managed Clients**
- **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:

- **Activities > Systems**
- **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 > Systems**
- **Health > Alerts**
- **Health > 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 > Systems**
- **Health > Capacity**
- **Activities > Systems**

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**.
2. Select the Search system.
3. In the **Detail** pane, 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**.
2. Select the Data Protection Advisor system.
3. In the **Detail** pane, 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 8

Reports

Learn about IDPA System Manager reports.

Topics include:

• Reports overview	78
• Run a report	78
• View the last report	79
• Backup Report Card	79
• Backup Client Summary	79
• Strike Summary	80
• Backup Data Backed Up Daily	80
• Backup Number of Jobs Backed Up Daily	81
• Data Domain Utilization	81
• Data Domain Tier Utilization	81
• Data Domain Daily Compression Statistics	81
• Data Domain Filesystem Utilization	82
• Data Domain DeDuplication Ratio	82
• Data Domain Active Streams	82

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 63 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.

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 9

Server Administration

Learn about IDPA System Manager server administration.

This chapter includes the following topic:

- [Change the IDPA System Manager IP address](#).....84

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
```

CHAPTER 10

Upgrading IDPA System Manager

Learn about upgrading from a previous release to IDPA System Manager 18.1.

This chapter includes the following topics:

- [Upgrade IDPA System Manager to version 18.1 on standalone server or virtual machine](#)..... 86
- [Install the IDPA System Manager OS update](#)..... 87
- [Migrating from Multiple Systems Management to IDPA System Manager](#)..... 87

Upgrade IDPA System Manager to version 18.1 on standalone server or virtual machine

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

Before you begin

Ensure that the system being upgraded meets the following requirements:

- Standalone server deployments require 1.5GHz processor.
- Virtual machine deployments require 2 CPUs with 1 core each.
- 6GB of RAM.
- 250 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 8u160 or greater is installed (packages `java-1_8_0-openjdk`, `java-1_8_0-openjdk-headless`, and `javapackages-tools`).

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, and time zone are configured.
- The environment is using static network settings.

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 18.1 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 18.1, type the following command:

```
java -jar emc-dpc-18.1.0-<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.

Install the IDPA System Manager OS update

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

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

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 7.4.1 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 11

Troubleshooting

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

Topics include:

• Directory structure and log information	90
• Troubleshooting LDAP	90
• Systems fail to activate	93
• Avamar systems fail to activate	94
• Secure storage	94
• Unlock a IDPA System Manager user account	96
• The SSO service fails to start on IDPA System Manager	96
• Disabling SSO	97
• Number of activities listed in IDPA System Manager does not match Avamar Administrator	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 `systemctl` 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.

Troubleshooting LDAP

Learn how to diagnose and resolve common LDAP configuration issues.

Checking the LDAP connection status

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 6 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.

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 **Activities > 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.

System misconfiguration. /etc/apache2/vhosts.d/vhost-ssl.conf not found

This message appears for Avamar version 7.4.1 without the required hotfix installed. The supported version of Avamar 7.4.1 is with 7.4.1-58_HF299182_48 hotfix.

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**.

Secure storage

IDPA System Manager includes a secure storage lockbox that is used to encrypt and store the system credentials of the systems IDPA System Manager monitors and manages.

When the secure storage is created, an encrypted secure storage password must be specified. The password is used along with System Stable Values (SSVs) to create an encryption key. The secure storage uses this encryption key to encrypt the system credentials.

Secure storage password requirements

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

Reset the secure storage

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

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-elg stop
bin/elgcli -reset -lockbox -password {original_password}
sudo service msm-elg start
```

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

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

Remove the secure storage

In certain situations, you may need to remove the secure storage, for example, when resetting the secure storage 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 secure storage, 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 secure storage, each system must be edited to enter the login credentials and store them in the secure storage.

Create the secure storage

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

Note

Each system must be edited to enter the login credentials and store them in the secure storage.

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
systemctl stop dpc-elg
bin/elgcli -create -lockbox -password
<secure_storage_password>
cd /var/lib/dpc/security/
chown dpc:dpc clp_lb.lb*
systemctl start dpc-elgsudo service dpc-elg start
```

The secure storage 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

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-sservice` file for editing by running the following command:

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

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

For example:

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

5. Save and close the `dpc-sservice` 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-sservice /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.
4. Restart the ELG service using the following command:

```
systemctl restart msm-elg.service
```

Results

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

Number of activities listed in IDPA System Manager does not match Avamar Administrator

In IDPA System Manager, the activity status information is based on the Policy rather than the individual client. As a result, the number of activities listed in IDPA System Manager does not match what is reported in Avamar Administrator. To compare activity status in IDPA System Manager to Avamar Administrator, add up the number of clients in each Policy for the particular activity status and time frame.

In IDPA System Manager, the clients are listed in the **Activities > Systems** page on the detailed pane. You can use the **Last 24 hours** time filter in both IDPA System Manager and Avamar Administrator to compare the information.

For example, if you run ten Policies with two clients each in the last 24 hours and each operation completes successfully, the IDPA System Manager Dashboard shows a **Completed** count of ten while the Avamar Administrator Dashboard would show a **Succeeded** count of 20.

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.

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.