

EMC Backup & Recovery Manager

Version 1.3

User Guide

302-002-003

REV 08

Copyright © 2012-2017 Dell Inc. or its subsidiaries. All rights reserved.

Published May 2017

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, 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.

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

CONTENTS

Figures		9
Tables		13
Preface		15
Chapter 1	Getting Started	19
	Product architecture.....	20
	IPv6 support.....	21
	Requirements.....	21
	Backup & Recovery Manager server software requirements.....	22
	Operating system software requirements for the Avamar and NetWorker adaptors.....	22
	Mobile application requirements.....	22
	Backup & Recovery Manager server installation requirements.....	23
	System requirements.....	24
	Data storage requirements.....	25
	Browser requirements.....	25
	Display requirements.....	25
Chapter 2	User Interface	27
	Backup & Recovery Manager user interface.....	28
	Header and Status bars.....	29
	Backup & Recovery Manager for Mobile.....	29
	Mobile security and access.....	30
	Mobile navigation, views, sorting and filtering.....	31
	Actions available for mobile.....	32
	Details on mobile.....	33
	Obtain the Backup & Recovery Manager mobile application.....	34
	Using online help.....	34
	Viewing context sensitive help.....	35
	Enable single sign-on.....	35
	Enabling Single sign-on.....	36
	Selecting the Avamar system from Preferences > Product launch links.....	36
	Exporting the security certificate to the Avamar system.....	37
	Importing the certificate to the Avamar server.....	41
	Launching Avamar applications.....	42
	Web browser authentication using Apache.....	43
	Using search.....	43
	Viewing search results.....	44
	Errors and Warnings pop ups.....	45
	Views menu filters.....	47
	Common views.....	47
	Alerts views.....	48
	Activities views.....	48

	Events views.....	49
	Systems views.....	51
	Exporting data to CSV.....	51
Chapter 3	Installation	53
	Installing the Backup & Recovery Manager server.....	54
	Installing the Backup & Recovery Manager server on a VM.....	54
	Installing the Backup & Recovery Manager server on physical hardware.....	56
	Upgrade to Backup & Recovery Manager 1.3.....	57
	Migrate data to Backup & Recovery Manager 1.3 and later.....	57
	Resetting the firewall rules after migration.....	58
	Copy the current certificate to Backup & Recovery Manager 1.3 or later.....	58
	The temporary password is printed in the log files after migration....	59
	Build to build upgrade of the Backup & Recovery Manager server.....	59
	Upgrading to the current Backup & Recovery Manager server.....	59
	Regenerate the SSL certificates.....	61
	Changing the network parameters post installation.....	61
	Backup & Recovery Manager adaptor installation.....	62
	Backup & Recovery Manager adaptor for Avamar installation and upgrade.....	62
	NetWorker adaptor installation and upgrade on Windows and Linux..	68
	Adding a Data Domain system.....	76
	Logging in to the Backup & Recovery Manager.....	76
	Reestablishing an expired session.....	79
	Disable the Backup & Recovery Manager adaptor for Avamar.....	79
	Disabling the Backup & Recovery Manager adaptor for Avamar 7.0 and earlier.....	80
	Disabling the Backup & Recovery Manager adaptor for Avamar 7.1 and later.....	80
	Uninstalling the Backup & Recovery Manager adaptor.....	80
	Uninstalling the Avamar adaptor.....	81
	Uninstalling the NetWorker adaptor.....	81
Chapter 4	Alerts	83
	Overview of Alerts.....	84
	System Summary.....	84
	Alerts columns.....	85
	Alert categories.....	86
	Excluding and including columns from the Alerts display.....	86
	Viewing repeated alerts.....	87
	Hiding alerts.....	88
	Viewing hidden alerts.....	88
	Unhiding alerts.....	89
	Acknowledging alerts.....	89
Chapter 5	Activities	91
	Overview of Activities.....	92
	Activities columns.....	92
	Excluding and including columns from the Activities display.....	92
	Activities details.....	93

	Avamar backup activity details summary.....	94
	NetWorker backup activity details summary.....	95
	Starting, stopping, and restarting backup jobs.....	97
	Avamar replication.....	98
	Avamar replication fields.....	98
Chapter 6	Events	101
	Overview of Events.....	102
	Events columns.....	102
	Events categories.....	102
	Excluding columns from the display.....	103
	View repeated events.....	103
	Hide events.....	104
	View hidden events.....	104
	Unhide events.....	105
Chapter 7	Systems	107
	Systems usage graph.....	108
	Systems Display.....	108
	Excluding columns from Systems.....	110
	Launching the native system consoles.....	110
	Managing Data Domain systems.....	114
	Removing a system.....	117
	Adding or modifying customer information.....	118
Chapter 8	Configuration	119
	Overview of Configuration.....	120
	Excluding and including columns from Configuration.....	120
	Adding or modifying Avamar replication jobs.....	121
	Starting and stopping Avamar replication jobs.....	125
	Disabling and enabling replication jobs.....	125
Chapter 9	Settings	127
	Introduction to settings.....	128
	User Administration.....	128
	Users.....	128
	Roles.....	131
	Preferences.....	133
	Date/Time Format.....	133
	Database.....	134
	Product launch links.....	135
	Security.....	136
	Changing a password.....	138
	Resetting the admin password.....	139
Chapter 10	Reports	141
	Types of reports.....	142
	Running a report.....	142
	Report Options.....	145
	Timeframe Options.....	145
	Display Options.....	146
	Status Options.....	146

	Report Content Options.....	146
	Exporting reports.....	147
Appendix A	Security Configuration	149
	Communication security.....	150
	Port usage.....	150
	Network encryption.....	151
	Cryptographic modules in the Backup & Recovery Manager.....	151
	Login, session, and password protection.....	152
	Invalidating ssh keys for login, disabling direct login for extra accounts, and removing deprecated accounts.....	153
	Firewall rules.....	153
	REST API.....	154
	Data security.....	154
	Access control.....	154
	Default accounts.....	154
	Authentication configuration.....	154
	User authorization.....	154
	Component access control.....	155
	Certificate management.....	155
	Web browser authentication using Apache.....	156
	Installing a self-signed or trusted certificate.....	156
	Creating a private key.....	157
	Generating a certificate signing request.....	158
	Changing the Backup & Recovery Manager Apache from self- signed to issued.....	158
Appendix B	Troubleshooting	163
	Managing the Backup & Recovery Manager server.....	164
	The regroup-alerts-events script.....	164
	Running the regroup-alerts-events script.....	164
	Customizing the log rotation policy schedule	165
	Adaptor log file location.....	165
	View log files.....	166
	Apache web server log files.....	166
	Tomcat log files.....	166
	Mongo database log file.....	167
	Backup & Recovery Manager application log files.....	167
	The bundlelogs utility.....	167
	Bundlelogs utility options.....	168
	Running the bundlelogs utility.....	168
	NetWorker adaptor options.....	168
	Editing adaptor options on Windows.....	168
	Editing adaptor options on Linux.....	169
	NetWorker adaptor command line options.....	169
	Avamar adaptor control script.....	174
	Backup & Recovery Manager error messages.....	175
Appendix C	Disaster Recovery	177
	Clone a Virtual Machine in the vSphere Client.....	178
	Prerequisites.....	178
	Cloning the Backup & Recovery Manager server.....	178
	Recovering the Backup & Recovery Manager server.....	179
	Re-registering the Avamar or NetWorker servers if required.....	179

Glossary

181

CONTENTS

FIGURES

1	Backup & Recovery Manager product architecture.....	20
2	Backup & Recovery Manager user interface.....	28
3	Header bar.....	29
4	Status bar.....	29
5	Mobile enabled.....	30
6	Mobile dashboard.....	30
7	Mobile device navigation.....	31
8	Sort fields.....	32
9	Mobile filters.....	32
10	Supported mobile actions.....	33
11	Drill down details.....	33
12	Backup & Recovery Manager help.....	34
13	Available Avamar systems.....	36
14	Avamar system.....	37
15	Security certificate information.....	38
16	Certificate details.....	39
17	Certificate Export Wizard.....	39
18	Certificate export status.....	40
19	Security exception information.....	40
20	Launch icon.....	42
21	Specify the Avamar system.....	43
22	Search list.....	44
23	Search results.....	45
24	Errors.....	46
25	Ten most recent warnings.....	47
26	Alerts views.....	48
27	Activities views.....	49
28	Events views.....	50
29	Systems views.....	51
30	Avamar Enterprise Manager.....	63
31	Go to Package Page status.....	64
32	Avamar Installation Manager.....	66
33	Hostname validation.....	66
34	Hostname Validation message.....	66
35	Overwrite prompt.....	72
36	Upgrade information.....	72
37	Setup wizard.....	72
38	Installation Directory.....	73
39	Installation prompt.....	74
40	Installation status.....	74
41	Installation completion.....	75
42	Login window.....	77
43	Failed login.....	77
44	Change Password window.....	78
45	Expired login session.....	79
46	Logout status.....	79
47	Alerts summary chart.....	84
48	Worst Systems.....	85
49	Worst Systems.....	85
50	Worst system launch.....	85
51	Sort Alerts columns.....	87
52	Repeated Alerts.....	87
53	Expanded repeated Alerts.....	87

54	Hide Alerts.....	88
55	View previously hidden Alerts.....	88
56	Hidden Alerts.....	89
57	Acknowledge Alerts.....	90
58	Dismiss Alerts.....	90
59	Sort Activities columns.....	93
60	Backup activity details.....	94
61	NetWorker backup activity details.....	95
62	Message text.....	96
63	Show backups since: options.....	97
64	Start, Stop and Restart permission.....	97
65	Start, Restart and Stop backup jobs.....	98
66	Sort Events columns.....	103
67	List repeated Events.....	104
68	Hide events.....	104
69	View Hidden	105
70	Hidden Events.....	105
71	Unhide Selected events.....	106
72	System Usage graph.....	108
73	Available systems.....	108
74	System details.....	109
75	Avamar System details with Meta Data usage graph.....	109
76	Available columns.....	110
77	Launch the Management Console.....	111
78	Java Web Start.....	111
79	Avamar Administrator Logon.....	112
80	NMC logon.....	113
81	Data Domain Enterprise Manager logon.....	113
82	Data Domain system.....	114
83	Manage Data Domain Systems.....	114
84	Add a Data Domain System.....	115
85	Connection failed error.....	115
86	Successful connection test.....	115
87	Change Data Domain credentials.....	116
88	Change Credentials fields.....	116
89	Test Connection window.....	117
90	Remove Data Domain systems.....	117
91	Remove the selected system prompt.....	118
92	Customer Information.....	118
93	Configuration columns.....	121
94	Avamar Target system.....	121
95	Avamar systems list.....	122
96	Replication schedule.....	122
97	Timeout and Limit network bandwidth fields.....	123
98	Available options for backup retention.....	123
99	Backup Clients.....	124
100	Completion status.....	124
101	Change status.....	124
102	Configuration error.....	124
103	Start a replication.....	125
104	Replication started.....	125
105	Settings menu.....	128
106	User Administration.....	128
107	Add a user.....	129
108	Edit an existing user.....	129
109	Login failed	131

110	Modify Administrator role error.....	132
111	New role.....	132
112	Role Privileges.....	133
113	Preferences.....	133
114	Date/Time Format options.....	134
115	Percentage Used setting.....	135
116	Database options.....	135
117	Product Launch Links.....	136
118	Manually set the User Inactivity Timeout.....	137
119	Change the login screen warning message.....	137
120	New login screen warning message.....	138
121	Change Password.....	138
122	New password fields.....	139
123	Report types.....	143
124	Report system options.....	143
125	Backup Summary report options.....	144
126	System Summary report options.....	144
127	Capacity usage report chart.....	144
128	Expired login session.....	153

FIGURES

TABLES

1	Revision history.....	15
2	Style conventions.....	16
3	Backup & Recovery Manager architecture.....	20
4	Data storage requirements.....	23
5	Hyper-V virtual machine requirements.....	23
6	Non-clustered memory, CPU, and disk.....	24
7	Data storage requirements.....	25
8	Backup & Recovery Manager user interface sections	28
9	Header components	29
10	Available help menu options	35
11	Common views filters.....	47
12	Alerts views filters.....	48
13	Activities views filters	49
14	Events views filters.....	50
15	Systems views filters	51
16	Data storage requirements.....	56
17	Installation Progress details.....	64
18	NetWorker adapter location.....	68
19	Alerts icons.....	84
20	Alerts columns.....	85
21	Alert categories.....	86
22	Backup details systems columns.....	92
23	Avamar backup details systems fields	94
24	NetWorker backup details systems fields	95
25	Avamar replication activities fields	98
26	Avamar replication details summary fields	99
27	Events section columns.....	102
28	Event categories	102
29	System types and states.....	109
30	Avamar replication configuration columns.....	120
31	Backup Retention options.....	123
32	User roles.....	131
33	Product Launch Links option.....	136
34	Available reports by system type	142
35	Report option icons	145
36	Default ports using the TCP protocol.....	150
37	Encryption strategies.....	151
38	Cryptographic modules.....	151
39	Default account names and passwords.....	154
40	Built-in user roles.....	155
41	Log file locations.....	166
42	Apache log files.....	166
43	Tomcat log files.....	166
44	Mongo logs.....	167
45	Backup & Recovery Manager logs.....	167
46	Bundlelogs utility usage.....	168
47	NetWorker adaptor options	169
48	Avamar adaptor control script	174
49	Backup & Recovery Manager error codes.....	175

TABLES

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 describes how to install, configure, and administer Backup & Recovery Manager.

Audience

This document is intended for the host system administrator, system programmer, or operator who will be involved in managing Backup & Recovery Manager for Avamar or NetWorker deployments.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
08	May 2017	Added the following content: <ul style="list-style-type: none">• Passwords cannot include the \$ character at the beginning or middle of the password.• It is recommended that you change the default password for the following users:<ul style="list-style-type: none">▪ admin▪ dpn▪ gsan▪ root▪ ucas• Instructions about how to invalidate ssh keys for login, disable direct login for extra accounts, and remove deprecated accounts.
07	January 2016	Adapter installation updates.
06	December 2015	Bugs addressed.
05	October 2015	Bugs addressed.

Table 1 Revision history (continued)

Revision	Date	Description
04	September 2015	Illustration updates.
03	September 2015	New NetWorker build information.
02	August 2015	NetWorker 9.0 functionality included.
01	June 2015	Initial release of this Backup & Recovery Manager User Guide.

Related documentation

The following provide additional information:

- Backup & Recovery Manager Release Notes
- Backup & Recovery Manager Sizing and Configuration Guide
- Avamar, Data Domain, DDBEA, NetWorker and ProtectPoint Compatibility Guide
You can access the Compatibility Guide from the Support website at <http://compatibilityguide.emc.com:8080/CompGuideApp/>.
- Avamar documentation
- NetWorker documentation

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.

Table 2 Style conventions (continued)

<code>Monospace bold</code>	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

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

Where to find product documentation

- <https://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 the following button:



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 the following button:



Live chat

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

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

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

Getting Started

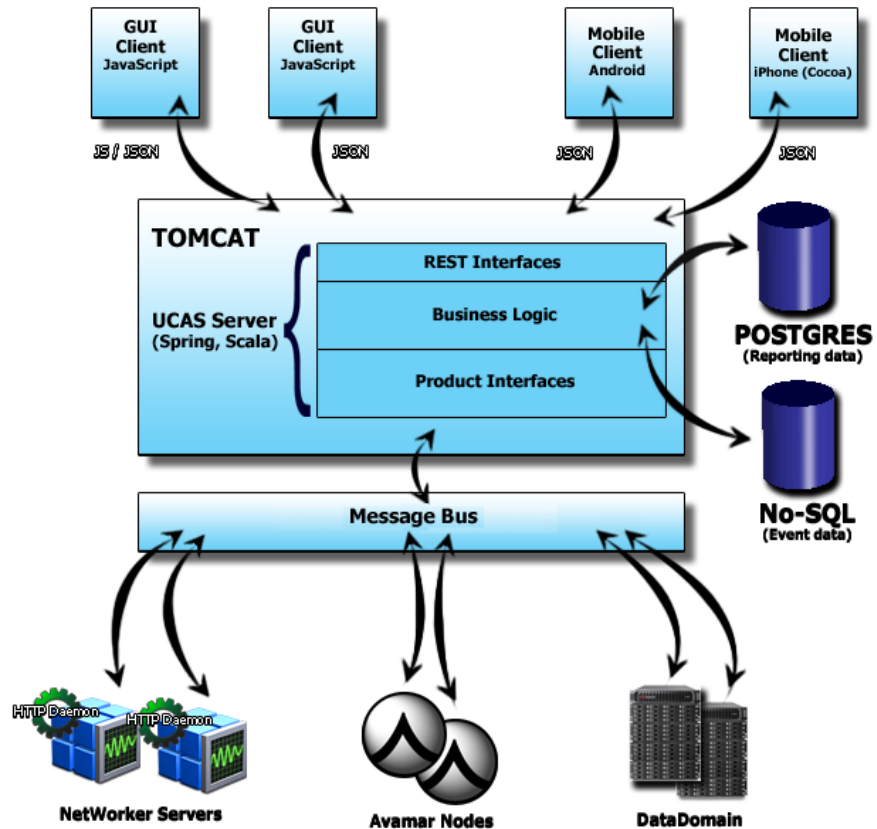
Backup & Recovery Manager runs in a server, supporting Avamar and NetWorker servers and Data Domain backup targets. The Backup & Recovery Manager runs on both physical or virtual servers. Avamar and NetWorker adaptors are installed on the respective Avamar & NetWorker systems to transmit messages and information over the message bus to be viewed in the Backup & Recovery Manager UI.

- [Product architecture](#).....20
- [IPv6 support](#)..... 21
- [Requirements](#)..... 21

Product architecture

The following figure illustrates the components of the Backup & Recovery Manager and the data flow.

Figure 1 Backup & Recovery Manager product architecture



The following table lists the components that make up the Backup & Recovery Manager architecture.

Table 3 Backup & Recovery Manager architecture

Component	Description
Client layer	Javascript, HTML
Application server	Deployed as a virtual application (OVA), or on a physical server
Storage layer	Used for storing reporting and monitoring data
Product layer	<ul style="list-style-type: none"> NetWorker adaptor binary on Windows and Linux with a proxy option (NetWorker releases 7.6.x and later) Avamar adaptor – Java on the Avamar grid (6.0 SP2, 6.1 and 6.1 SP1)

Table 3 Backup & Recovery Manager architecture (continued)

Component	Description
	<ul style="list-style-type: none"> Data Domain – SSH tunneling

Complete details on the supported versions of the Avamar and NetWorker software are available in the respective online software compatibility guides:

- The *Avamar Compatibility and Interoperability Matrix*
- The *NetWorker Software Compatibility Guide*

IPv6 support

Backup & Recovery Manager, a web service that is accessed through a browser is certified and supported in a dual-stack IPv4/IPv6 network environment. Avamar and NetWorker servers and browsers with either IPv4 or IPv6 addresses can communicate with the Backup & Recovery Manager server.

NOTICE

A pure IPv6 environment is not currently a supported configuration for a Backup & Recovery Manager server, however there are actions that allow this configuration to work.

If you choose to run in a pure IPv6 environment, the following actions are necessary:

- **Deployment:**
After the Backup & Recovery Manager server OVA is deployed, use the `yast lan` command as root from the VMware console to manually configure the IPv6 networking and IPv6 DNS servers.
- **Web access:**
When accessing Backup & Recovery Manager that is deployed on a dual-stack enabled network from an IPv6 web browser, ensure the network path from the browser to the BRM server supports IPv6 from end to end. Test the IP connection by using one of the following methods:
 - The `ping6` utility from the desktop to the IPv6 address of the Backup & Recovery Manager server.
 - Verify the connection with the network administrator.
If the IPv6 path is available from end to end, the Backup & Recovery Manager appliance can be accessed by surrounding the IPv6 address with square brackets [] and specifying the application path.
For example, if the IPv6 address of Backup & Recovery Manager is `2620:0:170:718:250:56ff:fe96:f998`, then the URL for access is `https://[2620:0:170:718:250:56ff:fe96:f998]/brm/` for initial login. This URL provides full, normal access to Backup & Recovery Manager.

Requirements

There are minimum hardware and software requirements that must be met to successfully deploy and install the Backup & Recovery Manager software.

Ensure that all current operating system patches or updates are installed.

Backup & Recovery Manager server software requirements

The Backup & Recovery Manager server can be installed on both a virtual host (vApp) and a physical host by using the SLES native installer.

- Minimum required versions for the Virtual Application (vApp):
 - ESXi
 - ESX 5.1, 5.5 and 6.0
 - VCenter Server 5.0 and 6.0
 - VSphere Client 5.0 and 5.1
- Native installer for SLES Linux:
 - The bootable .iso image requires a minimum of 3.3 GB free space on a DVD.
 - Two disks (operating system and MongoDB disks)
 - A minimum of 4 CPUs
 - A minimum 8 GB of RAM
 - A minimum 110 GB Disk
 - A DHCP server must be available on the network on which the server is running for a Backup & Recovery manager deployment

Operating system software requirements for the Avamar and NetWorker adaptors

For the supported version of Avamar or NetWorker, there are minimum required operating system software versions that must run the Backup & Recovery Manager software.

Note

Backup and Recovery Manager is not supported on Avamar Extended Retention Media Access Nodes.

- Avamar 6.0 SP2, 6.1, 6.1 SP1, and later
 - SLES Linux 11
 - RHEL 4
- NetWorker 7.6 and later
 - Microsoft Windows 2003, 2008, 2008 R2, Windows 2012, Windows 2012 R2
 - SLES Linux 11
- NetWorker 9.0 and later
 - Microsoft Windows 2003, 2008, 2008 R2, Windows 2012, Windows 2012 R2
 - Linux x64

Mobile application requirements

The Backup & Recovery Manager is available for use on mobile devices.

- The Backup & Recovery Manager mobile apps require Backup & Recovery Manager 1.2 or later server.

- The Backup & Recovery Manager mobile application is compatible with the following mobile devices:
 - iPad 2, iPad 3rd generation and later
 - iPad mini (iOS 6 and later)
 - Android version 3.1 and later on Android tablets

Backup & Recovery Manager server installation requirements

The Backup & Recovery Manager server (OVA) raw database is a temporary buffer for storing messages until they are processed.

Near the end of a Hyper_V or physical installation using ISO, the Backup & Recovery Manager server post installation script displays a premature login prompt.

The following four post-install scripts run:

- 01_OS_post_script.sh
- 02_BRM_UPGRADER_post_script.sh
- 03_BRM_INSTALLER_post_script.sh
- 04_CLEANUP_post_script.sh

While the 3rd script (03_BRM_INSTALLER_post_script) is running, the security patch installation of the new OS kernel displays a login prompt while the last of the updates are applied. When the post-install scripts complete, a reboot occurs.

Disregard the login prompt and wait for the process to complete and reboot rather than attempting to login at the prompt.

The following table provides Backup & Recovery Manager server memory requirements.

Table 4 Data storage requirements

Component	Memory per component (disk space)
Memory	8 GB

[Hardware requirements for the Hyper_V virtual machine](#) provides the minimum disk recommendations for the Backup & Recovery Manager server.

Hardware Requirements for the Hyper-V virtual machine

There are memory and storage requirements specific to the Backup & Recovery Manager server installation in Hyper-V virtualization.

The following table lists the memory and storage requirements for the Hyper-V machine.

Table 5 Hyper-V virtual machine requirements

Component	Requirement
Operating System platforms	Windows 2008 R2, Windows 2012, Windows 2012 R2.
Memory	The Backup & Recovery Manager server requires a minimum of 8200 MB of memory for Hyper-V configuration. However, it is recommended to provide 8700 MB of memory for the virtual machine to accommodate virtualization overhead.

Table 5 Hyper-V virtual machine requirements (continued)

Component	Requirement
Server storage	<ul style="list-style-type: none"> Provision the virtual machine with 2 IDE controllers (In Hyper-V it is not possible to boot from a SCSI controller). Provision two hard drives to attach to Controller 0: <ul style="list-style-type: none"> Hard Drive 1 (operating system) requires a minimum of 40 GB Hard Drive 2 (Mongodb) requires a minimum of 70 GB Connect the ISO image with Backup & Recovery Manager to a CD drive on Controller 1.
BIOS	Map the ISO image to the DVD drive on Controller 1. List CD first in the Startup Order section in the BIOS tab for the virtual machine by using the up/down arrows to adjust the order. If this is set incorrectly, the virtual machine does not find the ISO boot image to begin installation.
Network	<ul style="list-style-type: none"> A DHCP server must be available on the network on which the Hyper-V server is running for a Backup & Recovery Manager deployment. Ensure that the Enable virtual LAN identification option is not checked (enabled) in the Network Adapter tab for the virtual machine. If this option is enabled, it interferes with the virtual machine's ability to correctly use DHCP protocols.

System requirements

The following table lists the recommended and minimum required memory, CPU, and disk for the Backup & Recovery Manager server components.

Table 6 Non-clustered memory, CPU, and disk

	Memory	CPU	Disk
Recommended	8 GB	4 core, 2 GHz	1 TB
Minimum required	8 GB	4 core, 2 GHz	500 GB

Thin provisioning is an alternative for storage capacity for virtual disk allocation.

The following lists the available formats in which to store the virtual disk:

- Thick Provision Lazy Zeroed: (recommended) - Lazy Zero can take some time to initialize, although not as long as Eager Zero. The storage capacity for the entire virtual disk is allocated on the datastore at virtual disk create time if thick provisioning is selected. Thick provisioning does not fill the whole drive unless eager zeroed is selected.

- **Thick Provision Eager Zeroed:** Eager Zero yields the best performance, but also takes the most time to initialize. Pre-zeros all blocks on of the virtual disk on the datastore in advance.
- **Thin Provision:** Thin provisioning means that the capacity on the datastore is allocated to the virtual disk as required, up to the full size of the virtual disk and only uses what it needs. This is the fastest to initially deploy, but it is possible to over-allocate the datastore and if a co-resident VM fills up disk, space on the datastore can be exhausted and cause the other VMs using it to be blocked until space is released. If you choose this option make sure you do not over allocate disk in the datastore selected.

Data storage requirements

The Backup & Recovery Manager server (OVA) raw database is a temporary buffer for storing messages until they are processed. Both Avamar and NetWorker have minimum disk space requirements.

The following table provides a summary of storage requirements.

Table 7 Data storage requirements

Recommended raw storage for 24 hours of messages	Memory per server (disk space)
Avamar	50 Mb
NetWorker	2000 Mb

Note

This requirement is for both live message display and reports.

Browser requirements

There are minimum browser requirements for Google Chrome, Microsoft Internet Explorer, and Mozilla Firefox to run the Backup & Recovery Manager.

A list of browsers currently supported by the Backup & Recovery Manager is provided in:

- *The Avamar Compatibility and Interoperability Matrix*
- *The NetWorker Software Compatibility Guide*
- *The Backup & Recovery Manager Release Notes*

Note

Be sure that the pop-up blocker is turned off to allow UI and online help pop-ups.

Display requirements

The minimum recommended screen resolution is 1280 x 1024 for running the Backup & Recovery Manager in a web browser.

CHAPTER 2

User Interface

The Backup & Recovery Manager runs in a server, supporting Avamar and NetWorker servers and Data Domain backup targets. The Backup & Recovery Manager runs on a virtual server, and is now available as a mobile application for both Apple and Android tablets. Details on the Backup & Recovery mobile app and its requirements are available in [Backup & Recovery Manager mobile application](#).

- [Backup & Recovery Manager user interface](#)..... 28
- [Backup & Recovery Manager for Mobile](#)..... 29
- [Using online help](#)..... 34
- [Viewing context sensitive help](#)..... 35
- [Enable single sign-on](#)..... 35
- [Using search](#)..... 43
- [Errors and Warnings pop ups](#)..... 45
- [Views menu filters](#)..... 47
- [Exporting data to CSV](#)..... 51

Backup & Recovery Manager user interface

The Backup & Recovery Manager uses these sections to enable you to monitor Avamar, NetWorker, and Data Domain systems.

The following figure illustrates the Backup & Recovery Manager home page.

Figure 2 Backup & Recovery Manager user interface



The following table lists the sections available in the Backup & Recovery Manager user interface.

Table 8 Backup & Recovery Manager user interface sections

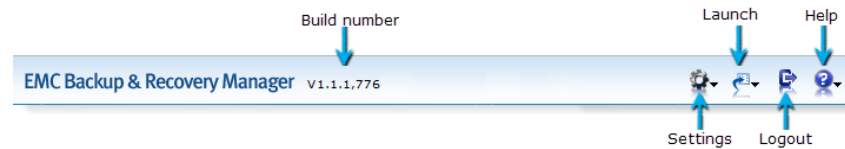
Backup & Recovery Manager tabs	Description
Alerts	View alerts from all monitored systems including backup failures, errors, warnings and media requests. Alerts often require user intervention.
Activities	View detailed information on jobs that are running, completed or queued on all monitored systems.
Events	View all events generated by monitored systems in the enterprise. The ability to filter and acknowledge events is also provided.
Systems	View detailed information for all Avamar, NetWorker, and Data Domain systems in the enterprise.
Configuration	Configure basic Avamar replication.
Reports	Run backup summary, configuration report (lists policy objects) and system summary reports for all monitored systems in the enterprise.

Header and Status bars

The Header bar provides the version and build information for the current installation of the Backup & Recovery Manager.

The following figure illustrates the information and options available on the Header bar.

Figure 3 Header bar



The following table describes the components included on the Backup & Recovery Manager Header page.

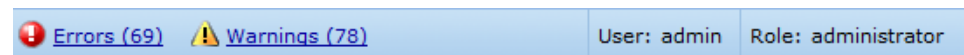
Table 9 Header components

Header component	Description
Settings	Provides access to configure settings for User Administration, Preferences, and the ability to change the password. Settings on page 127 provides complete details.
Launch	Is a quick launch option for the Avamar Client Manager, System Maintenance, and the Data Protection Advisor. Product launch links on page 135 provides complete details.
Logout	Logs the user out of the current session.
Help	Provides access to the Help Index, the product support and community pages, and details about the current installation of Backup & Recovery Manager. Using online help on page 34 provides details.

The Status bar at the bottom of the Backup & Recovery Manager window provides the number of Errors and Warnings with links to the worst systems. It also provides information on the currently logged in user and their role.

The following figure illustrates the information available on the Status bar.

Figure 4 Status bar



Backup & Recovery Manager for Mobile

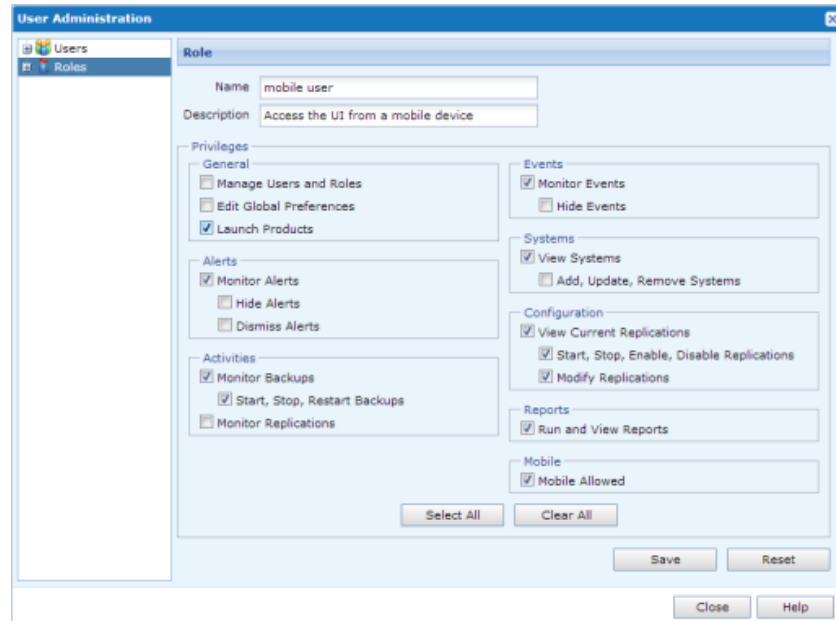
A new mobile application supporting Backup & Recovery Manager features and functionality.

Check [Requirements](#) for information on supported mobile devices and operating systems.

Mobile security and access

Mobile access is a role based privilege that is defined on the Backup & Recovery Manager server.

Figure 5 Mobile enabled



After the mobile application is installed, log in by using your Backup & Recovery Manager username and password and specifying the Backup & Recovery Manager server.

Figure 6 Mobile dashboard



The option to specify a passcode for mobile is available. Enabling a passcode provides secure access to the UI after a session timeout without having to re-enter the username and password.

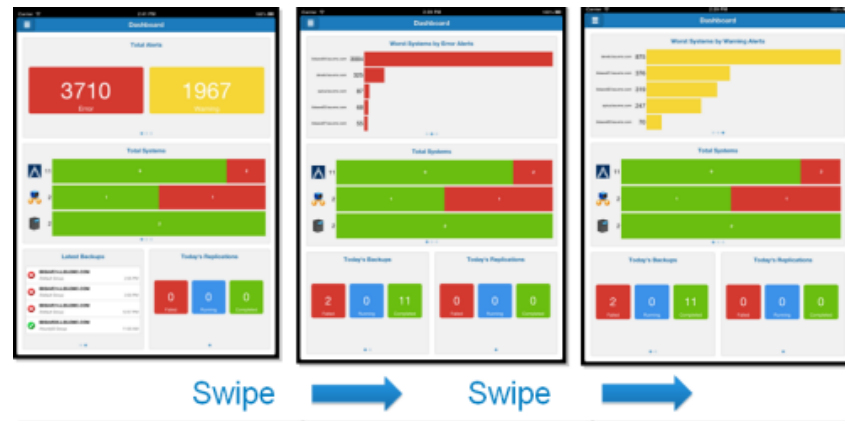
Mobile navigation, views, sorting and filtering

All the current Backup & Recovery Manager features are supported in the mobile application. User interaction supports native iOS and Android operating system swipes and taps to access multiple views and field sorting where available.

Navigation

The following is an example of Backup & Recovery Manager dashboard and how to navigate for different views.

Figure 7 Mobile device navigation



Views

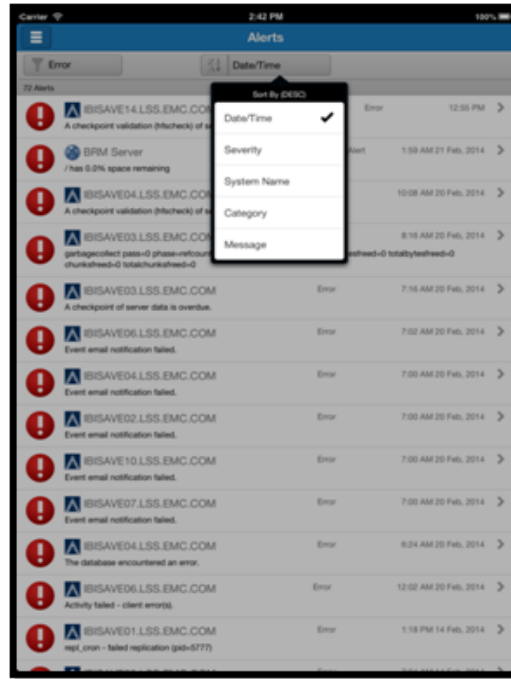
For Systems, the following display options are available by tapping the appropriate icon on the upper right hand corner of Systems:

- Tile
- List
- List/Details

Sorting

You can sort in List view by tapping in the drop-down list to select the field on which to sort.

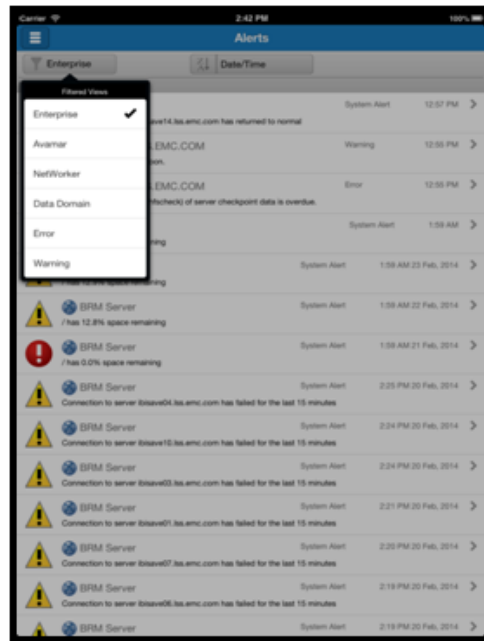
Figure 8 Sort fields



Filtering

Backup & Recovery Manager filtering views are supported for mobile. [Views filters](#) provides details on the available views.

Figure 9 Mobile filters



Actions available for mobile

Supported actions are located in the upper right corner of the UI sections that support the specified actions.

Figure 10 Supported mobile actions



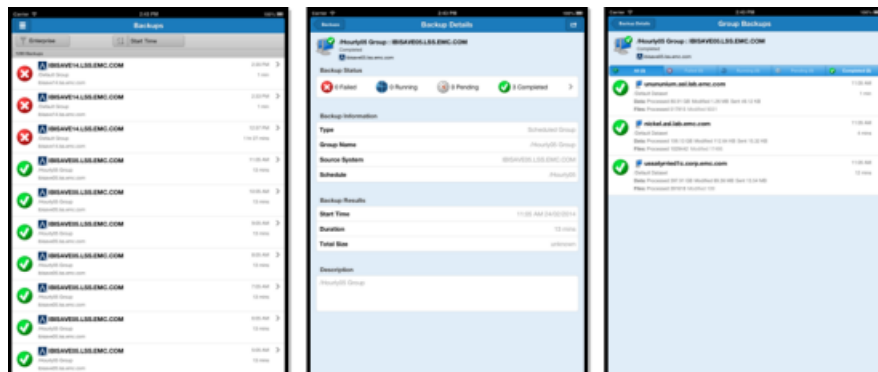
Supported actions:

- Start, Stop, Restart backups (Activities)
- Acknowledge Alerts (Alerts)
- Mail Details (Activities Backup Details)

Details on mobile

You can drill down to view additional details on the Backup & Recovery Manager mobile app by selecting the system.

Figure 11 Drill down details



Obtain the Backup & Recovery Manager mobile application

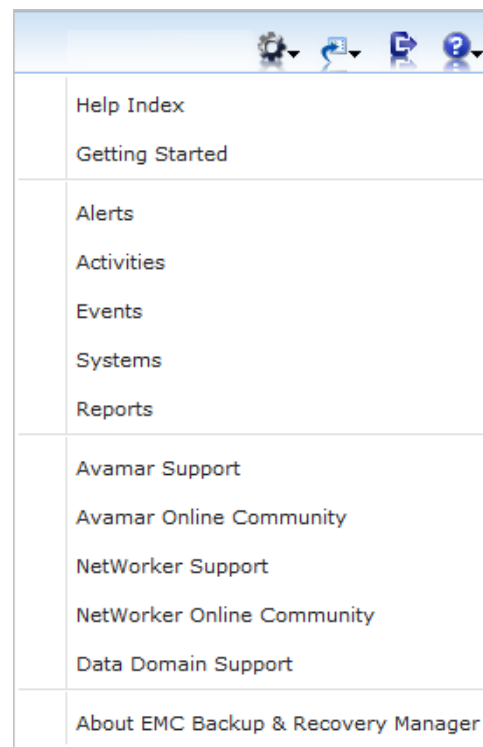
The Backup & Recovery Manager mobile application is available from the Apple App Store for iOS devices and Google Play for Android devices. You can test drive the application with canned data by using Demo mode.

Using online help


The Backup & Recovery Manager provides help for all sections of the GUI. You can view the help index from any window in the UI, and context sensitive help is available for all of the UI topics.

The following figure illustrates the help menu.

Figure 12 Backup & Recovery Manager help



Procedure

1. Click the question mark  icon in the upper right corner of the window.
2. A menu opens with the available options.
3. Select an option from the menu. The online help for the dialog opens in a new browser window.
4. Close the browser window to exit the online help.

NOTICE

Closing the browser window that contains online help does not terminate the EMC Backup & Recovery Manager session.

The following table lists the available help menu options in the Backup & Recovery Manager.


Table 10 Available help menu options

Help menu item	Description
Help Index	Opens the online help for the EMC Backup & Recovery Manager GUI.
Getting Started	Displays the Getting Started topics in a new browser window.
Alerts	Links to the Alerts topic in the online help.
Activities	Links to the Activities topic in the online help.
Events	Links to the Events topic in the online help.
Configuration	Links to the Configuration topic in the online help.
Systems	Links to the Systems topic in the online help.
Reports	Links to the Reports topic in the online help.
Avamar Support	Links to the Avamar technical support landing page.
Avamar Online Community	Links to the Avamar online community page.
NetWorker Support	Links to the NetWorker technical support landing page.
NetWorker Online Community	Links to the NetWorker online community page.
Data Domain Support	Links to the Data Domain technical support landing page.
About the Backup & Recovery Manager	Displays a dialog box that shows the current version of the application.

Viewing context sensitive help

Several topics in the Backup & Recovery Manager provide a question mark button in the title bar of the dialog box for information on the selected user interface element. Click the question mark to launch in a separate browser window the respective help topic.

Procedure

1. Click the question mark  icon in the upper right corner of the dialog box.
2. Online help for the dialog box opens in a new browser window.
3. Close the browser window to exit online help.

NOTICE

Closing the browser window that contains online help does not terminate the EMC Backup & Recovery Manager session.

Enable single sign-on

The Backup & Recovery Manager single sign-on functionality provides the ability for users to gain access to the Avamar Client Manager after logging in to the UI. As

different applications and resources support different authentication mechanisms, single sign-on internally translates and stores different credentials compared to what is used for initial authentication.

To enable single sign-on for Avamar 7.0, and Client Manager, refer to the following sections.

Enabling Single sign-on

The Preferences section of the Backup & Recovery Manager settings provides the ability for users to enable the single sign-on functionality.

Verify that **Preferences > Security > Single Sign-on > Enable Single Sign-on** is enabled. If not, click the check box to enable single sign-on.

NOTICE

Single sign-on is enabled by default at the time of installation or upgrade. If SSO is disabled, you must provide login credentials each time the Client Manager is launched from the Backup & Recovery Manager UI.

Selecting the Avamar system from Preferences > Product launch links

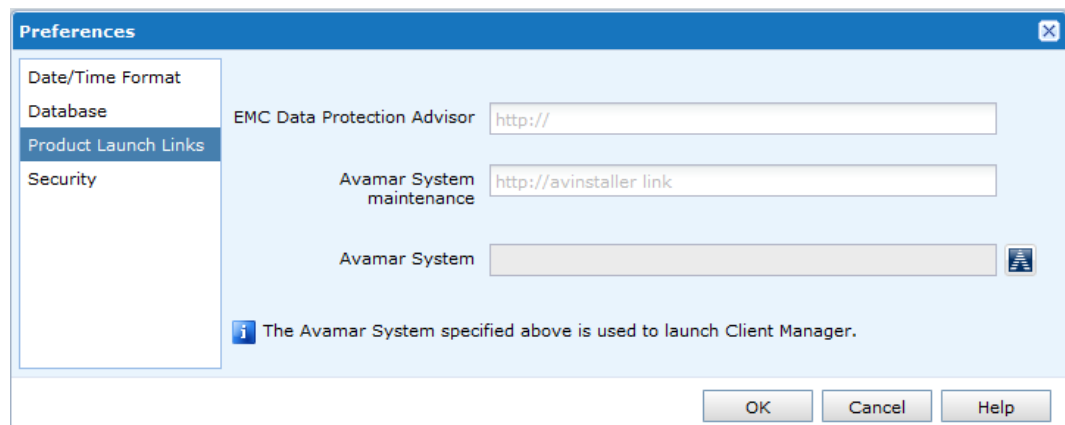
You can select the Avamar system for which to enable single sign-on in the Backup & Recovery Manager. Available Avamar systems are listed in Settings > Preferences > Product launch links.

Only users with Launch Products privileges can launch Avamar Client Manager. By default, the Administrator role has Launch Products privileges and can assign these privileges to other users.

Procedure

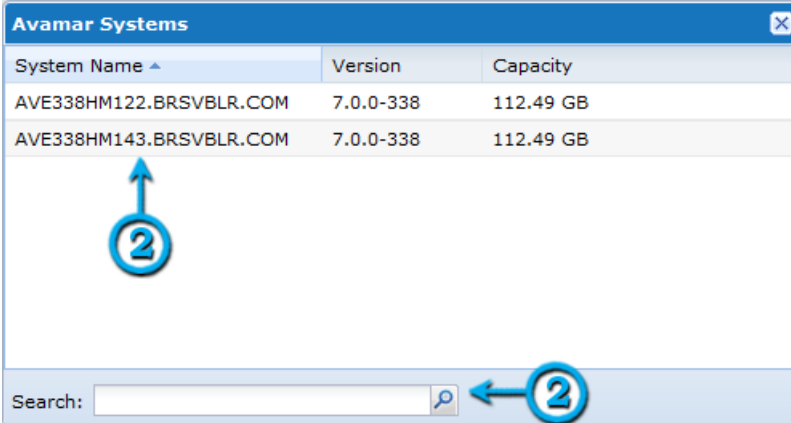
1. In **Preferences > Product Launch Links > Avamar System**, click the Avamar icon to display a list of available Avamar systems.

Figure 13 Available Avamar systems



2. Select the Avamar system from the list, or enter the Avamar system IP address, or the hostname in the search field and click the search icon.

Figure 14 Avamar system



System Name	Version	Capacity
AVE338HM122.BRSVBLR.COM	7.0.0-338	112.49 GB
AVE338HM143.BRSVBLR.COM	7.0.0-338	112.49 GB

Search:

NOTICE

The selected Avamar system is used to launch the Avamar Client Manager.

Exporting the security certificate to the Avamar system

The procedure to export the Backup & Recovery Manager security certificate to the Avamar system varies depending on the browser used.

The current *Avamar Product Security Guide* provides details on importing the security certificate on the Avamar system.

This section provides instructions on exporting the security certificate on the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

Note

If the Avamar server is at version 6.x, Single Sign-on is not supported and the logon screen for the selected Avamar program opens.

Exporting a security certificate in Google Chrome

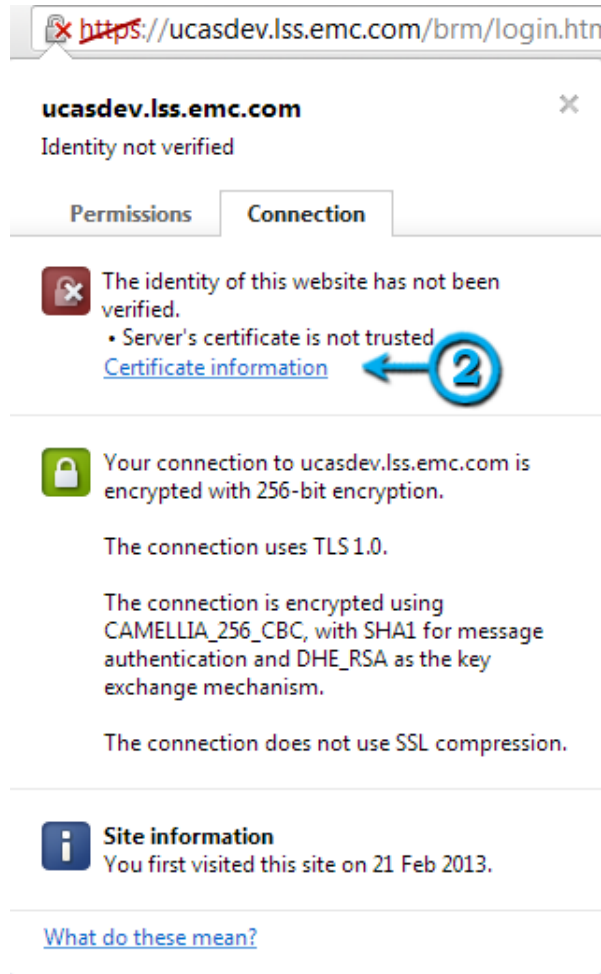
Use the Certificate Export wizard to add the appropriate security exception for the Backup & Recovery Manager on Google Chrome.

Perform the following steps to export the Backup & Recovery Manager security certificate to the Avamar system in Google Chrome.

Procedure

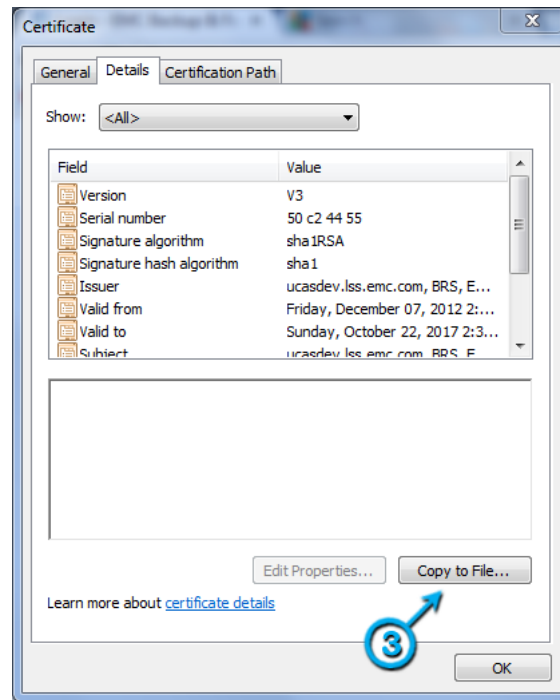
1. Click the SSL certificate padlock icon to the left of the URL in the Address bar.
2. Click **Certificate Information**.

Figure 15 Security certificate information



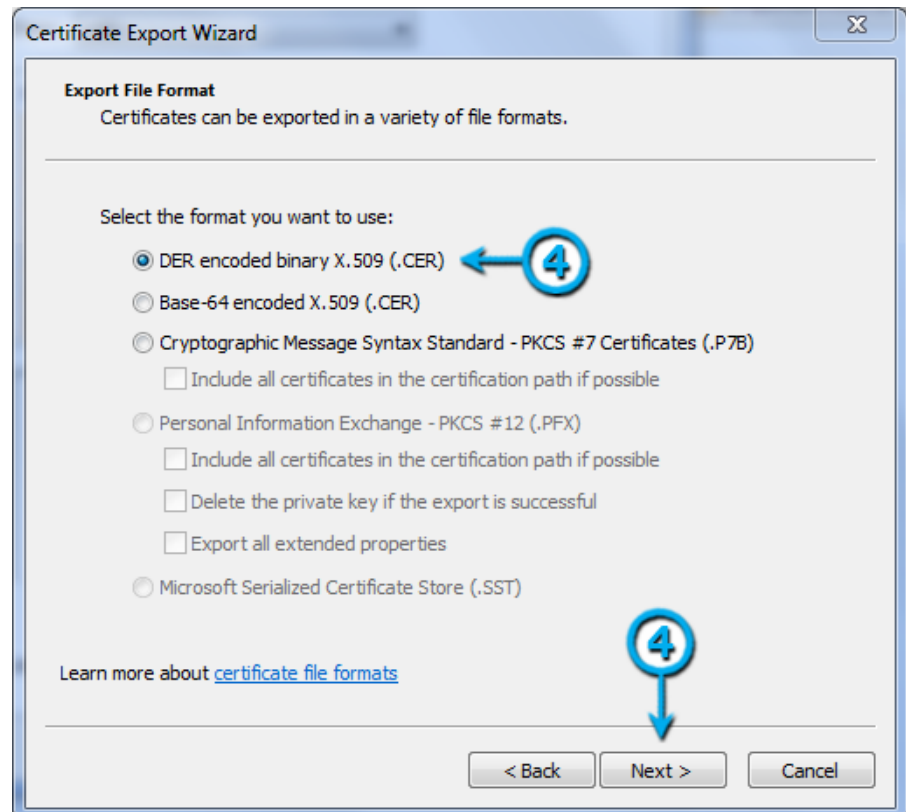
3. Click **Details** , and then click **Copy to File** to launch the wizard.

Figure 16 Certificate details



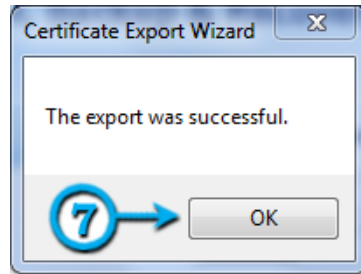
4. Select **DER encoded binary X.509** from the list, and click **Next**.

Figure 17 Certificate Export Wizard



5. Click **Browse** to select the security certificate, and click **Next**.
6. Click **Finish** to exit the wizard.
A dialog box is displayed notifying the user of the successful export operation.
7. Click **OK** to close the dialog box.

Figure 18 Certificate export status



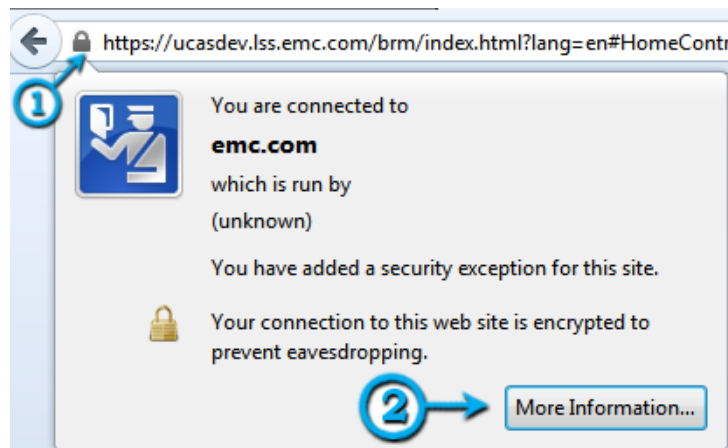
Exporting a security certificate in Mozilla FireFox

You can add the appropriate security exception for the Backup & Recovery Manager on Mozilla Firefox.

Procedure

1. Click the SSL certificate padlock icon to the left of the URL in the Address bar.
2. Click **More Information**.

Figure 19 Security exception information



3. Click **View Certificate**.
4. In the **Details** tab, click **Export**.
5. Select **X.509 Certificate (DER)** for **Save as Type**.
6. Click **Close** to exit.

Exporting a security certificate in Microsoft Internet Explorer

Use the Certificate Export wizard to add the appropriate security exception for the Backup & Recovery Manager on Microsoft Internet Explorer.

Procedure

1. Click the SSL certificate icon to the right of the URL in the Address bar.
2. Click **View Certificates**.
3. In the **Details** tab, click **Copy to File** to launch the wizard.
4. Select **DER encoded binary X.509** from the list and click **Next**.
5. Click **Browse** to select the security certificate, and click **Next**.
6. Click **Finish** to exit the wizard. A dialog box is displayed notifying the user of the successful export operation.
7. Click **OK** to close the dialog box.

Importing the certificate to the Avamar server

The Backup & Recovery Manager uses the `java keytool` command, a utility that manages/imports certificate keys. The `keytool` command is located in the Java bin directory (`/usr/java/jreVERSION/bin`), where `VERSION` is the specific Java Runtime Environment (JRE) version that is currently installed on the MCS.

NOTICE

If the security certificate that was exported from the Backup & Recovery Manager was not imported to the Avamar server, the following error message displays when attempting to launch the Avamar Client Manager:

```
{success:false, returnCode:'1', error:'The request failed.
Please see the server log or check the server status.',
title:'Unexpected Error' } 11cc301f-ecc5-497b-8333-3b647c06d958
Y2:11cc301f-ecc5-497b-8333-3b647c06d958
```

If the `/usr/java/jreVERSION/bin` directory is not in your path, either add it to the path, or specify the complete path when using `keytool`.

Procedure

1. Copy the `.keystore` from the `/root` directory of the Avamar server to a local directory.
2. Open Backup & Recovery Manager and export the certificate by clicking the lock icon on the browser tab and following the wizard.
Complete details on exporting the certificate from the Backup & Recovery Manager are available in [Exporting the security certificate to the Avamar system](#).
3. Copy the previously exported certificate to a folder in the Avamar server's root directory.
4. Verify whether or not the certificate exists in the `.keystore`:

```
keytool --list --keystore pathname.keystore
```

5. If the certificate exists, delete it by using the following command:

```
keytool -delete -alias ucashostname -keystore pathname.keystore
```

6. Import the certificate to the `.keystore`:

```
keytool --list -importcert --trustcacerts -alias ucashostname -
file Exportedcertificate -keystore pathname.keystore
```

7. Replace the `.keystore` to the Avamar server `/root` directory and restart `emtomcat`:

```
emwebapp -stop, start
```

For Avamar 7.2, you must restart the AVI application to update the keystore:

```
avinstaller.pl --stop
```

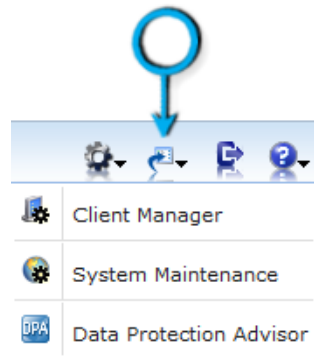
```
avinstaller.pl --start
```

8. Log in the Backup & Recovery Manager and launch the Client Manager.

Launching Avamar applications

The launch feature provides the ability to enable the CAS single-sign-on capability in Backup & Recovery Manager for Avamar Client Manager.

Figure 20 Launch icon



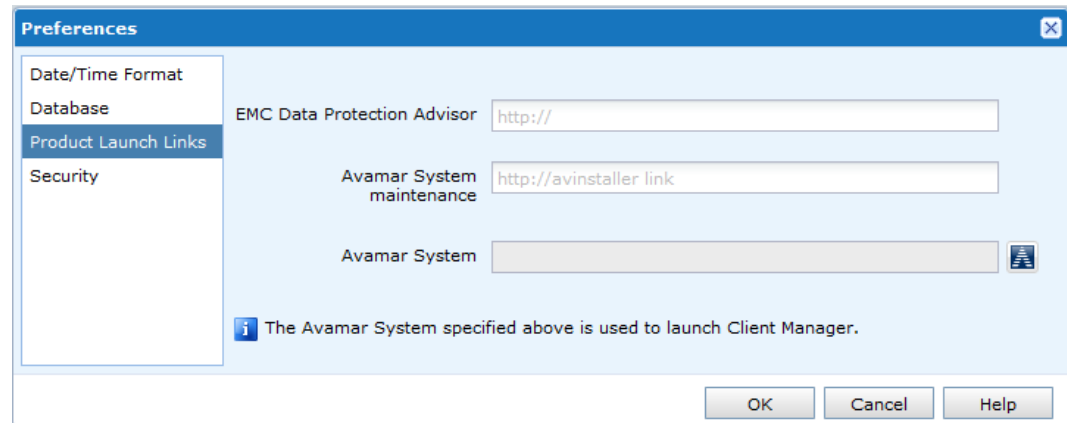
Procedure

1. Click the required option:
 - Client Manager
 - System Maintenance (AVinstaller)
2. Select the system from the list of systems available by clicking the Avamar icon.

NOTICE

Step 2 is only required if the Avamar system was not previously configured in **Settings > Preferences**.

3. Click **OK** to set the Avamar system and launch the respective UI.

Figure 21 Specify the Avamar system

Web browser authentication using Apache

The Backup & Recovery Manager server and adaptors use the Apache web server to provide a secure web browser-based user interface. Web browser connections for these applications use secure socket layer/transport layer security (SSL/TLS) to provide authentication and data security.

When a web browser accesses a secure web page from an unauthenticated web server the SSL/TLS protocol causes it to display an authentication warning. An unauthenticated web server is one that does not authenticate itself using a trusted public key certificate.

The Apache web server that is provided with the Backup & Recovery Manager is installed with a self-signed certificate, not a trusted public key certificate. The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server, but it cannot be used for authentication.

Complete details on using Apache to provide a secure web browser-based UI are available in the *Backup & Recovery Manager Release 1.1 Security Guide*.

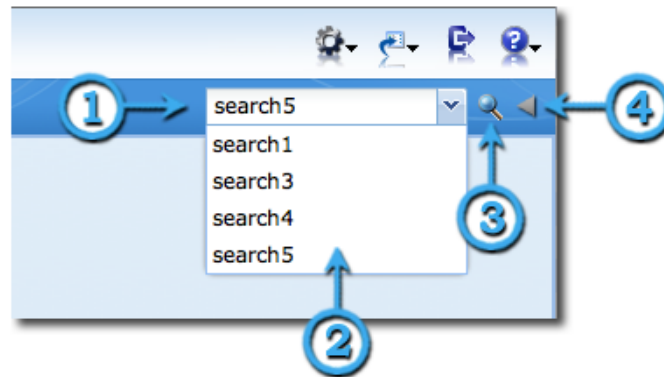
Using search

The Backup & Recovery Manager provides search functionality for every tab in the UI. Search strings are saved to enable users to access previously entered searches.

It is recommended that you use simple alphanumeric strings when using the search feature in Backup & Recovery Manager. To minimize search failures, do not use dates, times, or certain special characters. The special characters to avoid are :";-_*&^%!@#\$(+)\|<>.,?/".

Procedure

1. In the Backup & Recovery Manager, type the string for which to search in the **Search** box.
2. If applicable, click beside the search box to display a drop-down list of previous searches.
3. Click the search icon to begin the search.
4. Click the triangle to display previous search results.

Figure 22 Search list

Viewing search results

When the search completes, a window opens with the search results. You can use several categories for search summary reports.

The following lists the categories available for a search summary report:

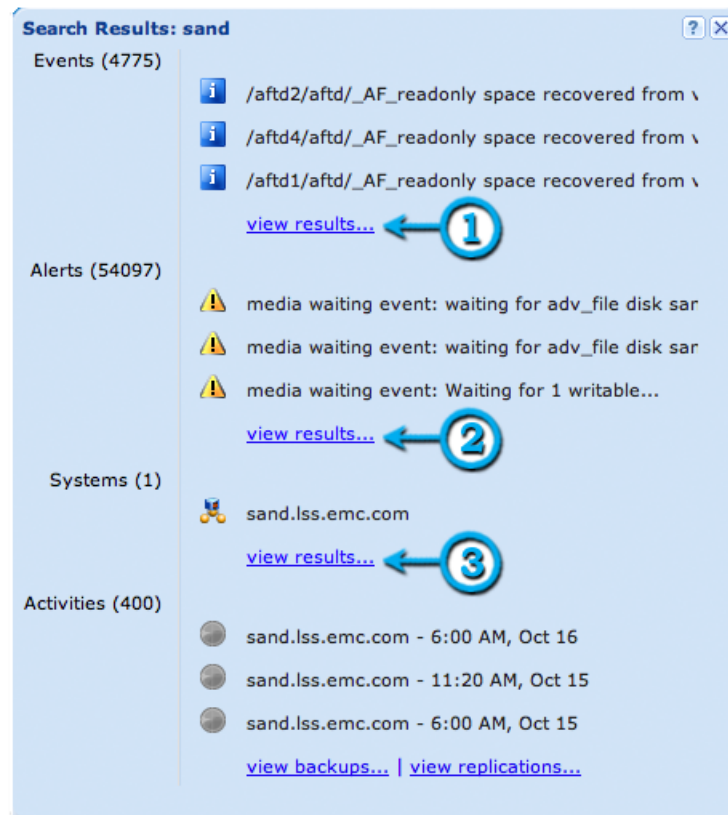
- Events
- Alerts
- Servers
- Activities

Note

The ability to sort on individual columns in any search results grid is available.

If there are results in a category, click **view results...** to display the specific results of the search.

Figure 23 Search results



Errors and Warnings pop ups

The total number of errors and warnings for all monitored systems is displayed in the lower left corner of the Backup & Recovery Manager (all sections). Click Errors (number) or Warnings (number) to open a popup window with the most recent errors and warnings (ten maximum).

This section provides details on understanding and using the errors and warnings pop ups:

- When the Backup & Recovery Manager encounters a new warning or critical alert message that has not been previously viewed, a pop up is triggered automatically. The automatic pop up displays the five most current warnings or critical alerts that might require user intervention. The Backup & Recovery Manager polls for new messages once every minute.

NOTICE

If more than five new critical alerts or warnings are found at one time since the last time polled, only the five most current messages are displayed.

- The pop ups provide an indication that an operation might need attention and provides the opportunity to determine if the alert or warning requires user intervention or if it can be ignored.

- Clicking the status bar link displays the ten most current messages for that type of alert. The messages are sorted from most recent descending to the least recent of the 10.
- All critical alerts or warning message pop ups display for 10 seconds. Move the cursor over the window to extend the display time.
- Click any message to navigate to the Alerts section. The selected message is highlighted in the alerts grid.
- Highlight the originally selected message to display it in the context of messages of a similar type.

Figure 24 Errors

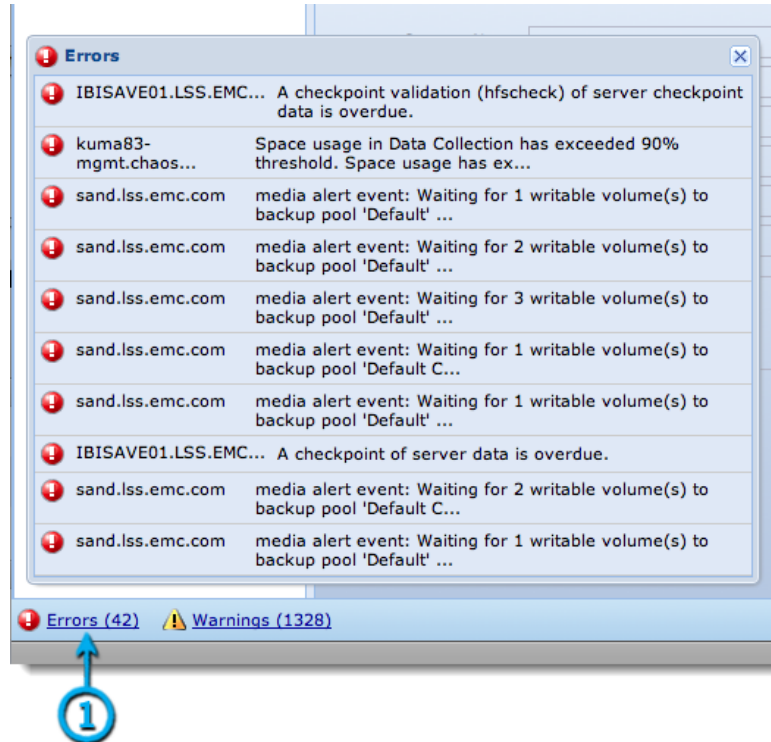
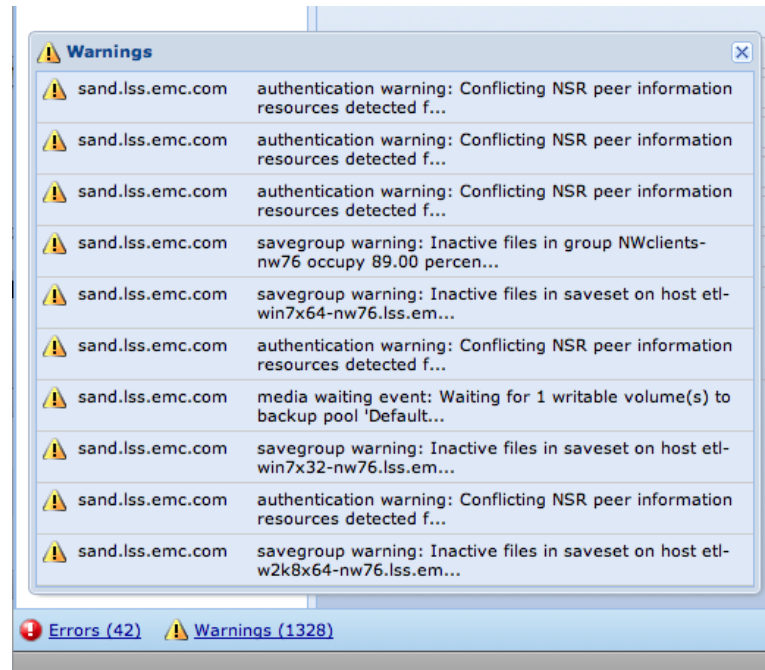


Figure 25 Ten most recent warnings

Views menu filters

Each section of the Backup & Recovery Manager provides views filters to customize the systems and information displayed.

The following section provides details on the common views filters and those specific to each section.

Common views

The following table lists the filters common to the Alerts, Activities, Events and Systems panels in Backup & Recovery Manager.

Table 11 Common views filters

View filter	Description
Enterprise	Clicking Enterprise filters the view to only display objects that are associated with Avamar, NetWorker, and Data Domain jobs and/or systems.
Avamar	Clicking Avamar filters the view to only display objects that are associated with Avamar jobs and/or systems.
NetWorker	Clicking NetWorker filters the view to only display objects that are associated with NetWorker jobs and/or systems.
Data Domain	Clicking Data Domain filters the view to only display objects that are associated with Data Domain jobs and/or systems.

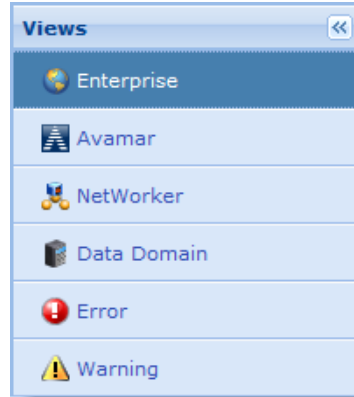
Alerts views

The Views menu that is located in the upper left corner of the Alerts section provides a list of available filters.

NOTICE

Only a single item can be selected. For example, there is no way to view only NetWorker errors. If Error is selected while viewing NetWorker, all errors for Avamar, NetWorker, and Data Domain are displayed.

Figure 26 Alerts views



The following table lists and describes the filters specific to the **Alerts Views** panel.

Table 12 Alerts views filters

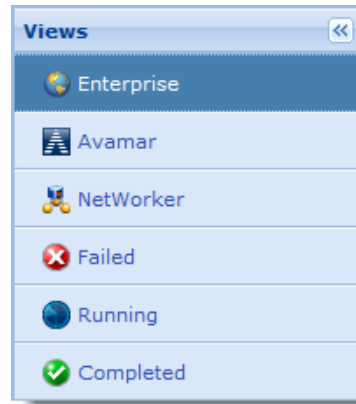
View filter	Description
Error	Systems that have an error are included in the Error filter list.
Warning	Systems that have an alert that requires immediate user intervention to avoid system component failure or data loss are included in the Warning filter.

Activities views

The **Views** menu located in the top left pane of the **Activities** window provides a list of available filters.

Note

Only a single item can be selected. For example, there is no way to view only failed Avamar jobs. If Failed is selected while viewing Avamar, all failed jobs for Avamar, NetWorker and Data Domain are displayed.

Figure 27 Activities views

The following table lists and describes the filters specific to the Activities Views panel.

Table 13 Activities views filters

Filter	Description
Failed	To view all jobs that have encountered failures during an operation, select Failed .
Running	To view jobs that are currently running an operation, select Running .
Completed	To view jobs that have completed all operations, select Completed .

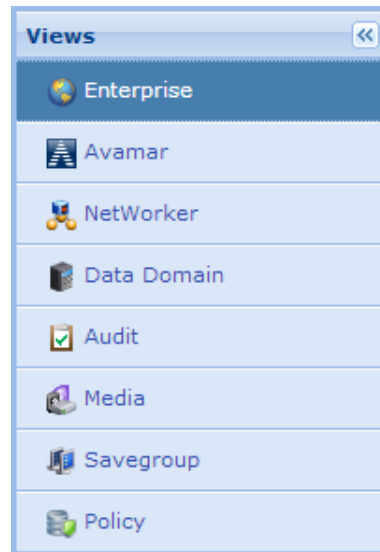
Events views

The **Views** menu that is located in the upper left pane of the **Events** section provides a list of available filters.

Note

The **Policy** filter is available for NetWorker backup events only.

Figure 28 Events views



The following table lists the filters specific to the **Events Views** panel.

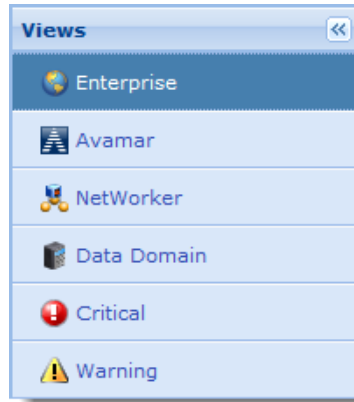
Table 14 Events views filters

Filters	Description
Audit	The Audit type event starts the Avamar audit logging feature which keeps a permanent log of system actions that are initiated by users.
Media	Lists events in the Media category that is generated by all systems in the enterprise.
Savegroup	Lists events in the Savegroup category that is generated by all systems in the enterprise.
Policy	Lists NetWorker Policy based backup events.

Systems views

The **Views** menu, which is located in the upper left pane of the **Systems** window provides a list of available filters.

Figure 29 Systems views



The following table lists and describes the filters specific to the Systems Views panel.

Table 15 Systems views filters

Filter	Description
Critical	Lists all systems with critical errors that require immediate attention.
Warning	Lists all systems with warnings for backup or replication operations.

Exporting data to CSV

Backup & Recovery Manager provides the ability to export **Systems**, **Events**, **Alerts**, and **Activities** (backup and replication) data to a Microsoft Office Excel Comma Separated Values File (CSV).

To export the data, use the **Export to CSV** icon (📄) in **Alerts**, **Activities**, **Systems**, **Events**, **Configuration**, and **Reports**.

CHAPTER 3

Installation

Install the EMC Backup & Recovery Manager to monitor Avamar, NetWorker and Data Domain systems. Review [Requirements](#) before beginning the installation of the Backup & Recovery Manager software.

- [Installing the Backup & Recovery Manager server](#)..... 54
- [Upgrade to Backup & Recovery Manager 1.3](#)..... 57
- [Build to build upgrade of the Backup & Recovery Manager server](#)..... 59
- [Changing the network parameters post installation](#)..... 61
- [Backup & Recovery Manager adaptor installation](#)..... 62
- [Logging in to the Backup & Recovery Manager](#)..... 76
- [Disable the Backup & Recovery Manager adaptor for Avamar](#)..... 79
- [Uninstalling the Backup & Recovery Manager adaptor](#)..... 80

Installing the Backup & Recovery Manager server

The Backup & Recovery Manager server can be installed on both virtual and physical hosts. A vSphere client is required for a virtual host and a DHCP server is required for a physical host.

Note

Configure Backup & Recovery Manager and all Avamar and NetWorker backup servers with the same network time protocol (NTP) server. If the clocks are not reasonably synchronized, it can result in a communication failure between Backup & Recovery Manager and the backup server.

The Backup & Recovery Manager server is deployed by using the following methods:

- [Installing the Backup & Recovery Manager server on a VM](#) on page 54
- [Installing the Backup & Recovery Manager server on physical hardware](#) on page 56

NOTICE

You must log in as root user to successfully complete the Backup & Recovery Manager server installation. Also, it is recommended that you change the password for the admin, dpn, gsan, root, and ucas users from the default (changeme) after installation.

Installing the Backup & Recovery Manager server on a VM

You can install the Backup & Recovery Manager server on a VM by first deploying and configuring the vApp and then verifying the deployment.

Deploying and configuring the Virtual Application (vApp)

NOTICE

If the IP address must be manually configured in the network environment, use the VMware console, rather than the SSH session to the Backup & Recovery Manager server. The VMware console is able to maintain a connection during the process, while the SSH might lose the connection during the IP change.

Procedure

1. From a vSphere client that connects to a VMware vCenter server with ESX hosts, click **File > Deploy OVF Template**.

Note

A vCenter server is required to deploy the OVA.

2. Browse to the BRS_EM_OVF.ova file and click **Next**.
3. In the .ova **Template Details** window, specify a **Name** and **Location** for the deployed template and click **Next**.
4. Select a destination storage for the VMFiles from the list and click **Next**.

5. Select the format in which to store the virtual disk:

- Thick Provision Lazy Zeroed (recommended)
- Thick Provision Eager Zeroed
- Thin Provision

NOTICE

Eager Zero yields the best performance, but also takes the most time to initialize. Thick provisioning does not fill the drive unless eager zeroed is selected. The storage capacity for the entire virtual disk is allocated on the datastore at virtual disk create time if thick provisioning is selected. Thin provisioning means that the capacity on the datastore is allocated to the virtual disk as required, up to the full size of the virtual disk.

6. Choose the networks for the deployed template to use:

- a. Select the appropriate subnet from the **Destination Networks** drop-down list.
- b. Click **Next**.

7. Complete the fields in the **Networking Properties** section of the window to customize the software for the deployment and click **Next**. The fields include:

- DNS
- Network1 IP address
- Network1 Netmask

8. In the **Ready to Complete** window, verify that the options are correct and click **Finish**, or click **Back** to change options.9. When the deployment completes successfully, click the deployed server in the vCenter and click **Power on the virtual machine**.

10. Use a secure shell client such as PuTTY or SSH to connect to the Backup & Recovery Manager server.

11. Type the **Hostname or IP address** to specify the destination in which to connect.**NOTICE**

Port 1315 must be available for SSH connections.

12. Connect to the Backup & Recovery Manager server as the ucas user:

```
ssh ucas@SERVER -p1315
```

The password is the default `changeme`.

13. Change to root user:

```
su - <root password>
```

Verifying the deployment

When the installation is complete, ensure that the Backup & Recovery Manager server was installed correctly on the vApp.

Procedure

1. Open a browser, type the following in the **Address** field, and then press **Enter**:

`https://<brm_server_IP>/brm`

The IP address might be different depending on the DNS setup in the environment.

NOTICE

It is recommended to bookmark the server location in order to easily navigate to it when required.

2. Type the default username `admin`.
3. Type the default password `changeme`.
4. Change the password when prompted.

The Backup & Recovery Manager opens in the browser window. [Logging in to the Backup & Recovery Manager](#) on page 76 provides detailed instructions about logging in to the Backup & Recovery Manager.

NOTICE

It is recommended that you change the password for the `admin`, `dpn`, `gsan`, `root`, and `ucas` users from the default (`changeme`) after installation.

Installing the Backup & Recovery Manager server on physical hardware

The Backup & Recovery Manager server can be installed on physical hardware by using an ISO image.

Before you begin

Before beginning, verify that the following hardware recommendations and requirements are met:

- A DHCP server must be available on the network on which the server is running for a Backup & Recovery Manager deployment.
- The Backup & Recovery Manager should be configured with an NTP (network time protocol) server to avoid timing issues.

NOTICE

NTP is configured in the operating system after Backup & Recovery Manager is deployed.

The following table provides a summary of Backup & Recovery Manager server hardware requirements.

Table 16 Data storage requirements

Component	Memory per component (disk space)
Memory	8 GB
System disk	40 GB
Database disk	70 GB

Procedure

1. Make the ISO image available on a DVD, and configure the server to boot from the DVD.
2. Boot from the native ISO image and allow it to check the system for hardware requirements.

NOTICE

If the system does not meet the requirements, an error message is displayed.

3. Set the lang/keyboard and configure the network when the installation completes.

NOTICE

The installation takes approximately 20–30 minutes on most hardware.

Native Installer fails when ISO is mounted with a CD not defined in the post script

During Native installation, the POST script attempts to mount `/dev/sr0` to obtain the required Backup & Recovery Manager files. However, if another CD is mounted (such as `/dev/sr1`), the mount fails, and reboots the system. For native installation of Backup & Recovery Manager on a physical computer, use the primary CD (`/dev/sr0`) for ISO mapping as is defined in the post deployment script.

Upgrade to Backup & Recovery Manager 1.3

Perform the tasks in the following sections before upgrading to Backup & Recovery Manager 1.3 and later from the current release.

NOTICE

If upgrading to Backup & Recovery Manager 1.3 from an earlier version of Backup & Recovery Manager, the `.run` file does not work.

1. Complete a fresh deployment of the Backup & Recovery Manager 1.3 server
2. Migrate data to the deployed Backup & Recovery Manager 1.3 server by using the migration script available at, `/opt/emc/ucas:`

```
migration-12-13
```

Migrate data to Backup & Recovery Manager 1.3 and later

Manual data migration is required to upgrade from the current version of Backup & Recovery Manager to Backup & Recovery Manager 1.3 and later.

Before you begin

You require the hostname or IP address for the current Backup & Recovery Manager server from which the data is migrating from, and the `ucas` user password.

Procedure

1. Log in to the Backup & Recovery Manager 1.3 virtual appliance as the `ucas` user:

```
ssh -p 1315 brm-current hostname or brm current-ip address
```

2. Run the following command to migrate data from the current version of Backup & Recovery Manager to version 1.3 and later:

```
migrate-current-13 brm-current-appliance-address brm-current-
appliance-ucas-user-password
```

The migration status is displayed.

Results

It can take approximately 30 minutes to migrate a 2.5 GB database.

Resetting the firewall rules after migration

After migrating to Backup & Recovery Manager 1.3 from a previous version of the Backup & Recovery Manager server (1.1, 1.2 or 1.2.1), the firewall rules must be reset.

Reset the firewall rules to ensure you can log in to the Backup & Recovery Manager 1.3 UI:

```
sudo /usr/sbin/iptables-restore < /opt/emc/ucas/packages/ucas-iptables
```

Copy the current certificate to Backup & Recovery Manager 1.3 or later

Communication between the Backup & Recovery Manager server and the backup servers requires certificates to validate the identity of hosts and to encrypt information. Certificates are tied to the IP address of the machine, so careful steps must be taken when copying certificates from one Backup & Recovery Manager server to another as part of a migration.

Before you begin

Reusing the certificates from the current Backup & Recovery Manager virtual appliance requires that you reuse the IP, and optionally the hostname.

Procedure

1. Log in to the Backup & Recovery Manager 1.3 or later virtual appliance as the UCAS user:

```
ssh -p 1315 current brm hostname or current brm ip address
```

2. Disable the firewall:

```
/etc/init.d/SuSEfirewall12_init stop
```

```
/etc/init.d/SuSEfirewall12_setup stop
```

3. Copy the certificates from the current appliance to the 1.3 or later appliance, and run the following command from the old appliance:

```
scp -P 1315 /opt/emc/ucas/security/* new brm hostname: or new
brm ip address:/opt/emc/ucas/security/
```

Existing files might be overwritten.

4. Make a note of the IP address and hostname of the current Backup & Recovery Manager:

```
ip addr show eth0
```

```
/sbin/hostname
```

5. Shutdown the current Backup & Recovery Manager server. While logged in to the current Backup & Recovery Manager server, enter the following command:

```
sudo shutdown -h now
```

6. Change the IP address and hostname to that of the current version:
 - a. As root user, run `yast lan`.
 - b. Verify the new IP and hostname settings for the newly migrated Backup & Recovery Manager 1.3 or later instance for the following tabs of the command interface, and select **Edit** in any of the tabs to make changes:
 - Overview
 - Hostname/DNS
 - Routing
7. Reboot the Backup & Recovery Manager 1.3 appliance by using the following command:


```
sudo shutdown -r now
```
8. Wait approximately 5 minutes for the reboot to complete, and then access Backup & Recovery Manager 1.3 and later by using the web browser to confirm that communication with the backup servers resumes.

The temporary password is printed in the log files after migration

Following the migration to Backup & Recovery Manager 1.3 from older Backup & Recovery Manager servers (1.1, 1.2 or 1.2.1), the temporary password is displayed in the log files:

```
Resetting BRM admin password
```

```
user admin password set to CDRuAR2BbLNySmSU
```

Change the password immediately after logging in to Backup & Recovery Manager following the migration.

Build to build upgrade of the Backup & Recovery Manager server

When upgrading to the current release of the Backup & Recovery Manager server, you should take a snapshot of the current installation.

Upgrading to the current Backup & Recovery Manager server

Before you begin

On the Purchase Order for Avamar, NetWorker, or the Data Protection Suite, EMC Sales lists Backup & Recovery Manager as a zero dollar order. When the order is filled, the required keys, download instructions including passwords are sent in an automated email. The password for the Backup & Recovery Manager `.zip` file is sent in an email.

Note

To upgrade from any earlier versions of Backup & Recovery Manager to version 1.3, perform a fresh server deployment, and then a data migration as described in [Upgrade to Backup & Recovery Manager 1.3](#) on page 57. Upgrading directly from the `.run` file does not work.

Procedure

1. Copy the `.run` installer binary to the Backup & Recovery Manager server by using a tool such as PuTTY (pscp):

```
pscp -P1315 brm-installer-<version>-Linux-x64.run ucas@BRM-  
SERVER:/tmp
```

Note

FTP is not supported for Backup & Recovery Manager. The Backup & Recovery Manager is a lightweight operating system, and does not have an FTP agent configured.

2. Connect to the Backup & Recovery Manager server as the ucas user:

```
ssh ucas@SERVER -p1315
```

3. Change to root user:

```
su - <root password>
```

4. Change to the `/tmp` directory:

```
cd /tmp
```

5. Ensure the installer binary (`.run` file) is executable:

```
chmod 755 brm-installer-<version>-Linux-x64.run
```

6. Become root user:

```
sudo /bin/bash
```

Ucas password:

The default password is changeme.

Note

It is recommended that you change the admin, dpn, gsan, root, and ucas users passwords from the default (changeme) immediately after installation.

7. Confirm that you are root user by using the `id` command:

```
# id
```

```
uid=0(root) gid=0(root) groups=0(root),104(mysql)
```

8. Run the installer.

Any required data migrations occur automatically during the installation.

If you try to run the Backup & Recovery Manager installer as a non-root user, the following error message displays, and the installer exits:

```
ucas@brm12-test2:/tmp $ ./brm-installer-Linux-x64.run  
Error: There has been an error.  
This installer requires root privileges. Please become  
superuser before  
executing the installer  
Press [Enter] to continue:
```

9. If problems occur during the installation, revert to the previous version by using the snapshot was taken in Step 1 of this procedure.

Regenerate the SSL certificates

When the hostname or IP address changes, run the following command to regenerate the SSL certificates for the Backup & Recovery Manager server:

```
sudo service tomcat-ucas gencert
```

Changing the network parameters post installation

You can change the Backup & Recovery Manager server name after the initial installation by using the yast set up tool.

Procedure

1. Connect to the Backup & Recovery Manager server as the ucas user:

```
ssh ucas@SERVER -p1315
```

2. Change to root user:

```
su - <root password>
```

3. Change the server name by using yast:

- a. Navigate to **yast > Network Devices > Network Settings**.
- b. Use the tab or the arrow keys to open the **Hostname/DNS** dialog box.
- c. Type the new name in the **Hostname/DNS** dialog box.

4. Add the new hostname to the certificate to avoid errors:

```
/etc/init.d/tomcat-ucas gencert
```

The command stops Tomcat, updates the security certificates, reboots Apache and restarts Tomcat. Messages similar to the following are displayed:

```
wd /opt/emc/ucas
path is /sbin:/usr/sbin:/usr/local/sbin:/usr/local/bin:/
bin:/usr/bin:/usr/X11R6/bin
path is now /usr/java/default/bin:/opt/emc/ucas/tomcat/bin:/
sbin:/usr/sbin:/usr/local/sbin:/root/bin:/usr/local/bin:/usr/
bin:/bin:/usr/bin/X11:/usr/X11R6/bin:/usr/games:/usr/lib/mit/
bin:/usr/lib/mit/sbin
library path is now
Stopping Tomcat Using CATALINA_BASE: /opt/emc/ucas/tomcat
Using CATALINA_HOME: /opt/emc/ucas/tomcat
Using CATALINA_TMPDIR: /opt/emc/ucas/tomcat/temp
Using JRE_HOME: /usr/java/ucasjre
Using CLASSPATH: /opt/emc/ucas/tomcat/bin/
bootstrap.jar:/opt/emc/ucas/tomcat/bin/tomcat-juli.jar
0
allowing 30 seconds for graceful shutdown...
Checking certificates... JMS Certificates already exist
Removing old certificate from keystore
Generating web certificates in /opt/emc/ucas
Certificate stored in file </opt/emc/ucas/security/
ucasWebCert.pem>
Certificate stored in file </opt/emc/ucas/security/
ucasWebCert.cert>
Certificate was added to keystore
[Storing /usr/java/ucasjre/lib/security/cacerts]
Finished generating web certificates
Updating server name in ssl conf
Restarting apache...
httpd running, stopping
```

```

httpd stopped
httpd NOT running
started httpd
Starting Tomcat Using CATALINA_BASE:   /opt/emc/ucas/tomcat
Using CATALINA_HOME:   /opt/emc/ucas/tomcat
Using CATALINA_TMPDIR: /opt/emc/ucas/tomcat/temp
Using JRE_HOME:        /usr/java/ucasjre
Using CLASSPATH:       /opt/emc/ucas/tomcat/bin/
bootstrap.jar:/opt/emc/ucas/tomcat/bin/tomcat-
juli.jarstarting tomcat...
tomcat pid 12968

```

Backup & Recovery Manager adaptor installation

Backup & Recovery Manager server 1.0 and 1.1 are not supported with the Backup & Recovery Manager 1.2, or 1.3 adaptors. Installing the Backup & Recovery Manager server 1.3 ensures that all new functionality in Backup & Recovery Manager 1.3 is available for use.

This section provides instructions for installing the Backup & Recovery Manager adaptors for Avamar and NetWorker.

Note

Before continuing with the installation of the Backup & Recovery Manager adaptor on Avamar 6.1 SP1 and later systems, you must contact EMC Support to obtain the most current MC hotfix. The hotfix is necessary for the Backup & Recovery Manager to work with the Avamar software.

Backup & Recovery Manager adapter for Avamar installation and upgrade

There are different methods for installing the adapter on Avamar 6.0.2 and 6.1 than 6.1 Service Pack 1 and later. You can configure the Backup & Recovery Manager adapter for Avamar during the Avamar installation or upgrade.

If the Avamar software has already been installed or upgraded, reconfigure the server hostname as described in [Reconfiguring the server hostname for the Avamar adapter](#).

Note

Backup and Recovery Manager is not supported on Avamar Extended Retention Media Access Nodes.

Install the Backup & Recovery Manager adapter for the following versions of the Avamar software:

- [Installing the adapter for Avamar 6.0.2 and Avamar 6.1.0](#) on page 63
- [Configuring the adapter for Avamar 6.1 SP1 and 7.0](#) on page 65

Installing the adapter for Avamar 6.0.2 and Avamar 6.1.0

Install the Backup & Recovery Manager adapter for Avamar 6.0.2 and Avamar 6.1 by using the Avamar Enterprise Manager.

Before you begin

Note

Before continuing with the Backup & Recovery Manager adaptor installation, you must contact EMC Support to obtain the most current MC hotfix.

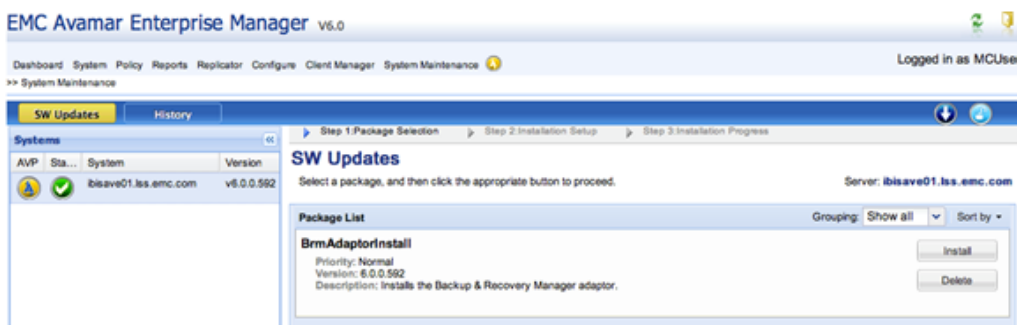
If the MC hotfix is not installed, the installation fails and this error is reported in the Information Log:

ERROR: The required MC hotfix has not been installed. You must abort and install the hotfix first. operation failed.

Procedure

1. Copy the Avamar MC patch package and the Backup & Recovery Manager adapter for Avamar on the Avamar utility node or single node server:
`/data01/avamar/repo/packages`
2. Log in to the Enterprise Manager. An example URL for the Avamar Enterprise Manager is:
`http://avamar.example.com/em`
3. Navigate to the **System Maintenance** window in the Avamar Enterprise Manager.

Figure 30 Avamar Enterprise Manager



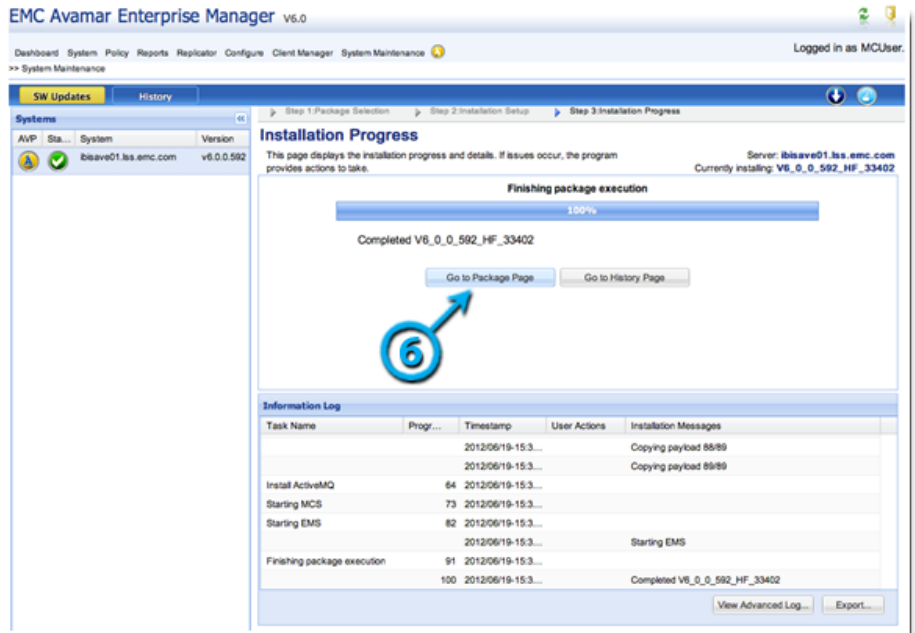
4. Click **Continue**.
5. When the installation completes, click **Go to Package Page**, and then click **Install** on the **BrmAdaptorInstall** package. Complete the adaptor installation:
 - a. Enter the Backup & Recovery Manager server hostname and click **Save**.

NOTICE

If you do not specify a hostname, the adapter is installed but not configured to report to a Backup & Recovery Manager server. Configure the adapter later if you do not complete the configuration at installation. [Reconfiguring the server hostname for the Avamar adapter](#) provides instructions on typing a Backup & Recovery Manager server hostname for the Avamar adapter.

b. Click **Continue**.

Figure 31 Go to Package Page status



6. Verify that the Avamar server is listed in the Backup & Recovery Manager server:
 - a. Log in to the Backup & Recovery Manager server.
 - b. Navigate to the Systems window and verify that the Avamar server is displayed in the list of systems.

NOTICE

Allow enough time (approximately 5 minutes) for the installation to complete and populate the Backup & Recovery Manager server’s system list.

The Installation Progress window displays a progress bar, status messages, and the Information Log table. The following table describes the information that is displayed on the progress bar.

Table 17 Installation Progress details

Item	Description
Progress bar	Displays the installation’s progress as a percentage. The percentage represents the number of tasks completed. Some tasks require more time than others.
Status messages	The installation displays the current task name above the progress bar and the associated status message below the progress bar.
Action buttons	When a problem occurs, the installation: Stops and displays a status message about the failure below the progress bar.

Table 17 Installation Progress details (continued)

Item	Description
	Displays action buttons relevant to the problem. For example: Skip this task, Undo this task, Undo All Changes , or Call EMC support . Undo All Changes returns the system to the kickstart state. The installation displays a confirmation dialog box, which requires a response before the undo operation can take place.
Details button	Opens the error log file that is specific to the failure. This button only appears if you are logged in to the EMC Customer Support account.
Information Log table	Provides details about each installation task.
View Advanced Log	Click View Advanced Log to open the workflow log file for this package installation. The View Advanced Log button is only available if you are logged in to the EMC Customer Support account.
Export	Click Export to save log information to a file. The Export as dialog box appears. Choose one of command buttons: Excel or PDF. Follow the prompts to save the log information to a file.

Configuring the adapter for Avamar 6.1 SP1 and 7.0

In Avamar 6.1 SP1 and 7.0 and later, the Backup & Recovery Manager adapter for Avamar is packaged with the Avamar software. Install the adapter by using the Avamar Installation Manager.

NOTICE

Before continuing with the installation of the Backup & Recovery Manager adapter on Avamar 6.1 SP1 and earlier systems, contact EMC Support to obtain the most current MC hotfix.

If the MC hotfix is not installed, the installation fails and this error is reported in the Information Log:

Error: The required MC hotfix has not been installed. Operation failed.

Avamar 6.1 SP2 and 7.0 and later do not require a hotfix.

If the Avamar software has already been installed or upgraded, complete the procedure in [Reconfiguring the server hostname for the Avamar adapter](#).

Procedure

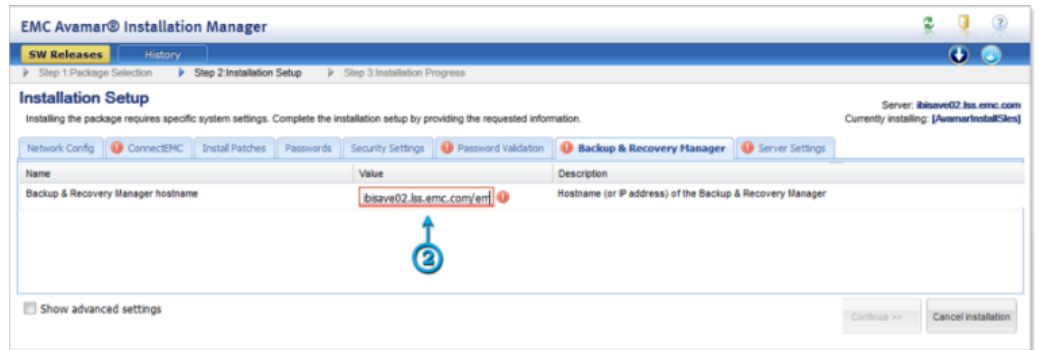
1. In the Avamar Installation Manager, select the Backup & Recovery Manager tab.
2. Type the Backup & Recovery Manager server hostname or IP address in the **Value** field.

NOTICE

If you do not specify a hostname, the Avamar adapter is installed but not configured to report to a Backup & Recovery Manager server. The adapter must be configured later if it was not configured at installation.

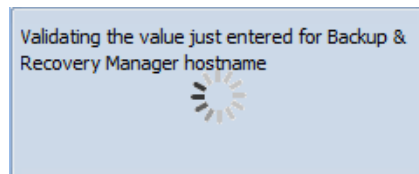
[Reconfiguring the server hostname for the Avamar adapter](#) provides instructions on typing a Backup & Recovery Manager server hostname.

Figure 32 Avamar Installation Manager



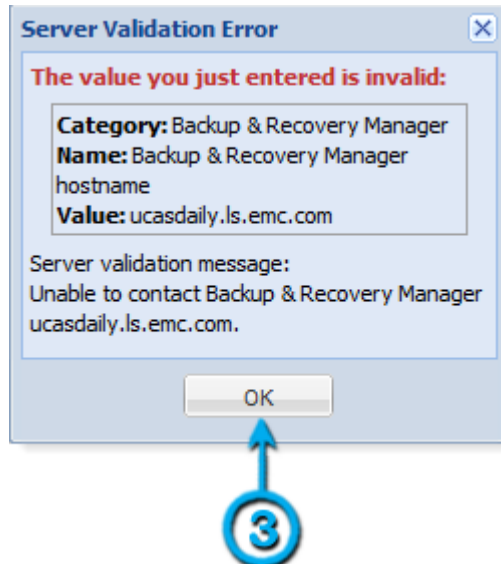
- A dialog box opens while the hostname is validated.

Figure 33 Hostname validation



- If the hostname does not resolve, an invalid value error is displayed.

Figure 34 Hostname Validation message



3. Click **OK** in the **Server Validation Error** dialog box, and re-enter a valid hostname in the **Value** field.
4. Click **Save**.

NOTICE

It can take up to 24 hours after a system is added to the Backup & Recovery Manager server before there is any data to report on.

Adding an Avamar server to the Backup & Recovery Manager for Avamar 7.1 and later

In Avamar 7.1 and Backup & Recovery Manager 1.2, all Avamar adaptor functionality is integrated into the Avamar software. There is no longer a separate adaptor. To improve security, it is now required to enter a Backup & Recovery Manager username and password to configure Avamar to communicate with Backup & Recovery Manager.

Before you begin

Ensure that the Backup & Recovery Manager is running before beginning the reconfiguration. Older versions of Avamar that are configured to communicate with Backup & Recovery Manager must be reconfigured after an upgrade to Avamar 7.1 due to improved security.

Procedure

1. Log in as root user on the Avamar utility node or single node server:

```
su -
```

2. Run the following `msgbrokerctl.pl` command:

```
msgbrokerctl.pl --setup --brmhost=<BRM hostname or IP address>
```

You are prompted to enter a Backup & Recovery Manager username and password. Optionally, you can specify the username and password for Backup & Recovery Manager by using the `msgbrokerctl.pl` command parameters, `--brmuser=<username>`, and `--brmpass=<password>`.

3. Start the process:

```
msgbrokerctl.pl --start
```

Reconfiguring the server hostname for the Avamar adaptor for Avamar 7.0 and earlier

If the Avamar server does not appear in the list of systems, reconfigure the Backup & Recovery Manager adaptor for Avamar.

This often occurs as a result of the following:

- The hostname of the Backup & Recovery Manager was changed
- A new Virtual Appliance (OVA) was deployed for the BRM (despite having used the same hostname as before)
- The hostname was not provided at the time of installation or upgrade.

- Avamar 6.1 SP1 was installed without providing the hostname or IP address of the Backup & Recovery Manager server.

Procedure

- To reconfigure the Backup & Recovery Manager adaptor for Avamar 7.0 and earlier:
 - Log in to the Avamar server utility node or single node server as admin.
 - Run the following commands in sequence:

```
$ adaptorctl.pl --stop
$ adaptorctl.pl --setup --jmsaddr=<BRM hostname>
$ adaptorctl.pl --start
```

NOTICE

Ensure that the script is in the path environment, or navigate to the path in which it is located and precede the command with `./`.

- Edit `mcsserver.xml` file:
 - Stop the Avamar Management Console Server (mcs) database:

```
dpnctl stop mcs
```

- Change the `enableBrmService` value to true:

```
/usr/local/avamar/var/mc/server_data/prefs/mcsserver.xml
<entry key="enableBrmService" value="true" />
```

- Restart mcs:

```
dpnctl start mcs
```

Reconfiguring the Backup & Recovery Manager adaptor for Avamar 7.1 and later

To reconfigure the Backup & Recovery Manager adaptor for Avamar 7.1 and later, perform the steps in [Adding an Avamar server to the Backup & Recovery Manager for Avamar 7.1 and later](#).

NetWorker adapter installation and upgrade on Windows and Linux

The NetWorker adapter can also be installed as a proxy to enable a separate system to act as a communication proxy between a NetWorker server and Backup & Recovery Manager. This option supports NetWorker server operating systems that do not have a native adapter (Solaris, AIX, HP-UX, and so on).

Table 18 NetWorker adapter location

NetWorker version	Adapter that is packaged with NetWorker	Path to adapter executable file	Description
7.6.0	No	Not applicable	The adapter is available from NetWorker software

Table 18 NetWorker adapter location (continued)

NetWorker version	Adapter that is packaged with NetWorker	Path to adapter executable file	Description
			downloads on EMC Online Support by Product, and must be installed separately.
7.6.1	No	Not applicable	The adapter is available from NetWorker software downloads on EMC Online Support by Product, and must be installed separately.
7.6.x	No	Not applicable	The adapter is available from NetWorker software downloads on EMC Online Support by Product, and must be installed separately.
8.0.x	No	Not applicable	The adapter is available from NetWorker software downloads on EMC Online Support by Product, and must be installed separately.
8.1.x	Yes	<ul style="list-style-type: none"> • Linux: /opt/nsr/bin • Windows: C:\Program Files\EMC NetWorker\nsr\bin 	The adapter executable is available after the NetWorker server is installed. Install the adapter by running the package.
8.2.x	Yes	<ul style="list-style-type: none"> • Linux: /opt/nsr/bin • Windows: C:\Program Files\EMC NetWorker\nsr\bin 	The adapter executable is available after the NetWorker server is installed. Install the adapter by running the package.

Table 18 NetWorker adapter location (continued)

NetWorker version	Adapter that is packaged with NetWorker	Path to adapter executable file	Description
			<p>Note</p> <p>The Backup & Recovery Manager adapter for NetWorker might not be packaged with NetWorker 8.2. Although the Backup & Recovery Manager adapters included with NetWorker 8.2 are operational, some functionality is not available. When installing, or upgrading to the Backup & Recovery Manager 1.2 server, you can manually install the most current build of the Backup & Recovery Manager adapter for NetWorker.</p>
8.5.x	Yes	<p>nsrmqctl path:</p> <ul style="list-style-type: none"> • Linux: /opt/nsr/nsmq/bin • Windows: C:\Program Files\EMC NetWorker\nsr\nsmq\bin 	<p>The NetWorker adapter is included with the NetWorker server installation. Register the adapter to the NetWorker server by using nsrmqctl.</p>
9.0.x	Yes	<p>nsrmqctl path:</p> <ul style="list-style-type: none"> • Linux: /opt/nsr/nsmq/bin • Windows: C:\Program Files\EMC NetWorker\nsr\nsmq\bin 	<p>The NetWorker adapter is included with the NetWorker server installation. Register the adapter to the NetWorker server by using nsrmqctl.</p>

Registering the Backup & Recovery Manager adapter for NetWorker 9.0 on Windows and Linux

Before you begin

It is required that the Backup & Recovery Manager server is installed before configuring the adapter.

Procedure

1. As root user, browse to the location of nsrmqctl:
 - For Windows, C:\Program Files\EMC NetWorker\nsr\nsrmq\bin
 - For Linux, /opt/nsr/nsrmq/bin

The adaptor is available with the NetWorker software package.

2. As root user, run the nsrmqctl command:

```
./nsrmqctl
```

3. Register the NetWorker server to Backup & Recovery Manager by using the following command:

```
monitor -u username -p password BRM IP
```

Check the logs at C:\Program Files\EMC NetWorker\nsr\nsrmq\logs (Windows), or /nsr/nsrmq/logs/nsrmq.log (Linux) for any issues.

4. Proceed to the Windows or Linux installation:
 - [Installing or upgrading the Backup & Recovery Manager adaptor for NetWorker on Windows](#)
 - [Installing or upgrading the Backup & Recovery Manager for NetWorker on Linux](#)

Installing or upgrading the Backup & Recovery Manager adaptor for NetWorker on Windows

For NetWorker server 8.1 and later, the NetWorker adaptor is included with the NetWorker server packages for Windows servers. Therefore, no separate download is required. It is required that the proxy host computer has network access to the NetWorker server.

Procedure

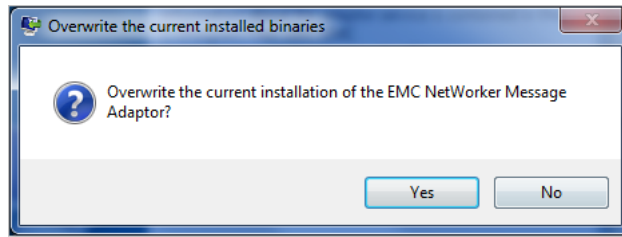
1. To begin the installation, run the NetWorker adaptor installer, and launch the Backup & Recovery Manager Setup Wizard. If there is a current installation of the adaptor installed:

NOTICE

If at any time during the installation you click **Cancel**, a dialog box prompts you to confirm the cancellation.

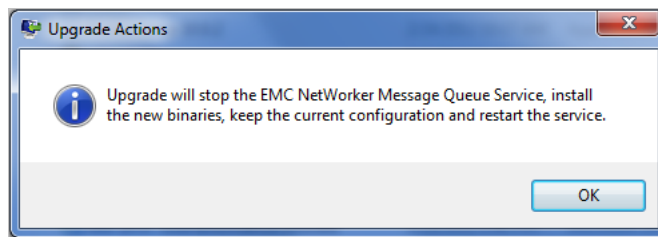
- a. When prompted to overwrite the current installation, click **Yes**.

Figure 35 Overwrite prompt



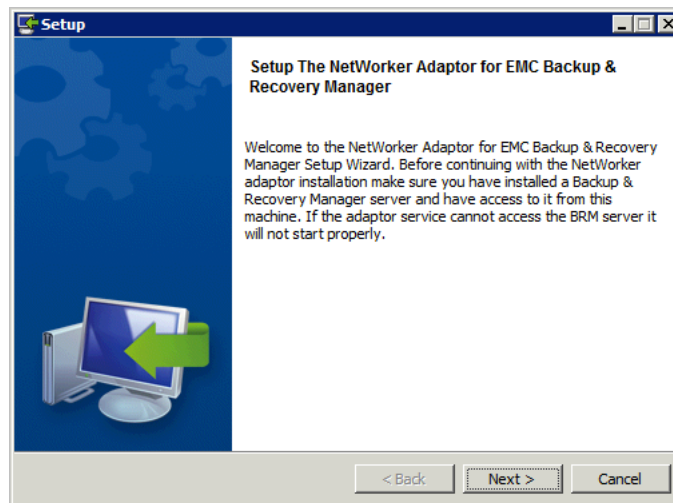
- b. To continue the installation and upgrade the Backup & Recovery Manager, click **OK**.

Figure 36 Upgrade information



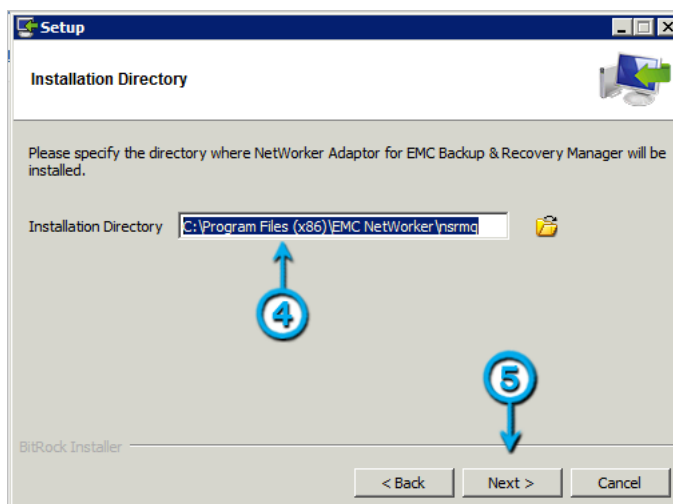
2. To begin the installation, click **Next**.

Figure 37 Setup wizard



3. To accept the License Agreement, select **I accept the agreement**, and then click **Next**.
4. In the **Installation Directory** field, accept the default installation location or type another location for the installation.

The Windows default installation directory is displayed. The default Linux directory is `/nsr/nsrmq`.

Figure 38 Installation Directory

5. Click **Next**.
6. Type the hostname or IP address of the NetWorker server.
7. Type the hostname or IP address of the Backup & Recovery Manager server to receive data from the adaptor.
8. Type the **Username** and **Password**.
9. Select the server, **BRM version 1.3**.
10. Click **Next**.
11. The NetWorker Adaptor can be installed on a proxy server to monitor a system with an operating system that is not supported by the Backup & Recovery Manager. For example, Solaris, AIX or HP-UX. If required, perform the following steps to grant access to the proxy system:
 - a. In NMC, open the **Administrator** interface for the NetWorker server.
 - b. In **Configuration**, select **User Groups**.
 - c. Double-click **Administration**.
 - d. Add the user and host (adaptor hostname) to the list of valid users.

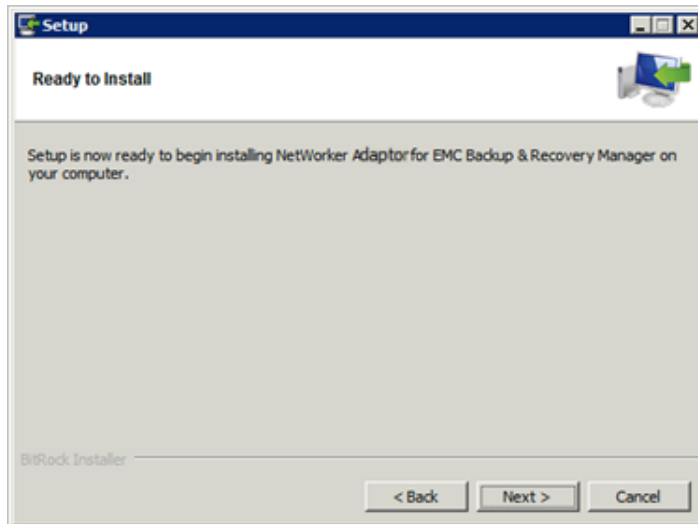
It is recommended that the proxy server is installed on a secure, protected NetWorker server to avoid losing data if a disaster occurs. Do not install the server on a desktop or laptop computer.

NOTICE

For proxy setups, the proxy host must have network access to the NetWorker server it is supporting.

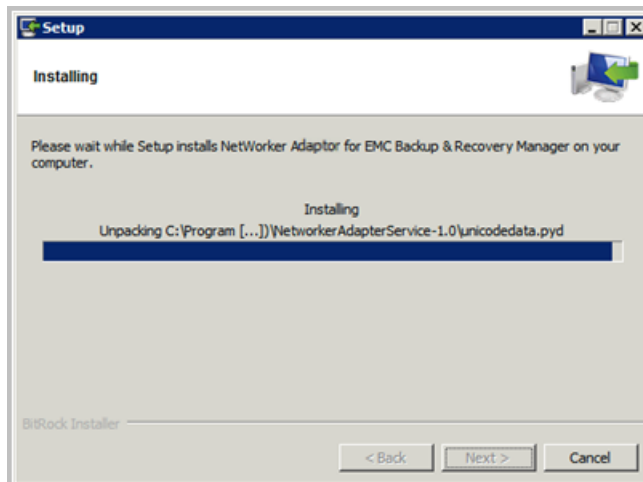
12. To begin the installation, click **Next**.

Figure 39 Installation prompt

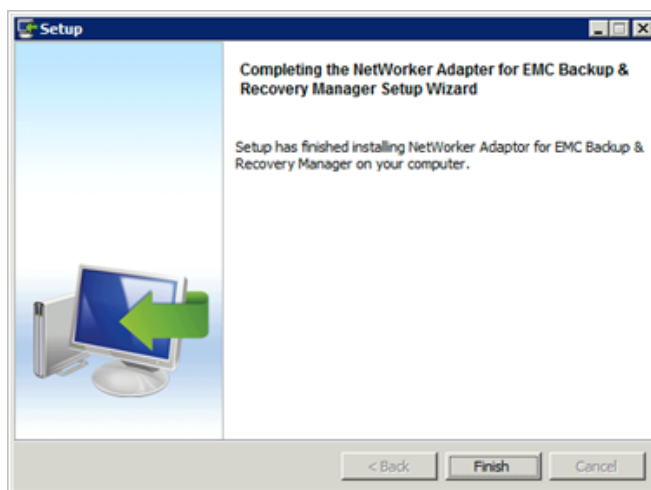


13. The installation proceeds.

Figure 40 Installation status



14. Click **Finish**.

Figure 41 Installation completion

The installation verifies the connection to both the Backup & Recovery Manager server and the NetWorker server.

After the installation completes a new Windows service that is called NetWorker ActiveMQ Adaptor starts on the host system. The adaptor automatically begins sending information to the Backup & Recovery Manager.

Installing or upgrading the Backup & Recovery Manager adaptor for NetWorker on Linux

For NetWorker server 8.1 and later, the NetWorker adaptor is included with the NetWorker server packages for Linux servers. Therefore, no separate download is required.

Procedure

1. Download NetWorker adaptor for Linux installer.
The adaptor is available with the NetWorker software package.
2. Run the installer:

```
sles64sptn21328:/ # NetWorkerAdaptor-build_numberlinux-x64.run
```
3. Press **Enter** to view the License agreement, and type **Y** to accept it.
4. Type the installation path:

```
/nsr/nsrmq
```
5. Enter the hostname or IP address of the NetWorker server.
6. Type the hostname or IP address of the Backup & Recovery Manager server to receive data from the adaptor.

NOTICE

The hostnames that are shown in steps 5 and 6 are examples and are different depending on your environment.

7. Type the Username, `admin`, and Password, `changeme`.
8. Select **Version 1.3** from the list.

This is the Backup & Recovery Manager server version.

9. Type **Y** to confirm the installation when prompted, **Do you want to continue?**

You can check the log, `/nsr/nsrmq/logs/nsrmq.log` for any issues.

Reconfiguring the server hostname for the NetWorker adaptor

If the NetWorker server does not appear in the list of systems, you can reconfigure the Backup & Recovery Manager adaptor for NetWorker.

This often occurs as a result of the following:

- The hostname of the Backup & Recovery Manager was changed.
- A new Virtual Appliance (OVA) was deployed for the Backup & Recovery Manager (despite having used the same hostname as before).
- The hostname was not provided at the time of installation or upgrade.

Note

To reconfigure a previously registered Backup & Recovery Manager NetWorker adaptor for the server hostname, you must provide the same username and password that is used during the initial installation. The error message, `unable to load SSL certificate` displays if the incorrect credentials are used.

Procedure

1. Stop the NetWorker adaptor:
 - On Windows, stop the adaptor service (nsrmqd)
 - On Linux, type the following command:


```
/etc/init.d/nsrmqd stop
```
2. Edit the `nsrmq.cfg` file:
 - Change the `nsrmq.cfg` file to update the `mq-host` entry to the new server.
 - Change the `nsrmq.cfg` file to update the `cert-file` entry to:


```
http://<new BRM hostname>/ucasCert
```
3. Register the NetWorker adaptor by using the following command:


```
nsrmqd.exe --mq-host=<brmhost> server=<NW server> --brm-username=<BRM user> --brm-password=<BRM user password>
```
4. Start the NetWorker adaptor:
 - On Windows, start the adaptor service (nsrmqd).
 - On Linux:


```
/etc/init.d/nsrmqd start
```

Adding a Data Domain system

[Managing Data Domain systems](#) on page 114 provides instructions on how to add, remove and modify Data Domain systems in the Backup & Recovery Manager.

Logging in to the Backup & Recovery Manager

You must log in to the Backup & Recovery Manager UI each time it is opened, or after an inactivity time out. The default user and password are `admin`, `changeme`

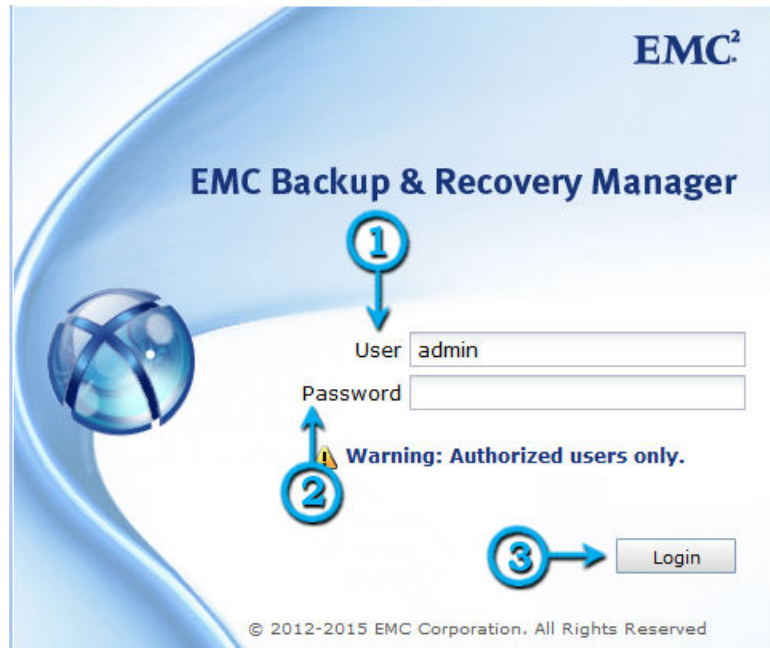
respectively. At the first login after installation, it is recommended to change the user and password from the default when prompted.

Procedure

1. Type the username.
2. Type the password.
3. Click **Login**.

The EMC Backup & Recovery Manager **Home** page opens.

Figure 42 Login window



The **User** and **Password** fields are required fields. After three failed attempts you are locked out for 15 minutes.

Figure 43 Failed login



Note

The Backup & Recovery Manager automatically logs out of sessions if for any reason the connection between the client and server is lost.

Common reasons for a login session to expire are:

- The Backup & Recovery Manager server is restarted
- The browser is closed completely while you are still logged in to the Backup & Recovery Manager
- All browser windows (or tabs) that are logged in to the Backup & Recovery Manager are closed, and not re-opened for 30 minutes or more
- Internet access is lost for more than 30 minutes.

At first login, you are prompted to change the password.

4. Type a new password in the **Password** field, and then type the new password in the **Confirm Password** field.

The password requirements are:

- Minimum of 9 characters
 - Minimum of 1 lowercase letter
 - Minimum of 1 uppercase letter
 - Minimum of 1 number
 - Minimum of 1 special character: !@#\$%^&*()-_
-

Note

Do not specify the \$ character at the beginning or middle of a password. The \$ character can be specified at the end of a password.

5. To save the password, click **Change Password**.

Figure 44 Change Password window

Change Password

Enter a new password:

Password

Confirm Password

Password Requirements:

1. Minimum of 9 characters in length
2. At least 1 lowercase letter
3. At least 1 uppercase letter
4. At least 1 numeric character
5. At least 1 special character: !@#\$%^&*()-_

3 →

NOTICE

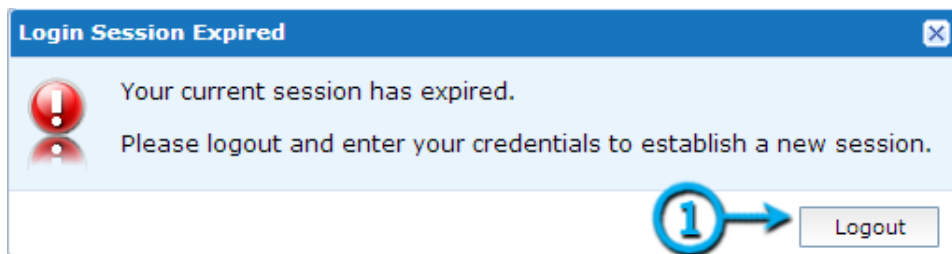
If you do not change the password from the default, you are prompted to do so each time you log in.

Reestablishing an expired session

Procedure

1. On the dialog box, click **Logout**.

Figure 45 Expired login session



2. To open the login screen, click **Login**.

Figure 46 Logout status



Disable the Backup & Recovery Manager adaptor for Avamar

Uninstalling the Avamar adaptor is only possible on Avamar 6.0.2 and 6.1.0. Beginning in 6.1 Service Pack 1, the adaptor is integrated into the Avamar software, and

uninstalling it can cause problems. Instead, disable the Backup & Recovery Manager adaptor for Avamar.

Disabling the Backup & Recovery Manager adaptor for Avamar 7.0 and earlier

Procedure

1. Stop the Avamar Management Console Server (mcs):

```
dpnctl stop mcs
```

2. Stop the adaptor:

```
adaptorctl.pl --stop
```

3. Disable the BrmService preference:

```
vi /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml
```

4. Change value for enableBrmService to `false`.

5. Remove the Backup & Recovery Manager files:

```
rm -rf /usr/local/avamar/var/brm
```

6. Start the Avamar mcs:

```
dpnctl start mcs
```

Disabling the Backup & Recovery Manager adaptor for Avamar 7.1 and later

Procedure

1. Stop the Avamar Management Console Server (mcs):

```
dpnctl stop mcs
```

2. Disable the BrmService preference:

```
vi /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml
```

3. Change the value for enableBrmService to `false`.

4. Start the Avamar mcs:

```
dpnctl start mcs
```

Uninstalling the Backup & Recovery Manager adaptor

You can uninstall the Backup & Recovery Manager adaptors if required by using the native rpm program for Avamar or the `uninstall` program for NetWorker.

Note

Uninstalling the Avamar adaptor is only possible on Avamar 6.0.2 and 6.1.0. Beginning in 6.1 Service Pack 1, the adaptor is integrated into the Avamar software, and uninstalling it can cause problems. Instead, disable the Backup & Recovery Manager adaptor for Avamar. Complete details for disabling the Avamar adaptor are available in [Disable the Backup & Recovery Manager adaptor for Avamar](#).

If required, uninstall the following adaptors:

- [Uninstalling the Backup & Recovery Manager adaptor for Avamar](#)

- [Uninstalling the Backup & Recovery Manager adaptor for NetWorker](#)

Uninstalling the Avamar adaptor

You can uninstall the Avamar adaptor by using the Linux rpm command.

Procedure

1. Stop the Avamar Management Console Server (mcs) database:
`dpnctl stop mcs`
2. Stop the adaptor:
`adaptorctl.pl --stop`
3. Stop the activemq:
`/usr/local/avamar-activemq/bin/activemq stop`
4. Disable the BrmService:
`vi /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml -`
change value for enableBrmService to false
5. Remove the brm files:
`rm -rf /usr/local/avamar/var/brm`
6. Remove the Avamar adaptor:
`sudo rpm -e avamar-adaptor`
7. Start the Avamar mcs database:
`dpnctl start mcs`

Uninstalling the NetWorker adaptor

You can uninstall the NetWorker server adaptor on Windows from the command prompt.

Procedure

1. Run the uninstall program located at, C:\Program Files (x86)\NetWorker Adaptor Service-1.0\Uninstall NetWorker Adapter for EMC Backup & Recovery Manager
2. Uninstall the NetWorker server adaptor on Linux and remove the Backup & Recovery Manager adaptor software package:
`rpm -e Uninstall NetWorkerAdaptor-1.0-linux-x64-installer.run`

CHAPTER 4

Alerts

This chapter includes the following topics:






- [Overview of Alerts](#)..... 84
- [System Summary](#)..... 84
- [Alerts columns](#)..... 85
- [Alert categories](#)..... 86
- [Hiding alerts](#)..... 88
- [Viewing hidden alerts](#)..... 88
- [Unhiding alerts](#)..... 89
- [Acknowledging alerts](#)..... 89

Overview of Alerts

The Alerts section allows you to view alerts (Errors and Warnings) for all monitored systems relating to backup failures, media requests, errors, and warnings that require immediate attention by the user. Errors and warnings for the Backup & Recovery Manager are also reported in Alerts.

The icons that are used in Alerts are listed in the following table.

Table 19 Alerts icons

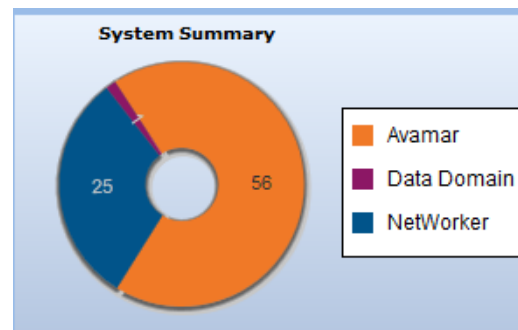
Icon	Description
	Error
	Warning
	Hide Selected
	Dismiss Selected
	View Hidden

System Summary

The Alerts System Summary provides information on Avamar, NetWorker, and Data Domain system errors and warnings.

The total number of errors and warnings for each system type are depicted in a pie chart with a legend.

Figure 47 Alerts summary chart



Individual bar charts depict the Total Errors and Total Warnings and which systems contain the most errors and warnings for the Worst Systems.

Figure 48 Worst Systems



Figure 49 Worst Systems



To obtain information on the Total Errors, or Total Warnings Worst Systems charts:

- Hover the cursor over any bar in the chart to display the worst system. In the worst system pop up, click **Launch** to open the native management console for the system.

Figure 50 Worst system launch



- Click any bar in the chart to display the list of errors or warnings for the worst monitored systems.
[Alerts columns](#) on page 85 provides complete details on the columns that are displayed in the worst systems list.

Alerts columns

The following table lists the columns in **Alerts** and their function.

Table 20 Alerts columns

Column	Description
Date/Time	Lists the date and time the alert occurred.
System	Lists the system on which the alert occurred.
Type	Lists the type of system on which the alert occurred: <ul style="list-style-type: none"> • Avamar • Data Domain • Backup & Recovery Manager

Table 20 Alerts columns (continued)

Column	Description
Category	Lists the category of the alert, such as Error, Warning, or System Alert.
Message	Lists the specific Error, Warning, or System Alert message that describes the alert. Multiple occurrences of the same message are combined. The number of occurrences is displayed as a link in brackets at the end of the message.

Alert categories

The following table lists the categories for system alerts.

Table 21 Alert categories

Item	Description
Warning	An alert that might be informational or require user intervention.
Error	An alert that requires immediate user intervention to avoid system component failure or data loss.
System Alert	An alert that Backup & Recovery Manager generates.
File system	An alert that is related to Data Domain system usage thresholds.
Replication	An alert that a Data Domain replication job generates. For example, problems with replication: <ul style="list-style-type: none"> • Pair status • Job progress • Process • Context performance

Excluding and including columns from the Alerts display

You can exclude and include columns from displaying in the tabular view.

Procedure

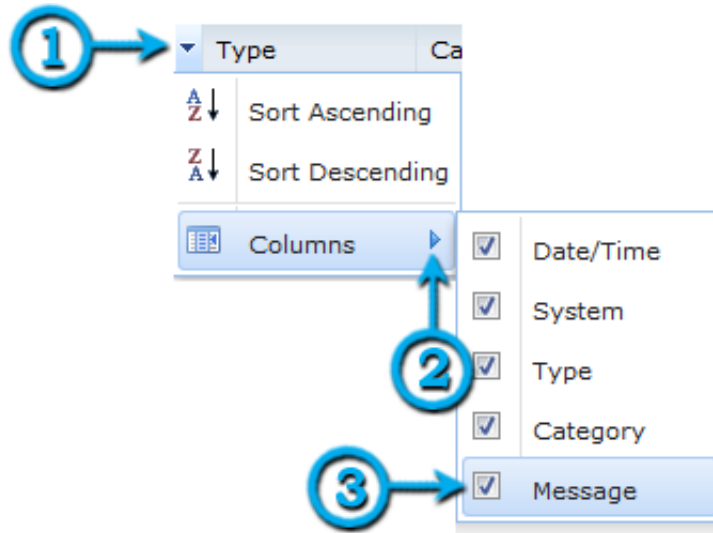
1. Click the arrow beside any column.
2. Click **Columns**.
3. Click the check box beside a column name to uncheck and exclude, or to check and include a previously excluded column.

NOTICE

All columns are included (checked) by default.

The following figure illustrates how to exclude or include columns.

Figure 51 Sort Alerts columns



Viewing repeated alerts

If an alert is repeated more than one time, a link is included in square brackets at the end of the message. The [repeated: 3] text at the end of a line indicates that there are three occurrences of the alert.

Figure 52 Repeated Alerts

Date/Time	System	Type	Category	Message
11:05 PM, Oct ...	IBISAVE08.LSS.EMC.COM	Avamar	Warning	perfbeat::outoftolerance mask=[] average=235.42 limit=23.5425 mbpersec=4.60 [repeated: 3]
2:02 PM, Oct 24	IBISAVE08.LSS.EMC.COM	Avamar	Error	hfscheck of cp.20121024180120 failed on error: MSG_ERR_NOLICENSE
2:59 AM, Oct 24	BRM Server	BRM	System Alert	/ has 16.3% space remaining 3
12:41 AM, Oct...	IBISAVE08.LSS.EMC.COM	Avamar	Warning	Address from reverse lookup failed to match client address. [repeated: 4]
2:03 PM, Oct 23	IBISAVE08.LSS.EMC.COM	Avamar	Error	hfscheck of cp.20121023180111 failed on error: MSG_ERR_NOLICENSE

To list all repeated alerts in a separate window, click [repeated: #].

Figure 53 Expanded repeated Alerts

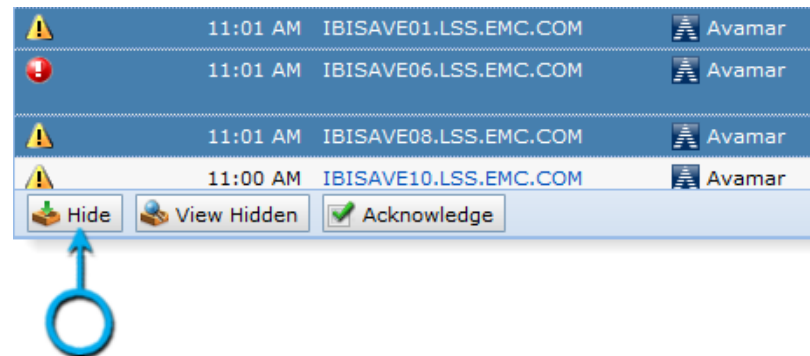
Alert Repeated 3 Times					
Date/Time	System	Type	Category	Message	
6:25 PM, Oct 24	IBISAVE08.LSS.EMC.COM	Avamar	Warning	perfbeat::outoftolerance mask=[] average=237.23 limit=23.7234 mbpersec=13.59	
2:35 PM, Oct 24	IBISAVE08.LSS.EMC.COM	Avamar	Warning	perfbeat::outoftolerance mask=[] average=144.44 limit=14.4442 mbpersec=11.15	
5:39 AM, Oct 24	IBISAVE08.LSS.EMC.COM	Avamar	Warning	perfbeat::outoftolerance mask=[] average=146.74 limit=14.6741 mbpersec=13.99	

Hiding alerts

You can hide alerts by selecting individual line items, by using multi-select Ctrl or Shift click, or by using multi-select Ctrl or Shift with the arrow keys, and then clicking Hide.

[Viewing hidden alerts](#) on page 88 provides details on how to view the previously hidden alerts.

Figure 54 Hide Alerts



NOTICE

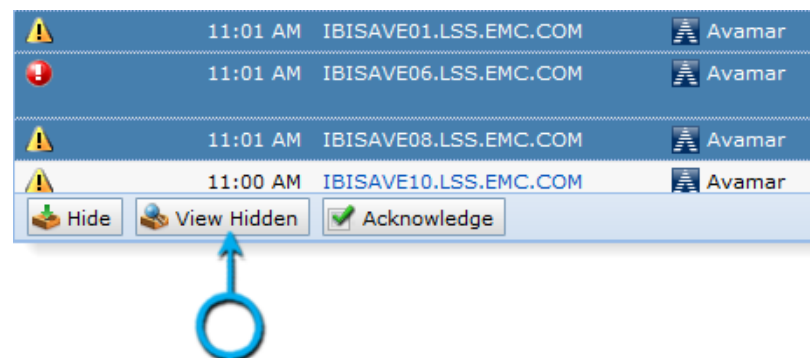
If an alert is hidden and another alert of same type is encountered on any monitored system, it will not appear in the system. Hidden alerts are not removed from the system.

Viewing hidden alerts

You can view alerts that were previously hidden by clicking View Hidden.

The **Hidden Alerts** window opens with a complete list of all hidden Errors and Warnings.

Figure 55 View previously hidden Alerts



Unhiding alerts

You can unhide alerts by selecting individual line items, by using multi-select **Ctrl** or **Shift** click, or by clicking **Select All** and then clicking **Unhide Selected**.

The previously hidden alerts will again be listed in Alerts.

Figure 56 Hidden Alerts



Acknowledging alerts

You can acknowledge alerts to dismiss, and remove them from the list.

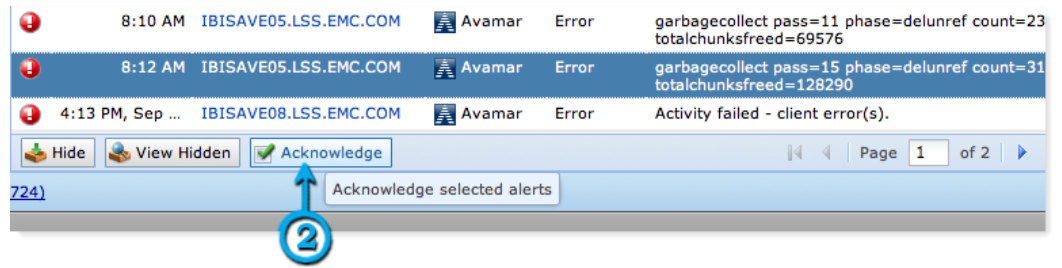
Procedure

1. Click the alerts to dismiss:
 - Select individual line items.
 - Use multi-select **Ctrl** or **Shift** click.
 - Use multi-select **Ctrl** or **Shift** with the arrow keys.
2. Click **Acknowledge**.

NOTICE

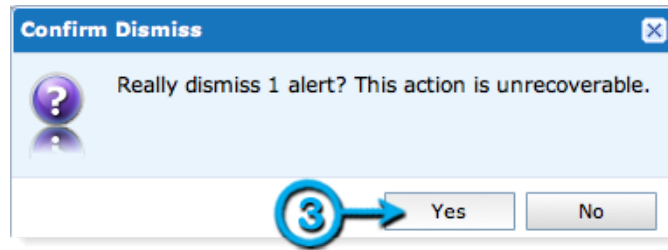
Acknowledging alerts permanently removes the alerts from the Backup & Recovery Manager.

Figure 57 Acknowledge Alerts



3. Click **Yes** to confirm the permanent removal of the selected alerts.

Figure 58 Dismiss Alerts



CHAPTER 5

Activities

This chapter includes the following topics:

- [Overview of Activities](#)..... 92
- [Activities columns](#)..... 92
- [Activities details](#)..... 93
- [Starting, stopping, and restarting backup jobs](#)..... 97
- [Avamar replication](#)..... 98

Overview of Activities

Click Activities to view detailed information on jobs that are running or completed on all monitored systems. This includes information on running backup operations, and replication jobs.

Activities columns

Backup and Replication Activities provides details on Avamar and NetWorker system backups and replications (Avamar).

The following table lists and describes the columns that are displayed in the Activities window.

Table 22 Backup details systems columns

Field	Description
Status	Lists the status of the backup operation. The status of operations that have failed, are running, completed, pending, cancelled, or aborted.
System	Lists the name of the Avamar or NetWorker system.
Protection Policy	Lists the policies that are associated with the NetWorker server.
Protection Type	Lists the group, client, or policy belonging to the NetWorker system.
Start	Lists the time that the backup began.
Duration	Lists the duration of the backup.
End	Lists the time that the backup completed.
Running	Indicates the number of group/client backups in progress for the specific backup operations.
Failed	Indicates the number of group/client failed backups for the specific backup operations.
Completed	Indicates the number of group/client completed backups for specific backup operations.
Pending	Indicates the number of group/client backups pending for the specific backup operations.
Storage Target	The server to which the data is backed up or replicated.

NOTICE

NetWorker client initiated backups (manual backups) are listed as ad hoc *<system name>* in the Group/Client column.

Excluding and including columns from the Activities display

You can customize the columns to display in the Activities window by excluding/including columns.

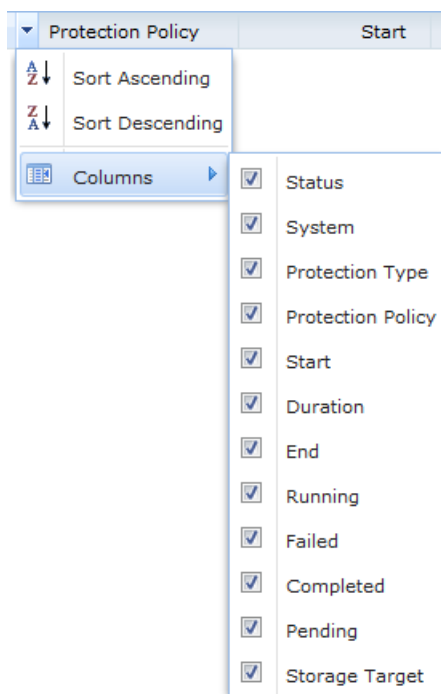
Procedure

1. Click the arrow beside any column.
2. Click **Columns**.
3. Click the check box beside a column name to uncheck and exclude, or to check and include a previously excluded column.

NOTICE

All columns are included (checked) by default.

Figure 59 Sort Activities columns



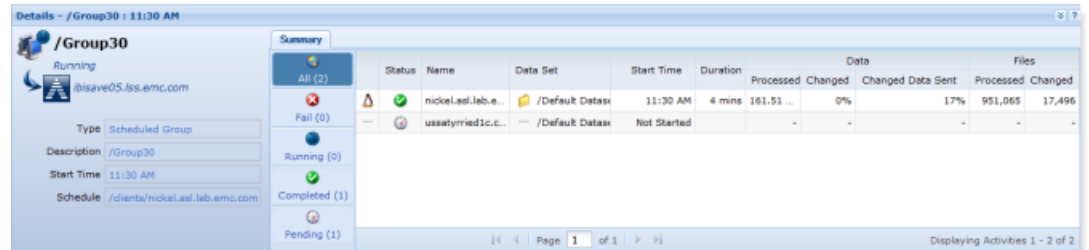
Activities details

The Backup Activities Details panel displays all configured systems with backup, replication (Avamar) jobs that failed, are pending, running or completed. Click on an individual server to display the Details panel with summary information.

Avamar backup activity details summary

The Details Summary grid displays additional details on specific Avamar backup groups and clients.

Figure 60 Backup activity details



The following table lists the Activities backup details fields.

Table 23 Avamar backup details systems fields

Field	Description
Status	Lists the specified group, or clients belonging to the group failed, are running, completed, or pending.
Name	Lists the name of the Avamar clients belonging to the selected group.
Data set	Lists the Data Set to which the client backup data is saved. An icon representing the backup type is included in the column.
Start Time	Lists the time that the backup began.
Duration	Lists the duration of the backup.
Data	<p>The data column includes the following sections:</p> <ul style="list-style-type: none"> • Processed: The amount of data that was processed during the backup. • Changed: The percentage of data that is new or modified on this machine. • Changed Data Sent: The percentage of the data in Changed that is sent to the backup server. The data sent to the backup server is typically less than 100% due to the effectiveness of deduplication. <p>The New Bytes column in the Avamar Activity monitor is not a column included in Backup & Recovery Manager. Calculate New Bytes by multiplying the value in Changed by the value in Changed Data Sent. For example, if Changed is 10% and Changed Data Sent is 50%, then $10\% \times 50\% = 5\%$.</p>
Files	<p>Lists the number of files that were processed during the job and how many of those files were changed.</p> <ul style="list-style-type: none"> • Processed

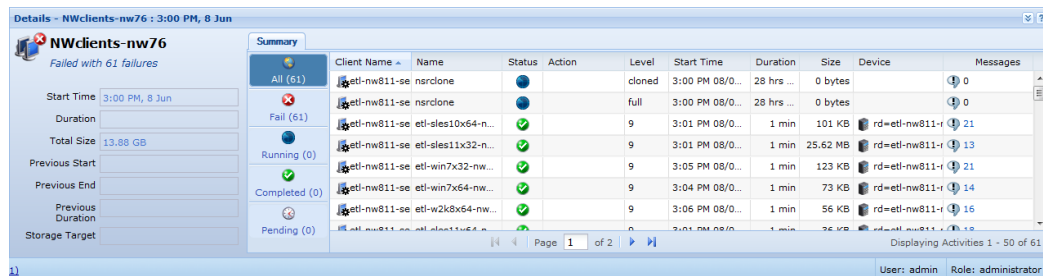
Table 23 Avamar backup details systems fields (continued)

Field	Description
	<ul style="list-style-type: none"> Changed

NetWorker backup activity details summary

The Details Summary grid displays additional details on specific NetWorker backup groups and clients.

Figure 61 NetWorker backup activity details

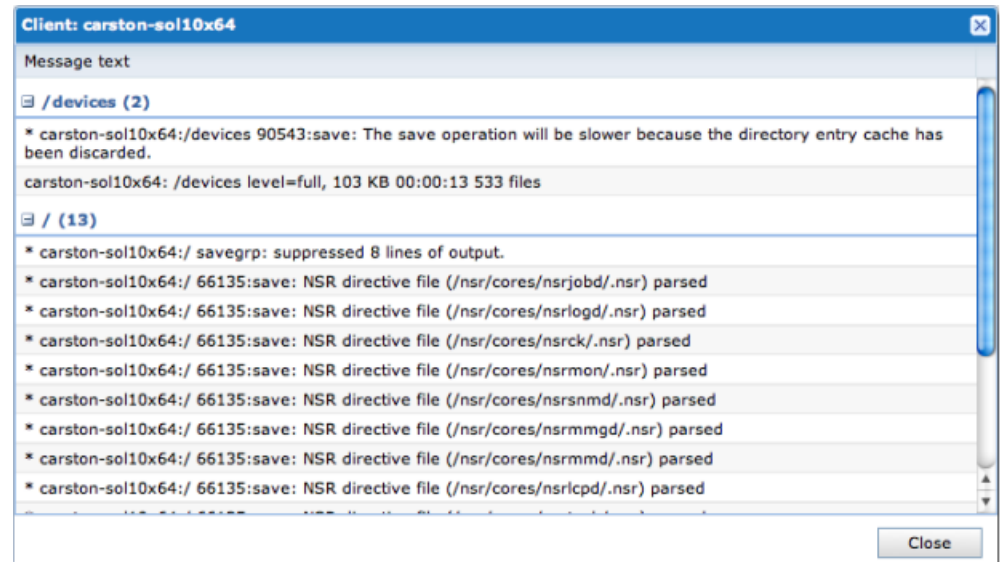


The following table lists the fields in the Activities backup details fields.

Table 24 NetWorker backup details systems fields

Field	Description
Client Name	Lists the name of the NetWorker client.
Save set	Lists the number of save sets in the backup operation. An icon representing the backup type is included in the column.
Status	Lists the current state of the backup job. For example, if it is currently running, complete, or if it failed.
Level	Lists the backup level that is used for the backup.
Action	Lists the Action that completed.
Start Time	Lists the time that the backup began.
Duration	Lists the duration of the backup.
Size	Lists the total size of the data that was backed up.
Device	The device to which the backup was written.
Messages	Lists the number of messages (Alerts or Warnings) that occurred during the backup. Click the number of messages to display the list of messages with their message text in a pop-up window.

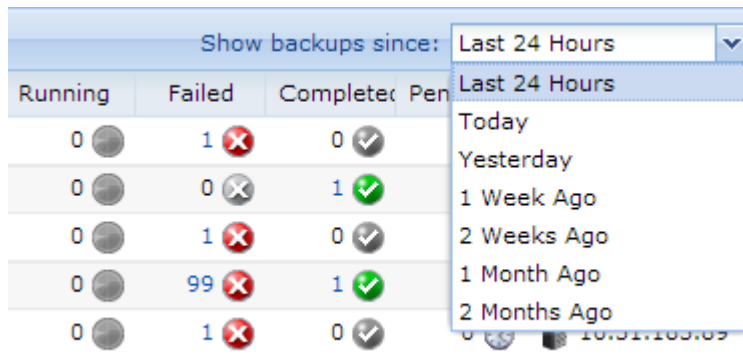
Figure 62 Message text



The following provides information on the columns in the details summary:

- The status column enables filtering of specific activity types and includes the count for each type:
 - Failed
 - Running
 - Completed
 - Pending
- Click Show backups since: To view backup status for a different time period. This option is available for:
 - Last 24 Hours
 - Today
 - Yesterday
 - 1 week ago
 - 2 weeks ago
 - 1 month ago
 - 2 months ago

Figure 63 Show backups since: options



Activities provides detailed information on setting up and monitoring Avamar system replication.

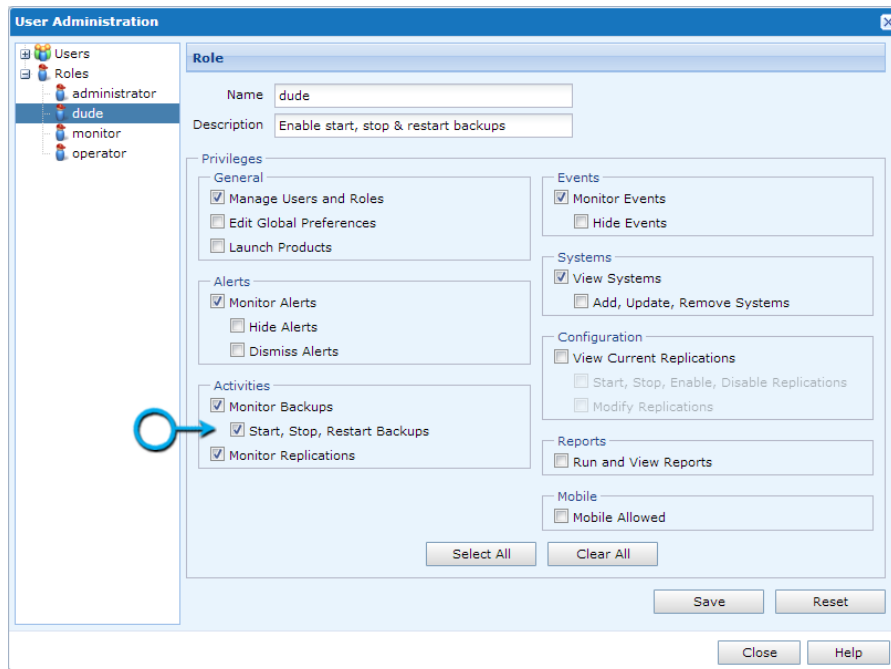
Starting, stopping, and restarting backup jobs

The Backup & Recovery Manager provides the ability to start, stop, and restart group backup jobs from Activities in Backup & Recovery Manager.

Before you begin

Only user roles with **Start, Stop, Restart Backups** enabled in **User Administration > Role** can perform these actions for group backup jobs. You can start and restart failed or stopped backup jobs, and stop backup jobs while they are running. The following figure illustrates the **Start, Stop, Restart Backups** option enabled in the **Activities** section for a **Role**.

Figure 64 Start, Stop and Restart permission



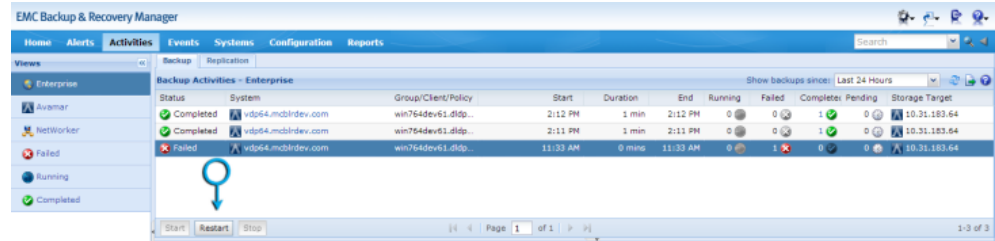
Procedure

1. Select the server or system for which to start, stop or restart the job.

2. Click **Start**, **Restart**, or **Stop** as required.

Results

The following figure illustrates the **Start**, **Restart** and **Stop** options for backup jobs. **Figure 65** Start, Restart and Stop backup jobs



Note

Restart is not supported for VMware backups, or NetWorker Policy based backups in **Activities** and is disabled. Use the **Start** button to start, or restart VMware, or NetWorker Policy based backups.

Avamar replication

Avamar replication transfers data from a source Avamar server to a destination Avamar server. You can restore all data from the destination server back to primary storage without having to stage the data through the source Avamar server.

To stop a configured replication operation from the **Activities Replication** section, click the row containing the running replication job and click **Stop**.

Avamar replication fields

The following table lists the Activities Replication fields.

Table 25 Avamar replication activities fields

Field	Description
Status	Current replication status. One of the following options: <ul style="list-style-type: none"> Running Not Running Not Running, Suspended Running, Suspended The Avamar Administration Guide provides complete details on these replication operation states.
Source System	The primary storage Avamar server from which the data is replicated to the destination/target Avamar server.
Target System	The destination to which the Avamar server replicated data is saved.
Size	The size of the data replicated.
Schedule	Date and time the replication operation is scheduled to start.

Table 25 Avamar replication activities fields (continued)

Field	Description
Start Time	The time the replication operation started.
Duration	The length of time the replication operation ran from start to end.
End Time	The time the replication operation ended.
Next Run	The next scheduled replication operation.

The following table describes the columns in the Avamar replication Activities system summary.

Table 26 Avamar replication details summary fields

Field	Description
Client Name	The name of the Avamar client.
Backup Number	The number that is assigned to the backup/replication job.
Status	Current replication status. One of the following: <ul style="list-style-type: none"> • Completed • Running • Failed
Plug-in Type	The Avamar plug-in that is used for the client.
Size	The size of the data replicated.
Start Time	The time the replication operation started.
End Time	The time the replication operation ended.
Duration	The length of time of the replication operation ran from start to end.

CHAPTER 6

Events

This chapter includes the following topics:

- [Overview of Events](#)..... 102
- [Events columns](#)..... 102
- [Events categories](#)..... 102
- [Excluding columns from the display](#)..... 103
- [View repeated events](#)..... 103
- [Hide events](#)..... 104
- [View hidden events](#)..... 104
- [Unhide events](#)..... 105

Overview of Events

Click Events to view all events such as configuration changes, and user logins generated by monitored systems in the enterprise. The ability to filter and acknowledge events is also available.

Events columns

The following table lists the Events columns and their function.

Table 27 Events section columns

Column	Description
Date/Time	Lists the date and time the event occurred.
System	Lists the system on which the event occurred. Clicking the system opens the system details.
Type	Lists the type of system on which the event occurred: <ul style="list-style-type: none"> • Avamar • NetWorker • Data Domain
Category	Lists the type of event. Events categories describes the categories that are used in the Events section.
Message	Lists the specific Error or Warning message that describes the event. View repeated events provides information on viewing repeated events.

Events categories

The following table lists the categories for system events.

Table 28 Event categories

Category	Description
Audit	An Avamar system record of actions that are initiated by users.
Garbage Collection	Avamar garbage collection status.
Index	System index related events.
Information	Informational event messages.
Media	NetWorker device and storage related events.
Policy	Policy related events.
Savegroup	NetWorker savegroup related events.

Table 28 Event categories (continued)

Category	Description
Warning	Critical system failure messages.
Write complete	Indicates that the write operation that is completed.

Excluding columns from the display

You can customize the events window by excluding/including the columns that display in the tabular view.

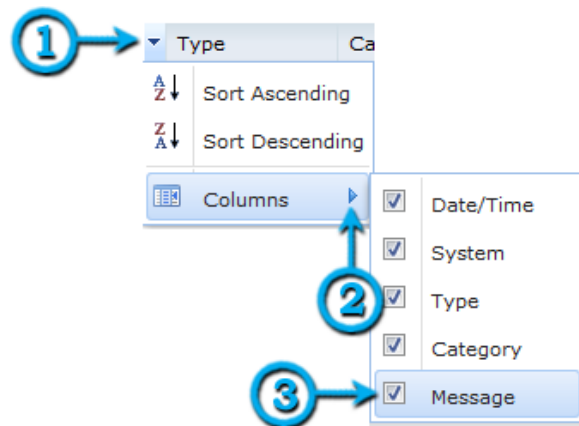
Procedure

1. Beside any column, click the arrow.
2. Click **Columns**.
3. To exclude the column, clear the checkbox, or to include a previously excluded column, select the checkbox.

NOTICE

All columns are selected by default.

Figure 66 Sort Events columns



View repeated events

If an event is repeated more than one time, a link is included in square brackets at the end of the message. The text, [repeated: 9] at the end of a line indicates that there are 9 occurrences of the event.

Click **repeated:** to list all repeated events in a separate window.

Figure 67 List repeated Events

Date/Time	System	Type	Category	Message
8:27 AM, Sep 22	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.
6:28 PM	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.
5:15 AM	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.
8:26 AM, Sep 20	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.
5:16 AM, Sep 19	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.
8:25 AM, Sep 18	bu-dt3-3.lss.emc.com	NetWorker	Savegroup	savegroup notice: Sybase_Partial completed, Total 1 client(s), 1 Succeeded. Please see group completion details for more information.

Hide events

You can hide listed events by selecting individual line items, using multi-select Ctrl or Shift click, or by using multi-select Ctrl or Shift with the arrow keys and clicking Hide.

The selected events will no longer be listed in Events.

The following figure illustrates the list of events available to hide.

Figure 68 Hide events

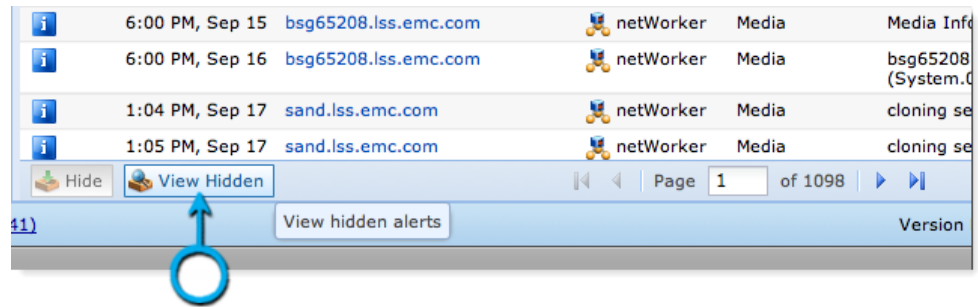
Date/Time	System	Type	Category	Message
6:00 PM, Sep 14	bsg65208.lss.emc.com	netWorker	Media	Media Info:
6:00 PM, Sep 14	bsg65208.lss.emc.com	netWorker	Media	Media Info: BSG69010_
6:00 PM, Sep 15	bsg65208.lss.emc.com	netWorker	Media	Media Info:
6:00 PM, Sep 16	bsg65208.lss.emc.com	netWorker	Media	bsg65208.lss.emc.com (System.00)
1:04 PM, Sep 17	sand.lss.emc.com	netWorker	Media	cloning sess
1:05 PM, Sep 17	sand.lss.emc.com	netWorker	Media	cloning sess

View hidden events

You can view events that were previously hidden. Click View Hidden, and the Hidden Events window opens with a complete list of all hidden errors and warnings.

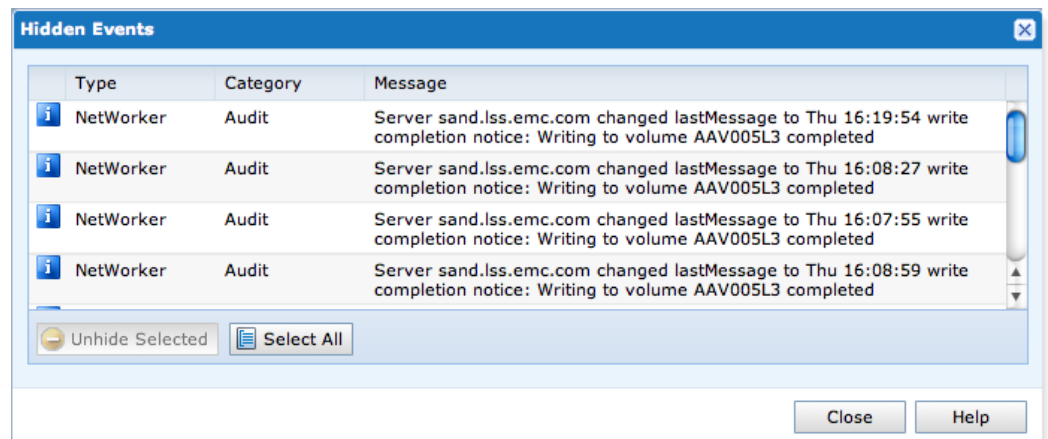
The following figure illustrates the View Hidden button.

Figure 69 View Hidden



The following figure illustrates the Hidden Events window.

Figure 70 Hidden Events



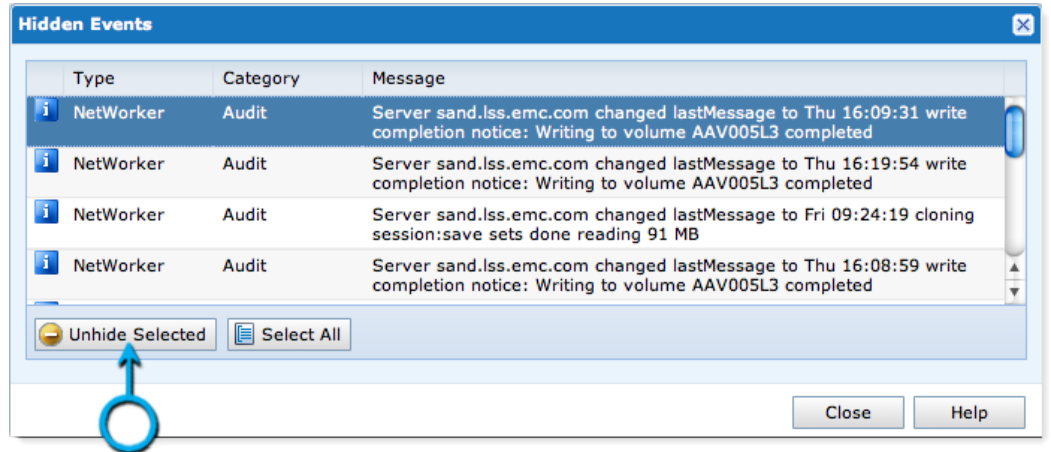
Unhide events

You can unhide previously hidden events by selecting individual line items, using multi-select Ctrl or Shift click, or clicking Select All and then clicking Unhide Selected.

Previously hidden events will again be listed in Events.

The list of events to unhide are illustrated in the following figure.

Figure 71 Unhide Selected events



CHAPTER 7

Systems

Click Systems to view detailed information for all systems in the enterprise. This chapter includes the following topics:

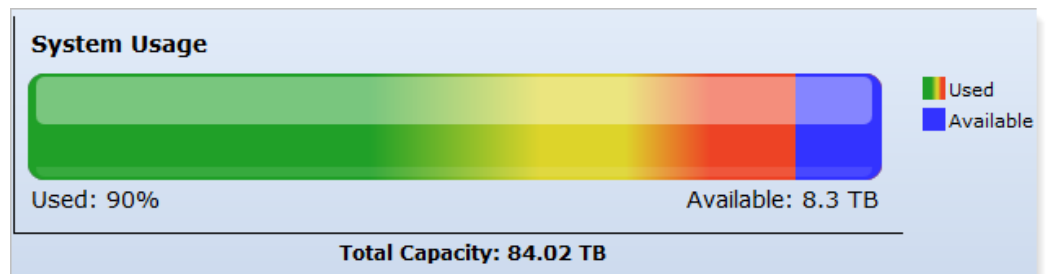
- [Systems usage graph](#).....108
- [Systems Display](#) 108
- [Launching the native system consoles](#)..... 110
- [Managing Data Domain systems](#)..... 114
- [Removing a system](#).....117
- [Adding or modifying customer information](#)..... 118

Systems usage graph

The system usage graph uses a color scale to represent the level of system usage.

- Green—represents a system with a safe level of available space.
 - Yellow to orange—indicates that the system is approaching a less acceptable amount of available space (80% warning threshold).
 - Red—indicates that the system has reached an unacceptable level of available space and requires intervention (95% warning threshold).
 - Blue—represents the amount of available space on the system.
- The following figure is an example of a System usage graph.

Figure 72 System Usage graph



Systems Display

The primary portion of the systems page is the systems list that is displayed in a tabular view.

Figure 73 Available systems

Type	Status	System Name/Model	Usage	Capacity	Days Until Full	Version
	✓	griffin-dd8.asl.lab.emc.com DD670	Used: 1% Available: 18 TB	18.29 TB	n/a	5.1.0.9-282511
	✓	dd660-2.lss.emc.com DD660	Used: < 1% Available: 12.85 TB	12.97 TB	n/a	5.3.0.2-351469
		griffin-dd0.asl.lab.emc.com	n/a	n/a	n/a	5.3.0.4-365563
	✓	qa-bw-4-mgmt.chaos.local DD880	Used: 75% Available: 20.88 TB	84.08 TB	n/a	5.3.0.4-366182
	✓	dd120-22.datadomain.com DD120	Used: 1% Available: 330.3 GB	334.1 GB	n/a	5.3.1.0-358461

Clicking a system in the list displays the System Details on the lower half of the window.

Figure 74 System details

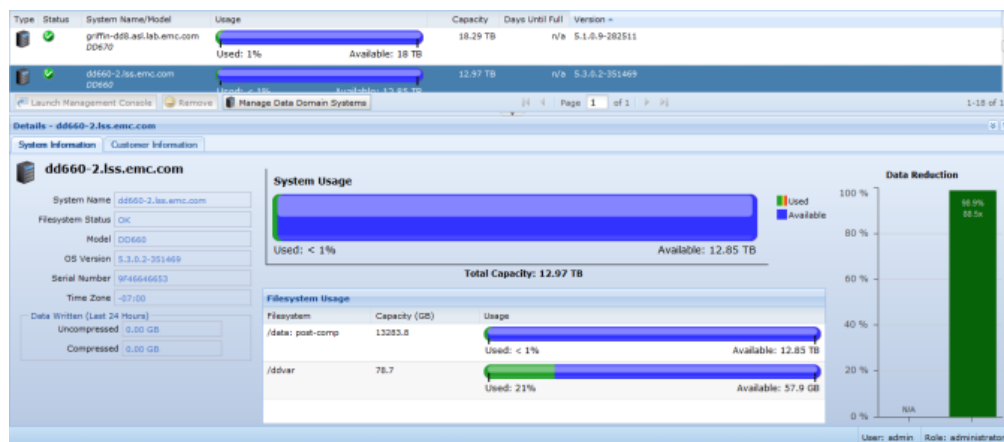
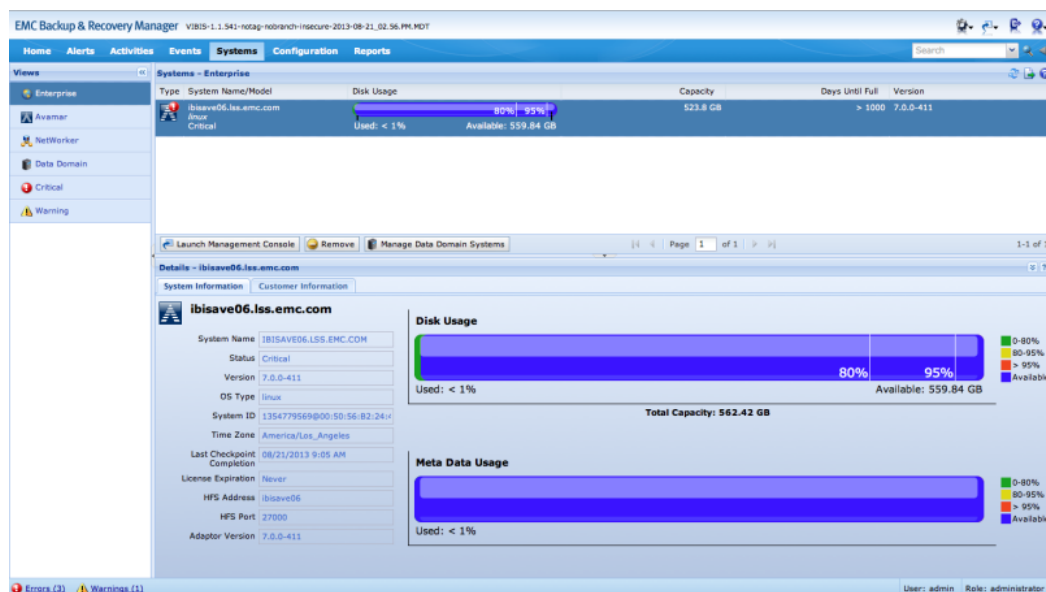


Figure 75 Avamar System details with Meta Data usage graph



The following table displays information about managed systems.

Table 29 System types and states






Type	Description
	Avamar server
	NetWorker server
	Data Domain server
	System critical notification
	System warning notification

Table 29 System types and states (continued)

Excluding columns from Systems

You can select columns to exclude/include in the systems display.

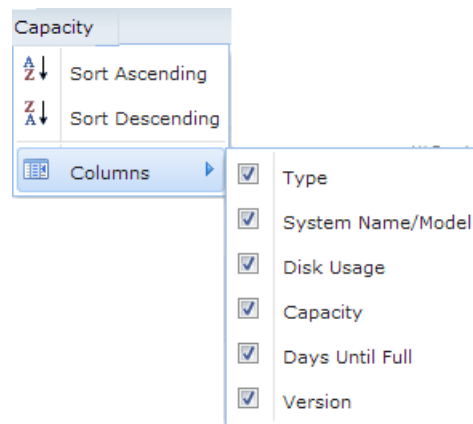
Procedure

1. Click the arrow beside any column.
2. Click **Columns**.
3. Click to clear the check box beside a column for which to exclude, or to check and include a previously excluded column.

NOTICE

All columns are included (checked) by default.

The following figure illustrates the available columns.

Figure 76 Available columns

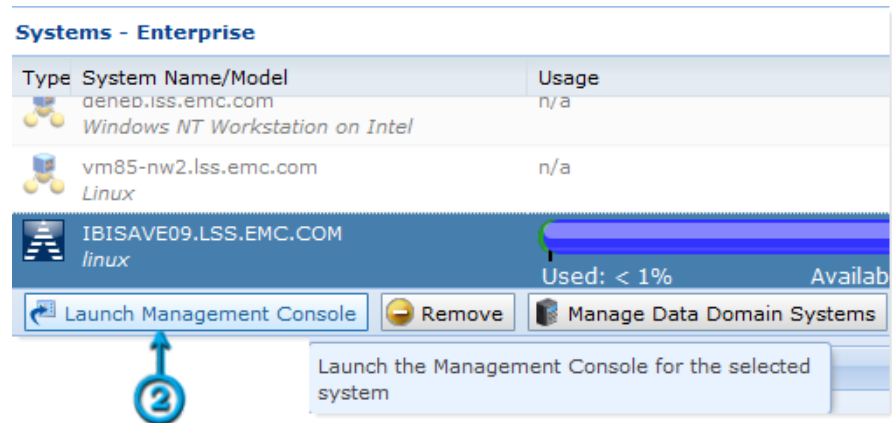
Launching the native system consoles

You can launch the Avamar Administrator, NetWorker Management Console, and the Data Domain Enterprise Manager from the System Details window.

Procedure

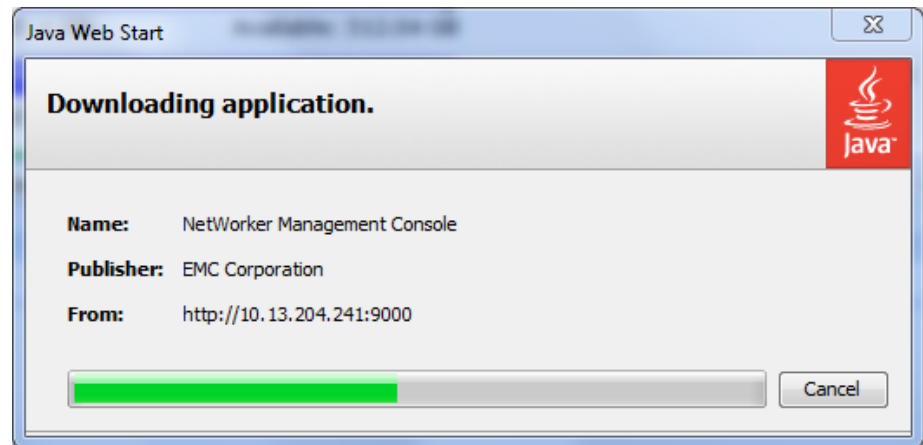
1. In the **Systems** window, click the server for which to launch the native console. Launch the Avamar Administrator.
2. Click the Launch Management Console.

Figure 77 Launch the Management Console



The **Java Web Start** window displays with the status of the NetWorker Management Console download.

Figure 78 Java Web Start



3. Type the **Username** and **Password** in the respective fields to start the appropriate native console.
 - Avamar Administrator

Figure 79 Avamar Administrator Logon

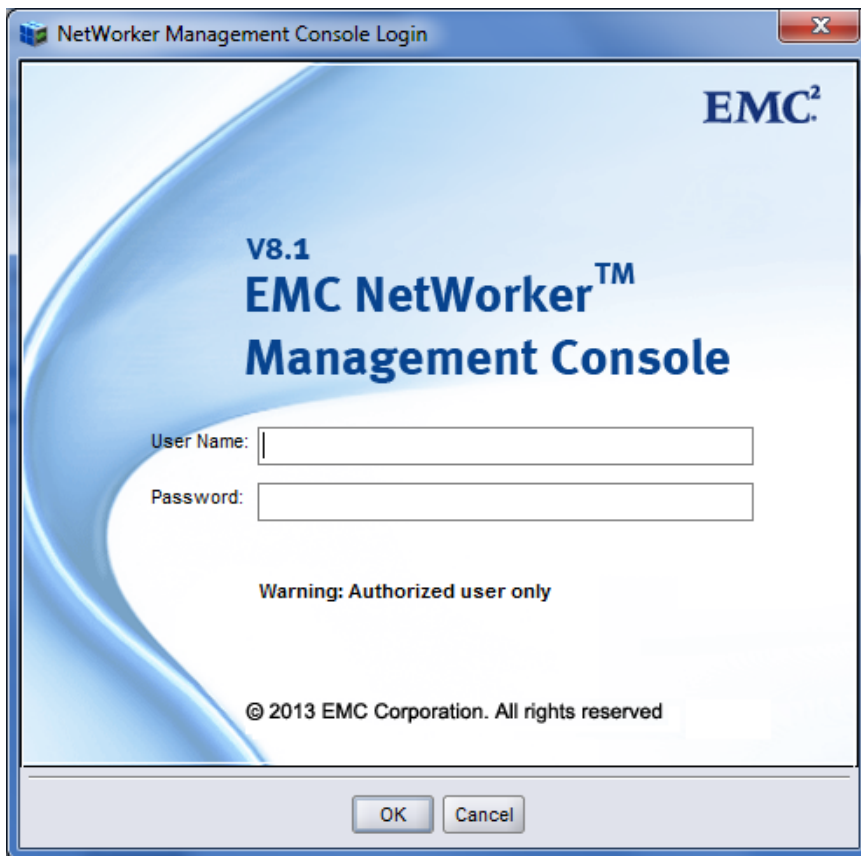


NOTICE

The Avamar Installation Manager is a function of the Avamar Administrator.

- NetWorker Management Console

Figure 80 NMC logon



The screenshot shows a Windows-style dialog box titled "NetWorker Management Console Login". The background is light blue with a white wave-like graphic on the left. The EMC logo is in the top right corner. The text "V8.1 EMC NetWorker™ Management Console" is centered. Below this are two input fields: "User Name:" and "Password:". A warning message "Warning: Authorized user only" is centered below the fields. At the bottom, there is a copyright notice "© 2013 EMC Corporation. All rights reserved" and two buttons: "OK" and "Cancel".

- Data Domain Enterprise Manager

Figure 81 Data Domain Enterprise Manager logon



The screenshot shows the login screen for Data Domain Enterprise Manager. The background is light blue with a white wave-like graphic on the left. The EMC logo with the tagline "where information lives" is in the top right corner. The text "Data Domain Enterprise Manager" is centered. Below this are two input fields: "Username" and "Password:". A blue link "[Login using enhanced security.](#)" is centered below the fields. At the bottom, there is a "Login" button and a copyright notice "Copyright © 2005-2010 EMC Corporation. All Rights Reserved."

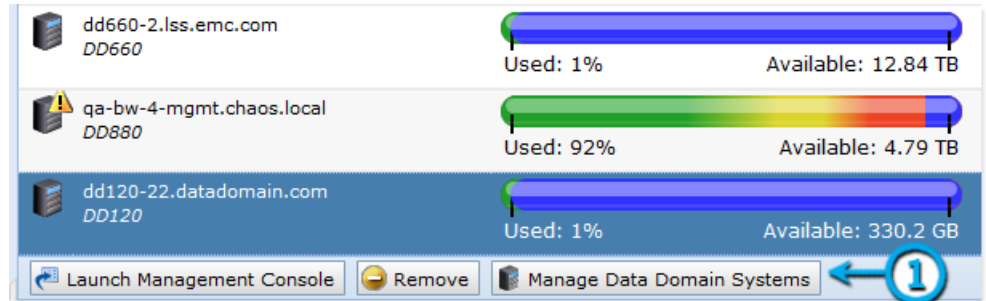
Managing Data Domain systems

In the Systems window, you can add, update, or delete Data Domain systems to be monitored in the Backup & Recovery Manager.

Procedure

1. In the **Systems Details** window, click the **Manage Data Domain Systems** to add, change credentials, remove or test a Data Domain system.

Figure 82 Data Domain system



2. In the **Manage Data Domain Systems** window:

- Click **Add** to add a new system and complete the fields in the **Add Data Domain System** dialog box.

Figure 83 Manage Data Domain Systems

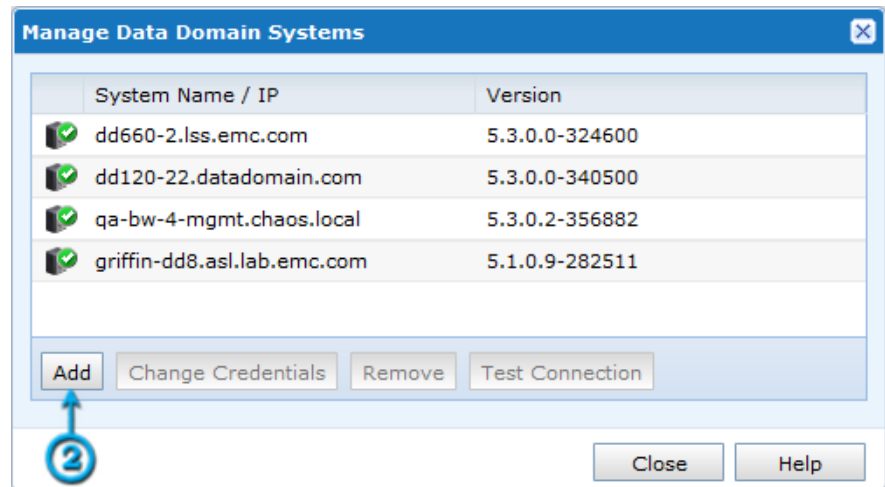


Figure 84 Add a Data Domain System

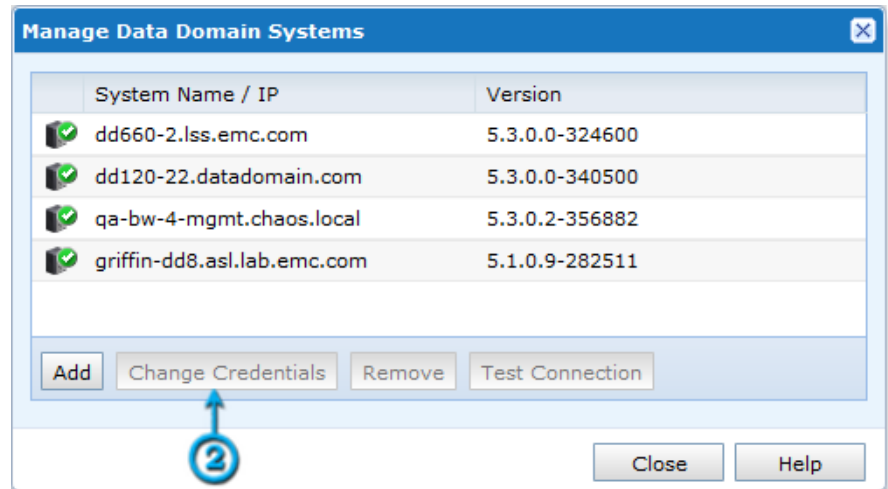
A connection status window opens to verify the connection. If the connection fails, a message displays.

A system for which the initial connection attempt fails can still be added.

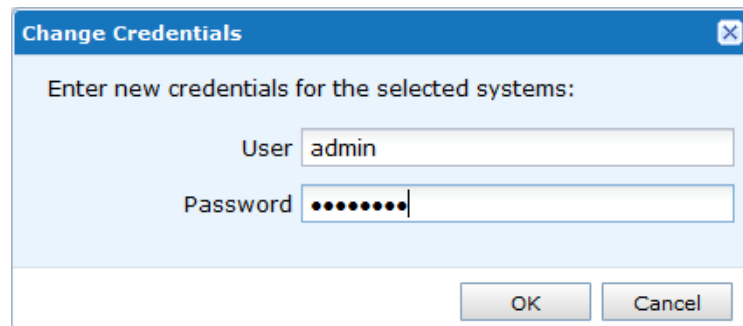
Figure 85 Connection failed error

Figure 86 Successful connection test

- Click **Change Credentials** to change the access credentials for a selected system.

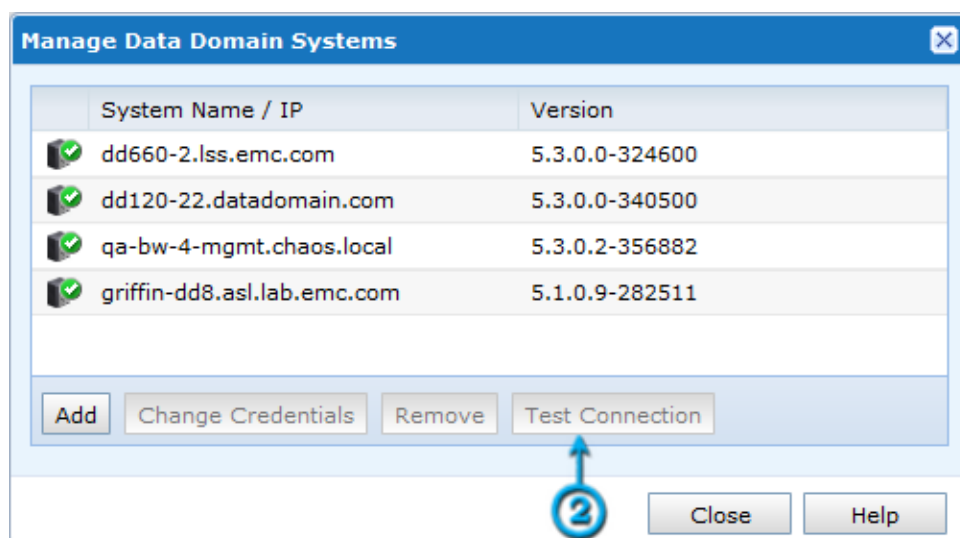
Figure 87 Change Data Domain credentials

- Type the **User** and **Password** in the respective fields.
Figure 88 Change Credentials fields

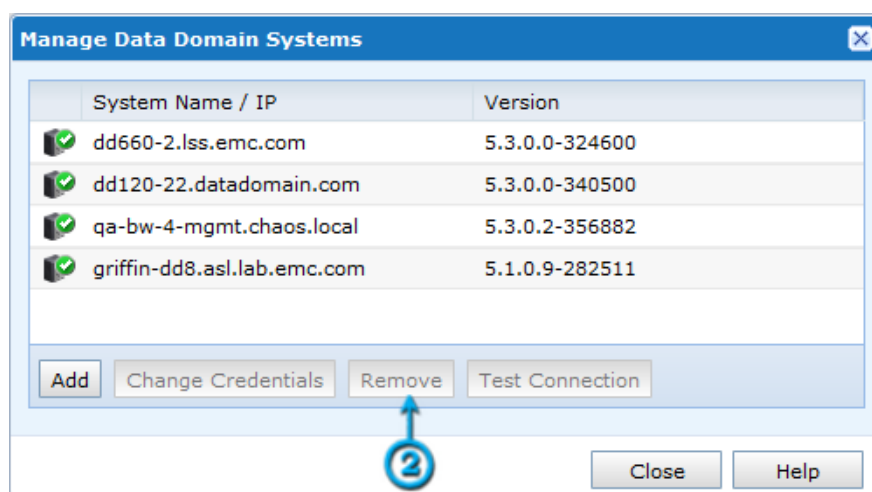


- Select a Data Domain system from the list and click **Test Connection** to verify that the system is connected.

Figure 89 Test Connection window



- Select a Data Domain system to remove from the list and click **Remove**.
Figure 90 Remove Data Domain systems

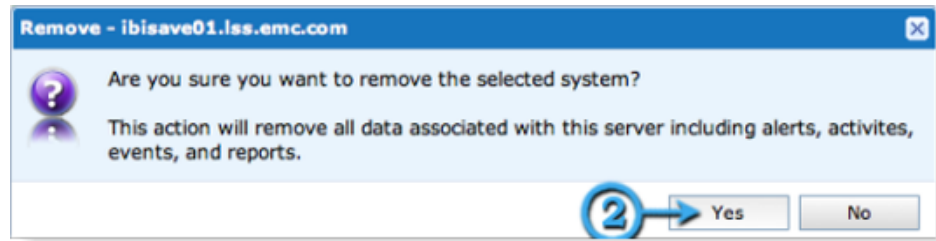


Removing a system

You can remove an Avamar, NetWorker, or Data Domain system from the Backup & Recovery Manager by selecting the system from the list of available systems.

Procedure

1. Click to select a system and then click **Remove**.
2. Click **Yes** when prompted to verify the removal.

Figure 91 Remove the selected system prompt**Results**

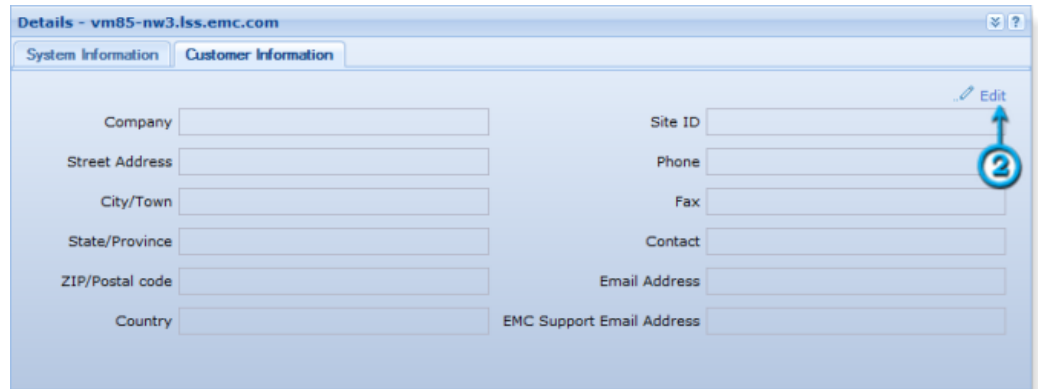
The system is no longer displayed in the systems list.

Adding or modifying customer information

Complete the fields in the Customer Information window. For geographically distributed environments, this section provides a location to keep information for specific system details.

Procedure

1. Click the system for which to edit the customer information.
2. Click **Edit** in the **System Information** panel.

Figure 92 Customer Information

3. Make the appropriate changes and click **Save**.

CHAPTER 8

Configuration

This chapter includes the following topics:

- [Overview of Configuration](#)..... 120
- [Excluding and including columns from Configuration](#)..... 120
- [Adding or modifying Avamar replication jobs](#)..... 121
- [Starting and stopping Avamar replication jobs](#)..... 125
- [Disabling and enabling replication jobs](#)..... 125

Overview of Configuration

Click Configuration to add or modify Avamar replication jobs. Avamar replication transfers data from a source Avamar server to a destination Avamar server. All data can be restored from the destination server back to primary storage without having to stage the data through the source Avamar server.

The details included for replicated Avamar servers are listed in the following table.

Table 30 Avamar replication configuration columns

Field	Description
Source System	The server from which the original data is copied.
Target System	The server to which the copied data is replicated.
Current State	Describes the state of the replication activity. The states are Idle, Queued, Running, Succeeded/Failed.
Last Run	The most recent replication that completed. The Last Run column links directly to the replication activity details.
Next Run	The next scheduled replication operation.

Excluding and including columns from Configuration

You can customize the display by excluding/including columns from the display in Configuration.

Procedure

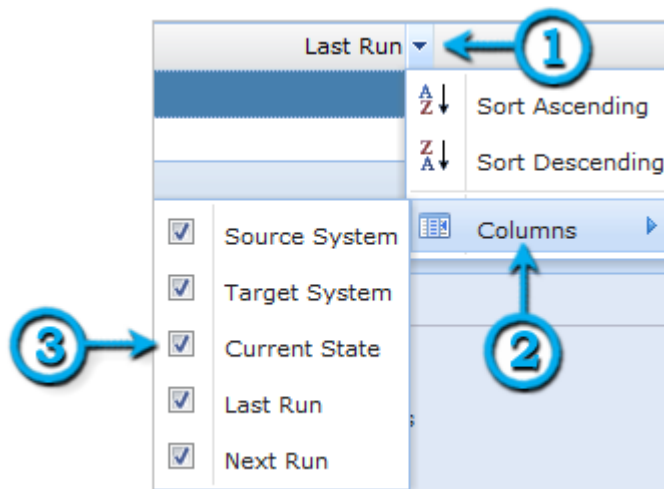
1. Click the arrow beside any column.
2. Click **Columns**.
3. Click the check box beside a column to uncheck and exclude, or to check and include a previously excluded column.

NOTICE

All columns are included (checked) by default.

The following figure illustrates the available columns.

Figure 93 Configuration columns



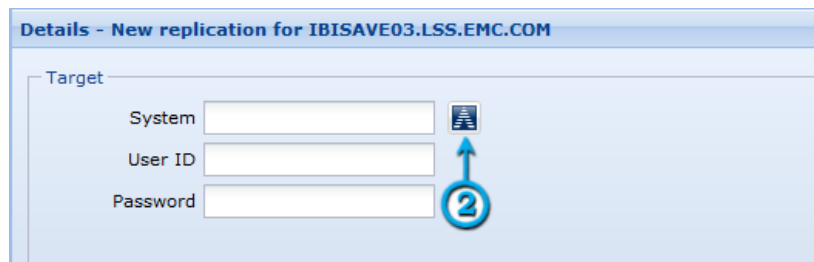
Adding or modifying Avamar replication jobs

You can add or modify Avamar replication jobs from the Backup & Recovery Manager.

Procedure

1. Select the source system for which to configure replication.
2. In the **Target** section, type the name of the destination system in the **System** field or click the Avamar icon to select an Avamar system from a list.

Figure 94 Avamar Target system



3. When you click the Avamar icon, a list of available Avamar systems opens.

Figure 95 Avamar systems list

System Name ^	Version	Capacity
AV000001.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000002.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000003.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000004.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000005.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000006.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000007.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000008.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000009.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000010.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000011.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000012.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000013.LAB.LOCAL	6.1.0-78	7248.4 GB
AV000014.LAB.LOCAL	6.1.0-78	7248.4 GB

Search:

4. In the **Schedule** section, specify the **Start Time** for the daily replication (default) from the drop-down list.

Figure 96 Replication schedule

Schedule

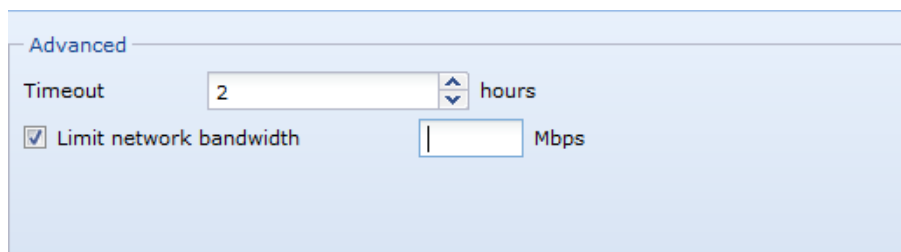
Schedule

Start Time

5. In the **Advanced** section:
 - a. Click the arrows to include a value (in hours) in the **Timeout** field.
 - b. Type a value in the **Mbps** field.

The Limit network bandwidth field sets the network utilization throttling that is used to specify the maximum average network utilization that is allowed in Mega Bits Per Second (Mbps). If the replication operation exceeds this setting, it is throttled back by introducing delays until the average network utilization falls below the specified threshold.

Figure 97 Timeout and Limit network bandwidth fields



6. In the **Backup Retention** section, select the appropriate value as listed in the following table.

Table 31 Backup Retention options

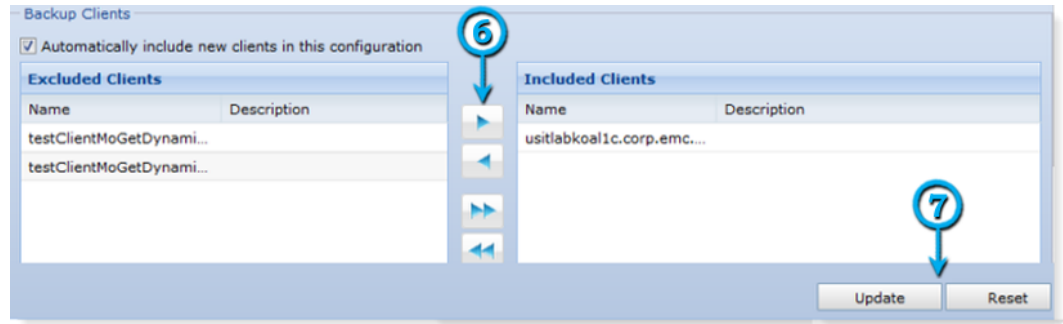
Option	Description
All Options	All Options checks all selections to replicate all backups.
Daily	Filters daily backups by retention level to replicate them.
Weekly	Filters weekly backups by retention level to replicate them.
Monthly	Filters monthly backups by retention level to replicate them.
Yearly	Filters yearly backups by retention level to replicate them.
Not Tagged	The Not Tagged option replicates backups without any retention level.

Figure 98 Available options for backup retention



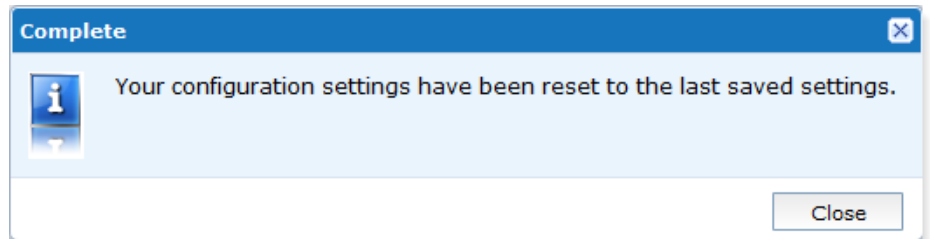
7. In the **Backup Clients** section:
 - a. Use the arrows to move clients between **Included Clients** and **Excluded Clients**.
 - b. Use the **Ctrl** and **Shift** keys with the arrow keys to select more than one client to move.
 - c. If required, click the check box to enable **Automatically include new clients to this configuration?**
8. Click **Reset** to discard changes or **Create** to save changes to the replication settings. You are notified when the settings are reset to the last saved configuration.

Figure 99 Backup Clients

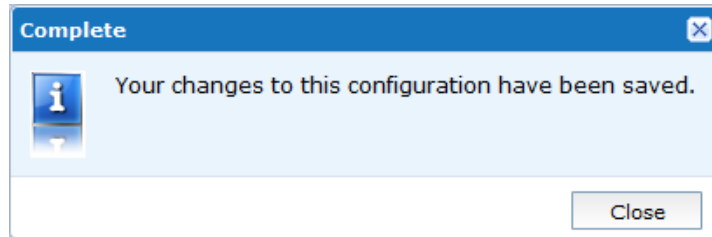


9. Click **Close** to close either of the following dialogs.

- The reset **Complete** dialog.
Figure 100 Completion status



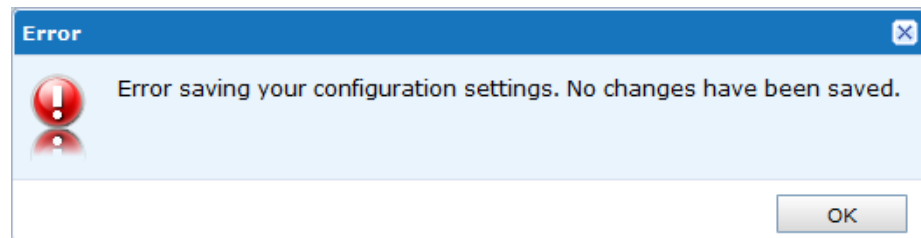
- The update **Complete** dialog.
Figure 101 Change status



Results

If the configuration is not successfully saved, an error is displayed.

Figure 102 Configuration error



NOTICE

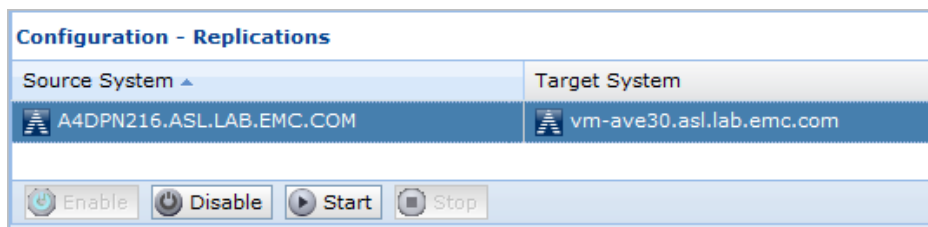
If you select another configuration, or leave the configuration section without clicking Create or Update, the configuration is reset to its previous state and not saved.

Starting and stopping Avamar replication jobs

The Backup & Recovery Manager provides the ability to start and stop Avamar replication jobs. The state of the replication job, Queued, Running, or Idle is displayed in the Status column.

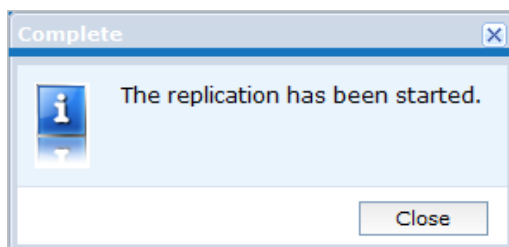
- Clicking **Start** sends a start request to the Avamar system. The status column changes to Queued until the Avamar system reports back that the replication operation has started, at which time the status changes to Running.
- Clicking **Stop** sends a stop request to the Avamar system. The status column changes to Queued until the Avamar system reports back that the replication operation has stopped, at which time the status changes to Idle.

Figure 103 Start a replication

**NOTICE**

Queued icons specific for a job queued to start and to stop differentiate between the two operations.

Figure 104 Replication started



Disabling and enabling replication jobs

The Backup & Recovery Manager provides the ability to disable or enable replication jobs rather than removing the jobs. Removing replication jobs also removes configuration settings.

Procedure

- Click **Disable** to stop future replication operations from running while preserving all current replication settings. Use this rather than Remove to stop replication jobs without losing configured settings.

- Click **Enable** to begin running configured replication jobs again as previously scheduled.

CHAPTER 9

Settings

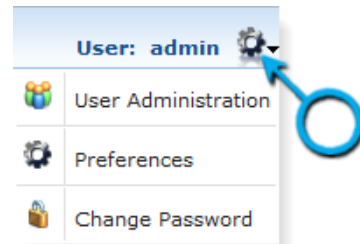
This chapter includes the following topics:

- [Introduction to settings](#)..... 128
- [User Administration](#)..... 128
- [Preferences](#)..... 133
- [Changing a password](#)..... 138
- [Resetting the admin password](#)..... 139

Introduction to settings

Clicking the Settings icon provides the ability to configure settings in the Backup & Recovery Manager for the environment, users, and preferences.

Figure 105 Settings menu

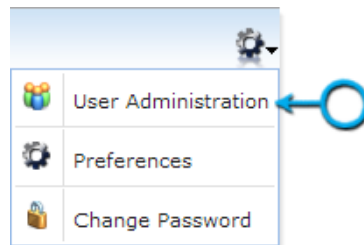


User Administration

Perform the following steps to configure users and roles.

1. Choose User Administration to configure users and roles.

Figure 106 User Administration



2. On the left panel, click **Users**.

Users

The Users section provides the ability to Add, Edit, Remove and Lock and Unlock users in the Backup & Recovery Manager.

Adding a user

Administrators can add new users to the Backup & Recovery Manager.

NOTICE

Administrator privileges are required to add new users.

Procedure

1. In the **User Administration** window, click **Add**.
2. In the **User** window, complete the fields in the **Profile** section.
3. In the **Authentication** section, type a **Password** and **Confirm** the password for Local (default) authentication.

The password requirements are:

- Minimum of 9 characters
- Minimum of 1 lowercase letter
- Minimum of 1 uppercase letter
- Minimum of 1 number
- Minimum of 1 special character

Note

Do not specify the \$ character at the beginning or middle of a password. The \$ character can be specified at the end of a password.

4. Click **Save**.
5. To exit the **User** window, click **Close**.

Figure 107 Add a user

Editing an existing user

You can edit an existing user in the Users section in User Administration.

NOTICE

Administrator privileges are required to edit existing users.

Procedure

1. Select the user from the list.
2. Click **Edit**.

Figure 108 Edit an existing user

User	First Name	Last Name	Role	Locked
a	a	a	operator	
admin	administrator	administrator	administrator	
automation	Test	Automation	administrator	

3. Make the required changes and click **Save**.

Removing a user

Administrators can delete users from the Backup & Recovery Manager.

NOTICE

There must be at least one user with administrative privileges.

Procedure

1. Select the user from the list.
2. Click **Delete**.
3. Click **Yes** when prompted **Are you sure you want to delete the selected users?**

NOTICE

Administrator privileges are required to delete existing users.

Locking and Unlocking users

The lock and unlock option provides the ability to inhibit user logins during critical times while avoiding the need to delete users.

Manually lock a user by selecting the user, and click **Lock** in the **User Administration** window.

After four unsuccessful Backup & Recovery Manager login attempts, a 15 minute lock out is applied. A message similar to the following is displayed:

Login failed. User is locked for 15 minutes.

Figure 109 Login failed



Contact your Administrator to remove the lock and reset your user name and password if required.

Roles

Specific roles can be applied to users providing them rights to specific operations in the Backup & Recovery Manager.

NOTICE

Customize user access without modifying the default settings in administrator, monitor, or operator by creating a new role. [Adding a new role](#) provides instructions on creating a new role.

The following table lists and provides a description of the specific user roles.

Table 32 User roles

Role	Description
Administrator	The administrator manages users and roles and can manually lock and unlock users, including those that exceed the allotted number of login attempts. The default admin cannot modify the administrator role.
Monitor	The monitor role provides the ability for Events, Alerts and Activities (Backup, and Replication) to be monitored.

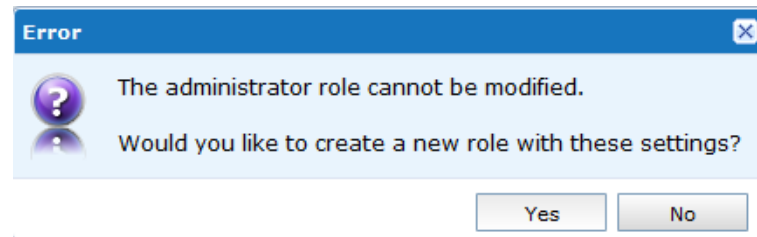
Table 32 User roles (continued)

Role	Description
Operator	The operator can manage Systems, Reports, and is able to perform all monitor functions as well.

Customize the monitor and operator user roles by adding or removing access by using the available attribute check boxes.

If you attempt to modify or remove the administrator role, an error is displayed.

Figure 110 Modify Administrator role error



Adding a new role

You can add a new role to customize user access without changing the administrator, monitor or operator role defaults.

Procedure

1. Click **Add**.
2. Select the attributes for the new role, and click **Save**.

Figure 111 New role

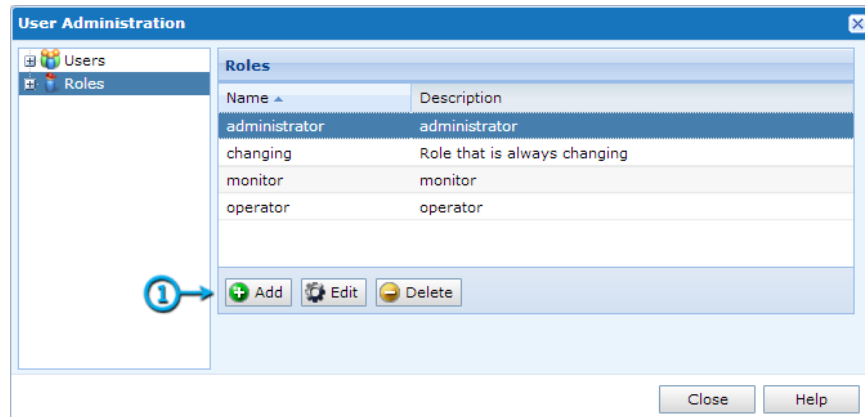
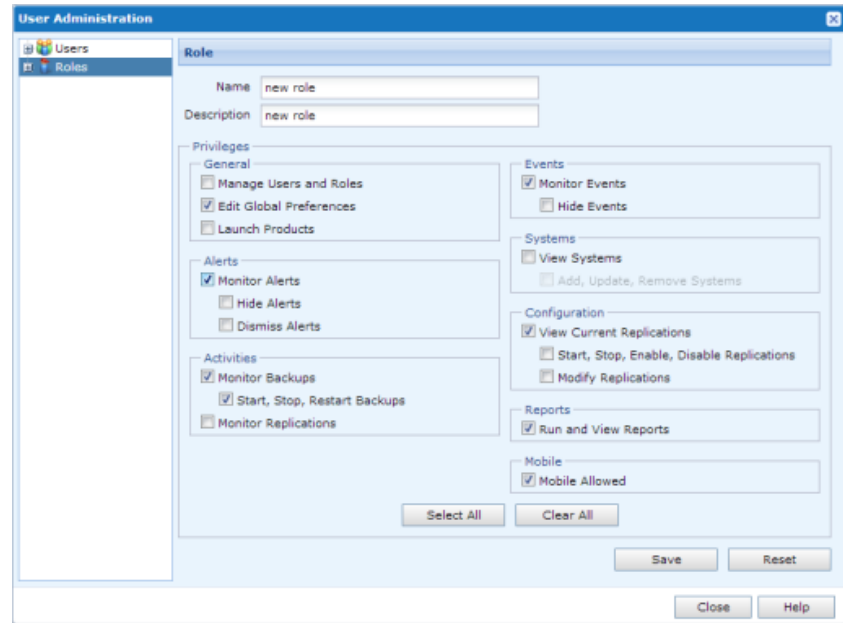


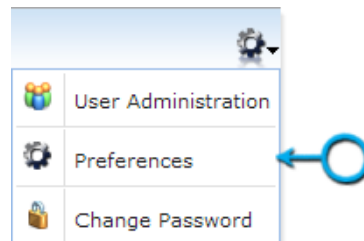
Figure 112 Role Privileges



Preferences

The Preferences section provides the ability to customize the Backup & Recovery Manager for your environment.

Figure 113 Preferences



Date/Time Format

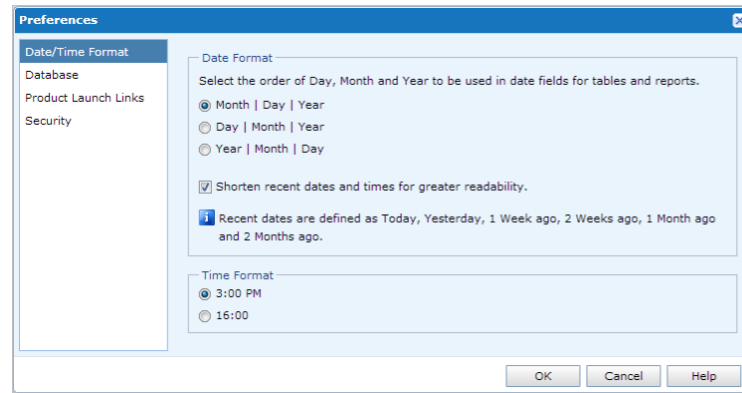
The Date/Time Format menu option provides the ability to select how the Backup & Recovery Manager displays the date and time in the respective fields.

The format that is chosen for the Date/Time format appears in the following:

- All grids that contain Date/Time columns
- Report options for date range

NOTICE

All report start and end dates use the 00:00:00 - 23:59:59 GMT format.

Figure 114 Date/Time Format options

Date format

The following supported date formats and browser language settings can determine the default:

- Day | Month | Year is the default setting for:
 - French
 - German
 - Italian
 - Spanish
- Month | Day | Year is the default if the browser language code does not match any language code.
- Year | Month | Day can be set as an option.
 Enable the option to shorten dates and times for greater readability. The recent date format is defined as Today, Yesterday, 1 week ago, 1 Month ago, and 1 year ago.

Time Format

Click to enable the preferred time format from one of the following:

- 12 hour (3:00 PM) is the default for browsers set to English
- 24 hour (1500) is the default for browsers set to French, German, Italian or Spanish

Database

The Database menu option provides the ability to specify Percentage Used Thresholds and Data Retention.

Setting Percentage Used Thresholds

Percentage Used Thresholds provides the ability to set the period of time that Alert and Reporting data remain until they are automatically removed from the system.

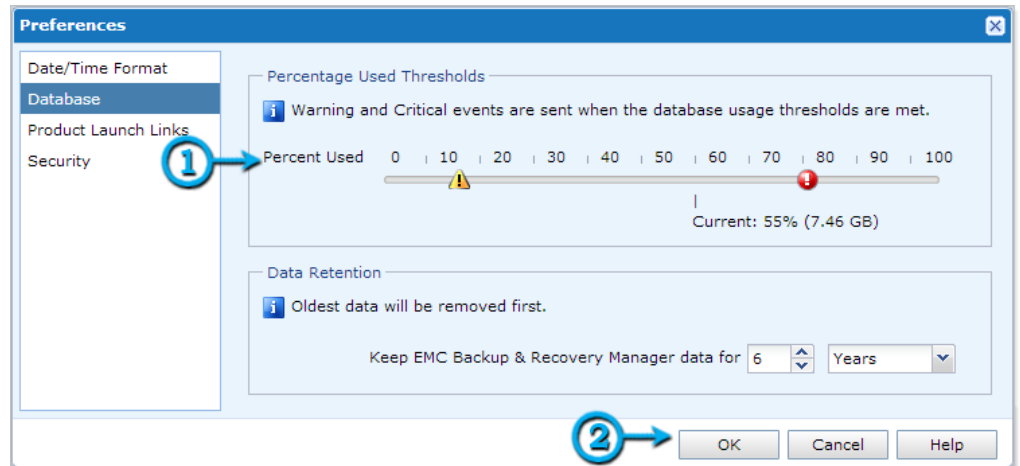
Procedure

1. Use the error and warning icons on the slider to set the percentage for which to receive notification that the system has reached its threshold.

- Click **OK** to save the settings and close the window.

The following figure illustrates the Percentage Used Thresholds slider.

Figure 115 Percentage Used setting



Setting Data Retention

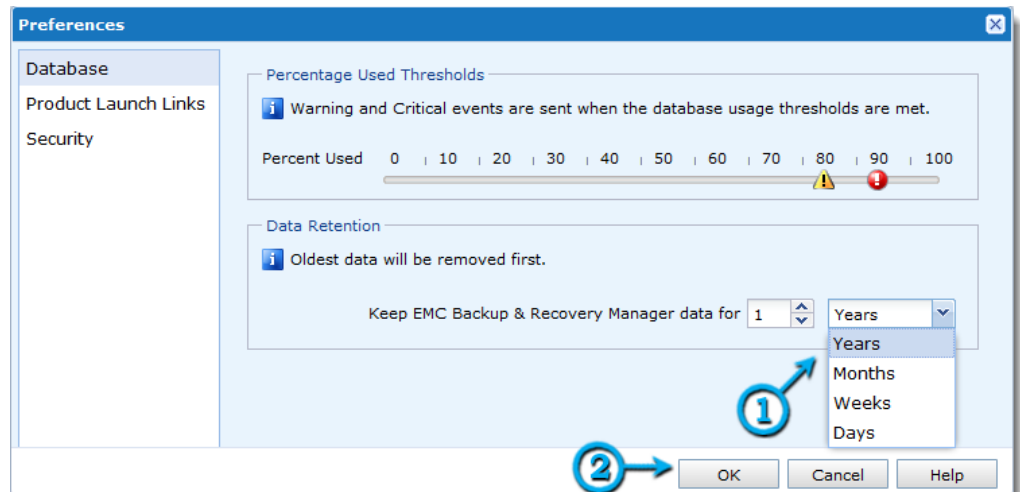
Data retention is the period of time for which the Backup & Recovery Manager data are kept.

Procedure

- Use the counter and the drop-down list respectively to select the number of Years, Months, Weeks, or Days to keep the Backup & Recovery Manager data.
- Click **OK** to save the settings and close the window.

The following figure illustrates the data retention settings.

Figure 116 Database options



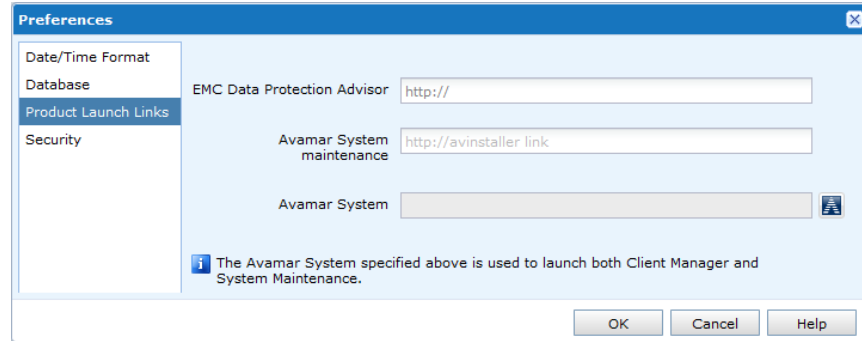
Product launch links

The Product launch links menu option is the location at which to specify the URL to access the EMC Data Protection Advisor (DPA). The Data Protection Advisor, Avamar

System, and Avamar System Maintenance fields must be complete here in order to launch the respective applications from Systems.

The following figure illustrates the Data Protection Advisor, Avamar System, and Avamar System Maintenance Product Launch Links.

Figure 117 Product Launch Links



The following table provides a complete description of the Product Launch Links option.

Table 33 Product Launch Links option

Option	Description
EMC Data Protection Advisor (DPA)	DPA is used to monitor a data protection environment. DPA also provides advanced administrative functions including analysis jobs, and troubleshooting data collection.
Avamar System maintenance	Enter the AVI URL of the Avamar server to launch and view the AVI page.
Avamar System	The selected Avamar system is used to launch the Avamar Client Manager.

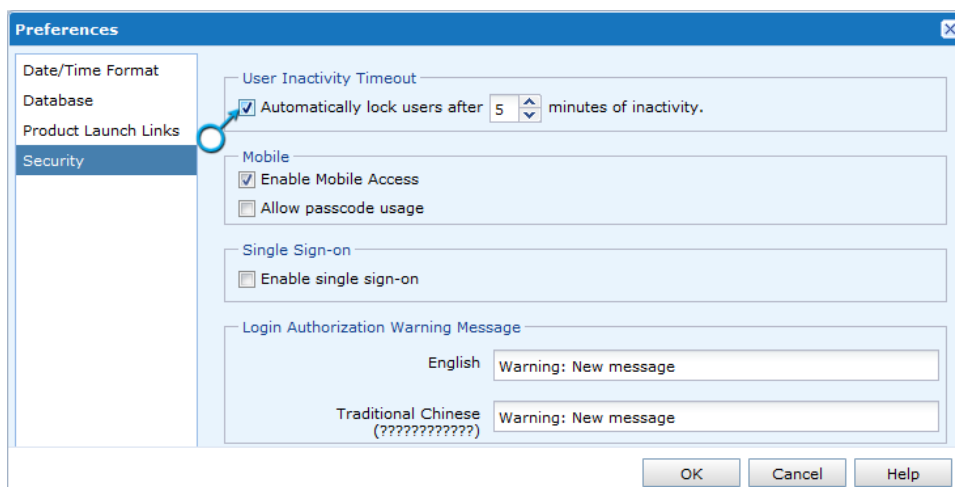
[Launch the Avamar application](#) provides complete details on enabling the Avamar system for Single Sign-on.

Security

The Security menu option provides the ability to set values for the following:

- **Mobile**
Click the check box to the left of the **Enable Mobile Access** and the **Allow passcode usage** options.

Allow passcode usage provides the mobile user the ability to set a unique passcode for the Backup & Recovery Manager on the mobile device. If this permission is set, the user is prompted to enter a passcode rather than a userid/password to access Backup & Recovery Manager Mobile.
- **User Inactivity Timeout**

Figure 118 Manually set the User Inactivity Timeout**Note**

User Inactivity Timeout is enabled to automatically lock users after 5 minutes by default. 30 minutes is the maximum value available.

- **Single Sign-on**
Complete details on single sign-on are available in [Enabling Single sign-on](#) on page 36.
- **Login authorization warning message**

Type a message in the Login authorization warning message dialog to display the text in the Backup & Recovery Manager login window.

The following figures illustrate the **Preferences > Security > Login Authorization Warning Message** dialog and the login screen where the new message is displayed.

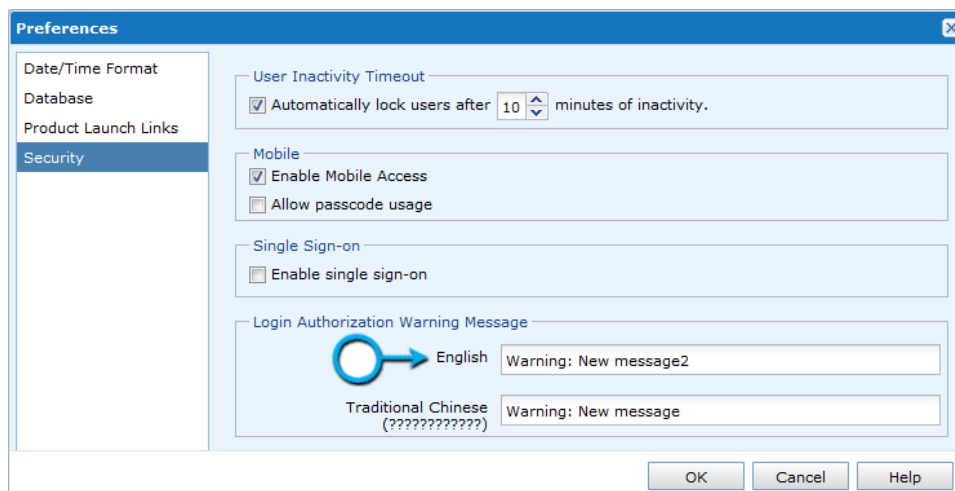
Figure 119 Change the login screen warning message

Figure 120 New login screen warning message

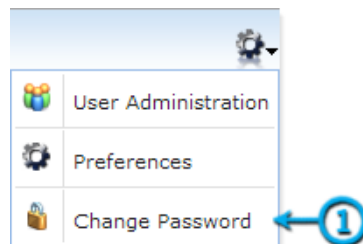


Changing a password

Procedure

1. In the **Settings** menu, click **Change Password**.

Figure 121 Change Password



2. Type a new password in the **Password** field, and then type the new password in the **Confirm Password** field.

The password requirements are the following:

- Minimum of 9 characters
- Minimum of 1 lowercase letter
- Minimum of 1 uppercase letter
- Minimum of 1 number

- Minimum of 1 special character: !@#\$%^&*()-_

Note

Do not specify the \$ character at the beginning or middle of a password. The \$ character can be specified at the end of a password.

3. To save the password, click **Change Password**.

Figure 122 New password fields

Resetting the admin password

You can use the `reset-user.sh` script to change the admin password.

If the admin user password is forgotten, the `reset_user.sh` script provides the administrator/root (super user) with the ability to reset it.

Procedure

1. Log in to the Backup & Recovery Manager server as root user:

```
su -
```

```
root password
```

2. Browse to `/opt/emc/ucas/tools/`.
3. Run the script including the username (`admin`):

```
./reset_user.sh admin
```

A random, auto-generated password is created.

4. Log in to the Backup & Recovery Manager UI with the new password.

CHAPTER 10

Reports

Reports provides the ability to run preconfigured reports for activities on all monitored systems in the enterprise.

Note

Running and exporting reports is not available for the Backup & Recovery Manager mobile applications.

This chapter includes the following topics:

- [Types of reports](#)..... 142
- [Report Options](#)..... 145
- [Exporting reports](#)..... 147

Types of reports

You can run preconfigured reports for activities on all monitored systems in the enterprise.

The following report types are available in the Backup & Recovery Manager:

- Backup Reports: Backup Summary
- System Reports
 - Systems Summary
 - Capacity & Usage
 - System Avg Daily Change Rate
 - Client Avg Daily Change Rate
- Configuration Reports: Configuration

Some reports are not available for all system types. The following table lists the reports available for the system types.

Table 34 Available reports by system type

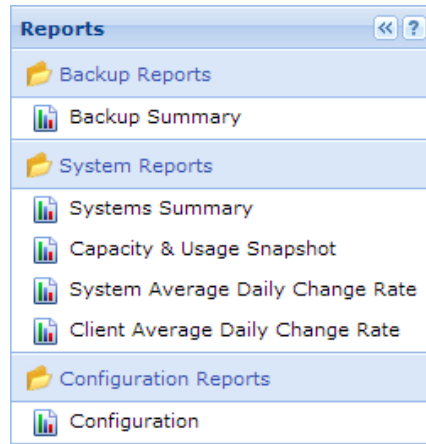
Report type	Report	Avamar	NetWorker	Data Domain
Backup report	Backup Summary	✓	✓	
System reports	System Summary	✓	✓	✓
	Capacity & Usage	✓		✓
	System Avg Daily Change Rate	✓		
	Client Avg Daily Change Rate	✓		
Configuration report	Configuration	✓	✓	

Running a report

Procedure

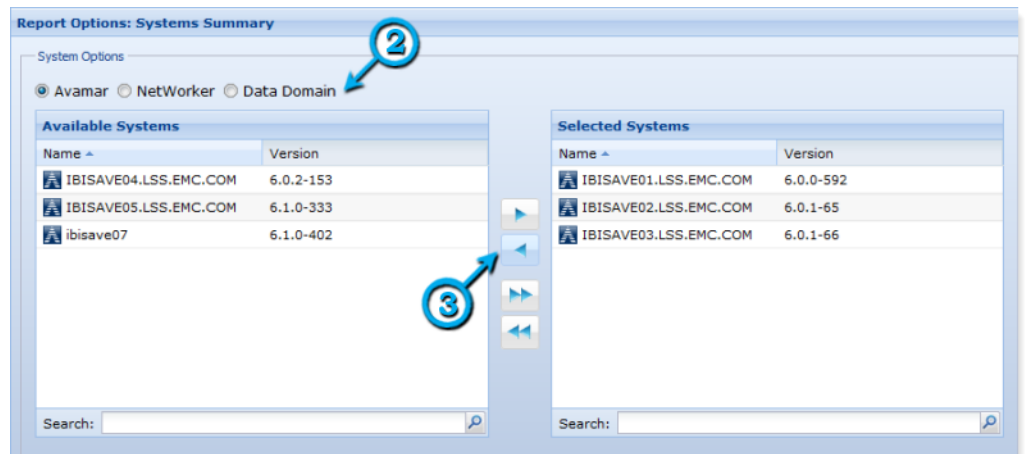
1. Click to select a report type from the list of reports.

Figure 123 Report types



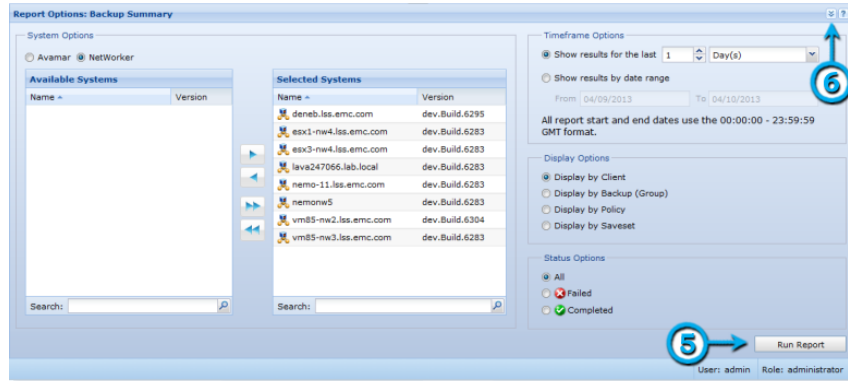
2. Click to select the system type, **Avamar**, **NetWorker** or **Data Domain**.
3. If required, select the systems and use the arrows to move from **Selected Systems** to **Available Systems** to exclude them from the report.

Figure 124 Report system options



4. Select the options to configure the report. [Report Options](#) on page 145 provides details on the options available for the report types.
5. Click **Run Report**.

Figure 125 Backup Summary report options



The Capacity & Usage Snapshot report includes a new Meta Data Used column. The following figures illustrate an example of the Capacity & Usage Snapshot options for an Avamar system and the resulting Capacity & Usage Snapshot chart with the Meta Data Usage points.

Figure 126 System Summary report options

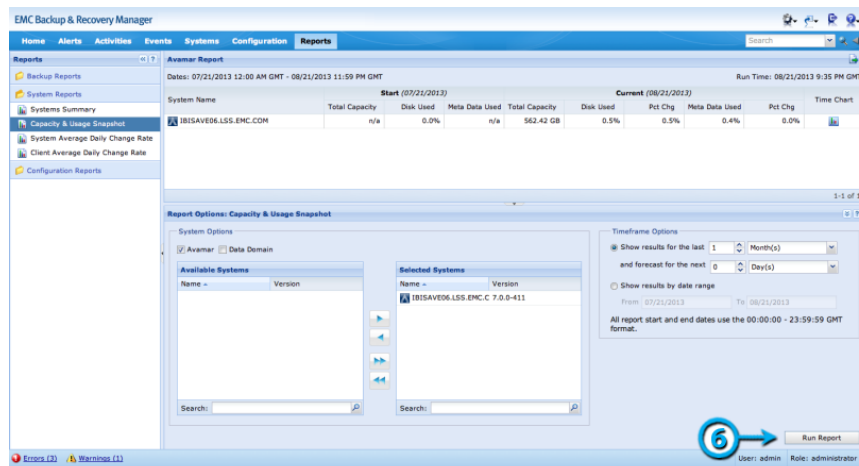
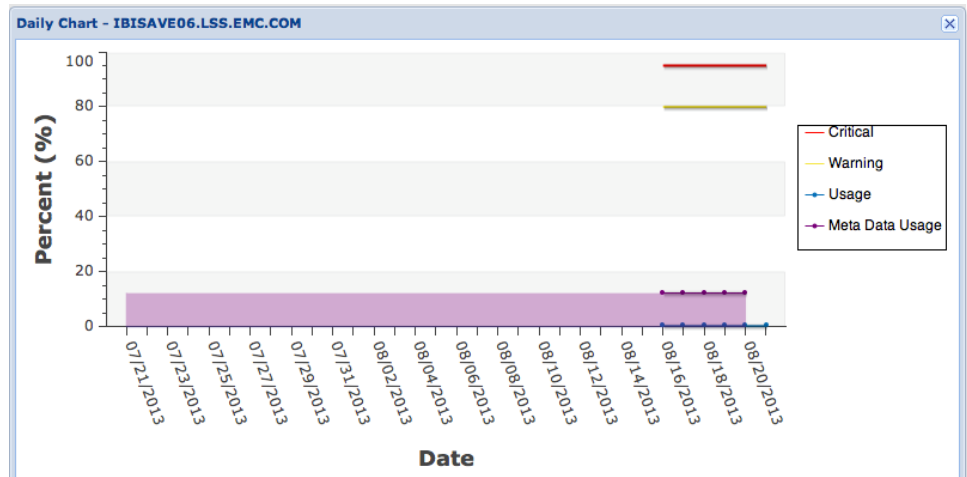


Figure 127 Capacity usage report chart






Note

For NetWorker 8.1 and later systems, Display Options includes Display by Policy to run Backup reports from the policy perspective for NetWorker 8.1 policy based backups.

[Display Options](#) on page 146 lists the specific options available for both Avamar and NetWorker systems.

6. When the report completes, click the arrows to collapse the **Report Options** panel to increase the report result viewable area.
7. Click the appropriate icon to change the report view or export the report. The following table lists the icons and their functions.

Table 35 Report option icons

Icon	Description
View table 	Click this icon to view the report as a table (default).
View chart 	Click this icon to view the report in a graphical format. Depending on the location of the chart icon, the results that are displayed vary: <ul style="list-style-type: none"> • A chart icon at the top of the report charts the results in the grid. • A chart icon in the row of results, charts a daily detailed breakdown for that system or client only.
Export 	Click to export the report. Exporting reports on page 147 provides details on exporting Backup & Recovery Manager reports.

Report Options

The report options provide the capability to configure the information contained in the reports.

Timeframe Options

Timeframe Options runs reports for a specified timeframe, and are available in the **Backup Summary** and all **System** reports.

- Show backups for the last:
 - Set the counter to the number of days, weeks, or months.
 - Any date range within the past year, up to 1 year of backups.
 - Specify the date range for the report.
 - Enter 0 in the days back and a value in forecast to run a report with no historical data.

- Show backups for last always ends with the most current day of data up to current date. The timeframe is back $<n>$ days back from today. The report may only have data up to the previous day of the current date (yesterday).
- And forecast for the next (Capacity & Usage system report only):
 - Set the counter to the number of days, weeks, or months.
 - Enter 0 in the forecast counter to exclude the forecast data from the report.
 - Forecast any date range back 1 year to forward 1 year.

Display Options

Display Options is available for the Backup Summary report, and allow you to configure the report for the following options:

- Avamar:
 - Display by Backup
 - Display by Client
 - Display by Group
- NetWorker:
 - Display by Client
 - Display by Backup (Includes Groups, Protection Policies, or Workflows depending on the NetWorker version.)
 - Display by Policy (NetWorker only, and includes both Data Protection Policies, or Protection Policies based on the NetWorker server version.)
 - Display by Saveset

Status Options

Status Options allow you to specify which backups are included in the report. Status Options is available for the Backup Summary report. You can select the following:

- All
- Failed
- Succeeded

Report Content Options

Configuration reports list the configuration items for the specified systems. The configuration items make up the backup and replication configurations for the system.

Report Content Options is available for the Configuration report only and provides the following options:

- Avamar:
 - Clients
 - Datasets
 - Groups
 - Retention Policies
 - Schedules
- NetWorker:

- Devices
 - Clients
 - Clones
-

Note

Clone activities for NetWorker 9.0 servers are displayed in the respective policy, but not in Clone Configuration reports. The Clone Configuration report does display scheduled clones for previous NetWorker server versions.

- Groups
- Policies
- Pools
- Schedules
- Storage Nodes

Exporting reports

Reports can be exported for use and contain all rows and columns in the grid (all data in the report) in csv format.

To export the report to csv format, click **Export**. Depending on the browser, one of the following will occur:

- The csv file is downloaded to the configured download folder
- A dialog displays prompting for the location in which to download the report

APPENDIX A

Security Configuration

This appendix includes the following topics:

- [Communication security](#)..... 150
- [Login, session, and password protection](#).....152
- [Firewall rules](#).....153
- [REST API](#).....154
- [Data security](#)..... 154
- [Access control](#)..... 154

Communication security

Communication security settings enable the establishment of secure communication channels between:

- Product components
- Product components and external systems or components.

Port usage

The ports that are listed in the following table are the Backup & Recovery Manager default ports for the various components all using the TCP protocol. Some of these ports can be changed. Various configuration files must be manually edited.

Table 36 Default ports using the TCP protocol

Component	Port	Source	Description
Backup & Recovery Manager Web Application	443	Avamar and NetWorker adaptors	Default port for secure HTTP connections. The Backup & Recovery Manager adaptors use this port to communicate with the Backup & Recovery Manager Web App.
RabbitMQ	5671	Avamar and NetWorker adaptors	Port for accepting SSL RabbitMQ connections.
RabbitMQ	5672	Internal Backup & Recovery Manager DD adaptor	Used by the adaptor to post messages from the DD server to the message bus. Not accessible from outside the Backup & Recovery Manager server.
Apache ActiveMQ	61610	NetWorker adaptor	Port for accepting SSL STOMP connections.
Apache ActiveMQ	61619	Avamar adaptor	Port for accepting SSL ActiveMQ connections.
Apache Tomcat	8009	End Apache server and the EMC client system making API calls	Port for accepting AJP connections in tomcat (localhost access only).
Apache Tomcat	9191	internal for localhost access	Port for accepting HTTP connections in

Table 36 Default ports using the TCP protocol (continued)

Component	Port	Source	Description
			tomcat (localhost access only).
SSH & SSH daemon (sshd)	1315	SSH clients connecting to Backup & Recovery Manager	Default SSH port to the Backup & Recovery Manager server.
Data Domain server	22	DD internal	This port is a communication target on the DD server. This port is closed on the Backup & Recovery Manager server.
AvInstaller service	8543 8580	Web browser clients	Ports to connect to the AvInstaller.

Network encryption

The following table contains the Avamar encryption strategies that are employed by the Backup & Recovery Manager feature for communication between components.

Table 37 Encryption strategies

Communication	Encryption type
Between web server and browser	SSL with server authentication
Between ActiveMQ and Avamar components	SSL with mutual authentication

For NetWorker, backup and archive data on UNIX and Windows hosts are encrypted with the aes Application Specific Module (ASM). The aes ASM provides 256-bit data encryption. Backup data is encrypted based on a user-defined pass phrase. If no pass phrase is specified, data is encrypted with a default pass phrase.

Cryptographic modules in the Backup & Recovery Manager

The following table is a list of cryptographic modules used in the Backup & Recovery Manager.

The cryptographic modules used in the Backup & Recovery Manager are not compliant with the Federal Information Processing Standard (FIPS 140-2).

Table 38 Cryptographic modules

Backup & Recovery manager Cryptographic modules			
AES128-SHA	DHE-DSS-AES128-SHA	EDH-DSS-DES-CBC-SHA	EXP-RC2-CBC-MD5
AES256-SHA	DHE-DSS-AES256-SHA	EDH-DSS-DES-CBC3-SHA	EXP-RC4-MD5

Table 38 Cryptographic modules (continued)

Backup & Recovery manager Cryptographic modules			
CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA	EDH-RSA-DES-CBC-SHA	EXP-RC4-MD5
CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA	EDH-RSA-DES-CBC3-SHA	RC2-CBC-MD5
DES-CBC-MD5	DHE-RSA-AES128-SHA	EXP-DES-CBC-SHA	RC4-MD5
DES-CBC-SHA	DHE-RSA-AES256-SHA	EXP-EDH-DSS-DES-CBC-SHA	RC4-MDRC4-SHA
DES-CBC3-MD5	DHE-RSA-CAMELLIA128-SHA	EXP-EDH-RSA-DES-CBC-SHA	RC4-SHA
DES-CBC3-SHA	DHE-RSA-CAMELLIA256-SHA	EXP-RC2-CBC-MD5	

Login, session, and password protection

It is recommended that you change the password for the admin, dpn, root, and ucas users from the default (changeme) after the Backup & Recovery Manager server installation.

The Backup & Recovery Manager provides the following protection for the GUI login and password protection:

- Users are required to change the password at the first GUI login
- Password requirements are the following:
 - Minimum of 9 characters
 - Minimum of 1 lowercase letter
 - Minimum of 1 uppercase letter
 - Minimum of 1 number
 - Minimum of 1 special character

Note

Do not specify the \$ character at the beginning or middle of a password. The \$ character can be specified at the end of a password.

- After 3 failed login attempts, the user is locked out of the system for 15 minutes

Note

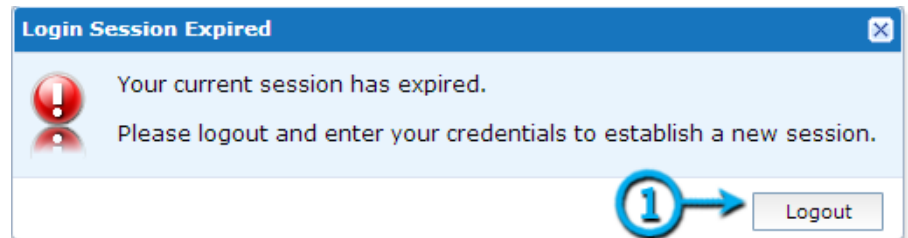
This setting is hard coded and cannot be changed.

- The Backup & Recovery Manager automatically logs out of sessions if for any reason the connection between the client and server is lost:
 - Common reasons for a login session to expire are:
 - The Backup & Recovery Manager server is restarted

- The browser is closed completely while you are still logged in to the Backup & Recovery Manager
- All browser windows (or tabs) that are logged in to the Backup & Recovery Manager are closed, and not re-opened for 30 minutes or more
- Internet access is lost for more than 30 minutes

The following figure illustrates the dialog that displays if the login session expires.

Figure 128 Expired login session



- Administrators can manually lock user access
Manually lock a user by selecting one or more users and clicking Lock in the User Administration window of Settings.

NOTICE

This option provides the ability to inhibit user logins during critical times while avoiding the need to delete users.

Invalidating ssh keys for login, disabling direct login for extra accounts, and removing deprecated accounts

Procedure

1. Log in as the root user.
2. To invalidate ssh keys for login, disable direct login for extra accounts, and remove deprecated accounts, run the following types of commands:

```
cp /dev/null ~admin/.ssh/authorized_keys2
cp /dev/null ~dpn/.ssh/authorized_keys2
cp /dev/null ~ucas/.ssh/authorized_keys2
cp /dev/null ~root/.ssh/authorized_keys2

chsh -s /sbin/nologin admin
chsh -s /sibn/nlogin dpn
userdel gsan
```

Firewall rules

The Backup & Recovery Manager has firewall rules on the Backup & Recovery Manager server appliance (OVA). These firewall rules control what network connections can be made to the system, and can be used to throttle SSH connection attempts or slow down port scans at the network layer.

The firewall rule set is available at `/opt/emc/ucas/packages/ucas-iptables` for the OVA.

REST API

It is possible to implement custom applications or widgets that make use of the REST API, but any such software will not be supported by EMC. This is not supported as the REST API might be subject to change without notice in future versions of the Backup & Recovery Manager.

Data security

The Backup & Recovery Manager encrypts all in-flight data.

Access control

Access control settings provide protection of resources against unauthorized access.

Default accounts

The following table contains the default Backup & Recovery Manager default account and its default password.

Table 39 Default account names and passwords

Account	Password	Description
admin	Set when the Backup & Recovery Manager feature is installed. The default password is changeme You are prompted to change the default password at first login.	The default user for the Backup & Recovery Manager.

Authentication configuration

The Backup & Recovery Manager requires configuration of an administrator at installation time. The administrator can create additional users after the Backup & Recovery Manager is installed.

User authorization

The privileges of Backup & Recovery Manager users are controlled by the roles to which they belong. Three built-in roles have been defined:

- Administrator
- Operator
- Monitor

The Backup & Recovery Manager administrator role also provides the ability to:

- Edit the existing roles to add or remove access capabilities
 - Create new roles to further control user access
 - Manually lock user accounts to disable login
- The following table provides a description of the available built-in user roles.

Table 40 Built-in user roles

Role	Description
Administrator	The administrator manages users and roles and can manually lock and unlock users, including those that exceed the allotted number of login attempts. The privileges of the administrator role cannot be modified.
Monitor	The monitor role provides the ability for Events, Alerts and Activities (Backup, and Replication) to be monitored.
Operator	The operator can manage Systems, Reports, and is able to perform all monitor functions as well.

Component access control

The following components of the Backup & Recovery Manager implement security features for access.

- Apache ActiveMQ Message Broker
- Apache Tomcat
- Mongo Database

Apache ActiveMQ Message Broker

Access to the ApacheActiveMQ message bus and HTTP is controlled by SSL mutual authentication. In SSL, this is accomplished by exchanging certificates.

Apache Tomcat

Apache Tomcat uses a certificate to authenticate itself to web clients.

Certificate management

Each Backup & Recovery Manager feature component that participates in SSL communications keeps its certificates in a Java KeyStore (JKS) file. The certificate is used for secure http access (https), and secure communication to the Backup & Recovery Manager adaptors.

“Key store” files contain certificates that components use to identify themselves as well as the certificates of entities they trust. Some components keep their certificates and the certificates of trusted entities in the same key store file, while others keep the certificates of trusted entities in a separate file called a trust store. Although key store and trust store files have the same JKS format, the Backup & Recovery Manager feature trust store files have a .ts suffix whereas the key store files have a .ks suffix.

NOTICE

JKS files can be managed with a Java tool called keytool. Keytool is part of the standard JDK, which is included in the Backup & Recovery Manager feature software.

In the Backup & Recovery Manager feature, there are JKS files for the following components:

- Message broker clients — containing a “key store” (and sometimes a “trust store”) containing certificates that are used for mutual authentication with the message broker
- Apache Tomcat — containing the certificate that Tomcat uses to authenticate itself to web clients

Web browser authentication using Apache

The Backup & Recovery Manager server and adaptors use the Apache web server to provide a secure web browser-based user interface. Web browser connections for these applications use secure socket layer/transport layer security (SSL/TLS) to provide authentication and data security.

When a web browser accesses a secure web page from an unauthenticated web server, the SSL/TLS protocol causes it to display an authentication warning. An unauthenticated web server is one that does not authenticate itself using a trusted public key certificate.

The Apache web server that is provided with the Backup & Recovery Manager is installed with a self-signed certificate, not a trusted public key certificate. The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server, but it cannot be used for authentication. By using a secure second channel to verify the certificate’s fingerprint, authentication can be achieved with self-signed certificates.

If required, a self-signed certificate other than the one provided by EMC can be inserted. The certificate signing request (CSR) is used to apply for a trusted certificate. To provide server authentication, and thereby prevent web browser warnings complete the following tasks:

- Install a self-signed or trusted certificate
- Create a private key
- Generate a certificate signing request

The tools that are used in these tasks are part of the OpenSSL toolkit. OpenSSL is provided with Backup & Recovery Manager.

Installing a self-signed or trusted certificate

The Apache web server that is provided with the Backup & Recovery Manager is installed with a self-signed certificate, not a trusted public key certificate. The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server, but it cannot be used for authentication.

NOTICE

Ensure that the trusted certificate is issued for the correct hostname. Configuring a hostname for the Backup & Recovery Manager appliance is a function that EMC cannot control and is the responsibility of the customer's IT department.

To install either a self-signed, or trusted certificate for the Backup & Recovery Manager Apache database, perform the following:

Procedure

1. Connect to the Backup & Recovery Manager server as the ucas user:

```
ssh ucas@SERVER -p1315
```

NOTICE

The Backup & Recovery Manager server does not provide an ssh agent, use an ssh client of your choice and be sure to specify port 1315 as the port for command line ssh.

2. Change to root user:

```
su -
```

3. Save in a temporary location, the EMC-provided certificate files:

- ucasWebCert.pem
- ucas-web-private.key

4. Copy their own certificate files to /opt/emc/ucas/security.

5. Set the owner and group of the new certificate files to the following:

- Owner: ucas
- Group: ucas

6. Set the permissions of the new certificate files to 0644:

```
chmod 0644
```

7. Edit /opt/emc/ucas/apache-fips/conf/conf.d/ucas-sles-ssl-standalone.conf. Change references to the certificate files to point to the new certificate files.

8. Restart the Apache web server.

NOTICE

This procedure should only be performed by advanced system administrators with knowledge of Apache web browser authentication.

Creating a private key

A private key can be generated with pass phrase protection and without pass phrase protection. It can also be generated using a random key generation algorithm. Use the method that is appropriate for the level of security that is required by your organization.

Procedure

1. Open a command shell and log in to Backup & Recovery Manager server:

- a. Log in to the server as admin.

- b. Switch user to root by typing:

```
su -
```

2. Generate the private key by typing:

```
openssl genrsa -out server.key 3072
```

where *server.key* is a name you provide for the private key.

The private key is created in the current working directory.

Generating a certificate signing request

Apply for a public key certificate from a Commercial CA, by sending the CA a certificate signing request (CSR).

Procedure

1. Open a command shell and log in to the Backup & Recovery Manager server as admin.
2. Switch user to root by typing:

```
su -
```

3. Generate the CSR by typing:

```
openssl genrsa -out server.key 3072
```

where *server.key* is a name you provide for the private key.

The private key is created in the current working directory.

Changing the Backup & Recovery Manager Apache from self-signed to issued

Change the Backup & Recovery Manager Apache from self-signed to issued to inhibit the certificate warning from displaying when connecting to the Backup & Recovery Manager appliance.

NOTICE

The keystore is `/opt/emc/ucas/security/ucas-web-keystore.ks` and the certificate is stored in this location as well.

This procedure replaces the self-signed descriptive information in the deployed cert with real information from your company. The security of an issued cert over the default installation a self-signed certificate is not improved, it only eliminates the warning. You can also view the certificate when connecting to the appliance by clicking the check box to trust the issuer.

The main purpose of a Certificate is to verify the identities of hostnames and network addresses. It is recommended that the Backup & Recovery Manager has a DNS entered hostname and that the external IP of Backup & Recovery Manager must resolve to that hostname. If this is not in sync, then your cert can still result in a warning.

Procedure

1. Take a snapshot of the Backup & Recovery Manager VMware appliance before beginning. This creates a working installation in the event there are problems during this procedure.
2. View the current key entry by entering the following command:

```
keytool -list -keystore /opt/emc/ucas/security/ucas-web-keystore.ks
Enter keystore password: Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
idhpc61.lss.emc.com, Aug 15, 2013, PrivateKeyEntry, Certificate
```

```
fingerprint (SHA1): B4:17:93:30:41:AE:23:69:23:17:EC:27:1E:
33:EA:08:F8:C9:A1:08
```

This displays the hostname that is previously configured for use with Backup & Recovery Manager.

3. Delete the default key entry:

```
keytool -delete -keystore /opt/emc/ucas/security/ucas-web-
keystore.ks -alias idhcp61.lss.emc.com
```

The alias parameter should match the hostname of the Backup & Recovery Manager as shown in [step 2](#) of this procedure.

4. Generate a new key pair for the new certificate.

```
keytool -genkeypair -keysize 3072 -alias idhcp61.lss.emc.emc -
validity 1780 -keyalg RSA -ext
san="DNS:idhcp61.lss.emc.com,DNS:idhcp61,IP:10.13.204.61,IP:
127.0.0.1,DNS:localhost" -keystore ucas-web-keystore.ks
Enter keystore password:
What is your first and last name?
[Unknown]: fqdn_hostname_of_your_BRM
What is the name of your organizational unit?
[Unknown]: YOUR_ORG_UNIT
What is the name of your organization?
[Unknown]: YOUR_COMPANY
What is the name of your City or Locality?
[Unknown]: YOUR_CITY
What is the name of your State or Province?
[Unknown]: YOUR_STATE
What is the two-letter country code for this unit?
[Unknown]: YOUR_COUNTRYIs CN=fqdn_hostname_of_your_BRM,
OU=YOUR_ORG_UNIT, O=YOUR_COMPANY, L=YOUR_CITY,
ST=YOUR_STATE,C=YOUR_COUNTRY correct? [no]: yes
```

For example, when generating the certificate use the fqdn, shortname, localhost and associated IP addresses as the subject and subject alternative name:

```
FQDN is idhcp61.lss.emc.com
SHORTNAME is idhcp61
ipaddress is 10.13.204.61
LOCALHOST is 'localhost'
LOCALHOST_IP is 127.0.0.1
```

At the command line, set the Subject Alternative Name = san, prefix DNS: before the hostnames, and IP: before any IP addresses.

5. Log in as the ucas user:

```
sh ucas@SERVER -p1315
```

6. Generate the certificate request (CSR):

```
keytool -certreq -keyalg RSA -alias idhcp61.lss.emc.com -
keystore /opt/emc/ucas/security/ucas-web-keystore.ks -file /tmp/
brm.csr enter keystone password: changeme content of /tmp/
brm.csr: -----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAkICAQAwZTElMAkGA1UEBhMCVVMxCzAJBgNVBAGTAKNPMRMwEQYDVQOH
EwpMb3Vpc3Zp
bGx1MQwwCgYDVQQKEwNFTUMxDDAKBgNVBAsTA0JSUzEYMBYGA1UEAxMPQlJTTIEVU
Z21uZWVyaW5n
```

```

MIIBojANBgkqhkiG9w0BAQEFAAOCAQY8AMIIBigKCAyEAmFMN5s2hMVuJZjPYvVDI
XFuMZOFcGRY0 Dlkx76gTF08miWHe7AOhMy+WmN3Qczj9Zo6nm/
uObroBtyyclmYyflAlT5qDP3JzKdIicG/Bi/k YYinauhtXpJbXlm2yrEASSvKV+
+cXYX32QYebkdkniNHj1I4DrdrbCZdPBE0YZcwM8AZGHdALYX1
lza7DgTW4A52LFwzH6DWz4MnBn8FZkP3udurZ6D0bFFKjNycw
+rRaUfIwbXfy2pfgSH7H+3SfI7E
ufJeDTJlYeDaU7DFLQHdmrpg0tp23C0XSFyJWv+IUnet44FbLlHBE6d3XuaL/
yXCFVlyY488iOJU a/SsRbFgUIzBKniTkHJFEdq9woJltUZjwxrINXhqM/
PImOXFVhTuxeAzk19Oodd6D1fO06KtptBu Wnic6/HgMLKWB/+XqXMrAS
+6MtfDOkH2KHA+VceuLzBhFO6Y/MloxQ2QVZ6DBUkxH23/SK+9TYMH fipuA/AG
+93lnOh2rqNZ7KGZAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAFMB0GAlUdDgQWBBRL
7rbP OmW0goy/
EgyWVVNTuPgmADANBgkqhkiG9w0BAQsFAAOCAyEAhcY8Zje3Gbk1PSxv6GQLHIIdY
voRX NGujNJs0N6GEHud5BQKjVGde3vwtFxfOzuK0iPyz76QIQ+e+B50x1B
+st1NPFzql8VrtT4MBIyDw FhQEDEDodKWqG7QTg4YVo8r0cC5HShiDe/
IgTVZ6oa0g8j5PDx00F4P3hw94FFpvXgoRh0sqykIY cLBjbbobBg/
ClXWiFaGjSDD1Dj3K9sOtWJ+YyWXUIos
+DZCBKgVf1TC77fGVpuTJzgD9ofSPFCXS
vzmpbFWhuFf1lC7NQtgmnZ6Gzld70M3K9m0kDmYZn/
bJyAoEqyoBteDw2E0i/YOj+kIsGpojmvS 6iKQ+gCt39IC1BHu9l6U4oXK581J/
EMGRWzrUxzsSxIXM3ydVhjc8SHZReqid/c3FQoXeDg7NKD9
0NzDOVupMoYRkNZmdzlmldqLuvjvnjxxkCDFd04SCsaOBnbX1vnLj4jvHk0My3bB
SiIBs9oEQ6oQ 6vNklXMjRe1Ku9r10g78UjA55o4f -----END NEW
CERTIFICATE REQUEST-----

```

7. Send the CSR to the certificate provider to issue a certificate and indicate that Apache SSL is the software from which the CSR was generated.
8. When you receive the new signed certificate, perform the following to prepare to swap certificates:

- a. Shutdown web/tomcat services:

```
sudo service tomcat-ucas stop
```

- b. Shut down the Backup & Recovery Manager web server:

```
sudo service apache-fips stop
```

9. Remove all existing certificates:

```
cd /opt/emc/ucas/security delete ucasWebCert.pem delete
ucasWebCert.cert
```

10. Perform the following for the signed certificate:

- a. Rename the new certificate:

```
/opt/emc/ucas/security/ucasWebcert.pem
```

- b. Copy the certificate to the following location:

```
/opt/emc/ucas/security/ucasWebcert.cert
```

11. Regenerate the private key from the keystore:

```
java -cp /opt/emc/ucas/packages/ucas-model-jar-with-
dependencies.jar com.emc.brsue.utils.DumpPrivateKey ./ucas-web-
keystore.ks changeme idhcp61.lss.emc.com > /opt/emc/ucas/
security/ucas-web-private.key
```

12. Set the permissions back to normal:


```
cd /opt/emc/ucas/security sudo chown ucas:ucas * chmod 640 *
```

13. Import the CA cert:

```
sudo keytool -import -v -noprompt -trustcacerts -alias  
puppet.lss.emc.com -keystore /usr/java/ucasjre/lib/security/  
cacerts -file rootCA.pem
```

14. Restart the Backup & Recovery Manager Apache and Tomcat services:

```
# start tomcat sudo service tomcat-ucas start # start apache  
sudo service apache-fips start
```

15. Verify that the Backup & Recovery Manager application has a new cert that is issued by your Certificate provider. This is rather than the default self-signed certificate.

```
# verify
```

16. If required, back this change out and revert to the original snapshot obtained in [step 1](#) of this procedure:

```
# backout procedure
```


APPENDIX B

Troubleshooting

Troubleshooting provides information on the log files available for the various components of the Backup & Recovery Manager for debugging and troubleshooting purposes.

- [Managing the Backup & Recovery Manager server](#) 164
- [The regroup-alerts-events script](#)..... 164
- [Customizing the log rotation policy schedule](#) 165
- [Adaptor log file location](#)..... 165
- [View log files](#).....166
- [The bundlelogs utility](#)..... 167
- [NetWorker adaptor options](#)..... 168
- [Avamar adaptor control script](#).....174
- [Backup & Recovery Manager error messages](#).....175

Managing the Backup & Recovery Manager server

You can restart all the Backup & Recovery Manager server daemons when the networking is configured.

Procedure

1. Restart the mongod and apache2 daemons:

```
sudo service mongod restart sudo service apache2 restart
```

2. Stop the tomcat-ucas daemon:

```
cd /opt/emc/ucas/tomcat/bin sudo service tomcat-ucas stop
```

3. Verify that the tomcat-ucas daemon is shutdown:

```
ps -ef | /bin/grep tomcat\bin\bootstrap | grep ucas | grep -v  
grep | grep ucas
```

If the tomcat-ucas process did not stop, type kill process id to stop the daemon.

If the kill process id also does not stop the daemon, type kill -9 process id.

4. Restart the tomcat-ucas daemon:

```
sudo service tomcat-ucas start
```

Results

The daemon options are start, restart, and stop.

The regroup-alerts-events script

Backup & Recovery Manager uses rules to group similar events and alerts together to make the alerts and events tables more readable. If new rules are added by using a Backup & Recovery Manager upgrade or patch, any events or alerts that occur after the upgrade are grouped according to the new rules. However, older events and alerts are not affected. The regroup-alerts-events script re-processes all the old events and alerts using the new rules. This organizes the alerts and events tables to make them more useful especially for Backup & Recovery Manager installations with large numbers of alerts and events.

During the upgrade process from BRM 1.0 to BRM 1.1-GA, this process runs automatically. The regroup script is only required in special cases.

Running the regroup-alerts-events script

You can add or modify the grouping rules manually. If it is required to modify the rules, run this script after an upgrade to apply the new rules to the old events and alerts.

Procedure

1. From a command terminal, connect to the Backup & Recovery Manager server as the ucas user:

```
ssh ucas@SERVER -p1315
```

2. Change to root user:

```
su - <root password>
```

3. run the script:

```
sudo regroup-alerts-events
```

4. View the script output in the `/tmp/event-alert-regrouper.log` file.

Customizing the log rotation policy schedule

By default, the Backup & Recovery Manager checks if the logs require rotation every minute by using the Linux crontab utility. You can change the frequency of the log rotation by following the standard conventions for crontab.

Before you begin

Knowledge of the vi editor is required to edit the logrotate policy schedule.

The crontab man page provides details for changing when scheduled jobs run.

The default setting is to check the logs once a minute:

```
* * * * * /usr/sbin/logrotate --state /opt/emc/ucas/
logrotate.status /opt/emc/ucas/packages/logrotate.conf &>/dev/null
```

Procedure

1. Login to the console or ssh as the ucas user:

```
sudo crontab -e
```

2. In vi, make the required edits to the schedule:

- To rotate the logs once every hour:

```
0 * * * * /usr/sbin/logrotate --state /opt/emc/ucas/
logrotate.status /opt/emc/ucas/packages/logrotate.conf
&> /dev/null
```

- To rotate the logs once a day:

```
0 0 * * * /usr/sbin/logrotate --state /opt/emc/ucas/
logrotate.status /opt/emc/ucas/packages/logrotate.conf
&> /dev/null
```

3. To save the changes, exit vi.
4. Verify that your changes are as expected by using the `sudo crontab -l` command.

Adaptor log file location

The Backup & Recovery Manager adaptor log files are located at:

- Avamar:
`/usr/local/avamar/var/brm/log`
- NetWorker on Windows:
`C:\Program Files (x86)\EMC NetWorker\nsrmq`
- NetWorker on Linux:

`/opt/NetWorkerAdapter-1.0/bin/nsrmq.log`

The file name is changed when the log rolls over and the next number is appended to the file, creating a new file. For example, `nsrmq.log.<1>`, `nsrmq.log.<2>` and so on.

View log files

The following table lists the log file locations:

Table 41 Log file locations

Log file	Log file location
Backup & Recovery Manager server	<code>/opt/emc/ucas/ucas-logs*</code>
Apache	<code>/opt/emc/ucas/apache-logs/*</code>
Tomcat	<code>/opt/emc/ucas/tomcat/logs/*</code>
Mongo	<code>/var/log/mongo/*</code>

Log files are available for the following:

- Apache web server
- Tomcat log files
- Mongo database log file
- Backup & Recovery Manager application log files

Apache web server log files

The following table lists the log files available for the Apache web server.

Table 42 Apache log files

Log file	Contents
<code>ucas-apache-error.log</code>	Errors from the Apache web server
<code>ucas-apache-rewrite.log</code>	Details of URL rewriting from the Apache web server
<code>ucas-apache-access.log</code>	Timestamped access information for all resources served by Apache

Tomcat log files

The following table describes the available log file for Tomcat: describes the tomcat log

Table 43 Tomcat log files

Log file	Contents
<code>catalina.out</code>	Tomcat startup and war deployment activities

Table 43 Tomcat log files

Mongo database log file

The following table describes the log file available for the Mongo database.

Table 44 Mongo logs

Log file	Content
mongod.log	Mongo database activities

Backup & Recovery Manager application log files

The following table lists log files available for the Backup & Recovery Manager applications.

Table 45 Backup & Recovery Manager logs

Log file	Content
ucas.log	All processing (debug, info, error, and warning) of the Backup & Recovery Manager server
activemq-messages.log	Debug messages specific to activemq
avamar-messages.log	Raw JSON messages received from the Avamar adaptor
networker-messages.log	Raw JSON messages received from the NetWorker adaptor

The bundlelogs utility

The bundlelogs utility is built into the Backup & Recovery Manager server (OVA). The utility provides the ability to gather diagnostic information.

The following is a list of the information collected by the bundlelogs utility:

- /opt/emc/ucas/ucas-logs*
- /opt/emc/ucas/apache-logs/*
- /opt/emc/ucas/tomcat/logs/*
- ps -ef
- free memory
- uptime
- server kernel and architecture
- mount
- df -h
- /var/log/mongo/*
- mongodump (enabled by default)

Bundlelogs utility options

The following table lists the options available for the bundlelogs utility.

Table 46 Bundlelogs utility usage

Option	Description
-h	Display the bundlelogs utility help.
-d	-d <number>, specify the number of days of Mongo database data to dump (default is 1 day)
-x	Exclude the Mongo database dump.

Running the bundlelogs utility

You can use the bundlelogs utility command to gather diagnostic information from Backup & Recovery Manager server for troubleshooting.

Use the following command to run the bundlelogs utility:

```
$ ucas@localhost:~ $ ./bundlelogs -h -d2 -x
```

The following is an example of the bundlelogs utility output:

```
$ which bundlelogs
/opt/emc/ucas/tools/bundlelogs
ucas@idhcp247:~ $ bundlelogs
Starting log collection....
preparing temp area to gather logs from BRM....
sending signal to dump thread states....
copying UCAS logs...
copying apache logs...
copying tomcat logs...
copying mongo logs
gathering kernel info, memory, process lists, uptimes, & mounted
filesystems...
dumping mongo database...
dumping mongo from 20:57 08/29/12
connected to: 127.0.0.1
Generating Log Bundle for 08-30-12-20.57 Completed.
=====
Logfile bundle in /opt/emc/ucas/mongo-data/
bundlelogs-09-05-12-18.06.tgz
Please upload this logbundle to your EMC counterpart working this
issue.
```

NetWorker adaptor options

The NetWorker adaptor options are provided to adjust the performance and debugging capabilities of the NetWorker adaptor on Windows and UNIX.

Editing adaptor options on Windows

Procedure

1. Shut down the NetWorker ActiveMQ Adaptor service.
2. Edit the configuration file:


```
C:\Program Files (x86)\NetWorker Adaptor
Service-1.0\nsrmq.cfg
```

3. Save the file.
4. Restart the adaptor service.

Editing adaptor options on Linux

Procedure

1. From a command terminal, shut down the adaptor process:

```
/etc/init.d/nsrmqd stop -> stop
```

2. Edit the configuration file:

```
/etc/init.d/nsrmq.cfg
```

3. Save the file.
4. Restart the adaptor process:

```
/etc/init.d/nsrmqd start -> start
```

NetWorker adaptor command line options

The following table lists the options, their description, and use for the NetWorker adaptor from the Linux command line only:

/etc/init.d/nsrmqd <option>.

Table 47 NetWorker adaptor options

Option	Option long	Default	/Description	Use
-n	no daemon	no daemon	Run in the foreground on UNIX when launched from a terminal	Used to run the application and control it from a shell (that is, be able to kill it with a Ctrl-C)
-m	-mq-host=	localhost	ActiveMQ or RabbitMQ server name or IP address to which to connect	Used to tell the adapter which machine the Backup & Recovery Manager server is running
-p	--mq-port=	61610	ActiveMQ or RabbitMQ SSL connection port	Used when the Backup & Recovery Manager server is either using

Table 47 NetWorker adaptor options (continued)

Option	Option long	Default	/Description	Use
				non-default ports or connecting without SSL
-s	--server=	localhost	NetWorker server name or IP address to which to connect	Used to run the adapter against a NetWorker server on a remote machine
-t	--target=	Backup & Recovery Manager Main Queue	Destination queue for JSON messages	Used to change the queue that the adapter sends its messages to (generally not needed)
-u	--uid=	Run as the user launching the process	The userID to run as	Useful when starting the process as root but having it run as a more restricted user
-g	--gid=	Use the groups of the user launching the process	The group ID to run as	Useful when starting the process as root but having it run in a more restrictive group
	--chroot=	Use the current root directory	Chroot to a specified directory before running	Used to help secure things as the directory is considered the root and the process does not read or write anything above that level
	--connect-interval=	60	Message bus reconnect interval in seconds	Used to define how long to wait between attempts to connect to the message bus/ Backup & Recovery Manager server

Table 47 NetWorker adaptor options (continued)

Option	Option long	Default	/Description	Use
	--events-interval=	30	Events polling interval in seconds	Used to change how often user configuration changes are sent to the Backup & Recovery Manager server in case either the server has been overloaded (set to a larger interval) or more timely updates are desired (set a smaller interval)
	--logfile=	nsrmq.log	Write log messages to the specified file (set to '-' to write to the console)	Used primarily for directing log output to the shell when running in the foreground
	--nwid=	Use the name of the NetWorker server host machine	Override the ID to which the NetWorker server is registered	Used primarily as a development tool for simulating multiple NetWorker servers from a single one
	--pidfile=	nsrmq.pid	Name of the pid file	Required when running multiple adapters from the same directory so they do not overwrite each others pid files
	--prefix=	nsrmq	Use the specified prefix when syslogging	Useful for organizations having a company specific logging format
	--reconnect-interval=	60	NetWorker server reconnect interval in seconds	Defines how long to wait between attempts to reconnect to the NetWorker

Table 47 NetWorker adaptor options (continued)

Option	Option long	Default	/Description	Use
				server when the connection is lost
	--register-interval=	3600	NetWorker server registration interval in seconds	Used to change how often the adapter sends the "baseline" registration messages including all the group results (running or not) and configuration parameters
	--result-interval=	60	Group results polling interval in seconds	Used to change how often results are sent for running groups in case the querying is overloading the NetWorker server
	--rundir=	Run in the current directory	Change to the specified directory before running	Used for alternative way to start multiple adapters in the same directory but not have them overwrite each others pid and log files
	--status-interval=	10	Status polling interval in seconds	Used to change how often the dynamic attributes are queried from the NetWorker server and sent as activities messages if either the NetWorker server it has been overloaded (set to a larger interval) or more timely updates are desired (set a smaller interval)

Table 47 NetWorker adaptor options (continued)

Option	Option long	Default	/Description	Use
	--timeout=	600	NetWorker query timeout interval in seconds	Used to define how long to wait for the NetWorker server to respond before considering it unavailable and attempting to reconnect
	--umask=	077	The (octal) file creation mask to apply (non-world readable)	The default file creation mask is used to only enable access to the user for which the process is running (for example, root), this option is useful for allowing others to view the files such as the log file. --umask=022 is used to enable log files as world readable
	--debug	Do not run in the debugger	Run the reactor in the Python debugger	
	--euid	Use the current user ID	Run as the effective user id rather than the real user id	Similar to uid, enables the process to be started by root but with lesser privileges. Retains the ability to regain privileges as needed
	--syslog	Log to a file	Log to syslog, not a file	Useful for organizations desiring a central logging location
	--no-ssl	Connect using SSL	Do NOT connect to the ActiveMQ	

Table 47 NetWorker adaptor options (continued)

Option	Option long	Default	/Description	Use
			server using SSL (requires overriding the default port)	
	--verbose	Standard logging level	Run in verbose mode to provide information on the NetWorker adaptor	
	--trace	Do not dump stack traces	Dump stack traces to the log when errors occur to provide information on the NetWorker adaptor	
	--version	Run as normal	Print the version information to provide information on the NetWorker adaptor and exit	
	--help	Run as normal	Display the help text and exit	

Avamar adaptor control script

The following Avamar control scripts enable you to complete Avamar tasks:

- For Avamar 7.0 and earlier:

```
adaptorctl.pl options
```

- For Avamar 7.1 and later:

```
msgbrokerctl.pl options
```

The following table lists the available options for the Avamar control script:

Table 48 Avamar adaptor control script

Avamar adaptor control script options	Description
--brmhost = <addresses>	For Avamar 7.0 and earlier, use only with --setup. Provide a comma separated list of one or more addresses, optionally

Table 48 Avamar adaptor control script (continued)

Avamar adaptor control script options	Description
	with a colon and port number that is specified for each address.
--help	Opens the help file for these options.
--jmsaddr=<addresses>	For Avamar 7.1 and later, use only with --setup. Provide a comma separated list of one or more addresses, optionally with a colon and port number that is specified for each address.
--setup	Setup ActiveMQ and the Avamar adaptor.
--start	Start the Avamar adaptor.
--status	Display the status of the Avamar adaptor.
--stop	Stop the Avamar adaptor.

Backup & Recovery Manager error messages

For Backup & Recovery Manager activities that do not successfully complete:

- A numeric error code is listed.
- Backup & Recovery Manager errors are listed as BRM in the Type column.
- The ability to sort and hide the messages is available. Double-click the error code to view a detailed explanation. The following table lists the error codes and their descriptions.

Table 49 Backup & Recovery Manager error codes

Numeric error code	Error code description
1	Connection to server <system name> has failed for the last <##> minutes.
2	Connection to server <system name> has returned to normal.
3	/opt/mongo-data has <##.#>% space remaining.
4	<##> records older than <date/time> were deleted. Current DB storage is <##.#> MB
5	User authentication to Data Domain system <system name> has failed.
6	Connection to Data Domain system <system name> has failed.

APPENDIX C

Disaster Recovery

This section provides the information on how to prevent a disaster by creating a duplicate of the Backup & Recovery Manager server for protection in the event of catastrophic data loss:

- [Clone a Virtual Machine in the vSphere Client](#)..... 178
- [Recovering the Backup & Recovery Manager server](#)..... 179

Clone a Virtual Machine in the vSphere Client

Cloning creates a duplicate of the virtual machine with the same configuration, installed software, and application data as the original at the point-in-time of the clone.

Optionally, customize the guest operating system of the clone to change the virtual machine name, network settings, and other properties. This prevents conflicts that can occur if a virtual machine and a clone with identical guest operating system settings are deployed simultaneously.

Complete details on cloning a virtual machine is available in the [ESXi and vCenter Server 5 documentation](#).

Prerequisites

The following prerequisites must be met before you begin the clone operation:

- Connect directly to the vCenter Server in order to clone a virtual machine. Virtual machines that are connected directly to an ESXi host cannot be cloned.
- To customize the guest operating system of the virtual machine, check that the guest operating system meets the requirements for customization.
- To use a customization specification, first create or import the customization specification.
- To use a custom script to generate the hostname or IP address for the new virtual machine, configure the script.

Cloning the Backup & Recovery Manager server

Cloning provides the ability to create a duplicate of the virtual machine with the same configuration, installed software, and application data as the original at the point-in-time of the clone.

Procedure

1. Right-click the virtual machine and select **Clone**.
2. Enter a virtual machine name, select a location, and click **Next**.
3. Select a host or cluster on which to run the new virtual machine.
4. Select a resource pool in which to run the virtual machine and click **Next**.
5. Select the datastore location to store the virtual machine files.
6. Select the format for the virtual machine's disks and click **Next**.
7. Select a guest operating system customization option.
8. Review the selections and select whether to power on the virtual machine or edit virtual machine settings.

Results

The cloned virtual machine is deployed. The virtual machine cannot be used or edited until the cloning is complete. This might take several minutes if the cloning includes creating a virtual disk. If required, cancel the cloning at any point before the customization stage.

Recovering the Backup & Recovery Manager server

You can recover the Backup & Recovery Manager server by using the Avamar VMware plugin.

Procedure

1. Configure VMware proxy with vCenter. The Avamar for VMware User Guide provides details on configuring the VMware proxy with vCenter.
2. Take a VM backup of the Backup & Recovery Manager server by using the Avamar Plugin. The Avamar for VMware User Guide provides details on backing up the Backup & Recovery Manager with the Avamar Plugin.
3. Restore the backed up VM by using Restore to New Virtual Machine. The Backup & Recovery Manager server is successfully recovered.
4. When the restore operation completes, edit the network configuration with same IP address.

NOTICE

This is a restriction for Linux VMs in VMware VM backups.

A new virtual NIC ID is created in the restored Backup & Recovery Manager server:

- a. Delete the old NIC card and provide all the Network information for the new NIC card.
- b. Restart the network services.
- c. Restart the Backup & Recovery Manager server.
- d. Login Backup & Recovery Manager.

Re-registering the Avamar or NetWorker servers if required

You can register or re-register the Avamar or NetWorker servers if they become offline in Systems. The server appears grayed out if it is offline.

Procedure

- For Avamar 7.0.x and earlier, use the following command:

```
adaptorctl.pl --setup --jmsaddr=<ucas server>
```
- For Avamar 7.1 and later, use the following command:

```
msgbrokerctl.pl --setup --brmhost=<ucas-server>
```
- For NetWorker, restart the NetWorker adaptor service.

GLOSSARY

This glossary contains terms related to disk storage subsystems. Many of these terms are used in this manual.

A

- adaptor** A Backup & Recovery Manager adaptor is the appliance that is used to interface with the Backup & Recovery Manager server on Avamar, NetWorker and Data Domain.
- Avinstaller** A backend service that executes and reports package installations. The Avinstaller is used to install the Avamar Backup & Recovery Manager adaptor.

B

- Backup & Recovery Manager server** The Backup & Recovery Manager server is the appliance which must be deployed in order to run the Backup & Recovery Manager adaptors.

C

- cache** Random access electronic storage used to retain frequently used data for faster access by the channel.
- checkpoint** Checkpoints are system-wide backups taken for the express purpose of assisting with disaster recovery.
- clone** Duplicate copy of:
- Backed-up data, which is indexed and tracked by the NetWorker server. Single save sets or entire volumes can be cloned.
 - Virtual machine with the same configuration, installed software and application data as the original at the point-in-time of the clone.

D

- dataset** A policy that defines a set of files, directories, and filesystems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

E

- enterprise** Computers and folders organized into a tree-based visual representation.

Enterprise Manager Server (EMS) The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar system information, and provides a mechanism for managing Avamar systems using a standard web browser. The EMS also communicates directly with Management Console Servers (MCS).

F

full replication A full “root-to-root” replication creates a complete logical copy of an entire source system on the destination system. The replicated data is not copied to the REPLICATE domain. Instead, it is added to the root domain just as if source clients had registered with the destination system. Also, source server data replicated in this manner is fully modifiable on the destination system. This replication method is typically used for system migration (from a smaller Avamar configuration to a larger, possibly multi-node configuration) or system replacement (for instance, in a case of disaster recovery).

G

- group**
- A level of organization in Avamar Administrator for one or more Avamar clients. All clients in an Avamar group use the same group policies, which include the dataset, backup schedule, and retention policy.
 - Client computer or group of clients that are configured to back up files during a NetWorker scheduled backup, according to a single designated schedule or set of conditions.

H

HFS Hash Filesystem. The content addressed storage area inside the Avamar server used to store client backups.

I

I/O device An addressable input/output unit, such as a disk or tape device.

ID Identifier, a sequence of bits or characters that identifies a program, device, controller, or system.

J

Java Type of high-level programming language that enables the same, unmodified Java program to run on most computer operating systems. **See [Java Virtual Machine \(JVM\)](#)**

Java archive (JAR) File that contains compressed components needed for a Java applet or application.

Java plug-in JVM that can be used by a web browser to run Java applets.

Java Virtual Machine (JVM) Execution environment for interpreting the Java programming language. Each operating system runs a unique JVM to interpret Java code.

K

KB Kilobyte, 1024 bytes.

L

label Electronic header on a volume used for identification by NetWorker or other data mover application.

Logical Volume Manager (LVM) Software that controls disk resources by mapping data between a logical view of storage space and the actual physical disks.

N

NetWorker Management Console (NMC) Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.

O

OVA Is the application server deployed as a virtual machine. The Backup & Recovery Manager server (OVA) raw database is a temporary buffer for storing messages until they are processed.

P

promotion The process of moving data from a track on the disk device to cache slot.

R

replication Replication is an optional feature that enables one Avamar server to store a read-only copy of its data on another Avamar server to support future disaster recovery of that server.

restore File or object restore. An operation that retrieves one or more filesystems, directories, files, or data objects from a backup and writes the data to a designated location.

roles A setting in the Backup & Recovery Manager that controls which operations each user can perform. Roles are assigned on a user-by-user basis.

S

save set Group of data from a single NetWorker client computer that is backed up on storage media.

U

- user**
1. A NetWorker user who can back up and recover files from a computer.
 2. A Console user who has standard access privileges to the Console server.

V

- volume**
- Unit of physical storage medium, such as a magnetic tape, optical disk, or filesystem used to store data. Backup data must be stored on a backup volume and cannot be stored on an archive volume or a clone volume.
 - Identifiable unit of data storage that may reside on one or more computer disks.