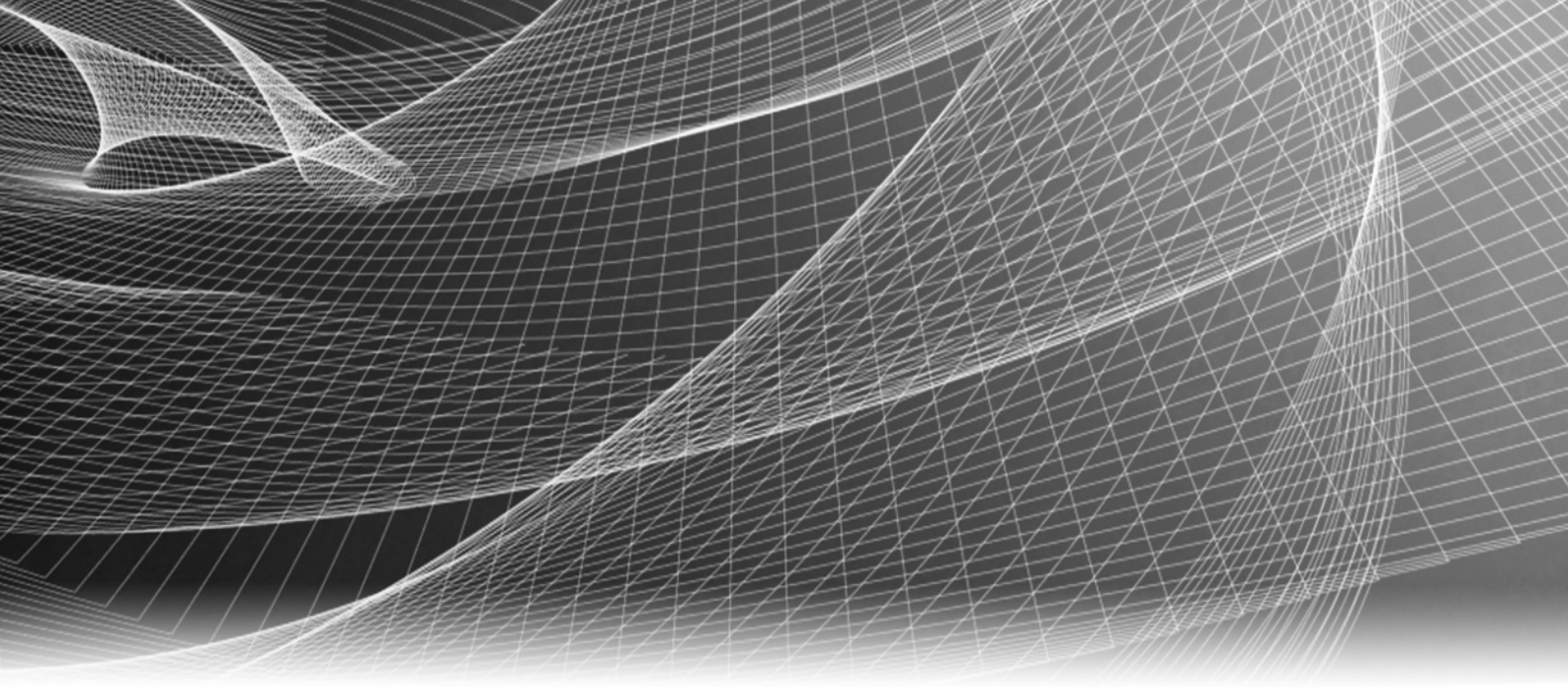


EMC® Avamar® 7.0

Administration Guide

P/N 300-015-221
REV 03

EMC²

Published November, 2013

EMC 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. EMC Corporation 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.

CONTENTS

Preface

Chapter 1 Introduction

EMC Avamar 26
Important terms and concepts 26
Avamar system 26
Avamar server 27
Node 27
Hard disk storage 27
Stripes 27
Object 27
Data deduplication 28
Replication 28
Functional overview 28
Avamar servers 28
Avamar clients 30
Avamar Administrator 31
Encryption 31
Avamar, IPv4, and IPv6 31

Chapter 2 Avamar Administrator

Installing Avamar Administrator 34
Installing on Microsoft Windows 34
Installing on Linux 35
Upgrading Avamar Administrator 36
Upgrading on Microsoft Windows 36
Upgrading on Linux 36
Uninstalling Avamar Administrator 37
Uninstalling on Microsoft Windows 37
Uninstalling on Linux 37
Session time-out 37
Setting a session time-out value 38
Starting Avamar Administrator 39
Avamar Administrator dashboard 42
Launcher buttons 42
System Information panel 43
Capacity panel 46
Activities panel 47
Critical Events panel 49
Exploring the Avamar Administrator user interface 50
Status bar 50
Launcher shortcuts 50
Status messages 51
Navigation tree features 53
Mouse shortcuts 53

Chapter 3 Domains, Clients, and Users

Domains 56
Understanding Avamar domains and subdomains 56
Creating a domain 57
Editing domain information 58
Deleting a domain 59
Clients 60
Understanding Avamar clients 60
Registering a single client 62
Batch client registration 63
Activating a client 66
Editing client information 67
Viewing client properties 68
Enabling and disabling a client 69
Retiring a client 70
Moving a client to a new domain 71
Deleting a client 71
Editing client paging settings 72
Using Avamar in non-pageable environments 74
Understanding users, authentication, and roles 76
Users 76
User authentication 77
Roles 78
Enabling user authentication 84
Enabling internal Avamar authentication 84
Enabling directory service authentication 84
Enabling selection of enterprise authentication 88
Managing user accounts 90
Adding a user to a client or domain 90
Editing user information 92
Deleting a user 93

Chapter 4 Backup, Restore, and Backup Management

Performing an on-demand backup 96
Restoring data from a backup 98
Finding a backup to restore 98
Restoring to the original location 101
Restoring to a different location 102
Restoring to multiple locations 105
Managing backups 108
Understanding backup expiration and deletion 108
Finding a backup to manage 108
Changing a backup expiration date 110
Changing backup retention types 111
Validating a backup 112
Viewing backup statistics 113
Deleting a backup 116
Monitoring backup, restore, or validation activities 116
Canceling a backup, restore, or validation 122

Chapter 5 Datasets, Schedules, and Retention Policies

Datasets 124
Understanding datasets 124

Dataset catalog 125
Creating a dataset 128
Editing a dataset 131
Copying a dataset 132
Deleting a dataset 133
Schedules 134
Understanding schedules 134
Schedule catalog 135
Creating a schedule 136
Editing a schedule 142
Copying a schedule 144
Deleting a schedule 144
Running a schedule now 145
Editing the Override Daily Schedule 145
Retention policies 147
Basic retention settings 147
Advanced retention settings 148
Minimal retention 148
Last backup retention 149
Retention policy catalog 149
Creating a retention policy 150
Editing a retention policy 151
Copying a retention policy 152
Deleting a retention policy 152
Enabling the Minimal Retention policy 153
Disabling the Minimal Retention policy 154

Chapter 6 Groups and Group Policies

Important terms and concepts 156
Group members 156
Group policy 156
Default Group 156
Default Proxy Group 156
Default Virtual Machine Group 156
vCenter groups 157
Inheritance and client overrides 157
Policy window overview 157
Groups tab 158
Clients tab 159
Creating a group 159
Editing group properties 164
Editing a single group 164
Editing multiple groups 164
Copying a group 165
Enabling and disabling a group 166
Deleting a group 166
Viewing the Group Summary Reports 167
Viewing the Group Status Summary 168
Managing group membership 169
Adding, removing, or moving group members 169
Editing client group memberships 170
Overriding group policy settings for a single client 171
Allowing users to initiate backups 171
Allowing users to select data source for on-demand backups 175

Allowing scheduled backups to run overtime 176
Changing the encryption setting 177
Allowing users to select an alternative backup start time 178
Assigning backup limits 180
Assigning a different dataset 181
Allowing users to add to source data 182
Assigning a different retention policy 184
Overriding group policy settings for multiple clients 185
Performing on-demand group and client backups 187
Perfoming on-demand group and client replications 188

Chapter 7 Events, Notifications, and Profiles

Important terms and concepts 190
Events 190
Audit logging 191
Customizing error events 191
Notifications 192
Profiles 193
Profile catalog 193
Editing system event profile properties 195
Creating a custom event profile 196
Editing custom event profile properties 203
Copying a custom event profile 204
Testing custom event profile notifications 205
Enabling and disabling a custom event profile 206
Deleting a custom event profile 206
Modifying “Email Home” configuration 206
Modify mcserver.xml Email Home settings 207
Monitoring the Avamar server using syslog 209
Prerequisite knowledge and resources 209
Overview 209
Configuring local syslog 211
Configuring remote syslog 213
Monitoring the Avamar server using SNMP 218
Prerequisite knowledge and resources 218
Overview 218
Task list 220
Configuring the Net-SNMP agent 220
Configure a custom event profile 223
Managing ConnectEMC 224
EMC Secure Remote Support (ESRS) 224
User-configurable transports 224
Enabling and disabling ConnectEMC 225
Stopping and starting ConnectEMC 226
Editing Primary and Failover transports 227
Editing the Notification transport 230
Testing transports 232

Chapter 8 Reporting

Avamar reports 234
Predefined reports 234
Report templates 236
Creating a report 237

Editing a report 240
Running a report 241
Deleting a report 242
Viewing the Client Summary Report 242
Viewing the Activity Report 246
Viewing the Replication Report 250
Backend capacity reports 252
Limitations 253
Running backend capacity reports from Avamar Administrator 253
Running backend capacity reports from the command line 254
Exporting displayed tabular data as CSV files 256
Activity Report 256
Replication Report 256
Client Summary Report 257
Event Management 257
Session Monitor 257
Support for third-party reporting tools 258
PostgreSQL 258
Crystal Reports templates 258
Setting up the PostgreSQL ODBC driver 258
Crystal Reports templates 260
Other third-party support 261

Chapter 9 Avamar Client Agent and Plug-in Management

Important terms and concepts 264
Disabling a version or build 264
Selective management of plug-in operations 264
Obsolete versions and builds 264
Agents Summary view 264
Plug-ins Summary view 265
Adding a build record 267
Editing version or build record settings 269
Deleting a build record 270
Enabling and disabling all client initiated activations 271
Enabling and disabling all client initiated backups 272

Chapter 10 Server Monitoring

Recommended daily server monitoring 274
Monitoring the server 274
Server Monitor tab 275
Server Management tab 278
Replication Storage Mapping tab 287
Session Monitor tab 287
Checkpoint Management tab 288
Verifying system integrity 289
Viewing system events 290
Filtering the Event Monitor display 292
Viewing the Audit Log 295
Filtering the Audit Log display 297
Viewing services information 299
Viewing a detailed client session log 301
Creating a Zip file for EMC Customer Support 303
Collecting and viewing log files 304

Chapter 11 Basic Server Administration

Avamar server functional block diagram 306
Data server 306
Management Console Server (MCS) 306
Enterprise Manager Server (EMS) 307
Viewing and editing server contact information 308
Avamar server maintenance activities and backup/maintenance windows 309
Maintenance activities 309
Backup/maintenance windows 309
Best practices 310
Acknowledging system events 311
Suspending and resuming backups and restores 312
Suspending and resuming scheduled operations 313
Enabling and disabling scheduled group backups 313
Suspending and resuming maintenance activities 314
Changing backup/maintenance window settings 314
Managing services 316
Canceling a client session 317
Resetting a client 318

Chapter 12 Server Shutdown and Restart

Shutting down the server 320
Restarting the server 321
Stopping the MCS 322
Starting the MCS 322
Getting MCS status 323

Chapter 13 Avamar Enterprise Manager

Capabilities and limitations 326
Multi-system management 326
Dashboard 326
Only one Avamar Enterprise Manager server is required 326
Monitoring multiple versions of Avamar systems 326
Use local MCS to authenticate Avamar Enterprise Manager logins 326
Avamar Enterprise Manager compared with Avamar Administrator 326
Web browser security settings 327
Browser security settings may impact login 327
Session time-out information 327
Comparison with EMC Backup & Recovery Manager 328
Shutting down the EMS 329
Restarting the EMS 329
Logging in to Avamar Enterprise Manager 330
Dashboard 331
System 335
Individual system information page 335
All servers information (detailed dashboard) page 343
Capacity 344
Policy 344
Reports 345
Running a report 346
Exporting a report as a CSV File 346
Replicator 346
Configure 347

Client Manager 348
System Maintenance 348
Monitoring other systems 348
Suspending and resuming system monitoring 350
Removing a system from the systems list 351
Monitoring Avamar 5.x systems 352
Obtain and install the server hotfix 352
Configure MCS web services 352
Add the system to Avamar Enterprise Manager 353
Launching Avamar Administrator from Avamar Enterprise Manager 353

Chapter 14 Capacity Management

Capacity limits and thresholds 358
Obtaining capacity utilization information 359
Avamar Administrator 359
Avamar Enterprise Manager 360
Capacity forecasting 361
Important limitation regarding capacity data after a rollback 362
Detailed utilization and forecasting 362
Customizing capacity limits and behavior 363
Avamar Administrator settings 363
Avamar Enterprise Manager settings 364
Updating Avamar application preference files 365
Server and client average daily change rates 366
Server data 366
Client data 367

Chapter 15 Replication

Overview 370
The REPLICATE domain 370
Policy-based versus cron-based replication 370
Limitations 371
Only static data is replicated 371
Avamar Administrator manages only one source server at a time 371
Time zones 371
Best practices 371
Avoid source and destination server incompatibilities 371
Schedule replication during periods of low backup activity 371
Optimize replication group size 372
Use a large timeout setting initially 372
Managing replication with Avamar Administrator 373
Replication groups 374
Destinations 382
Performing an on-demand group replication 384
Canceling a replication activity 385
Managing cron-based replication with Avamar Administrator 385
Viewing replication statistics with Avamar Administrator 388
Managing replication with Avamar Enterprise Manager 389
Replicator setup page 389
Replicator status page 391
Configuring or modifying replication settings 392
Getting replication status 393
Starting and stopping daily replications 394

Managing replication from the command line 394
Synopsis 395
Operations 395
Replicate options 395
Account options 398
Logging options 399
Target list 399
Avamar-only options 400

Chapter 16 Advanced Server Administration and Maintenance

Checkpoints 404
Creating a checkpoint 404
Validating a checkpoint 405
Deleting a checkpoint 406
Rolling back to a checkpoint 406
Clearing data integrity alerts 407
MCS configuration settings 408
Understanding MCS configuration settings 408
Backing up MCS data 409
Performing an on-demand MCS flush 409
Finding MCS backups in the system 410
Restoring MCS data 410
Reverting to default MCS preference settings 411
Configuring directory service information 412
Port requirements 412
Login requirements 412
Providing LDAP information 413
Providing NIS information 414
Testing a directory service entry 414
Error messages for unsuccessful tests 415
Text editing of ldap.properties and krb5.conf 416
Changing the time-out value 417
Setting last backup retention 419
Manually changing Avamar Administrator client preferences 420
Updating server licensing 420
Avamar products 420
Avamar products included in EMC Backup Software suite 420
License installation road map 421
Generating a license key information file 421
Generating a permanent license key file 423
Installing and activating the license 423
Using the change-passwords utility with default user accounts 424
Changing single-node server network settings 431
Custom notification for web browser logins 432
Adding a custom security notification 432
Configuring Avamar to use network address translation 432
Resolving NAT connection and configuration problems 434

Chapter 17 Server Updates and Hotfixes

Overview 436
Avamar Downloader Service 437
Avamar Downloader Service security 437
Avamar Downloader Service components 437

Avamar Downloader Service installation requirements 438
Installing the Avamar Downloader Service 439
Downloading the software 439
Installing the software 440
Defining an inbound rule for Microsoft Windows 7 hosts 441
Configuring the Avamar Downloader Service 442
Using the Avamar Downloader Service 444
Starting the Avamar Downloader Service configuration application 444
Using the Avamar Downloader Service menu options 445
Monitoring Avamar Downloader Service status 446
Checking the EMC repository 447
Checking for Avamar Downloader Service updates 448
Modifying the repository credentials 448
Modifying the username or password 450
Removing an Avamar system from the Known Systems list 451
Viewing version and copyright information 451
Troubleshooting Avamar Downloader Service issues 452
Not receiving files from the Avamar FTP site 452
Downloading a package fails 452
Temporary IPv6 addresses cause package download to fail 452
Uninstalling the Avamar Downloader Service 453
Installing packages from System Maintenance 453
Microsoft Windows browser requirements 453
EMC Customer Support account 453
Maintenance and SW Updates tabs 454
Installing workflow packages from the Maintenance tab 455
Installing patch and hotfix packages from the SW Updates tab 458
Deleting packages 459
Viewing installation history information 460

Chapter 18 Client System Recovery

Windows client system recovery 466
Red Hat and CentOS Linux system recovery 466
Prerequisites 466
Reconstruct partition table 466
Recovery target client preparation 468
Recovery procedure 468
Troubleshooting 473
SUSE Linux system recovery 474
Prerequisites 474
Reconstruct partition table 474
Recovery target client preparation 476
Recovery procedure 476
Troubleshooting 481
Oracle Solaris system recovery 482
Prerequisites 482
Procedure 483

Chapter 19 Avamar Client Manager

Capabilities 488
Starting Avamar Client Manager 488
Starting from Backup & Recovery Manager 488
Starting from Avamar Enterprise Manager 488

General information 489
Connection security 489
Apache web server authentication 489
Editing the session time-out period 489
Increasing the JavaScript time-out period 490
Configuration properties 491
Support for version 5.x servers 493
Global tools 494
Selecting a server 495
Filters 495
Viewing details 501
Exporting data 502
Setting the entries per page limit 502
Viewing tool tips 502
Overview page 503
Server Summary 503
Dashboard 504
Clients page 507
Client and server tools 507
Add Clients section 514
Registered Clients section 519
Activated Clients section 520
Failed Clients section 523
Idle Clients section 523
Upgrade Clients section 523
Policies page 527
Columns on the Policies page summary view 528
Adding clients to a group 528
Removing clients from a group 529
Viewing a group's dataset policy 529
Dataset policy details 529
Viewing a group's retention policy 530
Retention policy details 530
Viewing a group's schedule policy 530
Schedule policy details 531
Queues page 532
Columns on the Queues page summary view 532
Activation queue descriptions 533
Canceling a task 533
Logs page 534
Columns on the Logs summary view 534
Viewing the client log after upgrading an Avamar client 535
Clearing all log entries in a section 535

Chapter 20 Avamar Desktop/Laptop

Features 538
Environment requirements 539
Computer requirements 539
Network requirements 540
LDAP authentication requirements 540
Avamar authentication requirements 540
NIS authentication requirements 541
Avamar system requirements 541
User authentication 542

Pass-through authentication 542
LDAP authentication 544
NIS authentication 546
Avamar authentication 547
Apache web server authentication 549
Web UI port change 549
Changing the port on the client 550
Changing the port on the server 550
Secure token time-out value 551
Changing the secure token time-out value 551
Alternate file browsing method for clients 552
Rebranding the web UI 552
Checking the status of Avamar Desktop/Laptop server 553
Stopping and starting Avamar Desktop/Laptop server 554
User selectable backup start times 554
Requirements 554
Available start time list 554
Time zone 555
On-demand backups 555
On-demand backup limit 555
Retention policy 556
Disabling on-demand backups 557
Source data additions 558
Selectable backup sets 558
Enabling selectable backup sets 558
Restore of replicated backups 559
Restore from an alternate computer 559
Restoring from an alternate computer 560
Viewing history for an alternate computer 561
Disabling restore from an alternate computer 561
Restricting file access for Windows administrators 562
Server-class clients 562
Back up now dataset 563
Backup of large number of files 563
Backup on battery power 563
Disable restores 564
Restore data size limit 565
Setting a restore data size limit 565
Restore queue limit 566
Removing the restore queue limit 566
Avamar client software installation 567
Supported systems management tools 567
Push installation on Windows computers 567
Push installing on Macintosh computers 569
Local installation of the client 570
Remove the Avamar client software 571
Removing the software on Windows 571
Removing the software on Macintosh 571
Client log locations 571

Chapter 21 Data Domain Systems

Introduction to Avamar and Data Domain system integration 574
New features for Data Domain system integration 574
Architecture overview 575

Backup support 576
File system support 577
Avamar client support 577
NDMP support 578
Avamar checkpoint backup support 578
Backup 578
Restore 578
VMware Instant Access 579
Replication 579
Monitoring and reporting 579
Security 580
Encryption 580
User access 580
Data migration 580
Pre-integration requirements 580
Network throughput 581
Network configuration 581
NTP configuration 581
Licensing 581
Port usage and firewall requirements 582
Capacity 582
Data Domain system streams 582
Existing backup products in use with Data Domain 583
Preparing the Data Domain system for Avamar integration 583
Adding Data Domain systems to Avamar 585

Appendix A Command Shell Server Logins

User accounts 590
Starting command shell sessions 590
Switching user IDs 590
Using sudo 591
Prefixing commands with sudo 591
Spawning a sudo Bash subshell 591

Appendix B Plug-in Options

How to set plug-in options 594
Backup options 594
Restore options 597

Appendix C MCS and EMS Database Views

Data types 600
MCS database views 600
v_activities 600
v_activities_2 603
v_activity_errors 606
v_audits 606
v_client_backups_users 608
v_clientperftrack 609
v_clients 610
v_clients_2 612
v_compatibility 614
v_datasets 614
v_ddr_node_space 614

v_dpnsummary 615
v_dpn_stats 616
v_ds_commands 616
v_ds_excludes 616
v_ds_includes 617
v_ds_targets 617
v_dtlt_dataset_targets 617
v_dtlt_sched_override 618
v_ev_catalog 618
v_ev_cus_body 620
v_ev_cus_cc_list 620
v_ev_cus_codes 620
v_ev_cus_prof 621
v_ev_cus_prof_params 621
v_ev_cus_rpt 622
v_ev_cus_snmp_contact 622
v_ev_cus_syslog_contact 623
v_ev_cus_to_list 623
v_ev_unack 624
v_events 625
v_gcstatus 626
v_group_members 626
v_groups 627
v_node_space 627
v_node_util 628
v_plugin_can_restore 629
v_plugin_catalog 629
v_plugin_depends_upon 630
v_plugin_flag_groups 630
v_plugin_flag_pulldown 630
v_plugin_flags 631
v_plugin_options 632
v_plugin_state 632
v_plugins 633
v_repl_activities 633
v_repl_backups 635
v_report_filter 637
v_reports 637
v_retention_policies 637
v_sch_recurrence 638
v_schedules 639
v_schedules_2 640
v_serial_numbers 641
v_systems 641
EMS database views 642
v_avamar_server 642
v_compatibility 643

Glossary

TABLES

	Title	Page
1	Revision history	21
2	Dashboard launcher buttons	42
3	Dashboard detailed system state information	43
4	Scheduler status	45
5	Maintenance activities status	45
6	Dashboard detailed backup jobs status information	47
7	Dashboard Critical Events panel.	49
8	Status bar icons	50
9	Scheduler and backup dispatching status messages	51
10	Status messages for unacknowledged events	51
11	Operational status messages for Avamar or Data Domain	52
12	Entry element attributes	64
13	Client properties summary	68
14	Methods to browse to a backup by file or folder	101
15	Backup Statistics dialog box tabs	114
16	Backup Statistics dialog box tabs	115
17	Activity Monitor tab columns	117
18	Directories excluded from Default Dataset backups	126
19	Directories excluded from Unix Dataset backups	126
20	Directories excluded from Windows Dataset backups	127
21	Dereference flag and folder wildcard examples	130
22	Schedule types	134
23	Schedule catalog	135
24	Basic retention settings	147
25	Types of retention policies	149
26	Buttons on the Policy window's Groups tab	158
27	Buttons on the Policy window's Clients tab	159
28	Group Status Summary information	168
29	Event information	190
30	Test methods for custom event profile notifications	205
31	Syslog field and Avamar Event data mappings	211
32	Avamar MIB definition file locations	219
33	Edit Primary Transport dialog box settings	228
34	Predefined Avamar reports	234
35	Report templates	236
36	Avamar report template descriptions	239
37	Client Summary report column descriptions	243
38	Activity report column descriptions	246
39	Replication report column descriptions	250
40	Avamar Crystal Reports templates	261
41	Avamar agents property descriptions	265
42	Avamar plug-in property descriptions	266
43	System monitoring tools and tasks	274
44	Server Monitor Avamar tab properties	275
45	Server Monitor Data Domain tab properties	277
46	Bytes Protected Summary properties on the Server Management tab	279
47	Server properties on the Server Management tab	279
48	Module properties on the Server Management tab	281
49	Node properties on the Server Management tab	281
50	Partition properties on the Server Management tab	283

51 Data Domain system properties on the Server Management tab 284
52 Session Monitor tab properties 287
53 Checkpoint Management tab properties 288
54 Event Monitor columns 290
55 Event Monitor filtering criteria 293
56 Audit Log column information 295
57 Audit Log filter criteria 298
58 Services Administration tab properties 299
59 Comparison of enterprise management products 328
60 Dashboard page information 331
61 Server status information 336
62 System activity information 342
63 Avamar system column information on the Configure page 347
64 MCS web service configuration settings 352
65 Secure Protocol settings 353
66 Capacity limits and thresholds 358
67 Avamar Administrator capacity management preferences 363
68 Avamar Enterprise Manager capacity management preferences 364
69 Replication cron job information 386
70 Avamar Enterprise Manager replication management 389
71 Replicator setup for Avamar systems 390
72 Replicator status for Avamar systems 391
73 Replicate avrepl options 395
74 Account options for avrepl 398
75 Logging options for avrepl 399
76 Avamar-only advanced options for the avrepl command 400
77 Avamar server checkpoint states 404
78 MCS backup timestamp files 409
79 Error message information 415
80 KV pairs in ldap.properties 417
81 Common NAT connection and configuration problems and their solutions 434
82 Avamar Downloader Service components 437
83 Installation requirements for the Avamar Downloader Service 438
84 Avamar Downloader Service task tray icon menu options 445
85 Avamar Downloader Service monitor status messages 446
86 Options in the Show Advanced Settings dialog box. 449
87 Item and column descriptions 454
88 Installation Progress page item descriptions 457
89 Installation Progress page item descriptions 459
90 History table column information 461
91 Detail table column descriptions 462
92 Windows client system recovery publications 466
93 Target locations 482
94 Other system directories and virtual file systems 482
95 Avamar Client Manager properties 491
96 Limitations for moving clients to a new server 493
97 Descriptions of client status values 497
98 Descriptions of client activation status codes 499
99 Descriptions of Details panel fields for clients 501
100 Descriptions of Details panel fields for groups 501
101 Descriptions of the columns on the Server Summary section 503
102 Descriptions of the columns in the Server panel grid 505
103 Descriptions of columns on group associations lists 508
104 Descriptions of the group policy override settings 510
105 Descriptions of the summary information fields 511

106 Descriptions of the columns on the Backups tab 513
107 Descriptions of the columns on the Plug-ins tab 513
108 Select Retention Policy options 522
109 Descriptions of filters used when working with failed clients 523
110 Client version support for client and plug-in upgrades 524
111 Descriptions of package status values 526
112 Descriptions of the columns on the Policies page summary view 528
113 Descriptions of the attributes displayed in the dataset policy dialog box 529
114 Descriptions of the attributes displayed in the retention policy dialog box 530
115 Descriptions of the attributes displayed in the schedule policy dialog box 531
116 Descriptions of the columns displayed on the Queues page summary view 532
117 Descriptions of entries in the Description field of the Activation queue summary 533
118 Descriptions of the columns displayed in the logs summary view 534
119 Minimum requirements for client computers using Avamar Desktop/Laptop 539
120 Network requirements 540
121 LDAP authentication requirements 540
122 Avamar authentication requirements 540
123 NIS support requirements 541
124 Path to avscc.cfg 550
125 Path to Apache SSL configuration file 550
126 Operating systems and associated datasets used by on-demand backups 555
127 Possible values for limiting on-demand backups 556
128 Requirements for restoring from an alternate computer 559
129 Arguments to apply Windows install options 568
130 Paths to logs on Windows computers 572
131 Paths to logs on Linux computers and Mac computers 572
132 Licensing requirements 581
133 Data Domain requirements 583
134 Backup plug-in options 594
135 Restore plug-in options 597
136 Database view data types 600
137 MCS database v_activities view 600
138 MCS database v_activities_2 view 603
139 MCS database v_activity_errors view 606
140 MCS database v_audits view 606
141 MCS database v_client_backups_users view 608
142 MCS database v_clientperftrack view 609
143 MCS database v_clients view 610
144 MCS database v_clients_2 view 612
145 MCS database v_compatibility view 614
146 MCS database v_datasets view 614
147 MCS database v_ddr_node_space view 614
148 MCS database v_dpnsummary view 615
149 MCS database v_dpn_stats view 616
150 MCS database v_ds_commands view 616
151 MCS database v_ds_excludes view 616
152 MCS database v_ds_includes view 617
153 MCS database v_ds_targets view 617
154 MCS database v_dtlt_dataset_targets view 617
155 MCS database v_dtlt_sched_override view 618
156 MCS database v_ev_catalog view 618
157 MCS database v_ev_cus_body view 620
158 MCS database v_ev_cus_cc_list view 620
159 MCS database v_ev_cus_codes view 620
160 MCS database v_ev_cus_prof view 621

161 MCS database v_ev_cus_prof_params view 621
162 MCS database v_ev_cus_rpt view 622
163 MCS database v_ev_cus_snmp_contact view 622
164 MCS database v_ev_cus_syslog_contact view 623
165 MCS database v_ev_cus_to_list view 623
166 MCS database v_ev_unack view 624
167 MCS database v_events view 625
168 MCS database v_gcstatus view 626
169 MCS database v_group_members view 626
170 MCS database v_groups view 627
171 MCS database v_node_space view 627
172 MCS database v_node_util view 628
173 MCS database v_plugin_can_restore view 629
174 MCS database v_plugin_catalog view 629
175 MCS database v_plugin_depends_upon view 630
176 MCS database v_plugin_flag_groups view 630
177 MCS database v_plugin_flag_pulldown view 630
178 MCS database v_plugin_flags view 631
179 MCS database v_plugin_options view 632
180 MCS database v_plugin_state view 632
181 MCS database v_plugins view 633
182 MCS database v_repl_activities view 633
183 MCS database v_repl_backups view 635
184 MCS database v_report_filter view 637
185 MCS database v_reports view 637
186 MCS database v_retention_policies view 637
187 MCS database v_sch_recurrence view 638
188 MCS database v_schedules view 639
189 MCS database v_schedules_2 view 640
190 MCS database v_serial_numbers view 641
191 MCS database v_systems view 641
192 EMS database v_avamar_server view 642
193 EMS database v_compatibility view 643

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC Customer Support professional if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This guide describes how to configure, administer, monitor, and maintain the Avamar system.

Audience

The information in this guide is primarily intended for system administrators who are responsible for maintaining servers and clients on a network, as well as operators who monitor daily backups and storage devices.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
03	November 25, 2013	• Updated a dashboard label in "Avamar Administrator dashboard" on page 42. • Added cross-references to *EMC® Avamar® Metadata Capacity Reporting and Monitoring Release 7.0 Technical Note* in "Capacity panel" on page 46, "Dashboard capacity panel" on page 359, and "Architecture overview" on page 575. • Revised "Adding a user to a client or domain" on page 90 with new password length and complexity requirements.
02	August 31, 2013	Revised "Capacity panel" on page 46 to include information about Data Domain metadata usage.
01	July 10, 2013	Initial release of Avamar 7.0.

Related documentation

The following EMC publications provide additional information:

- *EMC Avamar Compatibility and Interoperability Matrix*
- *EMC Avamar Release Notes*
- *EMC Avamar Operational Best Practices*
- *EMC Avamar Product Security Guide*

- *EMC Avamar and Data Domain Integration Guide*
- All EMC Avamar client and plug-in user guides

Conventions used in this document

EMC uses the following conventions for special notices:

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to software or hardware operation.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: • System output, such as an error message or script • System code • Pathnames, filenames, prompts, and syntax • Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

The Avamar support page 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 EMC Customer Support.

To access the Avamar support page:

1. Go to https://support.EMC.com/products.
2. Type a product name in the **Find a Product** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to my products** in the top right corner of the **Support by Product** page.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. Review the following documents in addition to product administration and user guides:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

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

To search the EMC Knowledgebase:

1. Click the **Search** link at the top of the page.
2. Type either the solution number or keywords in the search box.
3. (Optional) Limit the search to specific products by typing a product name in the **Scope by product** box and then selecting the product from the list that appears.
4. Select **Knowledgebase** from the **Scope by resource** list.
5. (Optional) Specify advanced options by clicking **Advanced options** and specifying values in the available fields.
6. Click the search button.

Online communities

Visit EMC Community Network (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 EMC products.

Live chat

To engage EMC Customer Support by using live interactive chat, click Join Live Chat on the Service Center panel of the Avamar support page.

Service Requests

For in-depth help from EMC Customer Support, submit a service request by clicking Create Service Requests on the Service Center panel of the Avamar support page.

Note: To open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

To review an open service request, click the Service Center link on the Service Center panel, and then click View and manage service requests.

Facilitating support

EMC recommends that you enable ConnectEMC and Email Home on all Avamar systems:

- ConnectEMC automatically generates service requests for high priority events.
- Email Home emails configuration, capacity, and general system information to EMC Customer Support.

Your comments

Your suggestions help us to continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

BSGDocumentation@emc.com

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details that will help us address the documentation issue

CHAPTER 1
Introduction

The following topics introduce the EMC® Avamar® online data protection solution:

- EMC Avamar 26
- Important terms and concepts 26
- Functional overview 28

EMC Avamar

EMC Avamar solves the challenges associated with traditional backup, enabling fast, reliable backup and recovery for remote offices, data center LANs, and VMware® environments. Avamar backup and recovery software uses patented global data deduplication technology to identify redundant sub-file data segments at the source, reducing daily backup data by up to 500x—before it is transferred across the network and stored to disk. This enables companies to perform daily full backups even across congested networks and limited WAN links.

Key Avamar differentiators are:

- Deduplication of backup data at the source—before transfer across the network
- Enabling of fast, daily full backups across existing networks and infrastructure
- Reduction of required daily network bandwidth by up to 500x
- Up to 10x faster backups
- Encryption of data in flight and at rest
- Patented RAIN technology that provides fault tolerance across nodes and eliminates single points of failure
- Scalable grid architecture
- Reduction of total backup storage by up to 50x due to global data deduplication
- Daily verification of recoverability—no surprises
- Centralized web-based management
- Simple one-step recovery
- Flexible deployment options, including EMC Corporation Avamar Data Store package

Important terms and concepts

The following topics discuss important Avamar terms and concepts.

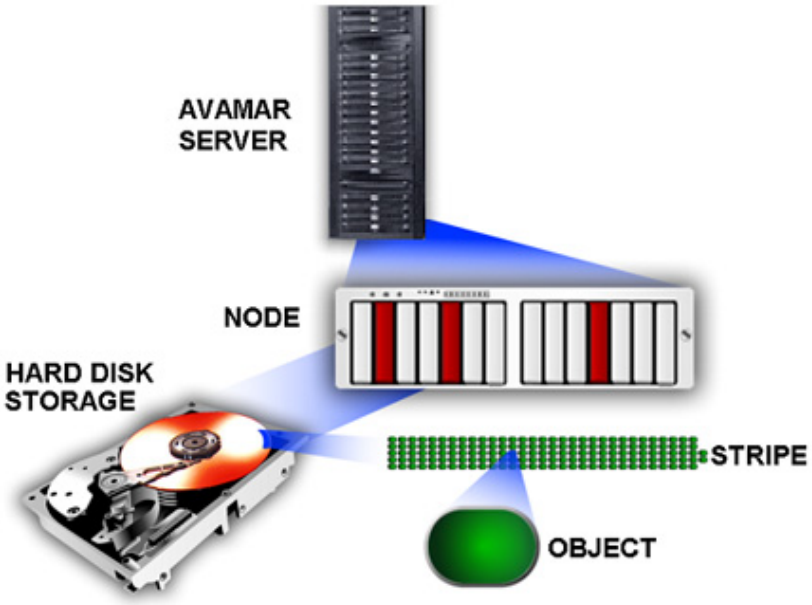
Avamar system

An Avamar system is a client/server network backup and restore solution that consists of one or more Avamar servers and the network servers or desktop clients that back up data to those servers. The Avamar system also provides centralized management through the Avamar Administrator graphical management console software application.

Avamar server

An Avamar server is a logical grouping of one or more nodes that is used to store and manage client backups.

Hardware manufacturers typically call their equipment servers (for instance, the Dell PowerEdge 2950 server). In the context of an Avamar system, this equipment is called a *node*.



Node

An Avamar node is a self-contained, rack-mountable, network-addressable computer that runs Avamar server software on the Linux operating system.

Hard disk storage

Avamar is a hard-disk based IP network backup and restore solution. Avamar servers manufactured by EMC use internal hard disk storage.

Stripes

A stripe is a unit of disk drive space managed by Avamar to ensure fault tolerance.

Object

In the Avamar system, an object is a single instance of deduplicated data. Each Avamar object inherently has a unique ID. Objects are stored and managed within stripes on the Avamar server.

Data deduplication

Data deduplication is a key feature of the Avamar system. Data deduplication ensures that each unique sub-file, variable length object is stored only once across sites and servers.

During backups, Avamar client software examines the client file system and applies a data deduplication algorithm that identifies redundant data sequences and breaks the client file system into sub-file, variable length data segments. Each data segment is assigned a unique ID. The client software then determines whether this unique ID has already been stored on the Avamar server. If this object resides on the Avamar server, a link to the stored object is referenced in the backup. Once an object has been stored on the server, it never has to be re-sent over the network, no matter how many times it is encountered on any number of clients. This feature significantly reduces network traffic and provides for greatly enhanced storage efficiency on the server.

Replication

Replication is a feature that enables efficient, encrypted, and asynchronous replication of data stored in an Avamar server to another Avamar server deployed in remote locations without the need to ship tapes. Replication is a scheduled process between two independent Avamar servers, providing a higher level of reliability for stored backups. Replication can be scheduled to run at off-peak hours to minimize bandwidth impact.

Functional overview

This topic provides detailed information about each part of the Avamar client/server system and describes how the parts interact with one another.

Avamar servers

All Avamar servers store client backups and also provide essential processes and services required for client access and remote system administration.

Avamar servers are available in either single-node or scalable multi-node configurations. For the most part, when using Avamar Administrator management console software, all Avamar servers look and behave the same. The main differences among Avamar server configurations are the number of nodes and disk drives reported in the server monitor.

Documenting specific differences in Avamar server hardware configurations is beyond the scope of this guide. Whenever specific limitations and best practices for certain configurations are known, they are noted. However, these occasional notes should not be considered definitive or exhaustive. Consult your EMC sales representative or an EMC reseller for additional information about specific hardware.

Nodes

The primary building block in any Avamar server is a node. Each node is a self-contained, rack-mountable, network-addressable computer that runs Avamar server software on the Linux operating system. Nodes can also contain internal storage in the form of hard disk drives. If the node is configured with internal storage (that is, a single-node server), it is internally mirrored to provide robust fault tolerance.

There are three types of nodes:

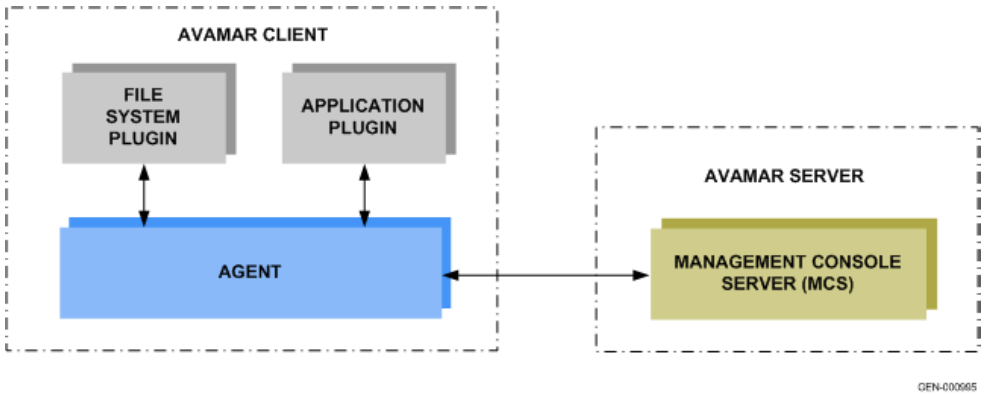
- **Utility node**—A utility node is dedicated to scheduling and managing background Avamar server jobs. In scalable multi-node Avamar servers, a single utility node provides essential internal services for the server (Management Console Server [MCS], cronjob, External authentication, Network Time Protocol [NTP], and Web access). Because utility nodes are dedicated to running these essential services, they cannot be used to store backups.
- **Storage nodes**—Storage nodes are nodes that store backup data. Multiple storage nodes are configured with multi-node Avamar servers based upon performance and capacity requirements. Storage nodes can be added to an Avamar server over time to expand performance with no downtime required. Avamar clients connect directly with Avamar storage nodes; client connections and data are load balanced across storage nodes.
- **NDMP Accelerator—**An NDMP Accelerator node is a specialized node that uses NDMP to provide data protection for certain NAS devices, including the EMC Celerra® IP storage systems and Network Appliance filers.

Single-node servers

Single-node Avamar servers combine all of the features and functions of utility and storage nodes on a single node.

Avamar clients

Avamar provides client software for various computing platforms. Each client comprises a client agent and one or more plug-ins.



Agents

Avamar agents are platform-specific software processes that run on the client and communicate with the Management Console Server (MCS) and any plug-ins installed on that client.

Plug-ins

The following topics provide details on the two types of Avamar plug-ins.

File system plug-ins

File system plug-ins are used to browse, back up, and restore files or directories on a specific client file system. Avamar currently provides plug-ins for the following operating systems:

- Free BSD
- HP-UX
- IBM AIX
- Linux
- Mac OS X
- Microsoft Windows
- Microsoft Windows Volume Shadow Copy Service (VSS)
- SCO OpenServer
- SCO UnixWare
- Oracle Solaris
- Novell NetWare
- VMware

Application plug-ins

Application plug-ins support backup and restore of databases or other special applications. Avamar currently provides plug-ins for the following applications:

- IBM DB2
- Lotus Domino
- Microsoft Exchange
- Microsoft Hyper-V
- Microsoft Office SharePoint Server (MOSS)
- Microsoft SQL Server
- NDMP for NAS devices, including EMC Celerra IP storage systems and Network Appliance filers
- Oracle
- SAP with Oracle
- Sybase ASE

Avamar Administrator

Avamar Administrator is a graphical management console software application that is used to remotely administer an Avamar system from a supported Windows client computer.

Encryption

Avamar can encrypt all data sent between clients and the server “in flight.” To provide enhanced security during client/server data transfers, Avamar supports two levels of “in-flight” encryption: medium and high. You can set the encryption level on a client-by-client basis in client properties, or for an entire group of clients in group properties. You also can disable “in-flight” encryption entirely.

Each individual Avamar server can also be configured to encrypt data stored on the server “at rest.” The decision to encrypt all data stored in an Avamar server is typically a one-time decision that is made when the server is initially deployed at a customer site.

Avamar, IPv4, and IPv6

Internet Protocol (IP) is a set of communication rules for routing traffic across networks to addressable devices like Avamar system components. Beginning with Avamar release 7.0, an Avamar system supports both Internet Protocol Version 4 (IPv4) and IPv6 address notation.

IPv4 notation

IPv4 notation is displayed as four octets, that is 1- to 3-digit base 10 numbers in a range of 0 to 255. Each octet is separated by periods and represents 8 bits of data for a total address space of 32 bits.

A subnet mask identifies a range (a subnet) of IP addresses on the same network. For Avamar purposes, the subnet mask is /24, representative of a 255.255.255.0 netmask.

Example of an IPv4 address and subnet mask: 10.99.99.99/24

IPv4 notation cannot be abbreviated. If an octet has zero (0) value, it is indicated by a 0.

IPv6 notation

IPv6 notation is displayed as 16 octets, that is 2-digit hexadecimal (base 16) numbers in a range of 00 to FF. Octets are combined by pairs into eight groups separated by colons, each group representing 16 bits of data for a total address space of 128 bits.

For Avamar purposes, the subnet mask (called prefix in IPv6) is /64.

Example of an IPv6 address and prefix:
2001:0db8:85a3:0042:1000:8a2e:0370:7334/64

As for a group with zero (0) value, IPv6 notation is different from IPv4 in that it can be abbreviated. For example, the following is a valid IPv6 address and prefix:
2001:db8:abcd:0012::0/64.

Avamar IP configurations

In the Avamar user interface, an IP address may be displayed in either IPv4 or IPv6 notation. The type notation you see is dependent on how that particular component was initially configured when the hardware and software were installed.

IPv4 and IPv6 are not interoperable. They operate in separate stacks (that is, parallel, independent networks).

Avamar can be set up in a dual stack configuration. In that case, each Avamar component may have an IPv4 address, an IPv6 address, or both (one primary and the other secondary). The Avamar user interface may display a component's primary address or both dual stack addresses. So if you see the following IP address for a particular device, it is configured as dual stack: 10.99.99.99/24,2001:db8:abcd:0012::0/64.

CHAPTER 2
Avamar Administrator

The following topics provide details on Avamar Administrator, the graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or client computer:

- Installing Avamar Administrator 34
- Upgrading Avamar Administrator 36
- Uninstalling Avamar Administrator 37
- Session time-out 37
- Starting Avamar Administrator 39
- Avamar Administrator dashboard 42
- Exploring the Avamar Administrator user interface 50

Installing Avamar Administrator

You can install Avamar Administrator on supported Microsoft Windows and 64-bit Linux platforms.

Updated, detailed client compatibility information is available in the *Avamar Compatibility and Interoperability Matrix* on EMC Online Support at https://support.EMC.com.

Installing on Microsoft Windows

To install Avamar Administrator on a computer running a supported version of Microsoft Windows:

1. On the computer where the software will be installed, open a web browser and type the following URL:

   http://AVAMARSERVER

   where AVAMARSERVER is the Avamar server network hostname or IP address.

   The EMC Avamar Web Restore web page appears.

2. Click **Downloads**.
3. Click **+** next to the **Windows for x86 (32 bit)** folder.
4. Click **+** next to the **Microsoft Windows XP, Vista, 7, 8, Microsoft Windows Server 2003** folder.
5. Locate the Java Runtime Environment (JRE) install package (it is typically the last entry in the folder).
6. If the JRE on the client computer is older than the JRE hosted on the Avamar server, download and install the newer JRE from the Avamar server as follows:
   a. Click the **jre-**VERSION**-windows-i586-p** install package.

      where VERSION is the JRE version.

   b. Open the installation file, or download the file, and then open it from the saved location.
   c. Follow the onscreen instructions to complete the JRE installation.
7. Click the **AvamarConsoleMultiple-windows-x86-**VERSION**.exe** install package.

   where VERSION is the Avamar Administrator software version.

   Avamar Administrator is only available as a 32-bit application. However, it will also run on 64-bit windows computers.
8. Open the installation file, or download the installation file, and then open it from the saved location.
9. Follow the onscreen instructions to complete the Avamar Administrator software installation.

Installing on Linux

To install Avamar Administrator on a computer running a supported version of Linux, download the install packages from the Avamar server, and then install the RPMs.

1. On the computer where the software will be installed, open a web browser and type the following URL:

   http://AVAMARSERVER

   where AVAMARSERVER is the Avamar server network hostname or IP address.

   The EMC Avamar Web Restore web page appears.

2. Click **Downloads**.
3. Click **+** next to the **Linux for x86 (64 bit)** folder.
4. Click **+** next to the **Red Hat Enterprise Linux 4** folder.
5. Locate the JRE RPM install package (it is typically the last entry in the folder).
6. If the JRE on the client computer is older than the JRE hosted on the Avamar server, download the **jre-**VER-PLAT**.rpm** install package to a temporary install folder such as /tmp.

   where VER is the JRE version, and PLAT is the computing platform.

7. Download the **AvamarConsole-linux-rhel4-x86_64-**VERSION**.rpm** install package to a temporary install folder such as /tmp.

   where VERSION is the Avamar Administrator software version.

   Use the Red Hat Enterprise Linux 4 install packages for all supported Linux versions.

8. Open a command shell and log in as root on the computer where the software will be installed.
9. Change directory to the temporary install folder used in steps 6 and 7. For example:

   cd /tmp

10. If you downloaded a JRE, install it by typing:

    rpm -ivh jre-VER-PLAT**.rpm**

11. Follow the onscreen instructions to complete the JRE installation.
12. Install Avamar Administrator by typing:

    rpm -ih AvamarConsole-linux-rhel4-x86_64-VERSION**.rpm**

    The following appears in the command shell:

    ```
    Please run /usr/local/avamar/VERSION/bin/avsetup_mcc to configure MC
    Client
    ```

13. Configure Avamar Administrator by typing:

    /usr/local/avamar/VERSION**/bin/avsetup_mcc**

    The following appears in the command shell:

    ```
    Enter the location of your JRE 1.6 installation
    [/usr/java/jre1.6u12]:
    ```

14. Press **Enter** to accept the default install location.

    The following appears in the command shell:

    ```
    Enter the root directory of your EMC installation
    [/usr/local/avamar/VERSION]:
    ```

15. Press **Enter** to accept the default install location.

    The following appears in the command shell:

    ```
    Avamar Administrator VERSION has been configured correctly. Type
    mcgui command to use it.
    ```

Upgrading Avamar Administrator

The following topics explain how to upgrade Avamar Administrator either on Microsoft Windows or on Linux.

Upgrading on Microsoft Windows

You can install multiple versions of Avamar Administrator on the same Microsoft Windows computer.

If you install Avamar Administrator on a computer where it is already installed, select a destination folder carefully during the installation procedure:

- To keep an older version, select a different installation folder.
- To directly upgrade the Avamar Administrator installation, select the same installation folder. The two versions are identified by their full version numbers.

Upgrading on Linux

To upgrade the Avamar Administrator software on the Linux platform, uninstall the previous version as described in "Uninstalling on Linux" on page 37, and install the new software as described in "Installing on Linux" on page 35. Use of the Linux software upgrade command (**rpm -Uh**) is not supported.

Uninstalling Avamar Administrator

The following topics explain how to uninstall Avamar Administrator on either Microsoft Windows or on Linux.

Uninstalling on Microsoft Windows

To uninstall Avamar Administrator on Microsoft Windows:

1. Select **Start** › **Programs** › **EMC Avamar** › **Administrator** › **VERSION** › **Uninstall** Avamar Administrator, where VERSION is the version to uninstall.
2. Click **OK** on the confirmation message.

Uninstalling on Linux

To uninstall Avamar Administrator on Linux:

1. Close Avamar Administrator.

   NOTICE

   You must close all open Avamar Administrator sessions before you can uninstall Avamar Administrator. Otherwise, the uninstall does not complete. An incomplete uninstall complicates future Avamar Administrator upgrades.

2. Open a command shell and log in as root on the computer that is currently running Avamar Administrator.
3. Type:

   ```
   rpm -qa | grep Av
   ```

   The following appears in the command shell:

   ```
   AvamarConsole-VERSION
   ```

4. Note the package name.
5. Type:

   ```
   rpm -e AvamarConsole-VERSION
   ```

   where AvamarConsole-VERSION is the Avamar software install package.

Session time-out

By default, an Avamar Administrator session remains active until a user closes the application by choosing **Exit** from the menu. To protect the assets available through Avamar Administrator, set a session time-out value. The value applies to all Avamar Administrator sessions connected to the Avamar server.

After you set a session time-out value, Avamar Administrator monitors the UI for activity. When Avamar Administrator detects no activity for the number of minutes set in the time-out value, it shuts down all processes, closes all windows, and displays the **Inactive** dialog box.

Avamar Administrator treats the following as activity:

- Mouse activity within the UI
- Keyboard activity within the UI

Setting a session time-out value

To set a session time-out value:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the Management Console Server (mcs) service by typing:

   ```
   dpnctl stop mcs
   ```

3. Change the working directory by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Open mcserver.xml in a plain text editor.
5. Find the mon node, and the entry with the consoleInactiveMinutesToReport key, as shown here:

   ```
   <node name="mon">
      <map>
         …
         <entry key="consoleInactiveMinutesToReport" value="-1" />
         …
      </map>
   </node>
   ```

   As indicated by the ellipsis (…), the mon node has many entries. Only the relevant entry appears here.
6. Change the value of the entry, as shown here:

   ```
   <node name="mon">
      <map>
         …
         <entry key="consoleInactiveMinutesToReport" value="n" />
         …
      </map>
   </node>
   ```

   where *n* is the session time-out value, in minutes.

7. Save the change and close the editor.
8. Restart mcs by typing:

   ```
   dpnctl start mcs
   ```

9. Close the command shell.

Avamar Administrator uses the new session time-out value the next time it connects with the Avamar server.

Starting Avamar Administrator

The following steps explain how to start Avamar Administrator when it is installed on the local computer. You also can launch Avamar Administrator from an Avamar Enterprise Manager session, as discussed in "Launching Avamar Administrator from Avamar Enterprise Manager" on page 353.

NOTICE

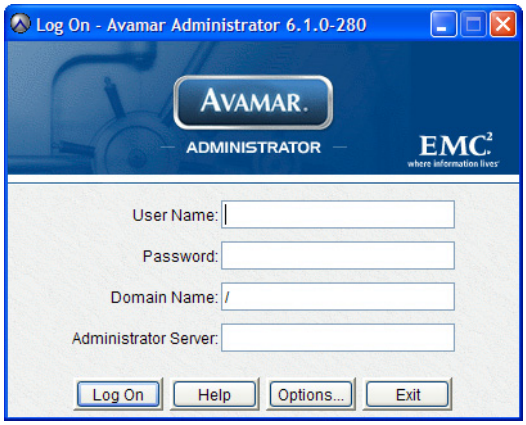
Avamar Administrator requires a minimum of 512 MB free system RAM in order to start. Otherwise, you might experience Java heap errors.

To start Avamar Administrator:

1. Launch Avamar Administrator:
   - On Microsoft Windows platforms, double-click the Avamar Administrator icon on the Windows desktop.
   - On Linux platforms, open a command shell and type:

     ```
     mcgui
     ```

   The login window appears.



2. In the **User Name** field, type a username.

   To access all Avamar Administrator features and functions, the account associated with this username must be assigned the role of Administrator. Other roles provide reduced functionality. "Roles" on page 78 provides details.

   - To authenticate using the internal authentication system, type only a username.
   - To authenticate using the enterprise authentication system (deprecated) or directory service authentication, type the username, the @ symbol, and the name of the external authentication server in the form:

     ```
     USER@EXT-AUTH-SERVER
     ```

     where USER is the username and EXT-AUTH-SERVER is the fully qualified domain name of the authentication server.

     For backward compatibility with Enterprise Authentication, an authentication attempt with a username formatted as "USER@EXT-AUTH-SERVER" is first checked through Enterprise Authentication. If authentication succeeds with that method, directory service authentication is not checked. If it fails, directory service authentication is checked. Directory service authentication is described in "Enabling directory service authentication" on page 84.

     The directory service authentication method uses a time-out value. By default, this is 60 seconds. To configure a different time-out value refer to "Changing the time-out value" on page 417.

3. In the **Password** field, type the password for the user account.
4. In the **Domain Name** field, type the Avamar administrative domain to log in to.
   - To log in to the root domain, use the default entry of a single slash (/) character.
   - To log in to a specific domain or subdomain, use the following syntax:

     ```
     /domain/subdomain1/subdomain2
     ```

     "Domains" on page 56 provides details.

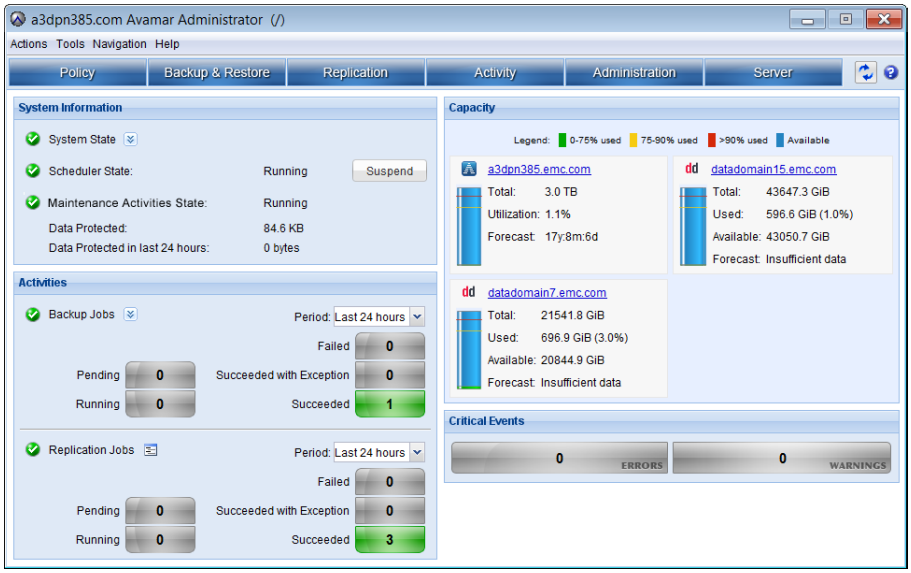
5. In the **Avamar Server** field, type the Avamar Administrator server name to log in to, as defined in the corporate Domain Name Server (DNS).

   NOTICE

   If you consistently log in to the same Avamar server or domain, click **Options** and type that server name and domain in the **Default Administrator Server** and **Default Domain** fields, respectively. The next time that you start Avamar Administrator, the **Administrator Server** and **Domain Name** fields on the login window are prepopulated with this information.

6. Click **Log On**.

   The Administrator dashboard appears.



"Avamar Administrator dashboard" on page 42 provides details for various dashboard features and functions.

NOTICE

Full dashboard functionality is only available to users assigned the role of Administrator. Other roles provide reduced functionality. "Understanding users, authentication, and roles" on page 76 provides details.

Avamar Administrator dashboard

After logging in, the Avamar Administrator dashboard appears:

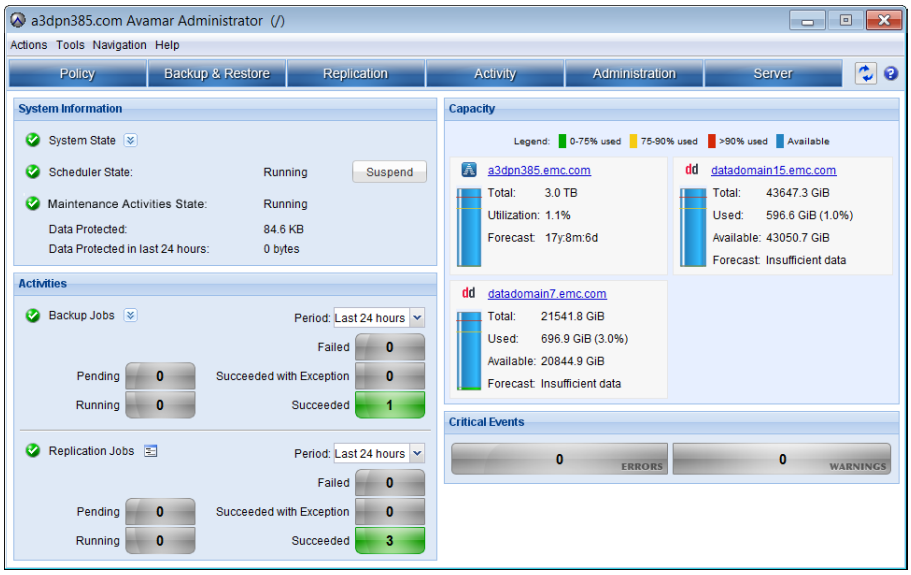


Figure 1 Avamar Administrator dashboard

Launcher buttons

Each of the dashboard launcher buttons invokes a different persistent window to perform specific tasks.

Table 2 Dashboard launcher buttons

Button	Description
Policy	Clicking **Policy** displays the Policy window, which is used to create and manage groups, datasets, schedules, and retention policies. Chapter 6, "Groups and Group Policies," provides details.
Backup & Restore	Clicking **Backup & Restore** displays the Backup, Restore and Manage window, which is used to perform on-demand backups, restores, and to manage backups. Chapter 4, "Backup, Restore, and Backup Management," provides details.
Administration	Clicking **Administration** displays the Administration window, which is used to create and manage domains, clients, users, system events, and services. Chapter 3, "Domains, Clients, and Users," and Chapter 16, "Advanced Server Administration and Maintenance," provide details.
Activity	Clicking **Activity** displays the Activity window, which is used to monitor backup, restore, backup validation, and replication activity. "Monitoring backup, restore, or validation activities" on page 116 provides details.
Server	Clicking **Server** displays the Server window, which is used to monitor server activity and client sessions. Chapter 16, "Advanced Server Administration and Maintenance," provides details.
Replication	Clicking **Replication** displays the Replication window, which provides policy-based replication features. Chapter 15, "Replication," provides details.

System Information panel

The System Information panel provides a quick “at-a-glance” view of important system statistics.

System State

The System State status icons aggregate the detailed system information as follows:

The system is fully operational.

There is an issue with the system that requires attention. However, backups can continue.

There is a problem with the system that requires immediate attention. Backups cannot occur until the problem is resolved.

Clicking shows detailed system state information.

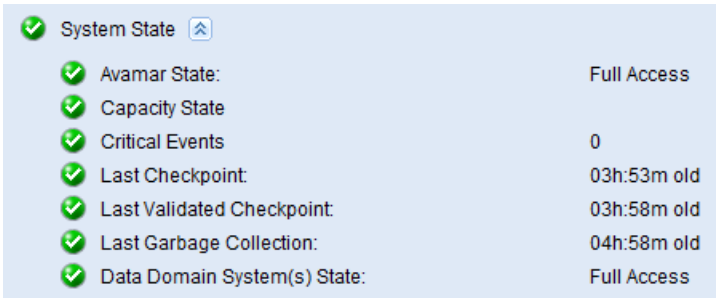


Figure 2 Dashboard System State details

The following table provides details about system state information in the dashboard.

Table 3 Dashboard detailed system state information (page 1 of 2)

Property	Description
Avamar State	Summary of Avamar server operational state. Icons communicate the following: The Avamar server is fully operational. There are one or more issues with the Avamar server that require attention. However, backups can continue. The Avamar server is one of the following operational states: – Inactive – Offline – Degraded – Unknown The current operational state of the Avamar server is also shown. “Runlevel” on page 282 provides details.
Capacity State	Summary of system capacity usage and health. Icons communicate the following: System has used ‹ 75% of total storage capacity. System has used › 75% but ‹ 90% of total storage capacity. Consider adding capacity or deleting old backups. System has used more than 90% of total storage capacity. No new backups are performed until you add capacity or delete old backups. “Capacity Management” on page 357 provides details.

Table 3 Dashboard detailed system state information (page 2 of 2)

Property	Description
Critical Events	Summary of unacknowledged system events. Icons communicate the following:  There are no critical system events which require acknowledgment.  One or more warnings events require acknowledgment.  One or more system error events require acknowledgment. "Acknowledging system events" on page 311 provides details.
Last Checkpoint	Elapsed time since last checkpoint was taken. Icons communicate the following:  Checkpoint successfully completed on this Avamar server within the past 24 hours.  › 24 hours but ‹ 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.  › 48 hours have elapsed since a checkpoint successfully completed on this Avamar server. "Checkpoints" on page 404 provides details.
Last Validated Checkpoint	Elapsed time since a checkpoint was last validated. Icons communicate the following:  Checkpoint validation successfully completed on this Avamar server within the past 48 hours.  › 48 hours but ‹ 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server.  › 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server. "Validating a checkpoint" on page 405 provides details.
Last Garbage Collection	Elapsed time since last garbage collection. Icons communicate the following:  Garbage collection successfully completed on this Avamar server within the past 30 hours.  Garbage collection has not successfully completed on this Avamar server within the past 30 hours.  Garbage collection encountered an error the last time it was run.
Data Domain System(s) State	Summarized operational state for all Data Domain systems which have been added to this Avamar server. Icons communicate the following:  All Data Domain systems are fully operational.  There one or more issues with Data Domain systems that require attention. However, backups can continue.  There one or more problems with Data Domain systems that requires immediate attention. Backups cannot occur until all problems are resolved. The summarized operational state of the Data Domain systems is also shown. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details.

Scheduler State

The Scheduler State communicates the following:

Table 4 Scheduler status

Icon	Message	Description
	Running	Scheduled activities, such as backups, email notifications, and replications, will occur at the scheduled time.
	Suspended	Scheduled activities, such as backups, email notifications, and replications, are suspended and will not resume until the scheduler is resumed.

Clicking **Suspend** suspends activities; clicking **Resume** resumes activities. "Suspending and resuming backups and restores" on page 312 provides details.

Maintenance Activities State

The Maintenance Activities State communicates the following:

Table 5 Maintenance activities status

Icon	Message	Description
	Running	Maintenance activities, such as checkpoints, checkpoint validation and garbage collection, will occur at the scheduled time.
	Suspended	Scheduled activities, such as checkpoints, checkpoint validation and garbage collection, are suspended and will not resume until maintenance activities are resumed. "Suspending and resuming maintenance activities" on page 314 provides details.

License Expiration

The calendar date on which this server's license expires.

If this server's license is perpetual (that is, it never expires), then license expiration is not shown.

Data Protected

The following data protection statistics are shown:

- Data Protected—The total amount of client data protected (in bytes).
- Data Protected in last 24 hours—The total amount of client data protected (in bytes) during the past 24 hours.

Capacity panel

The Capacity panel provides system capacity usage and forecasting information for the Avamar server and any Data Domain systems that have been added.

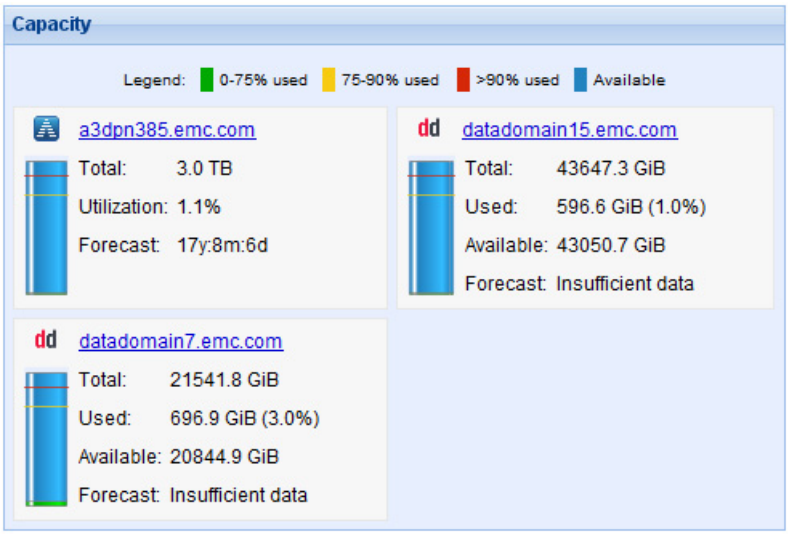


Figure 3 Dashboard Capacity panel

- Clicking an Avamar server name shows the Server Monitor, which can be used to view additional detailed system information. "Monitoring the server" on page 274 provides details.
- Clicking a Data Domain system name shows the Data Domain Enterprise Manager web page for that system.
- Each system component's capacity usage is shown as a vertical bar:
  - Available storage capacity is shown in blue.
  - 0-75% of total storage capacity utilization is shown in green to indicate safe capacity utilization.
  - 75-90% of total storage capacity utilization is shown in yellow to indicate that capacity utilization should be studied to determine if additional storage capacity should be added.
  - Greater than 90% is shown in red to indicate that storage capacity has reached the practical maximum limit.
- Each system component's total capacity is shown:
  - The unit of measure for Avamar server capacity is terabytes (TB).
  - The unit of measure for Data Domain systems is gibibytes (GiB).
- Each system component's current capacity usage is shown as a percentage of the total capacity for that component. Data Domain systems also show the amount of storage consumed in gibibytes (GiB).
- If the system has sufficient historical data, a capacity forecast is also shown as the expected period that each system component can consume storage at the current rate.

- If the Avamar system configuration includes a Data Domain system, then Avamar server capacity calculations include metadata usage for the Data Domain system. Clicking the Avamar server name displays a detailed capacity view of both Avamar server and Data Domain metadata utilization.

  The *EMC Avamar Metadata Capacity Reporting and Monitoring Release 7.0 Technical Note* provides more information about metadata capacity for backups stored on Data Domain systems. This technical note is available from EMC online support (https://support.emc.com).

"Capacity Management" on page 357 provides details about managing system storage capacity.

Activities panel

The Activities panel provides status and detailed information for backup and replication jobs.

Backup Jobs

The Backup Jobs status icons aggregate the detailed backup jobs status as follows:

Scheduled backups will occur at the scheduled time.

There is a problem with the system that requires immediate attention. Scheduled backups will not occur until the problem is resolved.

Clicking displays detailed backup jobs status information:

Figure 4 Dashboard Backup Jobs details

The following table provides details on the status information available for backup jobs in the dashboard.

Table 6 Dashboard detailed backup jobs status information (page 1 of 2)

Property	Description
Scheduler State	Summary of the scheduler state. Icons communicate the following: Running—Scheduled activities, such as backups, email notifications, and replications, will occur at the scheduled time. Suspended—Scheduled backups are suspended and will not resume until the scheduler is resumed.
Dispatcher State	Summary of dispatcher state. Icons communicate the following: Running—Scheduled backups will occur at the scheduled time. Suspended—The Avamar server has reached the health check limit. No future backups will occur until this is resolved. "Capacity limits and thresholds" on page 358 provides details.

Table 6 Dashboard detailed backup jobs status information (page 2 of 2)

Property	Description
Backup Groups Enabled	Summary of backup groups state. Icons communicate the following: At least one backup group is enabled. All backup groups are disabled. Clicking displays the Policy window Groups tab, which can be used to create new backup groups, or edit existing backup group properties. "Groups and Group Policies" on page 155 provides details.

The dashboard shows the number of currently running and pending backup jobs.

The dashboard also shows the number of past backup jobs that:

- Succeeded—These backup jobs successfully completed.
- Succeeded with exception—These backup jobs completed with errors.
- All Failures—These backup jobs failed because the client failed to perform backup.

The default time period for which to show past results is 24 hours. Other available time periods are 48 hours, Last week or Last 2 weeks.

Clicking any numeric button shows the Activity Monitor, which can be used to view detailed information for any backup job. "Monitoring backup, restore, or validation activities" on page 116 provides details.

Replication Jobs

The Replication Jobs status icons communicate the following:

Scheduled replication jobs will occur at the scheduled time.

One or more replication groups are disabled.

Scheduled replication jobs will not occur. This might be due to the scheduler being in a suspended state, all replication groups being disabled, or some other issue with the system.

Clicking shows the Replication window Groups tab, which can be used to create new replication groups, or edit existing replication group properties. "Managing replication with Avamar Administrator" on page 373 provides details.

The dashboard shows the number of currently running and pending replication jobs.

The dashboard also shows the number of past replication jobs that:

- Succeeded—These replication jobs successfully completed.
- Succeeded with exception—These replication jobs completed with errors.
- All Failures—These replication jobs failed.

The default time period for which to show past results is 24 hours. Other available time periods are 48 hours, Last week or Last 2 weeks.

Clicking any numeric button shows the Replication Report, which can be used to view detailed information for any replication job. "Viewing the Replication Report" on page 250 provides details.

Critical Events panel

The Critical Events panel shows the number of unacknowledged serious system errors and warnings that have occurred, as well as certain defined system alerts.

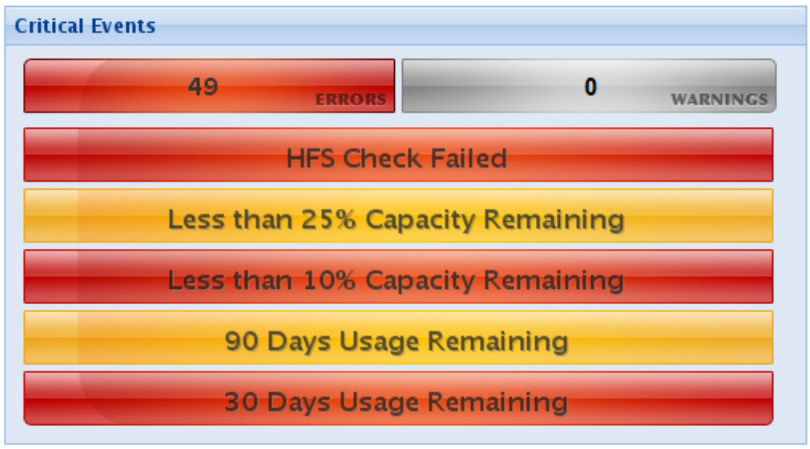


Figure 5 Dashboard Critical Events panel.

In order to clear these serious system errors and warnings (that is, reset the count to zero), you must explicitly acknowledge them. "Acknowledging system events" on page 311 provides details.

The following table describes each kind of error, warning, or alert.

Table 7 Dashboard Critical Events panel.

Error, Warning, or Alert	Description
Errors	Total number of hardware or nonhardware errors that require acknowledgement. Errors are more serious than warnings and should be immediately investigated.
Warnings	Total number of hardware or nonhardware warnings that require acknowledgement. Warnings are less serious than errors.
HFS Check Failed	The last checkpoint validation failed. This condition generated a data integrity alert, which should be investigated and addressed as soon as possible. "Validating a checkpoint" on page 405 and "Clearing data integrity alerts" on page 407 provide details.
Less Than 25% Capacity Remaining Less Than 10% Capacity Remaining	These alerts warn that the system is approaching critical system storage capacity usage thresholds. "Capacity Management" on page 357 provides details about managing system storage capacity.

Table 7 Dashboard Critical Events panel.

Error, Warning, or Alert	Description
90 Days Usage Remaining 30 Days Usage Remaining	These alerts warn that the system is approaching critical system storage capacity forecasting thresholds. "Capacity forecasting" on page 361 provides details about system storage capacity forecasting.

Exploring the Avamar Administrator user interface

The following topics explain the Avamar Administrator user interface.

Status bar

The status bar at the bottom of each Avamar Administrator persistent window conveys status information and provides a single-click shortcut to specific features and functions.

Launcher shortcuts

The icons on the left side of the status bar provide shortcuts to the six main Avamar Administrator windows. The following table provides details on the icons.

Table 8 Status bar icons

Icon	Window	Window description
	Policy	The Policy window is used to create and manage groups, datasets, schedules, and retention policies. Chapter 6, "Groups and Group Policies," provides details.
	Backup & Restore	The Backup, Restore and Manage window is used to perform on-demand backups, restores, and to manage backups. Chapter 4, "Backup, Restore, and Backup Management," provides details.
	Administration	The Administration window is used to create and manage domains, clients, users, system events, and services. Chapter 3, "Domains, Clients, and Users," and Chapter 16, "Advanced Server Administration and Maintenance," provide details.
	Activity	The Activity window is used to monitor backup, restore, backup validation, and replication activity. "Monitoring backup, restore, or validation activities" on page 116 provides details.
	Server	The Server window is used to monitor server activity and client sessions. Chapter 16, "Advanced Server Administration and Maintenance," provides details.
	Replication	The Replication window provides policy-based replication features. Chapter 15, "Replication," provides details.

Status messages

The right side of the status bar shows various status messages.

Scheduler and backup dispatching status

The scheduler controls whether scheduled backups occur. The backup dispatching status indicates whether backups can occur based on whether the health check limit has been reached. The following table lists the available status messages.

Table 9 Scheduler and backup dispatching status messages

Status message	Description
Sch/Disp: Running/Running	Backups will occur at the scheduled time. Scheduled backups are enabled, and the health check limit has not been reached.
Sch/Disp: Running/Suspended	Even though scheduled backups are enabled, backups will not occur at the scheduled time because the health check limit has been reached. Resolve the system capacity issues and acknowledge the system event to resume backups. Chapter 14, "Capacity Management," and "Acknowledging system events" on page 311 provide details.
Sch/Disp: Suspended/Running	Even though the health check limit has not been reached, backups will not occur at the scheduled time because scheduled backups are disabled. Backups can resume when you resume scheduled operations.
Sch/Disp: Suspended/Suspended	Backups will not occur at the scheduled time because scheduled backups are disabled and the health check limit has been reached. "Suspending and resuming scheduled operations" on page 313 provides details on reenabling the scheduler. Chapter 14, "Capacity Management," and "Acknowledging system events" on page 311 provide details on resolving the system capacity issues and acknowledging system events in order to resume scheduled backups.

Unacknowledged events

Certain system events to require acknowledgement by an Avamar server administrator each time they occur. The following table lists the available status messages.

Table 10 Status messages for unacknowledged events

Status message	Description
Have Unacknowledged Events	There are entries in the unacknowledged events list that must be explicitly acknowledged by an Avamar server administrator. Click the Unacknowledged Events status icon or text label to show the Administration window Unacknowledged Events pane (tab). "Acknowledging system events" on page 311 provides details.
No Unacknowledged Events	There are no entries in the unacknowledged events list.

Avamar server and Data Domain system status

This icon lists the operational status of either the Avamar server or any configured Data Domain systems. The following table lists the available status messages.

Table 11 Operational status messages for Avamar or Data Domain

Status message	Description
Server: Full Access	Normal operational state for an Avamar server. All operations are allowed.
Server: Admin	The Avamar server is in an administrative state in which the Avamar server and root user can read and write data; other users are only allowed to read data.
Server: Admin Only	The Avamar server is in an administrative state in which the Avamar server or root user can read or write data; other users are not allowed access.
Server: Admin Read Only	The Avamar server is in an administrative read-only state in which the Avamar server or root user can read data; other users are not allowed access.
Server: Degraded	The Avamar server has experienced a disk failure on one or more nodes. All operations are allowed, but immediate action should be taken to fix the problem.
Server: Inactive	Avamar Administrator was unable to communicate with the Avamar server.
Server: Node Offline	One or more Avamar server nodes are in an OFFLINE state.
Server: Read Only	The Avamar server is in a read-only administrative state in which all users can read data, but writing data is not allowed.
Server: Suspended	Avamar Administrator was able to communicate with the Avamar server, but normal operations have been temporarily suspended.
Server: Synchronizing	The Avamar server is in a transitional state. It is normal for the server to be in this state during startup and for short periods of time during maintenance operations.
Server: Unknown State	Avamar Administrator could not determine the Avamar server state.
Data Domain System Unresponsive	Avamar can connect to a Data Domain system, but there is a problem with the connection.
DD System: Inactive	Avamar cannot connect to a Data Domain system.

To suspend or resume Avamar server activities, click the **Server status** icon or text label to display the **Avamar Server** window **Session Monitor** tab. From there, select **Actions** › **Resume Backups/Restores** or **Actions** › **Suspend Backups/Restores** to resume or suspend server activities, respectively. "Suspending and resuming backups and restores" on page 312 provides details.

To view additional details about Data Domain system status, open the **Server window** by clicking **Navigation** › **Server**. Select the **Server Management** tab, and then select the Data Domain system in the tree. The Monitoring Status of the Data Domain system appears in the right pane. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details on the available detailed status messages.

Navigation tree features

The navigation trees in the Administration, Backup, Restore and Manage, and Replication windows provide several controls used to easily locate one or more clients:

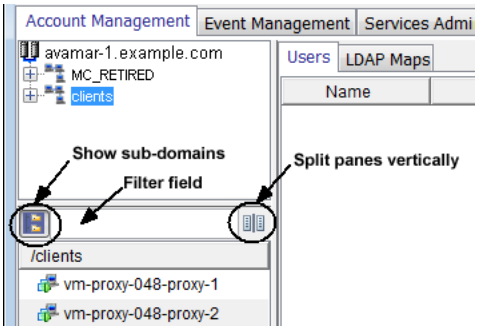


Figure 6 Split-pane navigation tree features

- The upper pane shows the Avamar server domain structure.
- The lower pane shows contents of any domain selected in the upper pane.
- Clicking the icon shows all clients in subfolders.
- Typing one or more characters filter field only shows clients that contain those characters.
- Clicking the icon splits the two panes vertically.

Mouse shortcuts

The Avamar Administrator user interface supports context-sensitive left-click, right-click, and double-click shortcuts.

Right-click

All GUI elements that can enable features or functions when clicked, have right-click support added to them. However, if the GUI element only acts as a navigation mechanism, there is no right-click support. For example, the Policy window client tree has a right-click shortcut menu because specific features and functions become available based on which node of the tree is selected.

Double-click

For all tables where properties or edit dialog boxes can be invoked, double-click any row of the table to display the properties or edit dialog box. Additionally, when lists are used rather than tables, double-click an element in the list to display the edit dialog box.

Sort column headings

Click a table column heading to sort that display by values in that column. For example, double-click the Activity Monitor State column to sort the Activity Monitor display by the state of each backup.

Press Shift and then click any table column heading to reverse sort the values in a table column.

CHAPTER 3
Domains, Clients, and Users

The following topics discuss how to administer Avamar domains, clients, and user accounts:

- Domains 56
- Clients 60
- Understanding users, authentication, and roles 76
- Enabling user authentication 84
- Managing user accounts 90

Domains

The following topics provide details on Avamar domains:

- "Understanding Avamar domains and subdomains" on page 56
- "Creating a domain" on page 57
- "Editing domain information" on page 58
- "Deleting a domain" on page 59

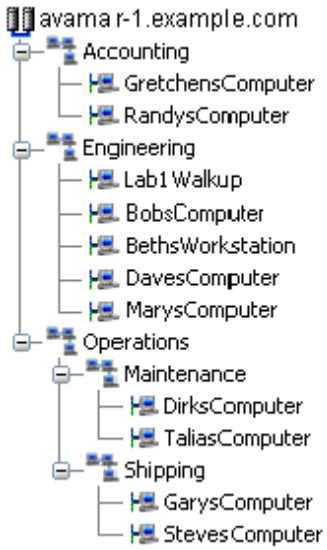
Understanding Avamar domains and subdomains

Avamar domains are distinct zones to organize and segregate clients in the Avamar server. This provides enhanced security by enabling you to define administrative user accounts on a domain-by-domain basis.

Avamar domains are completely internal to the Avamar server and have nothing to do with Internet domains.

Nested structure

You can nest domains to create a rich tree structure. Consider the following example Avamar domain.



The root domain, avamar-1.example.com, contains three departmental domains: Accounting, Engineering, and Operations. The Operations domain contains Maintenance and Shipping subdomains.

There is no functional difference between domains and subdomains. "Subdomain" is merely a term that refers to any domain nested within another higher level domain.

Hierarchical management

The real power of domains is that you can add administrators to a specific level on the client tree. These domain-level administrators can then manage the clients and policies within that domain.

For example, if you add an administrative user to the root domain, then that user can administer clients and policies anywhere in the system. However, if you add an administrative user to a domain, then that user can only administer clients and policies in that domain and its subdomains.

The procedures in this guide assume that you are logged in to the root domain. If you log in to a lower-level domain, you may not have access to specific clients, datasets, groups, and event management features outside that domain.

Special domains

You cannot delete the MC_RETIRED and REPLICATE domains.

The MC_RETIRED domain contains clients that have been retired, as discussed in "Retiring a client" on page 70. Its primary purpose is to facilitate restores from retired client backups.

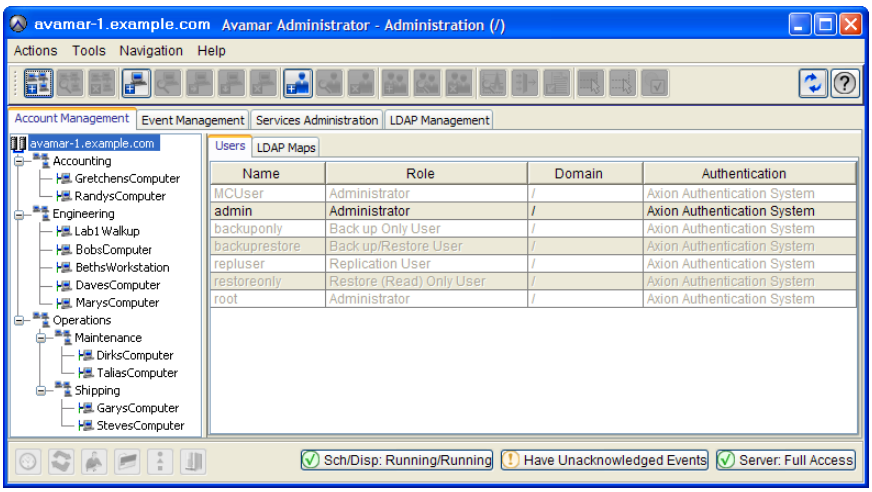
The REPLICATE domain contains replicated data from other servers, as discussed in Chapter 15, "Replication."

Creating a domain

To create an Avamar domain:

1. In Avamar Administrator, click the **Administration** launcher button.

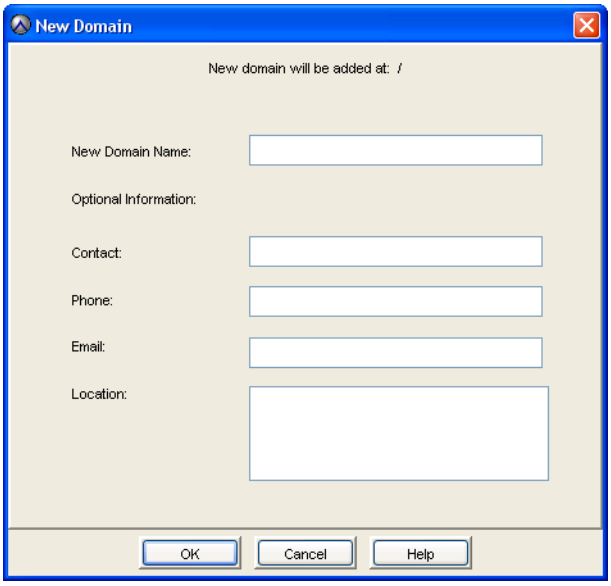
   The Administration window appears.



2. Click the **Account Management** tab.
3. In the left pane, select the location in the tree in which to create the domain.

4. From the **Actions** menu, select **Account Management** › **New Domain**.

   The New Domain dialog box appears.



5. In the **New Domain Name** field, type the name of the domain.

   Note: Domain names cannot exceed 63 characters. Also, do not use any of the following characters in the domain name: =~!@$^%(){}[]|,`;#\/:*?‹›'"&.

6. (Optional) In the **Contact** field, type the contact name.
7. (Optional) In the **Phone** field, type the contact telephone number.
8. (Optional) In the **Email** field, type the contact email address.
9. (Optional) In the **Location** field, type the contact location.
10. Click **OK**.

    A confirmation message appears.

11. Click **OK**.

Editing domain information

To edit contact and location information for a domain:

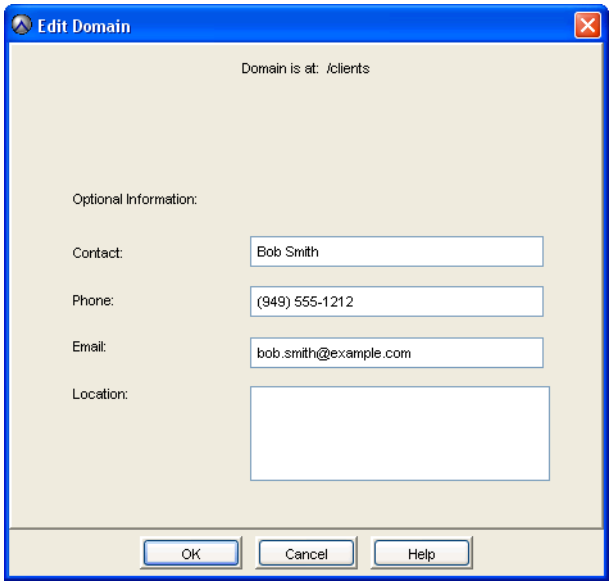
1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Account Management** tab.
3. In the tree, select the domain to edit.

4. From the **Actions** menu, select **Account Management** › **Edit Domain**.

   The Edit Domain dialog box appears.



5. Edit the domain contact information.
6. Click **OK**.
7. Click **OK** on the confirmation message that appears.

Deleting a domain

When you delete a domain, the process also deletes any clients in the domain. To preserve the clients in the system, move the clients to a new domain before you delete the domain.

In addition, if you use directory service authentication, then Avamar removes the LDAP maps that use that domain for access. The associated directory service groups are otherwise unaffected by the deletion.

To delete a domain:

1. (Optional) Move any clients in the domain to a new domain as discussed in "Moving a client to a new domain" on page 71.
2. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.
3. Click the **Account Management** tab.
4. In the tree, select the domain to delete.
5. From the **Actions** menu, select **Account Management** › **Delete Domain.**

   A confirmation message appears.
6. Click **Yes**.
7. Click **OK** on the second confirmation message that appears.

Clients

The following topics provide details on managing clients in an Avamar system:

- "Understanding Avamar clients" on page 60
- "Registering a single client" on page 62
- "Batch client registration" on page 63
- "Activating a client" on page 66
- "Editing client information" on page 67
- "Viewing client properties" on page 68
- "Enabling and disabling a client" on page 69
- "Retiring a client" on page 70
- "Moving a client to a new domain" on page 71
- "Deleting a client" on page 71
- "Editing client paging settings" on page 72

Understanding Avamar clients

Avamar clients are networked computers or workstations that access the Avamar server over a network connection.

Before Avamar can back up or restore data on a client, you must add, or *register*, the client with the Avamar server, and then activate the client.

To provide maximum flexibility in deploying Avamar clients, registration and activation are separate events that occur asynchronously. Although they often occur at nearly the same time, they can also occur hours, days, or even weeks apart.

Client registration

Client registration is the process of establishing an identity with the Avamar server. Once Avamar "knows" the client, it assigns a unique client ID (CID), which it passes back to the client during activation.

There are three ways to register a client:

- Client-side registration
- Interactive server-side registration
- Batch client registration

Client-side registration

The client-side registration process depends on the operating system. The *EMC Avamar Backup Clients User Guide* describes client-side registration for each supported operating system.

Client-side registration also activates the client at the same time. For this reason, client-side registration is very popular. However, the client is automatically added to the Default Group and must use the default dataset, schedule, and retention policy. As a result, this method may not provide enough control for some sites.

Interactive server-side registration

You can use Avamar Administrator to add a client to the system in a domain and group. This provides a high degree of control. For example, you can assign a specific dataset, schedule, and retention policy. However, it can be very time consuming if you need to add many clients.

Batch client registration

To support large sites with many clients, the batch client registration feature enables you to define multiple clients in a single client definition file, then import that file into the Avamar server. Batch client registration is very popular at large sites because it provides nearly as much control as interactively adding the client using Avamar Administrator but is much faster. "Batch client registration" on page 63 provides details.

Client activation

Client activation is the process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system. There are two ways to activate a client:

- Initiate activation from the client.

  This method is described in the *EMC Avamar Backup Clients User Guide*.

- Invite the client to activate with the server by using Avamar Administrator.

  To do this, open the **Actions** menu and select **Account Management** › **Invite Client**.

  Immediate activation by using Avamar Administrator requires the following:

  - Client must be present on the network
  - Avamar client software must be installed and running
  - Avamar server must be able to resolve the hostname that was used to register the client

  "Activating a client" on page 66 provides additional information.

NOTICE

HP-UX, Linux, and Solaris clients can either be activated during installation or from Avamar Administrator. There is no client-side command to initiate client activation on these computing platforms.

Client names

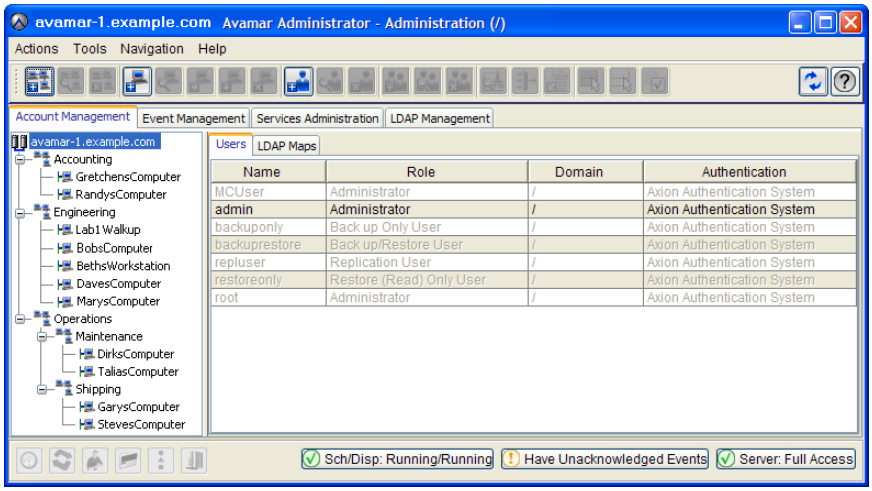
In Avamar Administrator, the client name must always be the client's hostname. Furthermore, if you need to change the client name in Avamar Administrator because the client hostname changed, you must first shut down the Avamar software on the client computer, change the client name by editing the client information as described in "Editing client information" on page 67, then restart the Avamar client software. This is the only way to ensure that the client maintains its registration with the Management Console Server (MCS) database, which ensures that past backups continue to be associated with the client.

Registering a single client

To add a client to the Avamar configuration, which registers the client:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.



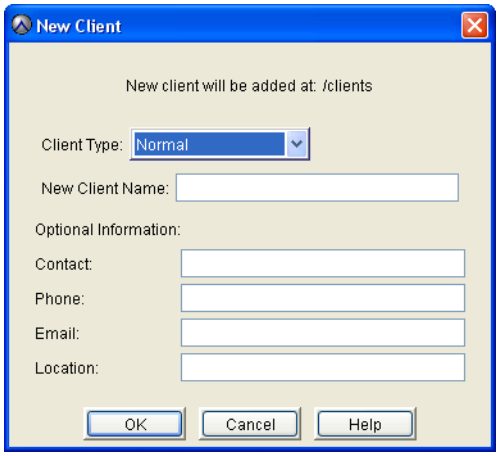
2. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the tree, select the domain for the new client.

4. From the **Actions** menu, select **Account Management** › **New Client**.

   The New Client dialog box appears.



5. From the **Client Type** list, select **Normal**.

   NOTICE

   VMware vCenter™, Image Proxy, and Virtual Machine client types are discussed in the *EMC Avamar for VMware User Guide*.

6. In the **New Client Name** field, type the client name.
7. (Optional) In the **Contact** field, type the contact name.
8. (Optional) In the **Phone** field, type the contact telephone number.
9. (Optional) In the **Email** field, type the contact email address.
10. (Optional) In the **Location** field, type the contact location.
11. Click **OK**.

    A confirmation message appears.
12. Click **OK**.

Batch client registration

To support large sites with many clients, Avamar provides a batch client registration feature that enables you to define multiple clients with a single "clients definition" file, then import that file into the Avamar server.

To import multiple clients:

1. Create the clients definition file.
2. Validate and import the clients definition file.

After batch client registration, you can activate these Avamar clients as discussed in "Client activation" on page 61.

Creating a clients definition file

Avamar supports two formats for the clients definition file:

- Extensible Markup Language (XML)
- Comma-Separated Values (CSV)

XML format

Extensible Markup Language (XML) clients definition files must have a .xml file extension and conform to the following structure and format:

```
<?xml version="1.0" encoding="UTF-8" ?>
   <registration_stream>
      <registrants>
         <entry
            host_name="MyClient.Example.com"
            mcs_domain="clients"
            mcs_group="MyGroup"
            dataset="MyDataset"
            retention_policy="MyRetentionPolicy"
            contact_address="192.168.31.5"
            contact_port="28002"
            access_list="user1@avamar:password, user2@LDAP"
            encryption="high"
            encryption_override="false"
         />
      </registrants>
   </registration_stream>
```

NOTICE

The clients definition file in this topic is for reference purposes only. Do not attempt to cut and paste this example into a clients definitions file. Invisible formatting characters will prevent you from successfully doing so.

Each client is defined using a separate "entry" element.

Table 12 Entry element attributes

Attribute	Description
`host_name`	Network hostname or IP address for this client.
`mcs_domain`	Optional Avamar domain for this client; overrides default domain (clients).
`mcs_group`	Optional default group for this client; overrides assignment to the Default Group. Chapter 6, "Groups and Group Policies," provides details.
`dataset`	Optional default dataset for this client to use during backups; overrides the default dataset that would normally be inherited from the group. "Datasets" on page 124 provides details.
`retention_policy`	Optional default backup retention policy for this client; overrides the default retention policy that would normally be inherited from the group. "Retention policies" on page 147 provides details.
`contact_address`	Optional client IP address.
`contact_port`	Set this to 28002, the default Avamar data port.
`access_list`	Optional list of users who can access the Avamar server from this client. The format is: `USER@AUTHENTICATION:password` If using the internal authentication system, the word "password" must follow the colon. This causes the system to prompt users for authentication when they access the system. If using an external authentication system, omit ":password." If defining multiple users, separate each user entry with a comma (,) and enclose the entire list of users in double-quotes.
`encryption`	Encryption method for client/server data transfer. Choices are: • **High**—The strongest available encryption setting for that specific client platform. • **Medium**—Medium strength encryption. • **None**—No encryption. **Note:** The exact encryption technology and bit strength used for any given client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.
`encryption_override`	Optional encryption override. If TRUE, this client does not use the group encryption method.

NOTICE

You can omit optional elements from an XML clients definition file.

CSV format

Comma-Separated Values (CSV) clients definition files use the same element and attribute names as the XML format. However, each client is defined on a single line, and each attribute value is separated by a comma, as shown in the following example:

```
host_name,mcs_domain,mcs_group,dataset,retention_policy,
   contact_address,contact_port,access_list,encryption,
   encryption_override
```

NOTICE

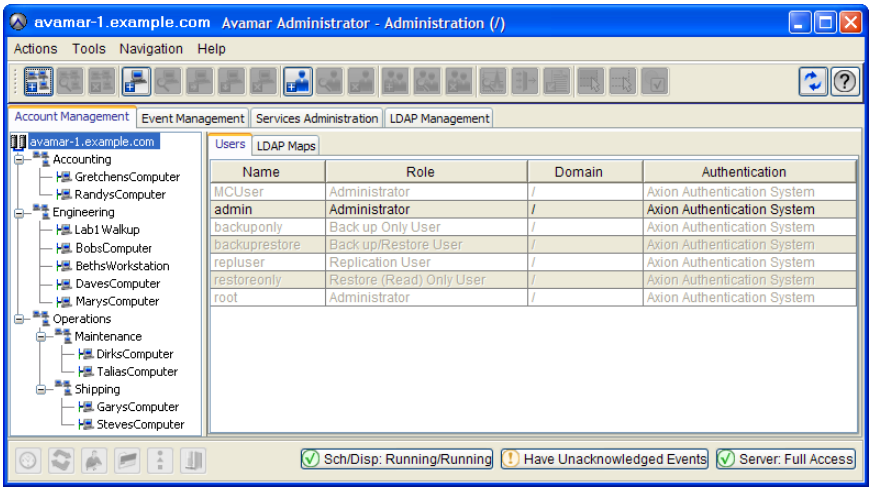
Space limitations in this guide prevent showing a client entry as it should appear, which is on a single line. However, a CSV file must define each client on a single line—no line feeds or carriage returns are allowed within a client entry. Supply values in place of the attribute names, and specify NULL for fields that have no value. Do not leave any fields blank.

Validating and importing a clients definition file

To validate and import the clients definition file:

1. In Avamar Administrator, click the **Administration** launcher button.

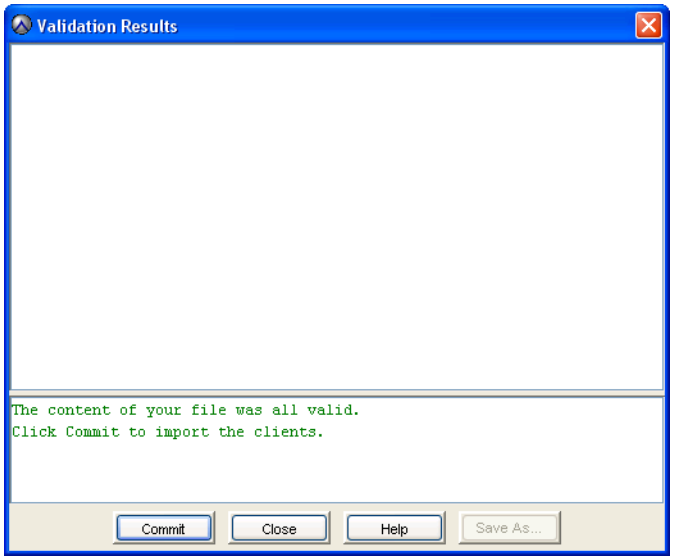
   The Administration window appears.



2. Click the **Account Management** tab.
3. From the **Actions** menu, select **Account Management** › **Import Clients from File**.

   The Validate dialog box appears.
4. Browse to and select the saved clients definition file.
5. Click **Validate**.

The Validation Results dialog box appears.



6. If the clients definition file is error free, click **Commit** to import the client list. Or, of the clients definition file contains errors, correct the errors, save the file again, and repeat the steps in this procedure.

   The Validation Results dialog box closes, and the new clients appear in the Account Management tree.

Activating a client

To activate a client that you added to the Avamar configuration:

1. Ensure that Avamar client software is installed and running on the client.
2. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.
3. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.
4. In the tree, select the client to activate.
5. From the **Actions** menu, select **Account Management** › **Invite Client**.

   The following status message appears: Client has been sent invitation to activate with the server.
6. Click **OK**.

Editing client information

In Avamar Administrator, the client name must always be the client hostname.

If you need to change the client name in Avamar Administrator because the client hostname changed, you must first shut down the Avamar software on the client computer, change the client name by way of this procedure, then restart the Avamar client software. This is the only way to ensure that the client maintains its registration with the Management Console Server (MCS) database, which ensures that past backups continue to be associated with the client.

To edit client information:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

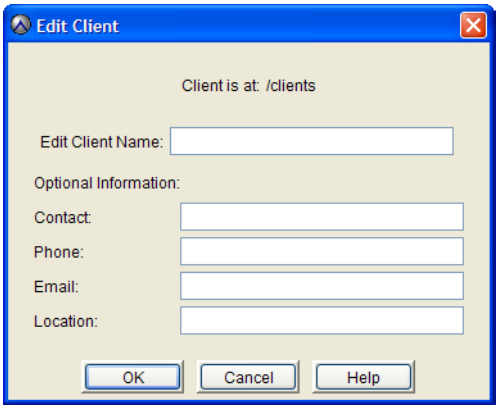
2. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the tree, select the client to edit.

4. From the **Actions** menu, select **Account Management** › **Edit Client**.

   The Edit Client dialog box appears.



5. Edit the name, contact information, or location information for the client.

6. Click **OK**.

   A confirmation message appears.

7. Click **OK**.

Viewing client properties

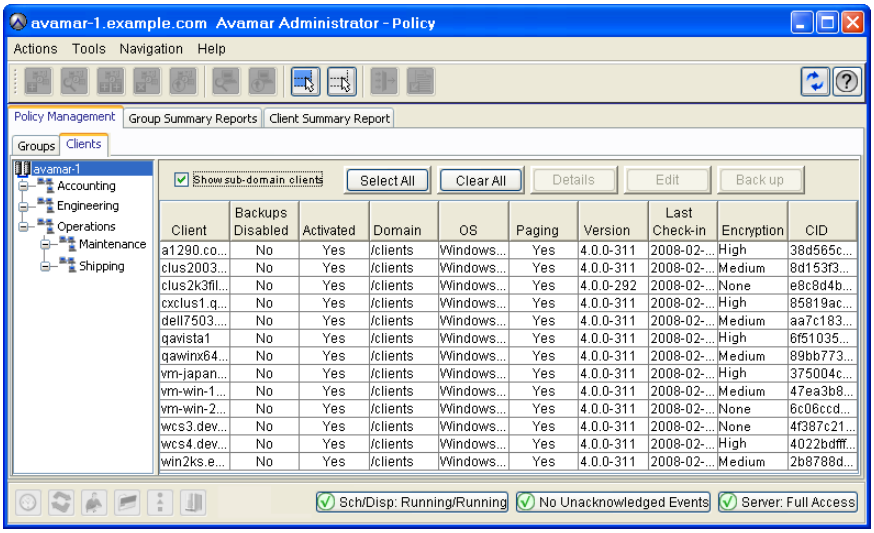
To view client properties:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.

3. Click the **Clients** tab.



4. Select the client.

   The client properties appear in the main pane of the window.

Table 13 Client properties summary

Column	Description
Client	Descriptive client name.
Backups Disabled	Whether Avamar can perform backups for the client. Regardless of this setting, the client can restore files as long as a previous backup exists in the system.
Activated	Whether the client is activated with the Avamar server.
Domain	The Avamar domain for the client.
OS	The operating system on the client.
Paging	Whether the client has provided the Avamar server with a page address and port number, thereby allowing it to perform on-demand backups and restores. In addition, Avamar Administrator can browse its file system during Avamar Administrator-initiated backups and restores.
Version	The version of Avamar client software on the client.
Last Check-in	The date and time that the Avamar client agent last checked in with the Avamar server.
Encryption	The encryption method used for client/server data transfer.
CID	The Client ID, a unique identifier for this client in the Avamar server. CIDs are assigned during client activation.

Enabling and disabling a client

You can disable a client so that it cannot use the Avamar server to back up files. This is typically done to place the system in a state that supports maintenance activities.

If a client has been disabled, you must reenable the client before backups for the client can resume.

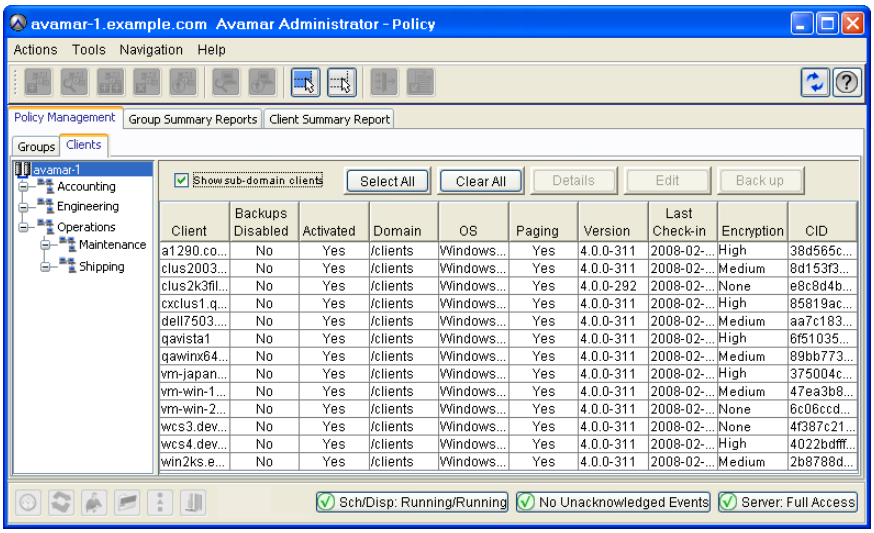
To disable and enable a client:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.

3. Click the **Clients** tab.



4. Select the client to disable or enable.

5. From the **Actions** menu, select **Client** › **Disable all backups of selected client**.

   A confirmation message appears.

6. Click **Yes**.

   When the client is disabled, a checkmark appears next to the **Disable all backups of selected client** option on the **Actions** › **Client** menu. When the client is enabled, the checkmark does not appear.

Retiring a client

When you retire a client, Avamar does not back up the client. However, old backups associated with a retired client are maintained in the system (subject to backup retention settings), and you can restore files from the client using Avamar Administrator.

To retire a client:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

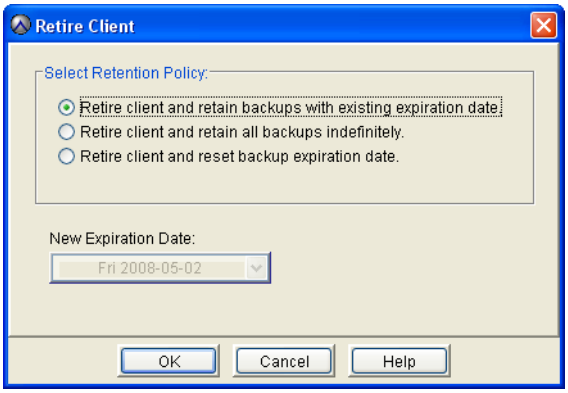
2. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the tree, select the client to retire.

4. From the **Actions** menu, select **Account Management** › **Retire Client**.

   The Retire Client dialog box appears.



5. Choose how long to keep backups for this client.

   - To keep backups until their existing expiration dates, select **Retire client and retain backups with existing expiration date**.
   - To keep backups indefinitely, regardless of the existing backup expiration dates, select **Retire client and retain all backups indefinitely**.
   - To keep backups until a new expiration date, select **Retire client and reset backup expiration date** and select a new backup expiration date.

6. Click **OK**.

   A confirmation message appears.

7. Click **Yes**.

Moving a client to a new domain

To move a client to a new domain:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

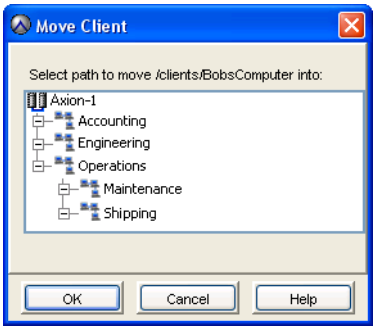
2. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the tree, select the client to move.

4. From the **Actions** menu, select **Account Management** › **Move Client**.

   The Move Client dialog box appears.



5. Select the new domain for the client.

6. Click **OK**.

Deleting a client

When you delete a client, Avamar permanently deletes all backups stored for that client. Therefore, you should only delete a client when you are certain that there is no reason to retain the backups. If there is any doubt, retire the client instead as described in "Retiring a client" on page 70.

To delete a client:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Account Management** tab.

   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the tree, select the client to delete.

4. From the **Actions** menu, select **Account Management** › **Delete Client**.

   A confirmation message appears.

5. Click **Yes**.

   A second confirmation message appears.

6. Click **OK**.

Editing client paging settings

Paging settings are used for communication between the MCS and the client. Paging settings are independent of the method used to register and activate the client.

Avamar Administrator offers two client paging modes:

- **Automatic**—Automatic is the default mode. When paging is set to Automatic, the MCS attempts to automatically determine appropriate paging settings for the client. If it is successful in doing so, the MCS sets the Enabled option and populates the Address and Port Number fields with the hostname or IP address and data port values, respectively. In automatic mode, these fields are read-only.

  In automatic mode, if the MCS receives updated paging information from the client, it automatically updates these fields with the new values.

- **Manual**—When paging is set to Manual, the Enabled option can be cleared to turn off automatic client paging, and the Address and Port Number fields accept new entries.

  Turning off automatic client paging (by clearing the Enabled option) is useful to support clients that might be off the network for extended periods of time, as can be the case with laptop computers. If client paging is turned off, these clients must initiate their own on-demand backups. For this reason, client paging should be enabled whenever possible.

  If Network Address Translation (NAT) is used, the MCS probably cannot automatically determine the correct client paging settings. If this is the case, set the paging mode to manual and type the correct IP address and data port in the Address and Port Number fields, respectively.

  In manual mode, the MCS never overwrites the Address and Port Number settings.

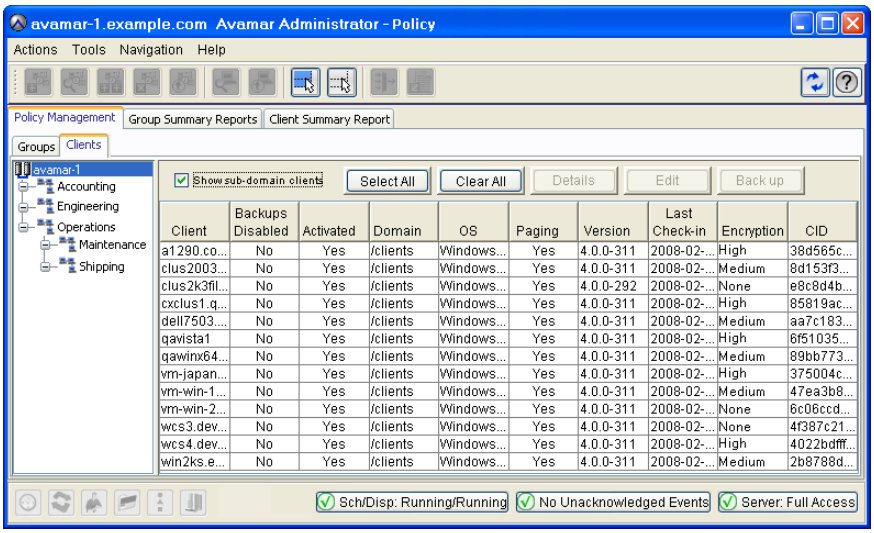
To edit client paging settings:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.

3. Click the **Clients** tab.

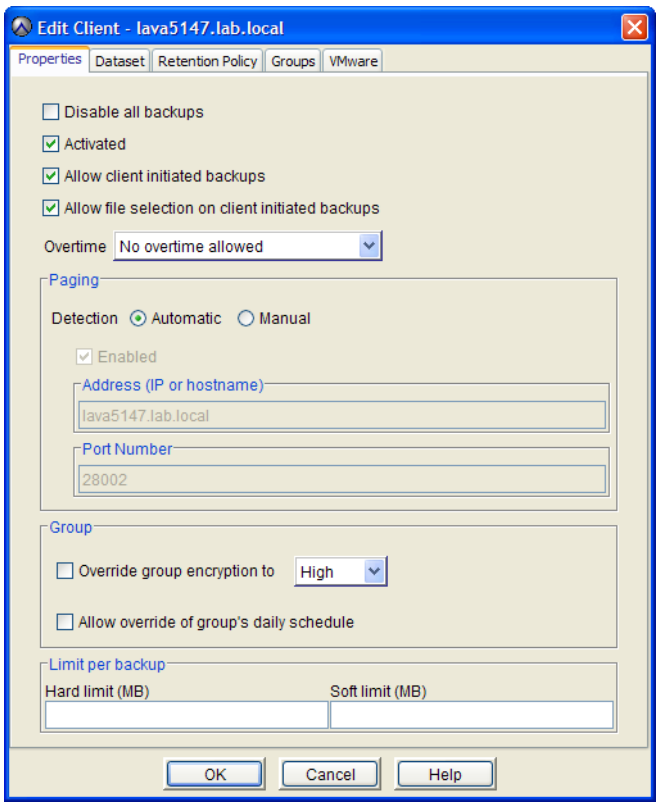


4. Select the client.

5. From the **Actions** menu, select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. Select either the **Automatic** or **Manual** paging mode.
8. If you selected the **Manual** paging mode, specify the client IP address and port number for client-MCS communications: The **Address** and **Port Number** fields are described below:
   - In the **Address** field, specify a valid (un-NAT'd) IP address for the client.

     NOTICE

     If the MCS was unable to automatically determine a hostname for this client in automatic mode, type an IP address in this field.

   - In the **Port Number** field, specify the data port number for client-MCS communications. The default data port is 28002.
9. Click **OK**.

Using Avamar in non-pageable environments

A client is *non-pageable* where the Avamar Administrator server running on the Avamar server utility node or on a single-node server cannot establish a TCP/IP connection to port 28002 on the Avamar client.

In environments where clients are non-pageable, there are limitations to using MCS. MCS cannot be used to start activation or pick up new backup or restore operations.

The client might be non-pageable in the following situations:

- The environment (including the client) has firewall rules that prevent incoming connections on port 28002 to the client.
- The client is behind a router that doesn't support port-forwarding for connections initiated from the Avamar server. (This is the common situation that managed service providers could encounter if they deploy Avamar without using VPN, for example.)
- The Avamar Administrator server cannot connect to the Avamar client on the paging address used by the Avamar Administrator server. One example of this is if the client is multi-homed and the paging address used by the Avamar Administrator server to connect to the client does not have a route to the paging address.
- The environment requires authentication to establish a host-to-host connection to port 28002 on the client, and the Avamar Administrator server process is not able to support the required authentication protocol.
- An IPSEC environment. In a Windows environment Microsoft best practices recommend enabling IPSEC, and clients are not pageable in an IPSEC environment.

You can use Avamar Administrator to perform backups or restores, or define policies. In some cases you will need to enter explicit path names. MCS should automatically detect non-pageable clients and adjust settings. Usually no manual changes are needed in MCS. You can check the Avamar Administrator Policy › Client tab and see if Paging is set to Yes or No for each client. It should be set to No if MCS cannot connect to the avagent.

The following limitations apply in Avamar Administrator when the client is non-pageable:

- You cannot browse the client file system when defining the datasets or when browsing to select a target for restore. The workaround is to explicitly define the backup dataset without browsing a client. During a restore, the workaround is to explicitly type in the restore target path.
- You cannot double-click on the Activities view to view client logs. The workaround is to have the owner of the client being backed up copy and send the logs when they are required to trouble-shoot a backup.
- You cannot page the client when there is a work order waiting for the client. In this case, the client will connect to the MCS and poll for the existence of a work order approximately once every minute.

Additional MCS limitations:

- If the MCS cannot page the client on port 28002, then Avamar cannot invite the client to activate through the Administration View in the MCS.
- If you are backing up several hundred or more non-pageable clients, the polling interval many need to be increased. The default setting for polling interval is 60 seconds. If MCS performance is slowing down, increase the polling interval until you achieve acceptable performance.

Understanding users, authentication, and roles

A user account in Avamar can administer a domain or client. The user account defines the authentication system that is used to grant users access to the Avamar server. It also defines the role for the user, which controls the operations that a user can perform. The following topics provide details:

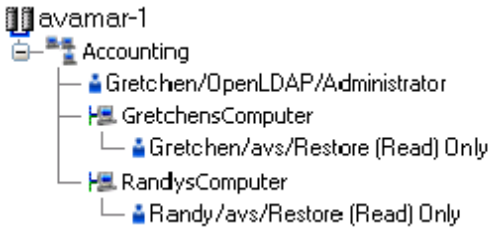
- "Users" on page 76
- "User authentication" on page 77
- "Roles" on page 78

Users

You can add user accounts to domains or individual clients. When you add a user account to a domain, the account can administer that domain and any subdomains beneath it. When you add a user account to an individual client, the account can perform backups and restores of that client, and access backups belonging to that client in the system.

In Avamar, users are entries in a domain or client access list. When you add a user account to the Avamar system, you are adding a new entry to a domain or client user access list.

Consider the following example:



User "Gretchen" has been added to both the Accounting domain and her computer. However, the authentication system and role are different. These are in fact two completely separate user accounts that happen to have the same username.

Avamar user accounts comprise the following pieces of information:

- Username—The username depends on the authentication system and must be in the format that the authentication system accepts. For example, the internal authentication system uses case-sensitive usernames, whereas Windows Active Directory usernames are case-insensitive. Usernames cannot be longer than 31 characters.
- Authentication system—An authentication system is a username/password system that is used to grant users access to the Avamar server. "User authentication" on page 77 provides details on supported authenticaton systems.
- Role—Roles define the allowable operations for each user account. "Roles" on page 78 provides details on the available types of roles.

User authentication

An authentication system is a username/password system that is used to grant users access to the Avamar server. Avamar supports three authentication systems:

- "Avamar internal authentication" on page 77
- "Directory service authentication" on page 77
- "Enterprise authentication" on page 77

Avamar internal authentication

With Avamar internal authentication, you define the username and password for Avamar user accounts, and Avamar stores the information. Usernames are case-sensitive and cannot be longer than 31 characters.

Directory service authentication

When you use directory service authentication to authenticate and assign roles to Avamar users, you can take advantage of a directory service that already exists in an organization. You can use any LDAP v.3-compliant directory service, such as Microsoft Active Directory Domain Services. Also, you can use a Network Information Service (NIS) on its own or with the LDAP services. "Enabling directory service authentication" on page 84 provides details on how to configure Avamar to use directory service authentication.

Enterprise authentication

With enterprise authentication, Avamar uses the Pluggable Authentication Module (PAM) library of the host Linux operating system to provide access to external authentication databases.

Enterprise authentication, which is described in the *Avamar Product Security Guide*, is deprecated and will be removed in future releases.

By default, you cannot select an enterprise authentication domain when you add a user to a domain or client in this Avamar release. However, if you upgraded to this release and you want to continue to use enterprise authentication, you can configure the system to enable selection of enterprise authentication when you add a user. "Enabling selection of enterprise authentication" on page 88 provides details.

How Avamar authenticates users and assigns roles

To provide backwards compatibility with Enterprise Authentication and to account for the possibility of users in more than one LDAP mapped group, Avamar uses the following authentication and role assignment sequence for each login attempt:

1. When the username is in the format USER, where USER is a username *without* @EXT-AUTH-SERVER appended, then Avamar checks the internal Avamar authentication database.

   If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database. If they do not match, then the login fails.

2. When the username is in the format USER@EXT-AUTH-SERVER, where USER is a username and EXT-AUTH-SERVER is the fully qualified domain name of the authentication server, then Avamar checks the login information using Enterprise Authentication.

If the username, password, and domain match, then the login is successful and Avamar assigns the user a role in the Avamar database.

If there is no match, then the evaluation continues.

3. When the username is in the format USER@EXT-AUTH-SERVER and authentication using Enterprise Authentication fails, then Avamar checks the LDAP mapping system.

   The login attempt is checked against all mapped groups for a match of each of the following identifiers:

   - Username, the portion of the User Name field entry *before* the @ symbol.
   - Password, as entered in the Password field.
   - Avamar domain, as entered in the Domain Name field.
   - Directory service domain, the portion of the User Name field entry *after* the @ symbol.

   When all identifiers match, the login is successful and Avamar assigns the user a role from the mapped group.

   A user can be the member of mapped groups in different directory service domains. The role of the mapped group that matches the directory service domain provided during login is assigned to the user for that session.

   When the user is a member of more than one mapped group in the same directory service domain, the role with the greatest authority is assigned.

4. When the login information does not meet the requirements of any of the previous steps, then the login fails and a failure message appears.

Roles

Roles define the allowable operations for each user account. There are three types of roles:

- "Administrator roles" on page 78
- "Operator roles" on page 79
- "User roles" on page 83

Administrator roles

Administrators are generally responsible for maintaining the system.

You can only assign the role of administrator to user accounts at a domain level. This includes the top-level (root) domain or any other domain or subdomain. You cannot assign this role to user accounts at a client level.

Root administrators

Administrators at the top-level (root) domain have full control of the system. They are sometimes referred to as "root administrators."

Domain administrators

Administrators at domains other than root generally have access to most of the features described in this guide, but typically can only view or operate on objects (backups, policy objects, and so forth) in that domain. Any activity that might allow a domain administrator

to view data outside that domain is disallowed. Therefore, access to server features of a global nature (for example, suspending or resuming scheduled operations, changing runtimes for maintenance activities, and so forth) is disallowed.

Furthermore, domain administrators:

- Cannot add or edit other subdomain administrators
- Cannot change their assigned role
- Can change their password

Operator roles

Operator roles are generally implemented to allow certain users limited access to certain areas of the system to perform backups and restores, or obtain status and run reports. These roles allow greater freedom in assigning backup, restore, and reporting tasks to persons other than administrators.

You can only assign operator roles to user accounts at the domain level. You cannot assign these roles to user accounts at the client level. Furthermore, to add the user account to subdomains, you must have administrator privileges on the parent domain or above.

There are four operator roles:

- Restore only operator
- Back up only operator
- Back up/restore operator
- Activity operator

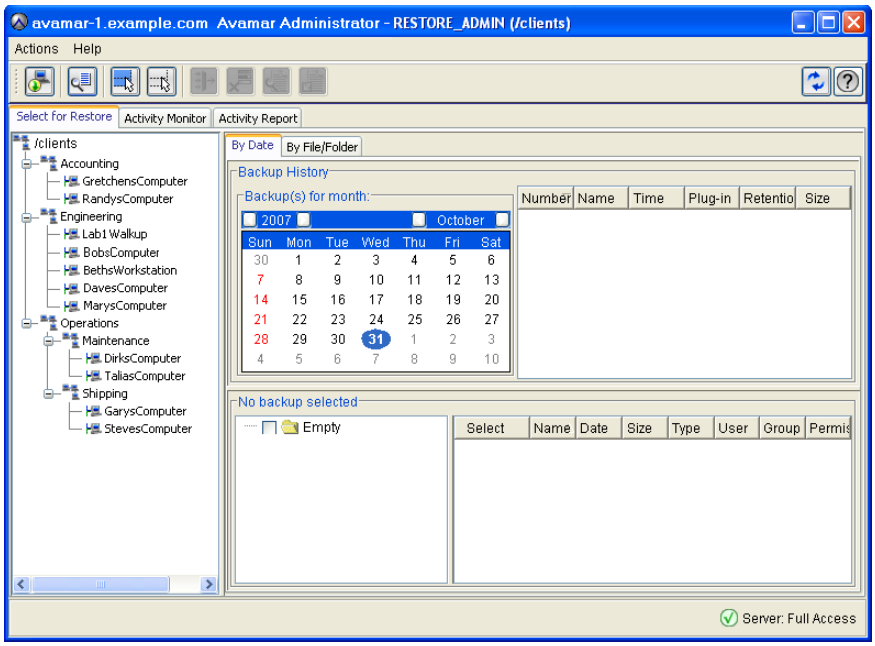
Users with an operator role do not have access to all features in Avamar Administrator. Instead, after login, they are presented with a single window that provides access to the features that they are allowed to use.

Restore only operator

Restore only operators are generally only allowed to perform restores and to monitor those activities to determine when they complete and if they completed without errors.

Restore only operators at the top-level (root) domain can perform restores for any client in the system. Restore only operators at a domain other than root can only perform restores for clients in that domain.

To enforce these constraints, restore only operators do not have access to all features in Avamar Administrator. Instead, after login, they are presented with the following window, which provides access to the features that they are allowed to use.



Restore only operators can perform the following tasks in the assigned domain:

- Restore backup data as described in Chapter 4, "Backup, Restore, and Backup Management."
- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 116.

By default, restore only operators cannot browse backups from the command line or using the Avamar Web Restore interface. To enable these activities for a restore only operator, add the noticketrequired privilege using the **avmgr chgv** command:

```
avmgr chgv --acnt=LOCATION --u=NAME --ud=AUTH \
   --pv="enabled,read,mclogin,noticketrequired"
```

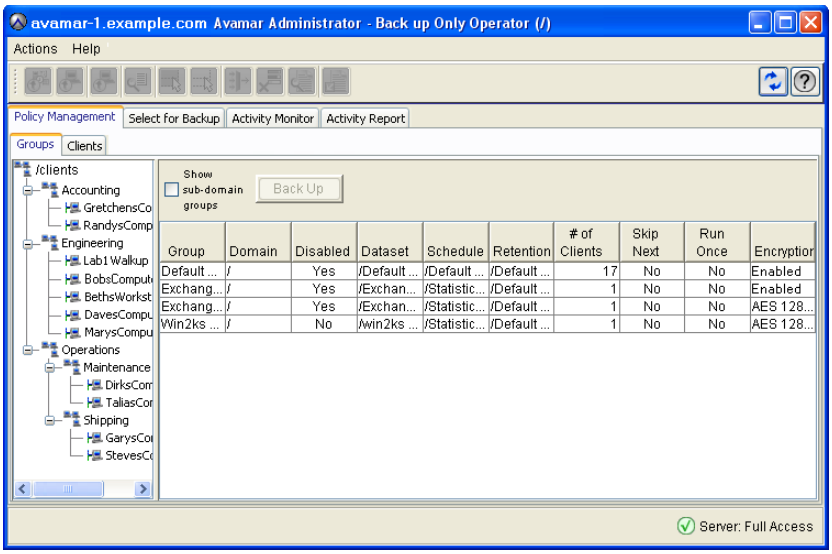
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user, and AUTH is the external authentication system used to authenticate the user.

Back up only operator

Back up only operators are generally only allowed to perform backups and to monitor those activities to determine when they complete and if they completed without errors.

Back up only operators at the top-level (root) domain can perform backups for any client or group in the system. Back up only operators at domains other than root can only perform backups for clients or groups in that domain.

To enforce these constraints, back up only operators do not have access to all features in Avamar Administrator. Instead, after login, they are presented with the following window, which provides access to the features that they are allowed to use.



Back up only operators can perform the following tasks in the assigned domain:

- Perform on-demand backups as described in "Performing an on-demand backup" on page 96.
- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 116.
- Initiate on-demand group backups as described in "Performing on-demand group and client backups" on page 187.

By default, backup only operators cannot perform backups from the command line. To enable command line backups for a restore only operator, add the noticketrequired privilege using the **avmgr chgv** command:

```
avmgr chgv --acnt=LOCATION --u=NAME --ud=AUTH \
   --pv="enabled,read,mclogin,backup,noticketrequired"
```

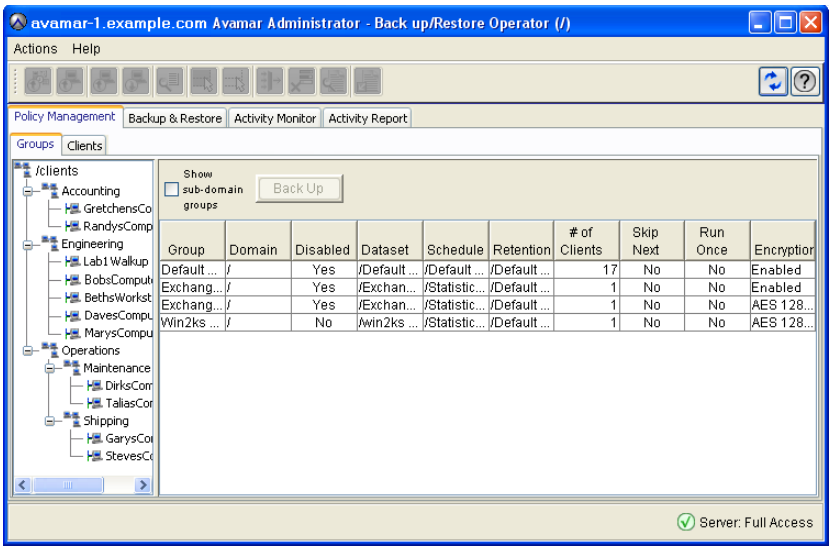
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user, and AUTH is the external authentication system used to authenticate the user.

Back up/restore operator

Back up/restore operators are generally only allowed to perform backups or restores and to monitor those activities to determine when they complete and if they completed without errors.

As with roles assigned to other domain user accounts, back up/restore operators at the top-level (root) domain can perform backups and restores for any client or group in the system. Back up/restore operators at domains other than root can only perform backups and restores for clients or groups in that domain.

To enforce these constraints, back up/restore operators do not have access to all features in Avamar Administrator. Instead, after login, they are presented with the following window, which provides access to the features that they are allowed to use.



Back up/restore operators can perform the following tasks in the assigned domain:

- Perform on-demand backups as described in "Performing an on-demand backup" on page 96.
- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 116.
- Perform a restore as described in Chapter 4, "Backup, Restore, and Backup Management."
- Initiate on-demand group backups as described in "Performing on-demand group and client backups" on page 187.

By default, back up/restore operators cannot browse backups from the command line or using the Avamar Web Restore interface, and cannot perform backups from the command line. To enable these activities for a restore only operator, add the noticketrequired privilege using the **avmgr chgv** command:

```
avmgr chgv --acnt=LOCATION --u=NAME --ud=AUTH \
   --pv="enabled,read,mclogin,backup,noticketrequired"
```

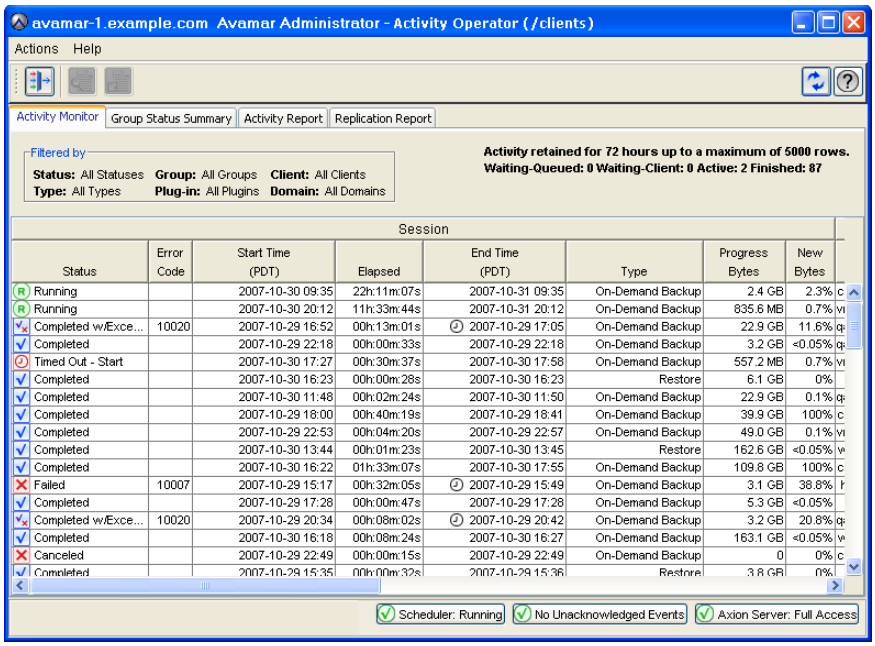
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user , and AUTH is the external authentication system used to authenticate the user.

Activity operator

Activity operators are generally only allowed to monitor backup and restore activities and to create certain reports.

Activity operators at the top-level (root) domain can view or create reports for backup and restore activities in all domains and subdomains. Activity operators at domains other than root can only view or create reports for backup and restore activities in that domain.

To enforce these constraints, activity operators do not have access to all features in Avamar Administrator. Instead, after login, they are presented with the following window, which provides access to the features that they are allowed to use.



Activity operators can perform the following tasks in the assigned domain:

- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 116.
- View the group status summary as described in "Viewing the Group Status Summary" on page 168.
- View the Activity Report as described in "Viewing the Activity Report" on page 246.
- View the Replication Report as described in "Viewing the Replication Report" on page 250.

User roles

User roles limit the operations allowed for a user account to a specific client.

Users assigned to one of the user roles cannot log in to:

- Avamar Administrator
- Enterprise Manager
- Avamar client web UI

There are four types of user roles.

Back Up Only User

Users assigned this role can initiate backups directly from the client using the **avtar** command line.

Restore (Read) Only User

Users assigned this role can initiate restores directly from the client using the **avtar** command line or Avamar Web Services.

Back Up/Restore User

Users assigned this role can initiate backups and restores directly from the client using the **avtar** command line or Avamar Web Services.

Restore (Read) Only/Ignore File Permissions

This role is similar to the Restore (Read) Only User role except that operating system file permissions are ignored during restores, thereby effectively allowing this user to restore any file stored for that Avamar client.

This role is only available when you use internal authentication.

Windows client user accounts should be assigned this role to ensure trouble-free restores, only if both of the following are true:

- Users are authenticated using Avamar internal authentication.
- The user will not access the Avamar client web UI.

Enabling user authentication

The following topics provide details on enabling user authentication for each supported authentication method:

- "Enabling internal Avamar authentication" on page 84
- "Enabling directory service authentication" on page 84
- "Enabling selection of enterprise authentication" on page 88

Enabling internal Avamar authentication

No additional steps are required to use internal Avamar authentication to authenticate user accounts. You define the username and password for each account when you add the user as described in "Adding a user to a client or domain" on page 90.

Enabling directory service authentication

When you use directory service authentication to authenticate and assign roles to Avamar users, you can take advantage of a directory service that already exists in an organization. You can use any LDAP v.3-compliant directory service, such as Microsoft Active Directory Domain Services. Also, you can use a Network Information Service (NIS) on its own or with the LDAP services.

To use directory service authentication for Avamar users:

1. Create directory service groups in the directory service (not in Avamar).

   Groups can range in size from one member to as many members as the directory service allows.

   Ideally, you should create directory service groups specifically for use with an Avamar LDAP map. By doing this, group composition is considered in the context of the level of Avamar access being granted. Also, the group name can include a common character pattern to simplify its discovery during mapping. For example, you could start each group name with the characters “av”, as in “avAdministrators”. This would enable you to search for all groups associated with Avamar by using the wildcard search string “av*”.

2. Configure Avamar to use the directory service, as described in “Configuring directory service information” on page 412.

3. Create an LDAP map to associate the directory service group to Avamar user information, as discussed in “Adding an LDAP map” on page 86. An LDAP map is a database construct that ties a group of users to the following Avamar user information:

   - Authentication system
   - Domain or subdomain access list
   - Role

   NOTICE

   When you delete a domain, Avamar removes the LDAP maps that rely on that domain for access. The directory service groups associated with the removed LDAP maps are not affected by the deletion.

Adding an LDAP map

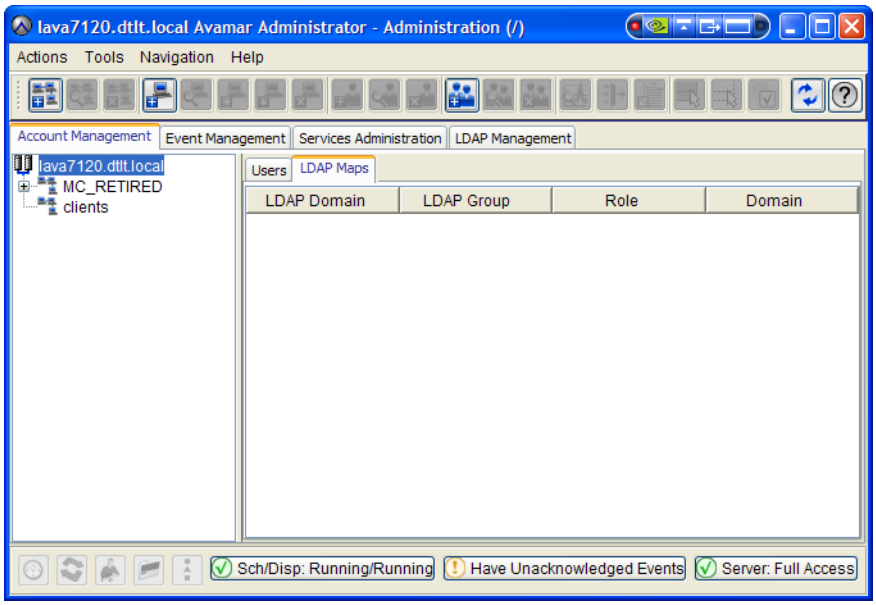
To add an LDAP map:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Account Management** tab.

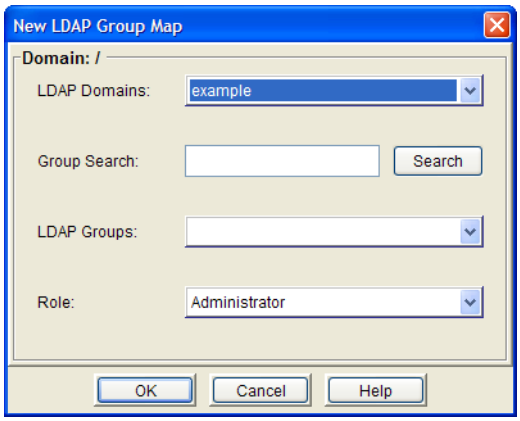
3. Click the **LDAP Maps** tab.



4. In the left-pane hierarchical tree, select a domain or a subdomain to specify the access level of the directory service group.

5. Select **Actions** › **Account Management** › **New LDAP Map**.

   The New LDAP Group Map dialog box appears.



6. From the **LDAP Domains** list, select a directory service domain to map.

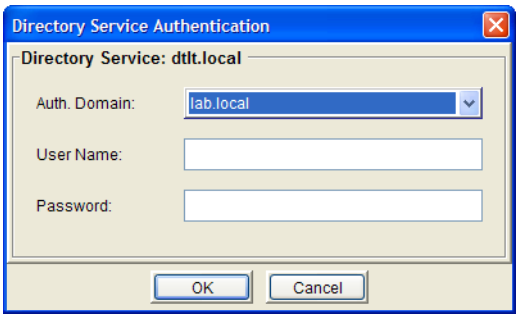
   If the list is empty, click Cancel to close the dialog box, configure directory service domains as described in "Configuring directory service information" on page 412, and then return to this task.

7. In the **Group Search** field, type a search string specific to the group being mapped.

   You can use an asterisk (*) as a wildcard that represents one or more alphanumeric characters.

8. Click **Search**.

   The Directory Service Authentication dialog box appears.



   Use this dialog to provide the authentication information required for querying the directory service. Authentication can be through a domain different from the one being mapped, as long as there is a trust relationship between the two domains.

9. From the **Auth Domain** list, select a domain to use for authentication.
10. In the **User Name** field, type a username for an account that has Read privileges for the domain.
11. In the **Password** field, type the password for the username.
12. Click **OK**.

    The Directory Service Authentication dialog closes and the search starts. The Search button changes to Stop. To terminate a search, click **Stop**.

    Searching a directory service can take a long time. The search is complete when groups appear in LDAP Groups.

13. From the **LDAP Groups** list, select the group to map.
14. From the **Role** list, select a role for the group. Roles are described in "Understanding users, authentication, and roles" on page 76.
15. Click **OK**.

    The group is mapped and the New LDAP Group Map dialog closes. Select the appropriate administrative node to see the mapping on the LDAP Maps tab.

Editing the role for an LDAP map

To edit the role assigned to an LDAP map:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.
2. Click the **Account Management** tab.
3. Click the **LDAP Maps** tab.
4. In the left-pane hierarchical tree, select a domain or a subdomain.

   The maps for the domain or subdomain appear in the LDAP Maps area.
5. Select the map to edit.
6. Select **Actions** › **Account Management** › **Edit LDAP Map**.

   The Edit LDAP Map dialog appears.
7. In **Role**, select a new role to assign to the map.
8. Click **OK**.

The map is assigned the new role. Group members are assigned the new role in all subsequent sessions.

Deleting an LDAP map

To delete an LDAP map:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.
2. Click the **Account Management** tab.
3. Click the **LDAP Maps** tab.
4. In the left-pane hierarchical tree, select a domain or a subdomain.

   The maps for the domain or subdomain appear in the LDAP Maps area.
5. Select the map to delete.
6. Select **Actions** › **Account Management** › **Delete LDAP Map**.

   The Delete LDAP Map dialog appears.
7. Click **Yes**.

Enabling selection of enterprise authentication

With enterprise authentication, Avamar uses the Pluggable Authentication Module (PAM) library of the host Linux operating system to provide access to external authentication databases.

Enterprise authentication, which is described in the *Avamar Product Security Guide*, is deprecated and will be removed in future releases. It is replaced by directory service authentication.

By default, you cannot select an enterprise authentication domain when you add a user to a domain or client in this Avamar release. However, if you upgraded to this release and you want to continue to use enterprise authentication, you can configure the system to enable selection of enterprise authentication when you add a user by changing the enterprise authentication selection setting in mcserver.xml.

To change the enterprise authentication selection setting:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the Management Console Server (mcs) service by typing:

   ```
   dpnctl stop mcs
   ```

3. Change the working directory by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Open mcserver.xml in a plain text editor.
5. Find the ldap node, and the entry with the enable_new_user_authentication_selection key, as shown here:

   ```
   <node name="ldap">
      <map>
         …
         <entry key="enable_new_user_authentication_selection"
   value="false" />
         …
      </map>
   </node>
   ```

   As indicated by the ellipsis (…), the ldap node has many entries. Only the relevant entry appears here.
6. Change the value of the entry to true:

   ```
   <node name="ldap">
      <map>
         …
         <entry key="enable_new_user_authentication_selection"
   value="true" />
         …
      </map>
   </node>
   ```

7. Save the change and close the editor.
8. Restart mcs by typing:

   ```
   dpnctl start mcs
   ```

9. Close the command shell.

Managing user accounts

The following topics provide details on adding, editing, and deleting a user account:

- "Adding a user to a client or domain" on page 90
- "Editing user information" on page 92
- "Deleting a user" on page 93

Adding a user to a client or domain

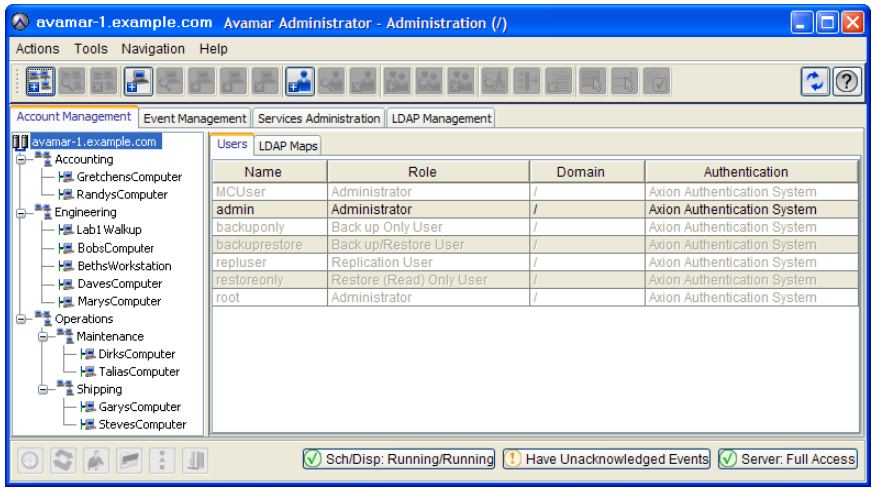
This topic describes how to add a user account to a client or domain when the user account is authenticated using Avamar internal authentication or the deprecated enterprise authentication system.

"Enabling directory service authentication" on page 84 provides details on adding a user that uses an existing directory service for authentication.

To add a user to a client or domain:

1. Review "Roles" on page 78 to ensure that you will assign the correct role to this user.
2. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.



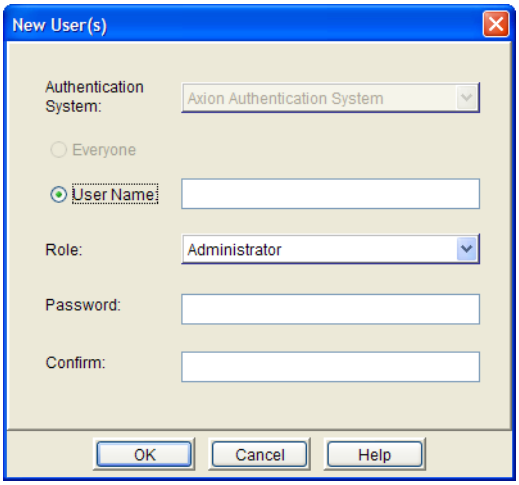
3. Click the **Account Management** tab.
4. Click the **Users** tab
5. In the left-pane hierarchical tree, select the domain or client for the new user.

   NOTICE

   You cannot add user accounts to the MC_RETIRED domain or to clients in the MC_RETIRED domain.

6. From the **Actions** menu, select **Account Management** › **New User(s)**.

   The New User(s) dialog box appears.



7. (Optional) From the **Authentication System** list, select an authentication system.

   The Authentication System list normally appears in a dimmed state, with Axion Authentication System (the internal system) selected. This indicates that the ability to select an enterprise authentication system is not currently enabled.

   The enterprise authentication system, which is described in the *EMC Avamar Product Security Guide*, is deprecated and will be removed in future releases. However it can be used with this release. To enable the ability to select an enterprise authentication system, complete the procedure described in "Enabling selection of enterprise authentication" on page 88.

   For a more robust alternative to enterprise authentication, use the method described in "Enabling directory service authentication" on page 84.

8. (Optional) If you select the enterprise authentication system, select the **Everyone** option to designate roles for all users on this client or domain.

9. Select the **User Name** option and type the new username.

   (Optional) If you use enterprise authentication, this must be the username assigned by that system.

   Usernames cannot contain more than 31 characters.

   Do not use any of the following characters in the user name: ~!@$^%(){}[]|,`;#\/:*?<>'"&.

10. From the **Role** list, select a role for the user.

11. In the **Password** field, type a password for the user.

    Passwords are case-sensitive and must:

    - Be 6-31 characters in length
    - Contain only alphanumeric, hyphen, period, or underscore characters
    - Contain at least one alphabetic character

    This field is not used with enterprise authentication.

12. In the **Confirm** field, retype the password.

    This field is not used with enterprise authentication.

13. Click **OK**.

    A confirmation message appears.

14. Click **OK**.

Editing user information

To edit user information:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Account Management** tab.

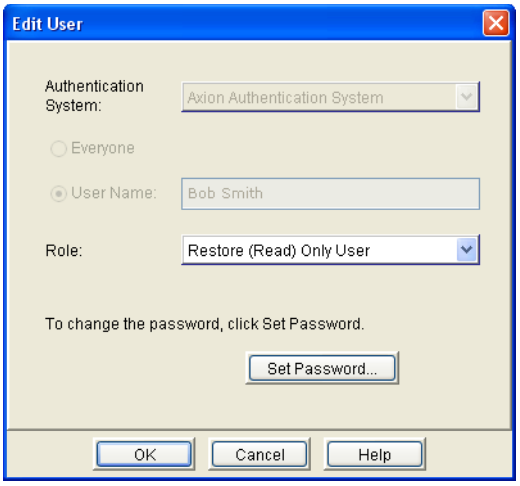
   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

3. In the left-pane hierarchical tree, select the domain or client with the user.

4. Select the user.

5. From the **Actions** menu, select **Account Management** › **Edit User**.

   The Edit User dialog box appears.



6. Select the role for the user.

7. (Optional) Change the password for the user:

   a. Click **Set Password**.

      The Set Password dialog box appears.

   b. Type the new password into both the **New Password** and **Confirm Password** fields.

   c. Click **OK** on the **Set Password** dialog box.

8. Click **OK**.

   A confirmation message appears.

9. Click **OK**.

Deleting a user

To delete a user:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Account Management** tab.
3. In the left-pane hierarchical tree, select the domain or client with the user.
4. Select the user to delete.
5. From the **Actions** menu, select **Account Management** › **Delete User**.

   A confirmation message appears.

6. Click **Yes**.

   A second confirmation message appears.

7. Click **OK**.

CHAPTER 4
Backup, Restore, and Backup Management

After you activate a client, you can back up and restore data on the client. The following topics describe how to perform on-demand client backups and restores using Avamar Administrator, as well as how to monitor and manage backups:

- Performing an on-demand backup 96
- Restoring data from a backup 98
- Managing backups 108
- Monitoring backup, restore, or validation activities 116
- Canceling a backup, restore, or validation 122

NOTICE

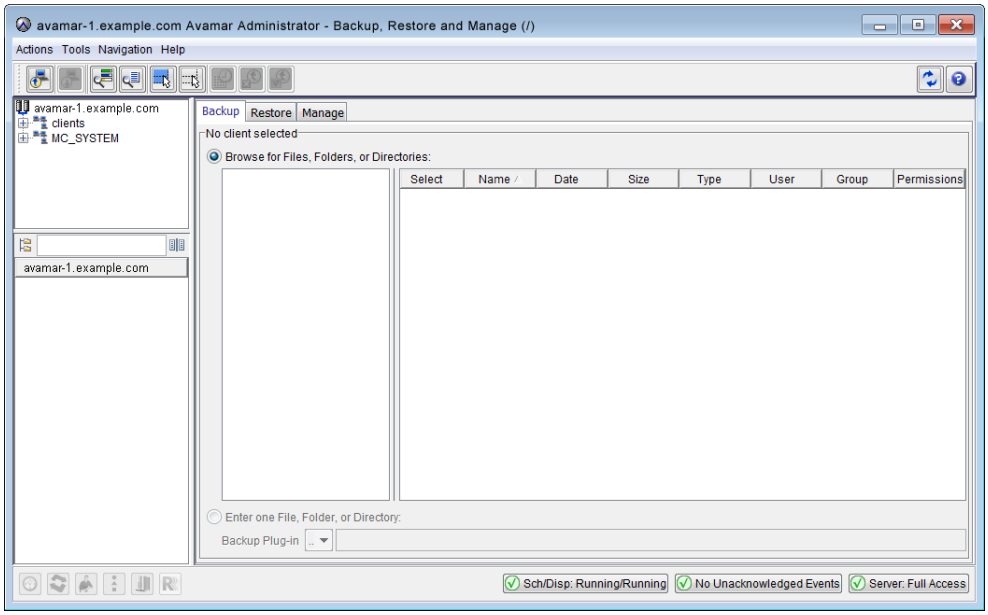
You can also automate backups by implementing a group policy to perform regularly scheduled backups for a group of clients. Chapter 6, "Groups and Group Policies," provides details.

Performing an on-demand backup

To perform an on-demand client backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.



2. Click the **Backup** tab.
3. Select a client in the clients tree.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

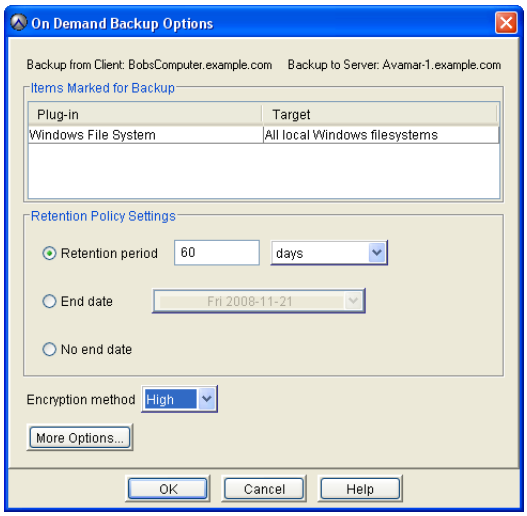
   The client file system appears as a browsable directory tree to the right of the clients tree. Selecting the checkbox next to a directory or file selects it for backup.

   A list of plug-ins installed on the selected client appears in the left pane.
4. Expand the node for the plug-in to use for the backup.
5. Browse to and select the data to back up.
6. If you browse the client file system, specify a valid client username and password, then click **OK**.

   The username and password must have read permissions on the files and directories that you select for backup.
7. (Optional) To view a summary of all directories and files that you selected for backup, select **Actions** › **Preview List**.

8. Select **Actions** › **Backup Now**.

   The On Demand Backup Options dialog box appears.



9. Select one of the following retention policies for this backup:

   - **Retention period**—Automatically delete this backup from the Avamar server after a specific number of days, weeks, months, or years. Select this option, and type the number of days, weeks, months, or years.
   - **End date**—Automatically delete this backup from the Avamar server on a specific calendar date. Select this option and browse to that date on the calendar.
   - **No end date**—Keep this backup for as long as this client remains active in the Avamar server.

10. Select one of the following encryption methods for client/server data transfer during this backup:

    - **High**—Strongest available encryption setting for that specific client platform.
    - **Medium**—Medium strength encryption.
    - **None**—No encryption.

    Note: The exact encryption technology and bit strength used for any given client/server connection is dependent on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

11. To include plug-in options with this backup, click **More Options**, and then configure the settings.

    The user guide for each plug-in provides details on each plug-in option.

12. Click **OK** on the **On Demand Backup Options** dialog box.

    The On Demand Backup Request dialog box indicates that the backup was initiated.

13. Click **Close**.

Restoring data from a backup

The following topics explain how to find a backup to restore and then perform a restore:

- "Finding a backup to restore" on page 98
- "Restoring to the original location" on page 101
- "Restoring to a different location" on page 102
- "Restoring to multiple locations" on page 105

NOTICE

The options for the restore destination depend on the plug-in type. For example, the SQL Server plug-in enables you to restore to a file instead of to SQL Server, and you cannot restore to multiple locations with the Oracle plug-in. The user guide for each plug-in provides details on the available options and how to perform each available type of restore.

Finding a backup to restore

You can find Avamar client backups for a restore either by date or by files and folders.

Some plug-ins, content, or restore types use only one method to locate backups. The guide for each plug-in provides details on which methods are available.

NOTICE

Avamar generally supports the use of specific supported international characters in directory, folder, and filenames. However, proper display of international language characters is contingent on the client computer's Java locale and installed system fonts being compatible with the original language. If you browse backups that were created with international characters and a compatible font is not installed, then any characters that cannot be resolved by the system appear as rectangles. This is a normal limitation of that particular situation and does not affect the ability to restore these directories, folders, or files. The *EMC Avamar Release Notes* provide additional international language support information.

The following topics provide details on finding a backup for a restore:

- "When to find a backup by date" on page 99
- "How to find a backup by date" on page 99
- "When to find a backup by file or folder" on page 100
- "How to find a backup by file or folder" on page 100

When to find a backup by date

Locate backups by date when:

- All data that the client backs up, such as databases, storage groups, or volumes, is backed up in a single backup set.
- The exact path or name of the file, folder, or database you want to restore is unknown.
- The content from a backup you want to restore is before a specific date or event. For example, you know approximately when a file or folder was lost or corrupted, and need to find the last backup before that date.
- The specific types of backups are known. For example, you run scheduled disaster recovery backups every Wednesday and Saturday night, and you run full volume backups daily. If you need to rebuild a server, you can select the disaster recovery backup with the date closest to the event that caused the loss of data.

How to find a backup by date

To find backups for a restore by date:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Restore** tab.
3. In the clients tree, select the client.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

4. Click the **By Date** tab.
5. Select a backup from the calendar:

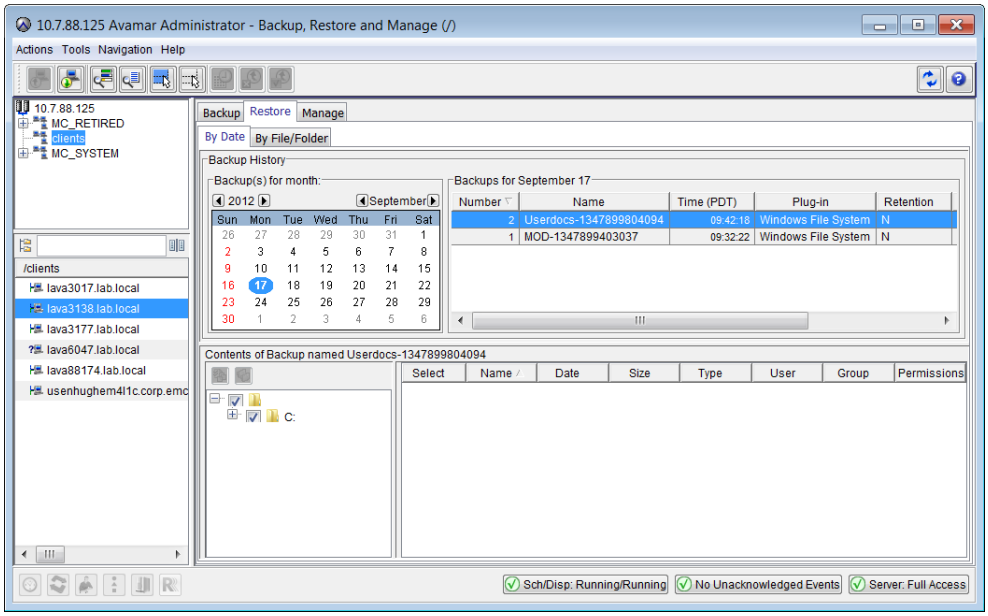
   a. Use the year and month navigational arrows to browse to a backup.

      Dates highlighted by yellow indicate a valid backup was performed on that date.

   b. Click a date highlighted by yellow.

   A list of backups that were performed on that date appears in the Backups table next to the calendar.

6. Select the backup to restore from the **Backups** table.



7. Select the data to restore from the **Contents of Backup** pane.
8. If you browse the client file system, specify a valid client username and password, then click **OK**.

   The username and password must have read permissions on the files and directories that you select for restore.
9. Select **Actions** › **Restore Now**.

When to find a backup by file or folder

Locate backups by the specific files or folders contained within each backup when:

- Data that the client backs up, such as databases, storage groups, or volumes, is backed up in separate backup sets. For example, you know that \\Server_Name\Databases\Database_1 is backed up in one backup set and \\Server_Name\Databases\Database_2 is backed up in another backup set. If you know the content you need is in Database_2, or is the entire Database_2 database, then you can specify the path or browse to the Database_2 folder.
- You want to see multiple versions of the same file.
- The date of the backup or what was saved in a backup is unknown, but you know the name of the file or folder.

How to find a backup by file or folder

To find a backup by specific files or folders in that backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. Click the **Restore** tab.

3. In the clients tree, select the client.

   You cannot view clients outside the domain for the login account. To view all clients, log in to the root domain.

4. Click the **By File/Folder** tab.

5. In the **Enter path to retrieve history for** text box, specify the path to the file or folder using one of the methods in the following table.

Table 14 Methods to browse to a backup by file or folder

Method	Steps
Type the path to the file or folder	Type the full path to the client directory or file in the **Enter path to retrieve history for** text box.
Browse to the file or folder	1. Click **Browse**. The Select File or Folder window appears. 2. Select the client. 3. Select the plug-in. A list of folders appears in a table to the right of the plug-ins pane. 4. Select the file or folder to restore. 5. Click **OK**. The selected file or folder appears in the Enter path to retrieve history for text box.

6. Click **Retrieve**.

   The Version History table lists all versions and sizes for that directory or file that have been backed up from the selected client.

7. Select the directory or file version in the **Version History** table.

   All backups for the selected client that contain the selected version appear in the Backups table next to the Version History table.

8. Select the backup to restore from the **Backups** table.

9. Select the data to restore from the **Contents of Backup** pane.

10. If you browse the client file system, specify a valid client username and password, then click **OK**.

    The username and password must have read permissions on the files and directories that you select for restore.

11. Select **Actions** › **Restore Now**.

Restoring to the original location

To restore backup data to its original location:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Restore** tab.

3. Locate and select a backup from which to restore data, as discussed in the following topics:
   - "How to find a backup by date" on page 99
   - "How to find a backup by file or folder" on page 100
4. Select **Actions** › **Restore Now**.

   The Restore Options dialog box appears.
5. Leave the default selection of the original client in the **Restore Destination Client** box.
6. Leave the default selection of the original backup plug-in in the **Restore Plug-in** list.
7. Select the encryption method to use for client/server data transfer during the restore.

   The exact encryption technology and bit strength used for a client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
8. Select **Restore everything to its original location**.
9. To include plug-in options with this restore, click **More Options**, and then configure the settings. The user guide for each plug-in provides details on each plug-in option.
10. Click **OK** on the **Restore Options** dialog box.

    The Restore Request dialog box indicates that the restore was initiated.
11. Click **Close**.

Restoring to a different location

To restore backup data to a single different location:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. Click the **Restore** tab.
3. Locate and select a backup from which to restore data, as discussed in the following topics:
   - "How to find a backup by date" on page 99
   - "How to find a backup by file or folder" on page 100
4. Select **Actions** › **Restore Now**.

   The Restore Options dialog box appears.

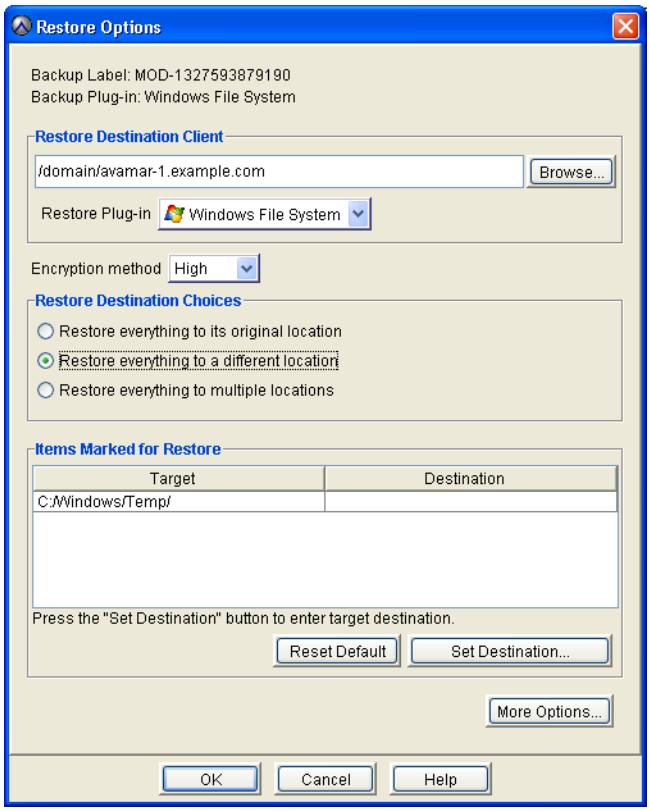
5. Select the destination client for the data to restore:
   - To restore to a different location on the same client, leave the default selection of the original client in the **Restore Destination Client** box.
   - To restore to a different client:
     a. Click the **Browse** button next to the **Restore Destination Client** box.

        The Browse for Restore Client dialog box appears.

     b. Browse to and select the destination client.

     c. Click **OK**.
6. Select the plug-in to use for the restore from the **Restore Plug-in** list.
7. Select the encryption method to use for client/server data transfer during the restore.

   The exact encryption technology and bit strength used for a client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
8. Select **Restore everything to a different location**.

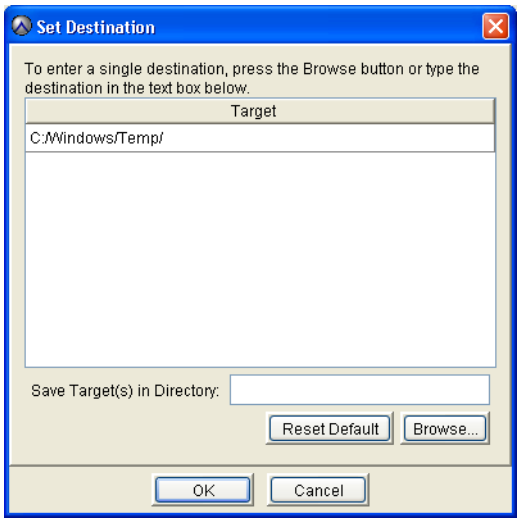


NOTICE

When you restore a single directory to a different location, Avamar restores only the contents of the directory. Avamar does not restore the original parent directory. However, if you restore two or more directories to a different location, then Avamar restores the original parent directories along with the contents of those directories.

9. Select the destination directory on the client for the data to restore:
   a. Click **Set Destination** below the **Items Marked for Restore** list.

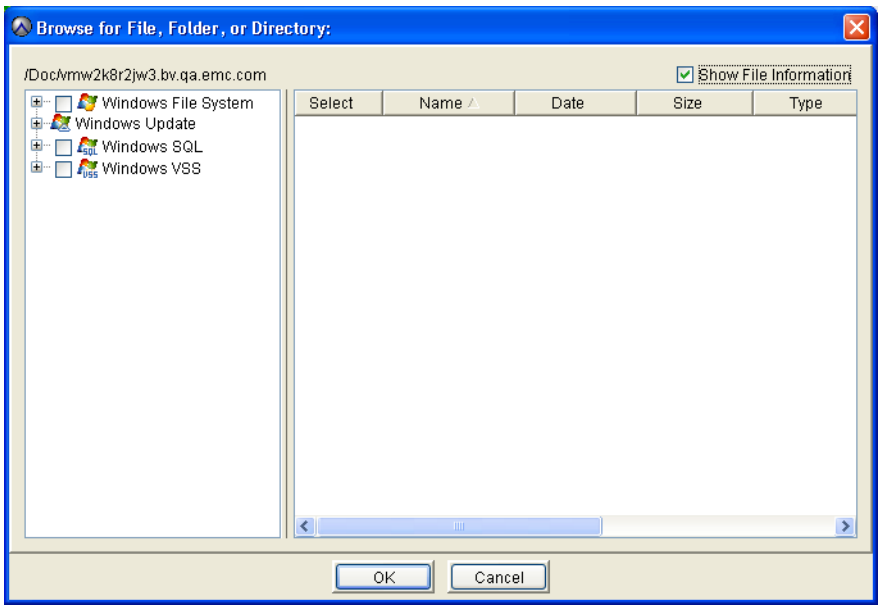
      The Set Destination dialog box appears.



   b. Type the path to the destination directory in the **Save Target(s) in Directory** box, or click **Browse** to browse to a directory.

      If you type a path and the directory does not already exist, then the restore process creates the directory.

      If you click Browse, then the Browse for File, Folder, or Directory dialog box appears, as shown in the following example.



   c. If you typed a path to the destination directory, then proceed to step f . Or, if you are browsing to a directory, then select the node for the plug-in in the left pane of the **Browse for File, Folder, or Directory** dialog box.

   d. Select the checkbox next to the target location.

e. Click **OK** on the **Browse for File, Folder, or Directory** dialog box.

   The target location appears in the Save Target(s) in Directory box.

f. Click **OK** on the **Set Destination** dialog box.

   When a file with the same name already exists in the path to which you are restoring a file, use the **Overwrite Existing Files** option on the **Restore Command Line Options** dialog box to control whether the restore process overwrites the file.

10. To include plug-in options with this restore, click **More Options**, and then configure the settings. The user guide for each plug-in provides details on each option.
11. Click **OK** on the **Restore Options** dialog box.

    The Restore Request dialog box indicates that the restore was initiated.

12. Click **Close**.

Restoring to multiple locations

To restore backup data to multiple locations on a destination client:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Restore** tab.
3. Locate and select a backup from which to restore data, as discussed in the following topics:

   - "How to find a backup by date" on page 99
   - "How to find a backup by file or folder" on page 100

4. Select **Actions** › **Restore Now**.

   The Restore Options dialog box appears.

5. Select the destination client for the data to restore:

   - To restore to multiple different locations on the same client, leave the default selection of the original client in the **Restore Destination Client** box.
   - To restore to multiple locations on a different client:

     a. Click the **Browse** button next to the **Restore Destination Client** box.

        The Browse for Restore Client dialog box appears.

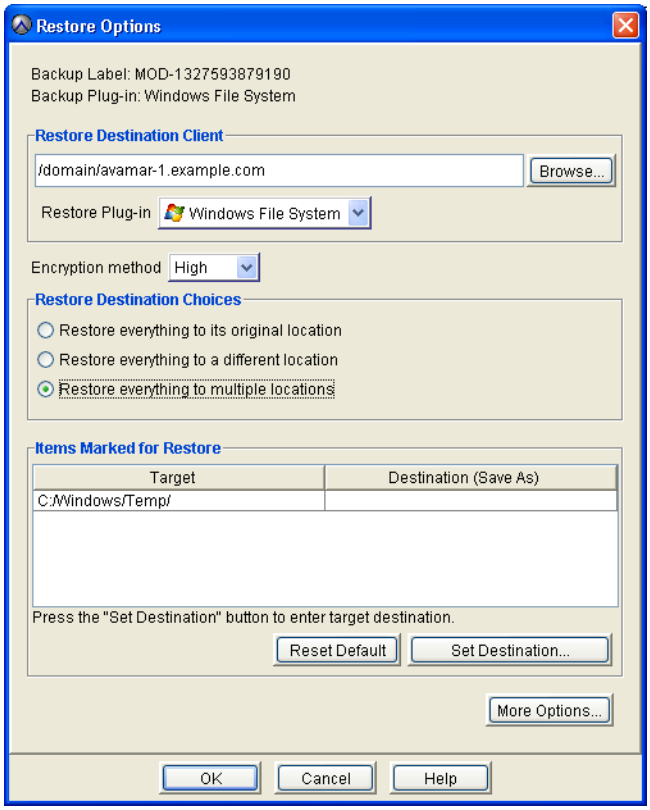
     b. Browse to and select the destination client.

     c. Click **OK**.

6. Select the plug-in to use for the restore from the **Restore Plug-in** list.
7. Select the encryption method to use for client/server data transfer during the restore.

   The exact encryption technology and bit strength used for a client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

8. Select **Restore everything to multiple locations.**



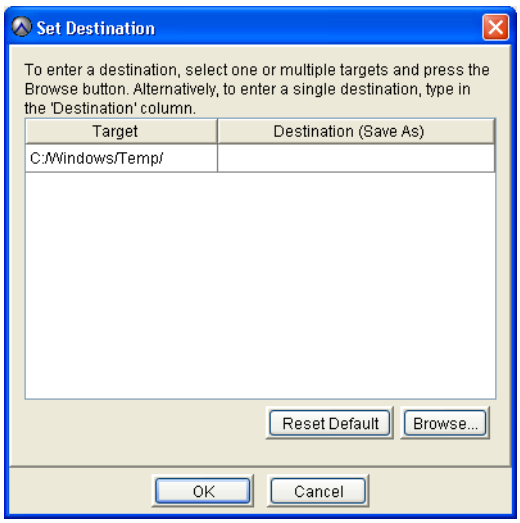
NOTICE

When you restore a single directory to a different location, Avamar restores only the contents of the directory. Avamar does not restore the original parent directory. However, if you restore two or more directories to a different location, then Avamar restores the original parent directories along with the contents of those directories.

9. Select the destination directories on the client for the data to restore:

   a. Click **Set Destination** below the **Items Marked for Restore** list.

      The Set Destination dialog box appears.

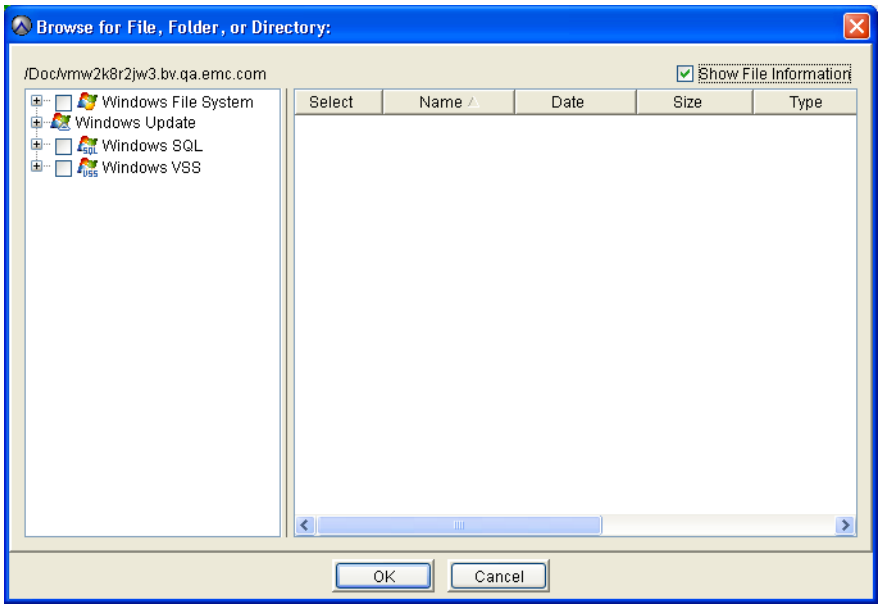


b. Select a row in the list.

c. Type the path to the destination directory in the **Destination (Save As)** column in the list, or click **Browse** to browse to a directory.

If you type a path and the directory does not already exist, then the restore process creates the directory.

If you click Browse, then the Browse for File, Folder, or Directory dialog box appears, as shown in the following example.



d. If you typed a path to the destination directory, then proceed to step g . Or, if you are browsing to a directory, then select the node for the plug-in in the left pane of the **Browse for File, Folder, or Directory** dialog box.

e. Select the checkbox next to the target location.

f. Click **OK** on the **Browse for File, Folder, or Directory** dialog box.

The target location appears next to the target in the list.

g. Repeat step b through step f for each row in the list on the **Set Destination** dialog box.

h. Click **OK** on the **Set Destination** dialog box.

When a file with the same name already exists in the path to which you are restoring a file, use the **Overwrite Existing Files** option on the **Restore Command Line Options** dialog box to control whether the restore process overwrites the file.

10. To include plug-in options with this restore, click **More Options**, and then configure the settings. The user guide for each plug-in provides details on each plug-in option.

11. Click **OK** on the **Restore Options** dialog box.

The Restore Request dialog box indicates that the restore was initiated.

12. Click **Close**.

Managing backups

After you perform an on-demand or scheduled backup, you can perform several management tasks with the backup, including changing the backup expiration date or retention type, or validating a backup. You also can view backup statistics or delete a backup.

The following topics explain how to manage backups:

- "Understanding backup expiration and deletion" on page 108
- "Finding a backup to manage" on page 108
- "Changing a backup expiration date" on page 110
- "Changing backup retention types" on page 111
- "Validating a backup" on page 112
- "Viewing backup statistics" on page 113
- "Deleting a backup" on page 116

Understanding backup expiration and deletion

An Avamar backup is represented as a hierarchical tree structure with the tip of the tree containing a root hash that points to the highest level of the backup.

The data contained in a backup is referenced by starting at the top of the tree and recursively moving down the tree until it reaches the data. The process for traversing the data contained in a backup is similar to traversing a directory tree to files.

When a backup expires, the root hash of the tree is deleted. At this point, Avamar users cannot recover data from the expired backup. A garbage collection process then runs on a nightly basis to clean up and reclaim space left over from orphaned data (data that is unique to the backups being expired) for backups that have previously expired.

Finding a backup to manage

There are three ways to find a backup to manage:

- "Finding a backup by calendar date" on page 109
- "Finding a backup by date range" on page 109
- "Finding a backup by retention type" on page 109

NOTICE

Avamar generally supports the use of specific supported international characters in directory, folder, and filenames. However, proper display of international language characters is contingent on the client computer Java locale and installed system fonts being compatible with the original language. When you browse backups that were created with international characters and a compatible font is not installed, any characters that cannot be resolved by the system appear as rectangles. This is a normal limitation of that particular situation and does not affect the ability to restore these directories, folders, or files. The *EMC Avamar Release Notes* provide additional international language support information.

Finding a backup by calendar date

To find a backup on a specific calendar date:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. In the clients tree, browse to and select the client with the backups to manage.
3. Click the **Manage** tab.
4. Select **By day**.
5. Select a backup from the calendar:
   a. Use the year and month navigational arrows to browse to a backup.

      Dates highlighted by yellow indicate a valid backup was performed on that date.
   b. Click a date highlighted by yellow.

   A list of backups that were performed on that date appears in the Backup History list.

Finding a backup by date range

To find a backup within a range of dates:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. In the clients tree, browse to and select the client with the backups to manage.
3. Click the **Manage** tab.
4. Select **By date range**.
5. Click the **From Date** list, and browse the calendar for the start date for the range.
6. Click the **To Date** list, and browse the calendar for the end date for the range.
7. Click **Retrieve**.

   A list of backups during the date range appears in the Backup History list.

Finding a backup by retention type

To find a backup with a certain retention type:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.
2. In the clients tree, browse to and select the client with the backups to manage.
3. Click the **Manage** tab.
4. Select **By retention**.
5. Select the checkbox next to the retention type for the backup.
6. Click **Retrieve**.

   A list of backups with the retention type appears in the Backup History list.

Changing a backup expiration date

To change the expiration date for a backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Manage** tab.

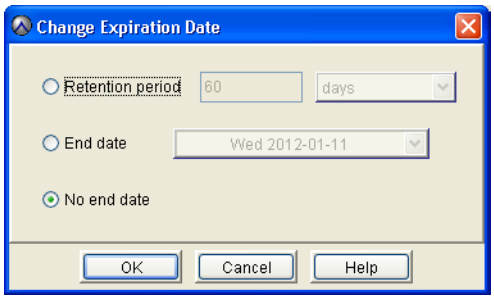
3. Find a backup to manage, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 109
   - "Finding a backup by date range" on page 109
   - "Finding a backup by retention type" on page 109.

4. In the **Backup History** list, select the backup to manage. To select multiple backups, press **Ctrl** while you select the backups.

5. Select **Actions** › **Change Expiration Date**.

   The Change Expiration Date dialog box appears.



6. Select the new expiration date:

   - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period** and then specify the number of days, weeks, months, or years for the retention period.
   - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
   - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.

7. Click **OK**.

   A confirmation message appears.

8. Click **Yes**.

   An event code dialog box appears.

9. Click **OK**.

10. Click **OK** on the confirmation message.

Changing backup retention types

To support certain advanced features, Avamar Administrator automatically assigns one or more retention types to every backup. For example, the first backup created on an Avamar system is tagged as a daily, weekly, monthly, or yearly. You can manually change the retention types assigned to a backup.

When you manually change the retention types assigned to a backup, especially one that has multiple retention types, be certain that you are not inadvertently removing a weekly, monthly, or yearly backup that you need to retain. For example, consider a backup that is assigned daily, weekly, monthly, and yearly retention types. If you remove the yearly retention type designation, you might not have another yearly backup in the system for quite a long time.

To change the retention types assigned to a backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Click the **Manage** tab.

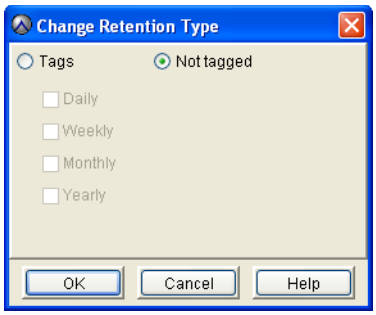
3. Find a backup to manage, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 109
   - "Finding a backup by date range" on page 109
   - "Finding a backup by retention type" on page 109.

4. In the **Backup History** list, select the backup to manage. To select multiple backups, press **Ctrl** while you select the backups.

5. Select **Actions** › **Change Retention Type**.

   The Change Retention Type dialog box appears.



6. Select one of the following retention types for the backups:

   - To explicitly assign a daily, weekly, monthly or yearly retention type to this backup, select **Tags** and then select the checkbox next to the retention types.
   - If you do not want to explicitly assign a daily, weekly, monthly, or yearly retention type to the backup, select **Not tagged**. The backup is designated as untagged.

7. Click **OK**.

   A confirmation message appears.

8. Click **Yes**.

   A second confirmation message appears.

9. Click **OK**.

Validating a backup

You can verify that files can be restored from a backup. This validation initiates a "virtual" restore of all files in the backup, but does not actually restore any files to the client file system.

To validate a backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

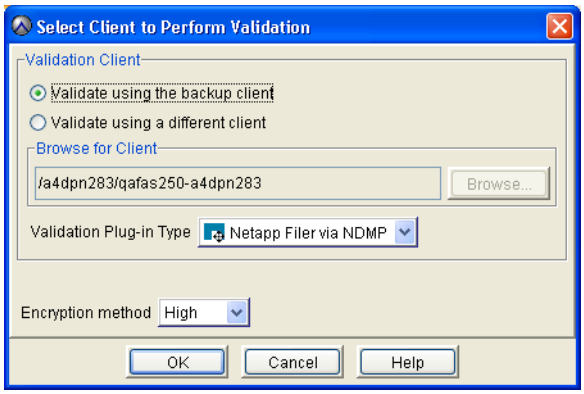
2. Find a backup to validate, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 109
   - "Finding a backup by date range" on page 109
   - "Finding a backup by retention type" on page 109.

3. In the **Backup History** list, select the backup to validate.

4. Select **Actions** › **Validate Backup**.

   The Select Client to Perform Validation dialog box appears.



5. Select the client on which to validate the backup:

   - To validate the backup on the same client from which the backup was originally performed, select **Validate using the backup client**.
   - To validate the backup on a different client, select **Validate using a different client**, and then click **Browse** to browse to the client.

6. From the **Validation Plug-in Type** list, select the plug-in on which to validate the backup. Only the plug-ins that are installed on the selected client appear in the list.

7. From the **Encryption method** list, select the encryption method to use for client/server data transfer during the validation.

   Note: The default encryption setting for backup validations is high, regardless of the encryption setting used for the original backup.

8. Click **OK**.

   A confirmation message appears.

9. Click **OK**.

Viewing backup statistics

You can view detailed statistics for completed backups from both the Backup Management window and the Activity window.

The Backup Management window provides statistics for any stored backup. However, the Activity window shows only recent backup activity. Typically, only the backups within the past 72 hours appear in the Activity window.

The same statistics appear for each backup, regardless of whether you view the statistics from the Backup Management window or the Activity window.

Viewing backup statistics from the Backup Management window

To view backup statistics from the Backup Management window:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

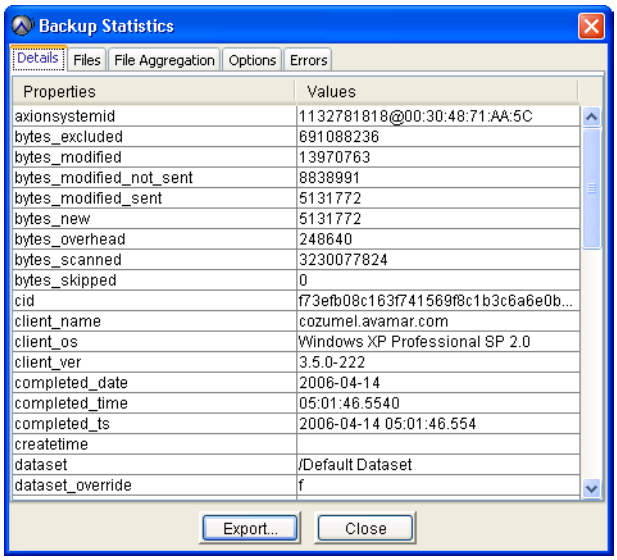
2. Find the backup, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 109
   - "Finding a backup by date range" on page 109
   - "Finding a backup by retention type" on page 109.

3. In the **Backup History** list, select the backup.

4. Select **Actions** › **View Statistics**.

   The Backup Statistics dialog box appears, as shown in the following example.



The following information appears on the tabs in the Backup Statistics dialog box.

Table 15 Backup Statistics dialog box tabs

Tab	Information
Details	Detailed information from the v_activities_2 database view, which is discussed in "v_activities_2" on page 603.
Files	A list of files included in the backup.
File Aggregation	A representative sampling of resource-intensive file types included in the backup, and aggregates deduplication statistics by file type.
Options	Any special options for the backup.
Errors	Any errors that occurred during the backup.

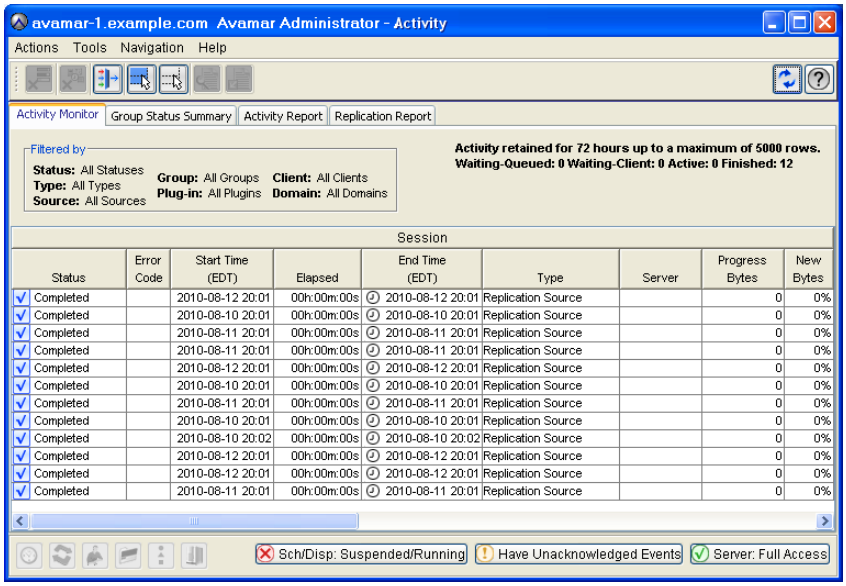
5. (Optional) To export the data on a tab of the **Backup Statistics** dialog box to a comma-separated values (.csv) file, click **Export** and then specify the location and filename for the file.
6. Click **Close**.

Viewing backup statistics from the Activity window

To view backup statistics from the Activity window:

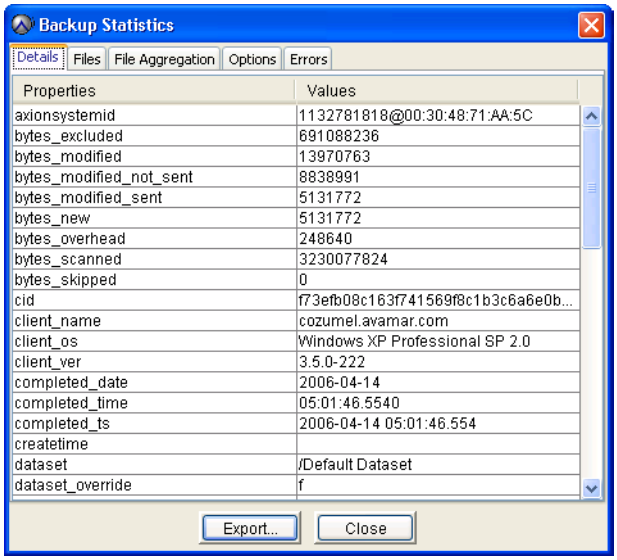
1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.



2. Click the **Activity Monitor** tab.
3. Select a backup activity from the list.
4. Select **Actions** › **View Statistics**.

The Backup Statistics dialog box appears, as shown in the following example.



The following information appears on the tabs in the Backup Statistics dialog box.

Table 16 Backup Statistics dialog box tabs

Tab	Information
Details	Detailed information from the v_activities_2 database view, which is discussed in "v_activities_2" on page 603.
Files	A list of files included in the backup.
File Aggregation	A representative sampling of resource-intensive file types included in the backup, and aggregates deduplication statistics by file type.
Options	Any special options for the backup.
Errors	Any errors that occurred during the backup.

5. (Optional) To export the data on a tab of the **Backup Statistics** dialog box to a comma-separated values (.csv) file, click **Export** and then specify the location and filename for the file.
6. Click **Close**.

Deleting a backup

When you delete a backup, Avamar immediately and permanently deletes all data in that backup from the server.

To delete a backup:

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The Backup, Restore and Manage window appears.

2. Find the backup to delete, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 109
   - "Finding a backup by date range" on page 109
   - "Finding a backup by retention type" on page 109.

3. In the **Backup History** list, select the backup to delete.

4. Select **Actions** › **Delete Backup**.

   A confirmation message appears.

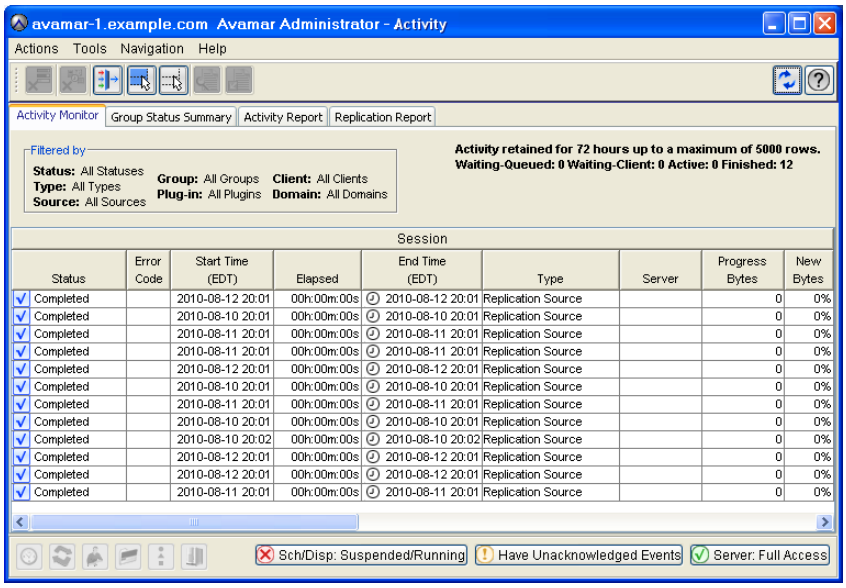
5. Click **OK**.

Monitoring backup, restore, or validation activities

To monitor backup, restore, and validation activities:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.



2. Click the **Activity Monitor** tab.

   By default, the Activity Monitor tab shows the most recent 5,000 client activities during the past 72 hours.

NOTICE

You can increase or reduce the amount of information shown in the backup activity monitor by manually editing the com.avamar.mc.wo completed_job_retention_hours preference in the /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml file, and then restarting the MCS.

The following table describes the information shown in the Activity window.

Table 17 Activity Monitor tab columns (page 1 of 4)

Column	Description
Session	
Status	One of the following: • **Canceled** —The activity was canceled, either by the client or from Avamar Administrator. • **Client Backup Disabled** —Backups are disabled for one or more group members. • **Client Not Registered**— One or more group members are not activated with the Avamar server. • **Completed** —The activity successfully completed. • **Completed w/ Exception(s)**—The activity completed with errors. Double-click the entry to view the full error log, which contains the activity failure codes. • **Config Files** • **Dropped Session** —The activity was successfully initiated, but because MCS could not detect any progress, the activity was forcefully canceled. • **Duplicate VM Targets** • **Expiration in past** • **Failed** —The client failed to perform the activity; the activity ended in an error condition. Double-click the entry to view the full error log, which contains the activity failure codes. • **Fault Tolerant** —The backup failed because the virtual machine client is running in fault tolerance mode. To back up this virtual machine while in fault tolerance mode, install the correct type and version of Avamar client software and use guest backups to protect the data. • **Hard limit exceeded** —The client's hard limit for backup data size was exceeded and the backup was canceled. • **No Client Contact** —The scheduled client did not check in. • **No Data** —The dataset did not define any data to back up, or the client does not have matching data to back up. • **No proxy** —The system failed to initiate a backup or restore for a virtual machine because no proxy was found to service the virtual machine. Verify that proxy clients have the datastores checked for protection. The selected proxy client datastores must match the datastores for virtual machines requiring protection. Additionally, for scheduled group backups, verify that the group has the proxies checked for protection of virtual machines belonging to the group. Verify that proxy clients are powered on, enabled, and registered. For restores, verify that there is an available proxy in the destination datacenter.

Table 17 Activity Monitor tab columns (page 2 of 4)

Column	Description
Status - continued	• **No Status** —The activity is not progressing as expected and the Avamar server cannot provide status. • **No vm** —The activity failed because the virtual machine client does not exist in vCenter. • **Option Incompatibility** —The activity failed due to the specification of an incompatible plug-in option. This is often occurs when you use an older client version that does not support a particular plug-in option. • **Partial Replication** • **Plug-in Disabled** —All operations have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 263 provides details. • **Restore Disabled** —All restore operations have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 263 provides details. • **Retention date expired** —The backup failed because the retention policy has already expired. In other words, the retention policy is set to a past date. • **Running** —The client is performing the activity. • **Scheduled Backup Disabled** —All scheduled backups have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 263 provides details. • **Stalled** —The activity is not progressing as expected. Because the Avamar server can provide status, the problem is assumed to be on the client. • **Suspended** —The activity has been suspended (work order suspended). • **Timed Out - End** —The client did not complete the activity in the allotted time. • **Timed Out - Response** —The client checked in and was sent backup activity but did not acknowledge. • **Timed Out - Start** —The activity failed to start (work order start time-out). • **Undefined** —The activity does not have a work order associated with it. • **Unknown** —The activity was passed an unknown exit code from the client agent. • **Unsupported backup** —Some aspect of this backup activity is not supported. For example, attempting to back up a VMware proxy client with a VMware Image backup dataset returns a status of Unsupported. • **Unsupported Number of Targets** —Backup dataset has defined more backup targets than plug-in supports. • **Validate Disabled** —All backup validation operations have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 263 provides details. • **Waiting** —The server is waiting for the client to initiate this activity.
Error Code	If the activity did not successfully complete, a numeric error code appears. Double-click the error code to view a detailed explanation.
Start Time	Date and time that this activity was initiated, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.
Elapsed Time	Elapsed time for this activity.

Table 17 Activity Monitor tab columns (page 3 of 4)

Column	Description
End Time	Date and time that this activity completed, adjusted for the prevailing time zone, which is shown in parentheses. Daylight Savings Time (DST) transitions are automatically compensated.
Type	This activity is one of the following: • **On-demand backup** • **Restore** • **Validate** • **Scheduled backup** • **Capacity Report** • **Replication Source** • **Replication Destination** • **Export** —backups are being exported to long-term storage media • **Import**—backups are being imported from long-term storage media • **Upgrade**—system is being upgraded as described in the *EMC Avamar System Upgrade Guide* **Notice:** Replication and long-term storage media are optional features that might not be available to all users.
Server	Server on which the activity occurred—either the Avamar server or a Data Domain system.
Progress Bytes	Total number of bytes examined during this activity.
New Bytes	Percentage of new bytes backed up to either the Avamar server or a Data Domain system. Low numbers indicate high levels of data deduplication.
Client	
Client	Avamar client name.
Domain	Full location of the client in the Avamar server.
OS	Client operating system.
Client Release	Avamar client software version. **Notice:** If this activity is a VMware image backup or restore, this is Avamar client software version running on the image proxy client.
Proxy	If this activity is a VMware image backup or restore, this is the name of the proxy client performing the backup or restore on behalf of the virtual machine. Blank for all other activities.
Policy	
Sched. Start Time	Date and time that this activity was scheduled to begin.
Sched. End Time	Date and time that this activity was scheduled to end.
Elapsed Wait	Total amount of time that this activity spent in the activity queue. That is, the scheduled start time minus the actual start time.

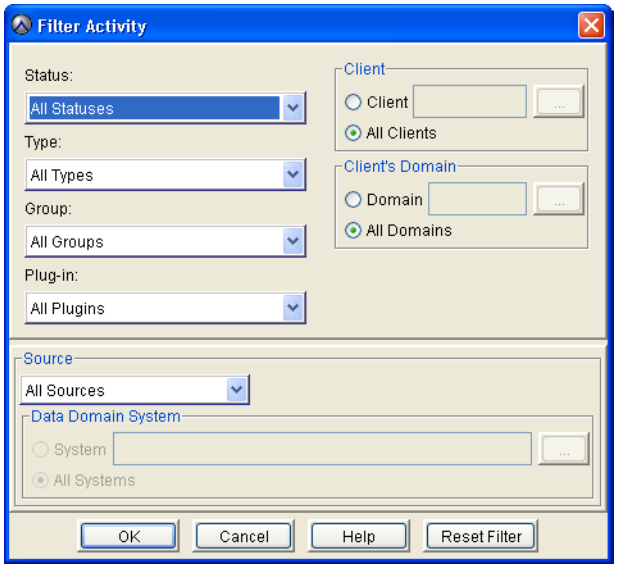
Table 17 Activity Monitor tab columns (page 4 of 4)

Column	Description
Group	Group that initiated this activity. One of the following: • If the activity was a scheduled backup, this is the group that this client was a member of when this scheduled activity was initiated. • **On-demand** is shown for other backup, restore and validation activities. • If the activity was a scheduled replication, this is the replication group. • **Admin On-Demand Group** is shown for-demand replication activities.
Plug-in	Plug-in used for this activity.
Retention	Retention types assigned to this backup. One or more of the following: • **D**—Daily • **W**—Weekly • **M**—Monthly • **Y**—Yearly • **N**—No specific retention type "Advanced retention settings" on page 148 provides additional information about advanced retention types.
Schedule	If the activity was a scheduled backup, this is the schedule that initiated this activity. On-Demand or End User Request is shown for all other activities initiated from Avamar Administrator or the client, respectively.
Dataset	Name of the dataset used to take the backup. If the activity is a replication job, this column lists the source system name on the destination system, and the destination name on the source system.
WID	Work order ID. Unique identifier for this activity.

3. (Optional) Filter the information in the **Activity Monitor** tab of the **Activity** window to show only activities with a specific state, type, group, client, or plug-in:

   a. Select **Actions** › **Filter**.

      The Filter Activity dialog box appears.



   b. Define the filtering criteria and click **OK**.

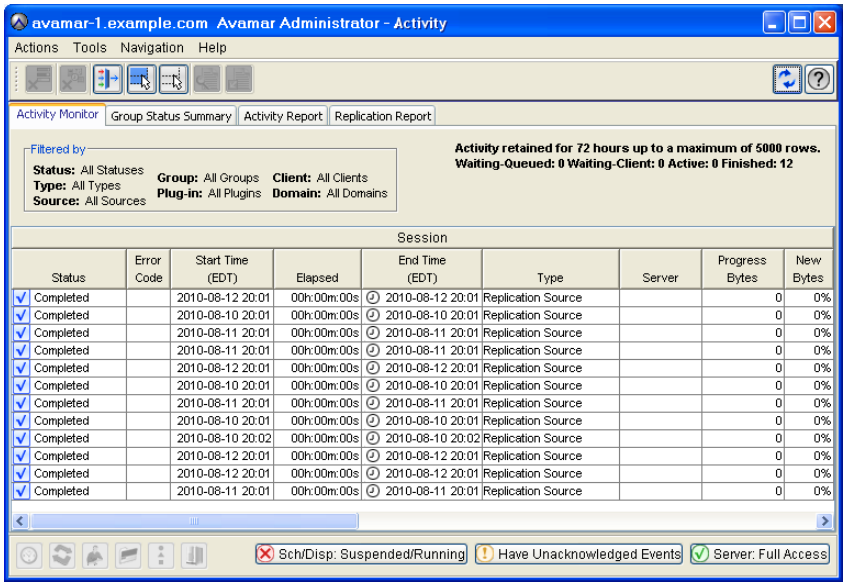
Canceling a backup, restore, or validation

You can cancel a backup, restore, or validation activity any time before it completes. However, it can take as many as five minutes to complete the cancellation. If the activity completes during this time, the cancellation does not occur.

To cancel an activity:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.



2. Click the **Activity Monitor** tab.

   The most recent 5,000 client activities during the past 72 hours appear on the Activity Monitor tab.

3. Select the activities to cancel.

4. Select **Actions** › **Cancel Activity**.

   A confirmation message appears.

5. Click **Yes**.

CHAPTER 5
Datasets, Schedules, and Retention Policies

Datasets, schedules, and retention policies are reusable objects that you can assign to more than one client or group. This reusability greatly reduces the amount of labor needed to automate and customize the Avamar server. The following topics describe how to create and manage Avamar datasets, schedules, and retention policies:

- Datasets 124
- Schedules 134
- Retention policies 147

Datasets

When you perform an on-demand backup, the selection of directories and files in a client file system for the backup is valid only for that backup. In other words, it is not saved for future backups.

Avamar datasets are a list of directories and files to back up from a client. Assigning a dataset to a client or group enables you to save backup selections.

Understanding datasets

Each dataset defines:

- Source data list
- Exclusion list
- Inclusion list
- Plug-in options

Source data list

Dataset definitions start with a source data list that consists of:

- Data from one or more plug-ins
- A defined file system hierarchy, either the entire file system or selected directories, within each plug-in

Exclusion and inclusion lists

Datasets can also narrow the scope of the source data list by explicitly defining certain directories and file types to exclude or include in each backup.

Because default dataset behavior is to include everything in the source data list, the explicit exclusion and inclusion lists typically contain only a few entries.

When you specify exclusions and inclusions, case-sensitivity varies according to the target computing platform for the backup. Exclusions and inclusions for Windows platforms are not case-sensitive, while exclusions and inclusions for most other platforms are case-sensitive.

NOTICE

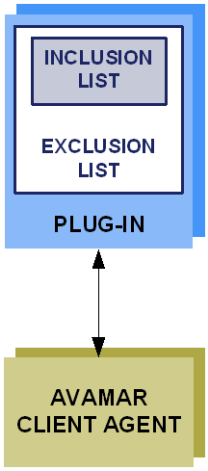
You cannot define inclusion and exclusion lists for VMware Image Backups.

Processing relationship

Avamar processes these dataset elements in the following order:

1. **Source data**—Source data from one or more plug-ins is defined. The default behavior is to include all data from all defined plug-ins.
2. **Exclusion list—**Next, the exclusion list is used to eliminate certain directories and file types from the dataset.
3. **Inclusion list**—Finally, the inclusion list is used to add back any files that were eliminated from the dataset in the exclusion list.

The following figure illustrates the processing relationship:



Plug-in options

Plug-in options enable you to further customize the behavior of a dataset. The user guide for each plug-in provides details on the options available for the plug-in.

Dataset catalog

The datasets in the following topics are available by default.

Base Dataset

The Base Dataset defines a set of minimum, or baseline, backup requirements. The initial settings in the Base Dataset are:

- No source data plug-ins
- No explicit exclusion or inclusion list entries

This is essentially an empty dataset.

Default Dataset

The Default Dataset defines persistent backup selections for the Default Group, which is described in "Default Group" on page 156. The initial settings in the Default Dataset are:

- All available source data plug-ins
- No explicit exclusion or inclusion list entries

This ensures that all members of the Default Group can back up their client computers regardless of platform type.

If you edit these settings, the changes are enforced on all members of the Default Group, unless another dataset is assigned at the client level as described in "Overriding group policy settings for a single client" on page 171.

The directories listed in the following table are also inherently excluded from all backups, even though they do not explicitly appear in the exclusion list.

Table 18 Directories excluded from Default Dataset backups

Exclusion	Description
.snapshot/	NetApp mounts
VARDIR/f_cache.dat	Local **avtar** file cache
VARDIR/p_cache.dat	Local **avtar** "is present" cache

Unix Dataset

The Unix Dataset is optimized for use with AIX, FreeBSD, HP-UX, Linux, and Solaris clients. The initial settings in the Unix Dataset are:

- Only the AIX, FreeBSD, HP-UX, Linux, Macintosh OS X, and Solaris file system source data plug-ins
- Explicit exclusion of various temp directories (/tmp, /var/tmp, /usr/tmp), core dump files (core), and local cache files (*cache.dat, *scan.dat)
- No explicit inclusion list entries

The directories listed in the following table are also inherently excluded from all Unix Dataset backups, even though they do not explicitly appear in the exclusion list.

Table 19 Directories excluded from Unix Dataset backups

Exclusion	Description
.snapshot/	NetApp mounts
VARDIR/f_cache.dat	Local **avtar** cache files
VARDIR/p_cache.dat	Local **avtar** cache files
/proc	Pseudo file system that cannot be restored
/dev	Excluded only if not running as root
/devices	Excluded only for Solaris

Windows Dataset

The Windows Dataset is optimized for use with Microsoft Windows clients. The initial settings in the Windows Dataset are:

- Only Windows file system source data plug-in
- No explicit exclusion or inclusion list entries

The directories listed in the following table are also inherently excluded from all Windows Dataset backups, even though they do not explicitly appear in the exclusion list.

Table 20 Directories excluded from Windows Dataset backups

Exclusion	Description
.snapshot/	NetApp mounts
VARDIR/f_cache.dat	Local **avtar** cache files
VARDIR/p_cache.dat	Local **avtar** cache files
All files referenced by the following registry keys: • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup • HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Files explicitly designated by Microsoft to exclude from backups
Temporary Internet files	Internet Explorer temporary files
outlook.ost	Outlook local cache files
outlook*.ost	Outlook local cache files

VMware Image Dataset

The VMware Image Dataset is the default dataset that is assigned to the Default Virtual Machine Group and other vCenter groups when they are first added. "Default Virtual Machine Group" on page 156 and "vCenter groups" on page 157 provide details.

In many respects, the VMware Image Dataset is simpler than most other datasets:

- The only available source data plug-ins are Linux and Windows virtual disks, and both are selected by default.
- The Select Files and/or Folders option, as well as the Exclusions and Inclusions tabs, are disabled.
- Change block tracking is enabled by default using an embedded utilize_changed_block_list=true plug-in option statement.

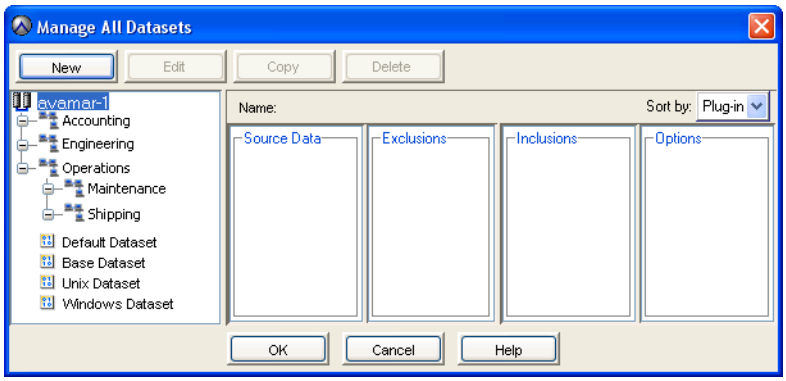
The *EMC Avamar for VMware User Guide* provides details on using the VMware Image Dataset to back up virtual machine data.

Creating a dataset

To create a dataset:

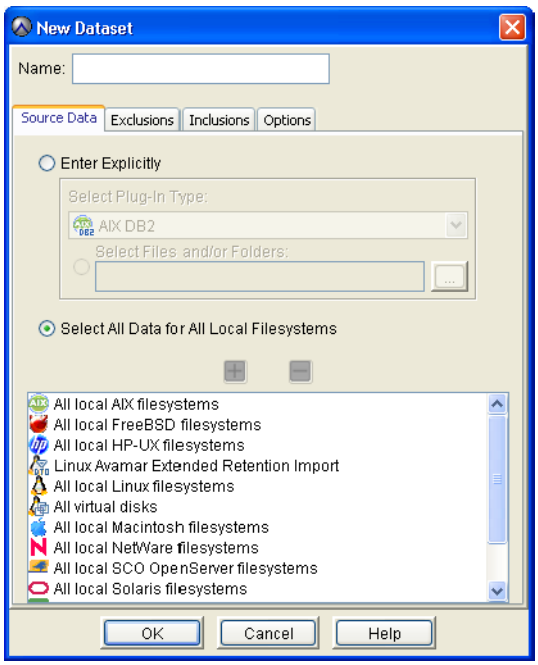
1. In Avamar Administrator, select **Tools** › **Manage Datasets**.

   The Manage All Datasets window appears.



2. Click **New**.

   The New Dataset dialog box appears.



3. Type a name for the dataset.

   Do not use any of the following characters in the dataset name: ~!@$^%(){}[]|,`;#\/:*?<>'"&.

4. Click the **Source Data** tab, and then define the source data plug-ins that contribute data to this dataset:
   - To include all plug-ins, select **Select All Data for All Local File Systems**. With this option, the dataset includes all data that is available using any of the plug-ins.
   - To include only specific plug-ins and limit the dataset to specific folders and files, select **Enter Explicitly**.
5. If you selected **Enter Explicitly** in the previous step, specify the plug-ins and data path:
   a. Remove all unwanted plug-ins from the list by selecting each one and clicking **-**.
   b. To add a plug-in, select the plug-in from the **Select Plug-In Type** list, and then click **+**.
   c. Specify a data path for the plug-in by clicking **Select Files and/or Folders**, browsing to or typing a valid data path for the plug-in, and then clicking +.

   NOTICE

   The Select Files and/or Folders option is not available for VMware Image Backups.

   For the following plug-ins, the first occurrence of an asterisk in a path is treated as a folder wildcard:

   - All local AIX file systems
   - All local FreeBSD file systems
   - All local HP-UX file systems
   - All local Linux file systems
   - All local Macintosh file systems
   - All local SCO OpenServer file systems
   - All local Solaris file systems
   - All local UnixWare file systems
   - All local Windows file systems

   For example, to specify the My Documents folder for all users on a Windows computer, type:

   ```
   C:\Documents and Settings\*\My Documents
   ```

   To specify the Documents folder for all users on a Macintosh, type:

   ```
   /Users/*/Documents
   ```

   NOTICE

   When you specify a data path, only the first occurrence of an asterisk is treated as a folder wildcard. Subsequent occurrences are interpreted literally.

   Except for using an asterisk character with the specified file system plug-ins, do not use any of the following characters in the data path: ~!@$^%(){}[]|,`;#:*?‹›'"&.

   To handle the change in the default location of user directories that occurred between Windows XP and Windows Vista/Windows 7, a dereference flag is available in the plug-in for all local Windows file systems.

The dereference flag acts as a substitute for the default location of user directories on those operating systems. The flag is:

#USERDOCS#

The following table provides examples of the dereference flag used in combination with the folder wildcard.

Table 21 Dereference flag and folder wildcard examples

Example	Entry that is replaced

`#USERDOCS#\*\Desktop`	On Windows XP:
	`C:\Documents and Settings\*\Desktop`
	
	On Windows Vista or Windows 7:
	`C:\Users\*\Desktop`

`#USERDOCS#\*\Favorites`	On Windows XP:
	`C:\Documents and Settings\*\Favorites`
	
	On Windows Vista/Windows 7:
	`C:\Users\*\Favorites`

`#USERDOCS#\*\Documents`	On Windows XP:
	`C:\Documents and Settings\*\Documents`
	
	On Windows Vista/Windows 7:
	`C:\Users\*\Documents`

`#USERDOCS#\*\My Documents`	On Windows XP:
	`C:\Documents and Settings\*\My Documents`
	
	On Windows Vista/Windows 7:
	`C:\Users\*\My Documents`

d. Repeat step b and step c for each plug-in and data path to include in the dataset.

6. Click the **Exclusions** tab, and then define the directories and files to exclude:

   a. Select a plug-in from the **Select Plug-in Type** list.

   b. Type a directory name or file type in the **Select Files and/or Folders** field. The entry may include wildcards.

   c. Click **+**.

   d. Repeat these steps for each exclusion.

   Typical exclusion lists include /temp files and directories and UNIX core dumps.

   NOTICE

   You cannot define exclusion lists for VMware Image Backups.

7. Click the **Inclusions** tab, and then define the directories and files to include because they would otherwise have been excluded by the exclusion list:
   a. Select a plug-in from the **Select Plug-in Type** list.
   b. Type a directory name or file type in the **Select Files and/or Folders** field. The entry may include wildcards.
   c. Click **+**.
   d. Repeat these steps for each inclusion.

   NOTICE

   You cannot define inclusion lists for VMware Image Backups.

   "Exclusion and inclusion lists" on page 124 provides details on inclusions.
8. Click the **Options** tab, and then set various plug-in options either by using the graphical controls or by typing option names and values as free text.

   NOTICE

   No error checking or validation is performed when you type option names and values as free text. In addition, free text entries override settings that you make using the graphical controls.

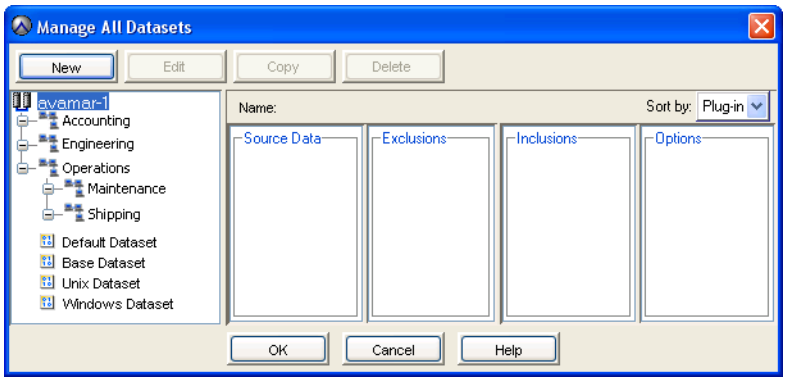
   The user guide for each plug-in provides details on the available options.
9. Click **OK**.

Editing a dataset

To edit a dataset:

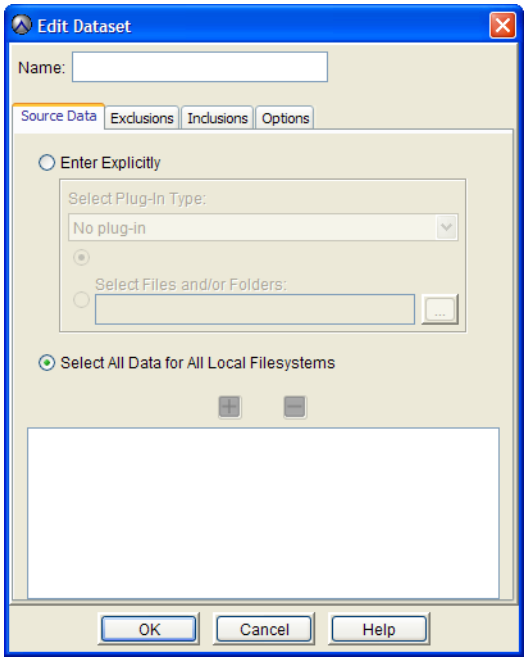
1. In Avamar Administrator, select **Tools** › **Manage Datasets**.

   The Manage All Datasets window appears.



2. Select a dataset and click **Edit**.

The Edit Dataset dialog box appears.



3. Edit the dataset information.

   "Creating a dataset" on page 128 provides details on dataset properties.

4. Click **OK**.

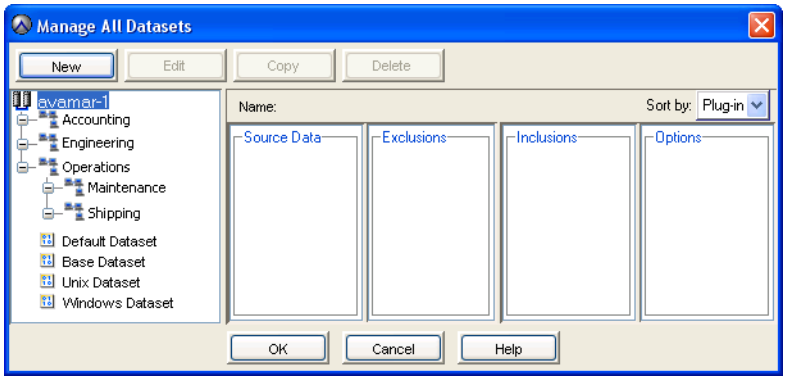
   Dataset changes take effect on the next scheduled backup. Backups that have already begun or have been completed are not affected.

Copying a dataset

To copy a dataset:

1. In Avamar Administrator, select **Tools** › **Manage Datasets**.

   The Manage All Datasets window appears.



2. Select the dataset and click **Copy**.

   The Save As dialog box appears.

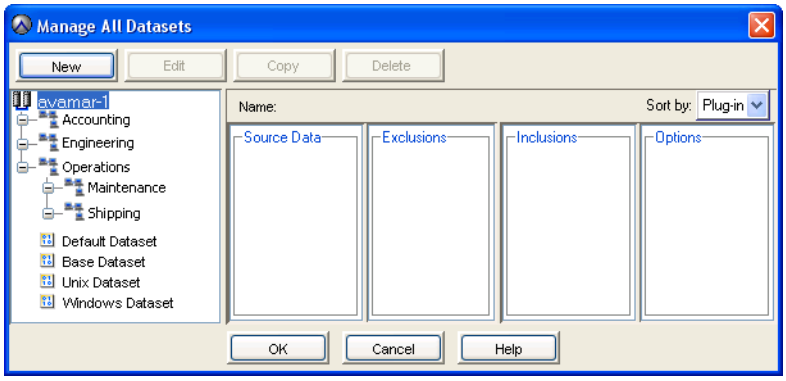
3. Type a name for the new dataset and click **OK**.

Deleting a dataset

To delete a dataset:

1. Ensure that the dataset is not currently assigned to a client or group. You cannot delete a dataset if it is currently assigned to a client or group.
2. In Avamar Administrator, select **Tools** › **Manage Datasets**.

   The Manage All Datasets window appears.



3. Select the dataset and click **Delete**.

   A confirmation message appears.
4. Click **Yes**.

Schedules

Schedules are reusable objects that control when the following activities occur:

- Group backups
- Custom event profile email notifications
- Policy-based replication

Understanding schedules

You can configure an Avamar schedule to repeat a system activity at one of the intervals listed in the following table.

Table 22 Schedule types

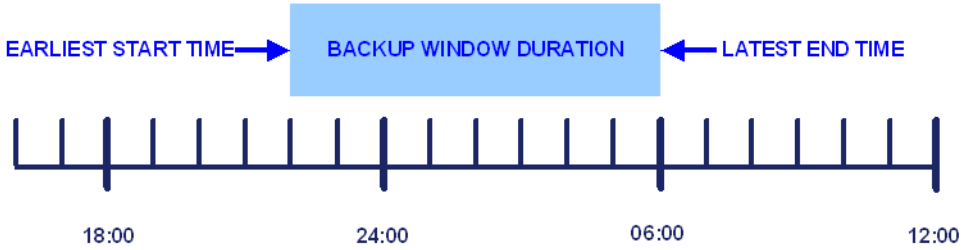
Schedule type	Description
Daily	Repeats a system activity every day at one or more times of the day. With daily schedules, you must also limit the duration of the activity to prevent job overlap.
Weekly	Repeats a system activity every week on one or more days of the week. With weekly schedules, you must also define the earliest start time for the activity, as well as the time at which the activity is stopped, even if it is still in progress.
Monthly	Repeats a system activity on a specific calendar date or on a designated day of the week each month, such as the first Sunday of every month. With monthly schedules, you must also define the earliest start time for the activity, as well as the time at which the activity is stopped, even if it is still in progress.
On-demand	Defines a schedule that does not run automatically. This option is useful for creating schedules that you can assign today but activate in the future, or to create schedules that are assigned to groups that only perform on-demand backups, such as groups that contain only laptop clients.

When you create a schedule, you also define when the schedule should take effect, and when it should be discontinued. For example, if you know that client computers used for a specific development project will be obsolete at a specific future date, you could create a schedule for those group backups that would automatically cease backups on a certain date. Similarly, if you are administering a large site, you could create schedules ahead of time, assign them to groups, and then activate them on a certain date. These group backups would not occur until the schedule took effect.

Because scheduled activities often straddle two calendar days, it is important to understand that Avamar allocates the full window of time to any activity initiated by a schedule. For example, consider a schedule with an earliest start time of 10 p.m., a latest end time of 6 a.m. (the following morning), and an end after date of December 31 of the current calendar year. On the evening of December 31, the activity starts as expected and runs until completed, typically sometime during the morning of January 1 the following year. However, beginning January 1, no new scheduled activities are initiated by this schedule.

Start time, end time, and duration

The following figure illustrates how the start time, end time, and duration of a schedule interact with one another, using the initial settings of the Default schedule:



This system activity would begin at 10 p.m. (22:00), and could run until 6 a.m. (06:00) the next day. This creates an effective eight-hour duration.

In practice, scheduled activities rarely start or end precisely on time. Actual start times are affected by server load, and actual end times are affected by the complexity of the activity. The complexity of the activity involves, for example, the amount of new client data that must be backed up, the number of group backups initiated, the number of email messages that must be sent, and so forth.

It must therefore be understood that specifying a schedule start time means that this is the *earliest possible time* that the system activity can begin. In addition, specifying a duration or end time establishes the *latest possible end time* for the system activity.

Schedule time zones

When schedules are created or edited, all times are shown relative to the local time zone for that Avamar Administrator client. For example, consider a schedule created by an administrative user in the Pacific Standard Time zone, with a next runtime of 10 p.m. If an administrative user in Eastern Standard Time views that same schedule in an Avamar Administrator session, then the next runtime would be localized and shown as 1 a.m. the following day (3 hours later).

Schedule catalog

The following schedules are available by default.

Table 23 Schedule catalog (page 1 of 2)

Schedule name	Description
Default Schedule	Controls backup scheduling for the Default Group. It is initially configured to run once per day at 10 p.m. If you edit these settings, the changes are enforced on all members of the Default Group.
Default Replication	Controls replication for replication groups. "Managing replication with Avamar Administrator" on page 373 provides details.
Daily Schedule	Avamar supplies a predefined Daily Schedule.
Evaluation Schedule	Controls when the Evaluation Profile email notification is sent. It is initially configured to run every Monday at 6 a.m.

Table 23 Schedule catalog (page 2 of 2)

Schedule name	Description
Notification Schedule	Controls when custom event profile email notification messages are sent.
Override Daily Schedule	Defines the available start times for clients that have the **Override group schedules** setting enabled. This schedule is editable. Copies of this schedule are not used with the **Override group schedules** setting.
Statistics Schedule	Controls how often various Avamar server statistics (for example, the Avamar server detail Bytes protected value) are retrieved or calculated. The default setting for this schedule is hourly.

Creating a schedule

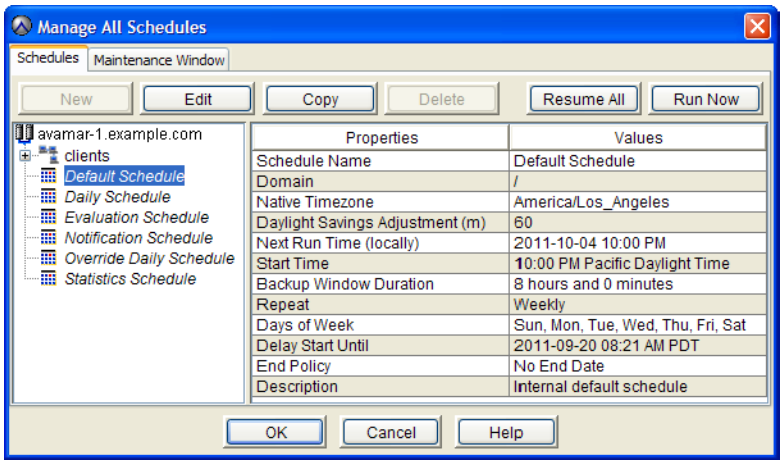
The steps to create a schedule depend on whether you are creating a daily, weekly, monthly, or on-demand schedule.

Creating a daily schedule

To create a daily schedule:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



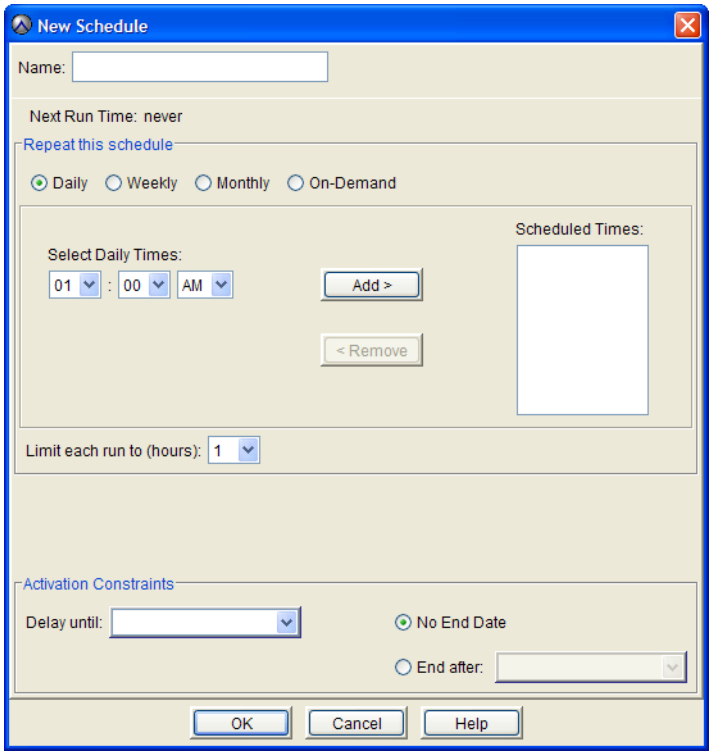
2. Click **New**.

   The New Schedule dialog box appears.

3. In the **Name** box, type a name for the schedule.

   Do not use any of the following characters in the name: ~!@$^%(){}[]|,`;#\/:*?‹›'"&.

4. Under **Repeat this schedule**, select **Daily**.



5. Use the **Select Daily Times** lists to specify the time of day at which the schedule should run, and then click **Add** to add the time to the **Scheduled Times** list.
6. Repeat the previous step for each time at which the schedule should run each day.

   To remove a time from the **Scheduled Times** list, select the time and click **Remove**.
7. Limit the duration of scheduled system activities to prevent job overlap by selecting a time limit from the **Limit each run to (hours)** list.
8. From the **Delay until** list, select the date when the schedule should take effect.

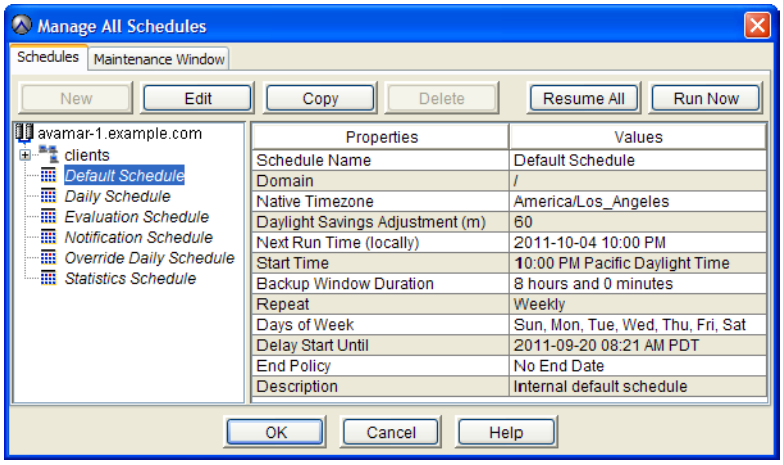
   To make a schedule effective immediately, select the current date from the list.
9. Choose when to discontinue the schedule:
   - To enable a schedule to run indefinitely, select **No End Date**.
   - To discontinue a schedule on a specific date, select **End after** and then select a date from the list.
10. Ensure that the date and time listed next to **Next Run Time** near the top of the **New Schedule** dialog box are correct.
11. Click **OK**.

Creating a weekly schedule

To create a weekly schedule:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



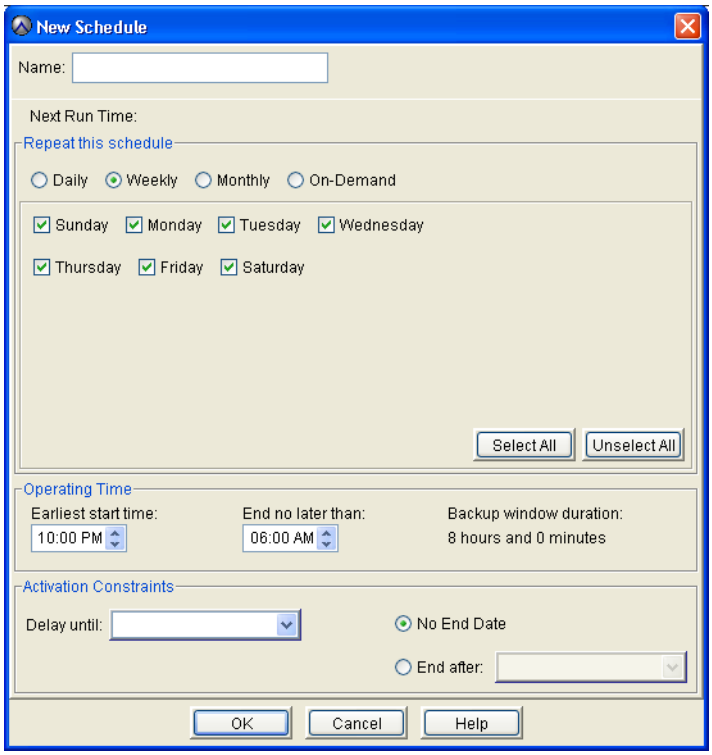
2. Click **New**.

   The New Schedule dialog box appears.

3. In the **Name** box, type a name for the schedule.

   Do not use any of the following characters in the name: ~!@$^%(){}[]|,`;#\/:*?‹›'"&.

4. Under **Repeat this schedule**, select **Weekly**.



5. Select the checkbox next to the days of the week on which the schedule should run.

6. Define the activity operating hours using the **Earliest start time** and **End no later than** boxes. You can type the times, or select the time and use the arrow buttons to change the times.

   Server workload affects the start time for an activity. In addition, the first time that a backup is performed for any client, the backup is allowed to continue past the specified end time. This is because initial backups can take significantly longer than subsequent backups of the same client.

7. From the **Delay until** list, select the date when the schedule should take effect.

   To make a schedule effective immediately, select the current date from the list.

8. Choose when to discontinue the schedule:

   - To enable a schedule to run indefinitely, select **No End Date**.
   - To discontinue a schedule on a specific date, select **End after** and then select a date from the list.

9. Ensure that the date and time listed next to **Next Run Time** near the top of the **New Schedule** dialog box are correct.

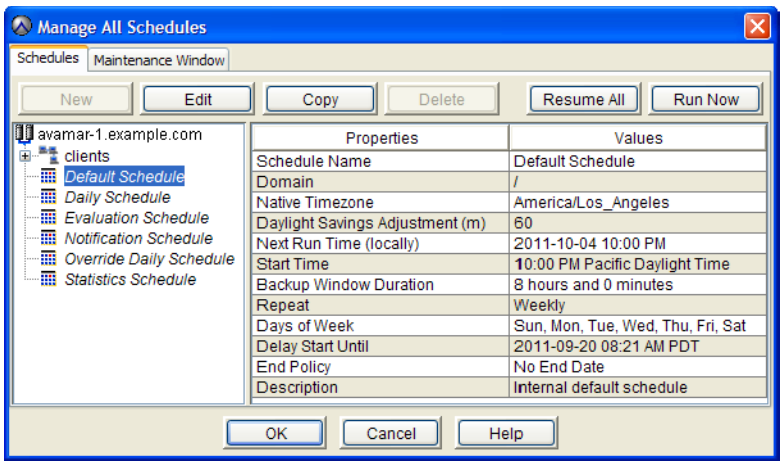
10. Click **OK**.

Creating a monthly schedule

To create a monthly schedule:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



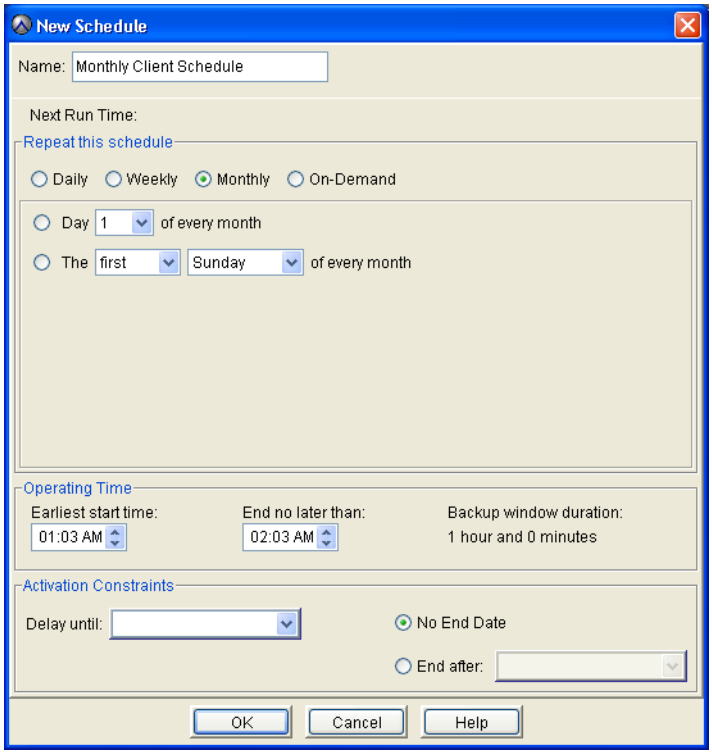
2. Click **New**.

   The New Schedule dialog box appears.

3. In the **Name** box, type a name for the schedule.

   Do not use any of the following characters in the name: ~!@$^%(){}[]|,`;#\/:*?‹›'"&.

4. Under **Repeat this schedule**, select **Monthly**.



5. Choose whether to repeat the activity on a specific calendar date or on a designated day of the week each month:
   - To repeat the activity on a specific calendar date, select **Day of every month**, and then select the day from the list.
   - To repeat the activity on a designated day of the week each month, select **The ... of every month** and then select the day from the lists.
6. Define the a logical window of time during which the system activity can take place using the **Earliest start time** and **End no later than** boxes. You can type the times, or select the time and use the arrow buttons to change the times.

   NOTICE

   Server workload affects the start time for an activity. In addition, the first time that a backup is performed for any client, the backup is allowed to continue past the specified end time. This is because initial backups can take significantly longer than subsequent backups of the same client.

7. From the **Delay until** list, select the date when the schedule should take effect.

   To make a schedule effective immediately, select the current date from the list.
8. Choose when to discontinue the schedule:
   - To enable a schedule to run indefinitely, select **No End Date**.
   - To discontinue a schedule on a specific date, select **End after** and then select a date from the list.

9. Ensure that the date and time listed next to **Next Run Time** near the top of the **New Schedule** dialog box are correct.
10. Click **OK**.

Creating an on-demand schedule

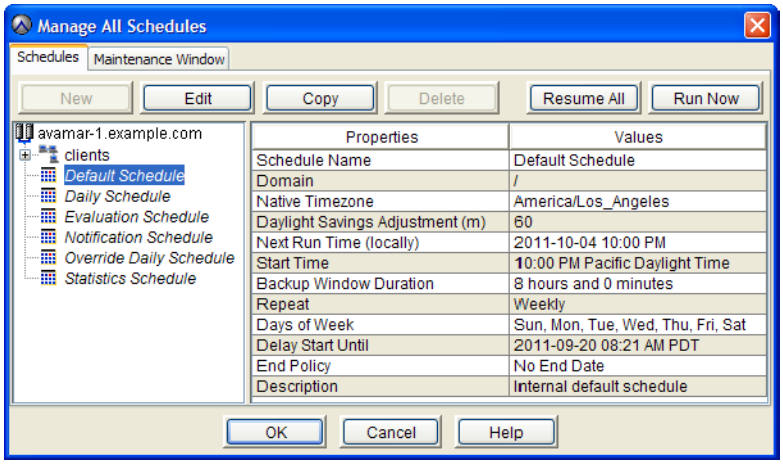
An on-demand schedule is useful in the following scenarios:

- You want to create a schedule that you can assign today but activate in the future.
- You have a group with clients that you only perform on-demand backups for, such as groups that contain only laptop clients.

To create an on-demand schedule:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



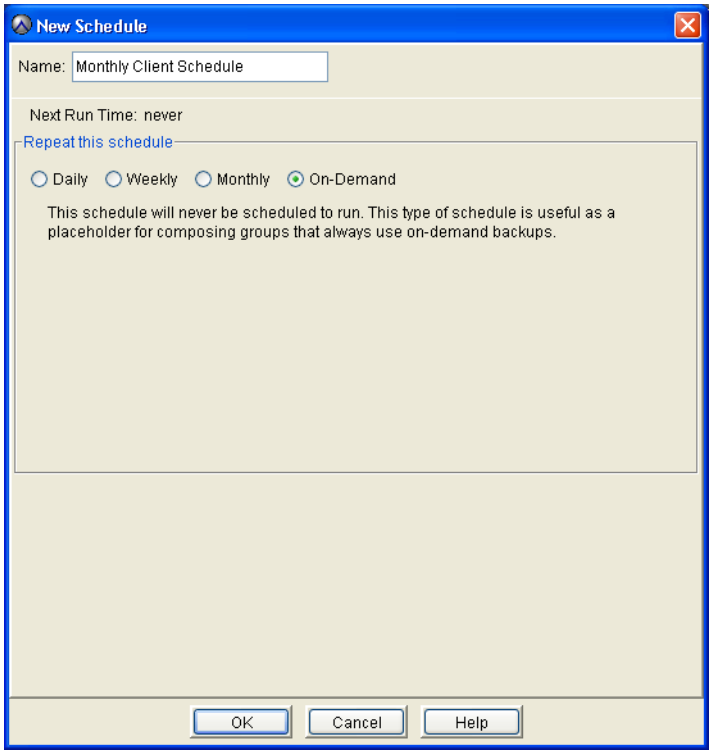
2. Click **New**.

   The New Schedule dialog box appears.

3. In the **Name** box, type a name for the schedule.

   Do not use any of the following characters in the name: ~!@$^%(){}[]|,`;#\/:*?‹›'"&.

4. Under **Repeat this schedule**, select **On-Demand**.



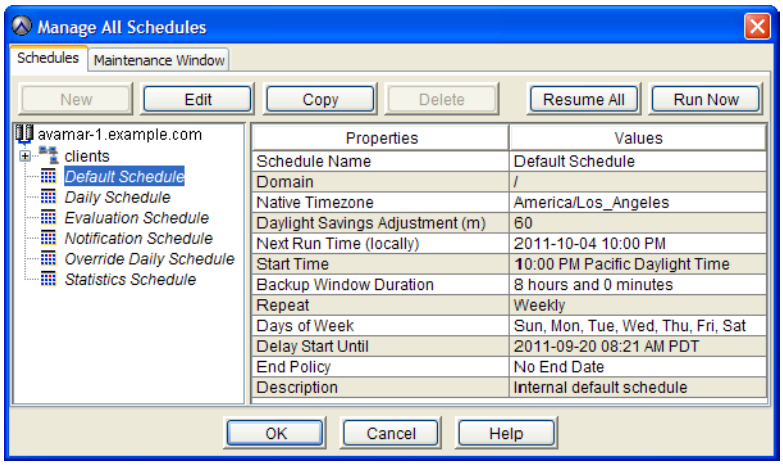
5. Click **OK**.

Editing a schedule

To edit a schedule:

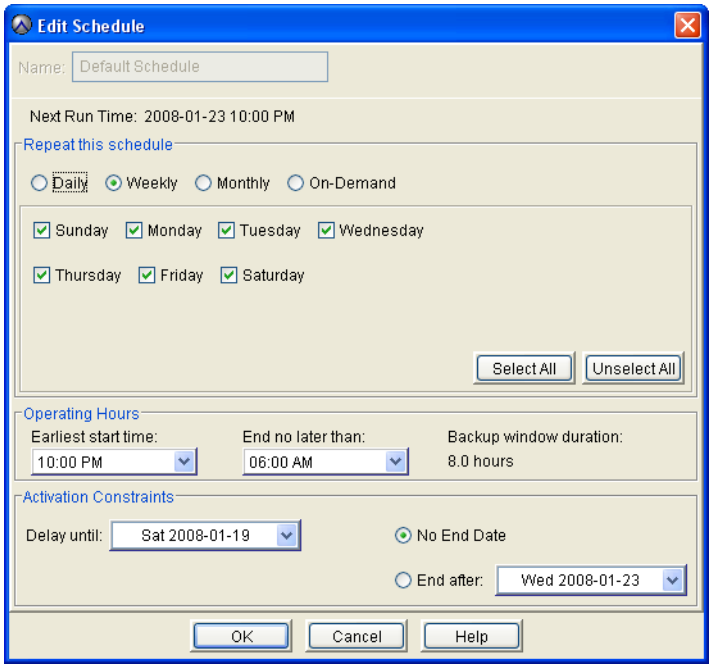
1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



2. Select a schedule from the list and click **Edit**.

The Edit Schedule dialog box appears.



3. Edit the schedule information.

   Details on schedule properties are available in the following topics:

   - "Creating a daily schedule" on page 136
   - "Creating a weekly schedule" on page 138
   - "Creating a monthly schedule" on page 139
   - "Creating an on-demand schedule" on page 141

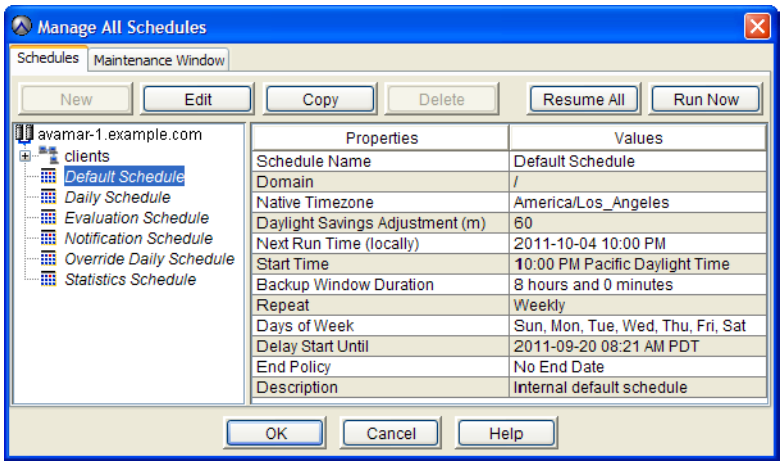
4. Click **OK**.

Copying a schedule

To copy a schedule:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



2. Select the schedule from the list and click **Copy**.

   The Save As dialog box appears.

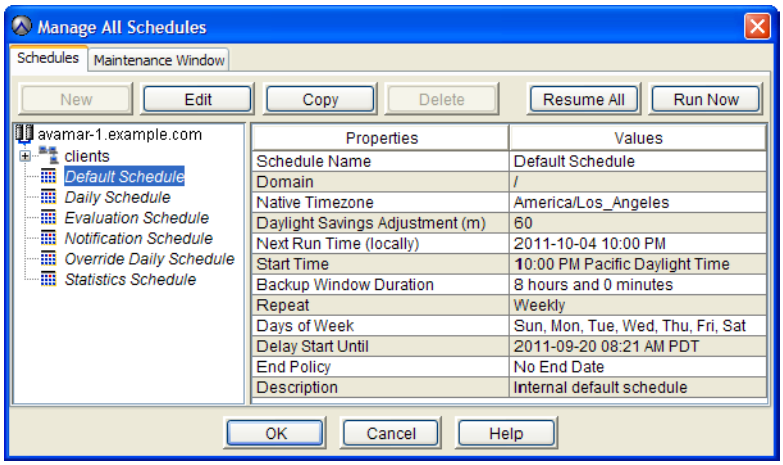
3. Type a name for the new schedule and click **OK**.

Deleting a schedule

To delete a schedule:

1. Ensure that the schedule is not currently assigned to a group. You cannot delete a schedule if it is currently assigned to a group.
2. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



3. Select the schedule from the list and click **Delete**.

   A confirmation message appears.

4. Click **Yes**.

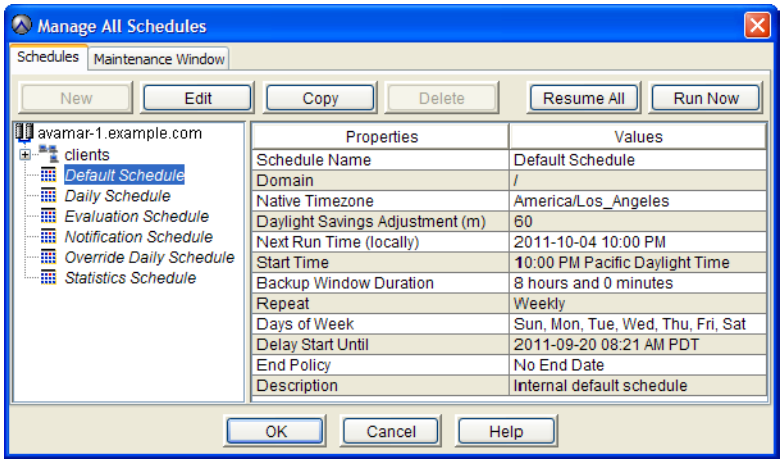
Running a schedule now

You can initiate scheduled operations immediately on an on-demand basis. The scheduler does not need to be running when you run a schedule on-demand.

To run a schedule now:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



2. Select a schedule from the list and click **Run Now**.

Editing the Override Daily Schedule

Use the Override Daily Schedule to configure the start times that are available when you enable **Allow override of group's daily schedule**, as described in "Allowing users to add to source data" on page 182. This schedule supplies the start times that users see and can select from when override group schedules is enabled for their client.

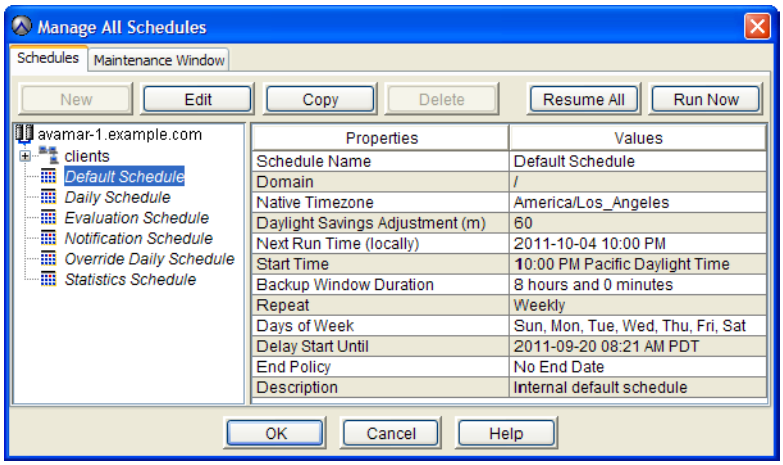
Users must have access to the web UI to view and select from the available start times. Access to the web UI is part of the enhanced features for enterprise desktop and laptop computers.

By default the override schedule contains no time entries. By adding time entries you make the entries available to all clients that have override group schedules enabled.

To add time entries to the override schedule:

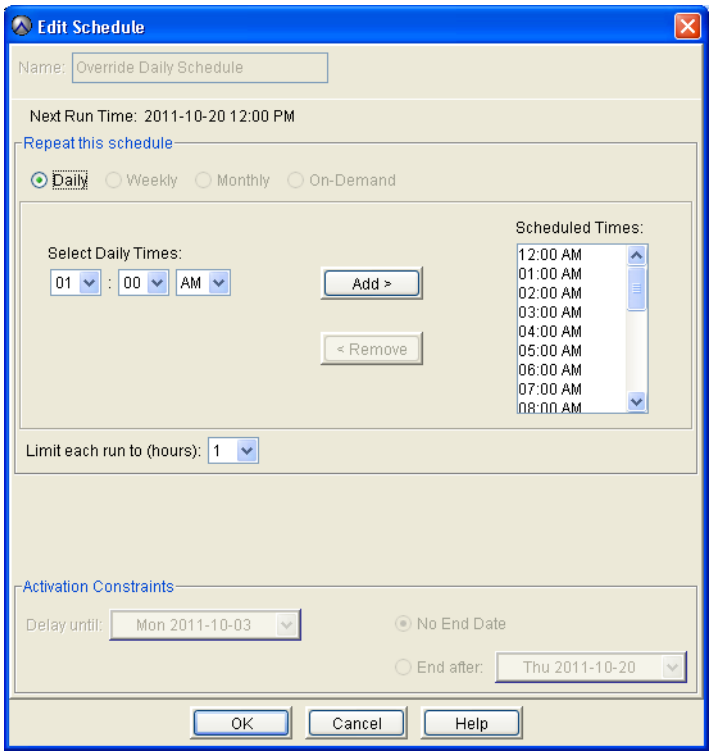
1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



2. From the list of schedules, select **Override Daily Schedule** and click **Edit**.

   The Edit Schedule dialog box appears. All fields are previously configured and cannot be changed, except Scheduled Times and Limit each run to (hours).



3. Use the **Select Daily Times** lists to specify a time of day to add to the selection list available to users on the web UI, and then click **Add** to add the time to the **Scheduled Times** list.

   To remove a time from the **Scheduled Times** list, select the time and click **Remove**.

4. Repeat the previous step to add additional time entries to the selection list available to users.
5. Limit the duration of scheduled system activities to prevent job overlap by selecting a time limit from the **Limit each run to (hours)** list.
6. Click **OK**.

Retention policies

Backup retention policies enable you to specify how long to keep a backup in the system.

A retention policy is assigned to each backup when the backup occurs. You can specify a custom retention policy when you perform an on-demand backup, or you can create a retention policy that is assigned automatically to a group of clients during a scheduled backup.

When the retention for a backup expires, then the backup is automatically marked for deletion. The deletion occurs in batches during times of low system activity.

If necessary, you can manually change the retention setting for an individual backup that has already occurred, as described in "Changing a backup expiration date" on page 110. If you change a configured retention policy, however, the change applies only to backups that occur after the change. The retention setting remains the same for backups that have already been performed. Therefore, it is very important to carefully consider and implement the best retention policy for a site before too many backups occur.

There are two types of retention settings:

- Basic retention settings specify a fixed expiration date.
- Advanced retention settings specify the number of daily, weekly, monthly, and yearly backups to keep.

Basic retention settings

Basic retention settings are used to assign a fixed expiration date to a backup using one the settings in the following table.

Table 24 Basic retention settings

Retention setting	Description
Retention period	Enables you to define a fixed retention period in days, weeks, months, or years after the backup is performed. For example, you could specify that backups expire after 6 months.
End date	Enables you to assign a calendar date as the expiration date. For example, you could specify that backups expire on December 31, 2013.
No end date	Enables you to keep backups indefinitely. This setting is useful for ensuring that all backups that are assigned this retention policy are retained for the life of the system.

Advanced retention settings

With advanced retention settings, you can dynamically assign backup expiration dates based on the number of daily, weekly, monthly, and yearly backups to retain in the system.

When you perform scheduled daily backups on a regular basis, some backups are automatically assigned an advanced retention type:

- The first successful scheduled backup each day is designated as the daily backup.
- The first successful scheduled backup each week is designated as the weekly backup.
- The first successful scheduled backup each month is designated as the monthly backup.
- The first successful scheduled backup each year is designated as the yearly backup.

For purposes of assigning advanced retention types, each day begins at 00:00:01 GMT, each week begins on Sunday, each month begins on the first calendar day of that month and each year begins on January 1.

NOTICE

You cannot apply advanced retention settings to on-demand backups. On-demand backups can occur at any time, and are therefore inherently asynchronous—the system cannot tag them as daily, weekly, monthly, or yearly.

You should always use retention policies with advanced retention settings in conjunction with daily scheduled backups. The reason for this is that the "Always keep: n weeks of daily backups" setting has no effect unless there are daily backups in the system. However, depending on which schedule you use, this may not always be the case. For example, if you assign a schedule to a group that only performs weekly backups, then there are no daily backups in the system.

Minimal retention

Minimal retention enables you to enforce a minimum basic retention setting across an entire site. For example, you can keep all backups for at least 90 days regardless of what other retention policies specify. This feature is intended to address the need of some enterprises to enforce site-wide minimum retention standards regardless of what individual organizations might decide to implement with other retention policies.

To enforce minimal retention, enable and configure the Minimal Retention policy, which is a default retention policy in the system. "Enabling the Minimal Retention policy" on page 153 provides details.

The Minimal Retention policy is a global system object that controls only the minimal retention setting. Therefore, you cannot assign the Minimal Retention policy to a group.

Last backup retention

To retain the last backup of all clients, even after the backup exceeds its retention period, enable last backup retention. Last backup retention changes the default retention behavior for client backups that occur after it is enabled. When this is enabled, the last backup of a client is not marked for deletion when its retention period expires.

Last backup retention is designed for clients that do not back up frequently. For those clients, the default behavior can lead to the last backup expiring before a new backup occurs. This could result in clients that do not have an available backup.

Clients that are not permanently connected to a domain, such as remote desktops and laptops, may encounter this situation more frequently than clients that have uninterrupted server access.

IMPORTANT

When you enable last backup retention, Avamar retains a single backup for each client, even if you perform multiple types of backups of a client. For example, if you perform bothfile system and application backups of a client, and the file system backup is the last backup, then all application backups can expire.

"Setting last backup retention" on page 419 describes how to enable last backup retention.

Retention policy catalog

The retention policies in the following table are available by default.

Table 25 Types of retention policies

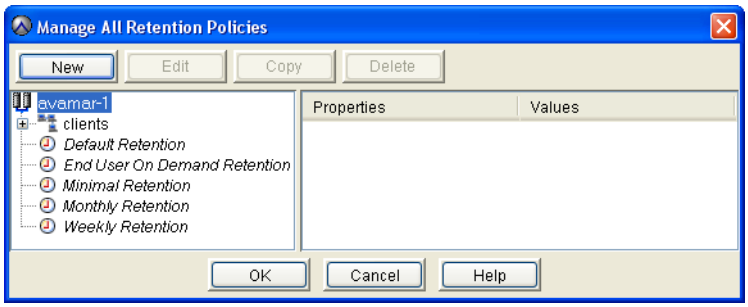
Retention policy type	Description
Minimal Retention	Controls the minimal retention feature, which is discussed in "Minimal retention" on page 148.
Default Retention	Defines backup retention settings for the Default Group. By default, the Default Retention policy assigns a retention period of 60 days and retains 60 days of daily backups.
End User On Demand Retention	Controls the retention settings for on-demand backups initiated by the client, such as when you use the Back Up Now command on the Avamar Windows client. Advanced retention settings are disabled on this retention policy because advanced retention settings never apply to on-demand backups. The End User On Demand Retention policy is a global system object that only controls retention for on-demand backups initiated by the client. Therefore, you cannot assign the End User On Demand Retention policy to a group.
Monthly Retention policy	Sets the expiration date to one month after the backup is performed.
Weekly Retention policy	Sets the expiration date to one week after the backup is performed.

Creating a retention policy

To create a retention policy:

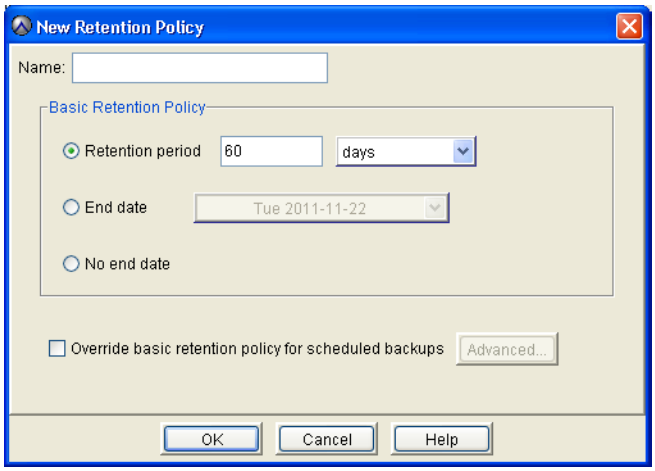
1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

   The Manage All Retention Policies window appears.



2. Click **New**.

   The New Retention Policy dialog box appears.



3. In the **Name** box, type a name for the retention policy.

   Do not use any of the following characters in the retention policy name: ~!@$^%(){}[]|,`;#\/:*?<>'"&.

4. Select the basic retention setting for the policy:

   - To automatically delete backups after a specific number of days, weeks, months, or years, select **Retention period** and specify the number of days, weeks, months, or years.
   - To automatically delete backups on a specific calendar date, select **End date** and then browse to that date on the calendar.
   - To keep backups for as long as a client remains active, select **No end date**.

   The best practice is to specify a retention that is greater than, or equal to, 14 days. When you create a retention policy for less than 14 days, an alert appears.

5. (Optional) Specify advanced retention settings:
   a. Select **Override basic retention policy for scheduled backups**.
   b. Click **Advanced**.

      The Edit Advanced Retention Policy dialog box appears.

   c. Specify the maximum number of daily, weekly, monthly, and yearly backups to retain.
   d. Click **OK**.

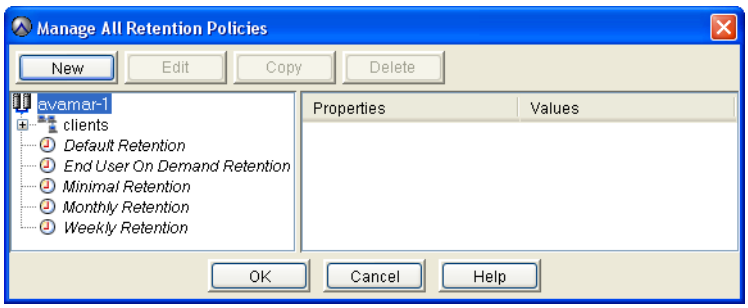
      The Edit Advanced Retention Policy dialog box closes.
6. On the **New Retention Policy** dialog box, click **OK**.

Editing a retention policy

To edit a retention policy:

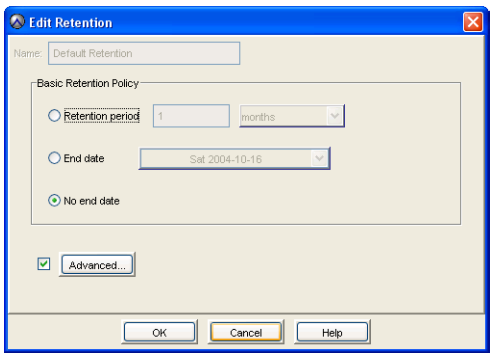
1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

   The Manage All Retention Policies window appears.



2. Select a retention policy from the list and click **Edit**.

   The Edit Retention Policy dialog box appears.



3. Edit the retention policy information.

   "Creating a retention policy" on page 150 provides details about retention policy properties. If you are editing the Minimal Retention policy, then the End date and No end date options are not available.

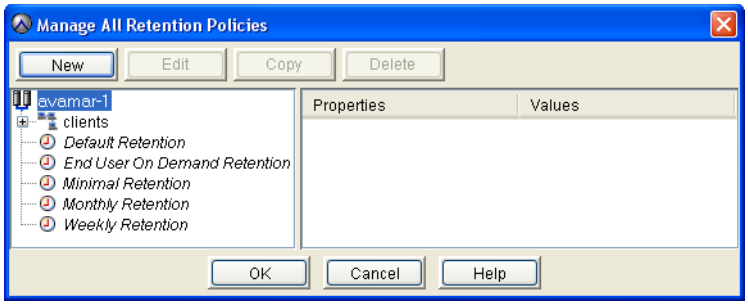
4. Click **OK**.

Copying a retention policy

To copy a retention policy:

1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

   The Manage All Retention Policies window appears.



2. Select a retention policy from the list and click **Copy**.

   The Save As dialog box appears.

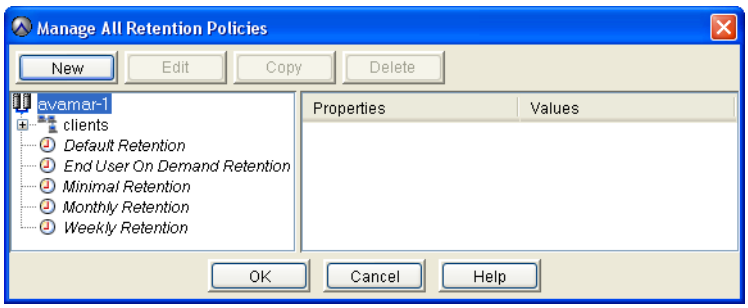
3. Type a name for the new retention policy and click **OK**.

Deleting a retention policy

To delete a retention policy:

1. Ensure that the retention policy is not currently assigned to a client or group. You cannot delete a retention policy if it is currently assigned to a client or group.
2. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

   The Manage All Retention Policies window appears.



3. Select a retention policy from the list and click **Delete**.

   A confirmation message appears.

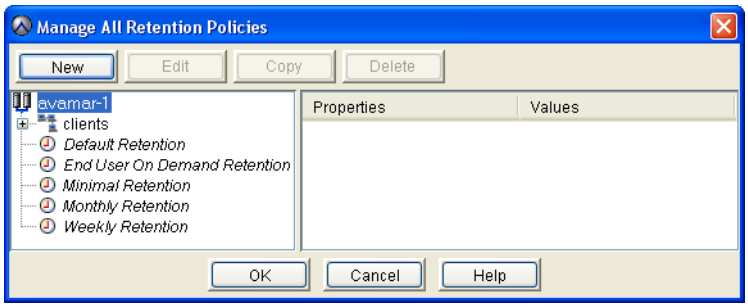
4. Click **Yes**.

Enabling the Minimal Retention policy

To enable the Minimal Retention policy:

1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

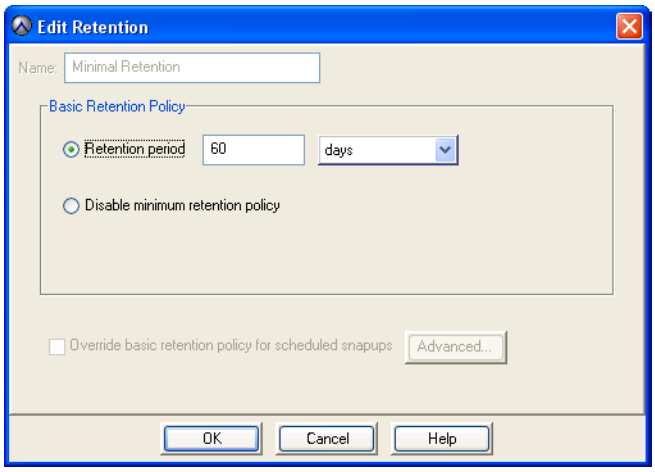
   The Manage All Retention Policies window appears.



2. Select the **Minimal Retention** policy and click **Edit**.

   The Edit Retention Policy dialog box appears.

3. Select **Retention period**.



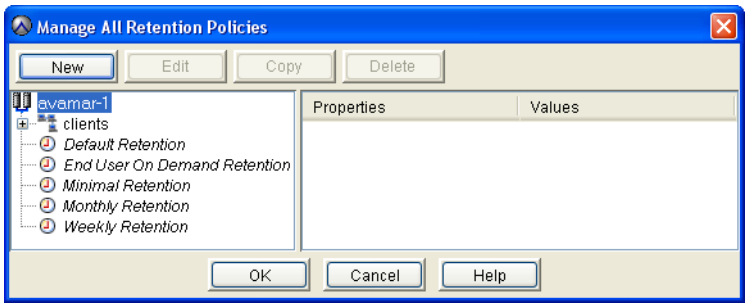
4. Specify the number of days, weeks, months, or years to ensure that backups are retained.
5. Click **OK**.

Disabling the Minimal Retention policy

To disable the Minimal Retention policy:

1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

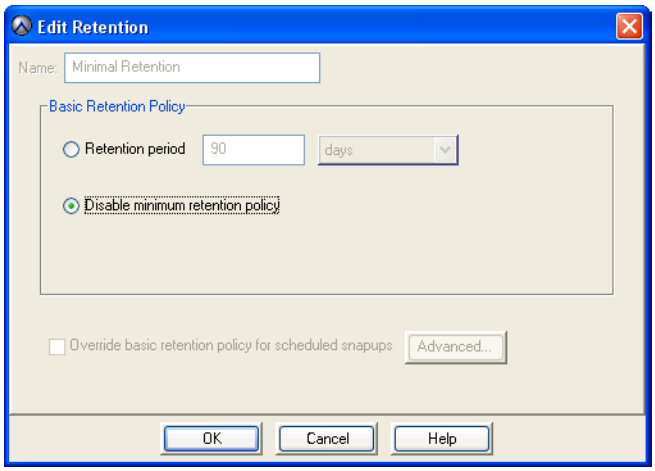
   The Manage All Retention Policies window appears.



2. Select the **Minimal Retention** policy from the list and click **Edit**.

   The Edit Retention Policy dialog box appears.

3. Select **Disable minimum retention policy**.



4. Click **OK**.

CHAPTER 6
Groups and Group Policies

The following topics describe how to create and manage Avamar groups and group policies:

- Important terms and concepts 156
- Policy window overview 157
- Creating a group..... 159
- Editing group properties..... 164
- Copying a group 165
- Enabling and disabling a group 166
- Deleting a group 166
- Viewing the Group Summary Reports 167
- Viewing the Group Status Summary 168
- Managing group membership 169
- Overriding group policy settings for a single client..... 171
- Overriding group policy settings for multiple clients 185
- Performing on-demand group and client backups..... 187
- Perfoming on-demand group and client replications..... 188

Important terms and concepts

Avamar uses groups to implement various policies to automate backups and enforce consistent rules and system behavior across an entire segment, or group, of the user community.

Group members

Group members are client machines that have been added to a particular group for the purposes of performing scheduled backups.

Because the normal rules for domain administrators apply, these clients must be located within the same domain or within a subdomain of where the group exists.

Group policy

In addition to specifying which clients belong to that group, groups also specify:

- "Datasets" on page 124
- "Schedules" on page 134
- "Retention policies" on page 147

These three objects comprise the "group policy." The group policy controls backup behavior for all members of the group unless you override these settings at the client level.

Default Group

If no other groups have been created, new clients will automatically be added to the Default Group.

In the default Avamar server configuration, the Default Group always uses the system default dataset, schedule, and retention policy. You cannot change these system default assignments. However, you can edit the settings within the system default dataset, schedule, and retention policy.

Default Proxy Group

The Default Proxy Group is the default group for VMware Image Proxy clients. You cannot delete the Default Proxy Group. Enabling the Default Proxy Group does not conflict with scheduled backups performed by other plug-ins configured on the proxy client.

Default Virtual Machine Group

New virtual machine clients are automatically added to the Default Virtual Machine Group when they are registered. You cannot manually delete the Default Virtual Machine Group, but it is automatically deleted if you delete the vCenter Domain.

vCenter groups

When you create a group in the vCenter domain, the group automatically becomes a "vCenter" group. This group behaves similar to non-vCenter groups except that it also provides the ability to specify which proxies are assigned to perform backups on behalf of its group members.

The *EMC Avamar for VMware User Guide* provides details about using the Default Proxy Group, Default Virtual Machine Group, and vCenter groups to manage the VMware Image backup and restore feature.

Inheritance and client overrides

Clients inherit dataset, schedule, and retention policy settings based on their membership in a group. For example, all members of the Default Group inherit the system default dataset, schedule, and retention policy.

You can override inherited dataset and retention policy settings by making explicit dataset or retention policy assignments for the client. However, schedules apply only to groups, not individual clients. "Assigning a different dataset" on page 181 and "Assigning a different retention policy" on page 184 provide details.

Policy window overview

The Policy window enables you to assign clients to a group and specify which dataset, retention policy, and schedule each group should use.

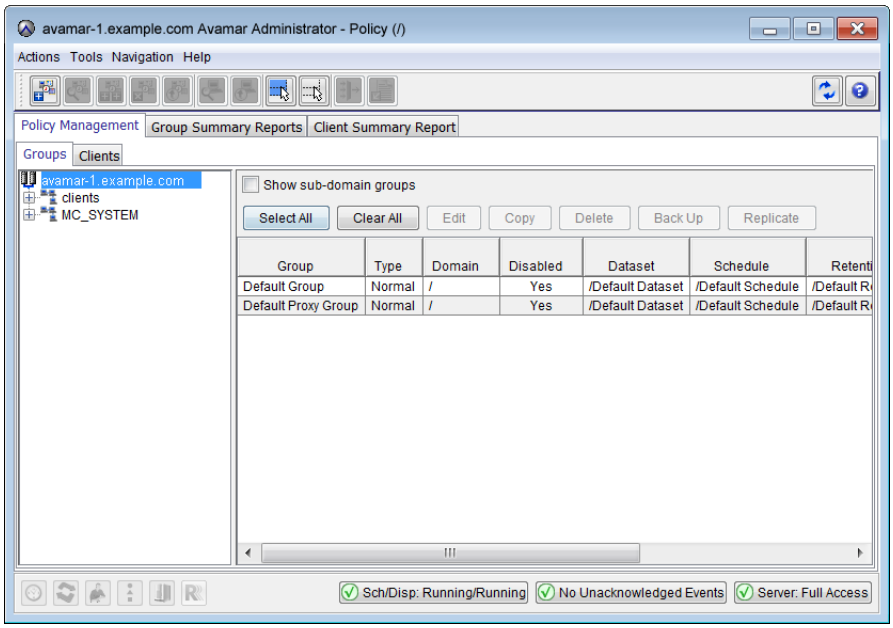


Figure 7 Policy window.

Groups tab

The Groups tab shows the groups for each domain, and enables you to view group properties in a tabular format.

To view groups in the current domain and all subdomains, select Show sub-domain groups.

The Groups tab also provides the action buttons described in the following table.

Table 26 Buttons on the Policy window's Groups tab

Button	Description
Select All	Click Select All to select all groups for edit.
Clear All	Click Clear All to clear the selection of all groups.
Edit	Select one or more groups and click Edit to display the Edit Group dialog box, which enables you to edit group properties. If multiple groups are selected, you can edit the following properties for all selected groups: • Disabled • Dataset • Schedule • Retention Policy • Encryption The domain that you log in to controls which datasets, retention policies, and schedules you can assign in the Groups tab. Only those datasets, retention policies, and schedules at the current and higher level appear. Datasets, retention policies, and schedules in lower subdomains do not appear.
Copy	Select a group and click Copy to display the Save As dialog box, which you can use to copy this group and all its properties to another domain. You cannot copy more than one group at a time.
Delete	Select a group and click Delete to permanently remove that group from the system. Deleting a group does not affect any client backups stored in the system. However, a client must always be a member of at least one group. Therefore, if you attempt to delete a group in which client members do not belong to another group, you are advised to move those clients to another group before the delete operation can proceed. You cannot delete more than one group at a time.
Back up	Select a group and click Back up to initiate an on-demand backup of that group.
Replicate	Select a replication group and click Replicate to initiate an on-demand replication of that group. This button is disabled for non-replication groups. "Managing replication with Avamar Administrator" on page 373 provides details about policy-based replication.

Clients tab

The Clients tab shows clients assigned to groups for each domain, and enables you to view client properties in a tabular format.

To view clients assigned to groups in the current domain and all subdomains, select Show sub-domain clients.

The Clients tab also provides the action buttons described in the following table.

Table 27 Buttons on the Policy window's Clients tab

Button	Description
Select all	Click Select All to select all clients for edit.
Clear all	Click Clear All to clear the selection of all clients.
Details	Select a client and click Details to display the Client Details dialog box, which shows the properties of the client. You cannot view details for more than one client at a time. "Viewing client properties" on page 68 provides details on specific client properties.
Edit	Select one client and click Edit to display the Edit Client dialog box. This dialog box enables you to override various group policy settings for a single client. This is described in "Overriding group policy settings for a single client" on page 171. Select multiple clients and click Edit to display the Edit Multiple Clients dialog box. This dialog box enables you to override various group policy settings for the selected group of clients. This is described in "Overriding group policy settings for multiple clients" on page 185.
Back up	Select a client and click Back up to initiate an on-demand backup of that client.
Replicate	Select a client and click Replicate to initiate an on-demand replication of that client. The client must already be a member of a replication group. "Managing replication with Avamar Administrator" on page 373 provides details about policy-based replication.

Creating a group

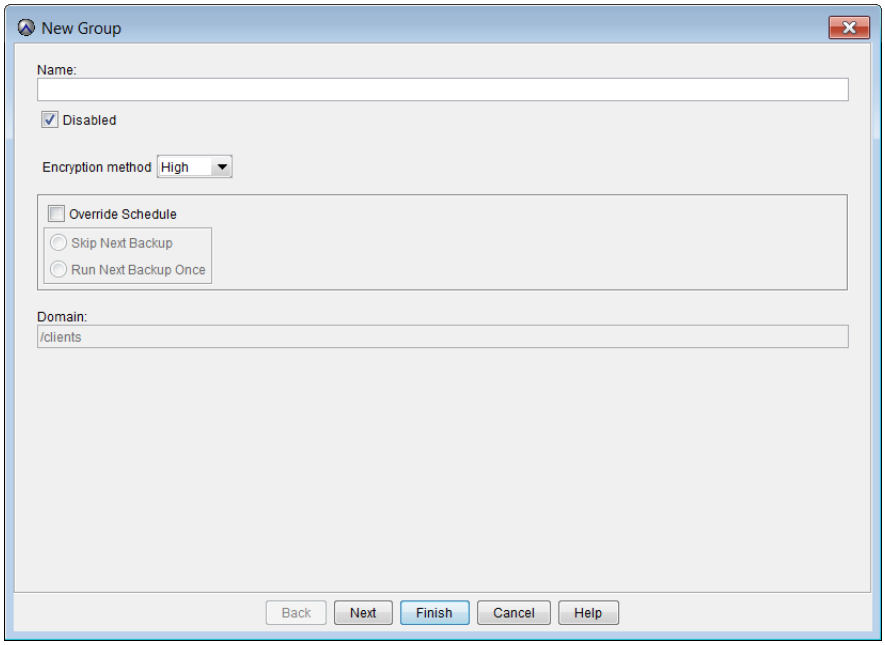
To create a group:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Select the **Groups** tab.
3. In the left pane, select the Avamar domain to which the group should belong.
4. Select **Actions** › **New Group**.

The New Group wizard appears.



5. In the **Name** box, type a name for the group.

   Do not use any of the following characters in the group name: ~!@$^%(){}[]|,`;#\/:*?<>'"&.

6. Clear the **Disabled** option to immediately enable regularly scheduled client backups for the group.

7. Select one of the following encryption methods for client/server data transfers:

   - **High**—Strongest available encryption setting for that specific client platform.
   - **Medium**—Medium strength encryption.
   - **None**—No encryption.

   Note: The exact encryption technology and bit strength used for any given client/server connection is dependent on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

8. Choose whether to use the assigned schedule for the group or to override the assigned schedule:

   - To use the assigned schedule, leave the **Override Schedule** checkbox clear.
   - To override the schedule:

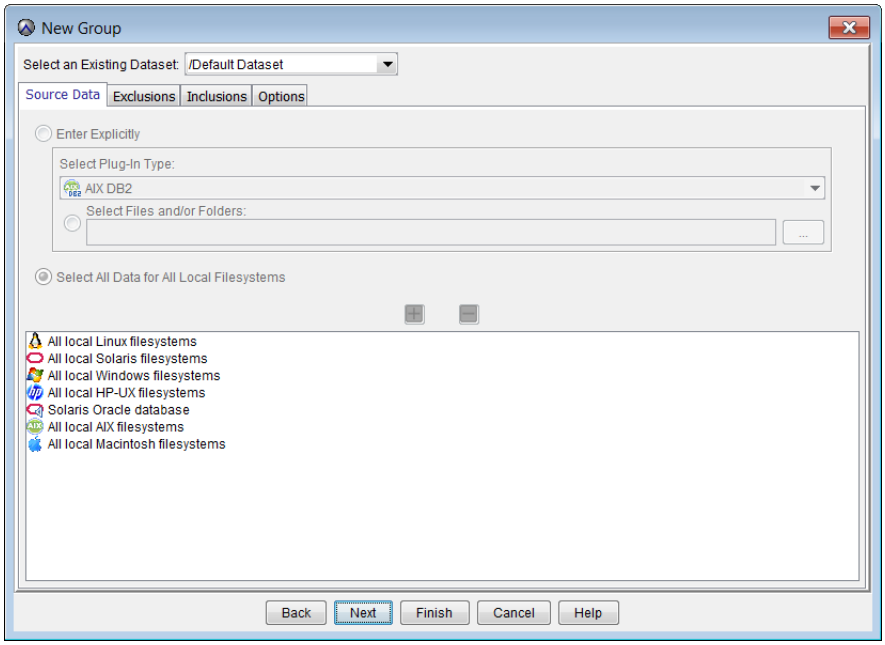
     a. Select **Override Schedule**.

        Selecting Override Schedule enables the Skip Next Backup and Run Next Backup Once options.

     b. Choose whether to skip the next scheduled backup entirely or to perform the next scheduled backup one time only by selecting either **Skip Next Backup** or **Run Next Backup Once**.

9. Click **Next**.

   The next New Group wizard screen appears with dataset information.

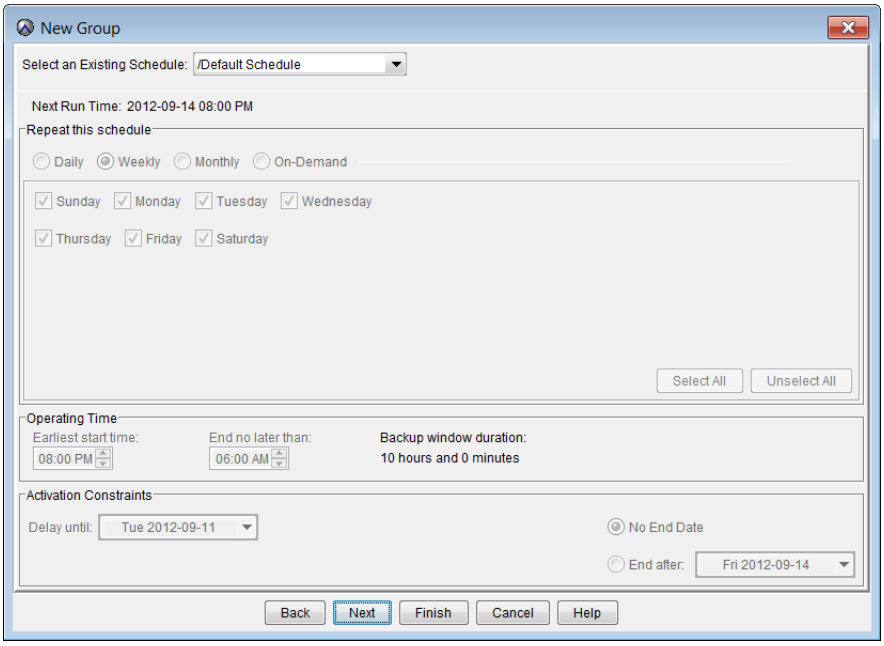


10. From the **Select An Existing Dataset** list, select a dataset for this group.

    You cannot edit datasets from this screen. Detailed dataset properties are shown so that you can review them prior to making a selection. "Datasets" on page 124 provides details.

11. Click **Next**.

    The next New Group wizard screen appears with schedule information.

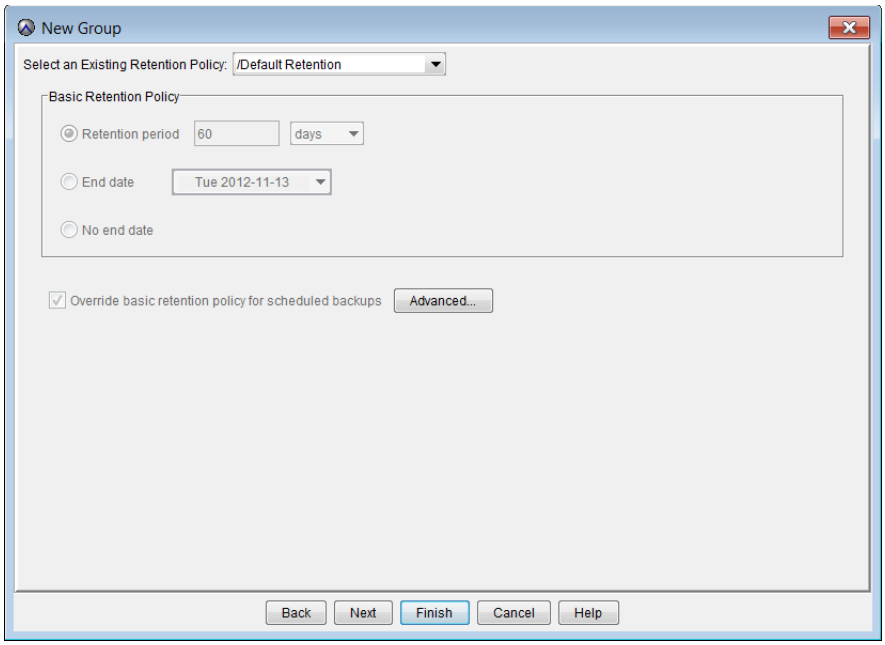


12. From the **Select An Existing Schedule** list, select a schedule for this group.

You cannot edit schedules from this screen. Detailed schedule properties are shown so that you can review them prior to making a selection. "Schedules" on page 134 provides details.

13. Click **Next**.

    The next New Group wizard screen appears with retention policy information.

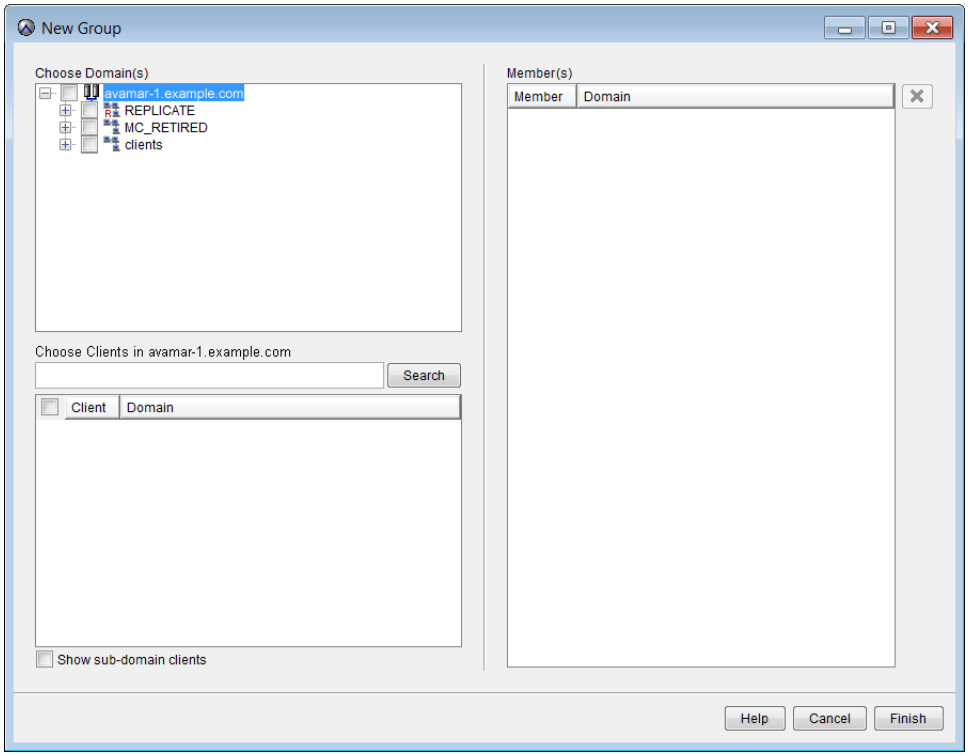


14. From the **Select An Existing Retention Policy** list, select a retention policy for the group.

    You cannot edit other retention policies from this screen. Detailed retention policy properties are shown so that you can review them prior to making a selection. "Retention policies" on page 147 provides details.

15. Click **Next**.

The final New Group wizard screen appears with a tree of domains and clients.



16. Complete the **Membership** settings as follows:
    - Select checkboxes next to one or more domains or clients.

      Selections appear in the **Member(s)** list.
    - To remove a member, select that **Member(s)** list entry and click **X**.
17. Click **Finish**.

    The New Group wizard closes and the new group appears in the Policy window.

Editing group properties

You can edit properties for a single group or for multiple groups. However, you cannot edit all group properties when you select multiple groups. The following topics provide details.

The Default Proxy Group and the Default Virtual Machine Group contain special settings that are only of interest to persons managing the VMware Image backup and restore feature. The *EMC Avamar for VMware User Guide* provides details on these special settings.

Editing a single group

To edit a single group:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group to edit.
5. Select **Actions** › **Group** › **Edit Group**.

   The Edit Group dialog box appears.

6. Edit the group information.

   You can edit only basic group properties, such as the name, client list, and the dataset, schedule, and retention policy assigned to the group. You cannot edit dataset, schedule, and retention policy properties from this dialog box.

   NOTICE

   You cannot edit Default Group policy object assignments. The Default Group always uses the default dataset, default schedule, and default retention policy. Therefore, the Dataset, Schedule, and Retention Policy tabs do not appear when you edit the Default Group.

7. Click **OK**.

Editing multiple groups

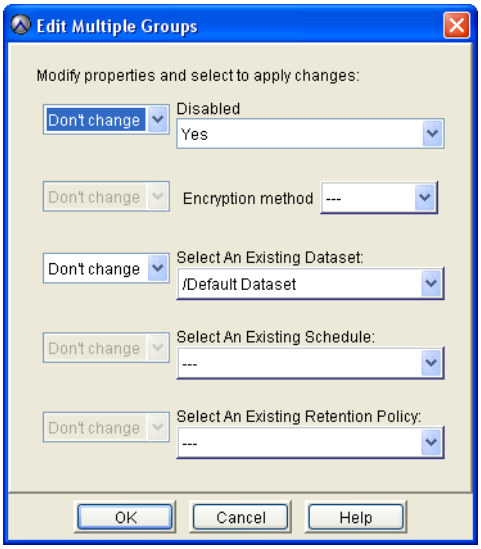
To edit multiple groups:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the groups to edit.
5. Select **Actions** › **Group** › **Edit Group**.

The Edit Multiple Groups dialog box appears.



6. To change a setting for the selected groups, select the new setting from the list, or select **Don't Change** to leave a setting unchanged for the selected groups.

   You can edit only basic group properties, such as whether the group is enabled or disabled, the encryption setting, and the dataset, schedule, and retention policy assigned to the groups. You cannot edit dataset, schedule, and retention policy properties from this dialog box.

7. Click **OK**.

Copying a group

You must copy groups within the same domain. You cannot copy a group to another domain.

To copy a group:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group to copy.
5. Select **Actions** › **Group** › **Copy Group**.

   The Save As dialog box appears.

6. Type a name for the new group.

   The **Domain** field is read-only and contains the current domain.

7. Select the **Include Client Members** to copy the entire client list to this new group.
8. Click **OK**.

Enabling and disabling a group

You can disable a group to prevent scheduled backups from occurring for the group. This is typically done to place the system in a state that supports various maintenance activities.

If you disable a group, you must re-enable the group to resume scheduled group backups.

To disable or enable a group:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Do one of the following:
   - To enable a group, select a group that is currently disabled, then clear the right-click **Disable Group** command.
   - To disable a group, select a group that is currently enabled, then select the right-click **Disable Group** command.

   A confirmation message appears.
5. Click **Yes**.

Deleting a group

Before you delete a group, you should make the clients in the group members of another group so that regularly scheduled backups for the clients continue uninterrupted. "Editing client information" on page 67 provides details on how to add clients to other groups.

To delete a group:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group to delete.
5. Select **Actions** › **Group** › **Delete Group**.

   A confirmation message appears.
6. Click **Yes**.

   A second confirmation message appears.
7. Click **OK**.

Viewing the Group Summary Reports

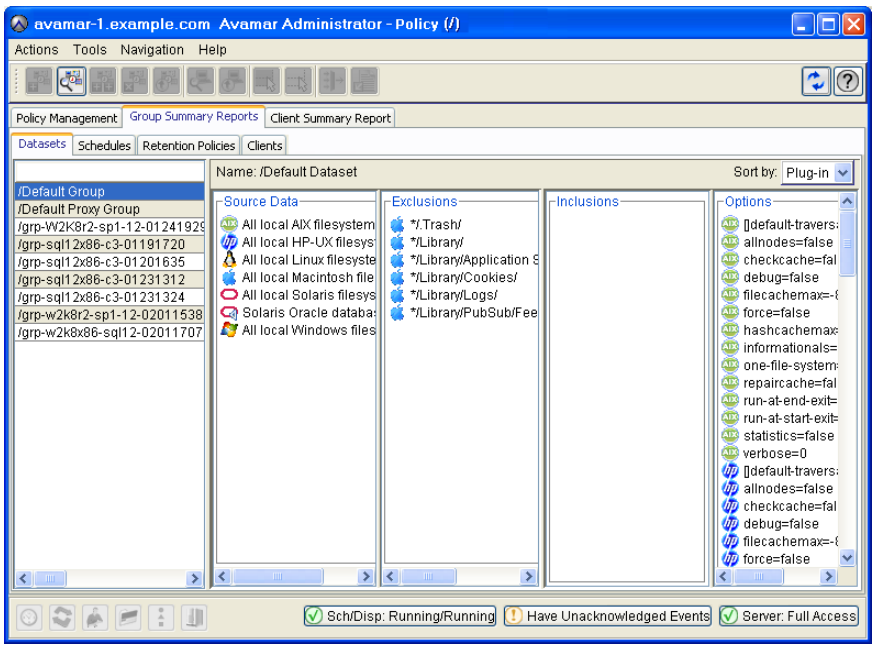
The Group Summary Reports are a combined “at a glance” view of all current group properties and settings, including group policy overrides. The reports also display the datasets, schedules, and retention policies assigned to various groups.

To view the Group Summary Reports:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Group Summary Reports** tab.



There are four tabs on the Group Summary Reports tab that provide details on the clients and policy for the group:

- **Datasets**—Shows which datasets are assigned to which groups, as well as the current properties for those datasets.
- **Schedules**—Shows which schedules are assigned to which groups, as well as the current properties for those schedules.
- **Retention Policies**—Shows which retention policies are assigned to which groups, as well as the current properties for those retention policies.
- **Clients**—Shows which clients are assigned to which groups, as well as any group policy overrides in effect for a particular client.

Viewing the Group Status Summary

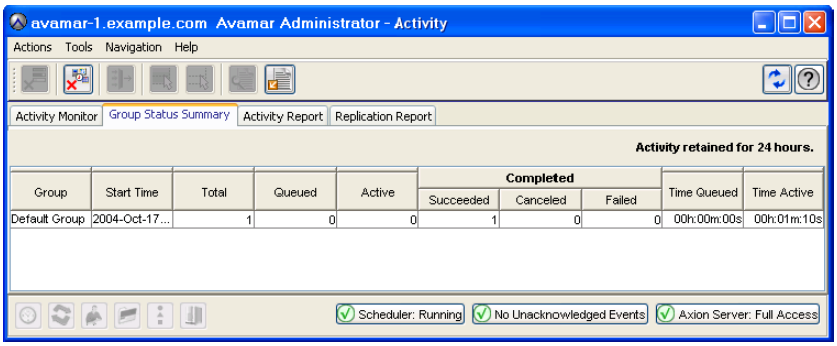
The Group Status Summary is a simplified presentation of all backup activity initiated as a result of group policies.

To view the Group Status Summary:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.

2. Click the **Group Status Summary** tab.



   The following table lists the information that appears on the Group Status Summary tab.

Table 28 Group Status Summary information

Column	Description
Group	Group name or “on-demand”. On-demand is a special logical grouping that summarizes all on-demand backup activity initiated from Avamar clients or Avamar Administrator. However, it is not a group in the Avamar server.
Start Time	Time that this group became eligible for the backup to run.
Total	Total number of backups initiated by way of this group policy.
Queued	Total number of backups, initiated by way of this group policy, that are currently in the scheduler queue.
Active	Total number of backups, initiated by way of this group policy, that are currently being performed.
Succeeded	Total number of backups, initiated by way of this group policy, that successfully completed.
Canceled	Total number of backups, initiated by way of this group policy, that were canceled before they could complete.
Failed	Total number of backups, initiated by way of this group policy, that did not successfully complete.
Time Queued	Interval from start time until the first client work order is started by any client in this group.
Time Active	Total amount of time used to perform all backup activities for this group. In other words, this is the interval from the time that the first client work order starts until the last client work order finishes.

Managing group membership

There are two ways to manage group membership in Avamar Administrator:

- **Group-centric**—Select a group, then add, move, or remove members, as discussed in "Adding, removing, or moving group members" on page 169.
- **Client-centric**—Select a client, then add or remove groups that the client is a member of, as discussed in "Editing client group memberships" on page 170.

You can add or remove multiple clients or groups during the same operation with either method of managing group membership.

The method that you use to manage group membership depends on the situation. For example, if you are adding or deleting multiple clients from a single group, then the group-centric method is efficient. Conversely, if you are adding or removing a single client from multiple groups, then the client-centric method is most efficient.

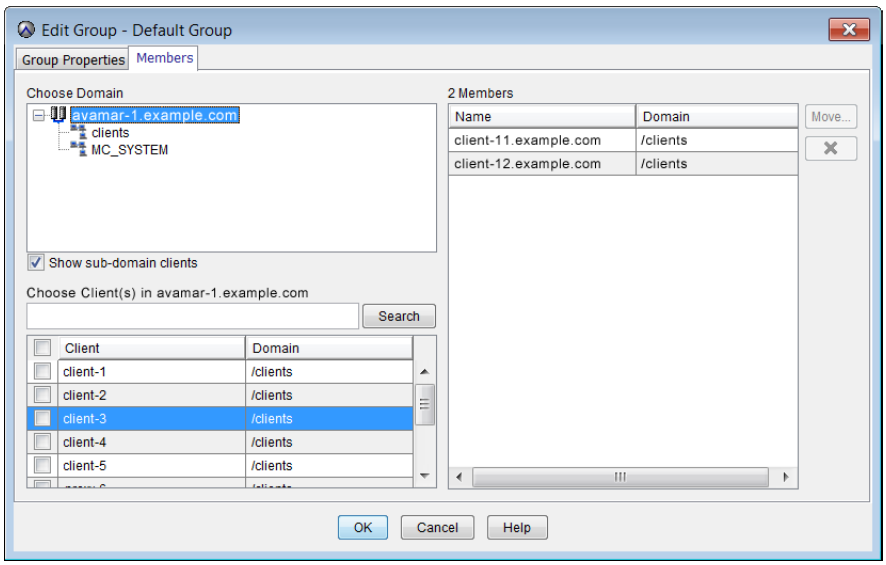
Adding, removing, or moving group members

To add, remove, or move group members:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups tab**.
4. Select a group to edit.
5. Select **Actions › Group › Edit Group**.

   The Edit Group dialog box appears.
6. Click the **Members** tab.



7. Do one of the following:
   - To add members, select checkboxes next to one or more clients. Selections appear in the **Member(s)** list.
   - To remove a member, select that **Member(s)** list entry and click **X**.
   - To move a member to another group:
     a. Select that **Member(s)** list entry and click **Move**.

        The Move Group Members dialog box appears.

     b. Select the new group for this member and click **OK**.

        The Move Group Members dialog box closes.
8. Click **OK**.

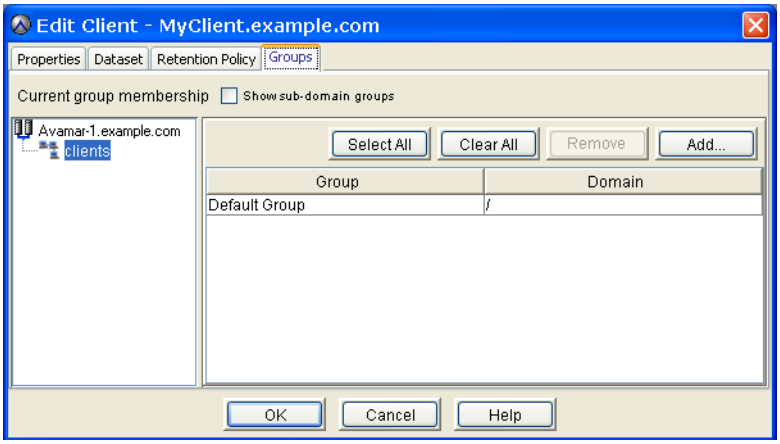
Editing client group memberships

To add or remove groups for a client:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select the client to edit.
5. Select **Actions › Group › Edit Client**.

   The Edit Client dialog box appears.
6. Click the **Groups** tab.



7. Add and remove groups for the client:
   - To add groups, click **Add**, select the groups, and then click **OK**.
   - To remove groups, select the groups from which to remove the client, and click **Remove**.
8. On the **Edit Client** dialog box, click **OK**.

Overriding group policy settings for a single client

The following sections describe how to override group policy settings for a single client:

- "Allowing users to initiate backups" on page 171
- "Allowing users to select data source for on-demand backups" on page 175
- "Allowing scheduled backups to run overtime" on page 176
- "Changing the encryption setting" on page 177
- "Allowing users to select an alternative backup start time" on page 178
- "Assigning backup limits" on page 180
- "Assigning a different dataset" on page 181
- "Allowing users to add to source data" on page 182
- "Assigning a different retention policy" on page 184

To implement group policy overrides for multiple clients, see "Overriding group policy settings for multiple clients" on page 185.

NOTICE

Too many overrides can make group policies less effective. Instead, implement a new group policy rather than repeatedly overriding an existing policy at the client level.

Allowing users to initiate backups

To allow users to initiate on-demand backups:

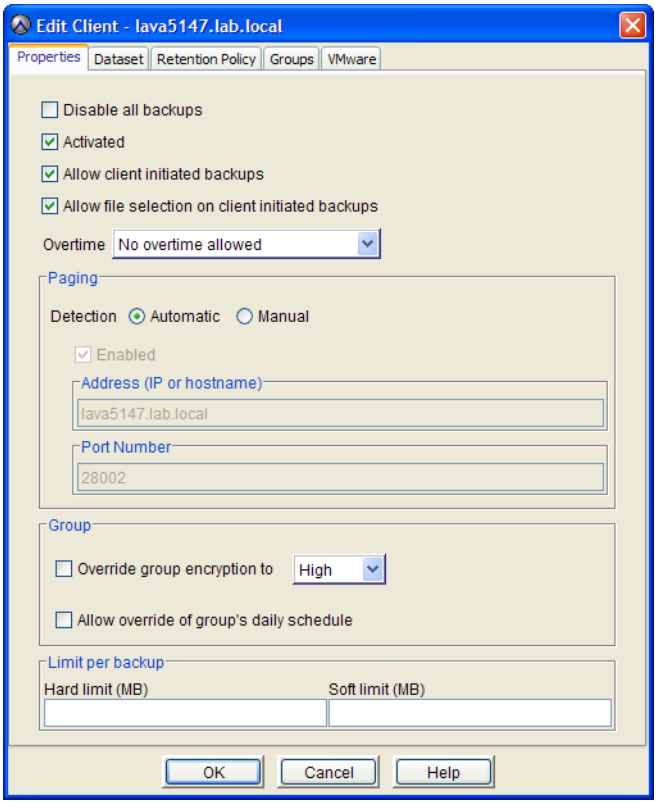
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.

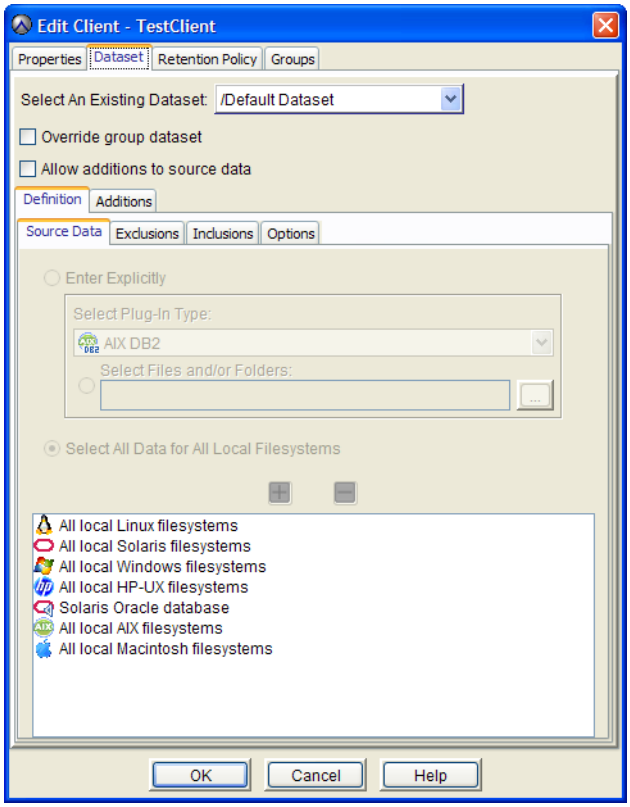


7. Select **Allow client initiated backups**.

   If no additional configuration is performed, backups initiated by this client include only those files selected by the user at the time the backup is started. In addition, End User On-Demand Retention, described in "Creating a retention policy" on page 150, is applied. However, you can enforce the use of a particular dataset and retention policy for all client-initiated backups.

8. To enforce the use of a particular dataset for all client-initiated backups:

   a. Click the **Dataset** tab.



   You cannot edit dataset properties in this window. Detailed dataset properties are shown so that you can review them before you make a selection.

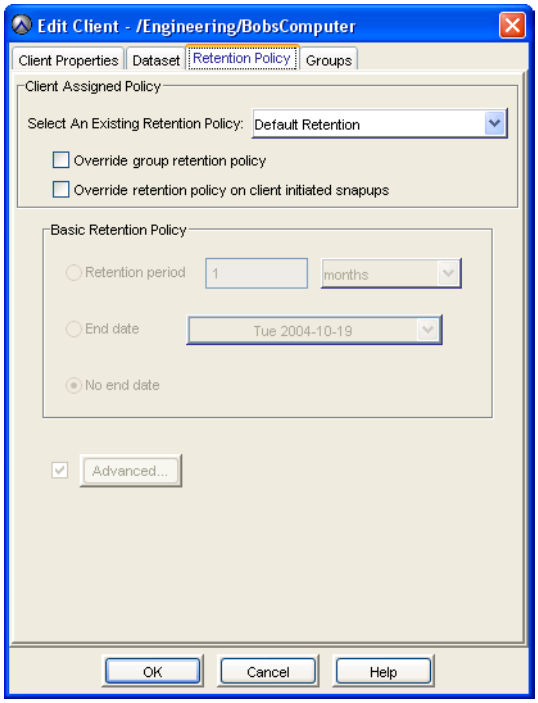
   b. Choose whether to use the group dataset or a different dataset for all client-initiated backups:

      – To use the dataset assigned to the group, clear the **Override group dataset** checkbox.

      – To use a different dataset, select the dataset from the **Select an Existing Dataset** list and then select the **Override group dataset** checkbox.

9. To enforce use of a particular retention policy for all client-initiated backups:

   a. Click the **Retention Policy** tab.



   You cannot edit retention policy properties in this window. Detailed retention policy properties are shown so that you can review them before you make a selection.

   b. Choose whether to use the group retention policy or a different retention policy for all client-initiated backups:

      – To use the retention policy assigned to the group, clear the **Override group retention policy** checkbox.

      – To use a different retention policy, select the retention policy from the **Select an Existing Retention Policy** list, select the **Override group retention policy** checkbox, and then select the **Override retention policy on client initiated backups** checkbox.

10. Click **OK**.

Allowing users to select data source for on-demand backups

You can permit users to create sets of folders and files to back up through an on-demand backup. When this feature is enabled, users can:

- Specify the folders and files to include in a backup set.
- Create multiple backup sets.
- Save backup sets for reuse.
- Perform an on-demand backup of the folders and files in the backup sets they create.

NOTICE

Folders and files selected through this feature are not subject to group dataset source limits, exclusions, or inclusions.

Automatic backup of clients according to their group policies is not affected by this feature.

User must have access to the Avamar client web UI from the client to create and save on-demand backup sets.

To use this feature, enable the Allow client initiated backups setting for the client, as described in "Allowing users to initiate backups" on page 171.

NOTICE

Windows, Mac, and Linux clients that use the desktop and laptop client enhancements require an additional configuration step to enable this setting. This is described in "Selectable backup sets" on page 558.

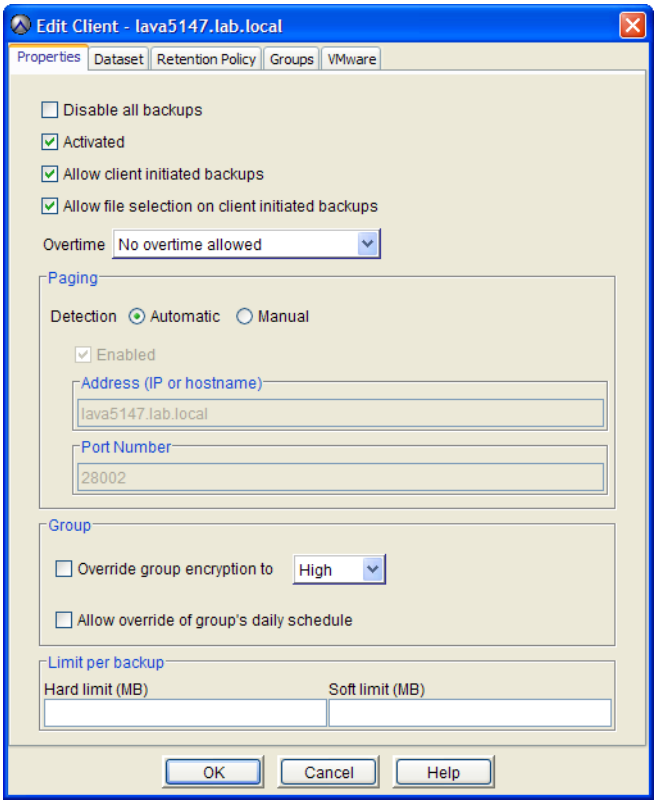
To enable user selection of data source for on-demand backups:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. Select **Allow client initiated backups**.
8. Select **Allow file selection on client initiated backups**.
9. Click **OK**.

Allowing scheduled backups to run overtime

You can override the group schedule duration setting for a client. This enables scheduled group backups initiated on the client to run as long as necessary for the backup to complete, regardless of the group schedule duration setting.

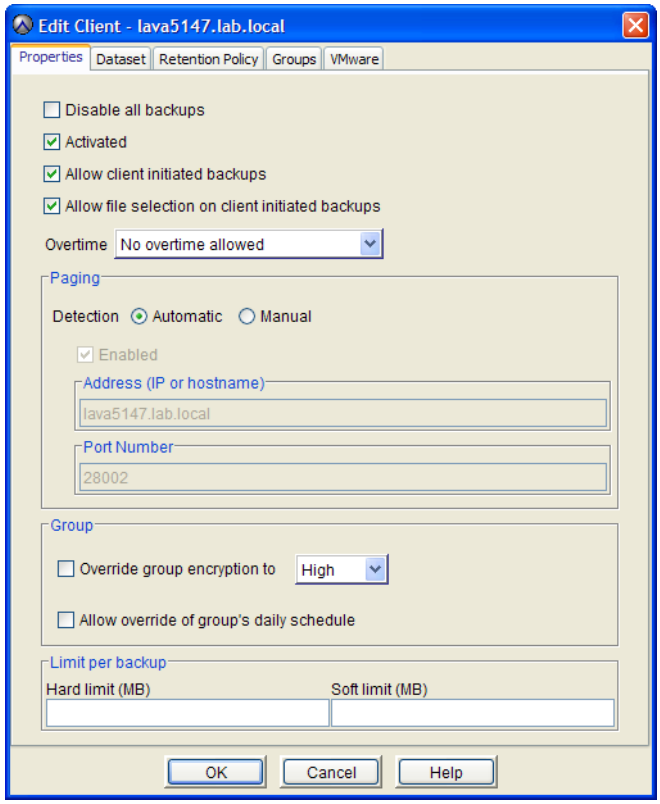
To allow scheduled backups to run overtime:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. Select one of these settings from the **Overtime** list:
   - **No overtime allowed**—Scheduled group backups are never allowed to run past the schedule duration setting.
   - **Always allow overtime**—Scheduled group backups are always allowed to run past the schedule duration setting.
   - **Overtime on next backup only**—Only the next scheduled group backup is allowed to run past the schedule duration setting.
   - **Overtime until successful backup**—Scheduled group backups are allowed to run past the schedule duration setting until a successful backup completes.
8. Click **OK**.

Changing the encryption setting

To change the client's encryption setting:

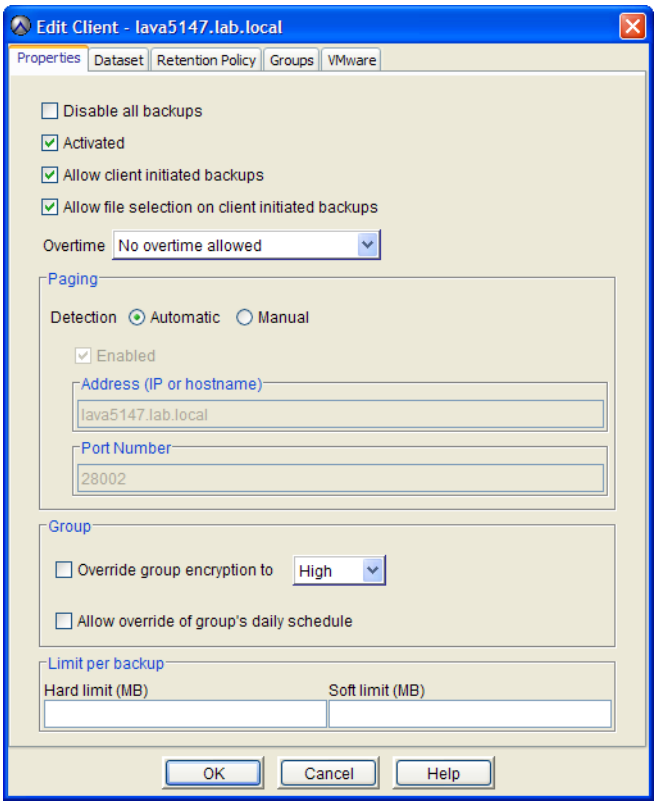
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.

5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. Select the encryption setting to use for client/server data transfer:

   The exact encryption technology and bit strength used for any given client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

8. Select **Override Group Encryption**.
9. Click **OK**.

Allowing users to select an alternative backup start time

The backup start time for a client is assigned through its group membership. You can allow users to select a different start time from a list of available times that you create.

In addition to enabling the policy override described here, the following requirements must be met:

- Add time entries to the override schedule as described in "Editing the Override Daily Schedule" on page 145.
- The group schedule being overridden must be a daily schedule.
- Users must have access to the web UI provided by the enhanced features for enterprise desktop and laptop computers.

More information about this feature is provided in "User selectable backup start times" on page 554.

To allow users to select an alternative backup start time:

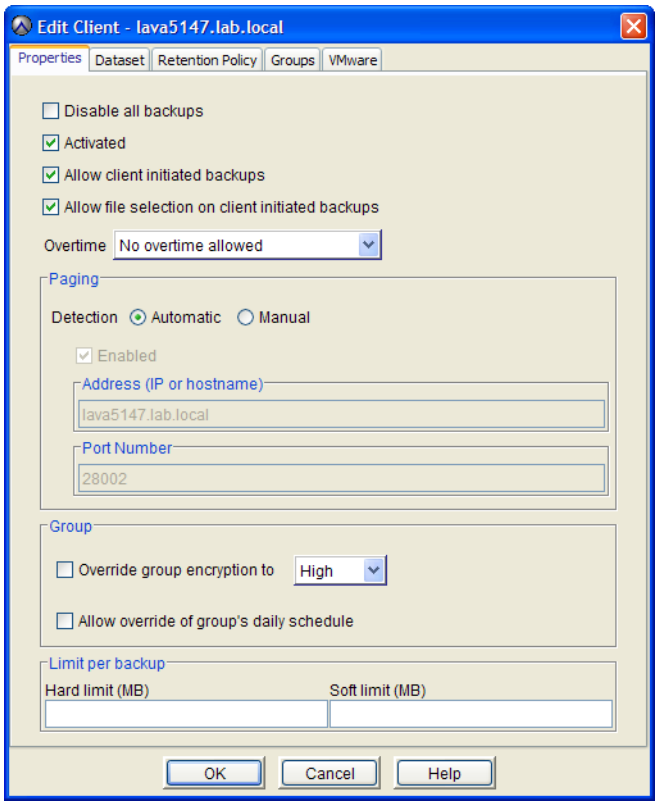
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. Select **Allow override of group's daily schedule**.
8. Click **OK**.

Assigning backup limits

To assign backup limits to a client:

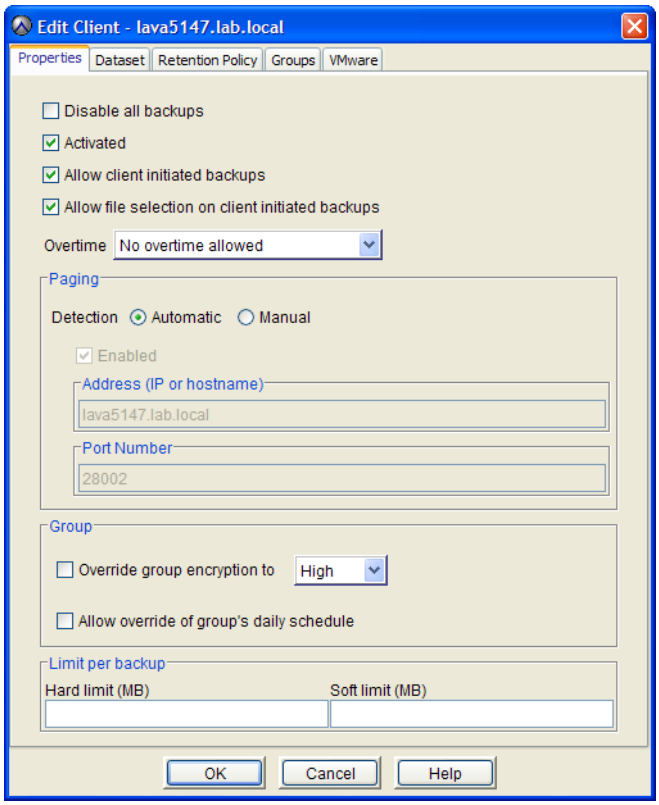
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Properties** tab.



7. In **Hard limit**, type an integer.

   This integer is the maximum allowed size, in megabytes, for the client's backups. Backups from the client that exceed that size are canceled. An acceptable value is any integer from **1** to ***99999*** (99,999 MB).

   When the client's hard limit is exceeded, the **Activity Report** entry for the client's backup displays `True` in the **hard_limit_exceeded** column, and the status entry `Hard limit exceeded` appears in the **Activity Monitor**.

8. In **Soft limit**, type an integer.

   This integer is the maximum size, in megabytes, beyond which the client's backups are flagged for excessive size. Backups from the client that exceed that size are allowed, but flagged in the Activity Report. An acceptable value is any integer from **1** to ***99999*** (*99,999* MB).

   When the client's soft limit is exceeded, the **Activity Report** entry for the client's backup displays `True` in the **soft_limit_exceeded** column, and the status entry `Completed` appears in the **Activity Monitor**.

9. Click **OK**.

Assigning a different dataset

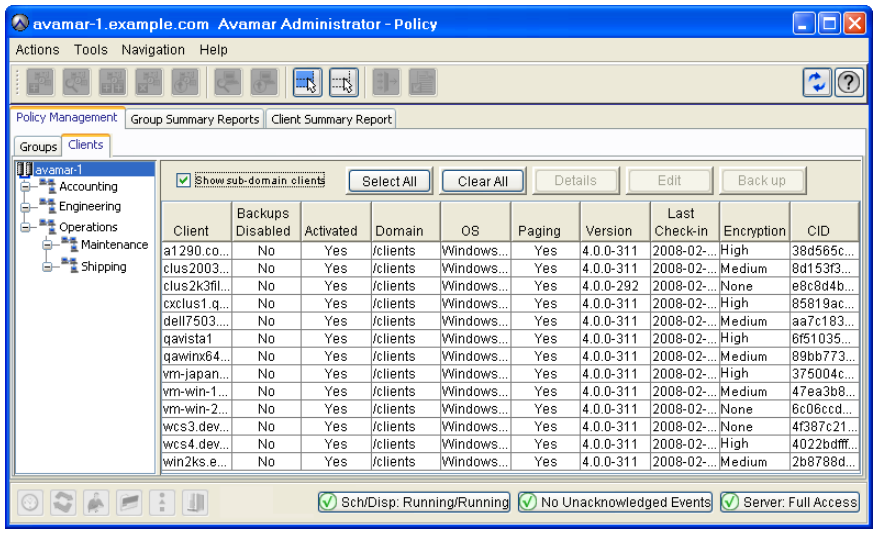
To assign a different dataset to a client:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.

3. Click the **Clients** tab.

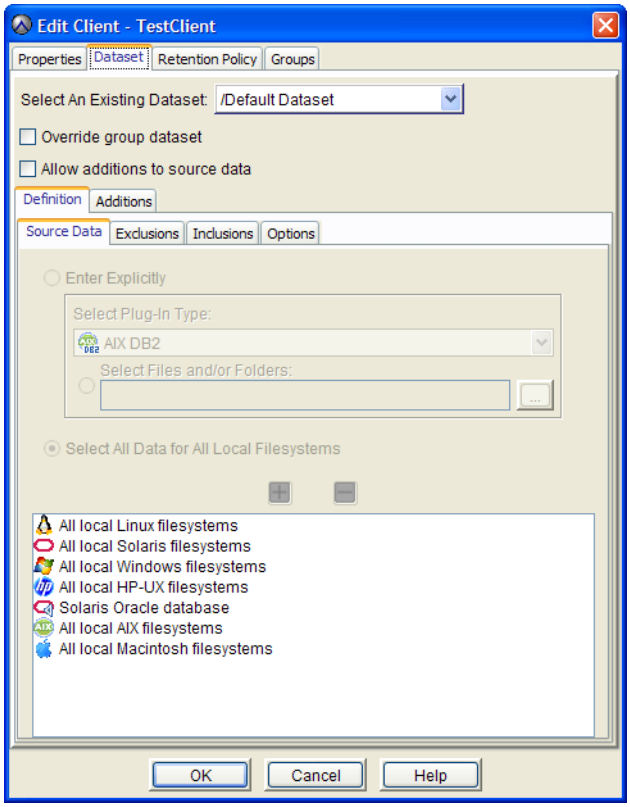


4. Select a client.

5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Dataset** tab.



7. Select a dataset from the **Select an Existing Dataset** list.

   You cannot edit dataset properties in this window. Detailed dataset properties are shown so that you can review them before you make a selection. "Editing a dataset" on page 131 provides details on how to edit dataset properties.

8. Select **Override group dataset**.

9. Click **OK**.

Allowing users to add to source data

You can allow users to add folders to the source data for the group datasets assigned to the users' clients. This is subject to the following rules:

- Group exclusion and inclusion lists are applied to the added data.
- The added data is included in every automatic and on-demand backup for every group assigned to the client.
- The user must have access to the Avamar client web UI from the client to add or remove data.

By default, this feature is disabled.

To enable user additions to source data:

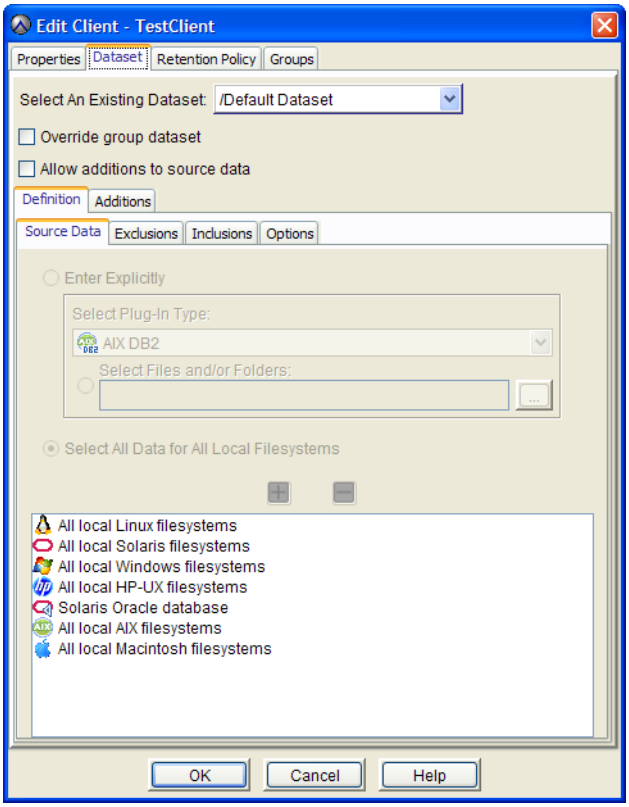
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Select **Actions** › **Client** › **Edit Client**.

   The Edit Client window appears.

6. Click the **Dataset** tab.



7. Select **Allow additions to source data**.

   NOTICE

   When users add source data, you can view the additions for each client by clicking the Additions tab on the Dataset tab of the Edit Client dialog box.

8. Click **OK**.

Assigning a different retention policy

The retention policy assigned to the client is the retention policy that is used for on-demand backups of the client. "Performing an on-demand backup" on page 96 provides details.

To assign a different retention policy to a client:

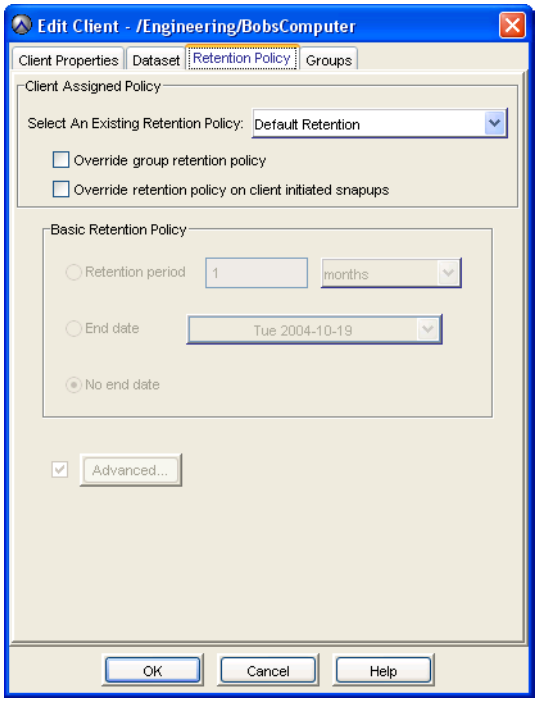
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The Edit Client window appears.

6. Click the **Retention Policy** tab.



7. Select a retention policy from the **Select an Existing Retention Policy** list.

   You cannot edit retention policy properties in this window. Detailed retention policy properties are shown so that you can review them before you make a selection. "Editing a retention policy" on page 151 provides details on how to edit retention policy properties.

8. Select **Override group retention policy**.
9. Click **OK**.

Overriding group policy settings for multiple clients

The following group policy override settings are available to selected groups of clients:

- Allow client initiated backups

  When enabled this setting allows users of the selected clients to initiate an on-demand backup. Additional information about this setting is available in "Allowing users to initiate backups" on page 171.

- Overtime

  When enabled this setting allows backups for the selected clients to run past the cut-off time specified for the group. Additional information about this setting is available in "Allowing scheduled backups to run overtime" on page 176.

- Encryption method and Override group encryption to

  These settings override the group's encryption setting. Additional information about this setting is available in "Changing the encryption setting" on page 177.

- Allow additions to source data

  When enabled, this setting allows users of the selected clients to add folders and files to the source data for all scheduled backups. Additional information about this setting is available in "Allowing users to add to source data" on page 182.

- Allow override of group's daily schedule

  When enabled, this setting allows users to select a backup start time different from the time assigned to the group. Additional information about this setting is available in "Allowing users to select an alternative backup start time" on page 178.

- Allow file selection on client initiated backups

  When enabled, this setting allows users of the selected clients to select folders and files to include in on-demand backups. Additional information about this setting is available in "Allowing users to select data source for on-demand backups" on page 175.

- Hard limit and Soft limit

  These settings specify the size beyond which a backup is canceled for being too large (hard limit) and the size beyond which a backup is flagged for size but allowed to complete (soft limit). Additional information about these settings is available in "Assigning backup limits" on page 180.

To override group policy settings for multiple clients:

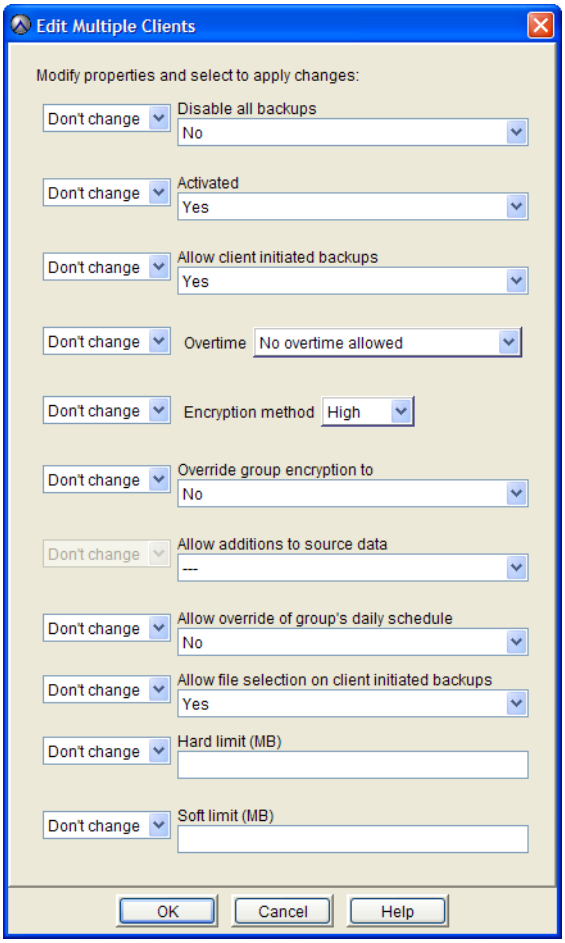
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select two or more clients.

5. Click **Edit**.

   The Edit Multiple Clients window appears. The current group setting appears in each field.



6. Change a setting in a field and, in the drop down list next to the field, select **Apply the change**.
7. Click **OK**.

The group policy override settings are applied to the selected clients.

Performing on-demand group and client backups

Occasionally, you may want to back up an entire group of clients, or an individual client at some time other than the regularly scheduled time. While you can perform individual on-demand backups for each client, this can be time-consuming if there are many clients. Furthermore, you cannot manage on-demand backups using advanced retention settings; they can only be assigned a static expiration date. Instead, you can perform an on-demand group backup, which may take less time and also enables you to manage the backups using advanced retention settings.

On-demand group backups

To perform an on-demand group backup:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select a group and click **Back Up**.

   A confirmation message appears.
5. Click **OK**.

On-demand client backups

You can also perform on-demand client backups from the Backup, Restore and Manage window. "Performing an on-demand backup" on page 96 provides details.

To perform an on-demand client backup:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client and click **Back Up**.

   A confirmation message appears.
5. Click **OK**.

Perfoming on-demand group and client replications

Occasionally, you may want to replicate an entire group of clients, or an individual client.

On-demand group replications

You can also initiate on-demand group replication from the Replication window. "Performing an on-demand group replication" on page 384 provides details.

To perform on-demand group replication:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group and click **Replicate**.

   A confirmation message appears.
5. Click **Close**.

On-demand client replications

To perform on-demand client replication:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select the group and click **Replicate**.

   The Select Group for Client Replicate dialog box appears.
5. Select a replication group from the Use Properties of group list.
6. Click **OK**.

   The Select Group for Client Replicate dialog box closes.

   A confirmation message appears.
7. Click **Close**.

CHAPTER 7
Events, Notifications, and Profiles

The following topics discuss Avamar events and features that generate notifications when specific events occur:

- Important terms and concepts 190
- Editing system event profile properties 195
- Creating a custom event profile 196
- Editing custom event profile properties 203
- Copying a custom event profile 204
- Testing custom event profile notifications 205
- Enabling and disabling a custom event profile 206
- Deleting a custom event profile 206
- Modifying “Email Home” configuration 206
- Monitoring the Avamar server using syslog 209
- Monitoring the Avamar server using SNMP 218
- Managing ConnectEMC 224
- Enabling and disabling ConnectEMC 225
- Stopping and starting ConnectEMC 226
- Editing Primary and Failover transports 227
- Editing the Notification transport 230
- Testing transports 232

Important terms and concepts

The following topics discuss the fundamental principles of Avamar events, notifications, and profiles.

Events

All Avamar system activity and operational status is reported as events to the MCS. Examples of Avamar events include client registration and activation, successful and failed backups, and hard disk status. Each event contains the information in the following table.

Table 29 Event information

Information	Description
Event code	Unique identifier
Date and time	Date and time the event was reported
Category	Category of event: • SYSTEM • APPLICATION • USER • SECURITY
Type	Type of event: • INTERNAL • ERROR • WARNING • INFORMATION • DEBUG
Summary	A one-line summary description of the event
Hardware source	System node that reported the event
Software source	System or application module that reported the event

A sequential listing of all event codes, including the previously described summary information, is available in /usr/local/avamar/doc/event_catalog.txt on the Avamar server.

Accessing the event catalog by using a web browser

The Avamar server also provides the contents of event_catalog.txt through a web server.

1. Open a web browser and type the following URL:

   http://AVAMARSERVER

   where AVAMARSERVER is the Avamar server network hostname (as defined in DNS) or IP address.

   You are redirected to the Avamar secure web server. The protocol changes to HTTPS. You may see an alert page if the server's certificate is not accepted by your web browser. Continue to the Avamar Web Restore Home page.

2. From the links at the top of the Avamar Web Restore Home page, click **Documentation**.

   The Avamar Documentation page appears.

3. Find the listing **Avamar Event Codes** and click the plus icon next to it.

   The listing expands and the **event_catalog.txt** link appears.

4. Click **event_catalog.txt**.

The event_catalog.txt file opens in the web browser.

Audit logging

System events with a category of SECURITY and type of AUDIT are used to implement the Avamar audit logging feature. This feature keeps a permanent log of system actions initiated by users. The data in this log enables enterprises that deploy Avamar to enforce security policies, detect security breaches or deviation from policies, and hold users accountable for those actions.

Only actions that are initiated by users are logged. Actions initiated by the system without a user account, such as scheduled backups, maintenance activities, and so forth, are not logged.

Because the underlying data for audit log entries are system events, this information is available in two places:

- Event Monitor, which also contains all other system events
- Audit Log, which only contains events that are also audit log entries

By default, audit log information is retained for one year.

You can increase or reduce the audit log retention period by editing the value of clean_db_audits_days in /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml, and restarting the MCS.

Customizing error events

By default, Avamar software continually monitors /var/log/messages for any occurrence of the case-insensitive search string “error.” Any occurrences of “error” create an event code of the type ERROR.

You can customize this default behavior by defining additional search strings that also create Avamar ERROR events. Add these additional search case-insensitive strings to /usr/local/avamar/var/mc/server_data/adminlogpattern.xml.

Notifications

The following features generate notifications when specific events occur.

Pop-up alerts

Events can be configured on an event-by-event basis to generate a graphical pop-up alert each time one of those events occurs. One significant limitation of this feature is that Avamar Administrator software must be running for the pop-up alerts to appear.

Acknowledgement required list

You can specify that when a certain event type occurs, the Avamar system administrator must acknowledge the event.

Email messages

You can specify that when a certain event type occurs, an email message is sent to a designated list of recipients. Email notifications can be sent immediately or in batches at scheduled times.

A typical batch email notification message looks like this:

```
MCS: avamar-1.example.com
   MCS Version: 6.1.0-nnn
   Avamar Server: avamar-1.example.com
   Avamar Server Version: 6.1.0-nnn

   Event profile: My Custom Profile
   Count of events: 3

   Summary of events:


   Type               Code         Count        Summary
   -----------        ------       ------       -------
   INFORMATION        22207           1         New group created
   INFORMATION        22208           1         Group modified
   INFORMATION        22209           1         Group deleted

   Event Code = 22207
   Event Date/Time = 5/10/12 09:58:20 PDT
   Event Type = INFORMATION
   Event Severity = OK
   Event Summary = New group created
   Software Source = MCS:CR

   Event Code = 22209
   Event Date/Time = 5/10/12 09:58:25 PDT
   Event Type = INFORMATION
   Event Severity = OK
   Event Summary = Group deleted
   Software Source = MCS:CR

   Event Code = 22208
   Event Date/Time = 5/10/12 10:55:28 PDT
   Event Type = INFORMATION
   Event Severity = OK
   Event Summary = Group modified
   Software Source = MCS:CR
```

Syslog support

You can specify that when an event type occurs, Avamar logs information to local or remote syslog files based on filtering rules configured for the syslog daemon that receives the events. Third-party monitoring tools and utilities capable of examining log entries can access the syslog files and process them to integrate Avamar event information into larger site activity and status reports. "Monitoring the Avamar server using syslog" on page 209 provides details.

SNMP support

The Avamar SNMP implementation provides two ways to access Avamar server events and activity completion status:

- SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled client (in this case, the Avamar server).
- SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications whenever designated Avamar events occur. You can configure an event type to output SNMP traps.

"Monitoring the Avamar server using SNMP" on page 218 provides details.

Profiles

Profiles are a notification management feature that are used to logically group certain event codes together and specify which notifications to generate when the events occur. There are two basic types of event profiles:

- **System profile**—There is only one System event profile. It contains all possible system event codes.
- **Custom profiles**—Custom profiles are used to send various notifications when certain system events occur. You can create as many custom profiles as you need to organize system events and generate notifications when any of those events occur.

Profile catalog

The default Avamar configuration includes the profiles described in this section.

System profile

There is only one System event profile. It contains all possible system event codes.

Evaluation profile

The Evaluation profile is primarily intended to be used to support system evaluations. If enabled, this profile generates an email notification and attaches two weeks' worth of Activities - DPN Summary report information to the email message. "Activities - DPN Summary" on page 234 provides details.

High Priority Events profile

The High Priority Events profile is enabled by default. This special event profile automatically emails the following information to EMC Customer Support (emailhome@avamar.com) twice daily:

- Status of the daily data integrity check
- Selected Avamar server warnings and information messages
- Any Avamar server errors

NOTICE

The only change you can make to the High Priority Events profile is to add email addresses to the Recipient Email List. If you require custom High Priority Events profile settings, copy it and then edit the copy.

"Modifying "Email Home" configuration" on page 206 provides additional information.

Local SNMP Trap profile

The Local SNMP Trap profile is read-only and is intended to be used for test purposes only. It is intended to be used to verify that traps are successfully generated and received by the local **snmptrapd** process, which then writes the trap information to a syslog file. "Monitoring the Avamar server using SNMP" on page 218 provides details.

Local Syslog profile

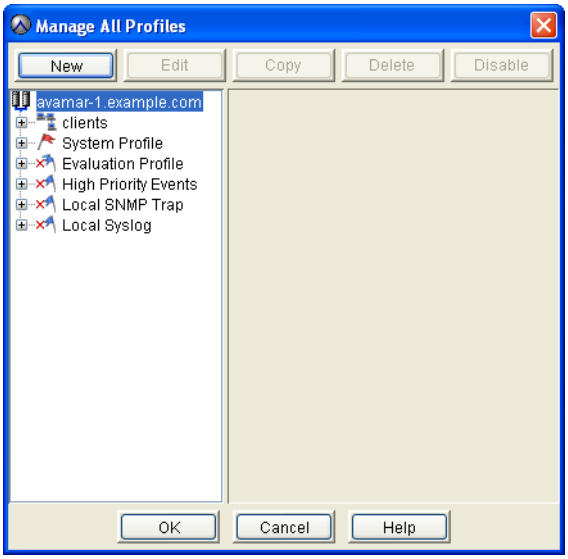
If enabled, the Local Syslog profile reports status by way of the local **syslogd** process on the Avamar server. "Monitoring the Avamar server using syslog" on page 209 provides details.

Editing system event profile properties

To edit system event profile properties:

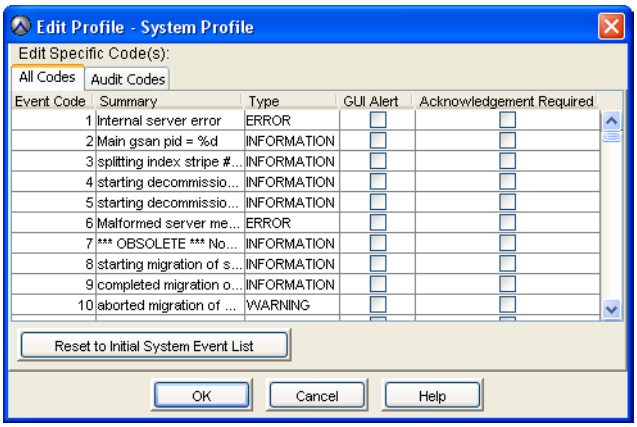
1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.



2. Select the **System Profile** in the tree pane and click **Edit**.

   The Edit Profile dialog box appears with a list of event codes.



3. To show a graphical pop-up alert on the Avamar Administrator client each time an event occurs, select the **GUI Alert** checkbox next to the event.
4. To add an entry to the common unacknowledged events list each time an event occurs, select the **Acknowledgement Required** checkbox.
5. Click **OK**.

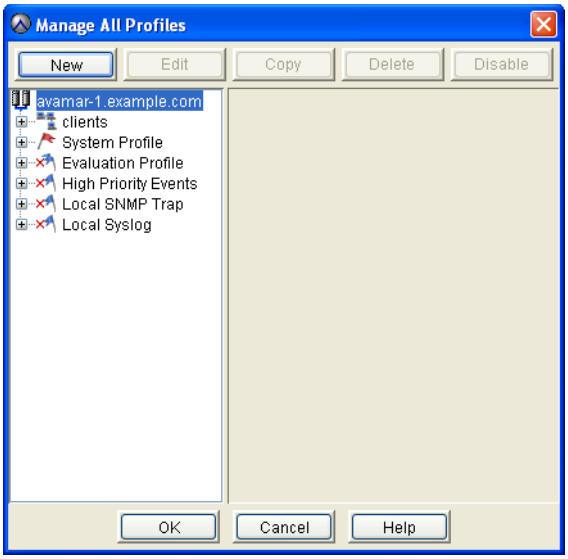
Creating a custom event profile

You cannot view system events and profiles outside the domain. This affects the profiles that you can edit and the events that you can add to a profile.

To create a custom event profile:

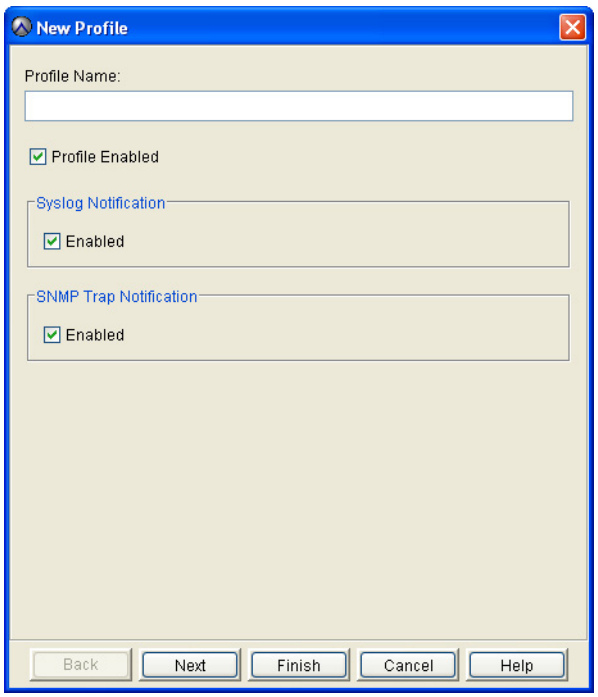
1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.



2. In the tree, select the domain for the custom event profile and click **New**.

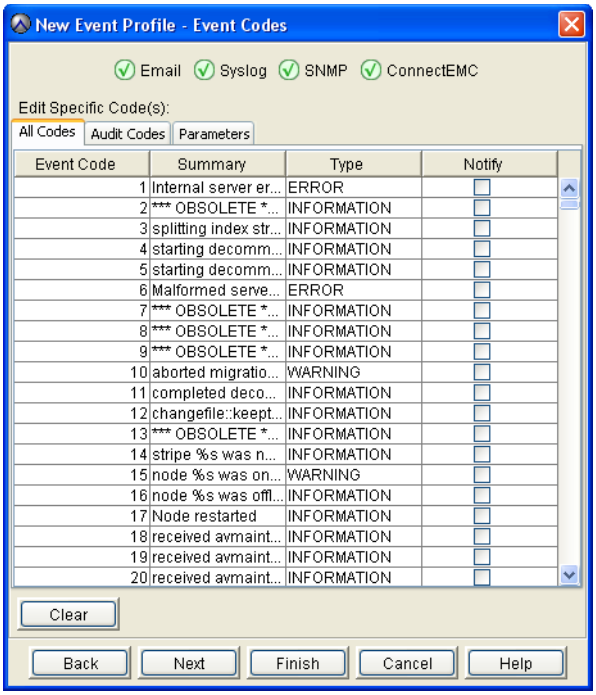
   The New Profile wizard appears.



3. Complete the settings in the **New Profile** wizard:
   a. In the **Profile Name** box, type a name for this event profile.
   b. Clear the **Profile Enabled** option to disable the event profile. You can enable it at a later time.
   c. Clear the **Syslog Notification – Enabled** option if you do not want to use the syslog notification feature with this profile,
   d. Clear the **SNMP Trap Notification – Enabled** option if you do not want to use the SNMP notification feature with this profile.
4. Click **Next**.

   The Event Codes wizard screen appears.

   If you are adding this custom event profile at the top-level (that is, not to a domain or subdomain), you can also change the parameters used to control capacity forecast alerts.



5. Specify which error codes should trigger notifications:
   a. Click the **All Codes** tab.
   b. Select the **Notify** option for one or more error codes.

NOTICE

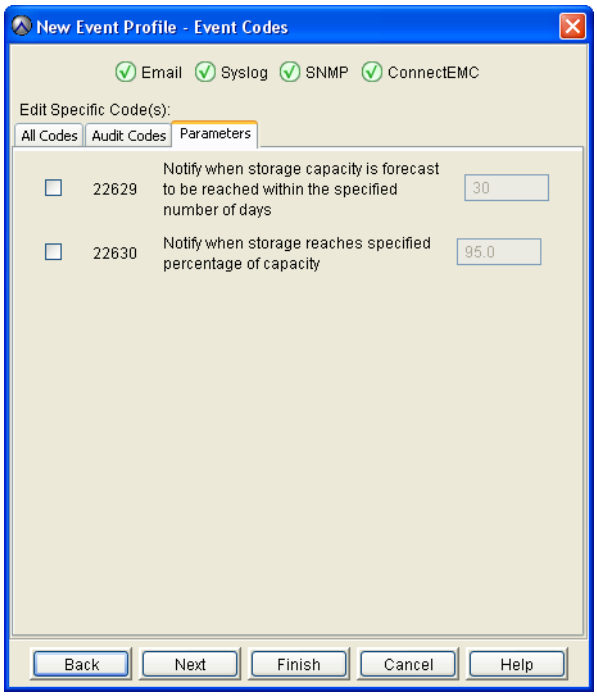
An asterisk (*) next to an event code indicates an event of such severity that a notification is sent when that event occurs, even if other event notifications are sent on a schedule.

6. Specify which audit codes should trigger notifications:
   a. Click the **Audit Codes** tab.
   b. Select the **Notify** option for one or more error codes.

   NOTICE

   An asterisk (*) next to an audit code indicates an event of such severity that a notification is sent when that event occurs, even if other event notifications are sent on a schedule.

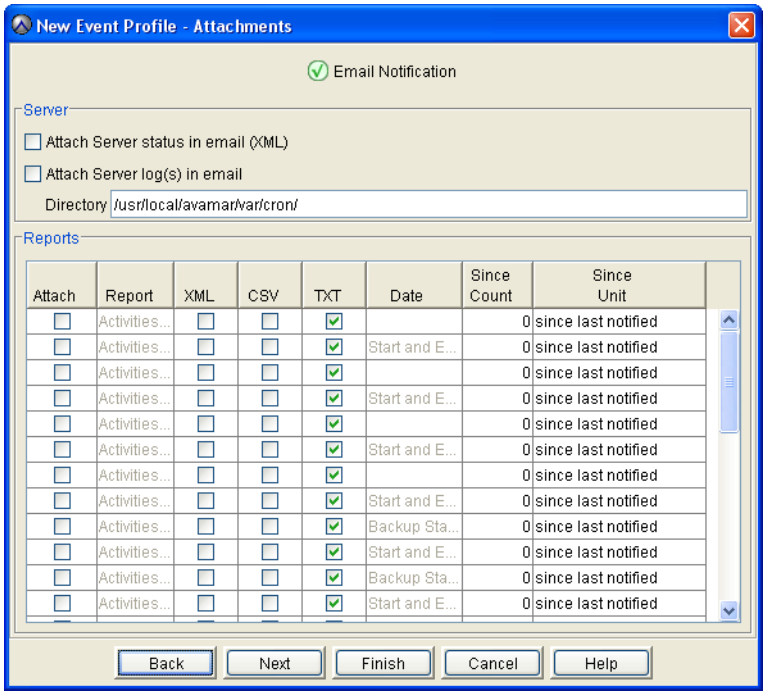
7. If you are adding this custom event profile at the top-level (that is, not to a domain or subdomain), specify the parameters to control capacity forecast alerts:
   a. Click the **Parameters** tab.



   b. Select the checkbox next to the parameter, and then type a new value for the parameter.
   c. Repeat the previous step as necessary for each parameter.

8. Click **Next**.

   The Attachments wizard screen appears.



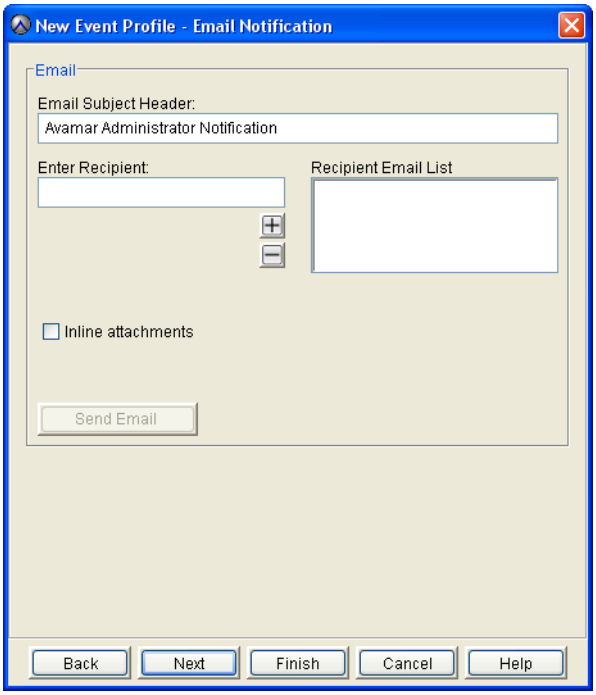
9. (Optional) To include a report of overall Avamar server status in XML format in email notification messages, select the **Attach Server status in email (XML)** checkbox.
10. (Optional) To include Avamar server logs in email notification messages, select the **Attach Server logs in email checkbox** and then type the full path to the location of Avamar server logs in the **Directory** text box. The default location is /usr/local/avamar/var/cron/.
11. Specify the reports to include in email notification messages:
    a. Select the **Attach** checkbox next to the report.
    b. Select the checkbox next to the file format in which to send the report.
       - **XML**—Extensible Markup Language (XML) file, useful for sharing data with other applications
       - **CSV**—Comma-Separated Values (CSV) text file, useful for importing into a spreadsheet
       - **TXT**—Plain text file
    c. Specify the number of historical reports of this type to send with each notification message using the **Since Count** and **Since Unit** fields. For example, send the past two months of these reports.

       The following values are available from the Since Count list:

       - day(s) ago
       - week(s) ago
       - month(s) ago
       - since last modified

12. Click **Next**.

    The Email Notification wizard screen appears.



13. Specify the recipients and options for the email notification messages:

    a. **In the Email Subject Header** box, type an email subject line for the notification message.

    b. Type an email address in the **Enter Recipient** box using the format, user@domain format, and then click **+**. Or, to remove a recipient from the **Recipient Email List**, select the recipient and click **-**.

    c. To insert all attachments into the body of the email notification message, select the **Inline attachment** option.

    NOTICE

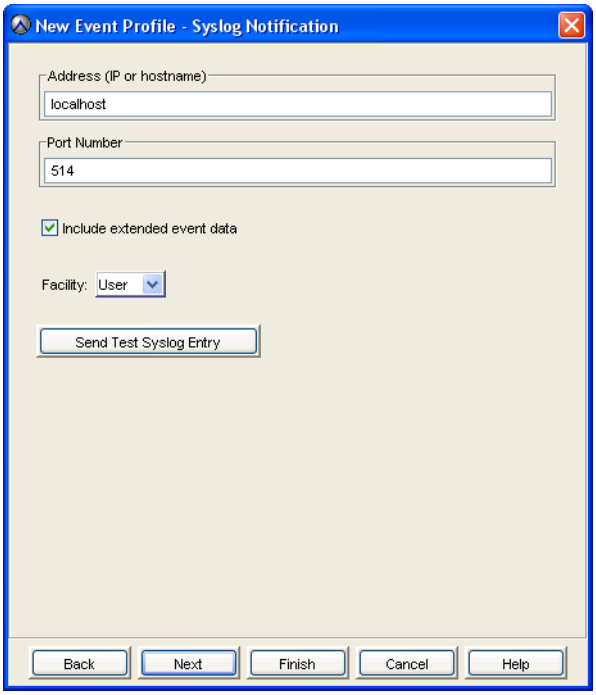
    When you insert the attachments, the email message may be very long.

    d. To immediately send a test email message, click **Send Email**.

    If the test email message is sent successfully, an "Email accepted by transport layer" confirmation message appears.

14. Click **Next**.

    The next wizard screen appears.



15. Specify syslog notification parameters as described below:

    a. In the **Address (IP or hostname)** box, type the IP address or hostname of the Avamar server node running the syslogd process.

    b. In the **Port Number** box, type the port number used for syslog communication.

    c. Select the **Include extended event data** option if you want to include extended event code information in the syslog message. This extended information is delimited using the following tags:

       – ‹Code›
       – ‹Type›
       – ‹Severity›
       – ‹Category›
       – ‹HwSource›
       – ‹Summary›
       – ‹active›
       – ‹lastEmailSendDate›
       – ‹domain›
       – ‹scheduleID›
       – ‹num_prefs›
       – ‹name›
       – ‹isSystem›

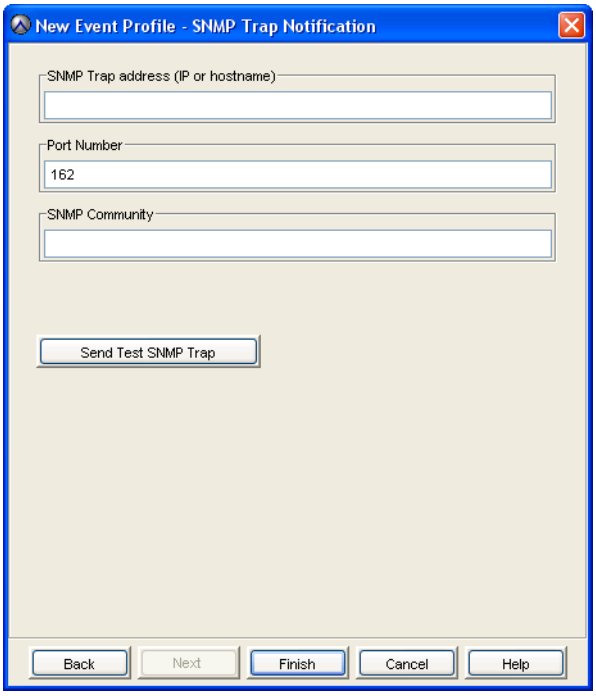
d. From the **Facility** list, select one of the following: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.

NOTICE

To test the syslog notification parameters, click **Send Test Syslog Entry**.

16. Click **Next**.

The next wizard screen appears.



17. Specify SNMP notification parameters:

a. In the **SNMP Trap Address (IP or hostname)** box, type the IP address or hostname of the computer running an application that is capable of receiving and processing an SNMP trap.

b. In the **Port Number** box, type the port number on the host machine that is listening for SNMP traps. The default data port is 162.

c. In the **SNMP Community** box, type the name of the SNMP community that the SNMP trap listener is configured to use.

NOTICE

The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application.

18. Click **Finish**.

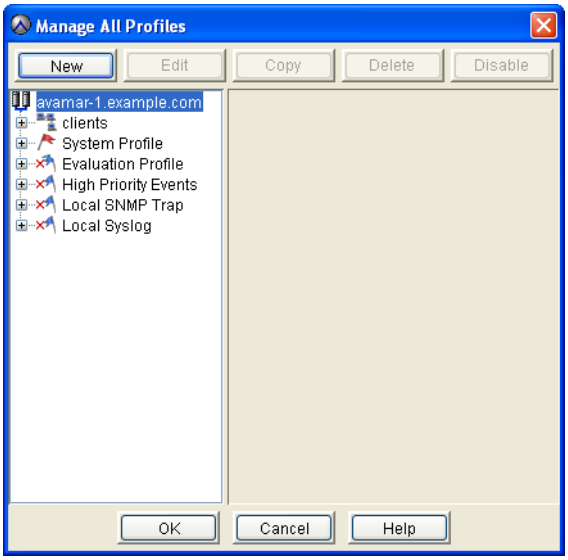
Editing custom event profile properties

You cannot view system events and profiles outside the domain that you are logged in to. This affects the profiles that you can edit and the specific events that you can add to any profile.

To edit the properties for a custom event profile:

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.



2. Select a custom event profile in the tree pane and click **Edit**.

   The Edit Profile dialog box appears.

3. Edit the custom event profile information.

   "Creating a custom event profile" on page 196 provides details on custom event profile properties.

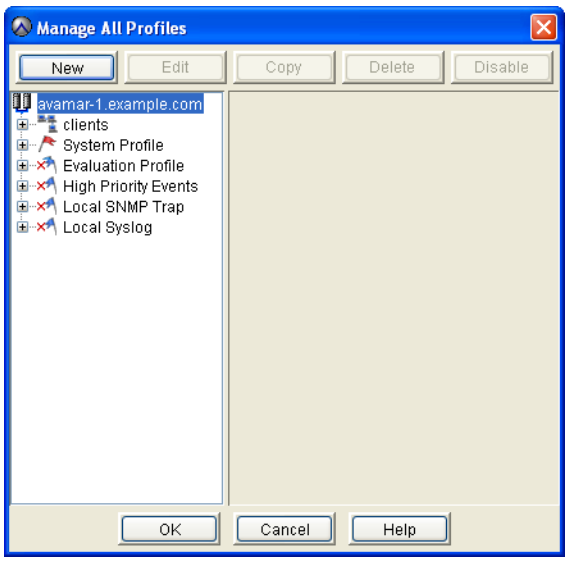
4. Click **OK**.

Copying a custom event profile

To copy a custom event profile:

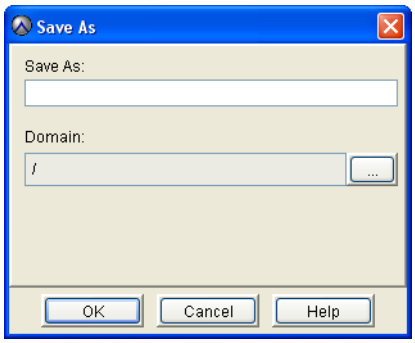
1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.



2. In the tree, select the profile and click **Copy**.

   The Save As dialog box appears.



3. Type a name for the new custom event profile in the **Save As** field.

   By default, the domain field is populated with the domain of the custom event profile that you copy.

4. (Optional) To copy the new custom event profile to a different domain, click the **...** button, browse to the new domain, and then click **OK**.

5. Click **OK**.

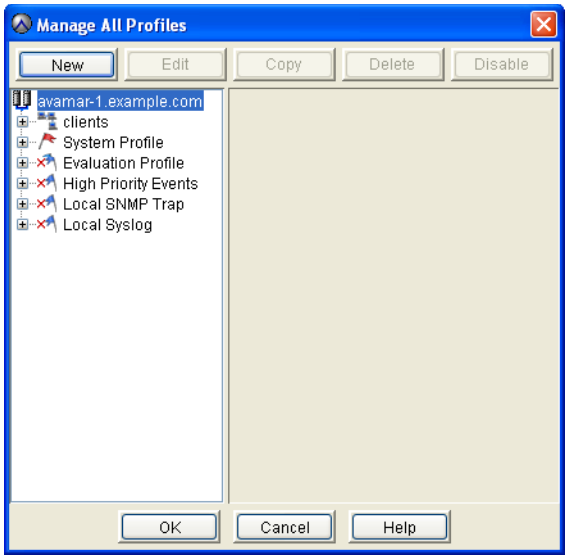
Testing custom event profile notifications

You can test custom event profile notification mechanisms by sending a short email message or writing a short message to the syslog file.

To test custom event profile notifications:

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.



2. Select a custom event profile in the tree pane and click **Edit**.

   The Edit Profile dialog box appears.

3. Test the custom event profile notification as described in the following table.

Table 30 Test methods for custom event profile notifications

Test Method	Do This
Send a test email message.	1. Click the **Email Notification** tab. 2. Click **Send Email**. If the test email message is successfully sent, an "Email accepted by transport layer" confirmation message appears. 3. Click **OK**.
Write a test message to the syslog file.	1. Click the **Syslog Notification** tab. 2. Click **Send Test Syslog Entry**. If the test syslog message is successfully written, an "Initiated syslog notification confirmation" message appears. 3. Click **OK**.
Send a test SNMP trap message.	1. Click the **SNMP Trap Notification** tab. 2. Click **Send Test SNMP Trap**. If the test SNMP trap message is successfully sent, an "Initiated SNMP trap notification" confirmation message appears. 3. Click **OK**.

4. Click **OK**.

Enabling and disabling a custom event profile

When you disable an event profile, no email notifications are sent until you reenable the profile. You can disable any profile except the System events profile.

To enable and disable a custom event profile:

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.

2. Select the event profile.
3. Click **Disable** to disable the event profile, or **Enable** to enable the event profile.

Deleting a custom event profile

You can permanently delete any custom event profile except the System events profile.

To delete a custom event profile:

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.

2. Select the event profile and click **Delete**.

   A confirmation message appears.

3. Click **Yes**.

Modifying “Email Home” configuration

When configured and enabled, the Email Home feature automatically emails configuration, capacity, and general system information to EMC Customer Support once daily, and critical alerts in near-real time on an as needed basis.

NOTICE

The Email Home feature is configured and enabled during installation. This section is intended only for changes to the feature after initial installation.

By default, notification schedule email messages are sent at 6 a.m. and 3 p.m. each day. The timing of these messages is controlled by the Notification Schedule, which is discussed in “Schedules” on page 134.

To properly configure the Email Home feature, you need the following mail settings:

- **Outgoing SMTP Mail Server Name**—This is the corporate outgoing SMTP mail server that is used to send Email Home messages.

  Typically, the outgoing SMTP mail server name is specified during initial Avamar server deployment. However, you must verify this setting. You can change this setting, if necessary.

  NOTICE

  In most cases, some arrangement must be made to enable emails originating from the Avamar server to be forwarded through the outgoing SMTP mail server to EMC Customer Support over the Internet.

- **Administrative Mail Sender Address**—For Email Home messages to be received by EMC Customer Support, they must be sent using a valid email address with access to a corporate outgoing SMTP mail server.

  NOTICE

  If you do not configure the Email Home feature to send messages from a valid email address, messages generated by the Email Home feature are rejected by the EMC incoming email server. EMC Customer Support is completely unaware that these programmatically-generated messages were rejected. In addition, because a valid sending email account is not known, programmatically-generated warnings to the sender that these messages could not be sent are never viewed by anyone who can correct the problem.

Modify mcserver.xml Email Home settings

To modify mcserver.xml Email Home settings:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Change directories by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

3. Open mcserver.xml in a UNIX text editor.

4. Find the com.avamar.asn.module.mail node, as shown here:

```
<root type="system">
   <node name="com">
      <node name="avamar">
         <node name="asn">
            <node name="module">
               <node name="mail">
                  <entry key="smtpHost" value="mail"/>
                  <entry key="admin_mail_sender_address"
value=""/>
```

NOTICE

Substantial portions of mcserver.xml have been omitted for clarity.

5. Verify that the smtpHost entry, which is `mail` in the previous step, is the name of the outgoing SMTP mail server as defined in corporate DNS, such as smtp.example.com.

NOTICE

The Avamar 6.0 and later server installation or upgrade fills in the smtpHost entry.

If this entry is not correct, edit it.

6. Change the admin_mail_sender_address entry to a valid email address, such as jsmith@example.com.
7. Save the changes.
8. Restart the MCS by typing:

```
dpnctl stop mcs
dpnctl start
```

9. Close the command shell.

Monitoring the Avamar server using syslog

UNIX and Linux systems provide a system logging feature called syslog, which collects system log messages and writes them to a designated log file. Avamar servers can be configured to send event information in syslog format.

The Avamar server supports both syslog and syslog-ng implementations.

Prerequisite knowledge and resources

Persons configuring syslog monitoring of an Avamar server should be familiar with basic syslog concepts. A complete discussion of basic syslog concepts and implementation is beyond the scope of this guide. The www.syslog.org website provides additional information.

Overview

This topic provides an overview of syslog implementations.

The syslogd process

At the operating system level, system monitoring and logging relies on the syslogd process to collect system log messages and write them to a designated log file. The syslogd process runs locally on every Avamar server node.

However, without additional configuration, each node's syslogd only collects system information for that node, and writes it to a local log file on that node. From a syslog perspective, each Avamar server node is unaware that any other server nodes exist. Nor is the utility node syslogd process aware that the Avamar Management Console Server (MCS) is collecting and logging Avamar event information.

The Local Syslog event profile

The default Avamar configuration includes a Local Syslog event profile. If enabled, this profile formats Avamar server event messages in syslog format, and sends this data to the local syslogd process running on the Avamar server utility node.

The Local Syslog event profile is read-only. You can enable it using the factory settings, but you cannot edit it. If you require custom syslog event profile settings, you must copy it, then edit the copy.

Local syslog monitoring

The most basic way to implement Avamar server syslog monitoring is to configure the MCS to output Avamar event information to the local syslogd process running on the utility node. The local syslogd service merges the Avamar event information with the operating system messages in a single local log file, as shown in the following diagram:

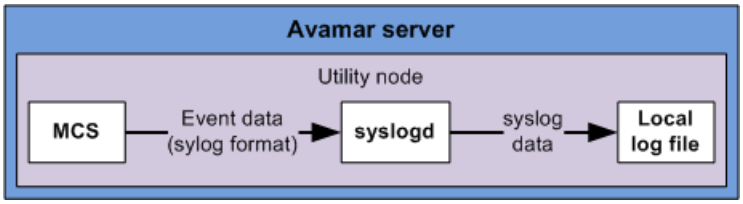


Figure 8 Local syslog monitoring functional diagram

Remote syslog monitoring

Remote syslog monitoring involves configuring each server node to send syslog data to a remote logging host, and creating a custom syslog event profile that sends Avamar server event messages in syslog format to the remote logging host, as shown in the following diagram:

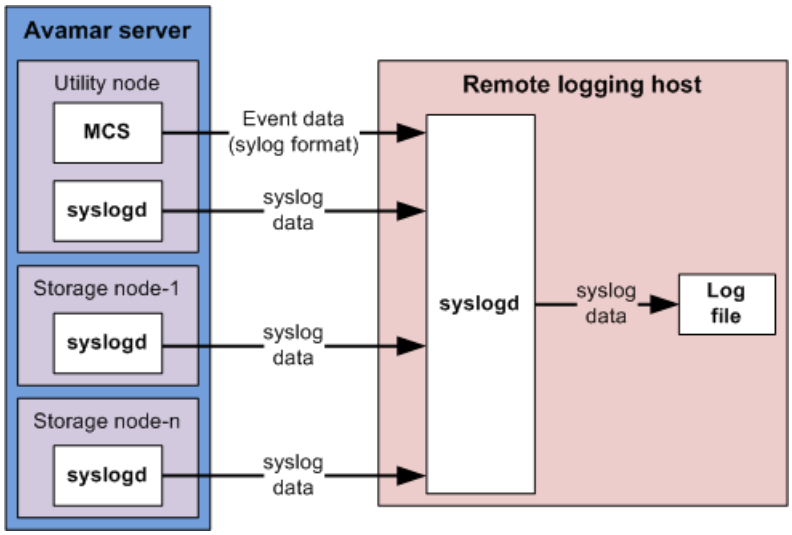


Figure 9 Remote syslog monitoring functional diagram

NOTICE

For maximum security, EMC recommends implementing remote syslog monitoring.

Data mapping

The following table describes how an event profile maps Avamar server event data to various syslog fields.

Table 31 Syslog field and Avamar Event data mappings

Syslog Field	Avamar Event Code Data
Facility	One of the following: • User • Local#, where # is a number from 0 to 7
Priority	One of the following: • debug, if the Avamar event type is DEBUG • err, if the Avamar event type is ERROR • info, if the Avamar event type is INFO • none, if the Avamar event type is INTERNAL • warning, if the Avamar event type is WARNING
Date	Avamar event date.
Time	Avamar event time.
Hardware Source	Avamar event hardware source.
Software Source	Avamar event software source.
Message	The following fields from the Avamar event code: • event code • category • summary • event data

Configuring local syslog

To configure local syslog monitoring:

- Enable the Local Syslog event profile, as described in "Enabling the Local Syslog event profile" on page 211.
- Configure the local utility node syslogd process to listen for syslog messages on the UDP port 514, as described in "Configuring the utility node syslogd process to listen for MCS event messages" on page 212.

Enabling the Local Syslog event profile

In order to format Avamar server event information in a syslog format, and output it to either a local or remote syslogd process, you must enable the Local Syslog event profile as follows:

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.

2. Select the **Local Syslog** event profile in the tree pane and click **Enable**.

Configuring the utility node syslogd process to listen for MCS event messages

This procedure describes how to configure the local utility node syslogd process to listen for MCS event messages on UDP data port 514.

Separate Instructions are provided for nodes running SUSE Linux Enterprise Server (SLES) and Red Hat Enterprise Linux (RHEL). Use the appropriate instructions for your server.

Configuring SLES single-node servers and utility nodes

The following instructions are applicable to most Avamar 6.0 and later single-node servers and utility nodes running SLES 11 or later.

1. Open a command shell and log in:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Open /etc/syslog-ng/syslog-ng.conf in a text editor, such as vi or Emacs.
4. Locate the following entry:

   ```
   #
   # uncomment to process log messages from network:
   #
   # udp(ip("0.0.0.0") port(514));
   ```

5. Add the following entry (including the comment):

   ```
   #
   # uncomment to process log messages from MCS:
   #
   udp(ip("127.0.0.1") port(514));
   ```

6. Save and close the file.
7. Restart the syslog process by typing:

   ```
   service syslog restart
   ```

8. Verify that syslog is listening on port 514 by typing:

   ```
   netstat -nap | grep 514
   ```

   The following appears in the command shell:

   ```
   udp 0 0 127.0.0.1:514 127.0.0.1:* 8043/syslog-ng
   ```

Configuring RHEL single-node servers and utility nodes

These instructions are applicable to older Avamar single-node servers and utility nodes running RHEL.

1. Open a command shell and log in:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Switch user to root by typing:

   ```
   su -
   ```
3. Open /etc/sysconfig/syslog in a text editor, such as vi or Emacs.
4. Locate the following entry:

   ```
   SYSLOGD_OPTIONS="-m 0"
   ```
5. Add the -r parameter to the SYSLOGD_OPTIONS entry as follows:

   ```
   SYSLOGD_OPTIONS="-r -m 0"
   ```
6. Save and close the file.
7. Restart the syslogd process by typing:

   ```
   service syslog restart
   ```

Configuring remote syslog

To configure remote syslog monitoring:

- Create a custom syslog event profile, as described in "Creating a custom syslog event profile" on page 213.
- Configure all server nodes to send syslog messages to the remote logging host, as described in "Configuring server nodes to send syslog messages to the remote logging server" on page 215.
- Ensure that the remote logging host is configured to listen for syslog messages over a LAN connection on UDP data port 514, as described in "Configuring the remote logging host" on page 216.

Creating a custom syslog event profile

1. In Avamar Administrator, select **Tools** › **Manage Profiles**.

   The Manage All Profiles dialog box appears.
2. Select the **Local Syslog** event profile in the tree pane and click **Copy**.

   The Save As dialog box appears.
3. Type a name for the new custom event profile in the **Save As** field.
4. Leave the domain set to root (/).

   Note: Custom syslog profiles must reside in the root domain.

5. Click **OK**.

   The Save As dialog box closes.

6. From the Manage All Profiles dialog box, select the custom event profile you created in steps 1—5 and click **Edit**.

   The Edit Profile dialog box appears.

7. Select the Syslog Notification tab and specify syslog notification parameters as described below:

   a. In the **Address (IP or hostname)** field, type the IP address or hostname of the remote logging host.

   b. In the **Port Number** field, leave the port number set to **514**.

   c. Select the **Include extended event data** option if you want to include extended event code information in the syslog message. This extended information is delimited using the following tags:

      - ‹Code›
      - ‹Type›
      - ‹Severity›
      - ‹Category›
      - ‹HwSource›
      - ‹Summary›
      - ‹active›
      - ‹lastEmailSendDate›
      - ‹domain›
      - ‹scheduleID›
      - ‹num_prefs›
      - ‹name›
      - ‹isSystem›

   d. From the **Facility** list, select one of the following: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.

   NOTICE

   To test the syslog notification parameters, click **Send Test Syslog Entry**.

8. Click **OK**.

   The Edit Profile dialog box closes.

Configuring server nodes to send syslog messages to the remote logging server

This topic describes how to configure Avamar server nodes to send syslog messages to a remote logging server over a LAN connection on UDP data port 514.

Separate Instructions are provided for Avamar 6.0 and later server nodes running SLES 11 or later, and older Avamar server nodes running RHEL.

Configuring SLES server nodes

The following instructions are applicable to most Avamar 6.0 and later server nodes running SLES 11 or later.

1. Open a command shell and log in:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Open /etc/syslog-ng/syslog-ng.conf in a text editor, such as vi or Emacs.
4. Add the following entry:

   ```
   destination logserver {udp("IP-ADDR" port(514)); };
   log { source(src); destination(logserver); };
   ```

   where IP-ADDR is the IP address of the remote logging host.
5. Save and close the file.
6. Restart the syslog process by typing:

   ```
   service syslog restart
   ```

7. If this is a multi-node Avamar server, configure the remaining server nodes by logging into each node as admin, and repeating steps 2—6.

Configuring RHEL server nodes

These instructions are applicable to older Avamar servers running RHEL.

1. Open a command shell and log in:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Open /etc/syslog.conf in a text editor, such as vi or Emacs.
4. Add the following entry:

   ```
   # Remotely log all messages.
   *.*       @SERVERNAME
   ```

   where SERVERNAME is the host name of the remote logging host.

5. Save and close the file.
6. Restart the syslog process by typing:

   ```
   service syslog restart
   ```

7. If this is a multi-node Avamar server, configure the remaining server nodes by logging into each node as admin, and repeating steps 2—6.

Configuring the remote logging host

EMC expects that sites implementing remote syslog monitoring of an Avamar server will in most cases already have a remote logging host configured and deployed.

Many different syslog monitoring tools are available. Any syslog monitoring tool will generally work with Avamar as long as it is configured to listen for remote syslog messages over a LAN connection on UDP data port 514.

A complete discussion of remote logging host configuration is beyond the scope of this publication. Refer to your operating system, or syslog monitoring tool documentation for additional information.

- "Configuring RHEL remote logging hosts running syslog" on page 216 provides details for configuring the remote syslog monitoring functionality offered by RHEL.
- "Configuring SLES remote logging hosts running syslog-ng" on page 217 provides details for configuring the newer remote syslog-ng functionality offered by SLES.
- "Suggested configuration for the remote logging host firewall" on page 217 provides information about configuring your firewall to allow UDP traffic on port 514 for a defined IP range.

Configuring RHEL remote logging hosts running syslog

To configure an RHEL remote logging host running syslog:

1. Open a command shell and log in to the remote logging host as root.
2. Open /etc/sysconfig/syslog in a text editor, such as vi or Emacs.
3. Locate the following entry:

   ```
   SYSLOGD_OPTIONS="-m 0"
   ```

4. Add the -r parameter to the SYSLOGD_OPTIONS entry as follows:

   ```
   SYSLOGD_OPTIONS="-r -m 0"
   ```

5. Save and close the file.
6. Restart the syslogd process by typing:

   ```
   service syslog restart
   ```

7. If you have a firewall enabled on the system, configure the firewall to allow UDP traffic on port 514 for a defined IP range. "Suggested configuration for the remote logging host firewall" on page 217 provides details.

Configuring SLES remote logging hosts running syslog-ng

To configure a SLES remote logging host running syslog-ng:

1. Open a command shell and log in to the remote logging host as root.
2. Open /etc/syslog-ng/syslog-ng.conf in a text editor, such as vi or Emacs.
3. Uncomment the following entry:

```
#
# uncomment to process log messages from network:
#
udp(ip("0.0.0.0") port(514));
```

4. Save and close the file.
5. Restart the syslog process by typing:

```
service syslog restart
```

6. Verify that syslog is listening on port 514 by typing:

```
netstat -nap | grep 514
```

   The following appears in the command shell:

```
udp 0 0 0.0.0.0:514 0.0.0.0:* 8043/syslog-ng
```

7. If you have a firewall enabled on the system, configure the firewall to allow UDP traffic on port 514 for a defined IP range. "Suggested configuration for the remote logging host firewall" on page 217 provides details.

Suggested configuration for the remote logging host firewall

When enabling the acceptance of remote log messages, it is important to restrict the source IPs of the remote log messages in iptables or another firewall in order to avoid Denial Of Service (DOS) attacks on the remote logging host. Rules for iptables similar to the following would allow client system logs to be allowed:

```
# Rules to allow remote logging for syslog(-ng) on the log HOST system
iptables -A INPUT -p udp -s 192.168.1.0/24 --dport 514 -j ACCEPT
```

or

```
iptables -A INPUT -p udp -s 192.168.1.12 -m mac --mac-source
   00:50:8D:FD:E6:32 --dport 514 -j ACCEPT

iptables -A INPUT -p udp -s 192.168.1.13 -m mac --mac-source
   00:50:8D:FD:E6:33 --dport 514 -j ACCEPT

iptables -A INPUT -p udp -s 192.168.1.14 -m mac --mac-source
   00:50:8D:FD:E6:34 --dport 514 -j ACCEPT

iptables -A INPUT -p udp -s 192.168.1.15 -m mac --mac-source
   00:50:8D:FD:E6:35 --dport 514 -j ACCEPT

...
```

where 192.168.1.0/24 is in the IP range of your Avamar server nodes.

Alternatively, you can also specify each IP on a single line and include the Mac address of that node's Network Interface Card (NIC). There are no rules needed for the outgoing syslog traffic on the client side. Restart iptables (or other firewall) for the rules to take effect.

Restart the firewall service on the remote logging host for the changes to take effect.

Restart the syslog-ng service on all server nodes and the remote logging host for the changes to take effect:

```
service syslog restart
```

Monitoring the Avamar server using SNMP

Simple Network Management Protocol (SNMP) is a protocol for communicating and monitoring event notification information between an application, hardware device, or software application and any number of monitoring applications or devices.

The Avamar server supports SNMP versions v1, v2c, and v3.

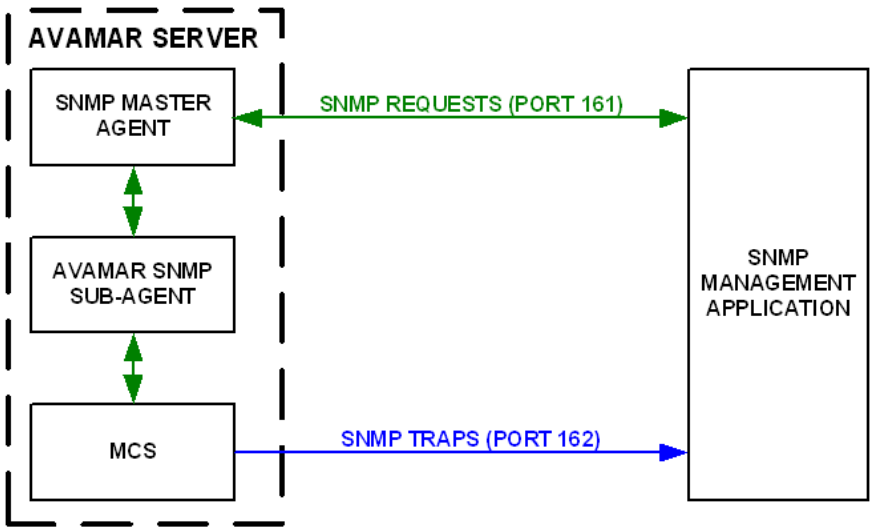
Prerequisite knowledge and resources

Persons configuring an Avamar server to send event information over SNMP should be familiar with basic SNMP concepts. A complete discussion of basic SNMP concepts and implementation is beyond the scope of this guide. The www.net-snmp.org website provides additional information.

Overview

The Avamar SNMP implementation provides two ways to access Avamar server events and activity status:

- SNMP requests
- SNMP traps



SNMP requests

SNMP requests provide a mechanism for SNMP management applications to "pull" information from a remote SNMP-enabled application or device (in this case, the Avamar server). The SNMP management application sends a request to an SNMP master agent running on the Avamar server. The SNMP master agent then communicates with the Avamar SNMP sub-agent, which passes the request to the MCS. The MCS retrieves the data and sends it back to the Avamar SNMP sub-agent, which passes it back to the management application by way of the SNMP master agent. Data port 161 is the default data port for SNMP requests.

SNMP master agent

Avamar servers purchased directly from EMC use the Net-SNMP master agent. Avamar servers built with other industry standard hardware likely use an SNMP master agent provided by the hardware manufacturer.

SNMP traps

SNMP traps provide a mechanism for the Avamar server to "push" information to SNMP management applications whenever designated Avamar events occur. Data port 162 is the default data port for SNMP traps. Typically, the SNMP management application listens for any SNMP traps generated by designated remote hosts.

Management Information Base (MIB)

Each SNMP application or device defines what information can be monitored or which traps are sent, and stores this information in a Management Information Base (MIB). SNMP management applications load various MIBs to determine what information can be expected from the respective SNMP applications or devices.

To enable an SNMP management application to monitor an Avamar server, the Avamar MIB definition file (AVAMAR-MCS-MIB.txt) must be loaded into the master MIB used by the SNMP management application. The Avamar MIB definition file can be found in the locations listed in the following table.

Table 32 Avamar MIB definition file locations

Computer/Server Type	MIB Location
Single-node server	/usr/local/avamar/doc
Multi-node server	/usr/local/avamar/doc on the utility node
Computer with Avamar Administrator	INSTALL-DIR/doc where INSTALL-DIR is typically: • C:\Program Files\avs\administrator on Microsoft Windows computers • /usr/local/avamar on Linux computers • /opt/AVMRconsl on Solaris computers

A copy of Avamar MIB definition file (AVAMAR-MCS-MIB.txt) also resides in the /usr/share/snmp/mibs directory on single-node servers and utility nodes. This copy is used by the Avamar SNMP sub-agent and should not be moved or distributed.

Task list

To configure Avamar server monitoring using SNMP:

1. Install and configure an AgentX compliant master agent:
   - If the Avamar server was purchased directly from EMC, the Net-SNMP master agent is already installed. However, you must configure the Net-SNMP agent as discussed in "Configuring the Net-SNMP agent" on page 220.
   - If the Avamar server is built with other industry standard hardware, you must install and configure the AgentX compliant master agent provided by the hardware vendor.
2. Configure a custom event profile to output designated Avamar server events to an SNMP trap as discussed in "Configure a custom event profile" on page 223.

Configuring the Net-SNMP agent

Avamar provides a command line utility (**avsetup_snmp**) for configuring the Net-SNMP agent to communicate with the Avamar server using the Avamar SNMP sub-agent.

To configure the Net-SNMP agent:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Type:

   ```
   cd /root
   avsetup_snmp
   ```

   The following information appears in the command shell:

   ```
   avsetup_snmp will help you set up your snmpd config file:
   /etc/snmp/snmpd.conf

   Enter the port to listen for SNMP requests on [161]:
   ```

4. Choose the SNMP request data port:
   - To use port 161, the default SNMP request data port, press **Enter**.
   - To use a different SNMP request data port, type the data port number and press **Enter**.

   If **avsetup_snmp** was not able to detect any SNMP communities, the following information appears in the command shell:

   ```
   No snmp v1/2 communities configured. Forcing access_control
   configuration.
   Running snmpconf to configure access_control group.
   reading: /etc/snmp/snmpd.conf
   Do you want to allow SNMPv3 read-write user based access (default =
   y):
   ```

5. Type **n** and press **Enter**.

   The following information appears in the command shell:

   ```
   Do you want to allow SNMPv3 read-only user based access (default = y)
   :
   ```

6. Type **n** and press **Enter**.

   The following information appears in the command shell:

   ```
   Do you want to allow SNMPv1/v2c read-write community access (default
   = y):
   ```

7. Type **n** and press **Enter**.

   The following information appears in the command shell:

   ```
   Do you want to allow SNMPv1/v2c read-only community access (default
   = y):
   ```

8. Press **Enter**.

   The following information appears in the command shell:

   ```
   Configuring: rocommunity
   Description:
      a SNMPv1/SNMPv2c read-only access community name
      arguments: community [default|hostname|network/bits] [oid]
   The community name to add read-only access for:
   ```

   The SNMP community is a text string that the local Net-SNMP agent uses to authenticate itself with the SNMP management application. MyCommunity is used as an example SNMP community for the remainder of this procedure.

9. Type the SNMP community and press **Enter**.

   The following information appears in the command shell:

   ```
   The hostname or network address to accept this community name from
   [RETURN for all]:
   ```

10. Press **Enter**.

    The following information appears in the command shell:

    ```
    The OID that this community should be restricted to [RETURN for
    no-restriction]:
    ```

11. Press **Enter**.

    The following information appears in the command shell:

    ```
    Finished Output: rocommunity public MyCommunity
    Do another rocommunity line? (default = y):
    ```

12. Type **n** and press **Enter**.

    The following information appears in the command shell:

```
The following files were created:
   snmpd.conf installed in /etc/snmp
System settings not configured. Forcing system_setup configuration.
Running snmpconf to configure system_setup group.
reading: /etc/snmp/snmpd.conf

Configuring: syslocation
Description:
   The [typically physical] location of the system.
   Note that setting this value here means that when trying to
   perform an snmp SET operation to the sysLocation.0 variable
   will make the agent return the "notWritable" error code. IE,
   including this token in the snmpd.conf file will disable
   write access to the variable.
arguments: location_string

The location of the system:
```

13. Type the physical location of the Avamar server and press **Enter**.

    The following information appears in the command shell:

```
Finished Output: syslocation "MyLocation"

Configuring: syscontact
Description:
   The contact information for the administrator
   Note that setting this value here means that when trying to
   perform an snmp SET operation to the sysContact.0 variable
   will make the agent return the "notWritable" error code. IE,
   including this token in the snmpd.conf file will disable
   write access to the variable.
arguments: contact_string

The contact information:
```

14. Type contact information (for example, email address, telephone extension, and so forth) and press **Enter**.

    The following information appears in the command shell:

```
Finished Output: syscontact "root@example.com Extension: 1234"
Do you want to properly set the value of the sysServices.0 OID (if
you don't know, just say no)? (default = y):
```

15. Type **n** and press **Enter**.

    The following information appears in the command shell:

```
The following files were created:
snmpd.conf installed in /etc/snmp
Enabling snmpd.
```

Configure a custom event profile

Local SNMP Trap profile

The default Avamar configuration includes a special Local SNMP Trap profile. If enabled, this profile outputs Avamar server event messages to the local Net-SNMP trap listener (snmptrapd process).

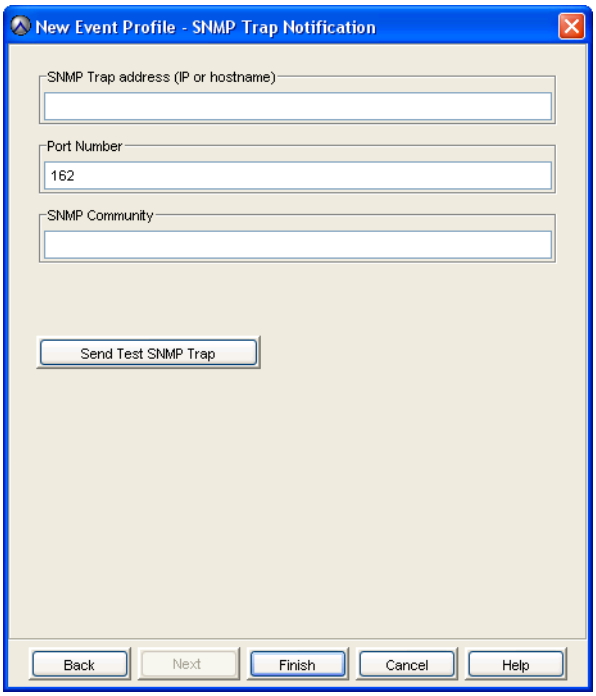
NOTICE

The Local SNMP Trap profile is read-only. You cannot edit it. Furthermore, it is intended to be used for test purposes only, to verify that traps are successfully generated and received by the local snmptrapd process, which then writes the trap information to a syslog file. In most cases, you must configure another custom profile to send Avamar SNMP traps to a remote Net-SNMP trap listener.

Using a custom event profile

If you create a custom event profile to support syslog monitoring, as discussed in "Creating a custom event profile" on page 196, ensure that the SNMP Trap Notification - Enabled option is selected on the first wizard screen.

Continue through the wizard screens until the SNMP Trap wizard screen appears.



Complete the settings in the wizard screen:

1. In the **SNMP Trap Address (IP or hostname)** box, type IP address or hostname of a computer with an application capable of receiving and processing an SNMP trap.
2. In the **Port Number** box, type the port number on the host machine that listens for SNMP traps.

3. In the **SNMP Community** box, type the name of the SNMP community that the SNMP trap listener is configured to use.

   NOTICE

   To test the SNMP notification parameters, click **Send Test SNMP Trap**.

Managing ConnectEMC

ConnectEMC is a program that runs on the Avamar server and that sends information to EMC Customer Support. ConnectEMC is typically configured to send alerts for high priority events as they occur, as well as reports once daily.

EMC Secure Remote Support (ESRS)

Beginning with Avamar 6.0, ConnectEMC is integrated with EMC Secure Remote Support (ESRS), provided that it is installed, operational, and network accessible by the Avamar server. Contact your EMC Sales Representative for additional information about implementing ESRS.

User-configurable transports

Although ConnectEMC is initially configured during Avamar server software installation, Avamar Administrator enables you to manage ConnectEMC settings, in the form of three user-configurable transports, after the server is operational:

- Primary Transport
- Failover Transport
- Notification Transport

The Primary and Failover Transport send alerts for high priority events as they occur. The Primary Transport is used unless it fails, at which time the Failover Transport is used.

The Notification Transport sends email notifications messages to one or more customer email addresses under certain conditions.

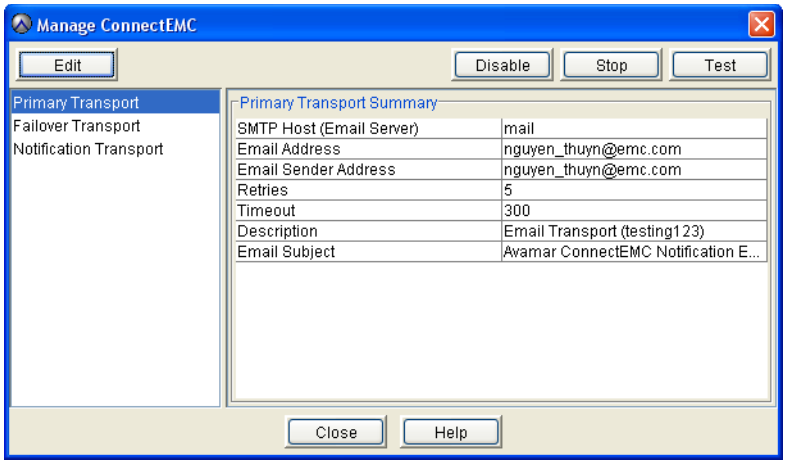
Enabling and disabling ConnectEMC

Disabling ConnectEMC causes the MCS to stop generating ConnectEMC messages until ConnectEMC is reenabled.

To enable and disable ConnectEMC:

1. In Avamar Administrator, select **Tools** › **Manage ConnectEMC**.

   The Manage ConnectEMC window appears.



2. Click **Enable** or **Disable** to enable or disable ConnectEMC messages, respectively.

   If you are disabling ConnectEMC, you are prompted to enter a password.

3. Enter a valid password and click **OK**.

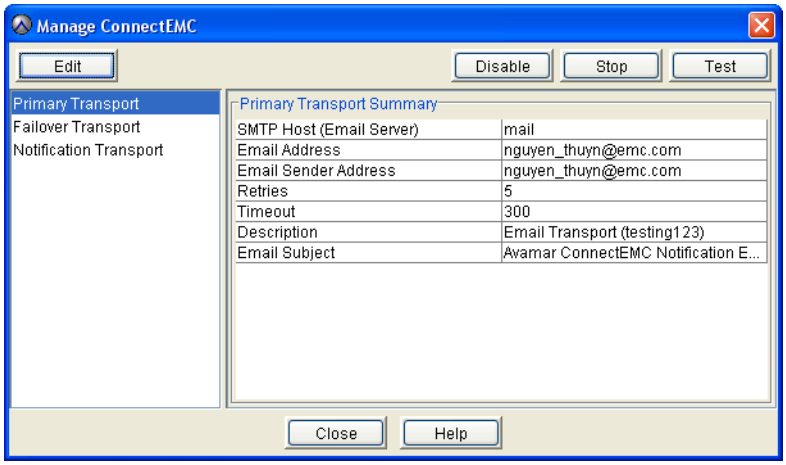
Stopping and starting ConnectEMC

Stopping ConnectEMC turns off the ConnectEMC process until such time as it is restarted. During this time, the MCS still generates ConnectEMC alerts. These alerts are queued until ConnectEMC is restarted.

To stop and start ConnectEMC:

1. In Avamar Administrator, select **Tools** › **Manage ConnectEMC**.

   The Manage ConnectEMC window appears.



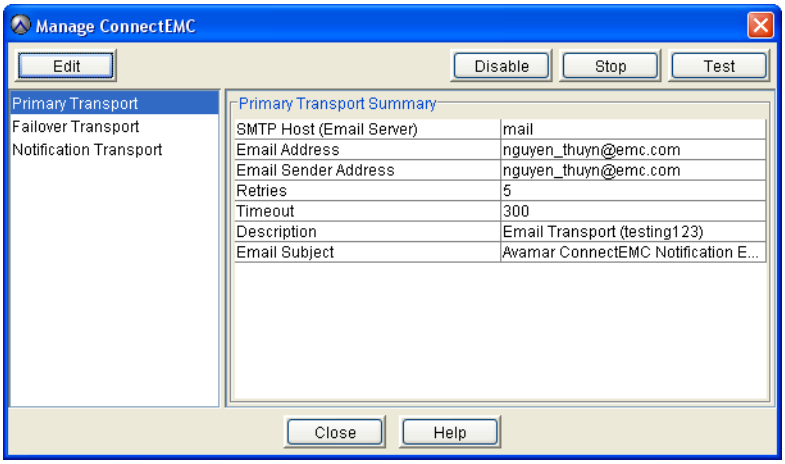
2. Click **Stop** or **Start** to stop or start the sending of ConnectEMC alerts, respectively.

Editing Primary and Failover transports

To edit settings for the Primary and Failover transports:

1. In Avamar Administrator, select **Tools** › **Manage ConnectEMC**.

   The Manage ConnectEMC window appears.



2. Select either the **Primary Transport** or the **Failover Transport**, and click **Edit**.

   NOTICE

   The Primary Transport is used as an example for the remainder of this procedure.

   The Edit Primary Transport dialog box appears.

3. Select one of the following from the **Transport Type** list:

   - **Email**
   - **FTP**
   - **HTTPS**

   NOTICE

   An operational ESRS gateway is required to use FTP or HTTPS transport types.

4. Specify the transport type settings in the **Edit Primary Transport** dialog box as discussed in the following table.

Table 33 Edit Primary Transport dialog box settings (page 1 of 2)

Transport Type	Settings to Configure
Email	To configure the Email transport: 1. In the **SMTP Host (Email Server)** field, specify the mail server hostname or IPv4 address. 2. In the **Email Address** field, specify one or more recipients of these emails. Separate multiple email addresses with commas. 3. In the **Email Sender Address** field, specify the email address from which to send the message. 4. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced Email Settings** dialog box: **Retries –** The number of retries to attempt before reporting a failure. The default setting is 5 retries. **Timeout –** The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds). **Description –** A description of this transport that appears in the Manage ConnectEMC window. The default description is Email Transport. **Email Subject –** The subject line in the email. The default subject line is Avamar ConnectEMC Notification Email. **Note:** Do not change the Email Subject unless instructed to do so by EMC Customer Support. Email messages with other subject lines might be rejected by EMC spam filters. 5. Click **OK**.
FTP	To configure the FTP transport: 1. In the **IP Address** field, specify an IPv4 address. 2. In the **Username** field, specify an FTP username. The setting depends on the FTP server software. 3. In the **Password** field, specify the password for the username. 4. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced FTP Settings** dialog box: **Retries –** The number of retries to attempt before reporting a failure. The default setting is 5 retries. **Timeout –** The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds). **Description –** A description of this transport that appears in the Manage ConnectEMC window. The default description is FTP Transport. **FEP Folder** – A unique customer UNIX path in the ConnectEMC Front End Processor (FEP). Use the folder location supplied by EMC Customer Support. **FTP Port** – An IP port. The default setting is port 21. **Mode –** Either Active or Passive. The default setting is Active. 5. Click **OK**.

Table 33 Edit Primary Transport dialog box settings (page 2 of 2)

Transport Type	Settings to Configure
HTTPS	To configure the HTTPS transport: 1. Type a valid ESRS Home page Universal Resource Locator (URL) in the **URL** field. Valid ESRS Home page URLs use the following format: **https://HOME-NAME[:PORT]/TARGET-DIRECTORY** where HOME-NAME, PORT, and TARGET-DIRECTORY are the home name, data port, and target directory, respectively. Use the ESRS Home page URL provided by EMC Customer Support. 2. (Optional) To configure advanced settings, click **Advanced**, and then specify the following settings in the **Edit Advanced HTTPS Settings** dialog box: **Retries –** The number of retries to attempt before reporting a failure. The default setting is 5 retries. **Timeout –** The number of seconds to wait before reporting that the operation timed out. The default setting is 5 minutes (300 seconds). **Private Key Pass Phrase –** The passphrase associated with the private key file. **Private Key File** – The filename of the private key file. **Client Certificate** – The client certificate to use. The default setting is "Default," which uses the certificate that the MCS uses. Otherwise, type the filename of the client certificate. **Server CA Bundle –** File containing a list of root certificates. **Verify Server Name –** Whether to verify the server name. Either Yes or No. The default setting is No. 3. Click **OK**. **Note:** Sample key files are provided in /opt/connectemc/certs/ and https-privatekey.pem. Sample client certificates are provided in /opt/connectemc/certs/ and https-cert.pem. Sample root certificate bundles are provided in /opt/connectemc/certs/ and https-ca-cert.pem.

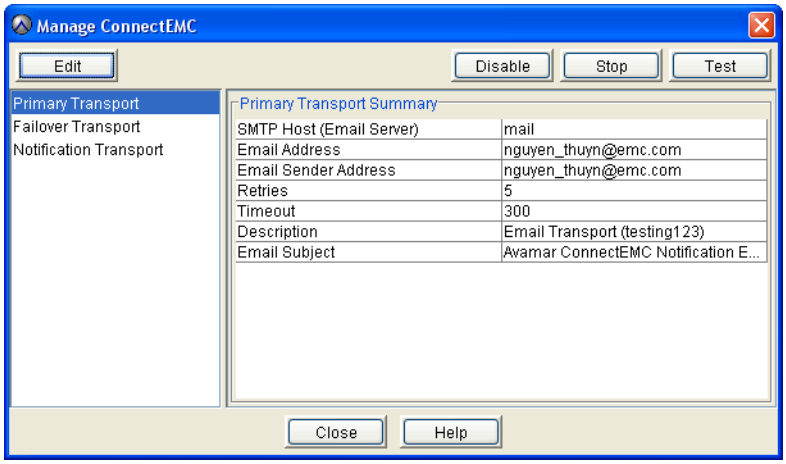
5. On the **Edit Primary Transport** dialog box, click **OK**.

Editing the Notification transport

To edit the Notification transport:

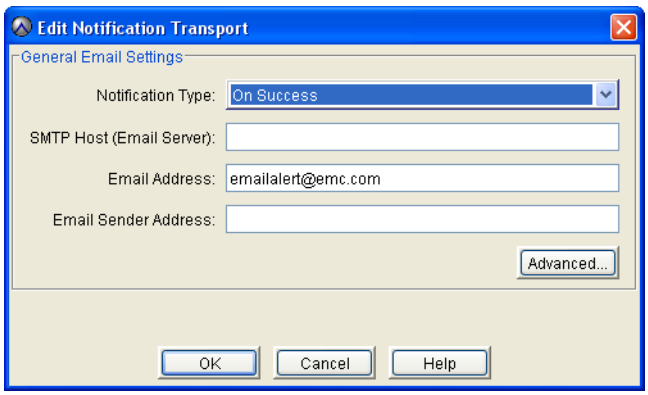
1. In Avamar Administrator, select **Tools** › **Manage ConnectEMC**.

   The Manage ConnectEMC window appears.



2. Select the **Notification Transport** and click **Edit**.

   The Edit Notification Transport dialog box appears.

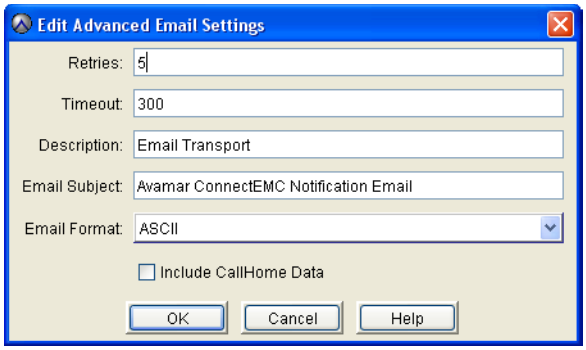


3. From the **Notification Type** list, select one of the following types:

   - **On Success**—Notify recipients when an event file is successfully transferred to EMC.
   - **On Failure**—Notify recipients when an event file is not successfully transferred to EMC.
   - **On Success or Failure**—Notify recipients when an attempt is made to transfer an event file to EMC, regardless of the outcome.
   - **On All Failure**—Notify recipients when all attempts to transfer an event file to EMC have failed.

4. In the **SMTP Host (Email Server)** box, type the mail server hostname or IPv4 address.
5. In the **Email Address** box, type one or more recipients of these emails. Separate multiple email addresses with commas.

6. In the **Email Sender Address** box, type the email address from which the notification is sent.
7. (Optional) To specify advanced settings, click **Advanced** and then specify the settings in the **Edit Advanced Email Settings** dialog box.



The settings described below are available in the Edit Advanced Email Settings dialog box:

- **Retries**—Number of retries to attempt before reporting a failure. The default setting is 5 retries.
- **Timeout**—Number of seconds to wait before reporting that the operation timed out. The default setting is 300 seconds (5 minutes).
- **Description**—Description of this transport in the Manage ConnectEMC window. The default description is Email Transport.
- **Email Subject**—The subject line in the email. The default subject line is Avamar ConnectEMC Notification Email.

  NOTICE

  Do not change the Email Subject unless instructed to do so by EMC Customer Support. Email messages with other subject lines might be rejected by EMC spam filters.

- **Email Format**—The format of the email, either **ASCII** or **HTML**. The default setting is **ASCII**.
- **Include CallHome Data**—If yes, attachments sent to ConnectEMC are also included in the notification email message.

8. Click **OK**.

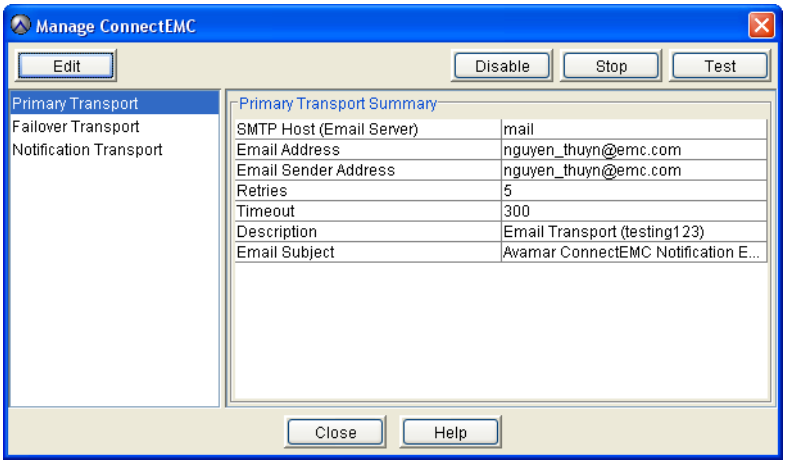
   The Edit Advanced Email Settings dialog box closes.
9. On the **Edit Notification Transport** dialog box, click **OK**.

Testing transports

To send test alerts and email messages:

1. In Avamar Administrator, select **Tools** › **Manage ConnectEMC**.

   The Manage ConnectEMC window appears.



2. Click **Test**.

CHAPTER 8
Reporting

Avamar provides several features that enable you to output reports of system information in various formats. Each method of generating reports is covered in greater detail in this chapter. The following topics provide details about creating these reports:

- Avamar reports 234
- Creating a report 237
- Editing a report 240
- Running a report 241
- Deleting a report 242
- Viewing the Client Summary Report 242
- Viewing the Activity Report 246
- Viewing the Replication Report 250
- Backend capacity reports 252
- Exporting displayed tabular data as CSV files 256
- Support for third-party reporting tools 258
- Setting up the PostgreSQL ODBC driver 258
- Crystal Reports templates 260
- Other third-party support 261

Avamar reports

The Avamar reports feature enables you to create, manage, and run system reports. When Avamar reports are run, the results appear in a separate dialog box. The report results can also be exported as a Comma-Separated Values (CSV) text file.

Predefined reports

The following table lists the predefined reports that are provided with Avamar.

Table 34 Predefined Avamar reports (page 1 of 3)

Report	Report contents
Activities - Bytes Protected Client	This report lists the quantity of primary data, in bytes, that is protected by the system for each client.
Activities - Bytes Protected Client - 2	This report is the same as the Activities - Bytes Protected Client report, except that you can specify an effective date range.
Activities - Bytes Protected Total	This report lists the total quantity of primary data, in bytes, that is protected by the system.
Activities - Bytes Protected Total - 2	This report is the same as the Activities - Bytes Protected Total report, except that you can specify an effective date range.
Activities - Client Perf Tracking	This report lists client performance statistics.
Activities - Client Stats	This report lists client statistics.
Activities - Client Stats - 2	This report is the same as the Activities - Client Stats reports, except that you can specify an effective date range.
Activities - DPN Summary	This report lists summary information about data stored in the Avamar server and statistical data for each client backup.
Activities - Exceptions	This report lists all activities within a specified period that succeeded with exceptions.
Activities - Exceptions (Extended)	This report lists all activities within a specified period that completed with exceptions.
Activities - Failed	This report lists all activities within a specified period that failed due to errors.
Activities - Licensed Bytes Protected Client	This report lists the quantity of primary data, in bytes, that is protected by the system for each client in the past 14 days. **Note:** This 14-day timeframe ensures that any backups that belong to clients that might have migrated to another Avamar server are not included in the licensing calculations for the server.
Activities - Licensed Bytes Protected Total	This report lists the total quantity of primary data, in bytes, that has been protected by the system in the past 14 days. **Note:** This 14-day timeframe ensures that any backups that belong to clients that might have migrated to another Avamar server are not included in the licensing calculations for the server.

Table 34 Predefined Avamar reports (page 2 of 3)

Report	Report contents
Activities - Licensed Client Stats	This report lists client statistics in the past 14 days. **Note:** This 14-day timeframe ensures that any backups that belong to clients that might have migrated to another Avamar server are not included in the licensing calculations for the server.
Activities - Licensed Plugin Stats	This report lists the total quantity of data protected, in bytes, by each data source plug-in. **Note:** This 14-day timeframe ensures that any backups that belong to clients that might have migrated to another Avamar server are not included in the licensing calculations for the server.
Activities - Plugin Client Stats	This report lists plug-in statistics in the past 14 days. **Note:** This 14-day timeframe ensures that any backups that belong to clients that might have migrated to another Avamar server are not included in the licensing calculations for the server.
Activities - Plugin Stats	This report lists plug-in statistics.
Activities - Plugin Stats - 2	This report is the same as the Activities - Plugin Stats report, except that you can specify an effective date range.
Activities - Success	This report lists all activities within a specified period that succeeded without exceptions.
Agents and Plugins - Client Count	This report lists all agents and plug-ins installed by all clients, and the count for each type.
Capacity Report	This report lists the available capacity of each server node.
Clients - No Activities	This report lists all clients that did not have any activities in specified period.
Clients - No Check Ins	This report lists all clients that did not check in with the server in the specified period.
Clients - Protected	This report lists: • All clients with at least one backup stored on the Avamar server • Plug-ins and counts for all clients • Client operating systems • Maximum bytes protected for each client • Total bytes protected for all clients
Clients - Unprotected	This report lists all clients that are known to the MCS but are not actively being protected for various reasons.

Table 34 Predefined Avamar reports (page 3 of 3)

Report	Report contents
Misc - Stats 1	For the specified period, this report lists: • Plug-ins installed on protected clients • Total bytes protected • Client operating systems protected • Maximum bytes protected for each client
System - Configuration Audit	This report lists all currently installed server operating system RPMs and a comparison against a master list that was used to initialize the system.
System - GSAN Perf Stats	This report lists data server (also known as GSAN) performance statistics that are useful for system tuning and debugging purposes. By default, this report is enabled in the High Priority Events profile, described on page 194.

Report templates

In addition to predefined reports, you can create reports based on the templates in the following table.

Table 35 Report templates

Template	Description
Activities	Show detailed information about system activities, such as backups, restores, backup validations, and replication.
Clients	Show detailed information about one or more backup clients.
Replication activities	Similar to Activities reports, but only show information related to replication.
Backend capacity	Show detailed information about the amount of physical server capacity used by each client. **Notice:** Do not run a backend capacity report for a client with backups on a Data Domain system. Otherwise, the report fails. Backend capacity reports cannot include data on a Data Domain system.

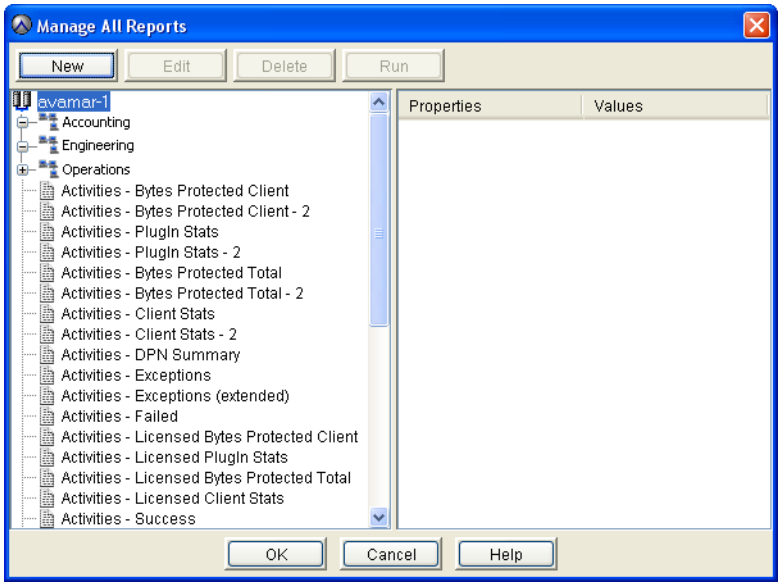
Creating a report

If you intend to send this report as a custom event profile attachment, create the report in the root domain. You cannot send reports created at lower levels as custom event profile attachments. "Creating a custom event profile" on page 196 provides details.

To create a report:

1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.



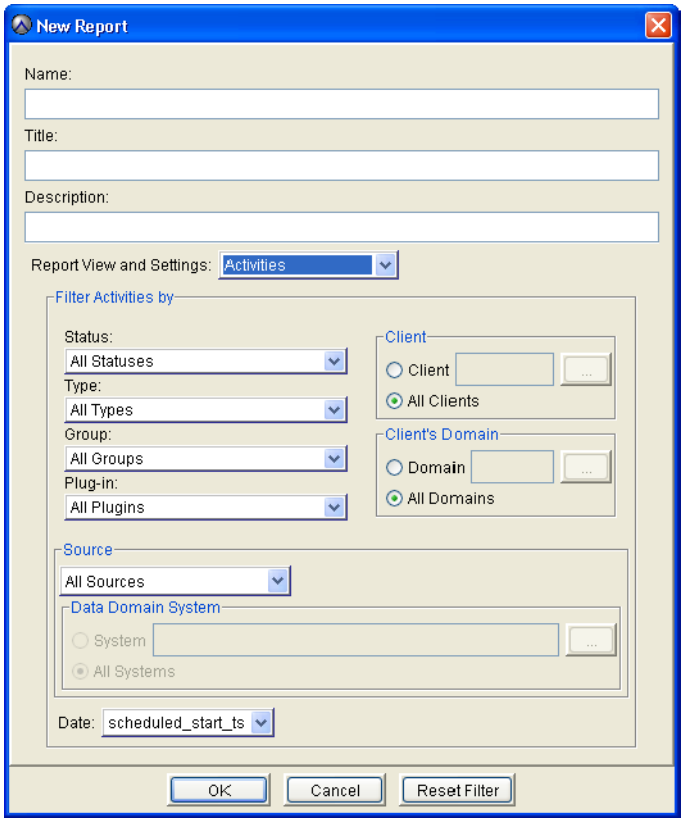
2. In the tree in the left pane, select a domain.

   The domain selection controls:

   - Content:
     - Reports instanced at the Avamar server (root) node can potentially include capacity usage data from the entire server, or specific subdomains.
     - Reports instanced in subdomains can only include capacity usage data for that subdomain.
   - Access:
     - Reports instanced at the Avamar server (root) node can only be run by root administrators.
     - Reports instanced in subdomains can be run by those domain administrators and root administrators, but not administrators of other domains.

3. Click **New**.

The New Report dialog box appears.



4. Specify a name, display title, and optional short description for the report in the **Name**, **Title**, and **Description** fields.
5. From the **Report View and Settings** list, select a report template:
   - Activities
   - Clients
   - Replication Activities
   - Backend Capacity

   "Report templates" on page 236 provides details on each template.

6. Complete the settings that appear for the report template, as described in the following table.

Table 36 Avamar report template descriptions

Report Template	Description
Activities, Replication Activities	For an activities or replication activities report, customize the report using any of the following criteria: • **Status** (for example, all statuses, all failures, all completed, and so forth) • **Type** (all types, on-demand backup, restore, scheduled backup, validate, all backups) • **Group** (all groups or a specific group) • **Plug-in** (for example, Microsoft Windows file system, Solaris Oracle RMAN database, and so forth) • **Client** name (all clients or a specific client) • **Client's Domain** (all domains or a specific domain) • **Date** (for example, scheduled start date, scheduled end date, completed date, and so forth) • **Source** (all sources, all Avamar servers, all Data Domain systems, or a specific Data Domain systems)
Clients	For a clients report, customize the report using any of the following criteria: • **Pageable** (whether the MCS can successfully page the client and receive a response) • **Date** client was registered, last checked in, or last backed up • **Client** name (all clients or a specific client) • **Client's Domain** (all domains or a specific domain)
Backend Capacity	For a backend capacity report, select clients to include in the report: 1. Click **Edit**. The Edit Backend Capacity dialog box appears. 2. To select all clients within a domain, select that domain checkbox. 3. To select individual clients, select a domain (highlight it but do not select the checkbox). Clients within that domain appear in the right pane. 4. In the right pane, select one or more clients to include in the report by selecting the checkbox next to each client. 5. Repeat steps 2—4 to select other clients within other domains. **Notice:** Do not run a backend capacity report for a client with backups on a Data Domain system. Otherwise, the report fails. Backend capacity reports cannot include data on a Data Domain system. 6. Click **OK**. The Edit Backend Capacity dialog box closes.

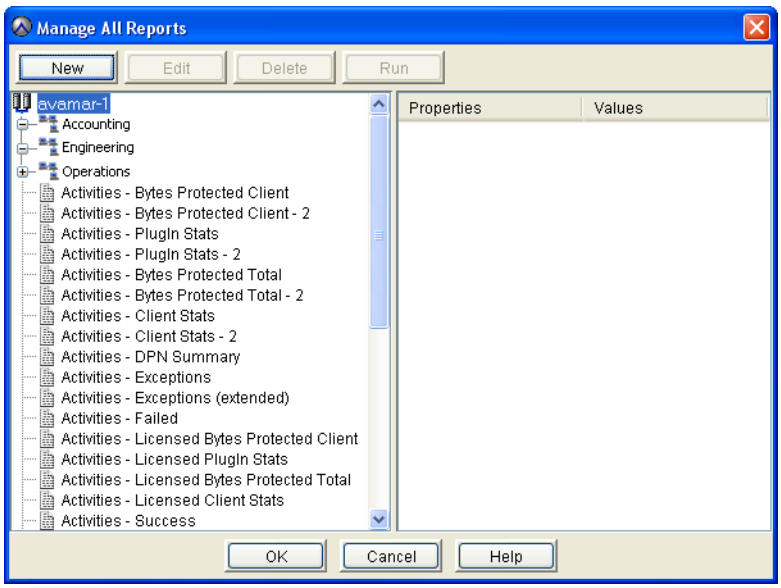
7. Click **OK**.

Editing a report

To edit a report:

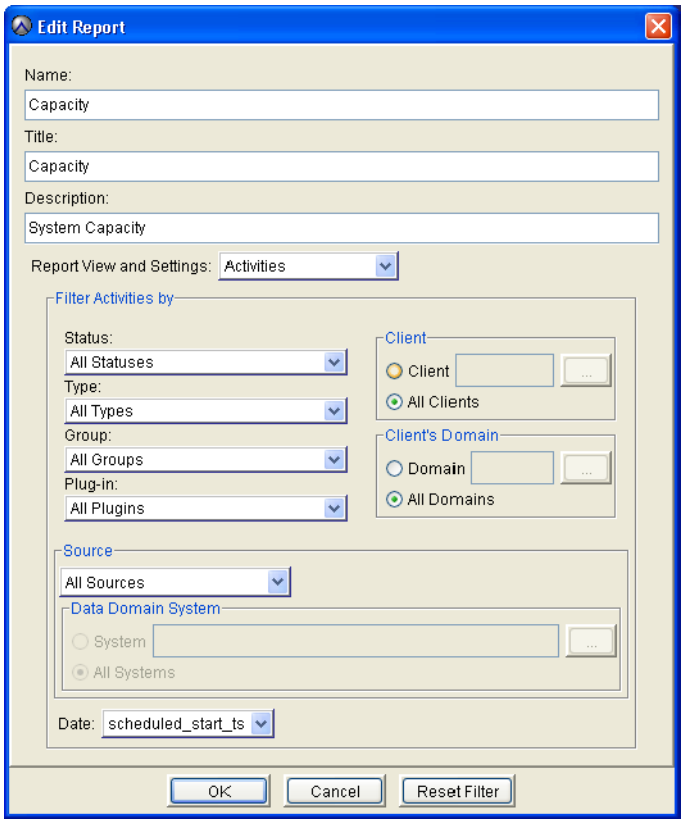
1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.



2. In the tree in the left pane, select the report and click **Edit**.

   The Edit Report dialog box appears.



3. Edit the report settings, which are described in "Creating a report" on page 237.
4. Click **OK**.

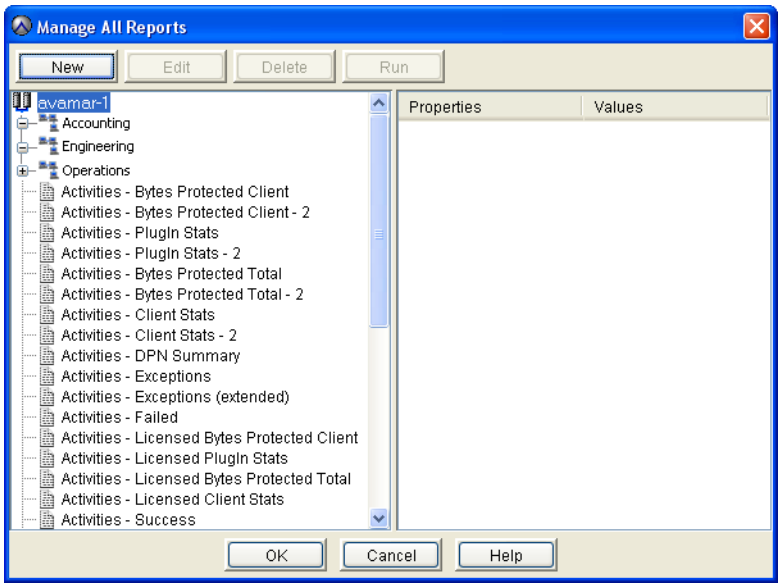
Running a report

Backend capacity reports are very resource intensive. Never run more than one backend capacity report at the same time.

To run a report:

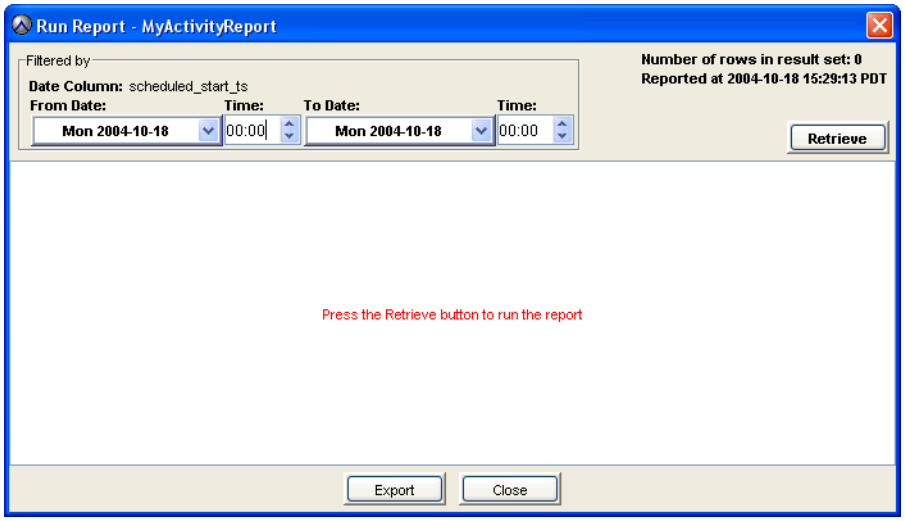
1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.



2. In the tree in the left pane, select the report and click **Run**.

   The Run Report dialog box appears.



3. Click **Retrieve** to display the report output.

4. (Optional) To export this data as a Comma-Separated Values (CSV) text file:
   a. Click **Export**.

      The Save dialog box appears.

   b. Browse to the folder in which to save the file, and type a descriptive filename in the **File name** box.

   c. Click **OK**.
5. Click **Close**.

Deleting a report

To delete a report:

1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.
2. In the tree in the left pane, select the report and click **Delete**.

   A confirmation message appears.
3. Click **Yes**.

Viewing the Client Summary Report

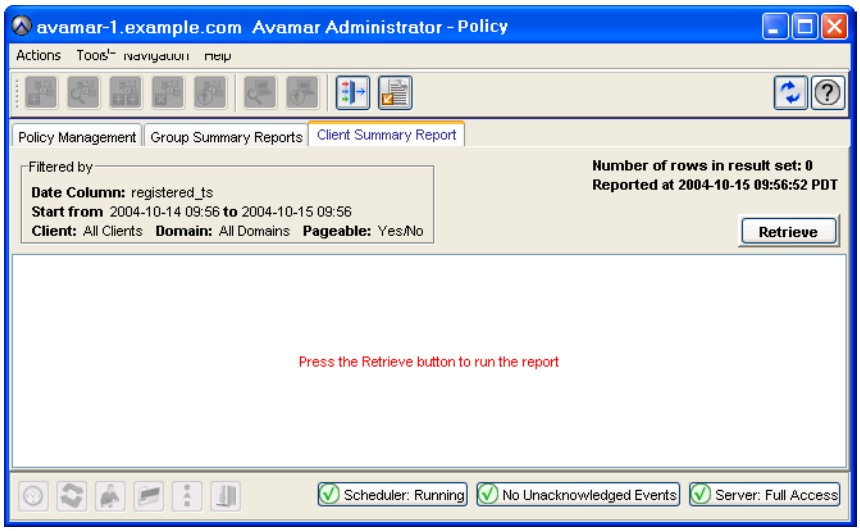
The Client Summary Report is a combined view of important client properties for all clients registered with this Avamar server.

To view the Client Summary Report:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.
2. Click the **Client Summary Report** tab.

   A blank Client Summary Report window appears.



3. Click **Retrieve**.

   The client summary report displays the information in the following table for each client registered on the server.

Table 37 Client Summary report column descriptions (page 1 of 2)

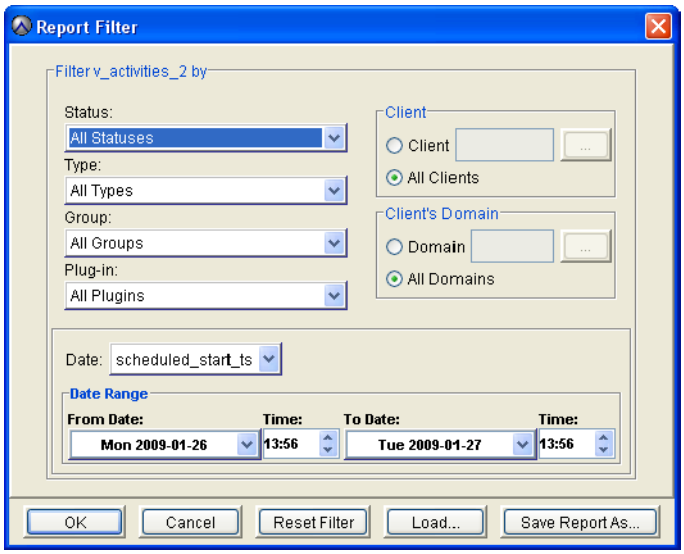
Column	Description
agent_version	Version of the agent that is installed.
allow_overtime	True if the client can ignore the scheduling window end time. See also overtime_option page 244.
allow_userinit_backup_file_sel	Allow file selection on user-initiated backups.
allow_userinit_backups	Allow user-initiated backups.
backed_up_ts	Last backup date and time.
can_page	True if MCS can call out to the client.
checkin_ts	Last check-in date and time.
cid	Client ID.
client_addr	Client IP address.
client_name	Client name.
client_type	Client type: • REGULAR • VMware vCenter • VMware Image Proxy • VMware Virtual Machine
contact_email	Contact email address.
contact_location	Contact location.
contact_name	Person to contact regarding issues with this client.
contact_notes	Contact notes.
contact_phone	Contact phone number.
created	Creation date.
ds_override	True if the client can override the group dataset.
enabled	True if the client can generate activities.
full_domain_name	Fully qualified client location.
has_backups	True if the client has backups.
modified	Date that client information was last edited.
os_type	Client OS type.
override_userinit_retpol	Override standard retention policy on user-initiated backups.

Table 37 Client Summary report column descriptions (page 2 of 2)

Column	Description
overtime_option	One of the following: • ALWAYS—Scheduled group backups are always allowed to run past the schedule duration setting. • NEXT—Only the next scheduled group backup is allowed to run past the schedule duration setting. • NEXT_SUCCESS—Scheduled group backups are allowed to run past the schedule duration setting until a successful backup is completed. • NEVER—Scheduled group backups are never allowed to run past the schedule duration setting. This value is automatically set to NEXT_SUCCESS when the client initially registers and is cleared after one backup successfully completes.
page_addr	IP address used to contact this client.
page_port	Data port used to contact this client.
pageadr_locked	True if the IP address cannot be updated automatically by the MCS.
plugin_for_last_backup	Plug-in used for the last backup.
rc_override	True if the client can override the group retry count setting.
registered	True if the client has checked in to MCS.
registered_ts	Registered date and time.
restore_only	True if the client can only do restores.
retry_cnt	Connection retry count.
rp_override	True if the client can override the group retention policy.
timeout	Connection time-out value.
tp_override	True if the client can override the group time-out period setting.

4. (Optional) To reduce the amount of report data, filter the report to show only records within a range of dates, for a client domain, or for a client by selecting **Actions › Filter**.

   The Report Filter dialog box appears.



5. Define the filtering criteria and click **OK**.

Viewing the Activity Report

The Activity Report provides detailed information for recent backup, restore, and validation activities.

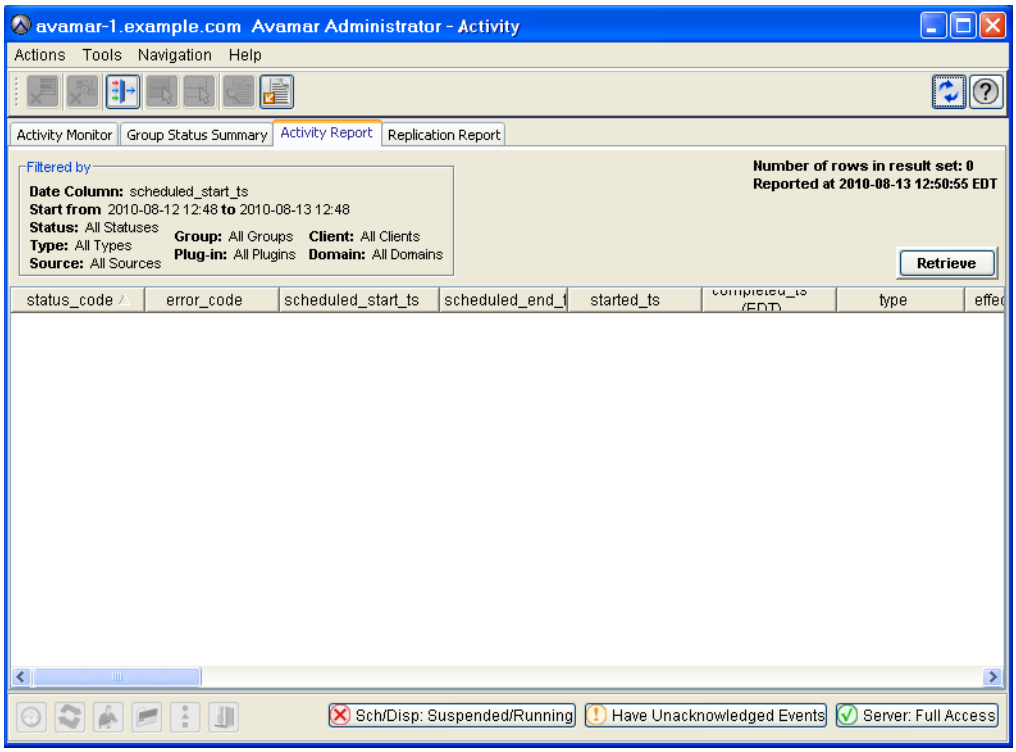
To view the Activity Report:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.

2. Click the **Activity Report** tab.

   A blank Activity Report window appears.



3. Click **Retrieve**.

   The activity report displays the information in the following table for each activity.

Table 38 Activity report column descriptions (page 1 of 4)

Column	Description
backup_label	Backup label. Blank for replication activities.
backup_number	Backup number. Blank for replication activities.
bytes_excluded	Total number of bytes intentionally excluded during this activity.
bytes_new	Total number of bytes processed during this activity after data deduplication.
bytes_overhead	Total number of overhead bytes.
bytes_scanned	Total number of bytes processed during this activity.

Table 38 Activity report column descriptions (page 2 of 4)

Column	Description
bytes_skipped	Total number of bytes unintentionally skipped (errors and so forth) during this activity.
cid	Client ID.
client_name	Avamar client name.
client_os	Client operating system.
client_ver	Avamar client software version.
completed_ts	Date and time that this activity ended, adjusted for the prevailing time zone, shown in parentheses.
current_retention	Current retention types assigned to this backup: • D—Daily • W—Weekly • M— Monthly • Y—Yearly • N—No specific retention type
dataset	Dataset used to perform this backup.
dataset_override	If true, the group dataset was not used for this activity.
ddr_hostname	Hostname of the Data Domain system on which the activity occurred, if the activity occurred on a Data Domain system.
domain	Full location of the client in the Avamar server.
effective_expiration	Calendar date and time that this backup will expire.
effective_path	For group-based backups, the dataset used in the backup.
encrypt_method2_sa	Identifies whether server authentication was enforced at the time of the backup (that is, if the mcserver.xml encrypt_server_authenticate preference was set to true at the time of the backup).
encryption_method	Encryption method used for client/server data transfer: • proprietary • ssl
encryption_method2	Encryption method used for client/server data transfer: • High—Strongest available encryption setting for that specific client platform. • Medium—Medium strength encryption. • None—No encryption. **Note:** The exact encryption technology and bit strength used for any given client-server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.
error_code	If the activity successfully completed, zero appears in this column. If the activity did not successfully complete, a numeric error code appears.
error_code_summary	If the activity did not successfully complete, a short summary of this error code.

Table 38 Activity report column descriptions (page 3 of 4)

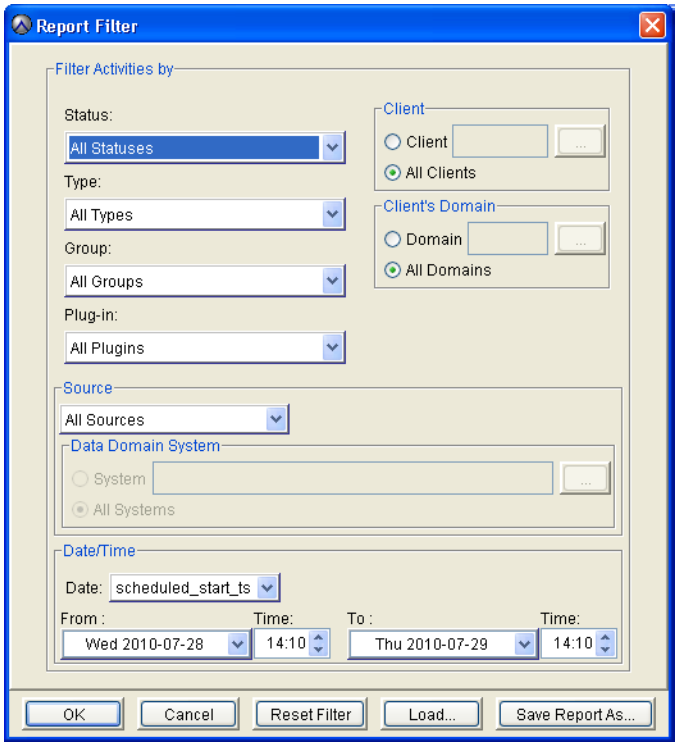
Column	Description
group_name	If the activity was a scheduled backup, this is the group that this client was a member of when this scheduled activity was initiated (clients can be members of more than one group). On-demand is shown for all other activities.
hard_limit_exceeded	Indicates whether a backup exceeded the hard limit set for the client. Value is true if limit was exceeded and false if limit was not exceeded.
initiated_by	For On-Demand Backup activity, the user that initiated the activity.
num_files_skipped	Total number of files unintentionally skipped (errors and so forth) during this activity.
num_of_files	Total number of files processed during this activity.
original_retention	Original retention types that were programmatically assigned to this backup when it occurred: • D—Daily • W—Weekly • M— Monthly • Y—Yearly • N—No specific retention type
plugin_number	Plug-in used for this activity.
proxy_cid	VMware proxy client unique ID.
retention_policy	Retention policy used to perform this backup.
retention_policy_override	If true, the group retention policy was not used for this activity.
schedule	If the activity was a scheduled backup, this is the schedule that initiated this activity. On-Demand or End User Request is shown for all other activities initiated from Avamar Administrator or the client, respectively.
scheduled_end_ts	Latest date and time this activity was scheduled to end, adjusted for the prevailing time zone, which is shown in parentheses.
scheduled_start_ts	Earliest date and time this activity was scheduled to begin, adjusted for the prevailing time zone, which is shown in parentheses.
server	Server on which the activity occurred, either the Avamar server or a Data Domain system.
session_id	Work order ID. Unique identifier for this activity.
soft_limit_exceeded	Indicates whether a backup exceeded the soft limit set for the client. Value is true if limit was exceeded and false if limit was not exceeded.
started_ts	Date and time that this activity started, adjusted for the prevailing time zone, which is shown in parentheses.

Table 38 Activity report column descriptions (page 4 of 4)

Column	Description
status_code	Numeric event code describing latest status of this activity.
status_code_summary	Short summary of this status code.
type	Type of activity: • On-Demand Backup • Scheduled Backup • Restore • Validate

4. (Optional) To reduce the amount of report data, filter the report to show only records within a range of dates, for a client domain, or for a client by selecting **Actions** › **Filter**.

   The Report Filter dialog box appears.



5. Define the filtering criteria and click **OK**.

Viewing the Replication Report

The Replication Report provides detailed information for recent replication operations.

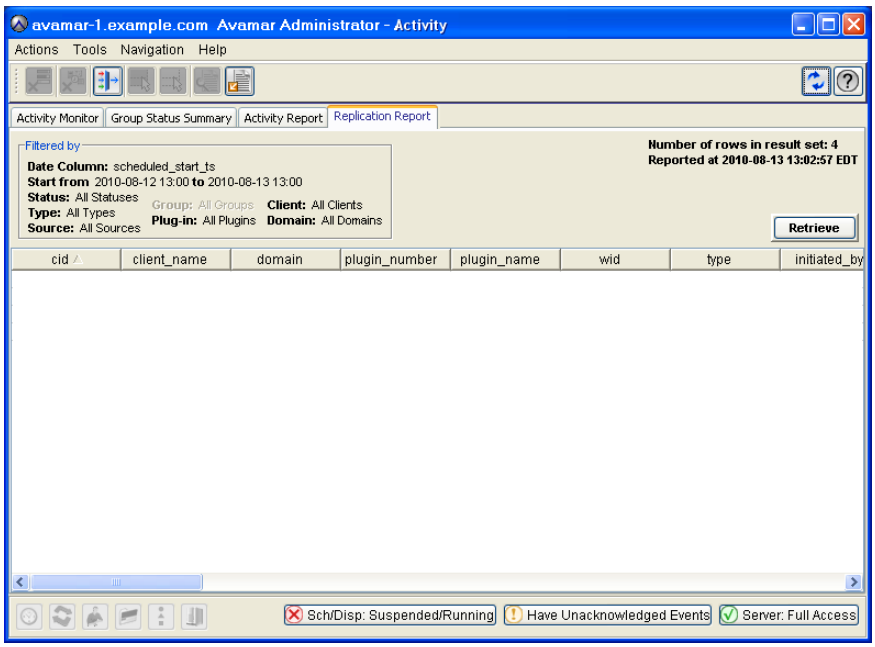
To view the Replication Report:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.

2. Click the **Replication Report** tab.

   A blank Replication Report window appears.



3. Click **Retrieve**.

   The Replication report displays the information in the following table for each replication operation.

Table 39 Replication report column descriptions (page 1 of 3)

Column	Description
bytes_excluded	Total number of bytes intentionally excluded during this replication operation.
bytes_new	Total number of bytes processed during this replication operation after data deduplication.
bytes_overhead	Total number of overhead bytes.
bytes_scanned	Total number of bytes processed during this replication operation.
bytes_skipped	Total number of bytes unintentionally skipped (errors and so forth) during this replication operation.
cid	Client ID.
client_name	Avamar client name.

Table 39 Replication report column descriptions (page 2 of 3)

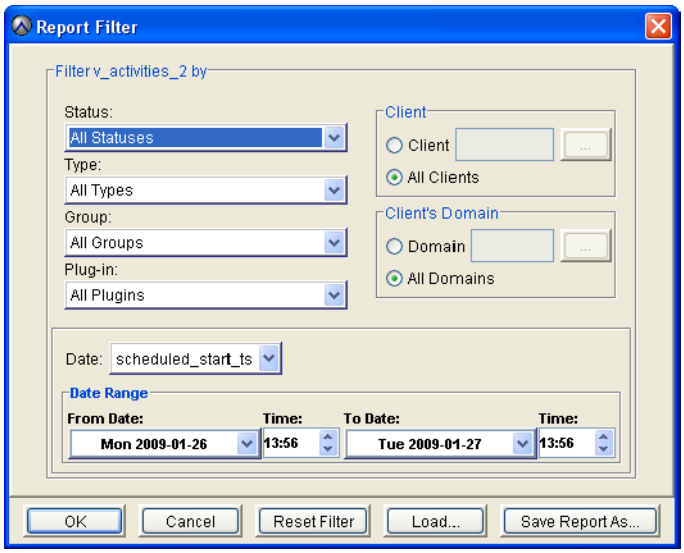
Column	Description
client_os	Client operating system.
client_ver	Avamar client software version.
completed_ts	Date and time this replication operation ended.
ddr_hostname	Hostname of the Data Domain system on which the activity occurred, if the activity occurred on a Data Domain system.
domain	Full location of the client in the Avamar server.
encryption_method	Encryption method used for client/server data transfer: • proprietary • ssl
encryption_method2	Encryption method used for client/server data transfer: • Medium—Medium strength encryption. • High—Strongest available encryption setting for that specific client platform. • None—No encryption. **Note:** The exact encryption technology and bit strength used for any given client-server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.
encrypt_method2_sa	Identifies whether server authentication was enforced at the time of the backup (that is, if the mcserver.xml encrypt_server_authenticate preference was set to true at the time of the backup).
error_code	If the replication operation did not successfully complete, a numeric error code appears.
error_code_summary	If replication operation did not successfully complete, a short summary of this error code.
group	Group that initiated the replication activity. One of the following: • If the activity was a scheduled replication, this is the replication group. • Admin On-Demand Group is shown for-demand replication activities.
hostname	Destination server hostname.
num_files_skipped	Total number of files unintentionally skipped (errors and so forth) during this replication operation.
num_of_files	Total number of files processed during this replication operation.
plugin_number	Plug-in used for this replication operation.
scheduled_end_ts	Date and time this replication operation was scheduled to end.
scheduled_start_ts	Date and time this replication operation was scheduled to start.
server	Server on which the activity occurred, either the Avamar server or a Data Domain system.
session_id	Work order ID, which is a unique identifier for this replication operation.

Table 39 Replication report column descriptions (page 3 of 3)

Column	Description
started_ts	Date and time this replication operation started.
status_code	Numeric event code returned by this replication operation.
status_code_summary	Short summary of this status code.

4. (Optional) To reduce the amount of report data, filter the report to show only records within a range of dates, for a client domain, or for a client by selecting **Actions** › **Filter**.

   The Report Filter dialog box appears.



5. Define the filtering criteria and click **OK**.

Backend capacity reports

Backend capacity reports show the amount of physical server storage capacity used. This calculation includes capacity optimized by data deduplication, but does not include capacity consumed by RAIN overhead.

Each report can be configured to report on the entire Avamar server, specific Avamar domains, or specific Avamar clients.

There are two ways to run backend capacity reports:

- From Avamar Administrator
- From the command line using the **backendreport** utility

Limitations

Backend capacity reports are subject to the following limitations:

- You cannot run more than one backend capacity report at a time.
- Running a backend capacity report is resource intensive.

  Avoid running a backend capacity report when backup or maintenance activities are in progress, or are scheduled to occur.
- Backend capacity reports cannot include Data Domain system data.

  If you run a backend capacity report that includes any clients with backups stored on a Data Domain system, the report will fail.

Running backend capacity reports from Avamar Administrator

Running a backend capacity report from Avamar Administrator is a two-task process. First, you must create a report from the backend capacity report template, then run the report.

Task 1: Creating a backend capacity report from the backend capacity report template

To create a backend capacity report from the backend capacity report template:

1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.
2. In the tree in the left pane, select a domain.

   The domain selection controls:

   - Content:
     - Reports instanced at the Avamar server (root) node can potentially include capacity usage data from the entire server, or specific subdomains.
     - Reports instanced in subdomains can only include capacity usage data for that subdomain.
   - Access:
     - Reports instanced at the Avamar server (root) node can only be run by root administrators.
     - Reports instanced in subdomains can be run by those domain administrators and root administrators, but not administrators of other domains.
3. Click **New**.

   The New Report dialog box appears.
4. Type a name, display title, and optional short description for the report in the **Name**, **Title**, and **Description** fields.
5. Select **Backend Capacity** from the **Report View and Settings** list.
6. Click **Edit**.

   The Backend Capacity dialog box appears.

7. (Optional) To view all clients within the selected domain, select **Show sub-domain clients**.
8. Select one or more domains or clients to include in this report.
9. Click **OK**.

   The Backend Capacity dialog box closes.
10. From the New Report dialog box, click **OK**.

    The New Report dialog box closes. The report appears in the left pane.

Task 2: Running a backend capacity report

To run a backend capacity report:

1. In Avamar Administrator, select **Tools** › **Manage Reports**.

   The Manage All Reports dialog box appears.
2. In the tree in the left pane, select a backend capacity report and click **Run**.

   The Run Report dialog box appears.
3. Click **Retrieve** to display the report output.
4. (Optional) To export this data as a Comma-Separated Values (CSV) text file:
   a. Click **Export**.

      The Save dialog box appears.
   b. Browse to the folder in which to save the file, and type a descriptive filename in the **File name** box.
   c. Click **OK**.
5. From the Run Report dialog box, click **Close**.

Running backend capacity reports from the command line

The **backendreport** command line utility returns backend capacity usage for the entire Avamar server, specific Avamar domains, or specific Avamar clients.

1. Open a command shell and log in to the server as admin.
2. Run the backend capacity report.
   a. To run a report on the entire Avamar server (all domains), type:

      ```
      backendreport
      ```

      Information similar to the following appears in your command shell:

      ```
      bytessent="1538144256"
      ==================== Finished backendreport ====================
      ```

      The bytessent value is the amount of backend capacity in bytes used by the entire server.

b. To run a report on a specific domain, type:

backendreport --include=/MyDomain

where MyDomain is the specific domain you want to include in this report.

Information similar to the following appears in your command shell:

```
bytessent="87356416"
==================== Finished backendreport ====================
```

The bytessent value is the amount of backend capacity in bytes used by all clients in the /MyDomain domain.

c. To run a report on a specific client, type:

backendreport --include=/MyDomain/MyClient

where MyDomain/MyClient is the path to the client you want to include in this report.

Information similar to the following appears in your command shell:

```
bytessent="163564"
==================== Finished backendreport ====================
```

The bytessent value is the amount of backend capacity in bytes used by MyClient.

d. To run a report in which a character string is used to match all clients in a domain with those characters anywhere in the client name, type:

backendreport --include=/MyDomain/vm

where /MyDomain is a domain in which only clients with ‘vm’ in the host name will be included in the report.

Information similar to the following appears in your command shell:

```
bytessent="278059"
==================== Finished backendreport ====================
```

The bytessent value is the amount of backend capacity in bytes used by all clients in the /MyDomain domain that have “vm” anywhere in the client name.

Exporting displayed tabular data as CSV files

You can export the following tabular data displayed within Avamar Administrator as Comma-Separated Values (CSV) text files:

- "Activity Report" on page 256
- "Replication Report" on page 256
- "Client Summary Report" on page 257
- "Event Management" on page 257
- "Session Monitor" on page 257

Activity Report

To export Activity report data:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.
2. Click the **Activity Report** tab.
3. Click **Retrieve** to populate this screen with information.
4. Select **Actions** › **Export Report**.

   The Save dialog box appears.
5. Browse to the folder in which to save the report data, and type a descriptive filename in the **File name** field.
6. Click **OK**.

Replication Report

To export Replication report data:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.
2. Click the **Replication Report** tab.
3. Click **Retrieve** to populate this screen with information.
4. Select **Actions** › **Export Report**.

   The Save dialog box appears.
5. Browse to the folder in which to save the report data, and type a descriptive filename in the **File name** field.
6. Click **OK**.

Client Summary Report

To export Client Summary report data:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Client Summary Report** tab.
3. Click **Retrieve** to populate this screen with information.
4. Select **Actions** › **Export Report**.

   The Save dialog box appears.

5. Browse to the folder in which to save the report data, and type a descriptive filename in the **File name** field.
6. Click **OK**.

Event Management

To export Events report data:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Event Management** tab.
3. Open the **Actions** menu and select **Event Monitor** › **Export Events Report**.

   The Save dialog box appears.

4. Browse to the folder in which to save the report data, and type a descriptive filename in the **File name** field.
5. Click **OK**.

Session Monitor

To export Sessions report data:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.

2. Click the **Session Monitor** tab.
3. Select **Actions** › **Export Sessions Report**.

   The Save dialog box appears.

4. Browse to the folder in which to save the report data, and type a descriptive filename in the **File name** field.
5. Click **OK**.

Support for third-party reporting tools

PostgreSQL

Avamar uses a PostgreSQL database to store various data. PostgreSQL is a highly regarded open-source Relational Database Management System (RDMS). Information in the Avamar database is accessible through any PostgreSQL-compliant Open DataBase Connectivity (ODBC) interface.

Crystal Reports templates

Crystal Reports is a popular database reporting tool. Avamar Administrator provides several Crystal Reports templates that you can use to quickly generate various Avamar system reports. You can also customize these templates or create new ones.

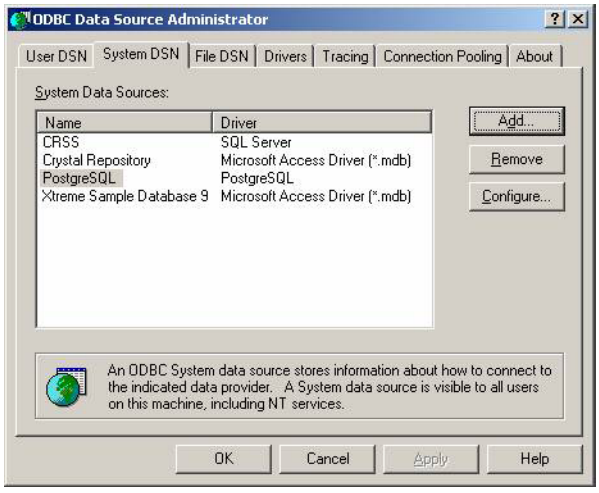
Setting up the PostgreSQL ODBC driver

To configure the Microsoft Windows PostgreSQL ODBC Driver on the local Windows client to support common third-party reporting packages such as Crystal Reports:

1. Download and install the latest driver from the PostgreSQL website (www.postgresql.org).
2. Open the Windows **Start** menu and select **Settings** › **Control Panel** › **Administrative Tools**.

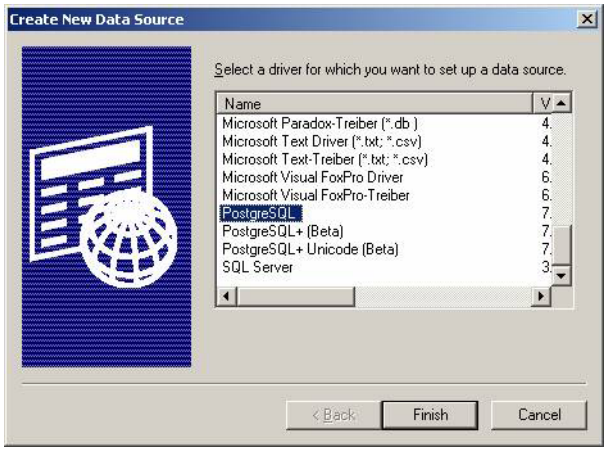
   The Administrative Tools window appears.
3. Double-click **Data Sources (ODBC)**.

   The ODBC Data Source Administrator appears.
4. Click the **System DSN** tab.



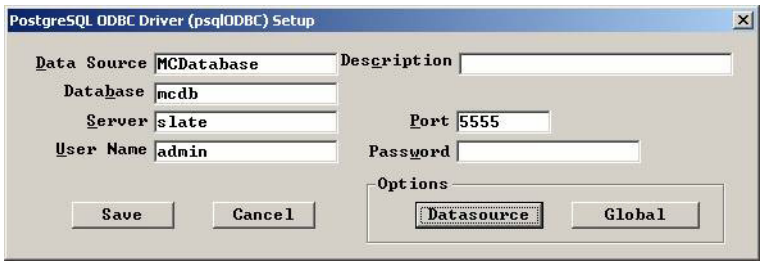
5. Click **Add**.

   The Create New Data Source dialog box appears.



6. Select the **PostgreSQL Driver** and click **Finish**.

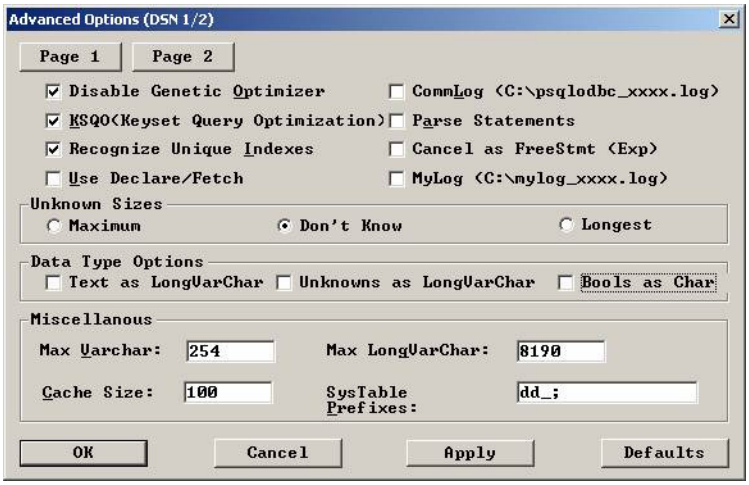
   The PostgreSQL ODBC Driver (psqlODBC) Setup dialog box appears.



7. In the **Data Source** box, type a short name, such as MCDatabase.
8. Leave the **Description** box blank.
9. In the Database box, type **mcdb**.
10. In the **Server** box, type the hostname where mcdb is running, such as dpn50mcs.
11. Leave the **Port** box set to 5555.
12. In the **User Name** box, type **viewuser**.
13. In the **Password** box, type **viewuser1**.

14. Click **Options** › **Datasource**.

    The Advanced Options (DSN 1 / 2) dialog box appears.



15. Select or clear the following:

    a. Under **Unknown Sizes**, select **Don't Know**.

    b. Clear **Text as LongVarChar**.

    c. Clear **Bools as Char**.

16. Click **OK**.

    The Advanced Options (DSN 1 / 2) dialog box closes.

17. Switch to the **PostgreSQL ODBC Driver (psqlODBC) Setup** dialog box and click **Save**.

    The PostgreSQL ODBC Driver (psqlODBC) Setup dialog box closes.

18. Switch to **ODBC Data Source Administrator** and click **OK**.

    The ODBC Data Source Administrator closes.

19. Close the **Administrative Tools** and **Control Panel** windows.

Crystal Reports templates

Avamar provides a set of Crystal Reports templates that you can use to generate reports. The default location for these templates is:

- C:\Program Files\avs\administrator\doc on Windows
- /usr/local/avamar/doc on Linux

A complete discussion of how to use Crystal Reports templates is beyond the scope of this guide. The Crystal Reports documentation provides information.

The following table lists the default Avamar Crystal Reports templates.

Table 40 Avamar Crystal Reports templates

Template Name (Filename)	Description
Client Installation Report (ClientInstallation.rpt)	This report contains information for all clients installed on the MCS when the report is run.
Errors and Warning Events Report (ErrorWarningEvents.rpt)	This report contains all events of warning or error severity within a specified date and time interval.
Events Report (AllEvents.rpt)	This report contains all events recorded by the MCS within a specified date and time interval.
Failed Restores Report (FailedRestores.rpt)	This report contains information for all failed restores within a specified date and time interval for all clients or for a specific client.
Failed Backups Report (FailedBackup.rpt)	This report contains information for all failed backups within a specified date and time interval for all clients or for a specific client.
Group Backup By Group Report (GroupbackupByGroup.rpt)	This report contains group backup statistics for all groups or for a specific group.
Group Backup By Schedule Report (GroupbackupByScheduled.rpt)	This report contains group backup statistics for backups initiated within a specified date and time interval.
Server Drive Capacity Report (ServerDriveCapacity.rpt)	This report provides hard drive capacity statistics for each server node based on the specified date and time interval.
Successful Restores Report (SuccessfulRestores.rpt)	This report contains information for all successful restores within a specified date and time interval for all clients or for a specific client.
Successful Backups Report (SuccessfulBackup.rpt)	This report contains information for all successful backups within a specified date and time interval for all clients or for a specific client.

Other third-party support

You can generate Avamar reports using any third-party PostgreSQL-compliant ODBC database reporting tool that runs on the platform. However, you must create report templates using the schema listings found in dbviews.sql. This file is located in the utility node /usr/local/avamar/lib/sql directory.

"MCS and EMS Database Views" on page 599 provides details on each view in dbviews.sql view and the individual columns storing data within each view.

CHAPTER 9
Avamar Client Agent and Plug-in Management

Each time a client communicates with an Avamar server, it identifies itself by sending the client ID, the specific agent version and build running on that client, and a list of plug-ins (version and build) currently installed on that client.

Occasionally, because of known incompatibilities, you may want to deny Avamar server access to all clients running a specific version (all builds) or a specific build of a client agent or plug-in. The following topics describe the mechanism for accomplishing this:

- Important terms and concepts 264
- Agents Summary view 264
- Plug-ins Summary view 265
- Adding a build record 267
- Editing version or build record settings 269
- Deleting a build record 270
- Enabling and disabling all client initiated activations 271
- Enabling and disabling all client initiated backups 272

"Avamar clients" on page 30 provides a general discussion of client agents and plug-ins and their role in the Avamar system.

Important terms and concepts

Disabling a version or build

You can deny access to the server on a version-by-version (all builds) or build-by-build basis. This is done by editing the properties for a particular agent or plug-in version or build and setting the Disable option.

Selective management of plug-in operations

You can also selectively allow or disallow the following plug-in operations for all clients running a specific plug-in version (all builds) or build:

- Client activations initiated from the client
- On-demand backups initiated from the client
- Scheduled backups
- Restores
- Backup validation
- Ability to browse stored backups on the server

"Editing version or build record settings" on page 269 provides details.

Obsolete versions and builds

Any specific version (all builds) or build that is designated as obsolete is denied access to the Avamar server. A build is designated as obsolete only in cases of known incompatibility between the client agent or plug-in and the specific version of server software that was installed. Therefore, to prevent potential problems, this obsolete designation cannot be overridden using the feature to edit properties for that version or build.

Agents Summary view

The Agents Summary view lists all client agent versions and builds potentially known to this Avamar server.

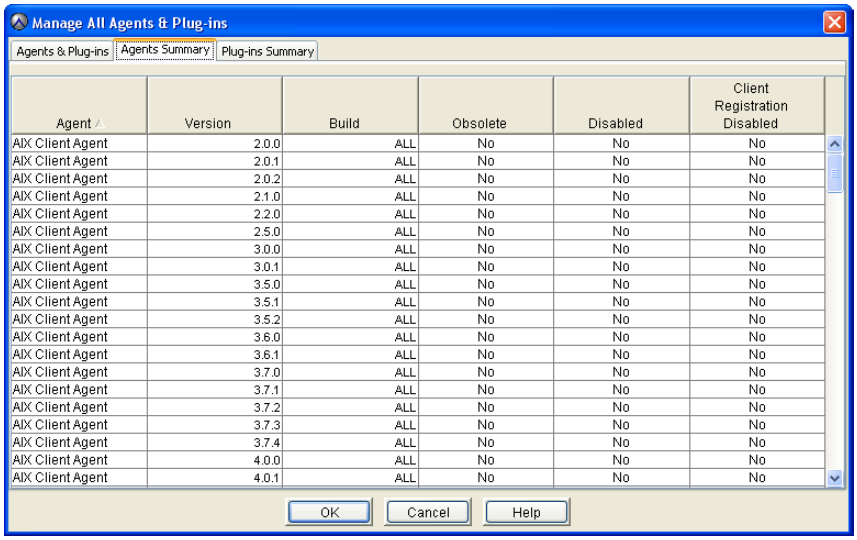
Agent versions and builds that are not supported by a version of Avamar server software appear as obsolete. Clients with these versions or builds are denied access to the server and must be upgraded before access is permitted. To determine the compatibility of client and server versions, refer to the *EMC Avamar Compatibility and Interoperability Matrix*, available on the EMC online support website at https://support.emc.com/products.

To display the Agents Summary view:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.

2. Click the **Agents Summary** tab.



The following table explains the properties for each client agent.

Table 41 Avamar agents property descriptions

Property	Description
Name	Name of this client agent.
Version	Specific version of this client agent.
Build	Either the specific software build of this client agent, or ALL if this entry is applicable to all builds.
Obsolete	Yes or no. If yes, the agents and plug-ins definition file has reported that this specific client agent version (all builds) or build has been superseded by a newer version or build.
Disabled	Yes or no. If yes, the MCS does not respond to communication requests from any client with this specific client agent version (all builds) or build.
Client Registration Disabled	Yes or no. If yes, clients running this agent version (all builds) cannot register with this Avamar server.

Plug-ins Summary view

The Plug-ins Summary view lists all client plug-ins versions and builds potentially known to this Avamar server.

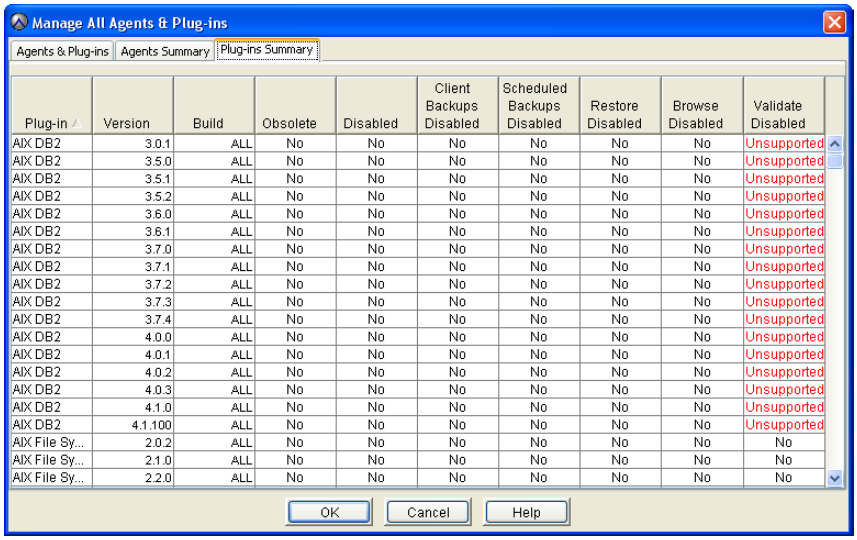
Specific plug-in versions and builds that are not supported by a version of Avamar server software appear as obsolete. Clients with these versions or builds are denied access to the server and must be upgraded before access is permitted. To determine the compatibility of client and server versions, refer to the *EMC Avamar Compatibility and Interoperability Matrix*, available on the EMC online support website at https://support.emc.com/products.

To display the Plug-ins Summary view:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.

2. Click the **Plug-ins Summary** tab.



Plug-in	Version	Build	Obsolete	Disabled	Client Backups Disabled	Scheduled Backups Disabled	Restore Disabled	Browse Disabled	Validate Disabled
AIX DB2	3.0.1	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.5.0	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.5.1	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.5.2	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.6.0	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.6.1	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.7.0	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.7.1	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.7.2	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.7.3	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	3.7.4	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.0.0	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.0.1	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.0.2	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.0.3	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.1.0	ALL	No	No	No	No	No	No	Unsupported
AIX DB2	4.1.100	ALL	No	No	No	No	No	No	Unsupported
AIX File Sy...	2.0.2	ALL	No	No	No	No	No	No	No
AIX File Sy...	2.1.0	ALL	No	No	No	No	No	No	No
AIX File Sy...	2.2.0	ALL	No	No	No	No	No	No	No

The following table explains the properties shown for each plug-in.

Table 42 Avamar plug-in property descriptions (page 1 of 2)

Property	Description
Name	Name of this plug-in.
Version	Specific version of this plug-in.
Build	Specific software build of this plug-in, or ALL if this entry is applicable to all versions.
Obsolete	Yes or no. If yes, the agents and plug-ins definition file has reported that this specific client plug-in version (all builds) or build has been superseded by a newer version or build.
Disabled	Yes or no. If yes, any client running this specific client plug-in version (all builds) or build is prevented from performing any backup, restore, or validation activities.
Client Backups Disabled	Yes or no. If yes, on-demand backups cannot be initiated by clients with this specific client plug-in version (all builds) or build.
Scheduled Backups Disabled	Yes or no. If yes, scheduled backups are not performed on clients with this specific client plug-in version (all builds) or build.
Restore Disabled	Yes or no. If yes, restores cannot be performed on clients with this specific client plug-in version (all builds) or build.

Table 42 Avamar plug-in property descriptions (page 2 of 2)

Property	Description
Browse Disabled	Yes or no. If yes, clients with this specific plug-in version (all builds) or build are not allowed to browse the restore calendar. Unsupported denotes that this specific plug-in version does not support selective management of this feature.
Validate Disabled	Yes or no. If yes, backup validations cannot be performed using this specific plug-in version. Unsupported denotes that this specific plug-in version does not support selective management of this feature.
Extended Cancel Timeout	Yes or no. If yes, clients with this specific plug-in version (all builds) or build are allowed additional time to cancel a work order before Avamar Administrator forcibly cancels it.

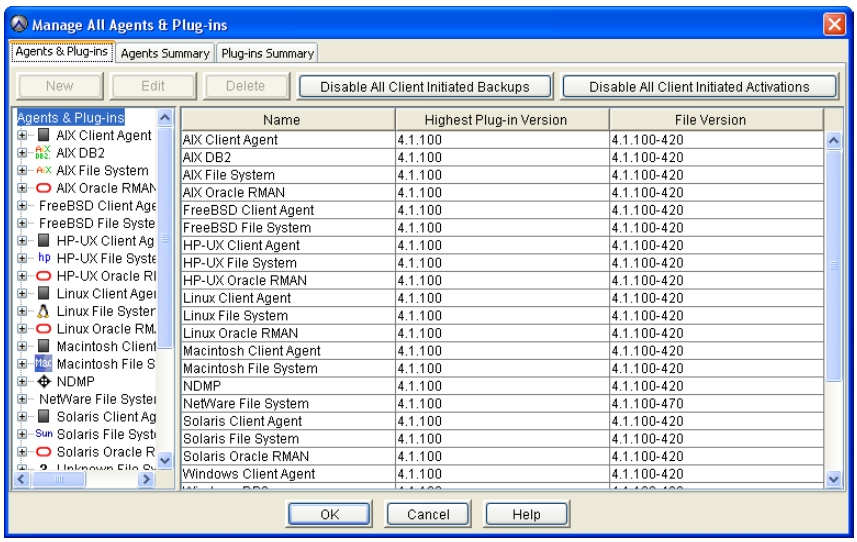
Adding a build record

You can add an MCS database record for a specific client agent or plug-in build. You can only add records at the build level; you cannot add a record for a new version (all builds). New version records are automatically added after Avamar server software upgrades.

To add a build record:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

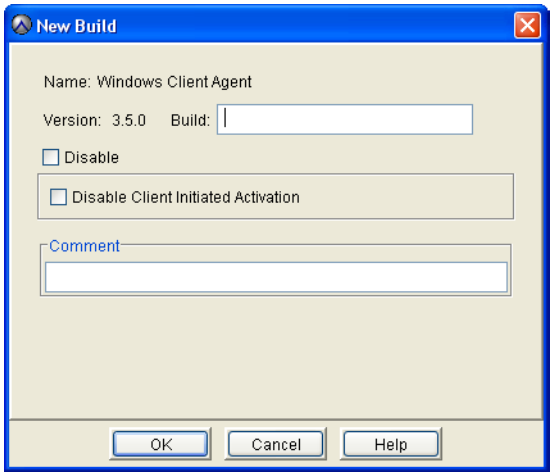
   The Manage All Agents & Plug-ins window appears.



2. In the tree, select the agent or plug-in version for the build.

3. Click **New**.

   The New Build dialog box appears.



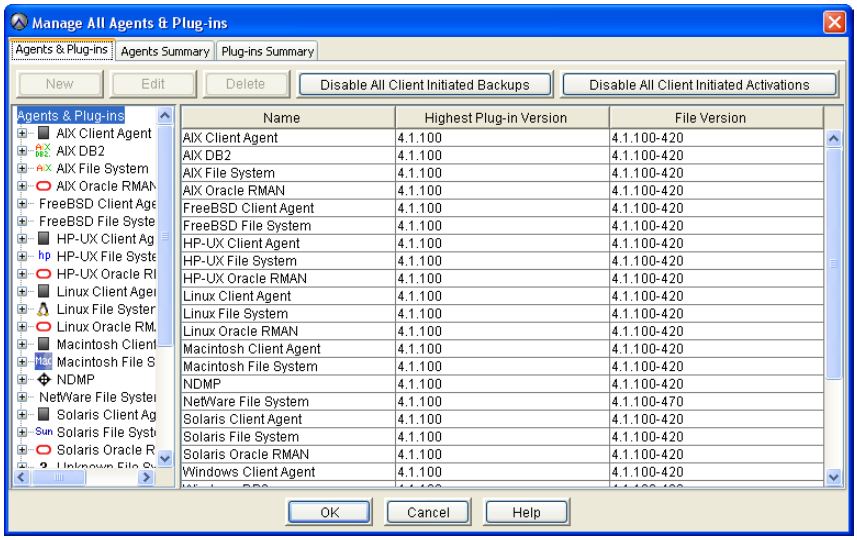
4. In the **Build** box, type a valid agent or plug-in build number.
5. To deny Avamar server access to any clients with this agent or plug-in build, select the **Disable** option.
6. To prevent any clients with this agent or plug-in build from registering with the Avamar server, select the **Disable Client Initiated Registration** option.
7. (Optional) Type a descriptive comment in the **Comment** box.
8. Click **OK**.

Editing version or build record settings

To edit version or build record settings:

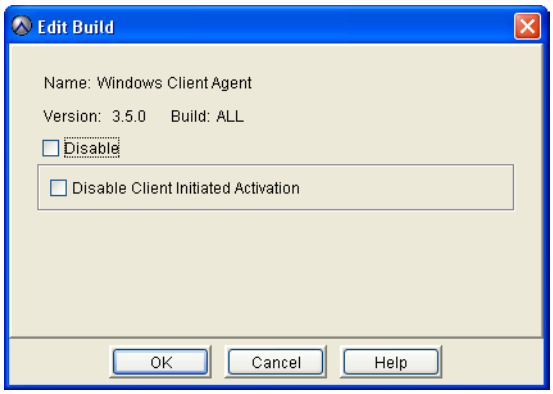
1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.



2. In the tree, select the agent or plug-in version or build to edit.
3. Click **Edit**.

   The Edit Build dialog box appears.



4. Edit the build information.

   "Adding a build record" on page 267 provides details on agent and plug-in build settings.

5. Click **OK**.

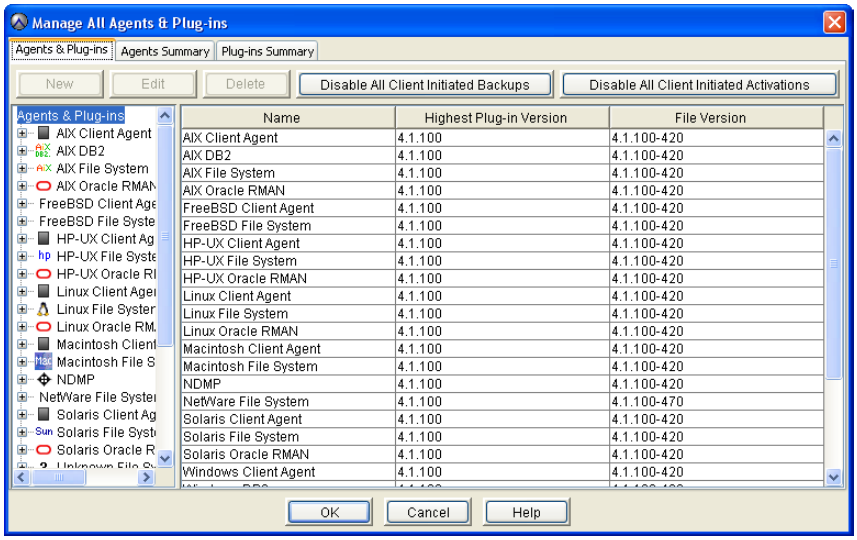
Deleting a build record

You can delete an MCS database record for a specific client agent or plug-in build. You can only delete records at the build level; you cannot delete a record for an entire version.

To delete a build record:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.



2. In the tree, select the agent or plug-in build to delete.
3. Click **Delete**.

Enabling and disabling all client initiated activations

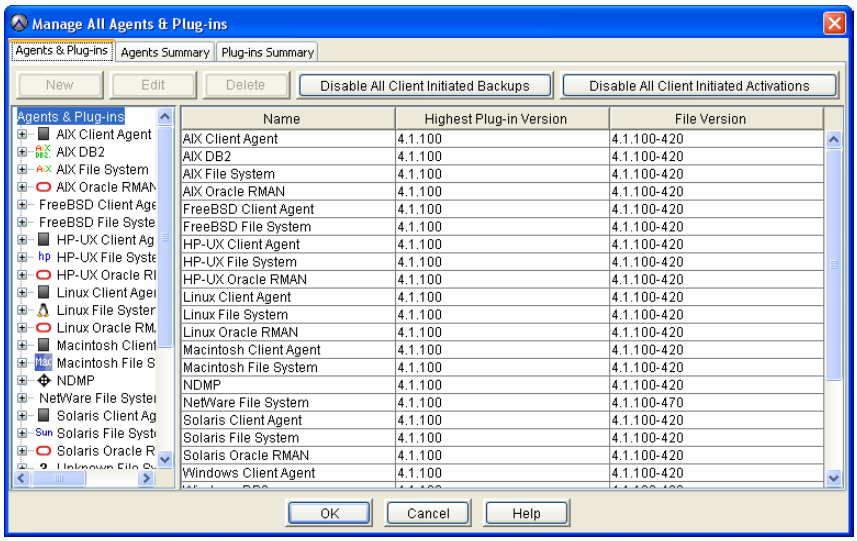
You can temporarily disable all new client initiated client activations. This is typically done to place the system in a state that supports various maintenance activities.

You can then re-enable client initiated activations.

To disable and enable client initiated activations:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.



2. Click either **Enable All Client Initiated Activations** or **Disable All Client Initiated Activations**.

Enabling and disabling all client initiated backups

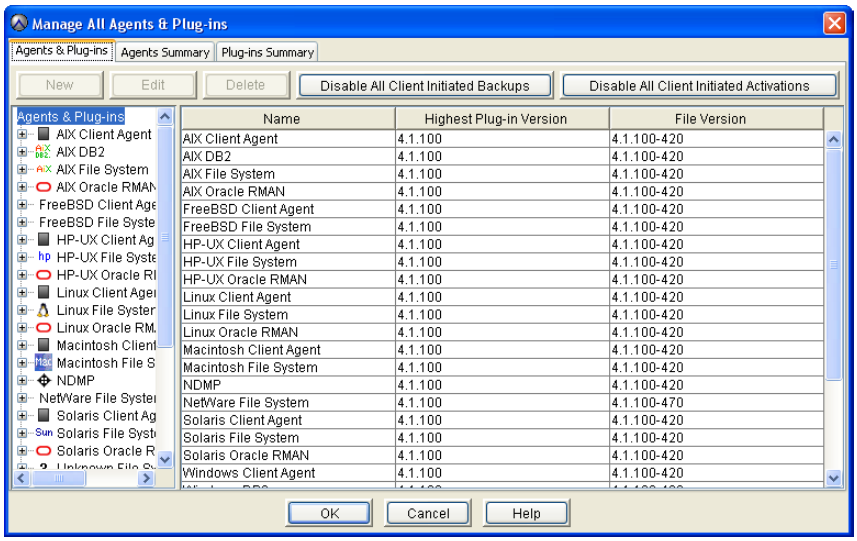
You can temporarily prevent Avamar clients from initiating on-demand backups. This is typically done to place the system in a state that supports various maintenance activities.

You can then re-enable all client initiated backups.

To disable and enable all client initiated backups:

1. In Avamar Administrator, select **Tools** › **Manage Agents & Plug-ins**.

   The Manage All Agents & Plug-ins window appears.



2. Click either **Enable All Client Initiated Backups** or **Disable All Client Initiated Backups**.

CHAPTER 10
Server Monitoring

This following topics describe how to monitor various aspects of Avamar server performance:

- Recommended daily server monitoring 274
- Monitoring the server 274
- Verifying system integrity 289
- Viewing system events 290
- Filtering the Event Monitor display 292
- Viewing the Audit Log 295
- Filtering the Audit Log display 297
- Viewing services information 299
- Viewing a detailed client session log 301
- Creating a Zip file for EMC Customer Support 303
- Collecting and viewing log files 304

Recommended daily server monitoring

To ensure that the Avamar server is working properly, EMC recommends that you perform the system monitoring tasks listed in the following table on a daily basis.

Table 43 System monitoring tools and tasks

Monitoring Tool	Monitoring Task
Activity Monitor, described on page 116	Investigate any abnormal client activity, such as backups that complete with exceptions.
Server Monitor, described on page 274	Confirm that the last checkpoint and validated checkpoint are recent. Ideally, they should have occurred within the past 24 hours.
Event Monitor, described on page 290	Investigate any system errors or warnings.
Unacknowledged Events list, described on page 311	Investigate and clear (acknowledge) any unacknowledged events.

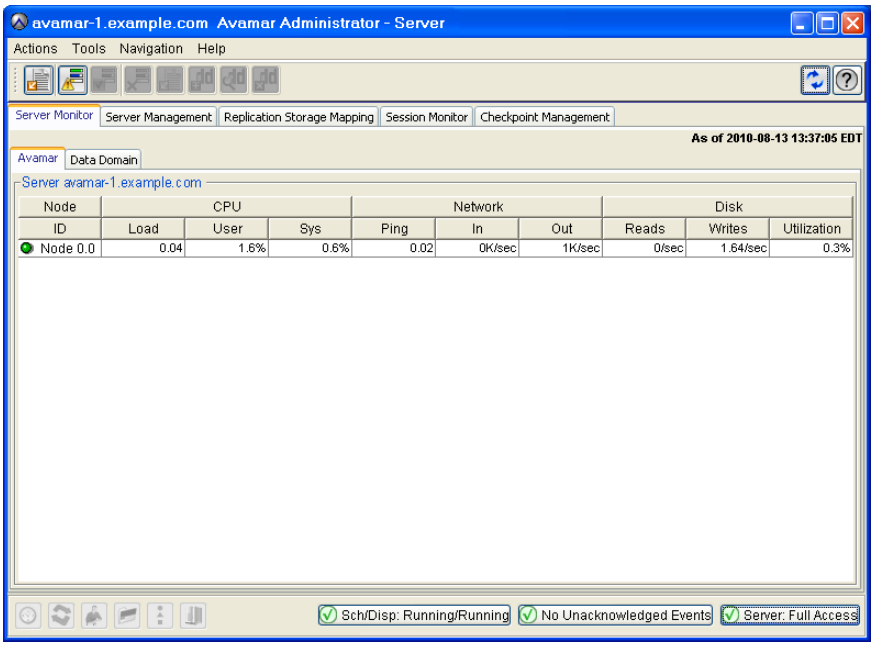
NOTICE

EMC recommends that you enable the Email Home feature and the ConnectEMC feature, which automatically email EMC Customer Service with the status of the daily data integrity check and other important server messages. "Modifying "Email Home" configuration" on page 206 and "Managing ConnectEMC" on page 224 provide details.

Monitoring the server

To monitor the server, click the **Server** launcher button in Avamar Administrator.

The Server window appears.



Server Monitor tab

The Server Monitor tab presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server, as well as any Data Domain system that might have been added to this system configuration.

Avamar tab

The Server Monitor Avamar tab presents a summarized view of CPU, network, and hard drive performance statistics for the Avamar server.

The following table describes the information available on the Server Monitor Avamar tab.

Table 44 Server Monitor Avamar tab properties (page 1 of 2)

Property	Description
Node	
Status indicators	One of the following:  Online (green)—The node is functioning properly.  Read-Only (blue)—This status occurs normally as background operations are performed and when backups have been suspended.  Time-Out (gray)—MCS could not communicate with this node.  Unknown (yellow)—Node status cannot be determined.  Offline (red)—The node has experienced a problem. If ConnectEMC has been enabled, a Service Request (SR) is logged. [1]
ID	Each node in the Avamar server has a unique logical identifier. This node ID is expressed in the following format: `MODULE.NODE` **Note:** Module and node numbering begins with zero. Therefore, the ID for the third node in the first module is 0.2.
CPU	
Load	Average number of CPU threads over the past minute.
User	Percentage of CPU capacity consumed by executing server instructions (anything other than operating system overhead).
Sys	Percentage of CPU capacity consumed by operating system overhead.
Network	
Ping	Time in seconds that this node took to respond to a ping request.
In	Received packet throughput reported in KB per second.
Out	Sent packet throughput reported in KB per second.

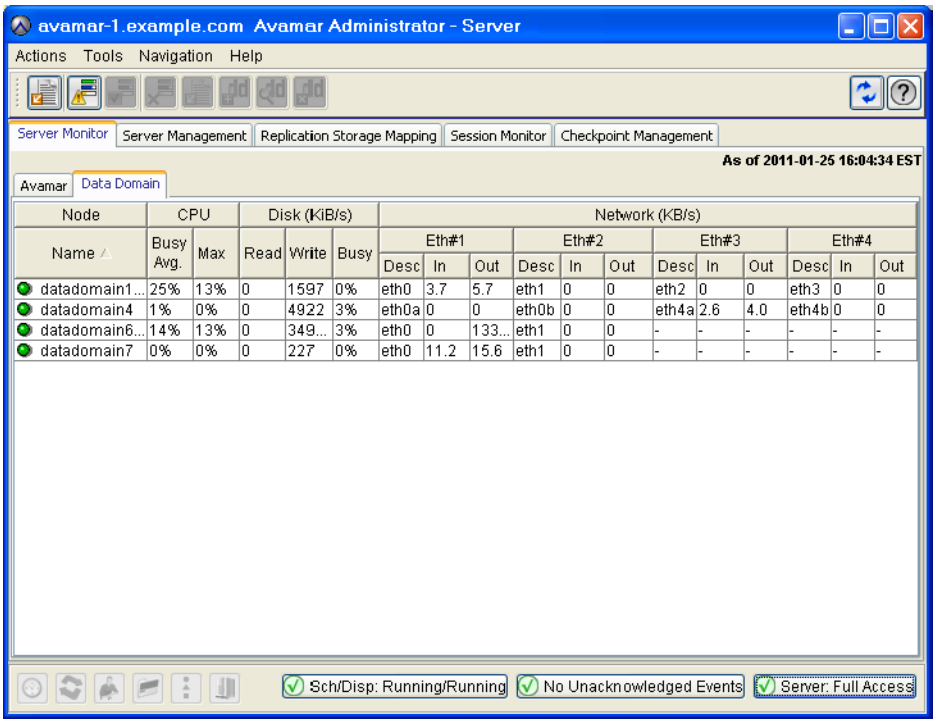
Table 44 Server Monitor Avamar tab properties (page 2 of 2)

Property	Description
Disk	
Reads	Average number of hard drive reads per second as reported by the operating system.
Writes	Average number of hard drive writes per second as reported by the operating system.
Utilization	Percentage of total available server storage capacity currently used.

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.

Data Domain tab

The Server Monitor Data Domain tab provides CPU, disk activity, and network activity for each node on the Data Domain system.



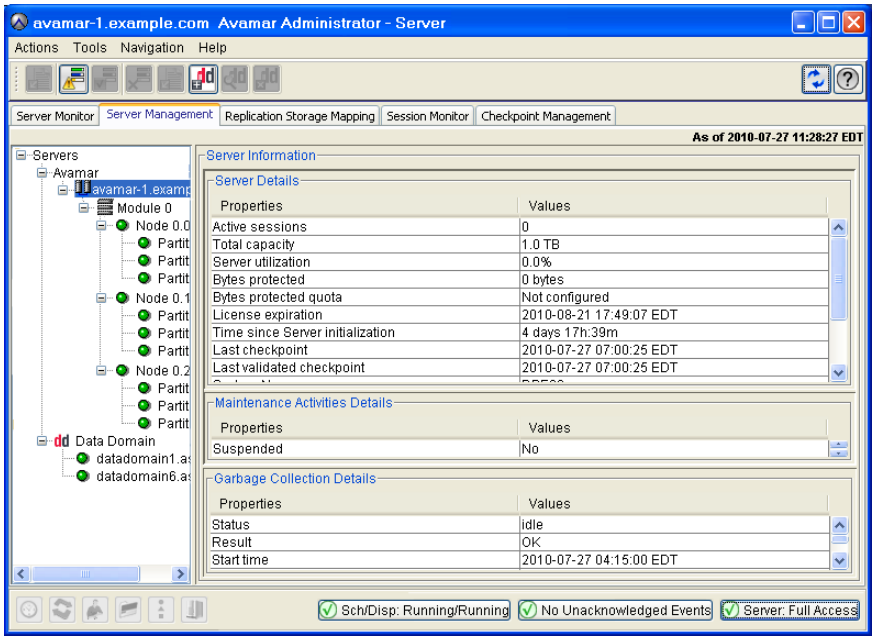
The following table describes the information available on the Server Monitor Data Domain tab.

Table 45 Server Monitor Data Domain tab properties

Property	Description
Node	
Status indicators	One of the following: OK (green)—The Data Domain system is functioning properly. Warning (yellow)—There is a problem with the Data Domain system, but backups and restores can continue. Error (red)—There is a problem with the Data Domain system, and backups and restores will not occur until the problem is resolved. If the status is yellow or red, you can view additional status information so that you can determine and resolve the problem. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details.
Name	Hostname of the Data Domain system as defined in corporate DNS.
CPU	
Busy Avg.	Average CPU usage as a percentage of total possible CPU usage.
Max	Maximum CPU usage that has occurred as a percentage of total possible CPU usage.
Disk (KB/S)	
Read	Disk read throughput in kilobytes per second.
Write	Disk write throughput in kilobytes per second.
Busy	Disk I/O usage as a percentage of total possible disk I/O usage.
Network (KB/S)	
Eth#1	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 1.
Eth#2	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 2.
Eth#3	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 3.
Eth#4	Desc—Description of the network interface. In/Out—Network bandwidth usage in kilobytes per second on network interface 4.
Note: The number of Eth# columns depends on the maximum number of network interfaces that the configured Data Domain systems support.	

Server Management tab

The Server Management tab shows a detailed view of the server hardware resources, including both the Avamar server and any configured Data Domain systems.



Avamar server information is listed under the Avamar folder in the tree, and configured Data Domain systems are listed under the Data Domain folder in the tree.

The information in the right pane of the window changes when you select different items in the tree:

- When you select the Servers node, the right pane shows a summary of bytes protected.
- When you select the Avamar or Data Domain nodes, the right pane is blank.
- When you select the Avamar server name, the right pane shows detailed information for the Avamar server.
- When you select a module, the right pane shows detailed information for that module.
- When you select a node, the right pane shows detailed information for that node.
- When you select a partition, the right pane shows detailed information for that logical hard drive partition.
- When you select a Data Domain system, the right pane shows detailed information for that Data Domain system.

NOTICE

Avamar is licensed in decimal units. Therefore, “Total capacity” and “Capacity used” are displayed in decimal units. All other parts of the product that output capacity are displayed in binary units.

The tables in the following topics provide details on the information that appears for each item in the tree.

Bytes Protected Summary

The following table provides details on the Bytes Protected Summary properties on the Server Management tab.

Table 46 Bytes Protected Summary properties on the Server Management tab

Property	Description
Properties	Name of the Avamar server and configured Data Domain systems.
Values	Number of bytes of protected data on the server or Data Domain system.

Server information

The following table provides details on the Server properties on the Server Management tab.

Table 47 Server properties on the Server Management tab (page 1 of 2)

Property	Description
Server details	
Active sessions	Current number of active client sessions. Click the Session Monitor tab for additional information. "Session Monitor tab" on page 287 provides details.
Total capacity	Total amount of server storage capacity.
Server utilization	Percentage of total available server storage capacity currently used. **Note:** This value is derived from the largest Disk Utilization value shown in the Server Monitor Avamar tab, and therefore represents the absolute maximum Avamar server storage utilization. Actual utilization across all modules, nodes and drives might be slightly lower. "Avamar tab" on page 275 provides details.
Bytes protected	Total amount of client data in bytes that has been backed up (protected) on this server.
Bytes protected quota	Maximum amount of client data in bytes that is licensed for protection on this server.
License expiration	Calendar date on which this server's licensing expires, or never if licensing is perpetual.
Time since Server initialization	Number of hours, days, and minutes that have elapsed since this Avamar server was initialized.
Last checkpoint	Date and time that the last server checkpoint was performed. Checkpoints are typically performed twice daily.
Last validated checkpoint	Date and time that the server checkpoint was last validated. Checkpoint validation normally occurs once per day. Therefore, the Last validated checkpoint time and Last checkpoint time might be different depending on the time of day that you view this information. **Note:** If the Last validated checkpoint and Last checkpoint times are more than 36 hours apart, this indicates that checkpoint validation is not occurring. This is a problem.[1]
System Name	User-assigned name of this Avamar server.

Table 47 Server properties on the Server Management tab (page 2 of 2)

Property	Description
System ID	Unique identifier for this Avamar server.
HFSAddr	Hash File System (HFS) address (Addr). This is the hostname or IP address that backup clients use to connect to this Avamar server.
HFSPort	Hash File System (HFS) data port. This is the data port that backup clients use to connect to this Avamar server. The default is port 27000.
IP Address	IP address of this Avamar server. If the HFSAddr is an IP address, this value is the same as the HFSAddr.
Maintenance activities details	
Suspended	One of the following: • No—Server maintenance activities are not currently suspended (that is, server maintenance activities will run normally during the next maintenance window). "Maintenance window" on page 310 provides details. • Yes—Server maintenance activities are currently suspended.
Garbage collection details	
Status	One of the following: • Idle—Garbage collection is not currently taking place. • Processing—Garbage collection is currently taking place.
Result	One of the following: • OK—Last garbage collection activity successfully completed. • Error code—Last garbage collection activity did not successfully complete.
Start time	Date and time that the last garbage collection activity began.
End time	Date and time that the last garbage collection activity ended.
Passes	Total number of passes during the last garbage collection activity.
Bytes recovered	Total amount of storage space in bytes that was recovered during the last garbage collection activity.
Chunks deleted	Total number of data chunks that were deleted during the last garbage collection activity.
Index stripes	Total number of index stripes.
Index stripes processed	Total number of index stripes that were processed during the last garbage collection activity.

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs.

Module information

The following table provides details on the Module properties on the Server Management tab.

Table 48 Module properties on the Server Management tab

Property	Description
Total capacity	Total amount of server storage capacity.
Server utilization	Percentage of total available server storage capacity currently used. **Note:** This value is derived from the largest Disk Utilization value shown in the Server Monitor Avamar tab, and therefore represents the absolute maximum Avamar server storage utilization. Actual utilization across all modules, nodes and drives might be slightly lower. "Avamar tab" on page 275 provides details.
Number of nodes	Total number of nodes in this module.
IP address	Base IP address of this module.

Node information

The following table provides details on the Node properties on the Server Management tab.

Table 49 Node properties on the Server Management tab (page 1 of 3)

Property	Description
Status indicators	One of the following: Online (green)—Node is functioning properly. Read-Only (blue)—This occurs normally as background operations are performed and when backups have been suspended. Time-Out (gray)—MCS could not communicate with this node. Unknown (yellow)—Node status cannot be determined. Offline (red)—Node has experienced a problem.[1]
Server details	
State	Current operational state of the server. One of the following: • ONLINE—Node is functioning properly. • DEGRADED—One or more disk errors have been detected. • OFFLINE—Node has experienced a problem.[2] • READONLY—This occurs normally as background operations are performed and when backups have been suspended.

Table 49 Node properties on the Server Management tab (page 2 of 3)

Property	Description
Avamar server details	
Runlevel	Current operational state of the server. One of the following: • fullaccess—This Avamar server is fully operational. • admin—Avamar server is fully operational but only the administrator root account can access the server. • adminonly—Avamar server is fully operational but only the administrator root account can access the server. • adminreadonly—Avamar server is in a read-only condition and only the administrator root account can access the server. • readonly—Avamar server is in a read-only condition. Restores are allowed but no new backups can be taken. • suspended—Scheduled backups are disabled and will not occur until you reenable the scheduler. • synchronizing—Avamar server is priming or synchronizing stripes. This is a temporary condition. Some operations might be delayed.
Server details	
Accessmode	Current access level of the server. The full server access mode is typically represented as three four-bit fields. For example: mhpu+mhpu+0000 The most significant bits show server privileges, the middle bits show root user privileges and the least significant bits show privileges for all other users. Individual bits in these fields convey the following information: • m—Migrate allowed. • h—Hash File System (HFS) is writable. • p—Persistent store is writable. • u—User accounting is writable.
Port	Data port used for intra-node communication.
Dispatcher	Data port used by various utilities to communicate with this node.
Server uptime	Number of hours, days and minutes that have elapsed since this Avamar server was initialized.
Total capacity	Total amount of server storage capacity.
Capacity used	Total amount of server storage capacity that has been used for any reason.
Server utilization	Percentage of total available node storage capacity currently used.
Number of stripes	Total number of stripes on this node.
Server version	Version of Avamar software running on this node.
OS details	
Version	Current operating system version running on this node.
Node uptime	Number of hours, days and minutes that have elapsed since this node was last booted.
Load average	The average number of CPU threads over the past minute.
CPU %	Percentage of this node's CPU currently being used.

Table 49 Node properties on the Server Management tab (page 3 of 3)

Property	Description
Ping time (sec)	Time in seconds this node took to respond to a ping request.
Disk reads	Number of hard drive read operations per second.
Disk writes	Number of hard drive write operations per second.
Network reads	Number of Kilobytes per second read by way of this node's network connection.
Network writes	Number of Kilobytes per second written by way of this node's network connection.
Hardware details	
IP address	IP address of this node.
MAC address	Media Access Control (MAC) address. A low-level hardware address that uniquely identifies this node in the Avamar server.
Number of partitions	Total number of logical hard drive partitions in this node.

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.
2. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.

Partition information

The following table provides details on Partition properties on the Server Management tab.

Table 50 Partition properties on the Server Management tab (page 1 of 2)

Property	Description
Status indicators	One of the following: Online (green)—The partition is functioning properly. Offline (yellow)—The partition has one or more offline stripes.[1] Read-Only (blue)—The partition is read-only. Nonfunctional (red)—The partition is not functioning.[2]
Server details	
Total capacity	Total amount of server storage capacity.
Server utilization	Percentage of total available partition storage capacity that is currently used.

Table 50 Partition properties on the Server Management tab (page 2 of 2)

Property	Description
State	Current operational state of this partition. One of the following: • ONLINE—The partition is functioning properly. • MIGRATING—Transitional state that might or might not be due to normal operation. • OFFLINE—Transitional state that might or might not be due to normal operation. • READY—Transitional state that might or might not be due to normal operation. • RESTARTING—Transitional state that might or might not be due to normal operation.
Number of offline stripes	Total number of stripes on this partition that are offline due to media errors.
Number of transitioning stripes	Total number of stripes on this partition that are in a transitional state that might or might not be due to normal operation.
Properties	Various operating system properties (if known).
Values	Settings for operating system properties (if known).

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs.
2. Search the knowledgebase at the EMC online support website, https://support.emc.com/products, for solution esg108474.

Data Domain system information

The following table provides details on the Data Domain system properties on the Server Management tab.

Table 51 Data Domain system properties on the Server Management tab (page 1 of 3)

Property	Description
Status indicators	One of the following:  Online (green)—The Data Domain system is functioning properly.  Offline (yellow)—The Data Domain system is offline. The *Data Domain Offline Diagnostics Suite User Guide*, available on https://my.datadomain.com, provides more information.  Read-Only (blue)—The Data Domain system is read-only.  Nunfunctional (red)—The Data Domain system is not functioning. The *Data Domain Offline Diagnostics Suite User Guide* provides more information.
Hostname	The network hostname of the Data Domain system as defined in DNS.
Total Capacity (post-comp size)	The total capacity for compressed data on the Data Domain system.
Server Utilization (post-comp use%)	The percentage of capacity used on the Data Domain system for any reason after compression of the data.
Bytes Protected	The total number of bytes of data that are protected, or backed up, on the Data Domain system. This value is the number of bytes before the data is compressed.
File System Available (post-comp avail)	The total amount of disk space available for compressed data in the DDFS.

Table 51 Data Domain system properties on the Server Management tab (page 2 of 3)

Property	Description
File System Used (post-comp used)	The total amount of disk space used in the DDFS for compressed data.
User Name	The username of the Data Domain OpenStorage (OST) account that Avamar should use to access the Data Domain system for backups, restores, and replication, if applicable. This username is specified when you add the Data Domain system to the Avamar configuration.
Default Replication Storage System	Whether the Data Domain system is configured as default replication storage. This option is selected or cleared when you add the Data Domain system to the Avamar configuration.
Maximum Streams	The maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores. This number is configured for the Data Domain system when you add the system to the Avamar configuration.
DDOS Version	Version number of the Data Domain Operating System (DD OS) on the Data Domain system.
Serial Number	The manufacturer's serial number for the disk in the Data Domain system.
Model number	Model number of the Data Domain system.
Monitoring Status	Monitoring status of the Data Domain system. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details on the available values.

Table 51 Data Domain system properties on the Server Management tab (page 3 of 3)

Property	Description
Monitoring status details	When the monitoring status is a value other than OK, then additional information appears in a list below the Monitoring Status row. The following rows describe the available values. **Note:** Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details on how to troubleshoot error conditions that result from each of these values.
	DD Boost licensing status, either: • DDBoost Licensed • DDBoost not Licensed
	DD Boost status, either: • DDBoost Enabled • DDBoost Disabled
	Whether the DD Boost user is enabled or disabled, either: • DDBoost User Enabled • DDBoost User Disabled
	DD Boost user status, either: • DDBoost User Valid • DDBoost User Changed
	DD Boost option status, either: • DDBoost Option Enabled • DDBoost Option Disabled • DDBoost Option not Available
	Status of the non-OST user, if configured, either: • Non-ost user state is Unknown • Non-ost user Invalid • Non-ost user disabled • Non-ost user is not an admin user **Note:** This row does not appear if the non-OST user has not been configured.
	SNMP status, either: • SNMP Enabled • SNMP Disabled
	Status of the Data Domain file system, either: • File System Running • File System Enabled • File System Disabled • File System Unknown • File system status unknown since SNMP is disabled
	Whether synchronization of maintenance operations, such as checkpoints, HFS checks, and Garbage Collection, between the Avamar server and the Data Domain system can occur, either: • Synchronization of maintenance operations is off. • Synchronization of maintenance operations is on.

Replication Storage Mapping tab

The Replication Storage Mapping tab is used to map replicated clients to a Data Domain system. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details.

Session Monitor tab

The Session Monitor tab shows a list of active client backup and restore sessions.

Table 52 Session Monitor tab properties

Property	Description
User	
User	Avamar user ID (account name).
Path	Specifies a hierarchical location in the Avamar server. This option is relative to the user's home location unless slash (/) is prefixed to the path designation, in which case an absolute path is assumed.
Domain	Avamar domain where this user resides.
Client ID	Unique identifier for this Avamar client.
Session	
Type	This activity is one of the following: • avtarbackup • avtarrestore
Root	Top level of the file system being backed up, restored, or validated.
Start time	Date and time that this client session started.
Plug-in	Plug-in used for this activity.
Session ID	Unique identifier for this client session.
Work order ID	Unique identifier for this activity.
Elapsed	Length of time that this client session has been running.
Progress bytes	Total number of bytes examined during this activity.
New bytes	Percentage of new bytes backed up to either the Avamar server or a Data Domain system. Low numbers indicate high levels of data deduplication.
System	
Name	Client hostname.
OS name	Operating system used by this client.
App version	Avamar client software version.

Checkpoint Management tab

The Checkpoint Management tab shows detailed information for all system checkpoints performed for this Avamar server. "Checkpoints" on page 404 provides details on checkpoints. The following table provides details on the information shown on the Checkpoint Management tab.

Table 53 Checkpoint Management tab properties

Property	Description
Status indicators	One of the following:  The checkpoint failed validation.  The checkpoint has not yet been validated.  Validation is currently being performed on this checkpoint.  The checkpoint passed validation.
Tag	Unique identifier for this checkpoint.
Time	Date and time that this checkpoint was taken.
Nodes	Total number of nodes involved in this checkpoint.
Stripes	Total number of stripes involved in this checkpoint.
Checkpoint validation	
Start Time	Date and time that this checkpoint validation was initiated.
Finished Time	Date and time that this checkpoint validation completed.
Errors	Number of errors encountered during this checkpoint validation.
Type	One of the following: • Full—Validation performed all checks. • Rolling—All new and modified stripes were fully validated, and a subset of unmodified stripes were validated.

Verifying system integrity

To verify Avamar server integrity, you must first ensure that a validated server checkpoint exists. You might also want to collect and examine the server log files, as described in "Collecting and viewing log files" on page 304, to ensure that no errors have occurred since that checkpoint was performed.

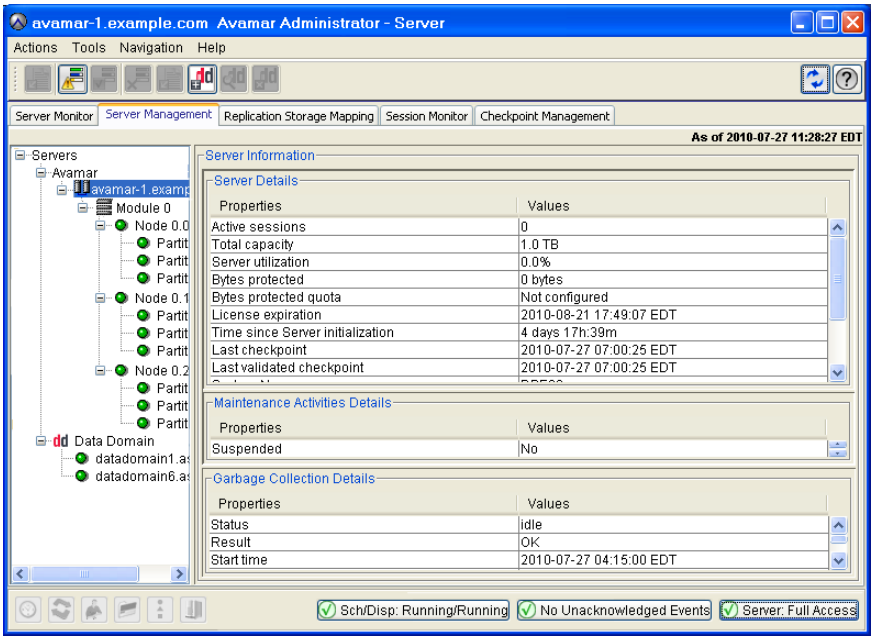
To very system integrity:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.

2. Click the **Server Management** tab.

3. Select the Avamar server name in the tree.



4. Verify that the **Last validated checkpoint** field shows a recent calendar date.

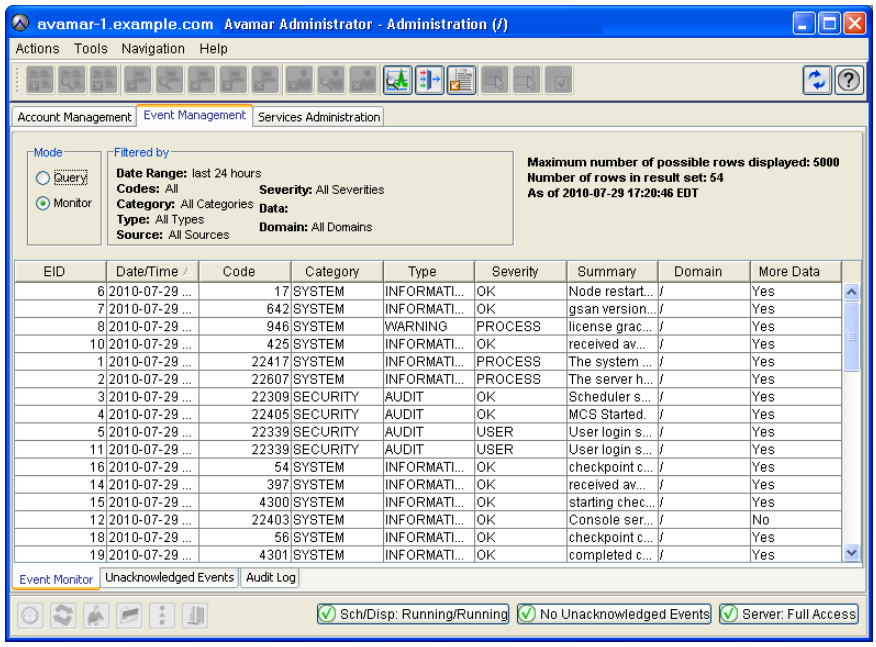
Viewing system events

To view system events:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Event Management** tab.



   The Event Monitor provides two basic display modes: query mode or monitor mode.

   - **Query Mode**—Setting the Query option places the Event Monitor in query mode, which shows the most recent 5,000 system events for a defined range of dates. "Filtering the Event Monitor display" on page 292 provides additional information about displaying a specific range of dates in the Event Monitor.
   - **Monitor Mode**—Setting the Monitor option places the Event Monitor in monitor mode, which shows the most recent 5,000 system events during the past 24 hours.

   The Filtered by fields show the current Event Monitor filtering settings. "Filtering the Event Monitor display" on page 292 provides additional information about filtering the Event Monitor display to show specific events.

3. Click the **Event Monitor** tab near the bottom of the window.

   The information in the following table appears in the Event Monitor.

Table 54 Event Monitor columns (page 1 of 2)

Column	Description
EID	ID number for the event.
Date/Time	Date and time that this event occurred.
Code	Event code number.

Table 54 Event Monitor columns (page 2 of 2)

Column	Description
Category	Event category. One of the following: • System • Application • User • Security
Type	Event type. One of the following: • Debug • Audit • Information • Warning • Error • Internal
Severity	Event severity. One of the following: • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Summary	Short description of this event.
Domain	Domain where this event occurred.
More Data	If Yes, additional detailed information is available by double-clicking the event entry or selecting the event (row) in the list and selecting Actions › Event Management › View Detail.

Filtering the Event Monitor display

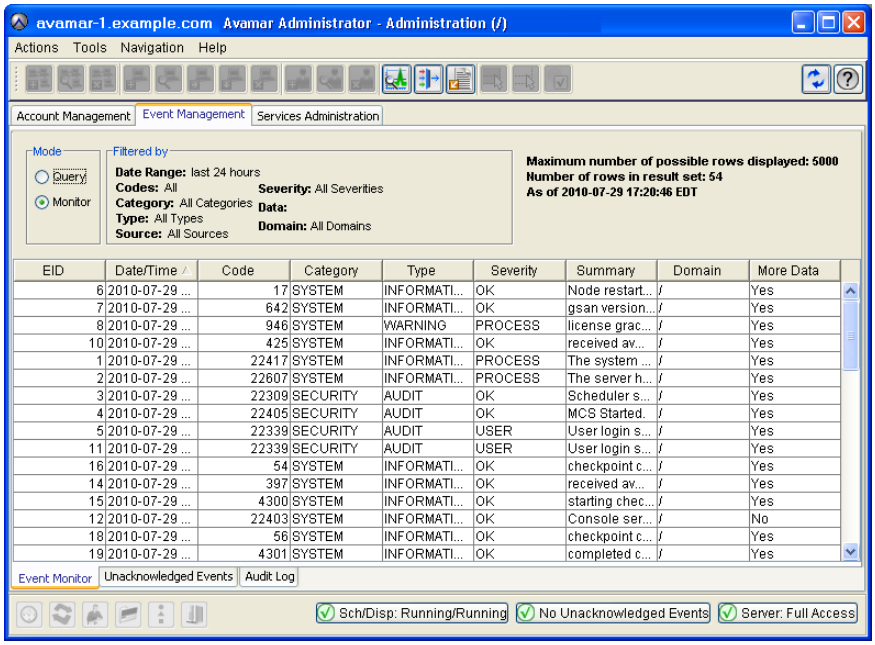
To filter the Event Monitor display:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

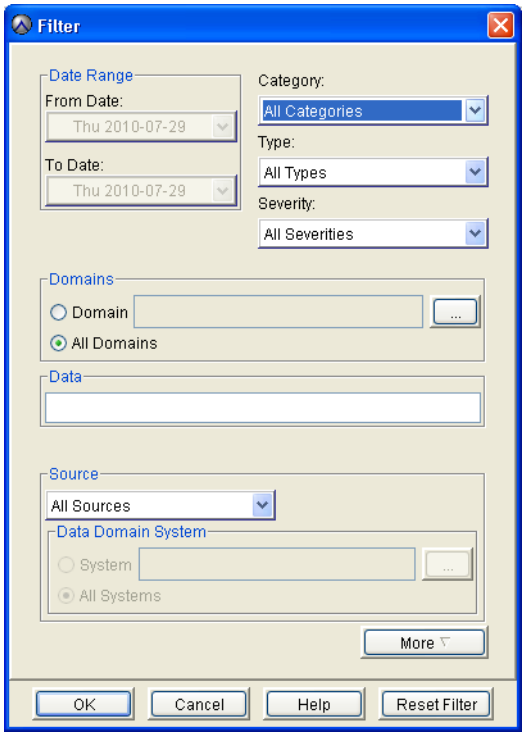
2. Click the **Event Management** tab.

3. Click the **Event Monitor** tab near the bottom of the window.



4. Open the **Actions** menu and select **Event Management** › **Filter**.

The Filter dialog box appears.



5. Define one or more of the filtering criteria described in the following table.

Table 55 Event Monitor filtering criteria (page 1 of 2)

Setting	Description
From Date	Used with the To Date field to define a specific range of dates in the Event Monitor. To type a range of dates, select the Query Mode option on the Event Monitor. Otherwise, the From Date and To Date fields are disabled.
To Date	Used with the From Date field to define a specific range of dates in the Event Monitor. To type a range of dates, select the Query Mode option on the Event Monitor. Otherwise, the From Date and To Date fields are disabled.
Category	Display events from the following categories: • All Categories • System • Application • User • Security
Type	Display events of the following types: • All Types • Debug • Audit • Information • Warning • Error • Internal

Table 55 Event Monitor filtering criteria (page 2 of 2)

Setting	Description
Severity	Display events of the following severities: • All Severities • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Domains	Select the All Domains option to display all events from all domains. To only show events from one domain, select the Domain option and type a domain name or click ... to browse to a domain.
Data	Only display events that contain these case-sensitive keywords in the event code data XML element. This promotes easy filtering on important keywords across event attributes. For example, filtering the Event Monitor display on “error” returns all events that contain the word “error” in any XML attribute (for example, category, type, or severity).
Source	Display events from all sources, from only the Avamar server, from all Data Domain systems, or from a single Data Domain system: • To view events from all sources, leave the default selection of All Sources in the list. • To view events from only the Avamar server, select Avamar from the list. • To view events from all Data Domain systems, select Data Domain Systems from the list and leave the default selection of All Systems. • To view events from a single Data Domain system, select Data Domain Systems from the list, select the System option, and then either type or browse to the Data Domain system.
More/Less	The More/Less button is used to display or hide advanced filtering features that enable you to include or exclude specific event codes. Clicking More displays an additional lower pane and the button name changes to Less. Clicking Less hides the additional lower pane and the button name changes to More.
Only include codes	Setting Only include codes filters the Event Monitor to display only those event codes in the list. The Only include codes and Exclude codes options are mutually exclusive (you cannot both exclude and include specific event codes at the same time).
Exclude codes	Setting Exclude codes causes the Event Monitor to not display any event codes in the list. The Only include codes and Exclude codes options are mutually exclusive (you cannot both exclude and include specific event codes at the same time).
Remove	Selecting an event code from the list and clicking Remove removes it from the include or exclude list.
Add to List	Typing a numeric event code in the entry field and clicking Add to list adds that event code to the include or exclude list.

6. Click **OK**.

Viewing the Audit Log

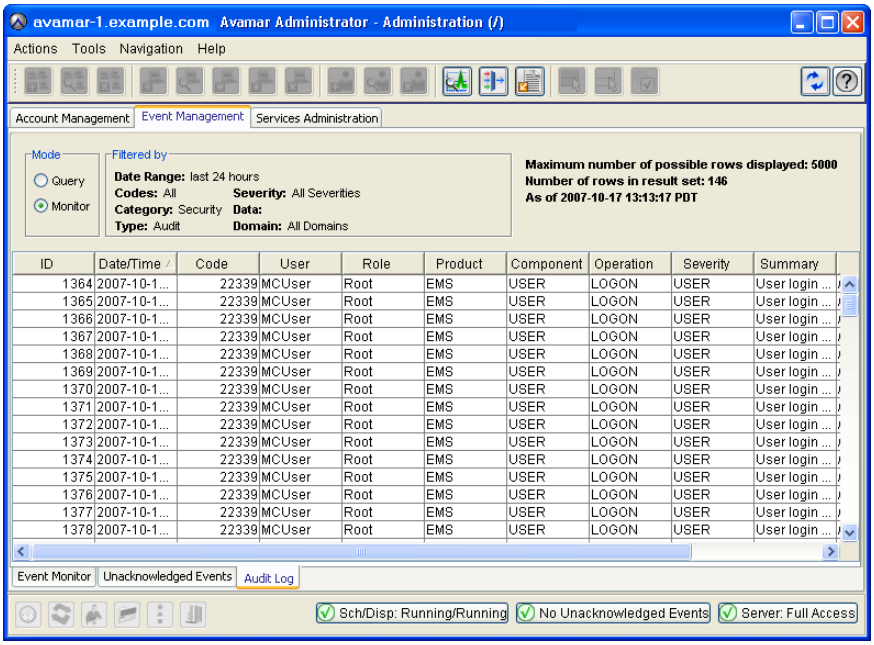
To view the Audit log:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Event Management** tab.

3. Click the **Audit Log** tab toward the bottom of the window.



The audit log provides two basic display modes: query mode or monitor mode:

- **Query mode**—Setting the Query option places the audit log in query mode, which shows the most recent 5,000 audit log entries for a defined range of dates. "Filtering the Audit Log display" on page 297 provides details on displaying a specific range of dates in the audit log.
- **Monitor mode**—Setting the Monitor option places the audit log in monitor mode, which shows the most recent 5,000 audit log entries during the past 24 hours.

The Filtered by fields show the current audit log filtering settings. "Filtering the Audit Log display" on page 297 provides additional information about filtering the audit log display to show specific audit log entries.

The following table describes the information that appears for each item in the audit log.

Table 56 Audit Log column information (page 1 of 2)

Column	Description
EID	Unique identifier for the audit log entry.
Date/Time	Date and time this action occurred.
Code	Event code number.

Table 56 Audit Log column information (page 2 of 2)

Column	Description
User	User ID that initiated this action.
Role	Role in effect when this action was initiated.
Product	One of the following: • EM—Avamar Enterprise Manager • EMS —Avamar Enterprise Manager server. • END_USER • MCCLI—Avamar Administrator Command Line Interface (CLI). • MCGUI—Avamar Administrator. • MCS—Avamar Administrator server. • NONE • SNMP_SUB_AGENT • TEST • WEB_RESTORE—Avamar web restore feature.
Component	Specific area within the product.
Operation	Specific action taken.
Severity	Event severity. One of the following: • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Summary	Short description of this action.
Domain	Domain where this action occurred.
More Data	If Yes, additional detailed information is available by double-clicking the event entry or selecting the event (row) in the list and selecting Actions › Event Management › View Detail.

Filtering the Audit Log display

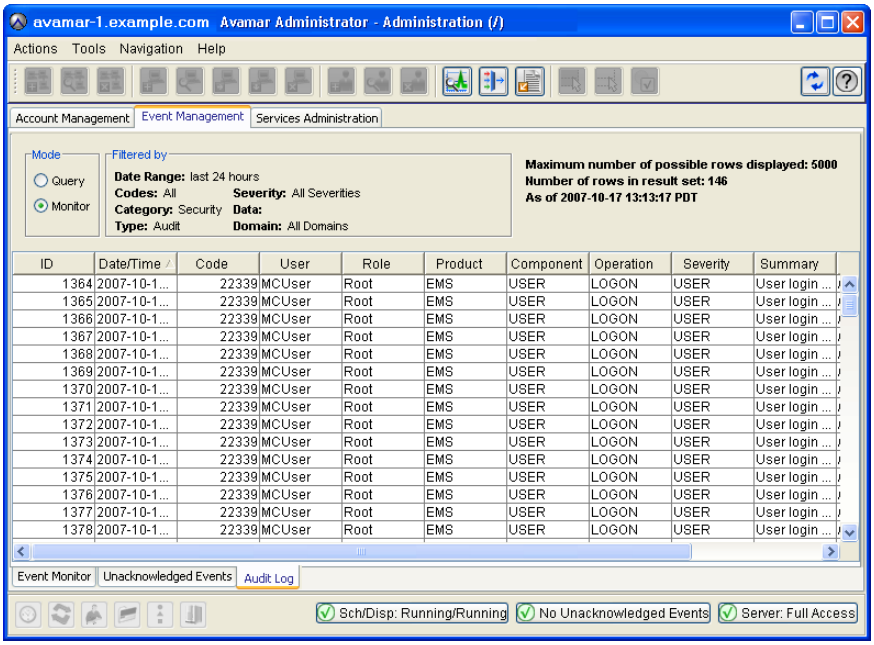
To filter the Audit Log display:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

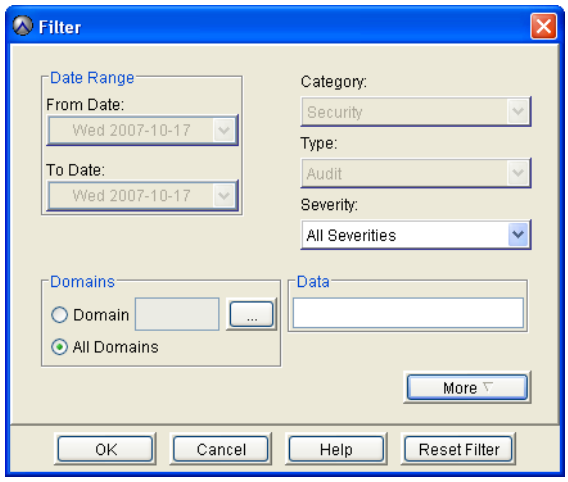
2. Click the **Event Management** tab.

3. Click the **Audit Log** tab near the bottom of the window.



4. Open the **Actions** menu and select **Event Management › Filter**.

   The Filter dialog box appears.



5. Define one or more of the filtering criteria listed in the following table.

Table 57 Audit Log filter criteria (page 1 of 2)

Setting	Description
From Date	Used with the To Date field to define a specific range of dates in the audit log. To type a range of dates, select the Query Mode option on the Audit Log tab. Otherwise, the From Date and To Date fields are disabled.
To Date	Used with the From Date field to define a specific range of dates in the audit log. To type a range of dates, select the Query Mode option on the Audit Log tab. Otherwise, the From Date and To Date fields are disabled.
Category	Security is the only available selection.
Type	Audit is the only available selection.
Severity	Display audit log entries of the following severities: • All Severities • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Domains	Select the All Domains option to display all audit log entries from all domains. To only show audit log entries from one domain, select the Domain option and type the domain, or click ... to browse to a domain.
Data	Only display audit log entries that contain these case-sensitive keywords in the event code data XML element. This promotes easy filtering on important keywords across audit log entry attributes. For example, filtering the audit log display on “error” returns all audit log entries that contain the word “error” in any XML attribute (for example, category, type, or severity).
More/Less	The More/Less button is used to display or hide advanced filtering features that enable you to include or exclude specific event codes. Clicking More displays an additional lower pane and the button name changes to Less. Clicking Less hides the additional lower pane and the button name changes to More.
Only include codes	Setting Only include codes filters the audit log to display only those event codes in the list. The Only include codes and Exclude codes options are mutually exclusive (you cannot both exclude and include specific event codes at the same time).

Table 57 Audit Log filter criteria (page 2 of 2)

Setting	Description
Exclude codes	Setting Exclude codes causes the audit log to not display any event codes in the list. The Only include codes and Exclude codes options are mutually exclusive (you cannot both exclude and include specific event codes at the same time).
Remove	Selecting an event code from the list and clicking Remove removes it from the include or exclude list.
Add to list	Typing a numeric event code in the entry field and clicking Add to list adds that event code to the include or exclude list.

6. Click **OK**.

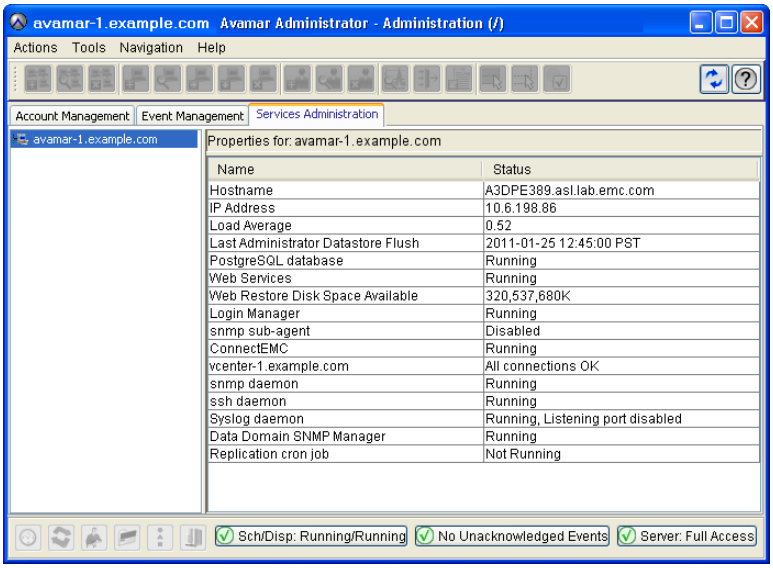
Viewing services information

To view services information:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Services Administration** tab.



   The Services Administration tab provides information about essential Avamar services (for example, syslog, NTP, Login Manager, and so forth), as described in the following table.

Table 58 Services Administration tab properties (page 1 of 2)

Service Name	Description
Hostname	Avamar server network hostname as defined in DNS.
IP Address	Avamar server IP address.
Load Average	Average number of CPU threads over the past minute.

Table 58 Services Administration tab properties (page 2 of 2)

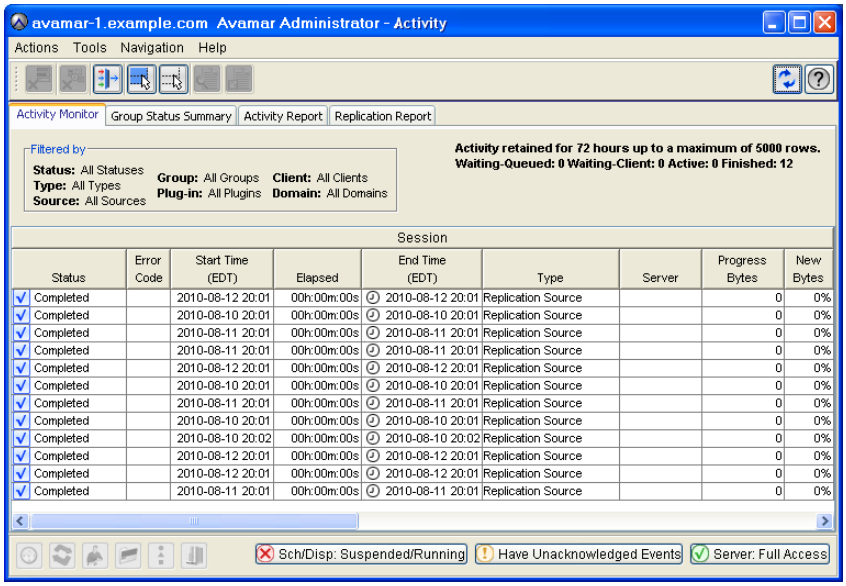
Service Name	Description
Last Administrator Datastore Flush	Date and time of the last MCS flush.
PostgreSQL database	Status of the MCS database.
Web Services	Status of the Avamar Web Access service.
Web Restore Disk Space Available	Number of hard drive bytes that Avamar Web Access can use to create the restore ZIP file. The *EMC Avamar Backup Clients User Guide* provides additional information about restoring client files using the Avamar Web Access feature.
Login Manager	Status of the Avamar Login Manager service.
snmp sub-agent	Status of the Avamar SNMP sub-agent service
ConnectEMC	Status of the ConnectEMC service.
VMware vCenter Connection Monitor	Status of the VMware vCenter connections. This service is only present if a vCenter client has been added to the system. The *EMC Avamar for VMware User Guide* provides additional information.
snmp daemon	Status of the Avamar SNMP master agent service.
ssh daemon	Status of the Avamar Secure Shell (SSH) service.
syslog daemon	Status of the Avamar syslog service.
Data Domain SNMP Manager	Status of the SNMP service for monitoring configured Data Domain systems.
Replication cron job	Status of the Avamar replication cron job. "Replication" on page 369 provides additional information.

Viewing a detailed client session log

To view a detailed client session log:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.

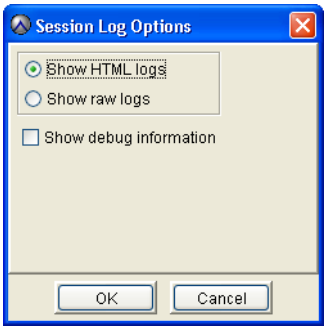


2. Click the **Activity Monitor** tab.

   By default, the Activity Monitor shows a detailed log of all client backup activity for the past 72 hours.

3. To set session log options, select **Action** › **Session Log Options.**

   The Session Log Options dialog box appears.



   The session log summary is formatted as HTML text by default. You can view the session log summary as unformatted text by selecting **Show raw logs**.

4. (Optional) To include debug information in the session log summary, select the **Show debug information** checkbox.

   This option is available when the **Show HTML log** option is selected.

5. Click **OK**.

6. Select an activity in the list.

7. Select **Actions** › **View Session Log**.

   The Activity Session Drill-down dialog box appears.

   When the session log summary is formatted as HTML text, hyperlinks for each log file are listed in the Log Files section.

8. (HTML format only) In the **Log Files** section, click on a hyperlink to jump to the log file.
9. To find a specific text string in the session log summary:
   a. Type a text string in the **Find** field.
   b. Click **Next**.

      The search function highlights text strings in yellow when they are found in the session log summary or displays the message, "String not found," when the text string is not found in the session log summary.

   c. Click **Previous** to find the previous occurrence of the text string.
10. To return to the top of the session log summary, click **Back to Top**.
11. To save the session log summary to a file:
    a. Click **Export**.

       The Save Session Log dialog box appears.

    b. Navigate to a destination folder for the file.
    c. Click **Save**.
12. To update the contents in the session log summary, click **Refresh**.
13. Click **Close** to close the **Activity Session Drill-down** dialog box.

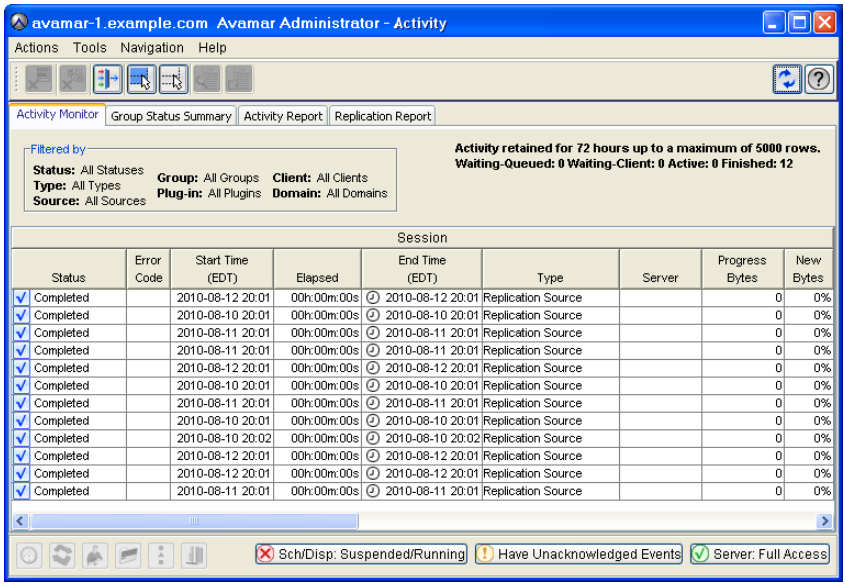
Creating a Zip file for EMC Customer Support

The **Activity** window enables you to create a Zip file for EMC Customer Support and upload the Zip file to the Avamar server.

To create a Zip file and upload it to the Avamar server:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.



2. Select an activity in the list.
3. Select **Actions** › **Download Support Bundle.**

   The Download Support Bundle dialog box appears.
4. Navigate to a directory for the zip file.
5. Click **Save**.

   The Download Support Bundle Progress dialog box appears, and a progress bar displays the download progress as a percent.
6. Click **Close** to close the Download Support Bundle Progress dialog box.
7. To create a Zip file and copy it to the Avamar server, select **Actions** › **Upload Support Bundle to Server.**

   The Upload Support Bundle Progress dialog box appears.

   The upload process creates a Zip file for session log summary information and copies the Zip file to the /tmp folder on the Avamar server.

Collecting and viewing log files

By default, the Avamar storage process log file (gsan.log) is limited to 25 MB in size and always contains the most recent information. Additional historic log files (for example, gsan.log.1, gsan.log.2, and so forth) might also exist.

To collect and view log files:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Create a new user-defined temporary directory and change directory to it by typing:

   ```
   mkdir DIR
   cd DIR
   ```

   where DIR is a new user-defined temporary directory. This directory is deleted after this procedure.
3. Retrieve copies of the storage node log files by typing:

   ```
   getlogs
   ```

   The **getlogs** command gathers the important log files from a particular node, compresses them into a single tar file (nodelogs.tgz), then copies these nodelogs.tgz files to numbered subdirectories in the current working directory.
4. Examine these nodelogs.tgz files for any entry that contains the string “ERROR.” To accomplish this, run the following shell commands, which write any nodelogs.tgz entries that contain the string “ERROR” to a user-defined temporary file:

   ```
   for p in [01].[!sm]*/nodelogs.tgz; do
   tar xzf $p
   grep ERROR: cur/gsan.log*
   rm -rf cur/*
   done
   ```

5. Remove the user-defined temporary directory by typing:

   ```
   cd ../
   rm -rf DIR
   ```

   where DIR is the user-defined temporary directory created in step 2 .

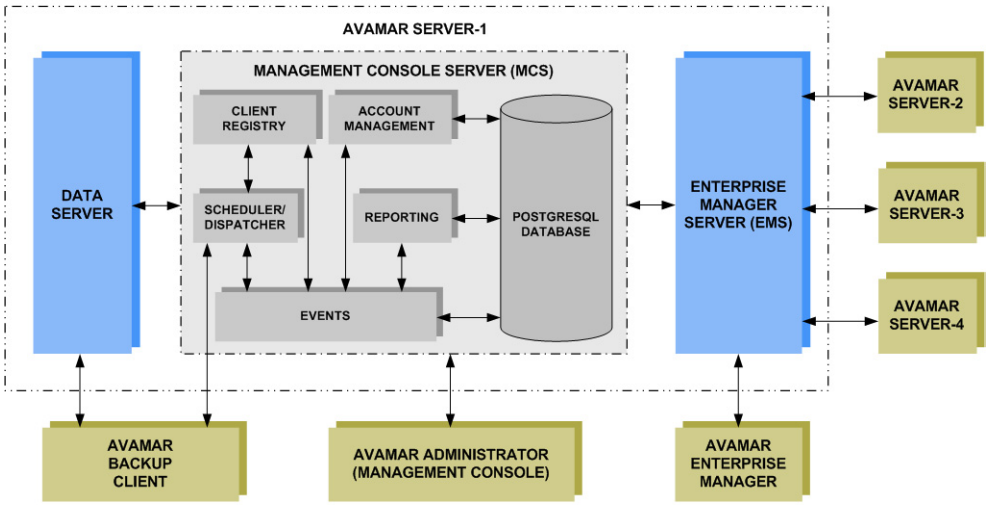
CHAPTER 11
Basic Server Administration

The following topics discuss basic Avamar server administrative concepts and tasks:

- Avamar server functional block diagram 306
- Viewing and editing server contact information 308
- Avamar server maintenance activities and backup/maintenance windows 309
- Acknowledging system events 311
- Suspending and resuming backups and restores 312
- Suspending and resuming scheduled operations 313
- Enabling and disabling scheduled group backups 313
- Suspending and resuming maintenance activities 314
- Changing backup/maintenance window settings 314
- Managing services 316
- Canceling a client session 317
- Resetting a client 318

Avamar server functional block diagram

The following diagram shows the major Avamar server functional blocks.



Data server

When performing a backup, restore, or validation, Avamar backup clients communicate directly with the data server. All scheduled backups are initiated by the MCS scheduler.

Management Console Server (MCS)

The Management Console Server (MCS) provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by the Avamar Administrator graphical management console.

Client registry

The client registry function controls client registration and activation. "Clients" on page 60 provides details.

Account management

The account management function is used to create and manage domains, clients, users, and groups. Chapter 3, "Domains, Clients, and Users," and Chapter 6, "Groups and Group Policies," provide details.

Reporting

The reporting function is used to create and export various reports. Chapter 8, "Reporting," provides details.

Events

The events function is used to display various system events and activities. "Viewing system events" on page 290 provides details.

Scheduler/dispatcher

The scheduler/dispatcher function controls when backup and restore jobs are performed, or if they can be queued for processing. Chapter 4, "Backup, Restore, and Backup Management," provides details.

PostgreSQL database

The MCS uses a PostgreSQL database to store various kinds of data. PostgreSQL is an open architecture. Information in the MCS database is accessible through any PostgreSQL-compliant ODBC interface.

The MCS database filename is mcdb, and it is located on the utility node in the /usr/local/avamar/var/mc/server_data/postgres directory.

MCS database contents are fully backed up on the Avamar server and can be restored as needed should the MCS fail.

NOTICE

The MCS database is intended for read-only access for reporting or query purposes. Do not manually modify any data in mcdb tables unless instructed to do so by EMC Customer Support. Directly modifying MCS operational data can cause loss of referential integrity, which could result in irretrievable loss of data.

Enterprise Manager Server (EMS)

The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar server information and provides a mechanism for managing Avamar servers using a standard web browser. The EMS also communicates directly with MCSs, which are an integral part of all Avamar systems in an enterprise. "Avamar Enterprise Manager" on page 325 provides details.

Viewing and editing server contact information

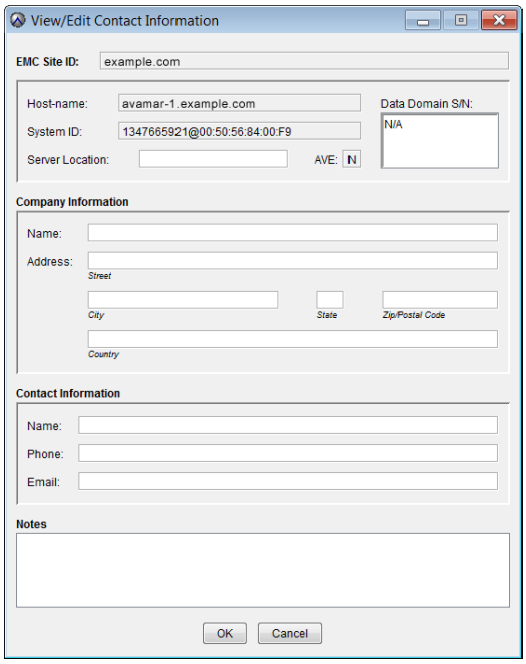
The Avamar server sends the information in the View/Edit Contact Information dialog box to EMC with every event it reports, including capacity reports that help prevent the system from exceeding critical thresholds. Keep this information current.

A server rollback applies the contact information that existed at the time of the checkpoint. When the rollback completes ensure that the information is current.

To view or edit server contact information:

1. In Avamar Administrator, select **Help** › **View/Edit Contact Information**.

   The View/Edit Contact Information dialog box appears.



2. View or edit the following:

   - **EMC site ID**—Unique customer site identifier, specified during initial server installation. This field is read-only.
   - **System ID**—Unique Avamar server identifier, created during initial server installation. This field is read-only.
   - **Data Domain S/N**—Serial number of any Data Domain systems that have been added to this server; not applicable (**N/A**) otherwise.
   - **Server location**—Physical location of the Avamar server at the customer site
   - **AVE**—Yes (**Y**) if this server is an Avamar Virtual Edition (AVE) server; no (**N**) otherwise. This field is read-only.
   - **Company Information**—Name and address of the company that owns this Avamar server.
   - **Contact Information**—Name, telephone number, and email address of the primary contact for this Avamar server.

3. Click **OK**.

Avamar server maintenance activities and backup/maintenance windows

This topic discusses Avamar server maintenance activities and backup/maintenance windows.

Maintenance activities

Avamar server maintenance comprises three essential activities:

- **Checkpoint**—A checkpoint is a snapshot of the Avamar server taken for the express purpose of facilitating server rollbacks.
- **Checkpoint validation** (also known as HFS check)—A Hash File System check (also known as HFS check) is an internal operation that validates the integrity of a specific checkpoint. Once a checkpoint has passed an HFS check, it can be considered reliable enough to be used for a server rollback.
- **Garbage collection**—Garbage collection is an internal operation that recovers storage space from deleted or expired backups.

Backup/maintenance windows

Each 24-hour day is divided into two operational windows, during which various system activities are performed:

- Backup window
- Maintenance window

The following figure shows the default backup and maintenance windows.

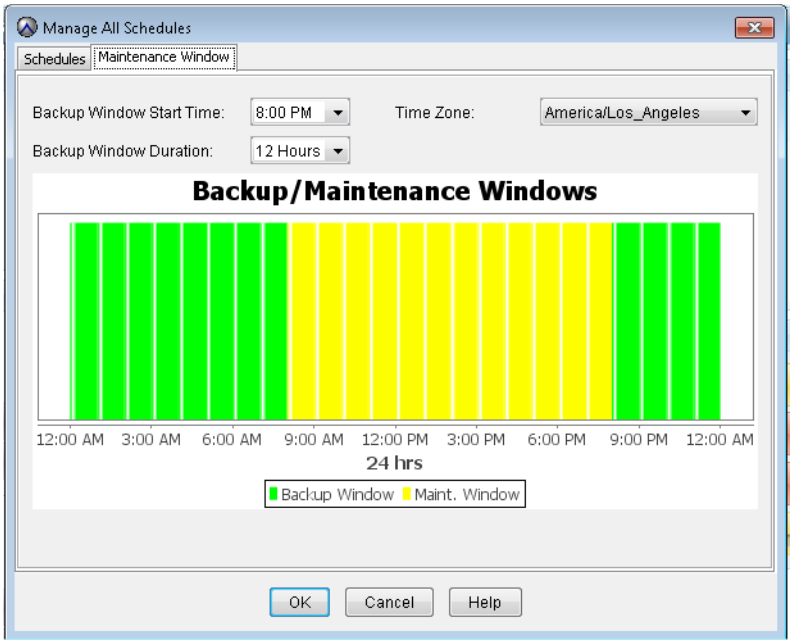


Figure 10 Default backup and maintenance window settings

Backup window

The backup window is that portion of each day reserved to perform normal scheduled backups. No maintenance activities are performed during the backup window.

The default backup window begins at 8 p.m. local server time and continues uninterrupted for 12 hours until 8 a.m. the following morning. You can customize the backup window start time and duration.

Maintenance window

The maintenance window is that portion of each day reserved to perform routine server maintenance activities, primarily garbage collection and checkpoint creation and validation.

Although you can perform backups and restores during the maintenance window, doing so impacts the backup, restore, and maintenance activities. For this reason, minimize any backup, restore, or administrative activities during the maintenance window. There might be brief periods of time when backup or administrative activities are not allowed.

The default maintenance window begins at 8 a.m. local server time and continues uninterrupted for 12 hours until 8 p.m. Although you cannot directly customize the maintenance window, its start time and duration are derived from backup window settings.

Best practices

Review the following scheduling best practices:

- **Limit on-demand backups during the maintenance window**

  You might want to advise users to avoid initiating any on-demand backups from their client computers during the first hour and thirty minutes of the maintenance window (8 a.m. to 8 p.m. local time for most systems).

- **Avoid initiating on-demand maintenance activities**

  Manually initiating maintenance activities such as checkpoint, checkpoint validation, or garbage collection temporarily disables all scheduled maintenance activities until the manually initiated operation completes. Unless there is a pressing need to initiate an on-demand maintenance activity, it is best to rely on scheduled maintenance activities to ensure that sufficient time is allocated for each activity daily.

Acknowledging system events

System events that are configured to require acknowledgement each time they occur, remain in the unacknowledged events list until they are explicitly cleared, or acknowledged, by an Avamar server administrator.

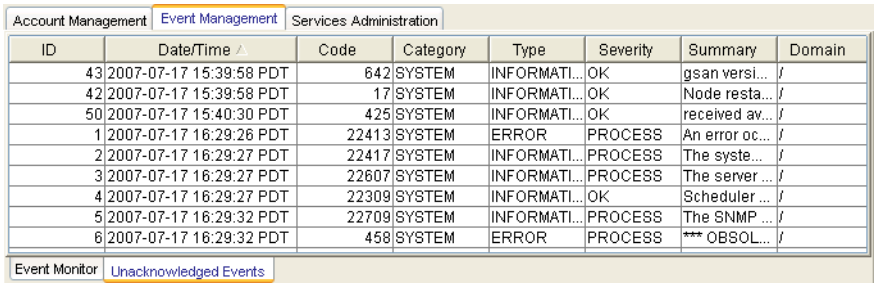
To acknowledge system events:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Event Management** tab.

3. Click the **Unacknowledged Events** tab near the bottom of the window.



4. Select one or more entries.

   Press and hold the **Shift** key to select an entire range of entries; press and hold the **Ctrl** key to select several individual (noncontiguous) entries.

5. Open the **Actions** menu and select **Event Management › Acknowledge Unacknowledged Events**.

   The selected events no longer appear in the list.

6. (Optional) Select **Actions › Event Management › Clear All Alerts** to clear the entire unacknowledged events list.

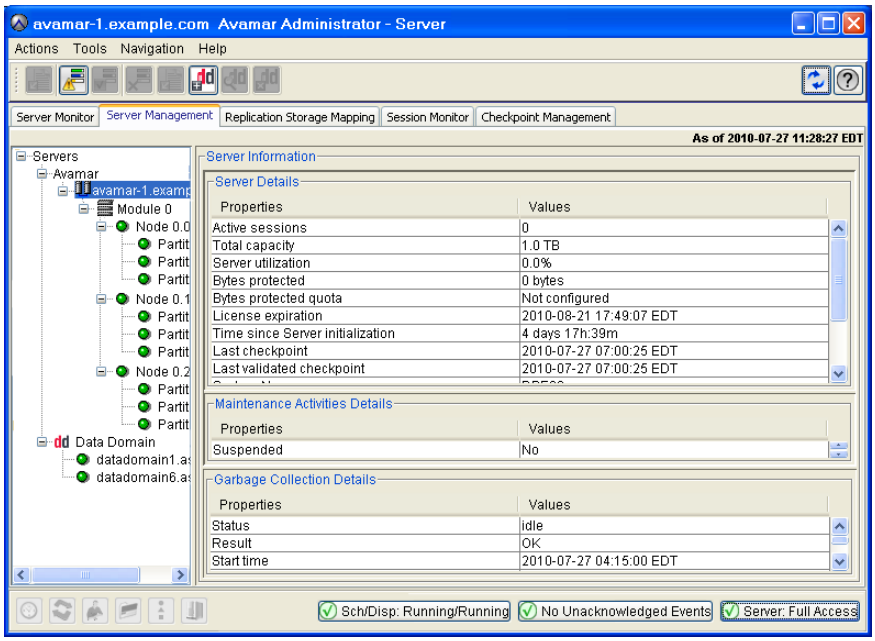
Suspending and resuming backups and restores

To suspend and resume backups and restores:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.

2. Click the **Server Management** tab.



3. In the tree pane, select the Avamar server node of the tree, as shown in the previous figure.

4. Open the **Actions** menu and select **Suspend Backups/Restores** or **Resume Backups/Restores**.

   A confirmation message appears.

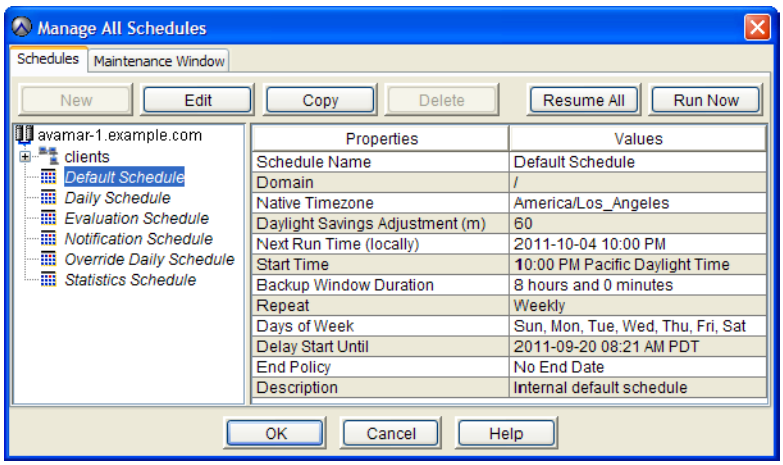
5. Click **Yes**.

Suspending and resuming scheduled operations

To suspend and resume scheduled operations:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.



2. Click **Suspend All** or **Resume All**.

Enabling and disabling scheduled group backups

To enable and disable scheduled group backups:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group.
5. Open the **Actions** menu and select **Group** › **Disable Group**.

   When the group is disabled, a checkmark appears next to the **Disable Group** option on the **Actions** › **Group** menu. When the group is enabled, the checkmark is cleared next to the option.

   A status message appears.

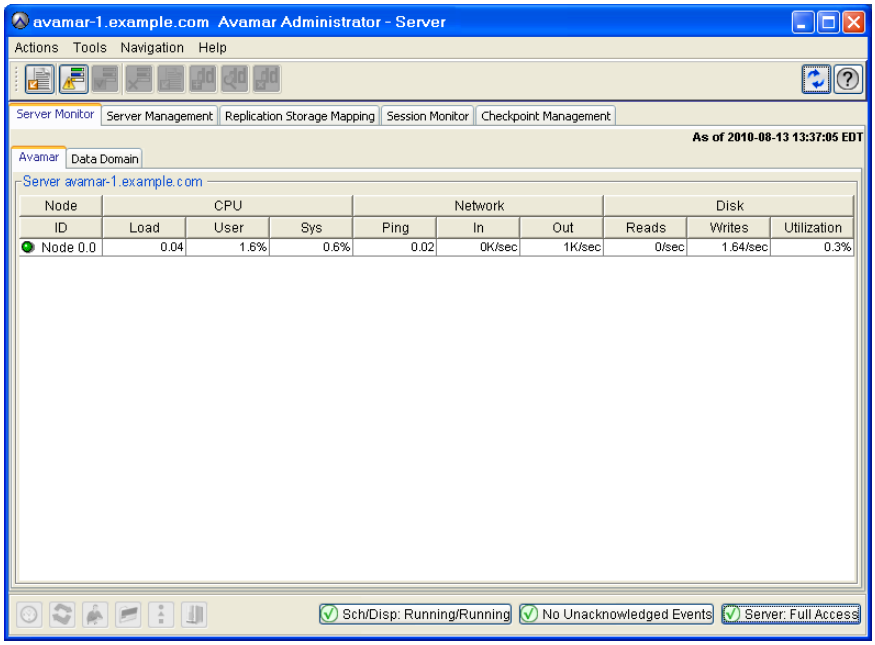
6. Click **Yes**.

Suspending and resuming maintenance activities

To suspend and resume maintenance activities:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.



2. Open the **Actions** menu and select **Suspend Maintenance Activities** or **Resume Maintenance Activities**.

   A confirmation message appears.

3. Click **OK**.

Changing backup/maintenance window settings

You can customize any of the following backup/maintenance window settings:

- Backup window start time
- Backup window duration
- Time zone

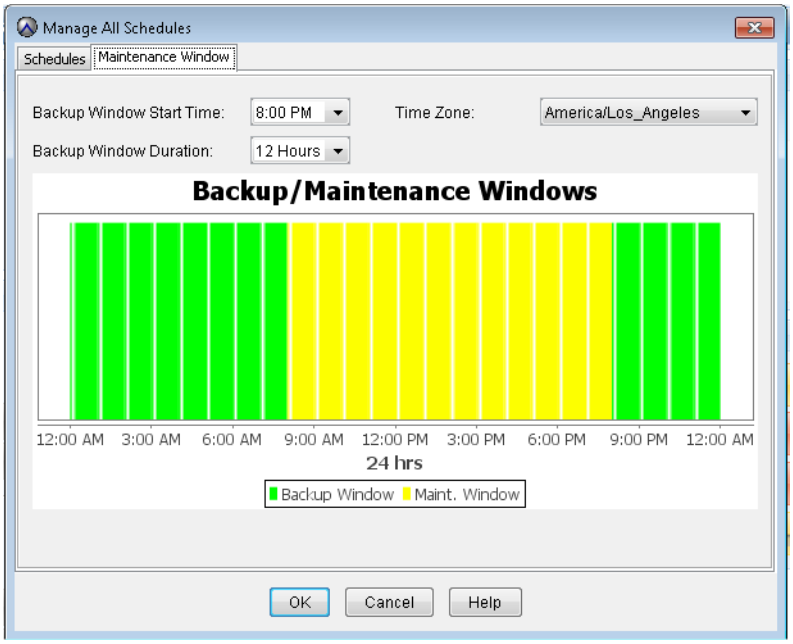
Any changes to the backup window duration also affect maintenance window duration. For example, changing the backup window duration from 12 hours to 14 hours reduces the maintenance window duration 2 hours.

To change backup/maintenance window settings:

1. In Avamar Administrator, select **Tools** › **Manage Schedules**.

   The Manage All Schedules window appears.

2. Click the **Maintenance Window** tab.



3. Change the backup window start time, duration, or time zone by selecting a new value from the corresponding list.

4. Click **OK**.

Managing services

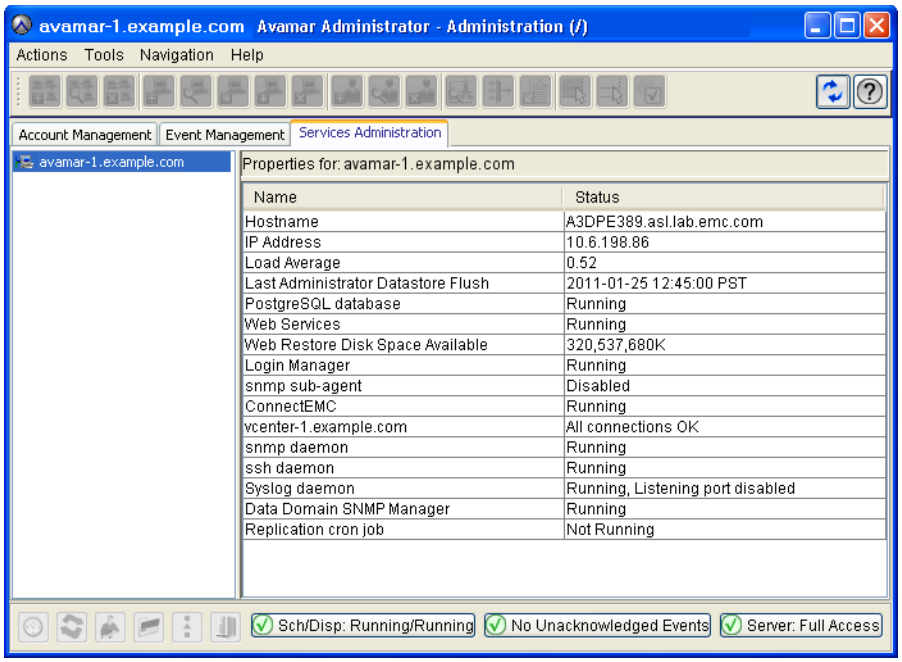
The Administration window Services Administration tab enables you to start, stop, suspend, or resume individual services.

To manage services:

1. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.

2. Click the **Services Administration** tab.



3. Manage the services:
   - To start a service, right-click the service and select **Start**.
   - To stop a service, right-click the service and select **Stop**.
   - To temporarily suspend a service until you explicitly resume it, right-click the service and select **Suspend**.
   - To resume a service that you previously suspended, right-click the service and select **Resume**.

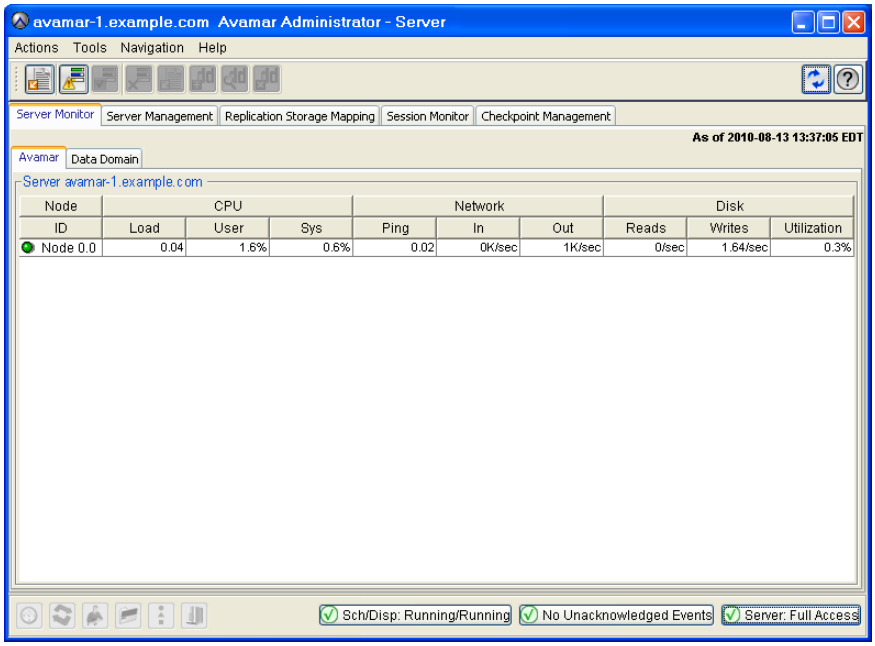
Canceling a client session

Occasionally, a client might experience unexpected system behavior while it is performing a backup or restoring files. In these cases, it might be necessary to force an end to these client sessions from Avamar Administrator.

To cancel a client session:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.



2. Click the **Session Monitor** tab.

   A list of active client sessions appears.

3. Select the client session to cancel.

4. Select **Actions** › **Cancel Session**.

   The Cancel Session Progress dialog box shows the progress of the cancel client operation. You can cancel the operation at any time by clicking **Cancel**.

5. When the **Cancel Session Progress** dialog box shows 100%, click **Close**.

   If you cannot cancel the client session, reset the client. This immediately and forcibly terminates active **avtar** session on that client. "Resetting a client" on page 318 provides details.

Resetting a client

Resetting a client immediately and forcibly terminates active client **avtar** session on that client. In most cases, you should try to cancel the client session before resetting it. "Canceling a client session" on page 317 provides details.

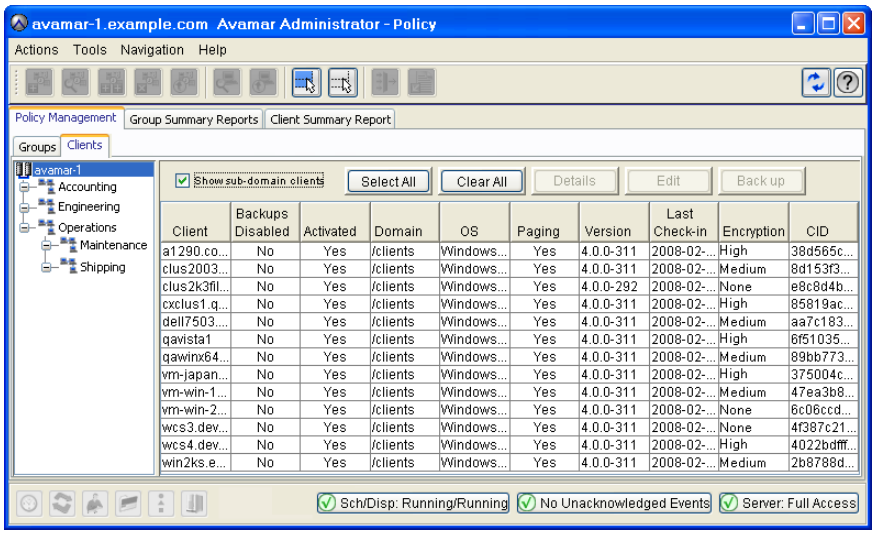
To reset a client:

1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.

3. Click the **Clients** tab.



4. Select the client to reset.

5. From the **Actions** menu, select **Client** › **Reset Client**.

CHAPTER 12
Server Shutdown and Restart

The following topics describe how to use the **dpnctl** program to gracefully shut down and restart the entire Avamar server or selected subsystems:

- Shutting down the server 320
- Restarting the server 321
- Stopping the MCS 322
- Starting the MCS 322
- Getting MCS status 323

Shutting down the server

Whenever possible, perform the following tasks as part of a full system shutdown:

- Verify system integrity as discussed in "Verifying system integrity" on page 289.
- Create and validate a server checkpoint as discussed in "Creating a checkpoint" on page 404 and in "Validating a checkpoint" on page 405.

NOTICE

If the system passed integrity checks, you do not need to create or validate a server checkpoint. However, there is no harm in doing so.

To shut down the server:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   dpnctl stop
   ```

   The following information might appear in the command shell:

   ```
   -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
   Do you wish to shut down the local instance of EMS?

   Answering y(es) will shut down the local instance of EMS
                   n(o) will leave up the local instance of EMS
                   q(uit) exits without shutting down
   y(es), n(o), q(uit/exit):
   ```

3. Type **y** to shut down the local EMS instance, or **n** to leave the local EMS instance running, and then press **Enter**.

   Information similar to the following appears in the command shell:

   ```
   dpnctl: INFO: Suspending backup scheduler...
   dpnctl: INFO: Backup scheduler suspended.
   dpnctl: INFO: Checking for active checkpoint maintenance...
   dpnctl: INFO: Terminating hfs integrity maintenance (hfscheck)...
   dpnctl: INFO: Shutting down dtlt...
   dpnctl: INFO: dtlt shut down.
   dpnctl: INFO: Shutting down EMS...
   dpnctl: INFO: EMS shut down.
   dpnctl: INFO: Shutting down MCS...
   dpnctl: INFO: MCS shut down.
   dpnctl: INFO: Shutting down gsan...
   dpnctl: INFO: gsan shut down.
   ```

Restarting the server

To bring an Avamar server back online after a system shutdown:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   dpnctl start
   ```

   The following information appears in the command shell:

   ```
   -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

   Action: starting all
   Have you contacted Avamar Technical Support to ensure that this
      is the right thing to do?

   Answering y(es) proceeds with starting all;
                   n(o) or q(uit) exits

   y(es), n(o), q(uit/exit):
   ```

3. Type **y** to proceed with restarting the server, and then press **Enter**.

   Information similar to the following appears in the command shell:

   ```
   dpnctl: INFO: Checking that gsan was shut down cleanly...
   dpnctl: INFO: Restarting the gsan (this may take some time)...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-gsan-restart-output-3366
   dpnctl: WARNING: 1 warning seen in output of "/usr/bin/yes no |
   /usr/local/avamar/bin/restart.dpn"
   dpnctl: INFO: Restarting gsan succeeded.
   dpnctl: INFO: gsan started.
   dpnctl: INFO: Starting MCS...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-mcs-start-output-3366
   dpnctl: INFO: MCS started.
   dpnctl: INFO: Starting EMS...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-ems-start-output-3366
   dpnctl: INFO: EMS started.
   dpnctl: INFO: Resuming backup scheduler...
   dpnctl: INFO: Backup scheduler resumed.
   dpnctl: INFO: Starting dtlt...
   dpnctl: INFO: dtlt started.
   ```

Stopping the MCS

To stop the MCS:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   dpnctl stop mcs
   ```

Starting the MCS

To start the MCS:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   dpnctl start mcs
   ```

3. Resume scheduled operations as discussed in "Suspending and resuming scheduled operations" on page 313.

Getting MCS status

To view the status of each MCS service and any available performance statistics:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   dpnctl status mcs
   ```

CHAPTER 13
Avamar Enterprise Manager

The following topics describe the Avamar Enterprise Manager, which is a web-based multi-system management console application that provides centralized Avamar system administration capabilities for larger businesses and enterprises:

- Capabilities and limitations 326
- Comparison with EMC Backup & Recovery Manager 328
- Shutting down the EMS 329
- Restarting the EMS 329
- Logging in to Avamar Enterprise Manager 330
- Dashboard 331
- System 335
- Capacity 344
- Policy 344
- Reports 345
- Replicator 346
- Configure 347
- Client Manager 348
- System Maintenance 348
- Monitoring other systems 348
- Suspending and resuming system monitoring 350
- Removing a system from the systems list 351
- Monitoring Avamar 5.x systems 352
- Launching Avamar Administrator from Avamar Enterprise Manager 353

Capabilities and limitations

This topic discusses various capabilities and limitations of Avamar Enterprise Manager.

Multi-system management

With Avamar Enterprise Manager, you can monitor all Avamar systems in the enterprise from a single web browser session. "Monitoring other systems" on page 348 provides additional information.

Dashboard

The integrated dashboard, described on page 331, provides an "at-a-glance" view that enables you to assess the operational status of each Avamar system and determine if backups are completing successfully.

Only one Avamar Enterprise Manager server is required

The Avamar Enterprise Manager Server (EMS) provides essential services required to display Avamar system information, and provides a mechanism to manage Avamar systems using a standard web browser. The EMS also communicates directly with MCSs, which are an integral part of all Avamar systems in an enterprise. Therefore, it is important to understand that only one operational EMS is required for an enterprise; you do not need to run EMS on every Avamar system, nor is it recommended to do so.

Monitoring multiple versions of Avamar systems

Avamar Enterprise Manager can manage Avamar 5.x, 6.x, or 7.0 systems. However, Avamar 5.x systems require additional configuration to enable monitoring with Avamar Enterprise Manager. "Monitoring Avamar 5.x systems" on page 352 provides additional information.

Use local MCS to authenticate Avamar Enterprise Manager logins

Only one operational EMS is required per enterprise, and there is usually no reason to authenticate Avamar Enterprise Manager logins using a remote MCS running on another Avamar host. Therefore, it is best to use the default installation and configuration options, which configure the EMS to use the local MCS (the MCS running on the same Avamar host) to authenticate Avamar Enterprise Manager logins.

Avamar Enterprise Manager compared with Avamar Administrator

Although the Avamar Enterprise Manager user interface is different from Avamar Administrator, the fundamental administrative principles and operations are similar. When you are familiar with how to administer an Avamar system with Avamar Administrator, you should be able to perform those same tasks with Avamar Enterprise Manager. The primary difference is that you can centrally administer every Avamar system in the enterprise from a single application, rather than launching multiple Avamar Administrator sessions.

Web browser security settings

The information presented in the remainder of this chapter assumes that you use Microsoft Internet Explorer 6 with the default security settings. If you use another web browser or other security settings, be prepared to answer Yes when presented with additional or different security prompts.

Browser security settings may impact login

Certain web browser security settings (for example, the Internet Explorer High security setting) are known to interfere with the ability to log into Avamar Enterprise Manager. If you use another web browser or other security settings, be prepared to answer **Yes** when presented with additional or different security prompts.

Session time-out information

The default session time-out setting for most Avamar Enterprise Manager features and functions is 72 hours. However, the dashboard page, described on page 331, and the replicator page, described on page 346, automatically refresh themselves every minute. Effectively, this means that if you leave the web browser pointed to the dashboard or replicator pages, the Avamar Enterprise Manager session continues indefinitely. However, if you leave the web browser pointed to any other page, the Avamar Enterprise Manager session automatically times out after 72 hours of inactivity. You can edit the default session time-out setting by changing the session-timeout preference in /usr/local/avamar-tomcat/webapps/cas/WEB-INF/web.xml.

Comparison with EMC Backup & Recovery Manager

This release is also supported by EMC Backup & Recovery Manager. Like Avamar Enterprise Manager, Backup & Recovery Manager manages all Avamar systems in the enterprise. However, Backup & Recovery Manager additionally has an integrated user interface to manage the enterprise's NetWorker servers and Data Domain backup targets.

The following table provides an overview comparison of the enterprise management capabilities of both products. The comparison focuses on Avamar-specific features and does not include the features in Backup & Recovery Manager that are specific to NetWorker servers and to Data Domain backup targets.

Table 59 Comparison of enterprise management products

	Avamar Enterprise Manager	Backup & Recovery Manager
Software host	Avamar utility node	VMware vSphere™ client
At-a-glance dashboard	Status view of Avamar systems	Select between consolidated and individual status views of: • Avamar systems • NetWorker servers • Data Domain backup targets
Detailed backup and capacity information for Avamar systems	Yes	Yes
Replication management	Yes	Yes
Launch other management applications	• Avamar Administrator • Avamar Client Manager • Avamar Installation Manager embedded in System Maintenance	• Avamar Administrator • Avamar Enterprise Manager • Avamar Client Manager • Avamar Installation Manager • AvInstaller service
Display warnings, errors, and system alerts	Yes	Yes, in a quick-look graphical display and in detailed text. Filter the view by product, system, and category.
Management reports: select, view, and export	• Backup • System	• Backup • System • Configuration

For complete information about Backup & Recovery Manager refer to the documentation provided with that product.

Shutting down the EMS

To perform an orderly shutdown of the Avamar Enterprise Manager Server (EMS):

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server, log in to the utility node as admin.
2. Type:

   ```
   dpnctl stop ems
   ```

3. Wait for dpnctl stop ems to complete.

Restarting the EMS

To restart the EMS following a shutdown:

1. Ensure that Avamar Enterprise Manager has been properly shut down.
2. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server, log in to the utility node as admin.
3. Type:

   ```
   dpnctl start ems
   ```

4. Wait for dpnctl start ems to complete.

Logging in to Avamar Enterprise Manager

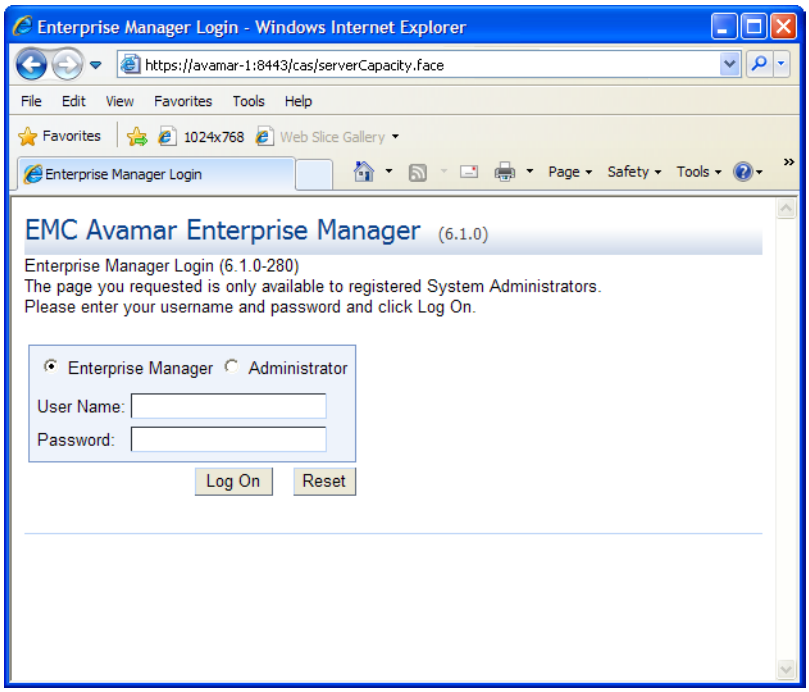
To log in to Avamar Enterprise Manager:

1. Point a web browser to the following URL:

   `http://AVAMARSERVER/em`

   where AVAMARSERVER is the hostname as defined in DNS.

   The Avamar Enterprise Manager Login page appears.



2. In **User Name**, type a username.

   The account associated with this username must be assigned the Avamar role of Administrator. "Roles" on page 78 provides details about Avamar roles.

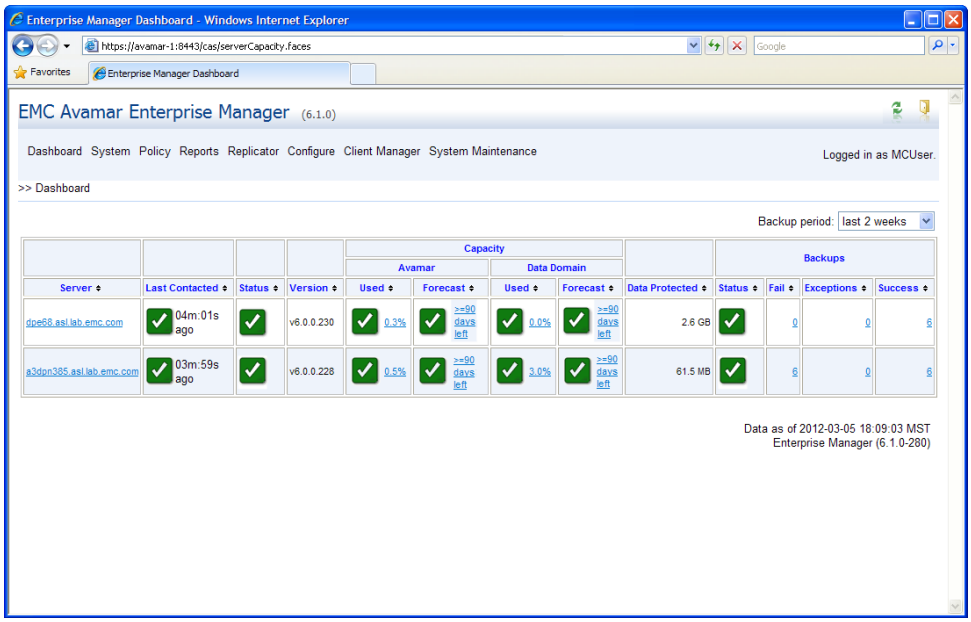
   The username is checked against the internal user database first. If no match is found, then it is checked using Enterprise authentication. If that is not enabled, or no match is found, it is checked using directory service authentication. Each of these forms of authentication, is described in "Enabling user authentication" on page 84.

3. In **Password**, type the password for the user account.
4. Click **Log On**.
5. If a **Security Warning** dialog box appears, click **Yes** to proceed with the login.

   The Dashboard page appears.

Dashboard

The Dashboard page provides an “at-a-glance” view that enables you to assess each Avamar server’s operational status and capacity utilization, as well as determine if scheduled backups are successfully completing.



Select Dashboard from any other page to view the Dashboard page.

The following table explains the information shown on the Dashboard page.

Table 60 Dashboard page information (page 1 of 4)

Information	Description
Backup period	This list box allows you to select an effective period of time for status shown in the Backups column. Choices are: • last 24 hours • last week • last 2 weeks • past month • past 3 months • past 6 months • past 9 months
Server	This column shows each server hostname as defined in corporate DNS. Click the server name to view the system information page for that Avamar server. “Individual system information page” on page 335 provides details.

Table 60 Dashboard page information (page 2 of 4)

Information	Description
Last Contacted	This column shows elapsed time since each Avamar server was last contacted by Avamar Enterprise Manager and data was collected. **Note:** If the last updated indicator shows a status other than green, all other displayed information for that system should be considered stale and might not reflect Avamar system status. Status icons communicate the following conditions:  Avamar Enterprise Manager is operating normally and is able to communicate and collect data at the specified refresh/polling interval from this Avamar server. The elapsed time since Avamar Enterprise Manager last communicated with this Avamar server is shown next to the status icon.  Last attempt by Avamar Enterprise Manager failed to communicate or collect data from this Avamar server. Avamar Enterprise Manager waits one minute and retries as many as three times before considering the refresh/polling cycle a failure. The specific reason for this condition appears next to the status icon. This condition can happen intermittently if network access to the Avamar server is slow or unreliable. It can also occur if that Avamar server is not running or has encountered an error or warning condition.  One of the following conditions: – Avamar Enterprise Manager failed to communicate and or collect data from an Avamar server for a specified number of refresh/polling cycles. – Avamar server hostname could not be resolved. – Avamar server login credentials (username or password) were refused. The default polling setting is three cycles (30 minutes total elapsed time based on a 10-minute refresh/polling cycle). The specific reason for this condition appears next to the status icon. Investigate and remedy any red status condition immediately to ensure that system operation is not adversely affected.
Status	Overall status of the Avamar server and any configured Data Domain systems.  The Avamar server and all configured Data Domain systems are fully operational.  There is an issue with either the Avamar server, a configured Data Domain system, or both that requires your attention. However, backups and restores can continue.  There is a problem with either the Avamar server, a configured Data Domain system, or both that requires your immediate attention. Backups and restores will not occur until the problem is resolved. Click the status icon to view the System Information page, which contains detailed information about the server.
Version	The version of the Avamar server software running on the server.

Table 60 Dashboard page information (page 3 of 4)

Information	Description
Capacity › Avamar › Used	This column shows summary status of how storage capacity is being used on the Avamar server. Detailed information includes the amount of storage capacity consumed in bytes and the amount of free storage capacity available as a percentage of total available storage capacity. Used status icons communicate the following conditions:  Avamar server has used less than 80% of total storage capacity.  Avamar server has used more than 80% but less than 95% of total storage capacity. Consider adding capacity or deleting old backups.  Avamar server has used more than 95% of total storage capacity. **Note:** No new backups are performed until you add capacity or delete old backups.[1] Click a capacity forecast icon to view the Capacity Utilization and Forecast, described in "Detailed utilization and forecasting" on page 362.
Capacity › Avamar › Forecast	Forecast status icons communicate the following conditions:  Avamar server is forecast to have 90 days or more storage capacity.  Avamar server is forecast to have less than 90 days of storage capacity.  Avamar server is forecast to have less than 30 days of storage capacity. Click a capacity forecast icon to view the Capacity Utilization and Forecast, described in "Detailed utilization and forecasting" on page 362.
Capacity › Data Domain › Used	This column shows summary status of how storage capacity is being used on the configured Data Domain systems. Used status icons communicate the following conditions:  The Data Domain systems have used less than 80% of total storage capacity.  The Data Domain systems have used more than 80% but less than 95% of total storage capacity. Consider adding capacity or deleting old backups.  The Data Domain systems have used more than 95% of total storage capacity. No new backups are taken until you add capacity or delete old backups.[1] Click a capacity forecast icon to view the Capacity Utilization and Forecast, described in "Detailed utilization and forecasting" on page 362.

Table 60 Dashboard page information (page 4 of 4)

Information	Description
Capacity › Data Domain › Forecast	Forecast status icons communicate the following conditions:  The Data Domain systems are forecast to have 90 days or more storage capacity.  The Data Domain systems are forecast to have less than 90 days of storage capacity.  The Data Domain systems are forecast to have less than 30 days of storage capacity. Click a capacity forecast icon to view the Capacity Utilization and Forecast, described in "Detailed utilization and forecasting" on page 362.
Data Protected	This column shows how much data is currently being protected on each Avamar server.
Backups › Status	This column provides a quick overview of scheduled backup status for each Avamar server. Status icons communicate the following conditions:  All scheduled backups successfully completed within the allotted period of time.  One or more scheduled backups successfully completed with exceptions.  One or more scheduled backups did not successfully complete within the allowed period of time. Click a backup status icon to view the Reports page, described in "Reports" on page 345.
Backups › Fail	The number of failed backups. Click a backup status icon to view the Reports page, described in "Reports" on page 345.
Backups › Exceptions	The number of backups that successfully completed with exceptions. Click a backup status icon to view the Reports page, described in "Reports" on page 345.
Backups › Success	The number of backups that completed successfully.

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.

System

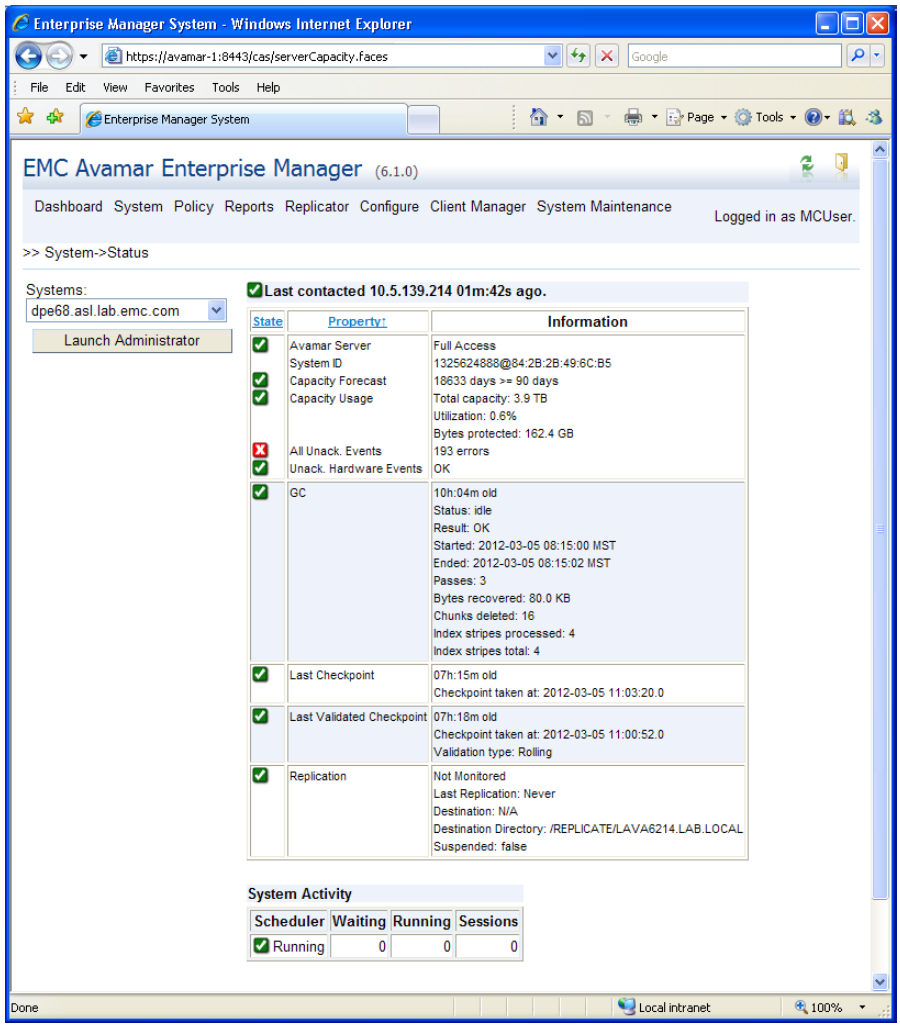
Avamar Enterprise Manager provides two kinds of system information pages:

- Individual system information pages, described in "Individual system information page" on page 335, enable you to view detailed information for a single Avamar server.
- The All systems information (detailed dashboard) page, described in "All servers information (detailed dashboard) page" on page 343, provides a consolidated detailed view of all Avamar servers.

Individual system information page

The individual system information page enables you to view detailed information for a specific Avamar server.

Click a system name on the Dashboard page or select an Avamar server from the Systems list box to view the individual properties page for that server.



Server status

The following table explains server status information.

Table 61 Server status information (page 1 of 6)

Information	Description
Last contacted	Elapsed time since each Avamar server was last contacted by Avamar Enterprise Manager and data was collected. **Note:** If Last updated shows a status other than green, all other information that appears for that server should be considered stale and might not reflect Avamar server status. Status icons communicate the following conditions:  Avamar Enterprise Manager can communicate with and collect data from this Avamar server. The elapsed time since Avamar Enterprise Manager last communicated with this Avamar server is shown next to the status icon.  Last attempt by Avamar Enterprise Manager failed to communicate or collect data from this Avamar server failed. "Dashboard" on page 331 provides additional information about refresh/polling intervals and associated status conditions.  One of the following conditions: – Avamar Enterprise Manager failed to communicate and or collect data from an Avamar server for a specified number of refresh/polling cycles. – Avamar server hostname could not be resolved.[1] – Avamar server login credentials (username or password) were refused.[2] Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.

Table 61 Server status information (page 2 of 6)

Information	Description
Avamar Server	The operational run level for the Avamar server. Status icons communicate the following conditions: Full access. This Avamar server is fully operational. This Avamar server is less than fully operational due to one of the following conditions: **Admin**—Avamar server is fully operational, but only the administrator root account can access the server. **Admin Only**—Avamar server is fully operational, but only the administrator root account can access the server. **Admin Read Only**—Avamar server is in a read-only condition, and only the administrator root account can access the server. **Read Only**—Avamar server is in a read-only condition. Restores are allowed, but no new backups can be performed. **Suspended**—Scheduled backups are disabled and will not occur until you re-enable the scheduler. "Suspending and resuming scheduled operations" on page 313 provides details. **Synchronizing**—Avamar server is priming or synchronizing stripes. This is a temporary condition. Some operations might be delayed. This Avamar server is experiencing one of the following conditions that requires immediate attention: **Inactive**—One or more storage nodes are unresponsive to communication requests from the local MCS (that is, nodes are functioning but frequently timing out on communication requests).[2] **Node Offline**—One or more storage nodes has experienced a problem.[3] **Not available**—Avamar Enterprise Manager cannot obtain any information from this Avamar server. This might indicate communication problems or errors in retrieving data.[2] Ensure that the Last updated status indicator is green. **Unknown State**—Avamar server is in an unknown state. It is either not running or does not respond to communication requests.[2] Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.
System ID	A system identification number for the Avamar server.
Capacity Forecast	Forecast status icons communicate the following conditions: Avamar server is forecast to have 90 days or more storage capacity. Avamar server is forecast to have less than 90 days of storage capacity. Avamar server is forecast to have less than 30 days of storage capacity.

Table 61 Server status information (page 3 of 6)

Information	Description
Capacity Usage	This row shows how much storage capacity is being used on that Avamar server. Detailed information includes: • Total capacity • Capacity used • Total bytes protected Status icons communicate the following conditions: Avamar server has used less than 80% of total storage capacity. Avamar server has used more than 80% but less than 95% of total storage capacity. Consider adding capacity or deleting old backups. Avamar server has used more than 95% of total storage capacity. No new backups are performed until you add capacity or delete old backups.[4]
All Unack. Events	This row shows whether there are any unacknowledged events on the Avamar server. Status icons communicate the following conditions: No warning or error events have occurred on this Avamar server that have not been explicitly acknowledged by an Avamar server administrator. "Acknowledging system events" on page 311 provides details. One or more warning events have been encountered on this Avamar server, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect server operation. One or more serious error events have been encountered on this Avamar server, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.
Unack. Hardware Events	This row shows whether there are any unacknowledged hardware events on the Avamar server. Status icons communicate the following conditions: No hardware warning or error events have occurred on this Avamar server that have not been explicitly acknowledged by an Avamar server administrator. "Acknowledging system events" on page 311 provides details. One or more hardware warning events have been encountered on this Avamar server, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect server operation. One or more serious hardware error events have been encountered on this Avamar server, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. **Note:** An automatic Service Request may already have been opened by the Connect EMC program.
Data Domain Server	The fully qualified domain name of the Data Domain system.

Table 61 Server status information (page 4 of 6)

Information	Description
Status	The overall status of the Data Domain system.  The Data Domain system is fully operational.  The Data Domain system is experiencing problems. However, backups to and restores from the Data Domain system can continue.  The Data Domain system is experiencing problems, and backups and restores will not occur until the problem is resolved. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for details on the available status messages.
Capacity Forecast	Forecast status icons communicate the following conditions:  The Data Domain system is forecast to have 90 days or more storage capacity.  The Data Domain system is forecast to have less than 90 days of storage capacity.  The Data Domain system is forecast to have less than 30 days of storage capacity.
Capacity Usage	This row shows how much storage capacity is being used on the Data Domain system. Detailed information includes: • Total capacity • Capacity used • Total bytes protected Status icons communicate the following conditions:  Less than 80% of total storage capacity is in use on the Data Domain system.  More than 80% but less than 95% of total storage capacity is in use on the Data Domain system. Consider adding capacity or deleting old backups.  More than 95% of total storage capacity is in use on the Data Domain system. No new backups are taken until capacity is added or old backups are deleted.[4]
All Unack. Events	This row shows whether there are any unacknowledged events for the Data Domain system. Status icons communicate the following conditions:  No warning or error events have occurred on this Data Domain system that have not been explicitly acknowledged by an Avamar server administrator. "Acknowledging system events" on page 311 provides details.  One or more warning events have been encountered on this Data Domain system, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect system operation.  One or more serious error events have been encountered on this Data Domain system, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that system operation is not adversely.

Table 61 Server status information (page 5 of 6)

Information	Description
Unack. Hardware Events	This row shows whether there are any unacknowledged hardware events on the Data Domain system. Status icons communicate the following conditions: No hardware warning or error events have occurred on this Data Domain system that have not been explicitly acknowledged by an Avamar server administrator. "Acknowledging system events" on page 311 provides details. One or more hardware warning events have been encountered on this Data Domain system, and these events have not been acknowledged. Review the server logs to ensure that these conditions do not adversely affect system operation. One or more serious hardware error events have been encountered on this Data Domain system, and these events have not been acknowledged. Investigate and remedy any red status condition immediately to ensure that system operation is not adversely affected. Please investigate using https://my.datadomain.com/.
GC	This row shows whether garbage collection (GC) is running or has successfully freed additional storage space on this Avamar server. Detailed information includes: • Started timestamp • Ended timestamp • Number of passes • MB scanned • Bytes recovered • Chunks deleted • Number of index stripes affected • Total number of index stripes scanned Status icons communicate the following conditions: Garbage collection successfully completed on this Avamar server within the past 30 hours. Garbage collection has not successfully completed on this Avamar server within the past 30 hours, possibly due to one of the following conditions: **In progress**—Garbage collection is currently running. **None**—Garbage collection has never successfully completed on this Avamar server. Garbage collection encountered an error the last time it was run. **Note:** Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. [5]

Table 61 Server status information (page 6 of 6)

Information	Description
Last Checkpoint	This row shows whether regularly scheduled checkpoints are successfully completing. The elapsed time since last successful checkpoint and the checkpoint time stamp are shown if at least one successful checkpoint has completed on this Avamar server. "None" indicates that no checkpoints are stored on this Avamar server. "Init" indicates that this is a new Avamar server and that the initial checkpoint has not yet completed. "Checkpoints" on page 404 provides details on checkpoints. Status icons communicate the following conditions: Checkpoint successfully completed on this Avamar server within the past 24 hours. More than 24 hours but less than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server. More than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.
Last Validated Checkpoint	This row shows whether regularly scheduled checkpoint validations are successfully completing on this Avamar server. "None" indicates that no checkpoints have ever successfully been validated on this Avamar server. "Errors" indicates that the last checkpoint validation operation failed. "Not configured" indicates that checkpoint validation is not enabled on this server. Status icons communicate the following conditions: Checkpoint validation successfully completed on this Avamar server within the past 48 hours. More than 48 hours but less than 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server. More than 72 hours have elapsed since a checkpoint validation successfully completed on this Avamar server. Validation type describes the extent of checking performed during the checkpoint. One of the following: **Full**—A full checkpoint (all checks) was performed. **Rolling**—A rolling checkpoint (all new and modified stripes fully validated and a subset of unmodified stripes were validated) was performed.
Replication	This row shows whether regularly scheduled replication is successfully completing on each Avamar server. "Failed" indicates that the last replication operation failed. "Disabled" indicates that the Avamar data replication feature is not enabled on this server. Status icons communicate the following conditions: Replication successfully completed on this Avamar server within the past 48 hours, or the Avamar data replication feature is not enabled on this server. More than 48 hours but less than 72 hours have elapsed since replication successfully completed on this Avamar server. More than 72 hours have elapsed since replication successfully completed on this Avamar server, or the last replication operation failed. Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected. The optional replication management feature is discussed in "Replication" on page 369.

1. Search the knowledgebase at the EMC online support website, https://support.emc.com/products, for solution esg114453.
2. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs.
3. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.
4. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.
5. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg112792.

System activity

The following table explains the System Activity information that appears on the System Status page in Avamar Enterprise Manager.

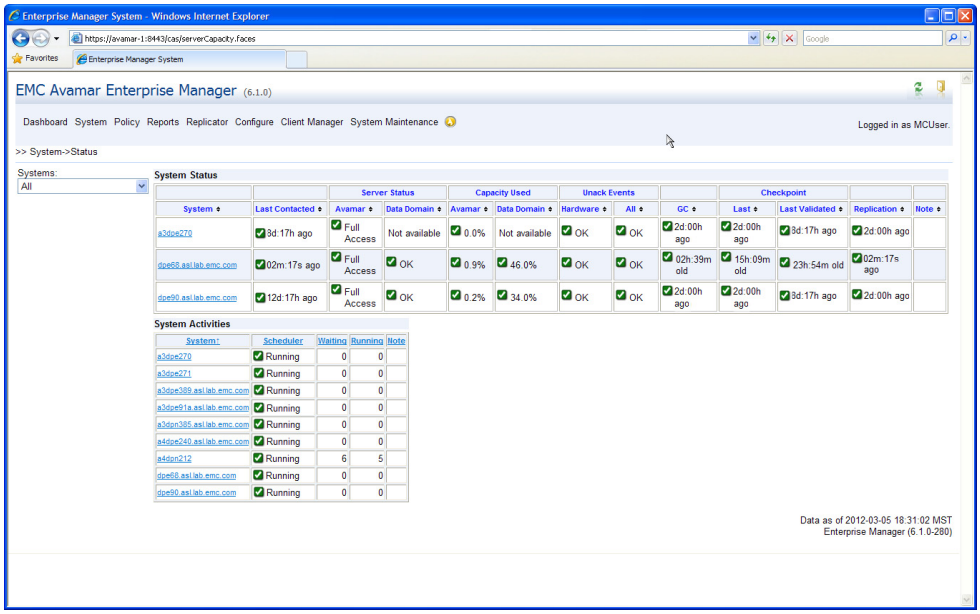
Table 62 System activity information

Information	Description
Scheduler	This column shows whether regularly scheduled server activities (for example, backups, maintenance activities) are enabled for this Avamar server. Status icons communicate the following conditions: Regularly scheduled activities are enabled (resumed) on this Avamar server. Regularly scheduled activities are suspended on this Avamar server. "Suspending and resuming scheduled operations" on page 313 provides details.
Waiting	Number of jobs in the server wait queue.
Running	Number of server jobs that are currently running.
Sessions	Number of active client sessions.

All servers information (detailed dashboard) page

The All systems information page provides a consolidated detailed view of all Avamar server status and information. This page is similar to the dashboard, described in "Dashboard" on page 331, but provides more detailed information.

Select System from any other page, or select All from the Systems list box on an individual system information page, described in "Individual system information page" on page 335, to view the all systems information (detailed dashboard) page.



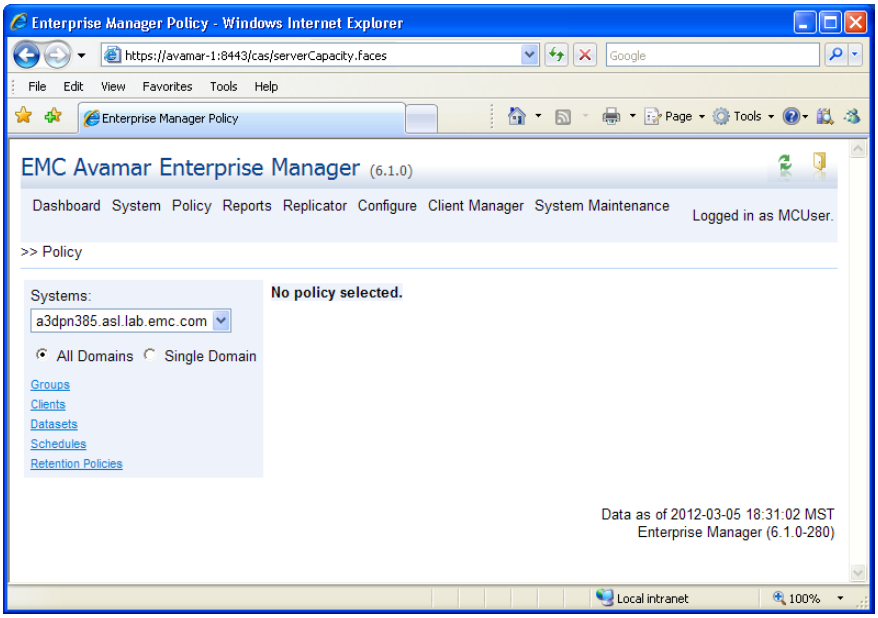
The information is the same as the information that appears for individual servers. "Individual system information page" on page 335 provides additional information.

Capacity

Avamar Enterprise Manager provides advanced capacity forecasting and reporting features that can assist you with monitoring and managing server storage capacity. Chapter 14, "Capacity Management," provides details.

Policy

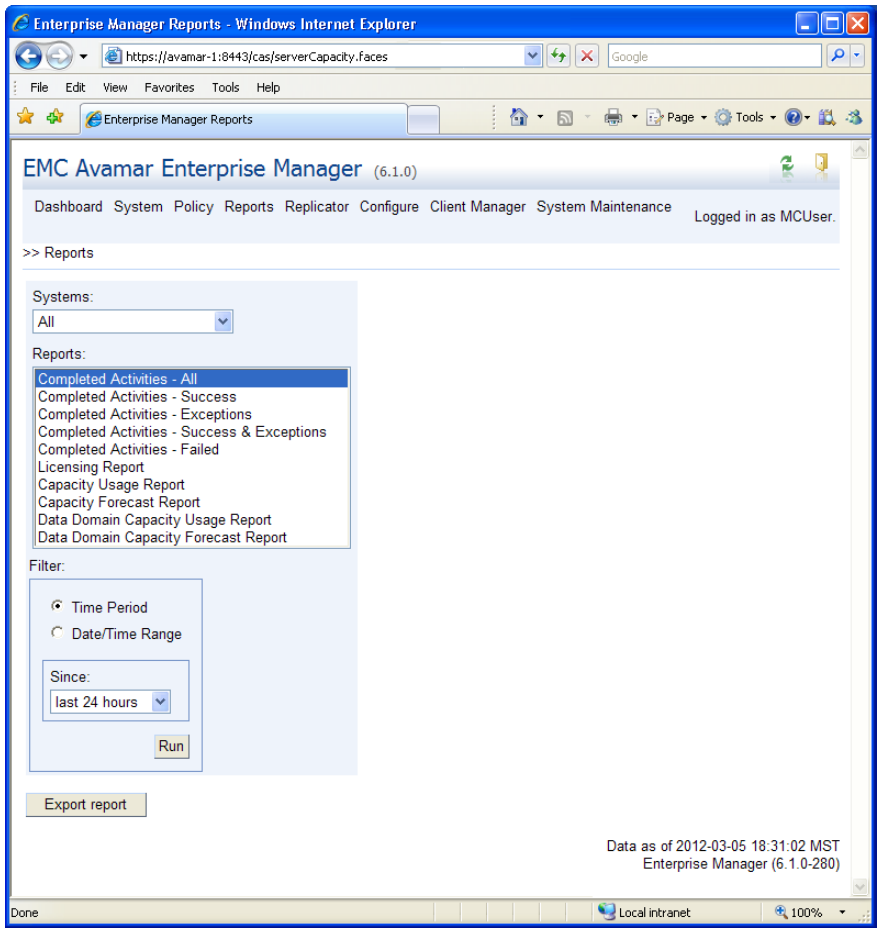
The Policy page lists the various policies in use for each Avamar server that you monitor. Select Policy from any other page to view the Policy page. Chapter 6, "Groups and Group Policies," provides details.



Only one kind of policy object can be shown at a time. Select the kind of policy object to view by selecting Groups, Clients, Datasets, Schedules, or Retention Policies. You can further refine the display by showing policy objects that reside in all domains or a single domain by setting the All Domains or Single Domain options, respectively.

Reports

The Reports page enables you to run various Avamar reports and export that information as a Comma-Separated Values (CSV) text file. Select Reports from any other page to view the Reports page.



"Avamar reports" on page 234 provides details on reports.

The Reports page provides two ways to specify an effective period of time each time a report is run:

- Set the Backup Period option to run a report that shows information for the past day (24 hours), past week, or past two weeks.
- Set the Date/Time Range option to define a specific range of calendar dates and times of day for a report. Only information occurring within that range of dates and times appears in the report.

Running a report

To run a system report:

1. Select a report from the **Reports** list.
2. Specify the time period for the report data using one of the following methods:
   - To include data for the past day (24 hours), past week, or past two weeks, select **Backup Period** and select the length of time from the list.
   - To include data for a range of calendar dates, select **Date/Time Range** and use the **From Date/Time** and **To Date/Time** fields to define the range of calendar dates.

     Click **...** to show a browsable calendar from which you can select a calendar date.
3. Click **Run**.

Exporting a report as a CSV File

To export report information as a CSV file:

1. Run a report as discussed in "Running a report" on page 346.
2. Click **Export this report**.

   NOTICE

   The remainder of this procedure uses Microsoft Internet Explorer 6 with the default security settings as an example. If you use another web browser or other security settings, the steps to perform this procedure might be different.

   The File Download dialog box appears.
3. Click **Save**.

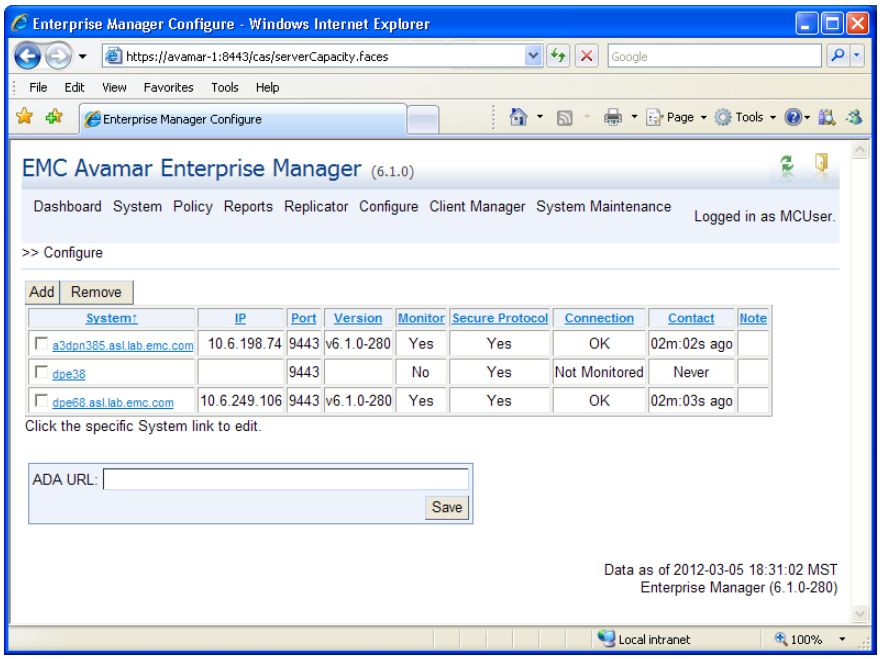
   The Save As dialog box appears.
4. Browse to the appropriate location and click **Save**.

Replicator

Replication is a 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. Chapter 15, "Replication," provides details.

Configure

The Configure page enables you to configure which Avamar systems to monitor.



Select Configure from any other page to view the Configure page.

The Configure page displays the information listed in the following table for each Avamar system that you have added to the Avamar Enterprise Manager configuration.

Table 63 Avamar system column information on the Configure page

Column	Description
System	Avamar server hostname (as defined in corporate DNS).
IP	Avamar server IP address.
Port	Data port used to communicate with this Avamar system.
Version	Specific version of Avamar software that runs on this server.
Monitor	If Yes, this Avamar system is being monitored with Avamar Enterprise Manager. If No, this Avamar system has been added to the Configure page Systems list, but is not being monitored.
Secure Protocol	If Yes, secure HTTPS protocol is used for all connections to this system. If No, unsecure HTTP protocol is used for all connections to this system.
Connection	If OK, connection with this Avamar system is functioning properly.
Contact	Elapsed time since this Avamar server was last contacted by Avamar Enterprise Manager and data was collected.
Note	Optional note or comment.

Client Manager

Client Manager is described in Chapter 19, “Avamar Client Manager.”

System Maintenance

The System Maintenance page enables you to install update and hot fix patches on the Avamar server. Chapter 17, “Server Updates and Hotfixes,” provides more information.

Monitoring other systems

By default, Avamar Enterprise Manager only shows operational status for the Avamar system that is running this instance of the EMS. To manage other Avamar systems in the enterprise, add them to the Avamar Enterprise Manager configuration.

To add an Avamar system to Avamar Enterprise Manager:

1. Open a web browser and log in to Avamar Enterprise Manager.

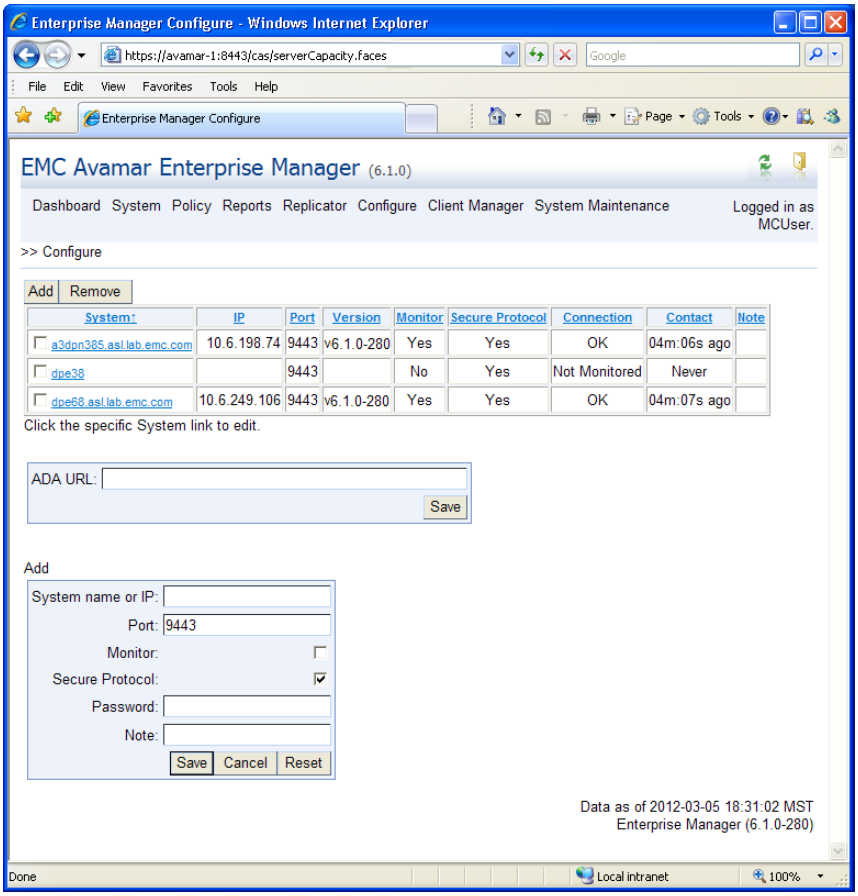
   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.

3. Click **Add**.

An Add block appears below the systems list.



4. In the **System name or IP** box, type the Avamar server hostname (as defined in corporate DNS) or IP address.
5. In the **Port** box, type the port used to communicate with this MCS.
6. To enable monitoring of this system with Avamar Enterprise Manager, select the **Monitor** option.

   Clear this option to add this system to the Configure page Systems list, but not monitor it.
7. To use a Hypertext Transfer Protocol Secure (HTTPS) connection to this server, select the **Secure Protocol** option:

   - If the mcserver.xml sdk_protocol setting is https, select the **Secure Protocol** option.
   - If the mcserver.xml sdk_protocol setting is http, clear the **Secure Protocol** option.

   "Configure MCS web services" on page 352 provides additional information.
8. In the **Password** box, type the Avamar administrative user account password.
9. In the **Note** box, type an optional note or comment.
10. Click **Save**.

Suspending and resuming system monitoring

At some point, you might want to suspend or resume monitoring of one or more Avamar systems. This typically occurs when a system is taken offline and placed back in service at a later date.

To suspend or resume monitoring:

1. Open a web browser and log in to Avamar Enterprise Manager.

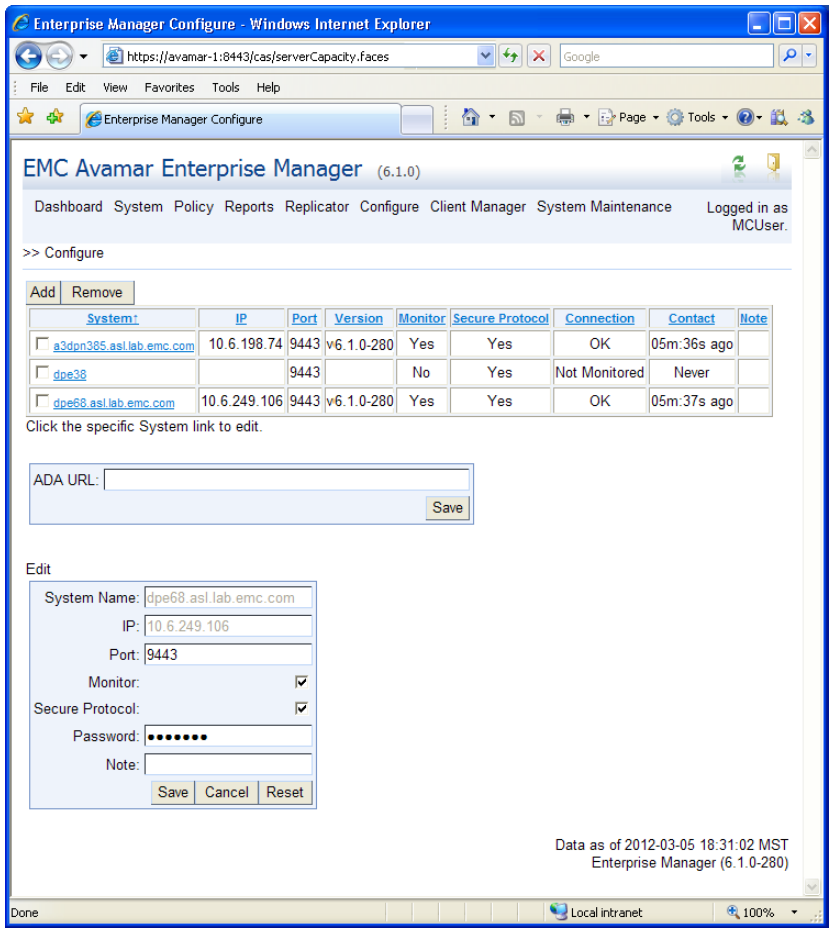
   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.

3. Click the server name.

   An Edit block appears below the systems list.



4. Clear the **Monitor** checkbox to suspend monitoring, or select the checkbox to resume monitoring.

Removing a system from the systems list

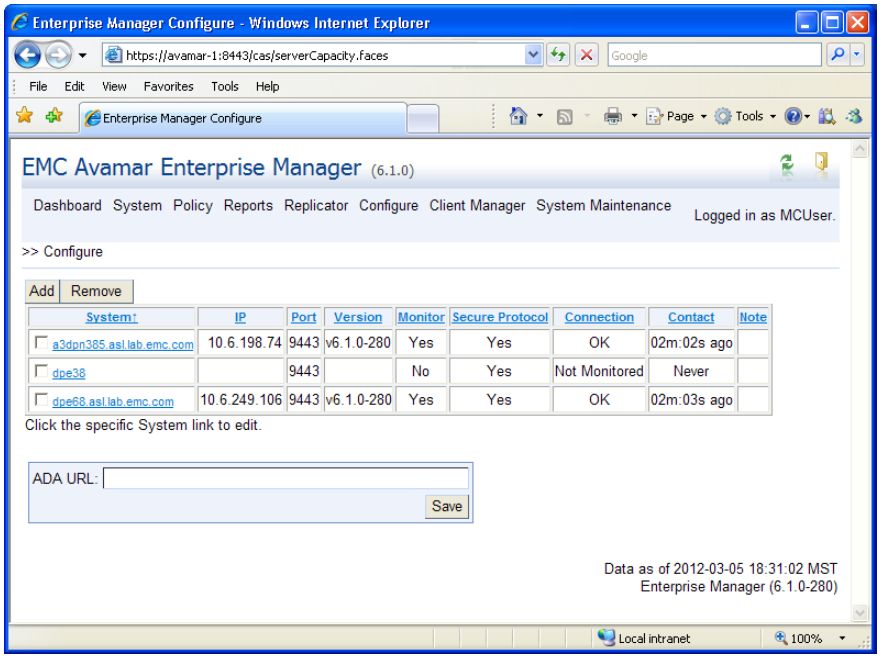
To remove a system from the list:

1. Open a web browser and log in to Avamar Enterprise Manager.

   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.



3. Select the checkbox next to the system.
4. Click **Remove**.

Monitoring Avamar 5.x systems

To monitor Avamar 5.x systems with Avamar Enterprise Manager, enable web services on those systems by performing the following configuration and setup tasks:

- "Obtain and install the server hotfix" on page 352
- "Configure MCS web services" on page 352
- "Add the system to Avamar Enterprise Manager" on page 353

Obtain and install the server hotfix

Obtain Hotfix 19760 for the Avamar server by contacting EMC Customer Support. Follow the instructions in the README file to install the hotfix.

Configure MCS web services

To enable web services, manually change settings in mcserver.xml:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the MCS by typing:

   ```
   dpnctl stop mcs
   ```

3. Open /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml in a UNIX text editor.
4. Locate and change the settings listed in the following table, which are found in com.avamar.mc.mcsdk.

Table 64 MCS web service configuration settings

Setting	Description
axis_home	Location (relative to the Avamar installation directory) where the packaged web application for apache axis2 and MCS web services components are installed. The default location is lib/axis2.war.
sdk_protocol	Specifies whether to use secure (https) or unsecured (http) web protocol. The default setting is secure (https).
sdk_port	Specifies the data port for web services communication. The default setting is data port 9443.
trust_keystore	Location (relative to the Avamar installation directory) of the key store file. The default key store file is lib/rmi_ssi_keystore.
trust_keystore_ap	Key store password.

The *EMC Avamar Product Security Guide* provides additional information about the MCS key store file.

5. Save the changes.
6. Restart the MCS by typing:

```
dpnctl start mcs
```

Add the system to Avamar Enterprise Manager

Add the system you just configured according to the instructions found in "Monitoring other systems" on page 348.

Be sure to set the Secure Protocol as described in the following table.

Table 65 Secure Protocol settings

mcserver.xml sdk_protocol setting	Required Secure Protocol option setting
https	Set the Secure Protocol option.
http	Clear the Secure Protocol option.

Launching Avamar Administrator from Avamar Enterprise Manager

You can launch Avamar Administrator directly from an Avamar Enterprise Manager session.

Avamar Enterprise Manager uses the Java Webstart technology from Sun Microsystems to implement this feature. Webstart is an environment for automatic downloading of the latest version of an application from the Web. By incorporating this technology into Avamar Enterprise Manager, you no longer have to manually install individual versions of Avamar Administrator software to maintain an Avamar system in the enterprise.

NOTICE

Under certain circumstances, stale Java temporary Internet files can cause errors when attempting to launch Avamar Administrator from an Avamar Enterprise Manager session. If this occurs on Windows computers, open the Windows Start menu and select Control Panel › Java. The Java Control Panel appears. In the Temporary Internet Files area, click Delete Files. A confirmation dialog box appears. Ensure that all temporary Internet file types are selected and click OK.

To launch Avamar Administrator from Avamar Enterprise Manager:

1. If you have not already done so, ensure that you are using the correct version Java Web Start Launcher:
   a. From Windows Explorer, select **Tools** › **Folder Options**.

      The Folder Options dialog box appears.

   b. Select the **File Types** tab.
   c. In the **Registered file types** list, select the **JNLP** file type and click **Change**.

      The Open With dialog box appears.

   d. Click **Browse**, then navigate to the directory where Java JRE 1.5.x is installed.
   e. In the bin folder, select **javaws.exe** and click **Open**.

      The Open With dialog box closes.

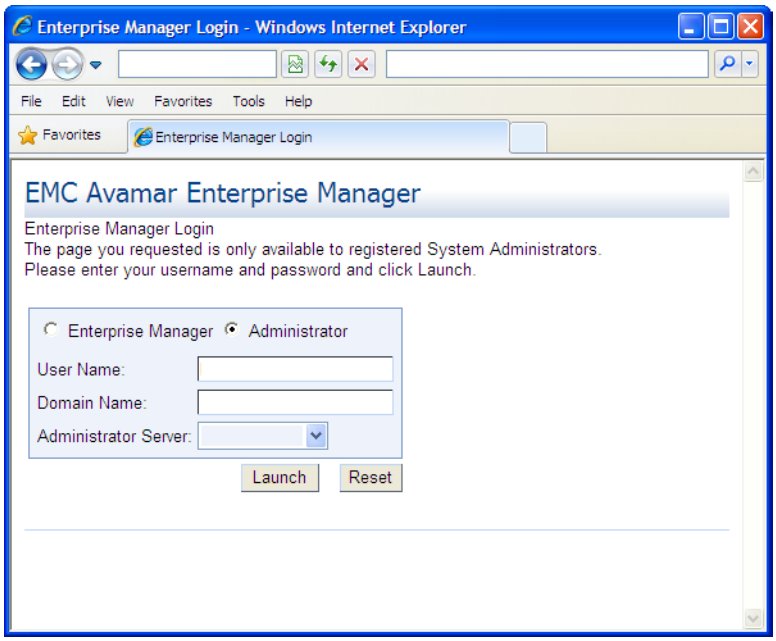
   f. Click **Apply** on the **Folder Options** dialog box.
2. Point a web browser to the following URL:

   `http://AVAMARSERVER/em`

   where AVAMARSERVER is the hostname as defined in DNS.

   The default Enterprise Manager Login page appears.
3. Select the **Administrator** option.

   The Avamar Enterprise Manager Login page for Avamar Administrator downloading appears.



4. In the **User Name** box, type the Avamar administrative user account ID.
5. In the **Domain Name** box, to log in to a domain other than the top-level (root) domain, type the domain path, such as /client/MyDomain.

6. In the **Administrator Server** list, select the system to manage.
7. Click **Launch**.
8. If you do not already have the required Java Runtime Environment (JRE) installed, install it.

   You are redirected to a specific area of the Sun Microsystems website to download and install the correct version of the JRE.

   If this occurs, read and follow the instructions on the Sun Microsystems web page.

   The Java loading... prompt appears.
9. If a **Security Warning** dialog box appears, click **Yes** to proceed with the login.

   The Avamar Administrator login window appears.
10. Type the Avamar administrative user account password in the **Password** text box.
11. Click **Log On**.

    The Administrator dashboard appears.

CHAPTER 14
Capacity Management

Managing server storage capacity is one of the most important aspects of administering an Avamar server. The following topics describe the available features and tools to assist you with properly monitoring and managing server storage capacity:

- Capacity limits and thresholds 358
- Obtaining capacity utilization information 359
- Capacity forecasting 361
- Detailed utilization and forecasting 362
- Customizing capacity limits and behavior 363
- Server and client average daily change rates 366

Capacity limits and thresholds

This following table describes how an Avamar server behaves as it crosses various consumed storage thresholds.

Table 66 Capacity limits and thresholds

Utilization	Status	Description
‹ 75%		When server storage utilization is ‹ 75% of total server storage capacity, the system is considered to have adequate capacity to store future backups. All visual capacity indicators are green.
75%		When server storage utilization reaches 75% of total server storage capacity, all visual capacity indicators turn from green to yellow. This is the level at which system administrators should study server storage utlization to determine if the server has adequate capacity to store future backups.
80%		When server storage utilization reaches 80%, a pop-up notification informs system administrators that the server has consumed 80% of its available storage capacity. This is to further emphasize that server storage utlization should be studied to determine if the server has adequate capacity to store future backups. All visual capacity indicators are yellow.
90%		When server storage utilization reaches 90% of total server storage capacity, all visual capacity indicators turn from yellow to red further emphasize that system administrators should study server storage utlization to determine if the server has adequate capacity to store future backups.
95%		Health check limit. The “health check limit” is the amount of storage capacity that can be utilized and still have a “healthy” server. When server storage utilization reaches the health check limit, backups that are in progress are allowed to complete, but all new backup activity is suspended by the dispatcher. A notification is sent in the form of a pop-up alert when you log in to Avamar Administrator. That system event must be acknowledged before any future backup activity can resume. “Acknowledging system events” on page 311 provides details. The default health check limit is 95%. You can customize this setting as discussed in “Customizing capacity limits and behavior” on page 363. However, setting this limit higher than 95% is not recommended.
100%		Server read-only limit. When server storage utilization reaches 100% of total storage capacity, it automatically becomes read-only. This is done to protect the integrity of the data already stored on the server.[1]

1. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs for the system. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.

Obtaining capacity utilization information

Both Avamar Administrator and Avamar Enterprise Manager provide real-time capacity utilization information.

Avamar Administrator

In Avamar Administrator, capacity utilization information for a single Avamar server is shown two places:

- Dashboard Capacity panel
- Server window Server Management tab

Dashboard capacity panel

The Avamar Administrator dashboard Capacity panel provides system capacity usage and forecasting information for the Avamar server and any Data Domain systems that have been added.

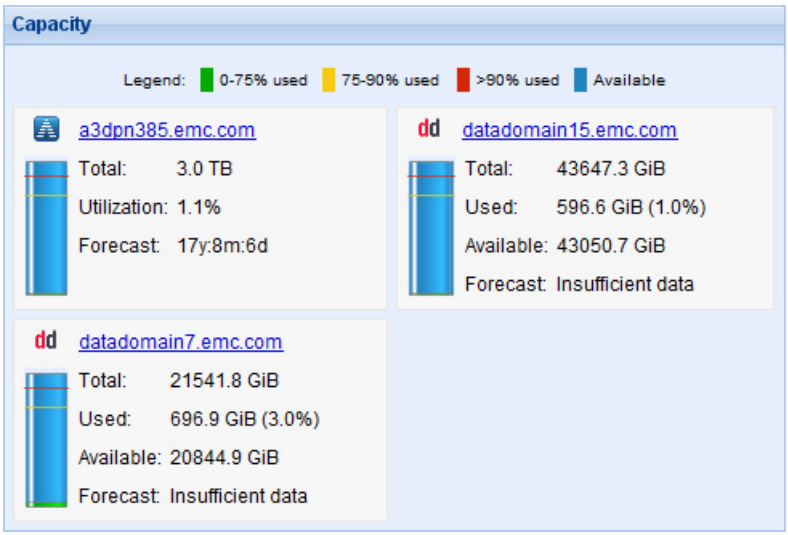


Figure 11 Dashboard Capacity panel

"Capacity panel" on page 46 provides details.

The *EMC Avamar Metadata Capacity Reporting and Monitoring Release 7.0 Technical Note* provides more information about metadata capacity for backups stored on Data Domain systems. This technical note is available from EMC online support (https://support.emc.com).

Server window Server Management tab

The Server window Server Management tab show system capacity usage information for the Avamar server and any Data Domain systems that have been added.

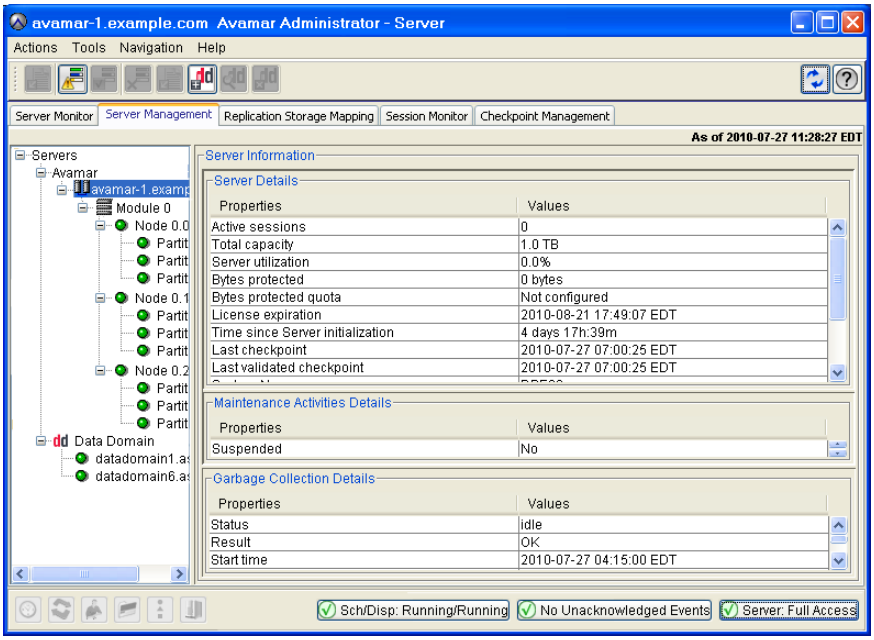
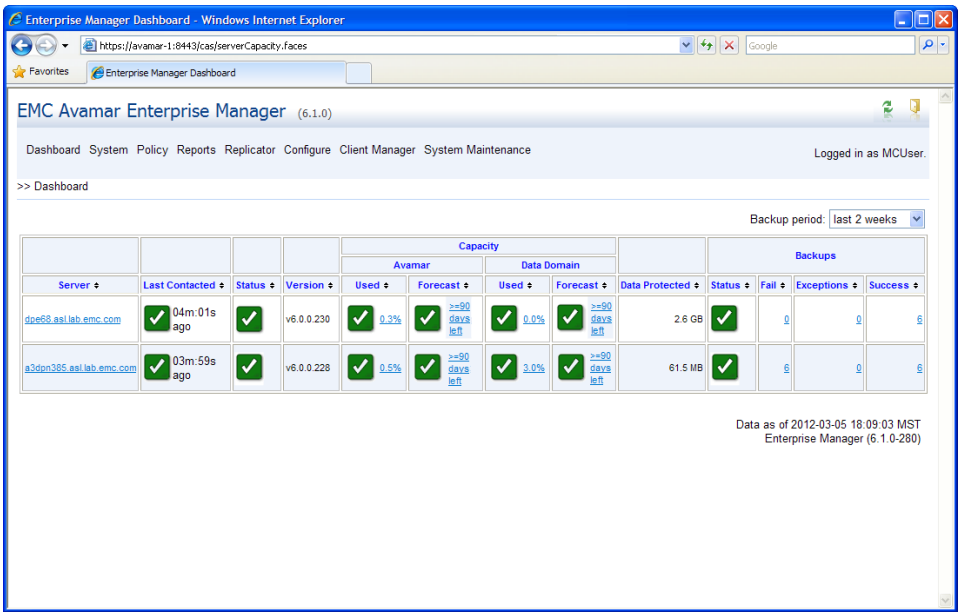


Figure 12 Server window capacity information

"Server Management tab" on page 278 provides details.

Avamar Enterprise Manager

In Avamar Enterprise Manager, consolidated capacity utilization information for all servers being monitored appears in the Dashboard, as shown in the following figure.



The Capacity column shows summary status of how storage capacity is being used on both the Avamar servers and configured Data Domain systems.

There are three possible status icons in the Capacity › Avamar › Used and Capacity › Data Domain › Used columns:

- The Avamar server or Data Domain systems have used less than 75% of total storage capacity.
- The Avamar server or Data Domain systems have used more than 80% but less than 90% of total storage capacity. Consider adding capacity or deleting old backups.
- The Avamar server or Data Domain systems have used 90% or more of total storage capacity. No new backups are allowed until you add capacity or delete old backups.

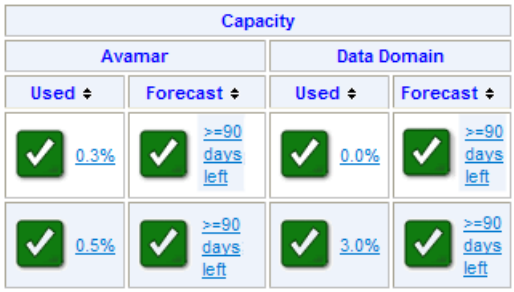
  If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at https://support.emc.com/products to view existing SRs for the system. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578.

Capacity utilization information is also shown on the information page for each server. "Individual system information page" on page 335 provides information about the Avamar Enterprise Manager Server information page.

Capacity forecasting

To help you understand how quickly storage capacity is consumed, each server continuously tracks and analyzes the rate at which storage capacity is consumed, and projects how long you can continue to consume storage capacity at that rate. This forecasting occurs continuously in the background.

The Avamar Enterprise Manager Dashboard, described in "Dashboard" on page 331, shows capacity forecasting results in the Capacity Forecast column for the Avamar server and for configured Data Domain systems, as shown in the following figure.



Capacity Forecast status icons communicate the following:

- The Avamar server or Data Domain systems are forecast to have 90 days or more storage capacity.
- The Avamar server or Data Domain systems are forecast to have less than 90 days of storage capacity.
- The Avamar server or Data Domain systems are forecast to have less than 30 days of storage capacity.

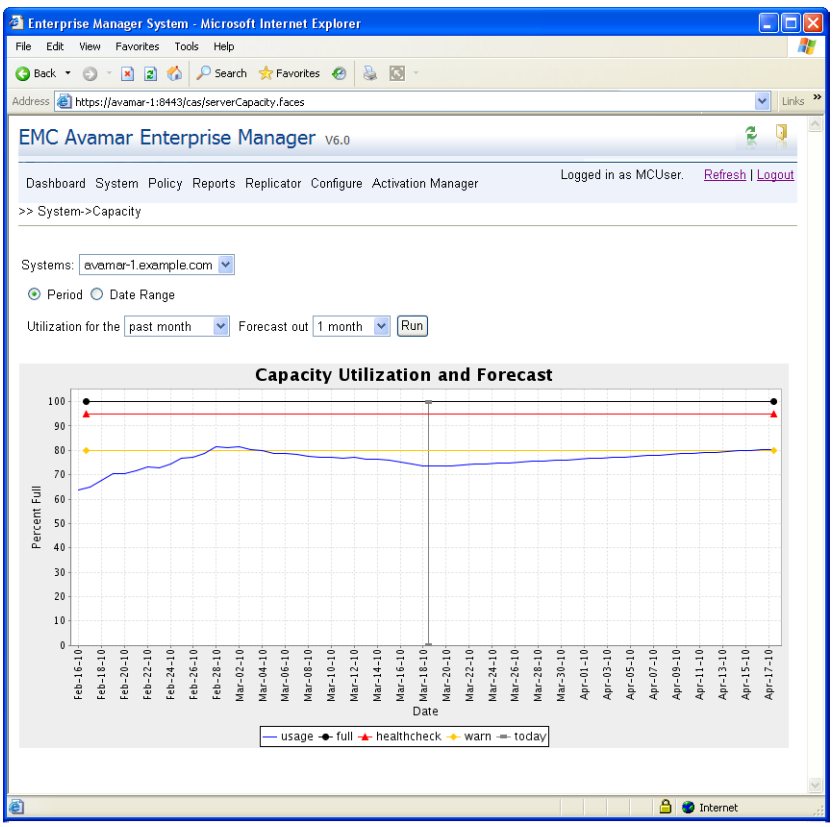
Important limitation regarding capacity data after a rollback

When an Avamar system rollback occurs, the historical capacity graph and report do not have any data from the date of the rollback to the checkpoint date. As a result, the graph shows a flat line and the capacity forecasting information and graph are skewed. In some cases, there is insufficient data to provide any information or graph at all. Forecasting information and graph become more accurate 30 days after the date of rollback.

Detailed utilization and forecasting

Avamar Enterprise Manager also provides graphing capabilities for both capacity utilization (that is, server storage capacity that has already been consumed) and capacity forecasting (that is, server storage capacity that is projected to be used in the future).

Place the mouse cursor over the System menu until a sub-menu appears, and then select Capacity to display the Capacity Utilization and Forecast page, as shown in the following figure.



You can customize the Capacity Utilization and Forecast page:

- **Period** or **Date Range**—If you select Period, menus control how much past utilization information appears. Available time periods are past month, 3 months, 6 months, and 9 months. If you select Date Range, you can type a custom range of dates for which to show capacity utilization.
- **Forecast out**—Capacity forecasting selections are 1 month, 3 months, 6 months, and 9 months in the future.

Customizing capacity limits and behavior

You can customize many of the settings that control capacity limits and behavior by editing one or more application preference files.

Avamar Administrator settings

To customize Avamar Administrator capacity management settings, change one or more of the following preferences in the com.avamar.mc.mcsm section of the /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml preferences file. The preferences are described in the following table.

Table 67 Avamar Administrator capacity management preferences (page 1 of 2)

Preference	Description	Default Setting
capErrPercent	When capacity usage reaches this percentage, the capacity state icon is red.	95%
capForecastDataDays	Amount of historical capacity usage data used for forecasting.	30 days
capForecastDataMinDays	Minimum amount of historical capacity usage data that is required to perform forecasting.	14 days
capForecastReachedDays	When forecasted capacity falls below this number of days, Avamar Administrator begins generating events that require acknowledgement and displaying pop-up alerts at login.	30 days
capMonitorIntervalMin	This setting controls how often the Avamar Administrator checks forecasted capacity.	1 day (daily)
capReachedPercentage	When total capacity utilization reaches this percentage threshold, Avamar Administrator generates an event notification that the system is full.	95%
capWarnPercent	When capacity usage reaches this percentage, the capacity state icon is yellow.	80%

Table 67 Avamar Administrator capacity management preferences (page 2 of 2)

Preference	Description	Default Setting
hcMonitorIntervalMin	This setting controls how often the Avamar Administrator performs a health check (that is, verifies whether consumed capacity has reached the health check limit).	1 day (daily)
hcOffsetROPercentage	Percentage that, when subtracted from the server read-only limit (100%), produces the health check limit.	5%
hcReminderIntervalMin	This setting controls how often the Avamar Administrator issues events and pop-up alerts once the health check limit has been reached.	60 minutes (hourly)

Avamar Enterprise Manager settings

To customize Avamar Enterprise Manager capacity management settings, you can edit one or more of the preferences in the com.avamar.mc.dashboard section of the /usr/local/avamar/var/em/server_data/prefs/emserver.xml preferences file. The preferences are described in the following table.

Table 68 Avamar Enterprise Manager capacity management preferences

Preference	Description	Default Setting
capWarnPercent	When capacity usage reaches this percentage, the capacity state icon is yellow.	80%
capErrPercent	When capacity usage reaches this percentage, the capacity state icon is red.	95%
capForecastWarnDays	When forecasted capacity falls below this number of days, the capacity forecast icon is yellow.	90 days
capForecastErrDays	When forecasted capacity falls below this number of days, the capacity forecast icon is red.	30 days

Updating Avamar application preference files

To update Avamar application preference files:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Shut down the system component:
   - To shut down Avamar Administrator, type:

     ```
     dpnctl stop mcs
     ```

   - To shut down Avamar Enterprise Manager, type:

     ```
     dpnctl stop ems
     ```

3. Open the preferences file in a UNIX text editor:
   - For Avamar Administrator:
     a. Type:

        ```
        cd /usr/local/avamar/var/mc/server_data/prefs
        ```

     b. Open mcserver.xml in a text editor such as vi or Emacs.
   - For Avamar Enterprise Manager:
     a. Type:

        ```
        cd /usr/local/avamar/var/em/server_data/prefs
        ```

     b. Open emserver.xml in a text editor such as vi or Emacs.
4. Save the changes.
5. Restart the system component:
   - To restart Avamar Administrator, type:

     ```
     dpnctl start mcs
     ```

   - To restart Avamar Enterprise Manager, type:

     ```
     dpnctl start ems
     ```

Server and client average daily change rates

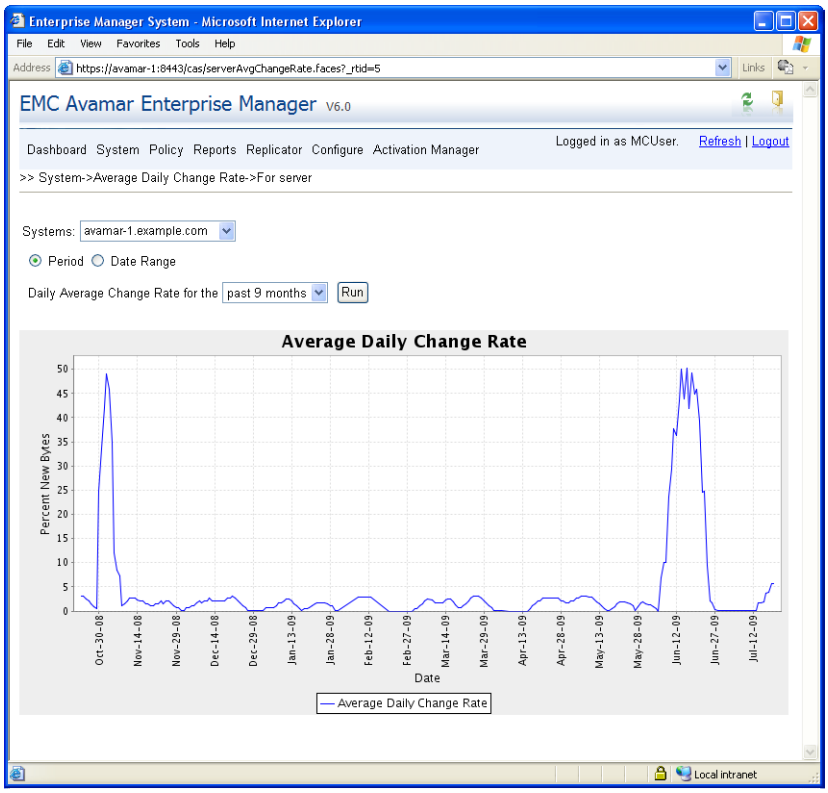
When managing server capacity, it is useful to know the average daily change rate for both the server and for individual clients.

For example, the server average daily change rate can spike upward for a few days immediately after you add several new clients, particularly database clients. This is to be expected. After a few days, data deduplication optimizes server storage efficiency, and the server daily change rate typically returns to normal.

However, if the server average daily change rate remains high for an extended period of time, it might be necessary to determine if this is due to one or more individual clients that might be experiencing less than expected data deduplication efficiencies.

Server data

In Avamar Enterprise Manager, place the mouse cursor over the System menu until a sub-menu appears, and select Average Daily Change Rate › For Server. The Average Daily Change Rate For Server page appears, as shown in the following example.

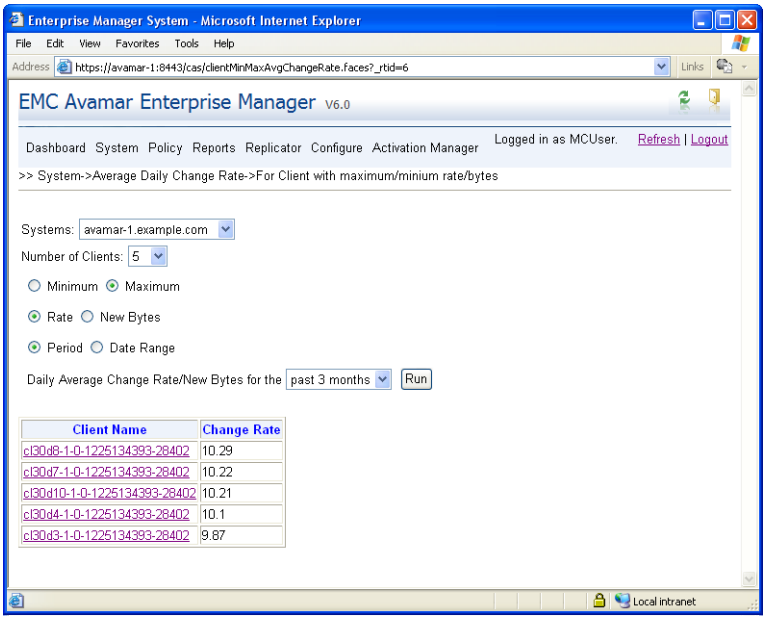


You can control the amount of daily change rate data that appears:

- If you select Period, menus control how much past daily change rate information appear. Available time periods are past month, 3 months, 6 months, and 9 months.
- If you select Date Range, you can select a custom range of dates for which to show server daily change rate data.

Client data

In Avamar Enterprise Manager, place the mouse cursor over the System menu until a sub-menu appears, and select Average Daily Change Rate › For Clients with Maximum/Minimum rate/bytes. The average daily change rate for client with maximum/minimum rate/bytes page appears, as shown in the following example.



You can customize this page as follows:

- **Number of Clients**—Select 5, 10, 20, or 50 clients for which to show daily change rate data.
- **Minimum** or **Maximum**—Select whether to show clients with the most (Maximum) or least (Minimum) daily change rate.
- **Rate** or **New Bytes**—Select whether to customize the display based on the percentage of new data (Rate) or absolute capacity used (New Bytes).
- **Period** or **Date Range**—If you select Period, menus control how much past daily change rate information appears. Available time periods are past month, 3 months, 6 months, and 9 months. If you select Date Range, you can select a custom range of dates for which to show daily change rate data.

Click a client name to display an average daily change rate graph for that client.

CHAPTER 15
Replication

The following topics describe the Avamar replication feature:

- Overview 370
- Limitations 371
- Best practices 371
- Managing replication with Avamar Administrator 373
- Managing cron-based replication with Avamar Administrator 385
- Viewing replication statistics with Avamar Administrator 388
- Managing replication with Avamar Enterprise Manager 389
- Managing replication from the command line 394

Overview

The replication process copies client backups from a source Avamar server to a destination Avamar server. Replication enables you to avoid data loss if the source Avamar server fails because copies of the backups are available on the destination Avamar server.

The REPLICATE domain

On the destination server, replicated backups are available in the REPLICATE domain. This domain contains a mirrored representation of the source server client tree on the destination server.

In the following example figure, a destination server called avamar-1 contains both local clients and replicated backups from the avamar-2 source server.

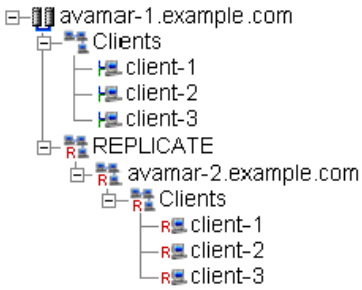


Figure 13 Example replication domain structure

All data in the REPLICATE domain is read-only. You can perform only the following operations on backups in the REPLICATE domain:

- Change the expiration date for a backup
- Validate backups on other clients not in the REPLICATE domain
- View backup statistics
- Delete a backup

You can restore data from clients in the REPLICATE domain to clients in other domains if the source Avamar server fails. EMC Professional Services must perform the redirected restore.

Policy-based versus cron-based replication

Prior to version 7.0, replication was implemented using a cron-based mechanism. Beginning with Avamar 7.0, cron-based replication has been deprecated in favor of a policy-based mechanism that is enabled by default on all new Avamar servers.

Policy-based replication uses special “replication groups,” which store the properties and settings used to schedule and manage replication operations. “Replication groups” on page 374 provides details.

Policy-based replication is the default for Avamar 7.0 and later servers. Existing servers can continue to use the cron-based replication mechanism concurrently with, or instead of policy-based replication

Limitations

The following topics discuss replication limitations.

Only static data is replicated

Each replication operation transfers all static data resident on the source Avamar server. It must be understood that at the time a replication operation is initiated, the replication operation can only process quiescent, or static, data resident on the source server. Therefore, any operation that writes data to the source server and has not fully completed (for example, an in-process backup, adding a user, editing a dataset, and so forth) is, in most cases, not part of that replication operation. However, that data is replicated during the next replication operation.

Avamar Administrator manages only one source server at a time

An important limitation of using Avamar Administrator to manage replication settings is that you are limited to managing one source server at a time. If there is more than one Avamar system in the environment, you may prefer to use the Avamar Enterprise Manager multisystem management console or the EMC Backup & Recovery Manager instead.

Time zones

Be advised that when you schedule replication activities, the start time is displayed in the local time zone, not the source or destination server time zone. For example, consider a situation in which you are in the Pacific time zone and the replication source server is in the Eastern time zone. If you, in the Pacific time zone, set replication to begin at 8 p.m., then the server in the Eastern time zone compensates for the three-hour difference between time zones and starts the replication job at 11 p.m.

Best practices

The following topics discuss best practices for replication.

Avoid source and destination server incompatibilities

Although replication between servers of different versions is supported, for best results, ensure that the destination server has the same or a later version of the Avamar software than the source Avamar server.

Schedule replication during periods of low backup activity

Because only completed client backups are replicated, you should make every effort to schedule replication during periods of low backup activity. This ensures that the greatest number of client backups replicate during each replication session.

Optimize replication group size

When using the policy-based mechanism to manage replication, optimize the size of each replication group so that all clients replicate successfully during each scheduled replication operation. If a group grows to be too large, either modify the schedule to enable more time, or split the group into two smaller groups, which can be independently scheduled.

Use a large timeout setting initially

For cron-based replication, if you specify an optional timeout value during installation and configuration, recent backups might not replicate. This is because the replication process can time out before all backups in the system successfully replicate. The timeout occurs because replication always replicates backups alphabetically by client name, and earliest backups before later backups.

Whenever possible, you should examine a sampling of recent replicated backups on the destination server to ensure that all are being replicated. It is often necessary to increase the optional timeout value during the first few weeks of replication sessions. Eventually, the replication process should normalize. As more data is replicated to the destination server, you can expect greater levels of data deduplication and decreased transfer times. At that time, you can decrease the timeout value.

NOTICE

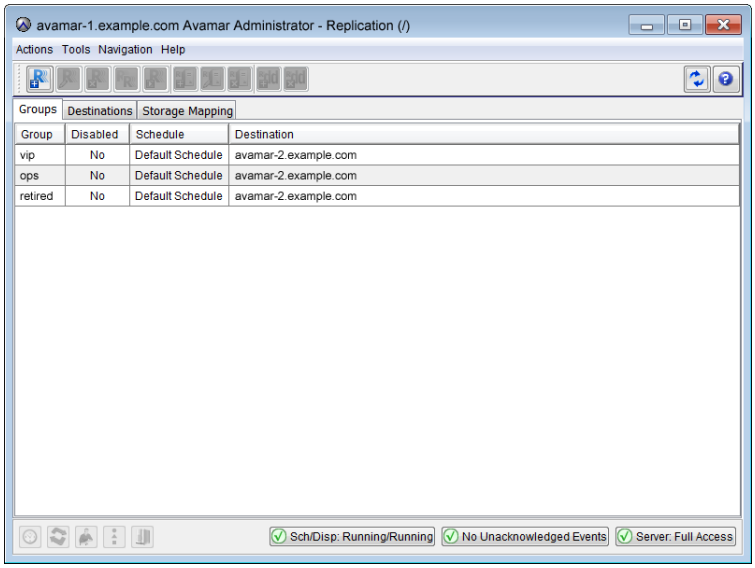
Normal source server background maintenance tasks such as hfscheck and garbage collection should not be performed while a replication session is in progress. Therefore, after you determine that the nightly replication window has normalized, you should optimize the length of the replication window accordingly.

The default cron-based timeout setting is 20 hours (72,000 seconds).

Managing replication with Avamar Administrator

To manage replication with Avamar Administrator, in Avamar Administrator, click the **Replication** launcher button.

The Replication window appears.



The Replication window provides the following capabilities:

- Replication groups:
  - "Adding a replication group" on page 375
  - "Editing a replication group" on page 380
  - "Copying a replication group" on page 381
  - "Enabling or disabling a replication group" on page 381
  - "Deleting a replication group" on page 382
- Destinations:
  - "Adding a destination" on page 382
  - "Editing a destination" on page 384
  - "Deleting a destination" on page 384
- Data Domain storage mappings:

  Refer to the EMC Avamar and EMC Data Domain System Integration Guide for details about mapping a domain and about deleting a domain mapping.

  Note: "Replication" on page 579 provides details about replication of Avamar data on a Data Domain system.

- "Performing an on-demand group replication" on page 384
- "Canceling a replication activity" on page 385

Replication groups

Replication groups are special groups that are only used to implement policy-based replication. Each replication group stores the following information:

- Group members—Which domains and clients are included in each replication operation
- Backup filtering—Which specific backups will be included in each replication operation
- Destination—Which Avamar server will receive the replicated backups, and which connection credentials will be used during each replication operation
- Scheduling—When and how often this group's backups will be replicated
- Retention—How long replicated backups will be retained on the destination server

Replication priority

When you add clients or domains to a replication group, position in the Member(s) list sets priority. Members at the top of the list have higher priority and are replicated first; members at the bottom of the list have lower priority and are replicated last.

Consider the following simplified replication group:

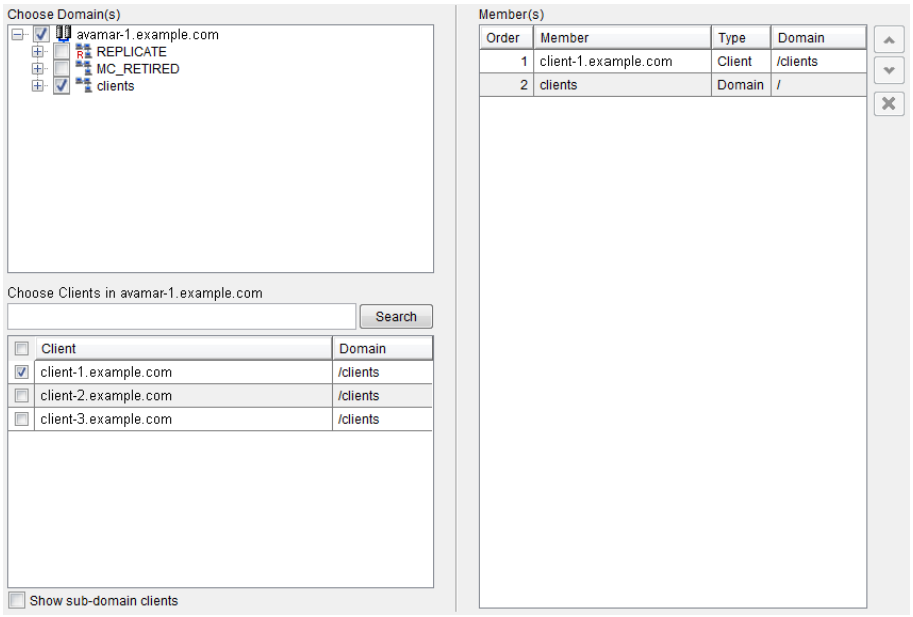


Figure 14 Replication priority example.

Note that client-1 has been added to this replication group as both an individual client and as a member of the Clients domain. Because the individual client entry appears first in the Member(s) list, client-1 has higher priority than the Clients domain. This means that client-1 will be replicated before any other members of the Clients domain.

Futhermore, each time a replication work order is created, duplicate client entries are automatically removed so that each client is only replicated once, even if it is added as both an individual client and a member of a domain.

Adding a replication group

To add a new replication group:

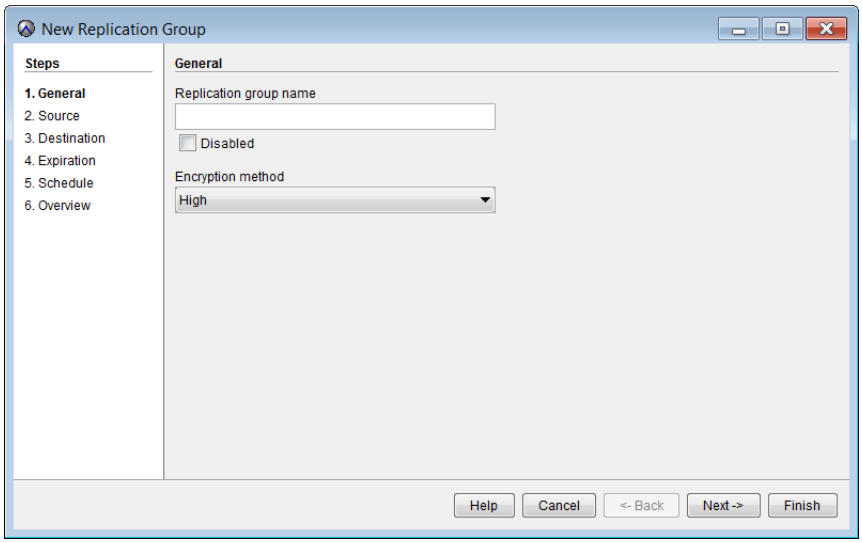
1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Select the **Groups** tab.

3. Select **Actions › New Replication Group**.

   The New Replication Group wizard General settings screen appears.



4. Complete the **General** settings as follows:

   a. Enter a name for this group in the **Replication group name** field.

   b. If you do not want this group to immediately begin replicating backups, select the **Disabled** option.

   c. Select one of the following **Encryption method** settings for source/destination data transfers:

      – **High**—Strongest available encryption setting for that specific destination server.

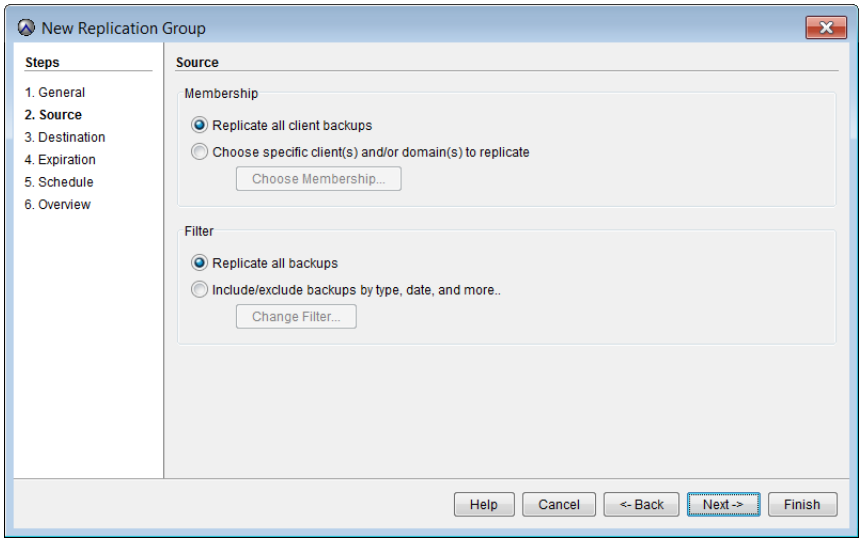
      – **Medium**—Medium strength encryption.

      – **None**—No encryption.

      Note: The exact encryption technology and bit strength used for any given source/destination connection depends on a number of factors, including the server platform and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

5. Click **Next**.

   The New Replication Group wizard Source settings screen appears.



6. Complete the **Source** settings as follows:

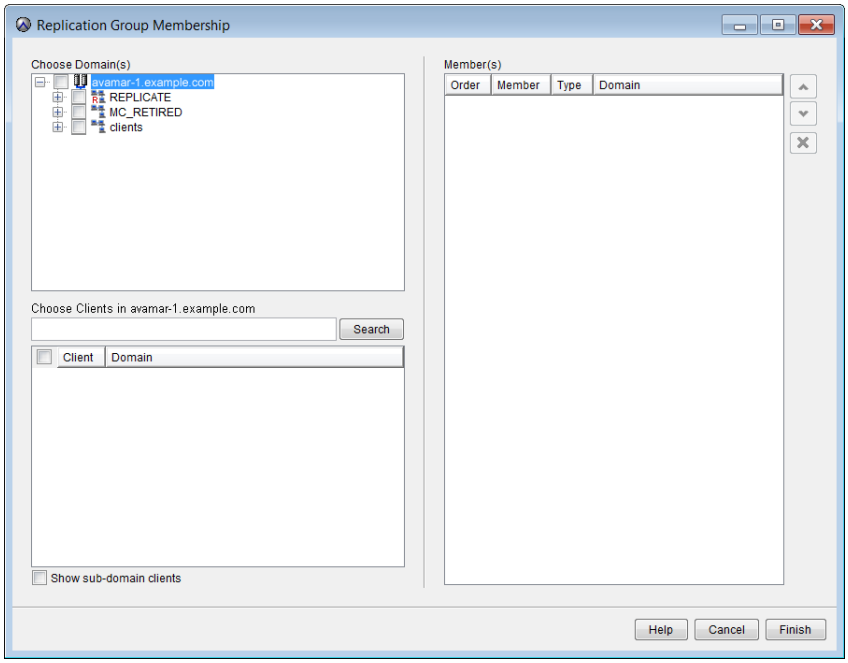
   a. To add all clients to this group, select the **Replicate all client backups** option.

   b. To add specific domains or clients to this group:

      – Select the **Choose specific client(s) and/or domain(s) to replicate** option.

      – Click **Choose Membership**.

        The Replication Group Membership dialog box appears.



c. Complete the **Membership** settings as follows:

   – Select checkboxes next to one or more domains or clients.

     Selections appear in the **Member(s)** list.

   – Set replication priority as necessary by selecting a **Member(s)** list entry and using the up or down arrows to move it higher or lower in the **Member(s)** list. "Replication priority" on page 374 provides details.

   – To remove a member, select that **Member(s)** list entry and click **X**.

   – Click **Finish**.

     The Replication Group Membership dialog box closes.

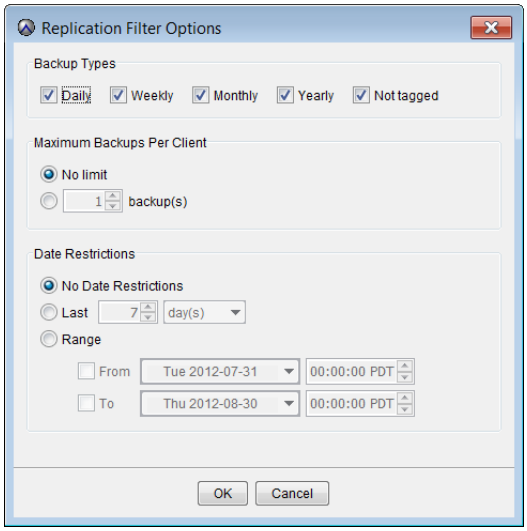
d. To include all backups from all group member clients, select the **Replicate all backups** option.

e. To only replicate certain backups from group member clients:

   – Select the **Include/exclude backups by type, date and more** option.

   – Click **Change Filter**.

     The Replication Filter Options dialog box appears.



   – Select one or more **Backup Types** › **Daily**, **Weekly**, **Monthly**, **Yearly**, or **Not Tagged** checkboxes.

     Note: You must make at least one backup type selection.

   – To replicate all backups for each group member client, select the **Maximum Backups Per Client** › **No Limit** option.

   – To only replicate a specific number of most-recent past group member client backups, specify the maximum number of past **Maximum Backups Per Client** › **backup(s)** to include.

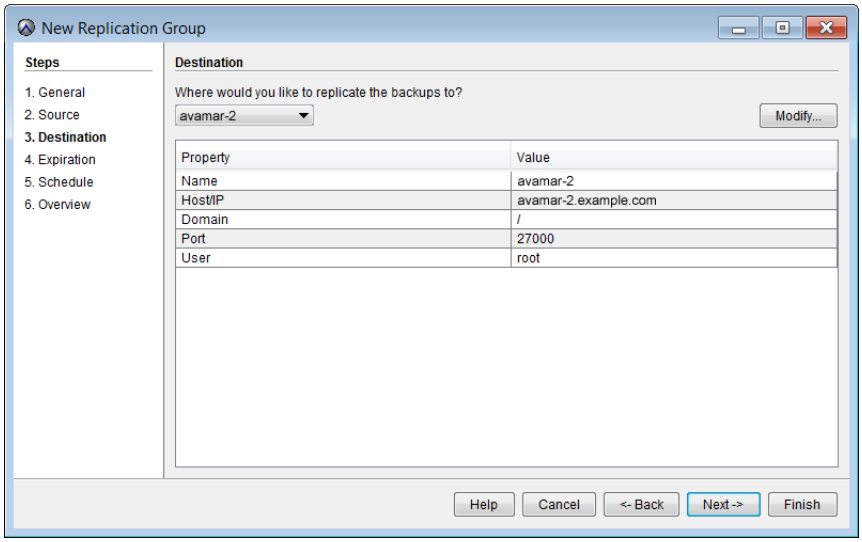
   – To replicate all backups for each group member client regardless of when they were taken, select the **Date Restrictions** › **No Date Restrictions** option.

- To only replicate group member client backups taken within a most recent time period, select the **Date Restrictions** › **Last** option, and specify the number of past **Day(s)**, **Weeks(s)**, **Month(s)**, or **Year(s)** to include.
- To only replicate group member client backups taken within a range of dates, select the **Date Restrictions** › **Range** option, and specify a custom range of dates in the **Before** and **After** fields.
- Click **OK**.

  The Replication Filter Options dialog box closes.

7. Click **Next**.

   The New Replication Group wizard Destination settings screen appears.



8. Complete the **Destination** settings as follows:

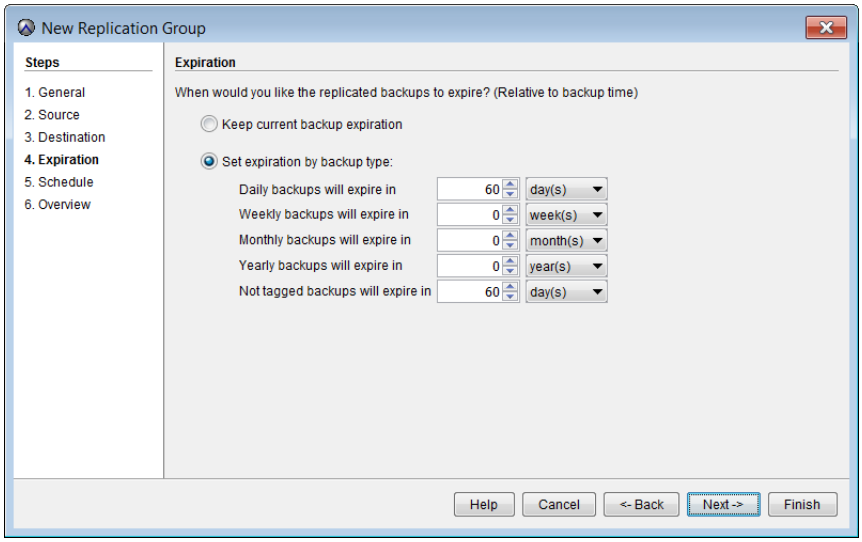
   a. To use an existing destination server, select it from the **Where would you like to replicate backups to?** list.

   b. To create a new destination server, select **New Destination** from the **Where would you like to replicate backups to?** list, then follow the instructions described in "Adding a destination" on page 382.

   c. To edit an existing destination's settings, select it from the **Where would you like to replicate backups to?** list, click **Modify**, then follow the instructions described in "Editing a destination" on page 384.

9. Click **Next**.

   The New Replication Group wizard Expiration settings screen appears.



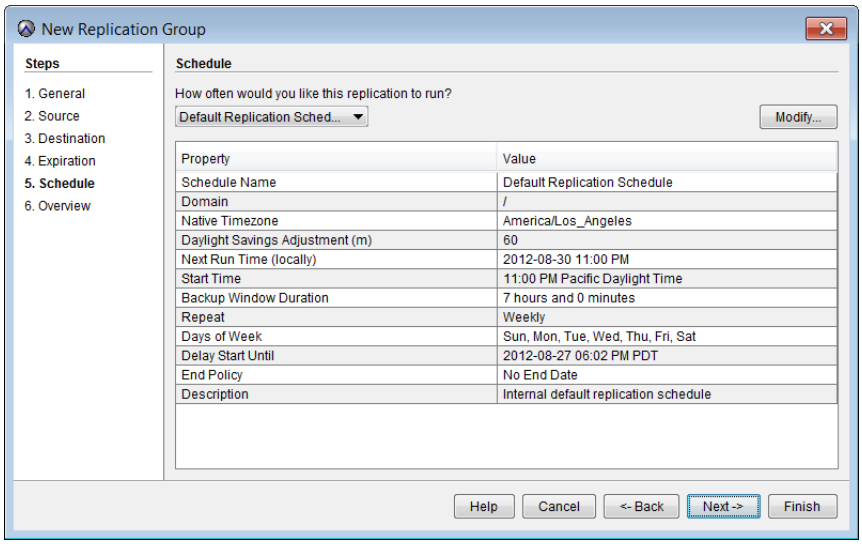
10. Complete the **Expiration** settings as follows:

    a. To keep each replicated backup's current expiration setting, select the **Keep current backup expiration** option.

    b. To specify custom expiration settings for each backup type, select the **Set expiration by backup type** option, then specify the number of days, weeks, months or years to retain each backup type.

11. Click **Next**.

    The New Replication Group wizard Schedule settings screen appears.



12. Complete the **Schedule** settings as follows:

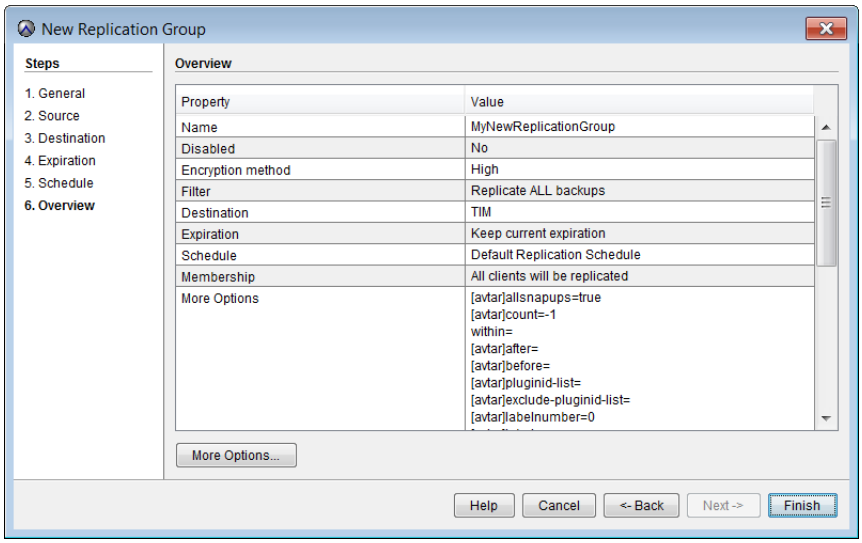
    a. To use an existing schedule, select it from the **How often would you like this replication to run?** list.

    b. To create a new schedule, select **New Schedule** from the **How often would you like this replication to run?** list, then follow the instructions described in "Creating a schedule" on page 136.

    c. To edit an existing schedule's settings, select it from the **How often would you like this replication to run?** list, click **Modify**, then follow the instructions described in "Editing a schedule" on page 142.

13. Click **Next**.

    The New Replication Group wizard Overview screen appears.



14. Review your settings.

15. (Optional) To include additional plug-in options for use with this replication group, click **More Options**, then configure them as described in "How to set plug-in options" on page 594.

16. Click **Finish**.

    The New Replication Group wizard closes, and the new replication group appears in the Replication window Groups tab.

Editing a replication group

To edit an existing replication group:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Select the **Groups** tab.

3. Select a group.

4. Select **Actions › Edit Replication Group**.

   The Edit Replication Group wizard appears.

5. Edit the replication group properties and settings.

   "Adding a replication group" on page 375 provides details about replication group properties and settings.

6. Click **OK**.

Copying a replication group

To copy an existing replication group:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Select the **Groups** tab.
3. Select a group.
4. Select **Actions › Copy Replication Group**.

   The Save As dialog box appears.

5. Type a name for the new group.

   The **Domain** field is read-only and contains the current domain.

6. Select the **Include Client Members** option to copy the entire client list to this new group.
7. Click **OK**.

Enabling or disabling a replication group

You can disable a replication group to prevent scheduled replications from occurring for that group. This is typically done to place the system in a state that supports various maintenance activities. If you disable a replication group, you must re-enable the group to resume scheduled replications.

To disable or enable a group:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Select the **Groups** tab.
3. Do one of the following:

   - To enable a replication group, select a disabled replication group, then select **Actions › Disable Replication Group**.

     The checkmark next to the **Actions › Disable Replication Group** command is cleared.

   - To disable a replication group, select an enabled replication group, then select **Actions › Disable Replication Group**.

     A checkmark appears next to the **Actions › Disable Replication Group** command.

   A confirmation message appears.

4. Click **Yes**.

Deleting a replication group

To delete an existing replication group:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.
2. Select the **Groups** tab.
3. Select a group.
4. Select **Actions › Delete Replication Group**.

   A confirmation message appears.
5. Click **Yes**.

Destinations

Destinations store the properties and settings necessary to communicate with another Avamar server. Each destination stores the following information:

- Server hostname or IP address
- User-defined common name (alias) for that server
- Data port used to communicate with that server
- Username and password used to authenticate with that server

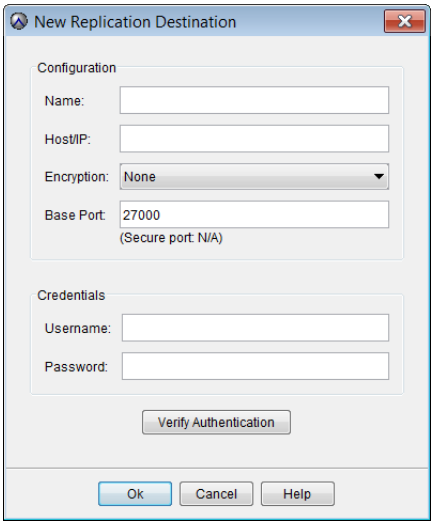
Adding a destination

To add a new replication destination:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.
2. Select the **Destinations** tab.
3. Select **Actions › New Destination**.

   The New Replication Destination dialog box appears.



4. Complete the following **Configuration** settings:
   a. Enter a short common name in the **Alias** field.
   b. Enter the destination server hostname or IP address in the **Host/IP** field.
   c. Select one of the following **Encryption** settings for replication data transfers:
      – **High**—Strongest available encryption.
      – **Medium**—Medium strength encryption.
      – **None**—No encryption.
   d. Enter the data port used to communicate with the destination server in the **Base Port** field.

      27000 is the default data port for Avamar client-server communications. You should leave this set to 27000 unless you have changed the Avamar client-server communication port setting on the destination server.

      If **High** or **Medium** encryption is selected in step c, an offset is applied to this base data port in order to facilitate connections through fire walls. The default offset is +2000. However, this offset can be changed to another value by manually editing the secured_port_offset preference in mcserver.xml, then restarting the MCS.
5. Complete the following **Credentials** settings:
   a. Enter a valid Avamar user account name in the **Username** field.
   b. Enter the password for the Avamar user account name in the **Password** field.
6. Click **Verify Authentication** to verify that the settings you have just entered will successfully authenticate with the destination server.

   A message appears notifying you that the authentication attempt either succeeded or failed.
7. Click **OK** to dismiss the message.
8. Do one of the following:
   - If authentication verification failed, repeat steps 4—7 until authentication verification succeeds.
   - If authentication verification succeeded, click **Save**.

Editing a destination

To edit an existing replication destination:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Click the **Destinations** tab.
3. Select **Actions › Edit Destination**.

   The Replication Destination dialog box appears.

4. Edit the destination properties and settings.

   "Adding a destination" on page 382 provides details about destination properties and settings.

5. Click **Save**.

Deleting a destination

To delete an existing replication destination:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Select the **Destinations** tab.
3. Select **Actions › Delete Destination**.

   A confirmation message appears.

4. Click **Yes**.

Performing an on-demand group replication

You can also initiate on-demand group and client replications from the Policy window. "Perfoming on-demand group and client replications" on page 188 provides details.

To initiate an on-demand group replication from Replication window:

1. In Avamar Administrator, click the **Replication** launcher button.

   The Replication window appears.

2. Click the **Groups** tab.
3. Select a group.
4. Select **Actions › Replicate Now**.

   The On-Demand Replication Request dialog box appears showing that a replication request has been initiated.

5. Click **Close**.

Canceling a replication activity

You can cancel a replication activity any time before it completes. However, it can take as long as five minutes to complete the cancellation. If the activity completes during this time, the cancellation does not occur.

To cancel a replication activity:

1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.

2. Click the **Activity Monitor** tab.

   The most recent 5,000 client activities during the past 72 hours appear on the Activity Monitor tab.

3. Select one or more activities to cancel.

4. Select **Actions** › **Cancel Activity**.

   A confirmation message appears.

5. Click **Yes**.

Managing cron-based replication with Avamar Administrator

Prior to version 7.0, replication was cron-based. Beginning with Avamar 7.0, cron-based replication has been deprecated in favor of a policy-based mechanism, as described in "Managing replication with Avamar Administrator" on page 373.

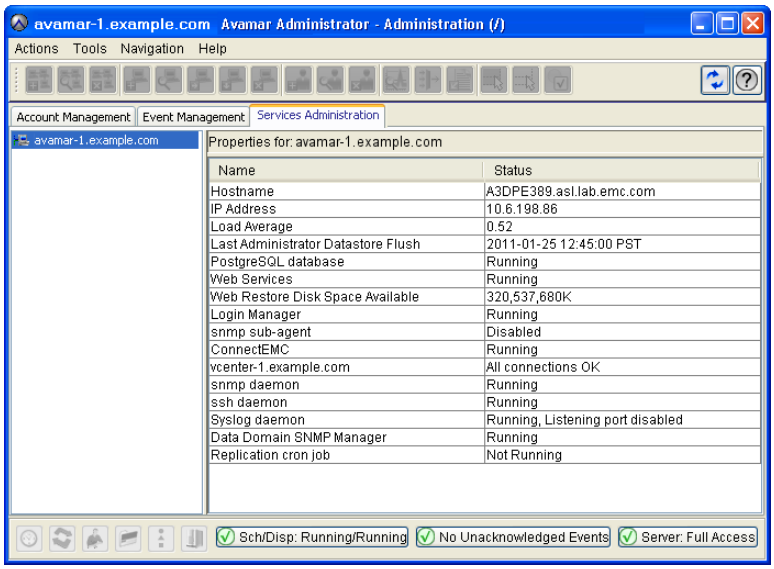
Older Avamar servers can continue to use the cron-based replication mechanism concurrently with policy-based replication.

To manage replication with Avamar Administrator:

1. In Avamar Administrator, click the **Administration** launcher button.

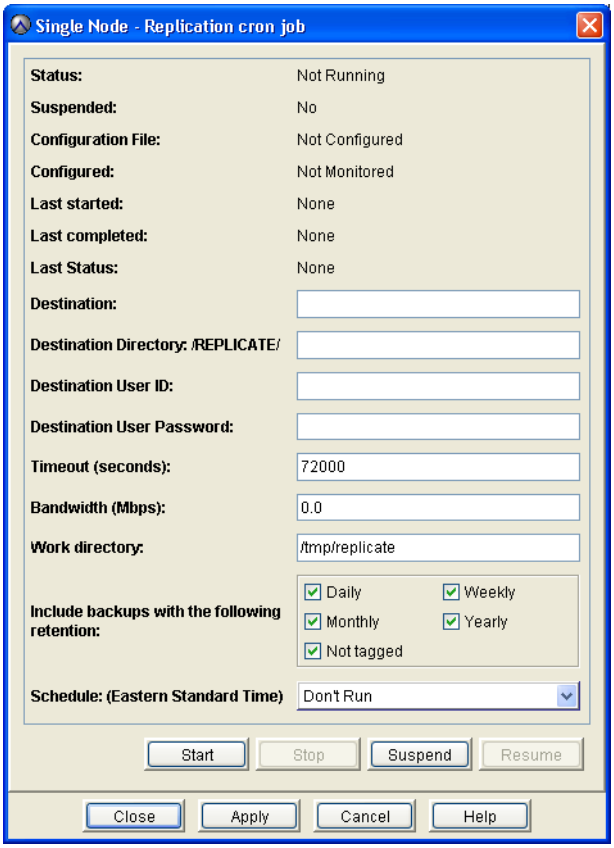
   The Administration window appears.

2. Click the **Services Administration** tab.



3. Double-click the **Replication cron job** entry in the properties table.

   The Replication cron job dialog box appears.



   The Replication cron job dialog box displays the information described in the following table.

Table 69 Replication cron job information (page 1 of 2)

Field	Description
Status	Current replication status. One of the following: • Running—Scheduled replication operations are occurring normally. • Not Running—Scheduled replication operations are not occurring normally. • Not Running, Suspended—Scheduled replication operations are not occurring normally, and replication operations will not occur until replication resumes on this Avamar server. • Running, Suspended—Replication operations were suspended while a replication job was running. When operations are resumed, this job will also resume from where it left off.
Suspended	Indicates whether scheduled replication operations have been started (No) or stopped (Yes).
Configuration File	Location of the repl_cron.cfg configuration file, which stores replication settings for this Avamar system.
Configured	Indicates whether scheduled replication is configured on this source Avamar server.

Table 69 Replication cron job information (page 2 of 2)

Field	Description
Last started	Start time of the last replication operation.
Last completed	Elapsed time since last replication operation completed.
Last Status	Status of the last completed replication operation. One of the following: • None—Status for last replication operation is not available. • Success—Last replication operation successfully completed. • Failed—One or more errors were encountered during the last replication operation. **Note:** In addition to viewing overall replication job status, you can view replication status on a client-by-client basis in the Activity window. "Monitoring backup, restore, or validation activities" on page 116 provides details.

4. In the **Destination** box, specify the destination Avamar server hostname (as defined in corporate DNS).
5. In the **Destination Directory: /REPLICATE/** box, specify the destination directory on the destination Avamar server.

   The default location is /REPLICATE/SOURCE, where SOURCE is the source Avamar server hostname that you selected in the systems list. You can edit the destination. However, the destination must always exist under the /REPLICATE domain.
6. In the **Destination User ID** box, specify the Avamar administrative user account ID (replonly) that is used to log in to the destination Avamar server.
7. In the **Destination User Password** box, specify the password for the Avamar administrative user account ID (replonly).

   NOTICE

   If you change the password for the replonly account on the target server, then remember to update the Destination User Password value in the replication configuration on the source server with the new password.
8. In the **Timeout (seconds)** box, specify the maximum length of time that each replication operation should run.
9. In the **Bandwidth (Mbps)** box, specify the network utilization throttling setting that specifies the maximum average network utilization 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.
10. In the **Work directory** box, specify the full path to the temporary folder or directory that is used to store replication log files.
11. (Optional) To limit the replication operation to only backups that have been assigned a specific retention type, select the checkbox next to the retention type in the **Include backups with the following retention** section.

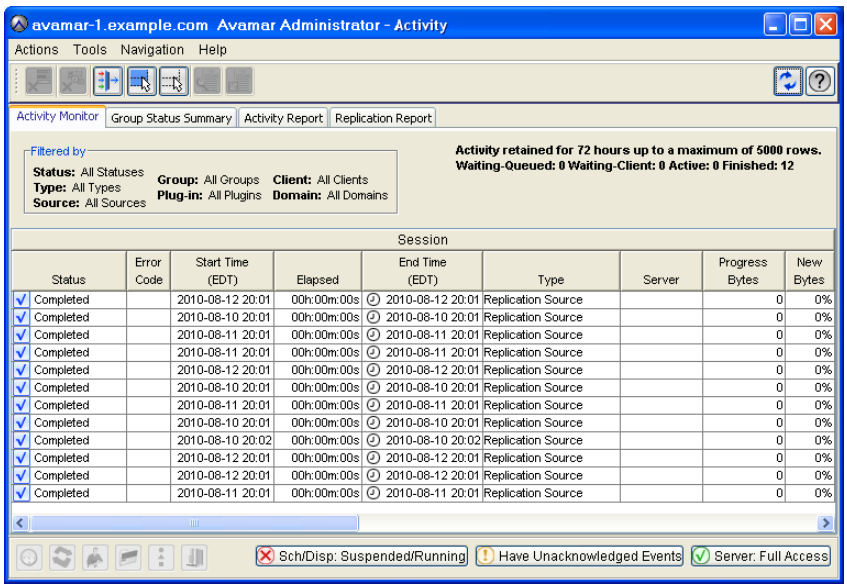
12. From the **Schedule** list, select the time of day at which to initiate replication, or select **Don't Run** to temporarily suspend replication.
13. Click **OK**.

Viewing replication statistics with Avamar Administrator

To view replication statistics with Avamar Administrator:

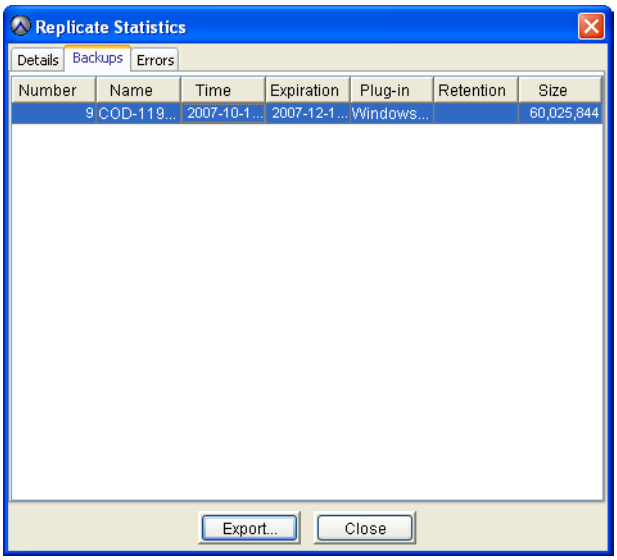
1. In Avamar Administrator, click the **Activity** launcher button.

   The Activity window appears.



2. Click the **Activity Monitor** tab.
3. Select a Replication Source or Replication Destination activity and select **Actions › View Statistics**.

   The Replicate Statistics dialog box appears.



The following tabs appear on the Replicate Statistics dialog box:

- **Details**—Shows detailed information from the v_repl_activities database view, as discussed in "v_repl_activities" on page 633.
- **Backups**—Shows a list of backups included in this replication operation.
- **Errors**—Shows any errors that occurred during this replication operation.

4. Click **Close**.

Managing replication with Avamar Enterprise Manager

Unlike the Avamar Administrator replication management feature, which is inherently constrained to managing replication settings for only one source Avamar server at a time, the Avamar Enterprise Manager replication management feature can manage replication for multiple Avamar servers.

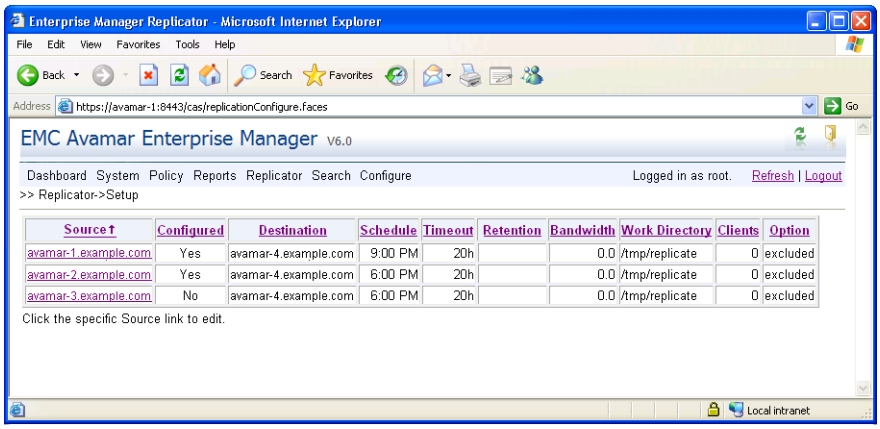
The following table describes the Avamar Enterprise Manager replication management pages

Table 70 Avamar Enterprise Manager replication management

Page	Purpose	Steps to open
Replicator Status	Shows status for replication operations	Place the mouse cursor over the Replicator menu until a sub-menu appears, and then select Status.
Replicator Setup	Used to configure replication	Place the mouse cursor over the Replicator menu until a sub-menu appears, and then select Setup.

Replicator setup page

The Replicator Setup page, shown in the following figure, is used to manage replication settings for the Avamar systems in the Avamar Enterprise Manager configuration.



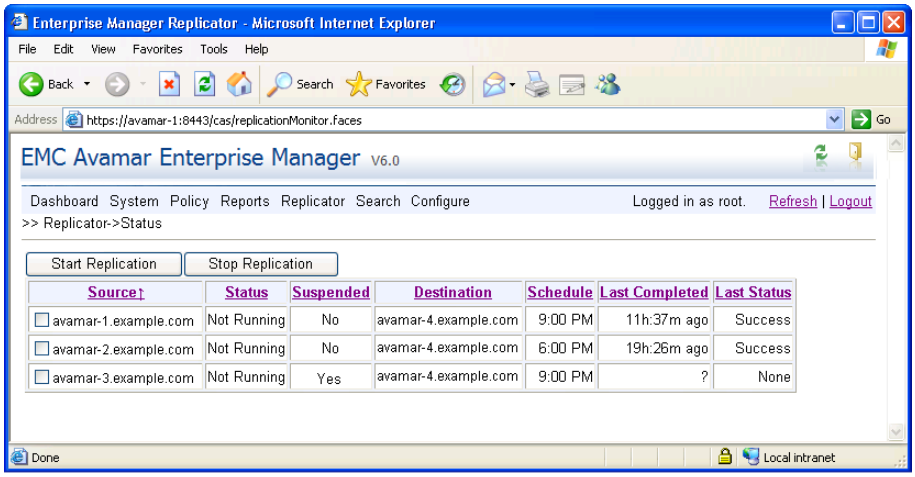
The following table lists the information that appears on the Replicator Setup page for each Avamar system in the Avamar Enterprise Manager configuration.

Table 71 Replicator setup for Avamar systems

Column	Description
Source	Source Avamar server hostname (as defined in corporate DNS).
Configured	Indicates whether the source Avamar server has been configured and enabled for replication. One of the following: • Not Monitored—This Avamar system is currently not being monitored by Avamar Enterprise Manager. To use the Avamar Enterprise Manager replication management feature on this system, enable or resume monitoring as discussed in "Suspending and resuming system monitoring" on page 350. • No—This Avamar system is not currently configured and enabled for replication operations. "Configuring or modifying replication settings" on page 392 provides information. • Yes—This Avamar system is configured and enabled for replication operations.
Destination	Destination Avamar server hostname (as defined in corporate DNS).
Schedule	Hour of the day that replication is scheduled to occur, or Don't Run if replication is temporarily suspended.
Timeout	Maximum length of time that replication activity is allowed to run.
Retention	Shows the retention types of the backups to replicate.
Bandwidth	Network utilization throttling setting. This setting specifies the maximum average network utilization 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.
Work Directory	Temporary folder or directory used to store replication log files.
Clients	Number of clients that have been explicitly included or excluded.
Option	True if clients are included. Otherwise, clients are excluded.

Replicator status page

The Replicator Status page shows consolidated daily replication status for each Avamar system in the Avamar Enterprise Manager configuration.



The following table lists the information that appears on the Replicator Status page for each Avamar system.

Table 72 Replicator status for Avamar systems

Column	Description
Source	Source Avamar server hostname (as defined in corporate DNS).
Status	Current replication status. One of the following: • Running—Scheduled replication operations are occurring normally. • Not Running—Scheduled replication operations are not occurring normally. • Not Running and Suspended—Scheduled replication operations are occurring normally, and no future replication operations will occur until replication resumes on this Avamar server.
Suspended	Indicates whether scheduled replication operations have been started (No) or stopped (Yes).
Destination	Destination Avamar server hostname (as defined in corporate DNS).
Schedule	Hour of the day that replication is scheduled to occur, or Don't Run if replication is temporarily suspended.
Last Completed	Elapsed time since the last replication operation completed.
Last Status	Status of the last completed replication operation. One of the following: • None—Status for the last replication operation is not available. • Success—The last replication operation successfully completed. • Failed—One or more errors were encountered during the last replication operation.

Configuring or modifying replication settings

To use Avamar Enterprise Manager to configure replication settings for an Avamar system:

1. Open a web browser and log in to Avamar Enterprise Manager.

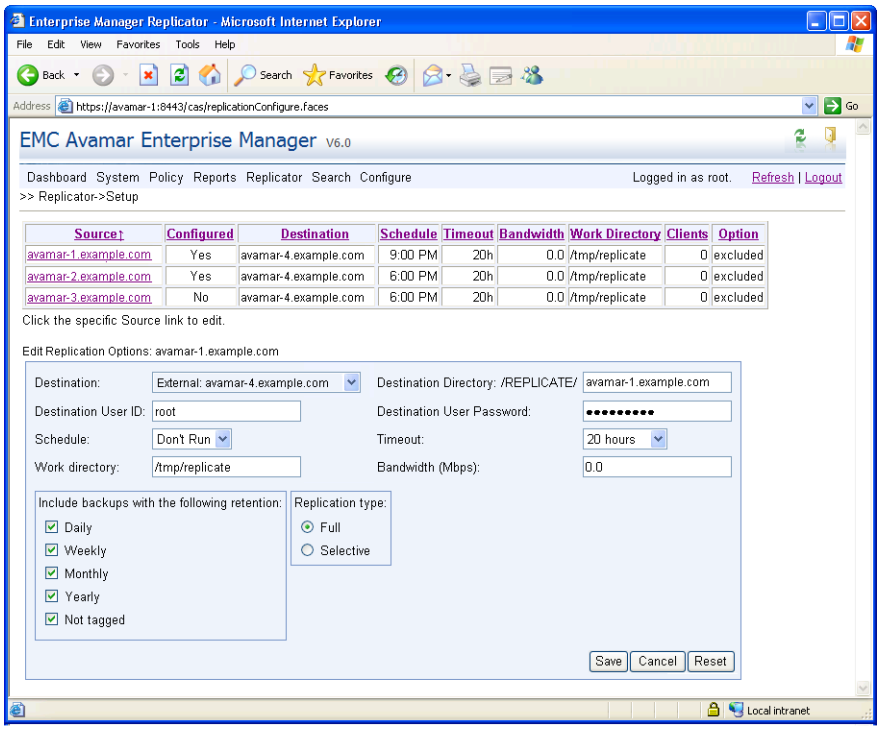
   The Dashboard page appears.

2. Place the mouse cursor over the **Replicator** menu until a sub-menu appears, and then select **Setup**.

   The Replicator Setup page appears.

3. Click the Avamar system link in the **Source** column.

   An Edit block appears below the systems list, which lists the replication settings for that Avamar system, as shown in the following example.



4. From the **Destination** list, select the destination Avamar server.

5. In the **Destination Directory: /REPLICATE/** box, select the destination directory on the destination Avamar server.

   The default location is /REPLICATE/SOURCE, where SOURCE is the source Avamar server hostname that you selected in the systems list.

   The destination must always exist under the /REPLICATE domain.

6. In the **Destination User ID** box, type a valid Avamar administrative user account ID that is used to log in to the destination Avamar server for replication. The default is the replonly account.

7. In the **Destination User Password** box, type the password for the Avamar administrative user account ID (replonly).

The password for the replonly account must be the same on both the source and destination server. If you change the password on one server, then remember to change it on the other server.

8. From the **Schedule** list, select the time of day at which to initiate replication for this server, or select **Don't Run** to temporarily suspend replication of this Avamar system.
9. From the **Timeout** list, select the maximum length of time that each replication operation should run.
10. In the **Work Directory** box, type the full path to the temporary folder or directory for storage replication log files.
11. In the **Bandwidth (Mbps)** box, type a network utilization throttling setting in Mega Bits Per Second (Mbps).

    "Replicator setup page" on page 389 provides additional information about this setting.
12. Under **Include backups with the following retention, select the checkbox next to the retention types of the backups to replicate.**
13. Under **Replication type**, select one of the following:
    - **Full**—Replicate data for all clients on the source Avamar server.
    - **Selective**—Include or exclude certain clients from replication operations.
14. If **Replication Type** is set to **Selective**, use the **Select Clients** section to include all clients, or include or exclude only those clients that match a pattern matching expression.

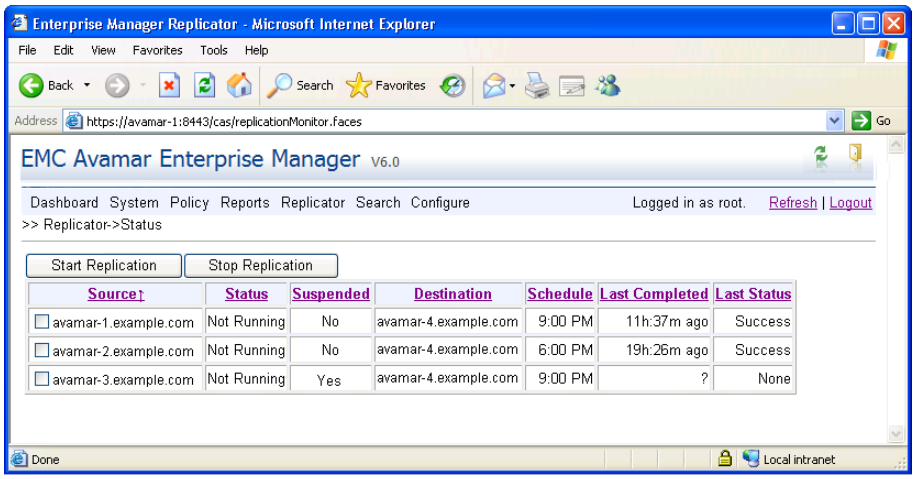
Getting replication status

To view the status of replication operations for one or more Avamar servers:

1. Open a web browser and log in to Avamar Enterprise Manager.

   The Dashboard page appears.
2. Place the mouse cursor over the **Replicator** menu until a sub-menu appears, and then select **Status**.

   The Replicator Status page appears.



The Replicator Status page shows consolidated daily replication status for each Avamar system that you are monitoring.

"Replicator status page" on page 391 provides details on the information shown on this page.

Starting and stopping daily replications

When you stop replication, the process cancels any replication operation that is currently in progress if that replication operation was initiated using Avamar Enterprise Manager. However, if the replication operation was initiated by way of a cron mechanism and you stop replication on that server, the replication operation runs to completion.

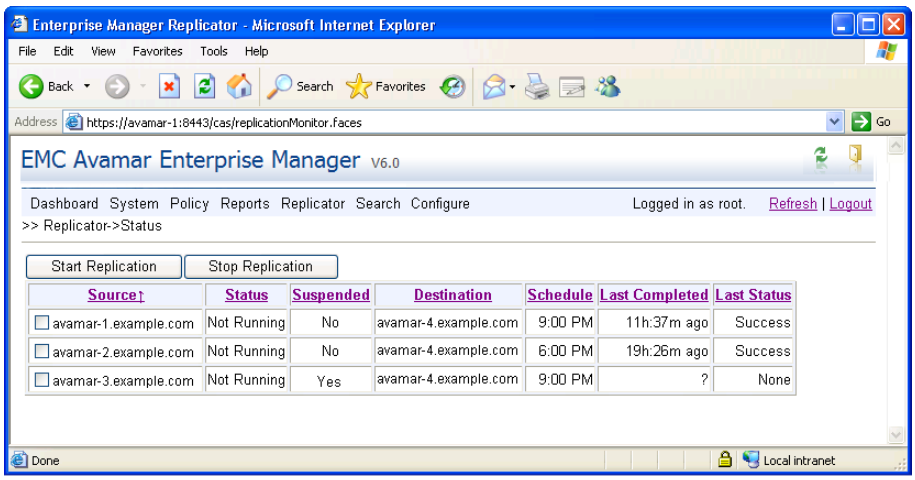
To start or stop daily replications:

1. Open a web browser and log in to Avamar Enterprise Manager.

   The Dashboard page appears.

2. Place the mouse cursor over the **Replicator** menu until a sub-menu appears, and then select **Status**.

   The Replicator Status page appears.



3. Select the checkbox next to the server for which to stop or start replication, and click either **Start Replication** or **Stop Replication**.

Managing replication from the command line

This topic explains how to use the **avrepl** command-line interface (CLI) to replicate data from one Avamar server to another destination Avamar server.

The **avrepl** binary is located in the \usr\local\avamar\bin directory on the server utility node and must be run from that location.

Synopsis

```
avrepl --operation=replicate [--account=LOCATION]
   [--[avtr]after=TIMESTAMP] [--[avtar]allbackups]
   [--backup-type=TYPE] [--[avtar]before=TIMESTAMP]
   [--[avtar]count=NUM] [--[replscript]dpnname=SRC-SERVER]
   [--[replscript]dstaddr=DEST-SERVER] [--[replscript]dstid=USER@PATH]
   [--dstpassword=PASSWORD] [--[replscript]dstpath=DOMAIN]
   [--[replscript]dstport=PORT]
   [--[avtar]expires={N | PERIOD | TIMESTAMP}]
   [--[avtar]exclude-pluginid-list=LIST] [--hfsaddr=AVAMARSERVER]
   [--[avtar]id=USER@AUTH]
   [{--[avtar]informationals=N | --[avtar]noinformationals}] [--log]
   [--logfile=FILE] [--nostdout] [--nowarnings] [--password=PASSWORD]
   [--[avtar]pluginid-list=LIST] [--quiet]
   [--[avtar]retention-type={daily | weekly | monthly | yearly | none}]
   [--server=AVAMARSERVER] [--[replscript]srcpath=DOMAIN]
   [--verbose | -v | --verbose=N] [--version] [--within=PERIOD]
   [TARGET-LIST]
```

Operations

The only supported operation for **avrepl** is --operation=replicate, which replicates data on one Avamar server to another destination Avamar server.

Replicate options

The following replicate options are available for **avrepl**.

Table 73 Replicate avrepl options (page 1 of 3)

Option	Description
--[avtar]after=TIMESTAMP	Specifies that only backups matching TIMESTAMP and later should be replicated. TIMESTAMP must be specified using 24 hour local timezone values conforming to the following syntax: YYYY-MM-DD HH:MM:SS Partial TIMESTAMP values are permitted; resolution is truncated to the last supplied value. For example, 2012-02 is equivalent to 2012-02-01 00:00:00. This option can also be used with --before=TIMESTAMP to define a range of effective dates. Only backups taken within this date range are replicated.
--[avtar]allbackups	If set false, only the most recent backup for each client is replicated. The default setting is true.
--backup-type=TYPE	Specifies a backup type to be included in the replication operation, where TYPE is one of the following: • differential • differential_full • incremental • incremental_full • level0_full • synthetic_full

Table 73 Replicate avrepl options (page 2 of 3)

Option	Description
--[avtar]before=TIMESTAMP	Specifies that only backups taken before TIMESTAMP should be replicated. TIMESTAMP must be specified using 24 hour local timezone values conforming to the following syntax: YYYY-MM-DD HH:MM:SS Partial TIMESTAMP values are permitted; resolution is truncated to the last supplied value. For example, 2012-02 is equivalent to 2012-02-01 00:00:00. This option can also be used with --after=TIMESTAMP to define a range of effective dates. Only backups taken within this date range are replicated.
--[avtar]count=NUM	Limits replicated backups to this maximum number (NUM) of most recent backups for each client.
--[replscript]dpnname=SRC-SERVER	Specifies a name to use to represent the source server (SRC-SERVER) on the destination server. This is the name that is used in the REPLICATE domain on the destination server. This option cannot be used with the --dstpath=DIR or --srcpath=DIR options. --dpn=SRC-SERVER is permissible equivalent.
--[avtar]exclude-pluginid-list=LIST	Constrains replication activity to exclude backups originally taken with one or more plug-in types, where LIST is a comma-separated list of one or more integer plug-in IDs.
--[avtar]expires={N | PERIOD | TIMESTAMP}	Specifies how long to retain replicated backups on the destination server. This can be done three different ways: • By specifying a number (N) of days • By specifying an expiration PERIOD (that is, a specific number of days, weeks, or months or years) • By specifying an absolute expiration TIMESTAMP If only a positive integer is supplied, that is assumed to be the number (N) of days to retain the replicated backups. If PERIOD is supplied, it must be one of the following: • DAYS=N • WEEKS=N • MONTHS=N • YEARS=N where N is a positive integer. For example, supplying --expires=YEARS=2 would cause replicated backups to be retained for two years on the destination server. Also, --expires=30 and --expires=DAYS=30 are equivalent. If TIMESTAMP is supplied, it must be a 24-hour local timezone value conforming to the following syntax: YYYY-MM-DD HH:MM:SS Partial TIMESTAMP values are permitted; resolution is truncated to the last supplied value. For example, 2012-02 is equivalent to 2012-02-01 00:00:00.
--help	Shows help, then exits.
--[avtar]pluginid-list=LIST	Constrains replication activity to include backups originally taken with one or more plug-in types, where LIST is a comma-separated list of one or more integer plug-in IDs.

Table 73 Replicate avrepl options (page 3 of 3)

Option	Description
--[avtar]retention-type={daily | weekly | monthly | yearly | none}	Constrains replication activity to only replicate backups assigned one of the following retention types: • daily—If supplied, only daily backups are replicated. • weekly—If supplied, only weekly backups are replicated. • monthly—If supplied, only monthly backups are replicated. • yearly—If supplied, only yearly backups are replicated. • none—If supplied, only backups without a specific replication type are replicated.
--[replscript]srcpath=DOMAIN	Specifies a location (DOMAIN) on the source Avamar server from which to begin replication. Only data beneath this location is replicated. The default setting is the top-level domain (/), which replicates the entire server. This option must be used in conjunction with the --dstpath=DOMAIN option and cannot be used with the --dpnname=SRC-SERVER option.
--version	Returns the **avrepl** software version.
--within=PERIOD	Replicates backups taken within this most recent time PERIOD, where PERIOD is one of the following: • days=N • weeks=N • months=N • years=N where N is a positive integer. For example, supplying --within=months=3 would replicate three months worth of backups for each client.

Account options

The following account options are available for **avrepl**.

Table 74 Account options for avrepl

Option	Description
--account=LOCATION	Specifies a hierarchical LOCATION on the destination Avamar server. This option is relative to the current home location, unless a slash (/) is used as a prefix to the path designation, in which case an absolute path is assumed. The default account is REPLICATE. --acnt=LOCATION and --path=LOCATION are permissible equivalents.
--[replscript]dstaddr=DEST-SERVER	Specifies a fully qualified DNS name or IP address of the destination Avamar server (DEST-SERVER).
--[replscript]dstid=USER@PATH	Authenticate on the destination Avamar server as this Avamar user ID (account name) at this domain. USER is the Avamar username, and PATH is the Avamar server domain. For example, supplying --dstid=admin@/REPLICATE/avamar-1, specifies that the admin user account on the destination server /REPLICATE/avamar-1 domain should be used to authenticate this replication session.
--dstpassword=PASSWORD	PASSWORD for the --dstid account. --dstap=PASSWORD and --dstpswd=PASSWORD are permissible equivalents.
--[replscript]dstpath=DOMAIN	Specifies a location (DOMAIN) on the destination Avamar server where replicated source data is stored. The default setting is the top-level directory (/), which stores the replicated data in a new domain named for the source Avamar server. This option must be used in conjunction with the --srcpath=DOMAIN option and cannot be used with the --dpnname=SRC-SERVER option.
--[replscript]dstport=PORT	Specifies the data PORT to use when connecting to the destination Avamar server. The default setting is 27000.
--hfsaddr=AVAMARSERVER	Source AVAMARSERVER IP address or fully qualified hostname (as defined in DNS).
--[avtar]id=USER@AUTH	Authenticate on the source Avamar server as this Avamar user ID (account name). USER is the Avamar username, and AUTH is the authentication system used by that user. The default internal authentication domain is “avamar.” For example: jdoe@avamar.
--password=PASSWORD	Specifies PASSWORD for the --id=USER@AUTH account. --ap=PASSWORD and --pswd=PASSWORD are permissible equivalents.
--server=AVAMARSERVER	AVAMARSERVER IP address or fully qualified hostname (as defined in DNS). --hfsaddr=AVAMARSERVER is a permissible equivalent.

Logging options

The following logging options are available for **avrepl**.

Table 75 Logging options for avrepl

Option	Description
--[avtar]informationals=N | --[avtar]noinformationals	Supplying --informationals=N sets the information level. For example, --informationals=3. Supplying --noinformationals disables all status messages.
--log	Logs to the FILE specified by --logfile=FILE. This is the default setting.
--logfile=FILE	Used with the --log option to specify the full path and filename of the log file.
--nostdout	Disables output to STDOUT. However, if --logfile=FILE is supplied, output still goes to log file.
--nowarnings	Disables warning messages.
--quiet	Disables both warnings and status messages. Equivalent to --noinformationals plus --nowarnings.
--verbose | -v | --verbose=N	Supplying either --verbose or -v enables all messages (status and warnings). Additional levels of verbosity can also be specified with --verbose=N, where N is the desired level of verbosity. The default verbosity level is 6.

Target list

You can include a list of clients and domains to replicate at the end of each **avrepl** command. If you do not supply a list, then all client backups on the entire source Avamar server are replicated. For example:

```
CLIENT1 CLIENT2 DOMAIN1 DOMAIN2
```

Separate multiple entries with white space.

Avamar-only options

Avamar-only options access advanced functionality that is normally reserved for use by EMC personnel only. Misuse of these advanced options can cause loss of data. If you are unsure about any aspect of these options, contact EMC Customer Support for additional information before using them.

Table 76 Avamar-only advanced options for the avrepl command (page 1 of 3)

Option	Description
--bindir=PATH	Sets the directory containing Avamar binary files. The default setting is /usr/local/avamar/bin.
--[replscript]exclude=PATTERN	Excludes clients containing PATTERN from a replication. PATTERN is a single matching pattern. Common glob operators (wildcards) such as asterisk (*) and question mark (?) are allowed. For example, --exclude=spot excludes any source path name that contains the pattern "spot." --exclude=/clients/ excludes all clients within the /clients domain. Multiple patterns can be separated by commas (for example, --exclude=spot,/clients/). Multiple --exclude options can also be used to specify more than one PATTERN.
--[avtar]exp-delta=PERIOD	Changes replicated backup expiration dates on the destination server by this PERIOD, where PERIOD is one of the following: • DAYS=N • WEEKS=N • MONTHS=N • YEARS=N where N is a positive or negative integer. For example, supplying --exp-delta=DAYS=-2 would decrease the backup expiration dates on the destination server by two days. --expires and --exp-delta are mutually exclusive.
--[avtar]expiration-policy=TYPE=PERIOD	Replicates backups of a specific retention TYPE within the specified PERIOD, where TYPE is one of the following: • dailies • weeklies • monthlies • yearlies and PERIOD is one of the following: • days=N • weeks=N • months=N • years=N where N is a positive integer. For example, supplying --expiration-policy=dailies=years=2 would replicate two years worth of daily backups for each client. --expiration-policy takes precedence over --expires.
--[replscript]forcecreate	Forces all accounts to be created on the destination server even when other options (for example, (for example, --include, --exclude, and so forth) are supplied.

Table 76 Avamar-only advanced options for the avrepl command (page 2 of 3)

Option	Description
--[replscript]force-move=BOOL	If set to 1 (true), forces a move to target server backup account. If set to 0 (false), does not force a move.
--[replscript]fullcopy	Asserts full "root-to-root" replication mode, which creates a complete logical copy of an entire source server on the destination server. Furthermore, the replicated data is not copied to the REPLICATE domain, it is added directly to the root domain just as if source clients had registered with the destination server. Also, source server data replicated in this manner is fully modifiable on the destination server.
--[replscript]globalcid	If supplied, global client IDs (CIDs) are used during replications. Global CIDs are primarily used to facilitate fast failovers from one server to another following a full "root-to-root" replication. This is the default setting.
--[avtar]label=NAME	Replicates backups when the label is NAME. -f NAME is a permissible equivalent.
--[avtar]label-pattern=PATTERN	Replicates backups when the labels match this PATTERN. PATTERN is a single matching pattern. Common glob operators (wildcards) such as asterisk (*) and question mark (?) are allowed. Multiple patterns can be separated by commas (for example, --exclude=spot,/clients/). Multiple --exclude options can also be used to specify more than one PATTERN.
--rechunk={disable | enable | default}	Controls whether replicated data should be rechunked to maximize data deduplication on the destination server. One of the following: • disable—Do not rechunk data before storing on the destination server. • enable—Rechunk data before storing on the destination server to maximize data deduplication. • default—Automatically rechunk data when source and destination server chunking parameters are different.
--[replscript]reportonly	Asserts report-only operational mode, which is used to predetermine the amount of storage a replication activity might consume on a destination server by running the replication job without actually saving any data to the destination server.
--[replscript]restore	Asserts restore operational mode. If you previously replicated a source Avamar server to a destination Avamar server, running **avrepl** from the destination server and supplying this command restores that data to the source Avamar server.

Table 76 Avamar-only advanced options for the avrepl command (page 3 of 3)

Option	Description
--[avtar]sequencenumber=ID	Specifies one specific backup to replicate. --labelnumber is a permissible equivalent.
--[replscript]small-client-mb=MB	Threshold under which a client's new data is considered "small." The default setting is 128 MB of new data. A setting of 0 disables this optimization.
--[avtar]throttle=MBPS	Controls rate at which the underlying **avtar** process sends data to the server. If --throttle=MBPS is supplied, **avtar** pauses as long as necessary after sending each packet to ensure that network usage does not exceed the specified maximum bandwidth; maximum bandwidth is specified in mega bits per second. For example, --throttle=5 uses half a 10Mbps connection, --throttle=0.772 restricts usage to one-half of a T1 link.

CHAPTER 16
Advanced Server Administration and Maintenance

The following topics describe Avamar server administration and maintenance tasks:

- Checkpoints 404
- MCS configuration settings 408
- Configuring directory service information 412
- Setting last backup retention 419
- Manually changing Avamar Administrator client preferences 420
- Updating server licensing 420
- Using the change-passwords utility with default user accounts 424
- Changing single-node server network settings 431
- Custom notification for web browser logins 432
- Configuring Avamar to use network address translation 432

NOTICE

Avamar server maintenance commands should only be used by authorized personnel who are thoroughly familiar with their intended use.

Checkpoints

Checkpoints are system-wide backups taken for the express purpose of assisting with disaster recovery. Checkpoints are typically scheduled during the maintenance window, which is discussed in "Backup/maintenance windows" on page 309.

In addition to the regularly scheduled twice daily checkpoints, you can create and validate additional server checkpoints at any time.

Checkpoint validation might take several hours, depending on the amount of data in the Avamar server. For this reason, each validation operation can be individually configured to perform all checks (full validation) or perform a partial "rolling" check, which fully validates all new and modified stripes, then partially checks a subset of unmodified stripes.

You can also delete checkpoints to reclaim server storage capacity.

Individual checkpoints shown in the Avamar Server window Checkpoint Management tab are always in one of the following states:

Table 77 Avamar server checkpoint states

State	Description
	Checkpoint failed validation or was canceled before it could complete.
	Checkpoint has not yet been validated.
	Validation is currently being performed on this checkpoint.
	Checkpoint passed validation.

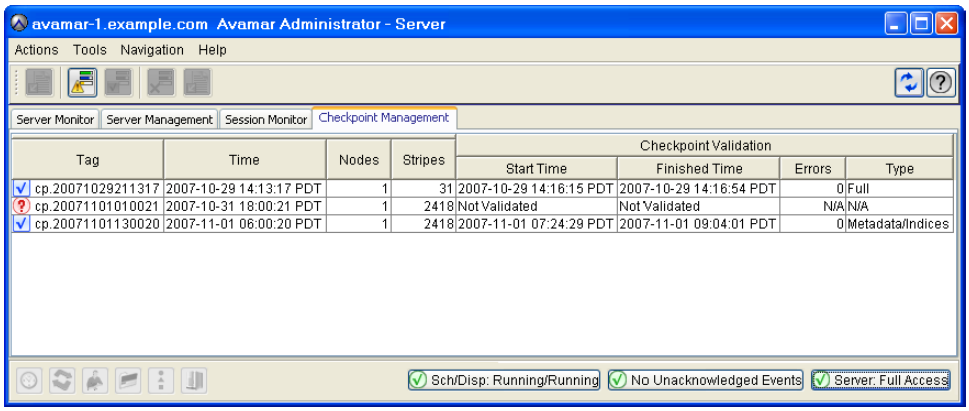
Creating a checkpoint

To create a checkpoint:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.

2. Click the **Checkpoint Management** tab.



3. Select **Actions** › **Create Checkpoint**.

   The Create New Checkpoint dialog box appears and shows the progress of the operation.

4. When the **Create New Checkpoint** dialog box shows that the checkpoint is complete, click **Close**.

Validating a checkpoint

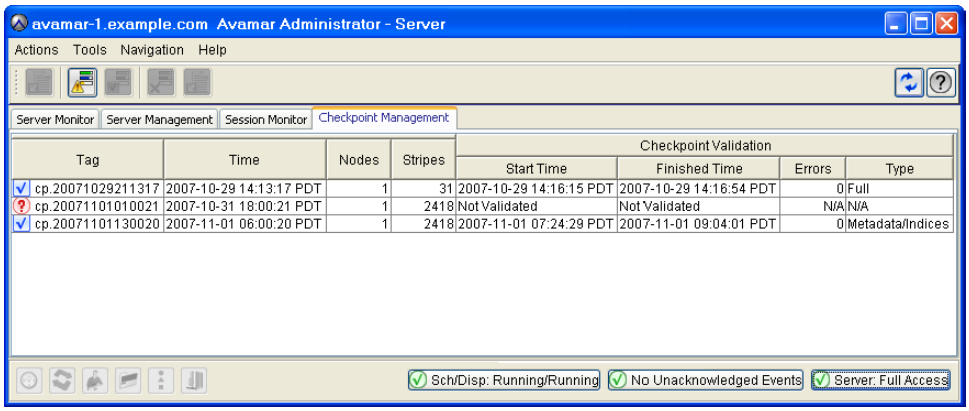
Checkpoint validations can take several hours to perform and only one checkpoint can be validated at a time.

To validate a checkpoint:

1. In Avamar Administrator, click the **Server** launcher button.

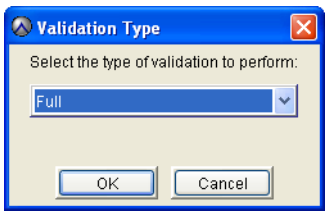
   The Server window appears.

2. Click the **Checkpoint Management** tab.



3. Select an unvalidated checkpoint and select **Actions** › **Validate Checkpoint**.

   The Validation Type dialog box appears.



4. Select one of the following the validation types:

   - **Full**—to performs all checks.
   - **Rolling**—To perform a partial, "rolling" check. This validation type fully validates all new and modified stripes, then partially checks a subset of unmodified stripes.

5. Click **OK**.

Deleting a checkpoint

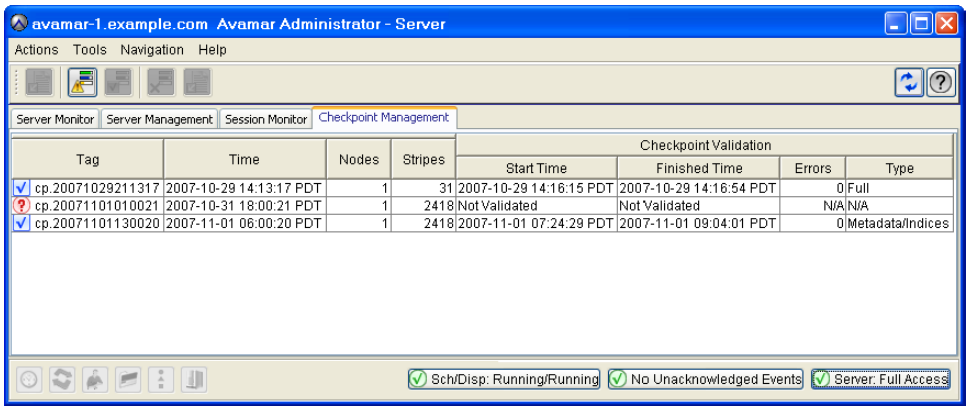
You can delete checkpoints to reclaim additional server storage capacity. Generally, it is best to delete unvalidated checkpoints before you delete validated checkpoints.

To delete a checkpoint:

1. In Avamar Administrator, click the **Server** launcher button.

   The Server window appears.

2. Click the **Checkpoint Management** tab.



3. Select the checkpoint to delete and select **Actions** › **Delete Checkpoint**.

   A confirmation message appears.

4. Click **Yes**.

Rolling back to a checkpoint

Rollback is the process of restoring the Avamar server to a known good state using data stored in a validated checkpoint.

If you added nodes to the Avamar server since the checkpoint occurred, remove the entries for the nodes from the probe.out file before the rollback.

You cannot roll back an Avamar 7.0 server to a version 4.x or earlier checkpoint.

To roll back to a checkpoint:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.

2. Shut down the server by typing:

   dpnctl stop

3. Display a list of checkpoints by typing:

   cplist

   A list of checkpoints appears in the command shell, as shown in the following example:

   ```
   cp.20080106170113 Fri Jan 6 17:01:13 2008 valid hfs del nodes 4 stripes 396
   cp.20080107170042 Sat Jan 7 17:00:42 2008 valid hfs del nodes 4 stripes 396
   cp.20080108170040 Sun Jan 8 17:00:40 2008 valid hfs ... nodes 4 stripes 396
   cp.20080109170043 Mon Jan 9 17:00:43 2008 valid hfs ... nodes 4 stripes 396
   ```

   In the list, each `cp.YYYYMMDDHHMMSS` entry is a checkpoint ID, `valid hfs` indicates a validated checkpoint, and `valid par` indicates a partially validated checkpoint.

   Generally, you should roll the system back to the latest fully validated checkpoint unless you have a good reason to roll back to an earlier checkpoint.

4. Use the date/time stamps to find the latest validated checkpoint, and note the checkpoint ID.

5. Initiate the rollback by typing:

   rollback.dpn --cptag=cp.YYYYMMDDHHMMSS >& FILE

   where cp.YYYYMMDDHHMMSS is the checkpoint ID and FILE is a user-defined temporary file.

6. Wait for the rollback to complete.

   The rollback might take up to one hour, depending on the amount of data present in the Avamar server. When the rollback is complete, the command prompt returns.

7. Open the user-defined temporary file created during the rollback and verify that the rollback successfully completed without errors.

   The server automatically restarts after a successful rollback.

Clearing data integrity alerts

To ensure data integrity, the Avamar server issues an alert any time a checkpoint validation fails. The only way to clear this alert is to contact EMC Customer Support and have them provide you with a reset code.

To clear the data integrity alert, enter that reset code in the **Type reset code** field and click **OK**.

MCS configuration settings

The following topics provide details on MCS configuration settings:

- "Understanding MCS configuration settings" on page 408
- "Backing up MCS data" on page 409
- "Performing an on-demand MCS flush" on page 409
- "Finding MCS backups in the system" on page 410
- "Restoring MCS data" on page 410
- "Reverting to default MCS preference settings" on page 411

Understanding MCS configuration settings

Avamar Administrator consists of both client and server software applications. You can independently configure each application by editing the appropriate preferences file.

The server preferences file is mcserver.xml. The client preferences file is mcclient.xml. Both files conform to the preferences.dtd XML Document Type Description (DTD) referenced by the JSDK 1.4 API.

Changes made to the server preferences file affect all Avamar Administrator sessions; changes made to a client preferences file only affect Avamar Administrator sessions on that client.

Default and live copies

Two copies of each of these files are present on the system:

- An initial default copy is used to initialize each application after installation.
- A live copy contains the current settings used by the application.

The default copies are located in the /lib directory for each application. The live copies are located in a "live file" directory. The default live file directory for each application is:

- /usr/local/avamar/var/mc/server_data/prefs (server live file directory)
- INSTALL-DIR/var/mc/gui_data/prefs (client live file directory)

where INSTALL-DIR is typically C:\Program Files\avs\administrator on Microsoft Windows computers, /usr/local/avamar on Linux computers or /opt/AVMRconsl on Solaris computers.

Initialization behavior

When either the server or client application is initialized, the respective default preferences file in the lib directory is loaded into memory and replicated to the live file directory.

NOTICE

Reinitializing a running MCS is highly destructive. It completely overwrites any custom preference settings stored in the live file and reverts the system configuration back to default settings. If this occurs, you must recover custom preference settings from a previous flush (backup) if they are overwritten.

Upgrade behavior

During server upgrades, any mcserver.xml entry that is marked with the merge="delete" attribute in the new default mcserver.xml file is not merged into the new live copy. These entries are obsolete. They are retained in the default mcserver.xml file so that the MCS knows to delete the preferences on an upgraded customer system.

Beginning with version 7.0, you can manually add a merge="keep" attribute to any entry in the live /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml file. Settings with merge="keep" attributes are retained in the new live copy following the upgrade process.

Backing up MCS data

To protect itself from hardware failures, the MCS backs up, or "flushes," its persistent data to the Avamar server that it manages. Flushes are done by way of an **avtar** client session.

Automatic flushes are normally performed hourly and as part of system checkpoints.

Avamar automatically creates the following timestamp files.

Table 78 MCS backup timestamp files

File	Description
flush.timestamp	Before every flush, a special timestamp file (flush.timestamp) is created in the server_data directory. This file includes the time and date of the flush. On a server rollback, this file is restored and can be used to verify that the rollback was successful to the selected time and date. The contents of flush.timestamp are also accessible by way of the **mcserver.sh --status** command, which is discussed in "Getting MCS status" on page 323.
init.timestamp	During system initialization, the init.timestamp file is created or overwritten in the server_data directory. This file includes the time and date of the system initialization and can be used to verify that initialization was successful on the selected time and date.

Performing an on-demand MCS flush

Automatic flushes are normally performed hourly and as part of system checkpoints. You can also force an on-demand flush.

To force an on-demand flush:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   mcserver.sh --flush
   ```

Finding MCS backups in the system

MCS flushes (backups) are stored under the /MC_BACKUPS account. You can get a list of MCS backups by browsing this account in the Avamar Administrator Backup & Restore window or by typing the following **avtar** command on a single command line:

```
avtar --backups --id=root --ap=PASSWORD --path=/MC_BACKUPS
    --hfsaddr=mydpn.Example.com --count=NUM
```

where PASSWORD is the Avamar root user account password (not the operating system root password) and NUM is the number of backups to list.

NOTICE

Space limitations in this guide cause the previous command example to wrap to more than one line. The command must be typed on a single command line (no line feeds or returns allowed).

A typical Avamar server takes 26 MCS flushes (backups) per day (one per hour and one each during the morning and evening system checkpoints). Therefore, to list all MCS flushes (backups) stored in the system for a predictable past number of days, specify --count=NUM in increments of 26. For example, --count=26 lists all backups stored in the system during the past day, --count=52 lists all backups stored in the system during the past two days, and so forth.

Restoring MCS data

To restore MCS data:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the MCS by typing:

   ```
   dpnctl stop mcs
   ```

3. Restore the MCS to the latest flush (backup) by typing:

   ```
   mcserver.sh --restore
   ```

   NOTICE

   You can also restore the MCS to a specific backup by including the **--labelnum=NUM** option. "Finding MCS backups in the system" on page 410 provides information on the option.

4. Open /usr/local/avamar/var/mc/server_log/restore.log to verify the success of the restore.

5. Restart the MCS by typing:

   ```
   dpnctl start mcs
   ```

6. Resume scheduled operations as discussed in "Suspending and resuming scheduled operations" on page 313.

Reverting to default MCS preference settings

To safely revert back to the initial default preference settings:

1. Open a command shell and log in using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the MCS by typing:

   ```
   dpnctl stop mcs
   ```

3. Change the working directory by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. In the current directory, rename mcserver.xml to old.mcserver.xml by typing:

   ```
   mv mcserver.xml old.mcserver.xml
   ```

5. Copy the default server preferences file into the current directory by typing:

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

   NOTICE

   Space limitations in this guide cause the previous **cp** command to wrap to more than one line. The **cp** command must be typed on a single command line (no line feeds or returns allowed).

6. Restart the MCS by typing:

   ```
   dpnctl start mcs
   ```

7. Resume scheduled operations as discussed in "Suspending and resuming scheduled operations" on page 313.

Configuring directory service information

Configure directory service information to allow Avamar products to authenticate users through an existing directory service. Use one or more LDAP v.3-compliant directory service domains, such as Microsoft Active Directory Domain Services domains. Also, use a single Network Information Service (NIS) on its own, or with the LDAP services.

The following Avamar products use existing directory services to authenticate users:

- Avamar Administrator (Optional)
- Avamar Enterprise Manager (Optional)
- Avamar Web Restore (Required)
- Avamar client web UI (Optional)

Information about a directory service must be provided to Avamar before the service can be used to authenticate users. To provide the required information, use the LDAP Management tool. This tool is part of Avamar Administrator.

Port requirements

To authenticate users through an LDAP v.3-compliant directory service (Kerberos or plain text), Avamar requires access to the following recognized ports on the Key Distribution Center (KDC):

- 88 - Kerberos authentication system
- 389 - Lightweight Directory Access Protocol (LDAP)
- 464 - Kerberos Change/Set password

The ports are defined in krb5.conf and ldap.properties. "Text editing of ldap.properties and krb5.conf" on page 416 provides information about editing these files.

Login requirements

The directory services configuration interface is only available to users that are assigned the Administrator role and are logged in to the root domain.

To log in to Avamar Administrator and use the directory service configuration interface:

1. Launch Avamar Administrator:

   The login window appears.

2. In **Username**, type a username for an account that is assigned the Administrator role at the root domain level.

   When a directory service is already configured, an account for an LDAP user with the Administrator role at the root domain level can be used. This login method is described in "Starting Avamar Administrator" on page 39.

3. In **Password**, type the password for the user account.

4. In **Domain Name**, use the default entry of a single slash (/) character.

   The single slash (/) character specifies the root domain. Root domain login is required.

5. In **Avamar Server**, type the Avamar Administrator server name to log in to, as defined in the corporate Domain Name Server (DNS).
6. Click **Log On**.

   The Administrator dashboard appears.
7. In Avamar Administrator, click the **Administration** launcher button.

   The Administration window appears.
8. Click the **LDAP Management** tab.

   This tab is only visible to users that are assigned the Administrator role and are logged in to the root domain.

Providing LDAP information

To provide information about an LDAP v.3-compliant directory service:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
2. Click **Directory Service Management**.

   The **Directory Service Management** dialog box appears.
3. Click **Add**.

   The **Adding a new Directory Service** section appears.
4. Select **LDAP**.
5. In **Enter a fully qualified domain name**, type the fully qualified domain name (FQDN) of a directory server.
6. (Optional) Select **Make this the default domain LDAP domain**.

   Select this for the server that represents the organization's default directory service domain.

   To allow the Avamar client web UI to authenticate users from Macintosh computers, the LDAP server assigned to Macintosh users must be configured as the default server.
7. Click **Add**.

   A confirmation dialog box appears.
8. Click **Yes**.

   A success message appears. If not, see "Error messages for unsuccessful tests" on page 415.
9. Click **OK**.

   The changes are immediately applied to the following services:

   - Management Console Server (mcs)
   - Enterprise Manager (em)
   - Desktop and Laptop (dtlt)
10. (Optional) Repeat these steps to add another authentication domain.

11. Click **Close**.

    The **Directory Service Management** dialog box closes.

Providing NIS information

To provide information about an NIS directory service:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
2. Click **Directory Service Management**.

   The **Directory Service Management** dialog box appears.
3. Click **Add**.

   The **Adding a new Directory Service** section appears.
4. Select **NIS**.
5. In **Enter a fully qualified domain name**, type the NIS domain name assigned when the NIS domain was set up.
6. In **NIS Domain IP address**, type the IP address of the NIS server.
7. Click **Add**.

   A confirmation dialog box appears.
8. Click **Yes**.

   A success message appears. If not, see "Error messages for unsuccessful tests" on page 415.
9. Click **OK**.

   The changes are immediately applied to the following services:

   - Management Console Server (mcs)
   - Enterprise Manager (em)
   - Desktop and Laptop (dtlt)
10. Click **Close**.

    The **Directory Service Management** dialog box closes.

Testing a directory service entry

To test a directory service entry:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
2. Click **Directory Service Management**.

   The **Directory Service Management** dialog box appears.
3. From **Configured Directory Services**, select one of the entries.

   The **Testing** section appears.

4. In **Username**, type the username for an account that is authorized to read the directory service database.
5. In **Password**, type the password associated with the username.
6. Click **Run Test**.

   The test results appear in a dialog box. If the test is not a success, see "Error messages for unsuccessful tests" on page 415.
7. Click **Close** to close the **Testing** section.
8. Click **Close**.

   The **Directory Service Management** dialog box closes.

Error messages for unsuccessful tests

When adding or testing a directory service configuration is unsuccessful, error messages appear. The following table lists some of the potential messages and provides a description of the cause.

Table 79 Error message information

Message	Description
Cannot discover KDC	A key distribution center (KDC) could not be found using the domain information provided.
No URL is present	The domain provided is not present in ldap.properties.
Parameters are not correct	Directory service domain information in ldap.properties is not valid.
Client not found in Kerberos database	Username that was provided is not valid.
Pre-authentication information was invalid	Password is not correct.
Query fails	User account does not have sufficient privileges to read the directory service database.
Clock skew too great	The differential between the clock on the Avamar server host and the clock on the directory service host is too large.
Cannot open LDAP configuration file	The ldap.properties file does not exist or the file's permissions prevent access.
Cannot open Kerberos configuration file	The krb5.conf file does not exist or the file's permissions prevent access.
GSS initiate failed	Credential authentication failed. Usually this is because reverse DNS is not properly configured. Add the KDC host to /etc/hosts on the Avamar server.
Cannot get kdc for realm	The KDC is not properly configured in krb5.conf.
Domain ‹domain› exists in ldap.properties file	The domain being added already exists in the ldap.properties file.

Text editing of ldap.properties and krb5.conf

The LDAP Management tool provides text editing capabilities for the directory service configuration files: ldap.properties and krb5.conf. Text editing of these files is only required when problems occur after providing LDAP and NIS information through the Add Domain button.

NOTICE

Text editing of these files should not be performed unti l you are sure you know the correct format for keys and values in each of thes files and you possess the required information about your directory services.

To edit ldap.properties or krb5.conf:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
2. Click **Edit LDAP file** to edit ldap.properties or click **Edit KRB5 file** to edit krb5.conf.

   The Edit ldap.properties file or the Edit krb5.conf file window appears.
3. Type additions and changes directly in the window.
4. Click **Save**.

   The additions and changes are written to the selected file.
5. Click **Close**.

   The window closes.

Formatting requirements of ldap.properties

The LDAP Management tool creates a properly formatted ldap.properties file. The recommended method for configuring ldap.properties is to use the LDAP Management tool.

A properly formatted ldap.properties complies with the following key and value (KV) pair rules:

- One LDAP URL KV pair for each LDAP server

  The LDAP URL KV pair maps an LDAP server to a specific domain controller.

  The LDAP URL KV pair format is:

  ldap.url.*ds.example.abc.com***=ldap://***dchost.r1.example.abc.com:389*

  where *ds.example.abc.com* is the FQDN of an LDAP server, *dchost.example.abc.com* is the FQDN of the domain controller for that server, and *389* is the port used by the LDAP service.
- Exactly one default server KV pair

  The default server KV pair is used during authentication of users on clients that are not mapped to a specific domain, such as local users and users logging in from a AIX, FreeBSD, HP-UX, Linux, SCO, or Solaris computer. The format is:

  ldap.qualified-name-default=*dshost.example.abc.com*

  where *dshost.example.abc.com* is the FQDN of the default LDAP server.

Other settings, in the form of key/value (KV) pairs, can be added to ldap.properties using the text editing window. Those settings are shown in the following table.

Table 80 KV pairs in ldap.properties

Key	Values	Description
user-login-module	kerberos ldap avamar mix	Controls the authentication mechanism used. The options are: • **kerberos**-LDAP authentication with Kerberos encryption • **ldap**-Plaintext LDAP authentication • **avamar**-Avamar authentication • **mix**-Both kerberos and avamar When this KV pair is missing from ldap.properties the default is: user-login-module=kerberos
avamar-authentication-domains		Required when ldap properties contains: user-login-module=mix. It takes as its value a comma-separated list of domains. Avamar authentication is applied to users from each listed domain. LDAP authentication is applied to all other users.
support-nis-authentication	true false	Enables (true) or disables (false) NIS authentication support. When this KV pair is missing from ldap.properties the default is: support-nis-authentication=false
nis.qualified-name-default		Specifies the domain name of the NIS domain server. Takes as its value the FQDN of the server.
nis.url.*nisdomainname*		Specifies the IP address of the NIS domain server, where *nisdomainname* is the value of nis.qualified-name-default.

Changing the time-out value

Directory service processes wait up to 300 seconds for a response from the directory service. After 300 seconds the attempt is discarded and a time-out message appears. The default 300 second time-out value can be changed.

The time-out value is used by the following directory service authentication processes:

- Authentication requests through the directory service.
- Adding a directory service, as described in "Providing LDAP information" on page 413 and "Providing NIS information" on page 414.
- Testing a directory service, as described in "Testing a directory service entry" on page 414.

To change the time-out value:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the Management Console Server (mcs) service by typing:

   ```
   dpnctl stop mcs
   ```

3. Change the working directory by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Open mcserver.xml in a plain text editor.
5. Find the ldap node, and the entry with the ldap_services_timeout_seconds key, as shown here:

   ```
   <node name="ldap">
      <map>
         …
         <entry key="ldap_services_timeout_seconds" value="300" />
         …
      </map>
   </node>
   ```

   As indicated by the ellipsis (…), the ldap node has many entries. Only the relevant entry appears here.
6. Change the value of the entry with key="ldap_services_timeout_seconds" to a new time-out value:

   ```
   <node name="ldap">
      <map>
         …
         <entry key="ldap_services_timeout_seconds" value="SS" />
         …
      </map>
   </node>
   ```

   where *SS* is the new time-out value, in seconds.
7. Save the change and close the editor.
8. Restart mcs by typing:

   ```
   dpnctl start mcs
   ```

9. Close the command shell.

Setting last backup retention

By default a backup is marked for deletion when its assigned retention period expires. With clients that do not back up frequently, this default behavior can lead to the last backup expiring before a new backup runs and clients that do not have an available backup.

Clients that are not permanently connected to a domain, such as remote desktops and laptops, can encounter this situation.

You can enable last backup retention to retain the last backup for all clients. When a new backup runs, the new backup becomes the "last backup" and the previous "last backup" expires or is retained according to its retention policy.

IMPORTANT

When you enable last backup retention, Avamar retains a single backup for each client, even if you perform multiple types of backups of a client. For example, if you perform both file system and application backups of a client, and the file system backup is the last backup, then all application backups can expire.

To enable last backup retention:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Change directories by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
3. Open mcserver.xml in a plain text editor.
4. Find the dpn node.
5. In that node, find the "keep_last_backup" key and change the key's value from "false" to "true":

   Change:

   ```
   <entry key="keep_last_backup" value="false" />
   ```

   to:

   ```
   <entry key="keep_last_backup" value="true" />
   ```
6. Save the change and close the editor.

7. Restart the MCS by typing:

```
dpnctl stop mcs
dpnctl start mcs
```

8. Close the command shell.

Manually changing Avamar Administrator client preferences

Some Avamar Administrator client preferences can be changed directly from Avamar Administrator. However, a number of preferences can only be changed by editing mcclient.xml.

To manually change Avamar Administrator client preferences:

1. Close Avamar Administrator.
2. Open var/mc/gui_data/prefs/mcclient.xml in a text editor such as vi or Emacs.
3. Edit the preference elements.
4. Save the changes.

   The changes take effect the next time you start Avamar Administrator.

Updating server licensing

An Avamar server requires a license key for permanent operation. Upon acceptance of the order, EMC licensing provides you with assigned license keys for the Avamar software. You also receive the Customer Account ID and Asset ID, which are required to generate a permanent license.

Avamar products

Obtain assigned license keys for standard Avamar products from the Avamar download center: Subscribenet.

To access Subscribenet, type the login credentials provided in the email sent to you from emc@subscribenet.com. If you cannot find the email from emc@subscribenet.com:

1. Send an email to licensing@emc.com to request the Avamar license keys.
2. Include the EMC product SO number in the email.

   The EMC product SO number is required.

The return time for an email response is 48 hours.

Avamar products included in EMC Backup Software suite

Obtain assigned license keys for Avamar products included in EMC Backup Software suite models, from Powerlink (http://Powerlink.EMC.com).

1. Log in to Powerlink with your Powerlink username and password.
2. Under **Support**, navigate to **Software Downloads and Licensing**, then **License Management**.

3. Click on **Avamar** to access the Flexera Website.
4. Follow the instructions on the Welcome Letter received from emc@flexnetoperations.com.

License installation road map

Use the following road map for all license installations:

1. Generate a gsankeydata.xml license key information file as described in "Generating a license key information file" on page 421.

   The gsankeydata.xml license key information file is later used to generate the permanent license key.

   NOTICE

   You may have already generated this file during the Avamar server software installation and configuration. If so, you do not need to perform the steps in "Generating a license key information file" on page 421.

2. If you have login credentials to the Avamar License Portal, use the portal to generate a license key file as described in "Generating a permanent license key file" on page 423.
3. Install the license on the Avamar server as described in "Installing and activating the license" on page 423.

Generating a license key information file

To generate a gsankeydata.xml license key information file:

1. Open a command shell and log in by using one of the following methods:
   - To log in to a single-node server, log in to the server as admin.
   - To log in to a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Type:

   ```
   gathergsankeydata
   ```

   The following information appears in the command shell:

   ```
   Enter your Avamar system customer account number:
   ```

3. Type the Avamar system customer account number and press **Enter**.

   A valid Avamar system customer account number (account ID) conforms to the following format:

   CN-YYMMDDNNNNN

   where:

   - YY is a two-digit year.
   - MM is a two-digit month.
   - DD is a two-digit day of the month.
   - NNNNN is a five-digit numerical sequence.

   The following information appears in the command shell:

   ```
   Enter your Avamar system asset ID number:
   ```

4. Type the Avamar system asset ID number and press **Enter**.

   A valid Avamar system asset ID number (asset reference ID) conforms to the following format:

   A-YYYYNNNNNN

   where:

   - YYYY is a four-digit year.
   - NNNNNN is a six-digit numerical sequence.

   The following information appears in the command shell:

   ```
   Please enter the Internet domain for this account:
   ```

5. Type the Internet domain and press **Enter**.

   Information similar to the following appears in the command shell:

   ```
   Your answers were:
   Customer account ID: [CN-10062212345]
   Customer asset ID: [A-2010123456]
   Internet domain: [emc.com]
   Is this correct? [y(es), n(o), e(xit)]:
   ```

6. Type **y** and press **Enter**.

   The local directory now contains the gsankeydata.xml license key information file. This file is used to generate the permanent license key.

Generating a permanent license key file

To generate a permanent license key file, you must have login credentials to the Avamar License Portal. You receive login credentials to the Avamar License Portal after you complete Avamar installation training certification and accept the EMC confidentiality agreement.

If you do not have login credentials to the Avamar License Portal:

1. Send an email to licensing@emc.com to request an Avamar llicense key generation. The subject line must contain the following text: ONSITE Priority Request: Avamar License Key Generation.
2. Provide the gsankeydata.xml file and the authorized quantity of Terabyte Licenses you want to allocate to the system.

   EMC Licensing then provides you with an XML file that contains an activated license key.

Installing and activating the license

After you receive the license key file from either EMC Licensing or from the key generation process in "Generating a permanent license key file" on page 423, you can install and activate the license.

To install and activate the license:

1. Log in to the email account to which the license key file was sent.
2. Open the email message from info@Avamar.com with a subject line of EMC Avamar Key Information.

   The email message contains the license key file as an attachment. The file uses the following naming convention:

   ```
   ASSET-NAME_Key.xml
   ```

   where ASSET-NAME is typically the Avamar server hostname as defined in DNS.
3. Save the ASSET-NAME.xml email attachment to a temporary directory or folder.
4. Use **WinSCP** or an equivalent program to copy the ASSET-NAME.xml license key file from the temporary directory or folder to the appropriate location described below:
   - For administering a single-node server, the license key file is located in the /tmp directory on the Avamar server.
   - For administering a multi-node server, the license key file is located in the /tmp directory on the Avamar server utility node.
5. Switch to the command shell session and ensure that you are still logged in as user admin, and that the admin OpenSSH key is loaded.
6. Ensure that the Avamar server subsystem (also known as GSAN) is running by typing:

   `dpnctl status gsan`

   If gsan is running, then the following information appears in the command shell:

   ```
   dpnctl: INFO: gsan status: ready
   ```

7. Change file permissions on the ASSET-NAME.xml license key file and activate the license by typing the appropriate commands depending on server status:

   - If the server is running, type:

     ```
     chmod 644 /tmp/ASSET-NAME.xml
     avmaint license /tmp/ASSET-NAME.xml --avamaronly
     ```

   - If the server is not running, type:

     ```
     cd /usr/local/avamar/etc
     mv license.xml license.xml.old
     cp /tmp/ASSET-NAME.xml license.xml
     chmod 644 license.xml
     ```

   where ASSET-NAME.xml is the license key file.

8. If the Avamar server is not running, start it. Chapter 12, "Server Shutdown and Restart," contains information about starting the Avamar server.

9. Verify that the server license is correctly installed by typing:

   ```
   avmaint license --avamaronly
   ```

   License information appears in the command shell.

Using the change-passwords utility with default user accounts

This procedure describes how to use the **change-passwords** interactive utility to change various operating user account and Avamar server user account passwords, as well as create new OpenSSH keys.

The **change-passwords** utility guides you through the following operations:

- Changing operating system login passwords for the admin, dpn, and root accounts
- Creating new admin and dpnid OpenSSH keys
- Changing internal Avamar server passwords for the root and MCUser accounts

To change operating user account passwords or Avamar server user account passwords, or to create new OpenSSH keys:

1. Open a command shell and log in using one of the following methods:

   - To log in to a single-node server, log in to the server as dpn.
   - To log in to a multi-node server, log in to the utility node as dpn.

2. Type:

   ```
   change-passwords
   ```

   If you run **change-passwords** on a multi-node server, the following information appears in the command shell:

   ```
   Do you wish to change passwords and/or passphrases on all nodes?
      Answering y(es) changes this set of nodes:
         #.s    -- all utility/services nodes
         #.#    -- all data nodes.
      Answering n(o) will afford you the opportunity to install
      existing SSH keys onto other nodes.

   y(es), n(o), h(elp), q(uit/exit):
   ```

3. Do one of the following:

   - To change passwords on all nodes, type **y** and press **Enter**.
   - To change passwords on selected nodes, type **n** and press **Enter**.

   The following information appears in the command shell:

```
Identity added: /home/dpn/.ssh/dpnid (/home/dpn/.ssh/dpnid) Identity
added: /home/dpn/.ssh/dpnid.prev (/home/dpn/.ssh/dpnid.prev)
Identity
added: /home/dpn/.ssh/dpnid.orig (/home/dpn/.ssh/dpnid.orig)

Do you wish to specify one or more additional SSH passphrase-less
   private keys that are authorized for root operations?
Answer n(o) here unless there are known inconsistencies in
   ~root/.ssh/authorized_keys2 files among the various nodes (as
might be evident if you had been prompted for a root password in a
previous run of this program).
Note that the following keys will be used automatically (there is
   no need to re-specify them here):
       /home/dpn/.ssh/dpnid
       /home/dpn/.ssh/dpnid.prev
       /home/dpn/.ssh/dpnid.orig

y(es), n(o), h(elp), q(uit/exit):
------------------------------------------------------------
```

4. Type **n** and press **Enter**.

   The following information appears in the command shell:

```
The following is a test of root authorization with the currently
   loaded SSH key(s).

   If during this test you are prompted for an OS root password,
   then you might be missing an appropriate "dpnid" key for one
   or more nodes.
       -> In that event, re-run this program and, when prompted,
          specify as many SSH private key files as are necessary
          in order to complete root operations on all nodes.

Starting root authorization test with 15 second timeout...
End of root authorization test.
------------------------------------------------------------
```

   The following information appears in the command shell:

```
------------------------------------------------------------
Change OS (login) passwords?
y(es), n(o), q(uit/exit):
```

5. Do one of the following:

   - If you want to change admin, dpn, or root operating system user account passwords, type **y** and press **Enter**.
   - If you do not want to change admin, dpn, or root operating system user account passwords, type **n** and press **Enter**. Proceed to step 16 .

   The following information appears in the command shell:

```
------------------------------------------------------------
Change OS password for "admin"?
y(es), n(o), q(uit/exit):
```

6. Do one of the following:
   - If you want to change the admin operating system user account password, type **y** and press **Enter**.
   - If you do not want to change the admin operating system user account password, type **n** and press **Enter**. Proceed to step 10 .

   The following information appears in the command shell:

   ```
   Please enter a new OS (login) password for user "admin".
   (Entering an empty (blank) line twice quits/exits.)
   ```

7. Type the new admin operating system user account password and press **Enter**.

   The following information appears in the command shell:

   ```
   Please enter the same OS password again.
   (Entering an empty (blank) line twice quits/exits.)
   ```

8. Retype the new admin operating system user account password and press **Enter**.

   The following information appears in the command shell:

   ```
   Accepted OS password for "admin".
   ------------------------------------------------------
   Change OS password for "dpn"?
   y(es), n(o), q(uit/exit):
   ```

9. Do one of the following:
   - If you want to change the dpn operating system user account password, type **y** and press **Enter**.
   - If you do not want to change the dpn operating system user account password, type **n** and press **Enter**. Proceed to step 13 .

   The following information appears in the command shell:

   ```
   Please enter a new OS (login) password for user "dpn".
   (Entering an empty (blank) line twice quits/exits.)
   ```

10. Type the new dpn operating system user account password and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the same OS password again.
    (Entering an empty (blank) line twice quits/exits.)
    ```

11. Retype the new dpn operating system user account password and press **Enter**.

    The following information appears in the command shell:

    ```
    Accepted OS password for "dpn".
    ------------------------------------------------------
    Change OS password for "root"?
    y(es), n(o), q(uit/exit): y
    ```

12. Do one of the following:
    - If you want to change the root operating system user account password, type **y** and press **Enter**.
    - If you do not want to change the root operating system user account password, type **n** and press **Enter**. Proceed to step 16 .

    The following information appears in the command shell:

    ```
    Please enter a new OS (login) password for user "root".
    (Entering an empty (blank) line twice quits/exits.)
    ```

13. Type the new root operating system user account password and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the same OS password again.
    (Entering an empty (blank) line twice quits/exits.)
    ```

14. Retype the new root operating system user account password and press **Enter**.

    The following information appears in the command shell:

    ```
    Accepted OS password for "root".
    ========================================================
    Change SSH keys?
    y(es), n(o), q(uit/exit): y
    ```

    The following information appears in the command shell:

    ```
    ========================================================
    Change SSH keys?
    y(es), n(o), q(uit/exit):
    ```

15. Do one of the following:
    - If you want to change admin or dpnid OpenSSH keys, type **y** and press **Enter**.
    - If you do not want to change admin or dpnid OpenSSH keys, type n and press Enter. Proceed to step 22 .

16. Do one of the following:
    - If you want to create new admin or dpnid OpenSSH keys, type **y** and press **Enter**.
    - If you do not want to create new admin or dpnid OpenSSH keys, type n and press Enter. Proceed to step 18 .

    The following information appears in the command shell:

    ```
    --------------------------------------------------------
    Change SSH key for "admin"?
    y(es), n(o), q(uit/exit):
    ```

17. Do one of the following:
    - If you want to create a new admin OpenSSH key, type **y** and press **Enter**.
    - If you do not want to create a new admin OpenSSH key, type **n** and press **Enter**. Proceed to step 21 .

    The following information appears in the command shell:

    ```
    Please enter a new SSH key passphrase for user "admin".
    (Entering an empty (blank) line twice quits/exits.)
    ```

18. Type the new admin OpenSSH passphrase and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the same SSH key again.
    (Entering an empty (blank) line twice quits/exits.)
    ```

19. Retype the new admin OpenSSH passphrase and press **Enter**.

    The following information appears in the command shell:

    ```
    Accepted SSH key for "admin".
    ------------------------------------------------------
    Redo passphrase-less elevated-privilege SSH key "dpnid"?
    y(es), n(o), h(elp), q(uit/exit):
    ```

20. Do one of the following:

    - If you want to create a new dpnid OpenSSH key, type **y** and press **Enter**.
    - If you do not want to create a new dpnid OpenSSH key, type **n** and press **Enter**.

    NOTICE

    This task requires knowledge of the internal Avamar server root user account password.

    The following information appears in the command shell:

    ```
    ======================================================
    Change Avamar Server passwords?
    y(es), n(o), q(uit/exit):
    ```

21. Do one of the following:

    - If you want to change the MCUser or internal root Avamar server user account passwords, type **y** and press **Enter**.
    - If you do not want to change the MCUser or internal root Avamar server user account passwords, type n and press Enter. Proceed to step 30 .

    The following information appears in the command shell:

    ```
    Please enter the CURRENT Avamar Server password for "root"
    (Entering an empty (blank) line twice quits/exits.)
    ```

22. Type the current internal Avamar server root user account password (not the operating system root password) and press **Enter**.

    The following information appears in the command shell:

    ```
    Checking Avamar Server root password (300 second timeout)...
    Avamar Server current root password accepted.
    ------------------------------------------------------
    Change Avamar Server password for "MCUser"?
    y(es), n(o), q(uit/exit): y
    ```

23. Do one of the following:

    - If you want to change the internal Avamar server MCUser password, type **y** and press **Enter**.
    - If you do not want to change the internal Avamar server MCUser password, type **n** and press **Enter**. Proceed to step 27 .

    The following information appears in the command shell:

    ```
    Please enter a new Avamar Server password for user "MCUser".
    (Entering an empty (blank) line twice quits/exits.)
    ```

24. Type the new internal Avamar server MCUser password and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the same Avamar Server password again.
    (Entering an empty (blank) line twice quits/exits.)
    ```

25. Retype the new internal Avamar server MCUser password and press **Enter**.

    The following information appears in the command shell:

    ```
    Accepted Avamar Server password for "MCUser".
    ------------------------------------------------------
    Change Avamar Server password for "root"?
    y(es), n(o), q(uit/exit):
    ```

26. Do one of the following:

    - If you want to change the internal Avamar server root password, type **y** and press **Enter**.
    - If you do not want to change the internal Avamar server root password, type **n** and press **Enter**. Proceed to step 30 .

    The following information appears in the command shell:

    ```
    Please enter a new Avamar Server password for user "root".
    (Entering an empty (blank) line twice quits/exits.)
    ```

27. Type the new internal Avamar server root password and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the same Avamar Server password again.
    (Entering an empty (blank) line twice quits/exits.)
    ```

28. Retype the new internal Avamar server root password and press **Enter**.

    The following information appears in the command shell:

    ```
    Accepted Avamar Server password for "root".
    ------------------------------------------------------
    Do you wish to proceed with your password changes on the selected
    node?
       Answering y(es) will proceed with password updates.
       Answering n(o) or q(uit) will not proceed.

    y(es), n(o), q(uit/exit): y
    ```

    The following information appears in the command shell:

    ```
    ======================================================
    Change the server lockbox administrative passphrase?
    y(es), n(o), h(elp), q(uit/exit): y
    ```

29. Do one of the following:

    - If you want to change the server lockbox passphrase, type **y** and press **Enter**.
    - If you do not want to change the server lockbox passphrase, type **n** and press **Enter**. Proceed to step 33 .

    The following information appears in the command shell:

    ```
    ------------------------------------------------------
    Change the server lockbox administrative passphrase?
    y(es), n(o), h(elp), q(uit/exit): y

    Please enter the CURRENT server lockbox administrative passphrase.
    Enter ? or help for help.

    (Entering an empty (blank) line twice quits/exits.)
    ```

30. Type the old server lockbox passphrase and press **Enter**.

    The following information appears in the command shell:

    ```
    Please enter the NEW server lockbox administrative passphrase.
    Enter ? or help for help.

    (Entering an empty (blank) line twice quits/exits.)
    ```

31. Type the new server lockbox passphrase and press **Enter**.
32. Do one of the following:

    - If you want to accept changes made to passwords or OpenSSH keys during this utility session, type **y** and press **Enter**.
    - If you want to exit this utility session without making changes to passwords or OpenSSH keys, type **n** and press **Enter**.

The following information appears in the command shell:

```
Changing OS passwords...
[Logging to /usr/local/avamar/var/change-passwords.log...]
Done changing OS passwords...
Changing Avamar Server passwords...
Checking MCS Status...
Stopping MCS...
Starting process of updating Administrator configuration...
Running script to update Administrator configuration on node 0.s...
[Logging to /usr/local/avamar/var/change-passwords.log...]
Done with updating Administrator configuration on node 0.s...
Starting process of updating client configurations...
Running script to update client configuration on 0.s...
[Logging to /usr/local/avamar/var/change-passwords.log...]
Updating client configuration on node 0.0...
Done updating client configuration on 0.0...
Checking MCS Status...
Starting MCS...
Starting process of changing SSH keys...
Running script to update SSH keys on node 0.s...
[Logging to /usr/local/avamar/var/change-passwords.log...]
Done with updating SSH keys on node 0.s...
-------------------------------------------------------
Done.
NOTES:
- If you had custom public keys present in the
   authorized_keys2 files of any Avamar OS users
   (admin, dpn, root) be aware that
    you may need to re-add your custom keys.
- Please be sure to resume schedules via the
   Administrator GUI.
```

33. Resume scheduled operations by performing the following:
    a. In Avamar Administrator, select **Tools** › **Manage Schedules**.

       The Manage All Schedules window appears.

    b. Click **Resume All**.

Changing single-node server network settings

To change a single-node server's network settings, follow the instructions in the *Changing the Name and IP Addressing of Avamar Systems Tech*nical Note. All Avamar documentation, including this technical note, is available from the EMC online support website at https://support.emc.com/products. The part number for this technical note is 300-007-53.

Custom notification for web browser logins

A custom security notification can be included on the login page of Avamar Enterprise Manager and on the login page of Avamar Web Restore. This notification typically explains that only authorized users are permitted access. It can also list the penalties for unauthorized access.

To implement a custom notification add a plain-text file with the correct filename to the /usr/local/avamar/var/em/server_data/ directory.

Avamar provides some support for HTML tags and CSS inline styles in this plain-text formatted file.

Adding a custom security notification

To add a custom security notification:

1. Create a file in a plain-text editor.
2. Save the file with the correct filename for the intended login screen, as follows:
   - Avamar Enterprise Manager login screen, use:
     `disclaimer_EM.txt`
   - Avamar Web Restore login screen, use:
     `disclaimer_Web_Restore.txt`
3. Add content.

   HTML tags and CSS inline styles can be used.
4. Copy the file to the following location on the utility node or single-node server:

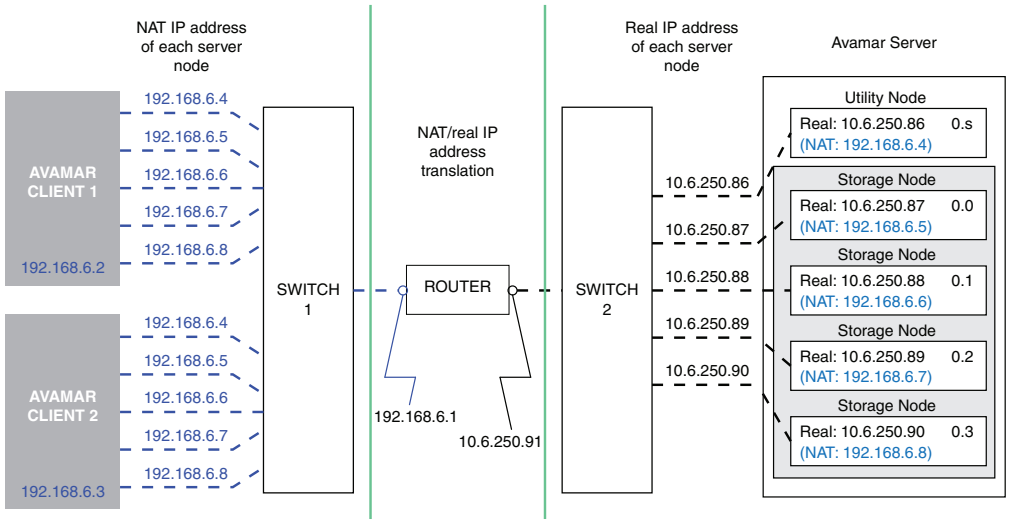
   `/usr/local/avamar/var/em/server_data/`

Configuring Avamar to use network address translation

This topic applies only to Avamar configurations that use Network Address Translation (NAT).

Starting with version 5.0, some or all Avamar clients can access Avamar storage nodes by using a set of addresses that undergo NAT. To make NAT information known to the Avamar server, the probe.xml file must contain nat-address elements for storage nodes. After a client makes initial contact with the Avamar server's utility node, the Avamar server provides a set of routable addresses for the storage nodes to each client. In the absence of a nat-address element, a client uses a pre-configured "real" (untranslated) network-interface address.

The following figure illustrates an example of a 1x4 multi-node server configuration in which Avamar uses NAT.



GEN-001232

The following instructions explain how to set up the probe.xml file (node resource database) to enable the Avamar server to use NAT. These instructions assume that each Avamar node has a unique address (from the Avamar clients' perspective), and that you configure a router on the network to apply transparent one-to-one network address translation. You can also use these instructions to enable NAT for use in a single-node server configuration.

NOTICE

Setting up the hardware for NAT is beyond the scope of this guide.

To configure Avamar to use NAT:

1. Use either the **dpnnetutil** or **nodedb** program to add NAT addresses to probe.xml.
   - An example command using **dpnnetutil**:

     ```
     su - root
     dpnnetutil
     ```

     Respond to the interactive prompts displayed by **dpnnetutil**.
   - An example command using **nodedb**:

     ```
     nodedb update if --addr=10.6.250.87
     --new-nat=192.168.6.4=192.168.6.5
     ```

     The **nodedb** command updates an existing network interface element in the probe.xml file with NAT information that corresponds to the example diagram shown on the previous page.
2. If the Avamar storage subsystem is currently stopped, restart it by typing:

   ```
   dpnctl start gsan
   ```

3. If the Avamar storage subsystem is currently running, re-read the probe.xml file by typing:

   ```
   avmaint networkconfig /usr/local/avamar/var/probe.xml --avamaronly
   ```

4. Register clients by using the **avregister** (UNIX) or **avregister.bat** (Windows) command, or by using Avamar Administrator.

   - An example command to register a UNIX client using **avregister**:

     ```
     /usr/local/avamar/bin/avregister
     ```

     Respond to the interactive prompts displayed by **avregister**.

     To determine whether NAT is in use, the client and Avamar server must have a network connection.

   - "Client registration" on page 60 provides more information about registering clients from Avamar Administrator.

Resolving NAT connection and configuration problems

The following table provides solutions for common NAT connection and configuration problems.

Table 81 Common NAT connection and configuration problems and their solutions

Problem	Solution
Avamar server terminates with a FATAL ERROR message.	Ensure that the probe.xml file: 1. Exists in the /usr/local/avamar/var/ directory. 2. Is a valid XML file and adheres to the node resource database format. 3. Lists NAT IP addresses correctly. Use the nodedb print --say command to view the contents of probe.xml. The --say option shows the path and name of the current node resource database.
Server/client connection fails.	Use network diagnostic tools such as ping, traceroute, tracert, or iperf to verify network connectivity.

CHAPTER 17
Server Updates and Hotfixes

The following topics describe how to install updates and hotfix patches on an Avamar server by using the System Maintenance page in Avamar Enterprise Manager.

- Overview 436
- Avamar Downloader Service installation requirements 438
- Installing the Avamar Downloader Service 439
- Configuring the Avamar Downloader Service 442
- Using the Avamar Downloader Service 444
- Troubleshooting Avamar Downloader Service issues 452
- Uninstalling the Avamar Downloader Service 453
- Installing packages from System Maintenance 453
- Viewing installation history information 460

Overview

As part of an Avamar server software installation or upgrade, EMC Customer Support installs the following software:

- Avamar Downloader Service software on a standalone Microsoft Windows server that allows network access to EMC sites on the Internet and all internal Avamar servers.
- AvInstaller on the utility node in a multi-node environment or the server in a single-node environment.

  The AvInstaller installation provides the Avamar Installation Manager user interface.

The Avamar Downloader Service installation creates the following components:

- Local repository in the installation directory.

  This directory is where the Avamar Downloader Service puts packages it fetches from the EMC repository.
- Start menu group Programs › EMC Avamar Downloader Service 7.0.0.*build* that contains:
  - Avamar Downloader Service Configuration
  - Avamar Downloader Service Monitor
- Desktop shortcut to the Avamar Downloader Service configuration application.

The AvInstaller manages the following components:

- EMC repository manifest file
- Download packages from the Avamar Downloader Service
- /data01/avamar/repo/packages directory
- Dependency and version checks of the download packages
- Temporary directory used to extract the packages

NOTICE

Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.

Avamar Downloader Service

The Avamar Downloader Service file distribution process uses minimal bandwidth by downloading only files that you request through the Avamar Installation Manager or System Maintenance in the Avamar Enterprise Manager. The Avamar Downloader Service uses a local file cache to ensure that a file is fetched only once from the EMC repository no matter how many times an Avamar system requests the file. You can remove old files from the local repository to free disk space.

Avamar Downloader Service security

The Avamar Downloader Service validates each package it downloads to ensure the package has been properly signed and transmitted.

The Avamar Downloader Service accepts incoming requests only from Avamar systems that are on a known systems list. The Avamar Downloader Service encrypts outgoing communication to the EMC repository by using SSL (Secure Socket Layers) over an HTTP connection.

NOTICE

If a customer site prohibits access to the Internet, you can manually copy packages to the /data01/avamar/repo/packages directory on the utility node or single-node server instead of installing the Avamar Downloader Service. The AvInstaller manages download packages that are copied to the /data01/avamar/repo/packages directory.

Avamar Downloader Service components

Table 82 on page 437 describes the components of the Avamar Downloader Service.

Table 82 Avamar Downloader Service components (page 1 of 2)

Component	Description
Avamar Downloader Service Windows service	Monitors the EMC repository. When a package is available for an Avamar system, the AvamarDownloaderService service automatically downloads the package and pushes it to the local repository on the Avamar utility node or single-node server.
Avamar Downloader Service configuration application	A user interface that enables you to configure and modify Avamar Downloader Service configuration parameters.
Avamar Downloader Service monitor	A process that provides status message about the Avamar Downloader Service

Table 82 Avamar Downloader Service components (page 2 of 2)

Component	Description
Task tray icon	
	Appears after you install the Avamar Downloader Service. After you configure a system, the task tray icon changes to the icon shown in the next row of this table.
	Appears after you configure the Avamar Downloader Service. Moving the mouse over this icon displays status messages from the Avamar Downloader Service monitor. "Monitoring Avamar Downloader Service status" on page 446 provides more information. Right-clicking this icon displays eight options: • Configure Service • Open Repository • Run Diagnosis • Check for New Packages • Show Advanced Settings • Check for Updates • About • Exit "Using the Avamar Downloader Service menu options" on page 445 provides more information about the task tray icon options.

Avamar Downloader Service installation requirements

The Avamar Downloader Service is available as either a 32-bit or 64-bit application. You install the Avamar Downloader Service on a Microsoft Windows server. This system can be a desktop or laptop system. Table 83 on page 438 provides the installation requirements for the Avamar Downloader Service.

Table 83 Installation requirements for the Avamar Downloader Service

Software/hardware	Requirement
Operating system	• Microsoft Windows Server 2012 • Microsoft Windows Server 2008 • Microsoft Windows Server 2003 SP1, SP2, R2 • Microsoft Windows 8 • Microsoft Windows 7 • Microsoft Windows Vista • Microsoft Windows XP SP3
File system	Any file system
Hard drive space	Minimum of 12 MB
RAM	Minimum of 20 MB

Hotfix requirement for 64-bit Windows XP and 64-bit Windows 2003 server

Apply Microsoft's "Disabling File System Redirection" hotfix before installing the Avamar Downloader Service on the following operating systems:

- Microsoft Windows Server 2003 SP1 (64-bit)
- Microsoft Windows Server 2003 SP2 (64-bit)
- Microsoft Windows XP SP3 (64-bit)

IMPORTANT

Only apply this hotfix to operating systems that require it. Contact Microsoft for additional information about the hotfix.

To apply the hotfix:

1. Download the "Disabling File System Redirection" hotfix from Microsoft.

   Refer to http://support.microsoft.com/kb/942589.

2. Following Microsoft's instructions, install the hotfix on the Windows computer.
3. Restart the Windows computer.

After completing this task, follow the instructions in "Installing the Avamar Downloader Service" on page 439.

Installing the Avamar Downloader Service

You install and configure the Avamar Downloader Service on a Microsoft Windows system that has network access to the Avamar server.

Downloading the software

The following procedure downloads the Avamar Downloader Service software.

1. Log in to the Windows host system as an administrator.
2. Type the URL of the Avamar server into the web browser:

   http://*Avamar_server*

   where *Avamar_server* is the Avamar system network hostname (as defined in DNS) or IP address.

   The EMC Avamar Web Restore page appears.

3. Click **Downloads**.

   The Downloads list appears.

4. Click **+** next to the platform heading for the Windows computer.
5. Click **+** next to the operating system heading for the Windows computer.
6. Click the link for **AvamarDownloaderService-windows-***platform***-***version***.exe**.

   where:

   - *platform* is the type of Windows platform (32-bit or 64-bit).
   - *version* is the version of the Avamar server software (6.1.0-280, for example).

   A dialog box prompts you to either run the file or save it.

7. Save the installation file to a temporary directory.

Installing the software

The following procedure installs the Avamar Downloader Service software.

1. Navigate to the directory that contains **AvamarDownloaderService-windows-***platform*-*version*.exe, and then double-click the file to start the installation.

   The Welcome to the Avamar Downloader Service Setup Wizard appears.

2. Click **Next**.

   The Destination Folder page appears.

3. Click **Next** to accept the default folder, C:\Program Files\EMC\Avamar Downloader Service.

   To install the Avamar Downloader Service in a folder other than the default folder:

   a. Click **Change**.

      The Change destination folder dialog box appears.

   b. Browse to a folder to use for the installation.

   c. Click **OK** to accept the folder and to close the dialog box.

   d. Click **Next** to continue.

      The Ready to install Avamar Downloader Service page appears.

4. Click **Install**.

   The Installing Avamar Downloader Service page appears, which displays a progress bar as the installation proceeds.

   After the installation completes, the Completed the Avamar Downloader Service Setup Wizard page appears.

5. Click **Finish**.

   The installation adds an Avamar Downloader Service icon to the Control Panel and the system tray. The installation also adds the AvamarDownloaderService to Windows Services.

6. (Microsoft Windows 7 only) Define an inbound rule in the Windows Firewall with Advanced Security interface. "Defining an inbound rule for Microsoft Windows 7 hosts" on page 441 provides instructions.

Defining an inbound rule for Microsoft Windows 7 hosts

Microsoft Windows 7 security rules block port 21, which prevents the Avamar Downloader Service from requesting files from ftp.avamar.com. To address this issue, you must define a custom inbound rule in the Windows Firewall with Advanced Security interface.

The following procedure defines an inbound rule for Microsoft Windows 7 64-bit and 32-bit host systems.

1. Select **Control Panel › Windows Firewall › Advanced Settings**.

   The Windows Firewall with Advanced Security interface appears.

2. In the navigation pane, click **Inbound Rules**.

3. In the **Actions** pane, click **New Rule**.

   The New Inbound Rule Wizard appears.

4. In the New Inbound Rule Wizard:

   a. Select **Custom**, and then click **Next**.

      The Program page appears.

   b. Select **This Program Path:** and type the appropriate path in the text box:

      – For Windows 7 64-bit, type:

        C:\Program Files\EMC\Avamar Downloader Service Setup x64\avamardownloaderService.exe

      – For Windows 7 32-bit, type:

        C:\Program Files\EMC\Avamar Downloader Service\avamardownloaderService.exe

   c. Click **Next**.

      The Protocols and Ports page appears.

   d. Click **Next**.

      The Scope page appears.

   e. Click **Next**.

      The Action page appears.

   f. Select **Allow the connection**, and then click **Next**.

      The Profile page appears.

   g. Select the **Domain**, **Private**, and **Public** checkboxes, and then click **Next**.

      The Name page appears.

   h. Type a name and description for the rule:

      – In the **Name** text box, type **Avamar Downloader Service Program from EMC**.

      – In the **Description (optional)** text box, type **C:\Program Files\EMC\Avamar Downloader Service**.

i. Click **Finish** to close the **New Inbound Rule Wizard**.

5. In the **Windows Firewall with Advanced Security** interface verify that the **Inbound Rules** list contains the **Avamar Downloader Service Program from EMC** entry.

Configuring the Avamar Downloader Service

Before you can use the features in the Avamar Downloader Service, you must first configure it.

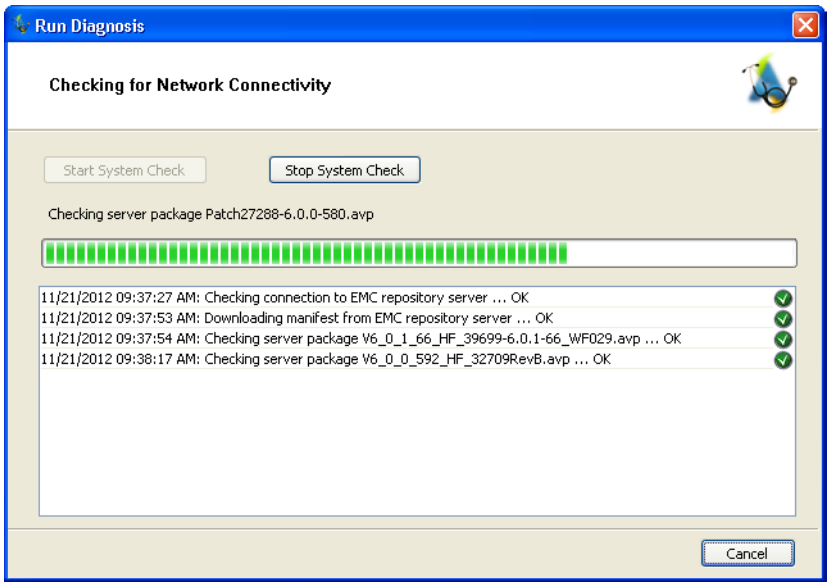
1. Click Avamar Downloader Service task tray icon.

   The Welcome! page appears.

2. Click **Check For Network Connectivity**.

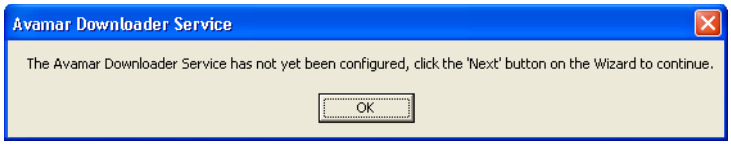
   Two windows appears:

   - Run Diagnosis.



The Run Diagnosis window checks network connectivity between the Windows server and the EMC repository server. This process takes a few minutes. You can let the process run while you configure the Avamar Downloader Service.

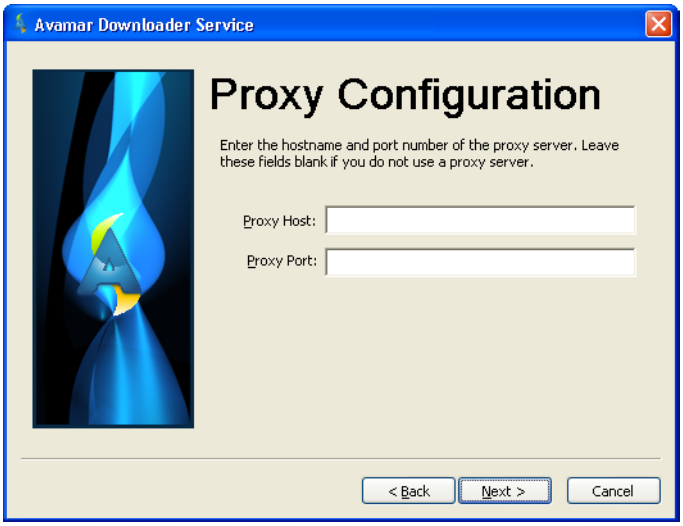
- Avamar Downloader Service.



This message dialog box appears if the Avamar Downloader Service has not been configured.

3. Click **OK** in the Avamar Downloader Service dialog box to start the configuration process.
4. Click **Next**.

   The Proxy Configuration page appears.



5. (Optional) Complete the settings for the **Proxy Configuration** page:

   a. For **Proxy Host**, type the hostname or the IP address for the proxy server (for example, proxy.example.com or 10.220.330.40).

   b. For the **Proxy Port**, type the port number for the proxy server.

   If the configuration does not use a proxy server, leave both fields blank.

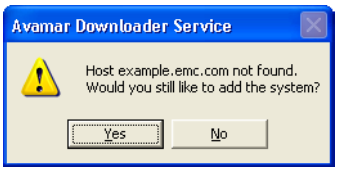
6. Click **Next**.

   The Avamar Systems page appears.

7. Click **Add**.

   The Avamar Downloader Service - Add Known System dialog box appears.

8. In the **Avamar Downloader Service - Add Known System** dialog box, complete the settings:
   a. In the **Hostname** field, type the IP address or hostname.
   b. In the **Username** field, type **root**.
      The value for the Username field is the Linux operating system root user.
   c. In the **Password** field, type the root password.
      The value for the Password field is the Linux operating system root password.
   d. In the **Confirm Password** field, retype the root password.
9. Click **OK**.
   The system is added to the Known Systems list.
   If the hostname cannot be resolved, the following informational message appears:



   Click **Yes** to add the system or **No** to cancel the add operation.
   You can still add systems with unresolvable hostnames, such as offline systems, to the Known Systems list.
10. Repeat steps 7–9 to add all remaining Avamar systems.
11. Click **Next**.
    The Review Configuration page appears.
12. Review the configuration details, and then click **Finish**.
    The task tray icon changes to  .

Using the Avamar Downloader Service

This topic describes how to use the Avamar Downloader Service.

Starting the Avamar Downloader Service configuration application

To start the Avamar Downloader Service configuration application, use one of the following methods:

- Click the task tray icon.
- Right-click the task tray icon and select **Configure Service**.
- Double-click the Avamar Downloader Service desktop icon.
- From the **Start** menu, select **Programs** or **All Programs** › **EMC Avamar Downloader Service 7.0.0-***build* › **Avamar Downloader Service Configuration.**

Using the Avamar Downloader Service menu options

All functions of the Avamar Downloader Service are available from the task tray icon's popup menu.

To view this menu, right-click the Avamar Downloader Service task tray icon.

Table 84 on page 445 describes the menu options available from the Avamar Downloader Service task tray icon.

Table 84 Avamar Downloader Service task tray icon menu options

Option	Description
Configure Service	Runs the Avamar Downloader Service Configuration application.
Open Repository	Opens the Windows Explorer and displays the C:\Program Files\EMC\Avamar Downloader Service\repository directory, which contains the manifest.xml file. The manifest.xml file lists all the server, client, and workflow packages currently available for download from the EMC repository.
Run Diagnosis	Checks network connectivity between the Windows server and the EMC repository server. • To start a system check, click **Start System Check**. • To stop a system check, click **Stop System Check**. • To close the Run Diagnosis window, click **Close**.
Check for New Packages	Retrieves the manifest.xml file from the EMC repository server and downloads it to the C:\Program Files\EMC\Avamar Downloader Service\repository directory. To close the Check for New Packages window, click **Close**.
Show Advanced Settings	Displays the Show Advanced Settings window. This window includes the Repository Credentials tab. You modify the repository credentials in this window.
Check for Updates	Installs the latest version of the Avamar Downloader Service on the repository FTP server.
About	Displays version and copyright information.
Exit	Closes the Avamar Downloader Service task tray icon.

Monitoring Avamar Downloader Service status

The Avamar Downloader Service monitor automatically starts when you log in to the Windows server that runs the Avamar Downloader Service. To view the status from the monitor, move the mouse over the task tray icon.

Table 85 on page 446 lists Avamar Downloader Service monitor status messages.

Table 85 Avamar Downloader Service monitor status messages

Status message	Description
Avamar Downloader Service	Default status message.
Authentication Failure with the EMC Repository.	HTTP basic authentication failure.
Authentication Failure with one or more “Known Systems.”	HTTP basic authentication failure including: • Failed communication with the EMC repository. • SSL (Secure Socket Layers) handshake failed. • HTTP dropped connection. • HTTP NAK (negatively acknowledged message).
Failed communication with one or more “Known Systems.”	• SSL handshake failed. • HTTP dropped connection. • HTTP NAK.
Failed file download from the EMC repository.	File transfer was aborted.
Failed file transfer to one or more known systems.	File transfer was aborted.
Network Error	Windows 7 firewall settings prevent the Avamar Downloader Service from requesting files from the Avamar FTP site.
Out of space.	The Avamar Downloader Service file cache is full. To free up disk space, remove files from the local repository.
Running.	The service is running and communicating with all known systems as well as the EMC repository.
Socket failure on host computer.	• Either the Microsoft Windows machine is out of socket resources or there is a binding problem with the NIC. • Deadlock condition within Winsock.
Waiting for configuration.	The Avamar Downloader Service was installed, but not configured.

Starting the monitor

The monitor starts automatically when you log in to the Windows server.

You can manually start the monitor from the Windows **Start** menu:

- On Windows Server 2003, Windows XP, or Windows Vista, select **Programs › EMC Avamar Downloader Service 7.0.0.***build* **› Avamar Downloader Service Monitor**.
- On Windows Server2008 or Windows 7, select **All Programs › EMC Avamar Downloader Service 7.0.0.***build* **› Avamar Downloader Service Monitor**.

Stopping the monitor

To stop the monitor, right-click the Avamar Downloader Service task tray icon, and then select **Exit**.

Checking the EMC repository

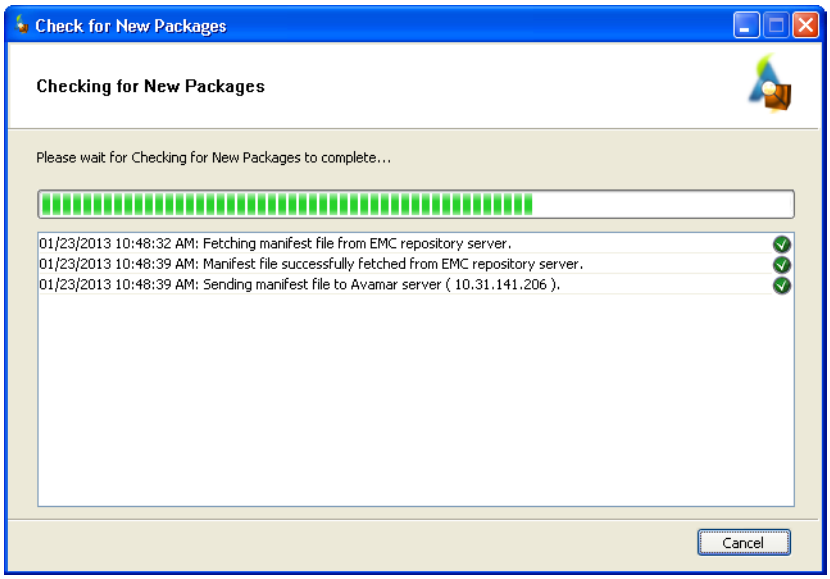
You can check the EMC repository for updates at any time.

1. Click Avamar Downloader Service task tray icon.

   The Welcome! page appears.

2. Click **Check for New Packages**.

   The Check for New Packages dialog box appears:



   The Avamar Downloader Service performs the following tasks:

   - Downloads the manifest file to the local repository on the Windows server, and then pushes the installation packages to the Avamar systems that have been configured.
   - Deletes expired files from the file cache. By default, the expiration period is 30 days.
   - Displays status information.
     - A check mark next to a status messages indicates that the process was successful.
     - An **X** next to a status message indicates that the process failed.

   NOTICE

   You cannot click **Check for New Packages** if the status of the Avamar Downloader Service is anything other than OK or “waiting for new files.”

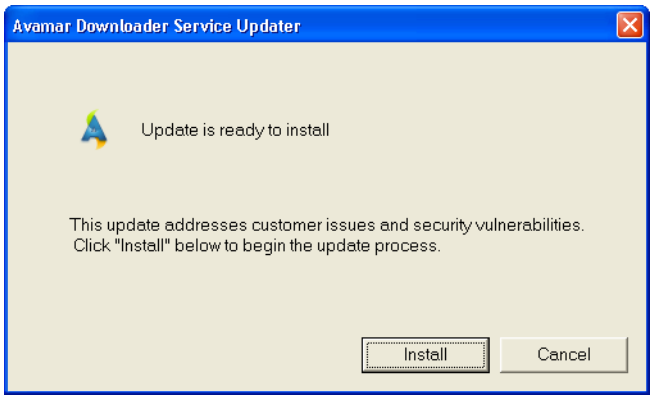
3. Double-click the **X** next to a status message to view more details about the failure.
4. Click **Close** to exit the **Check for New Packages** dialog box.

Checking for Avamar Downloader Service updates

The following procedure checks for updates and installs them on the Windows system.

1. Right-click Avamar Downloader Service task tray icon and select **Check for Updates**.

   The Avamar Downloader Service Updater dialog box appears.



2. Click **Install**.

   The Welcome to the Avamar Downloader Service Setup Wizard appears.
3. Follow the installation prompts. "Installing the software" on page 440 provides more information.

   This process updates the Avamar Downloader Service software to a newer build.

Modifying the repository credentials

The Avamar Downloader Service application includes the Show Advanced Settings option, which enables you to specify an alternate repository. By default, the Avamar Downloader Service uses the EMC repository.

NOTICE

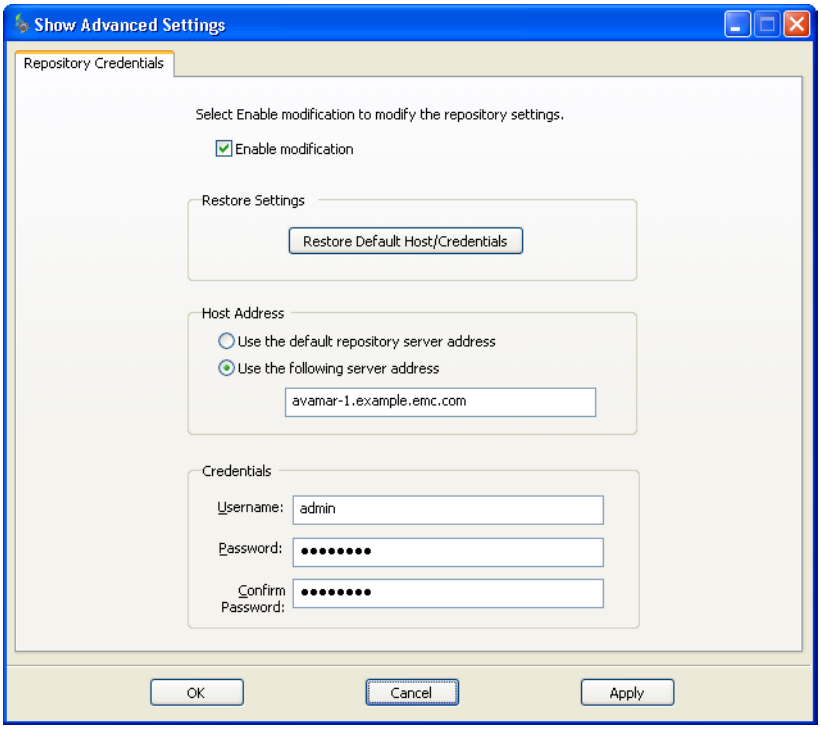
Under most circumstances, you do not need make any changes from the Show Advanced Settings dialog box.

The following procedure changes repository settings.

1. Right-click the Avamar Downloader Service task tray icon and select **Show Advanced Settings**.

   The Show Advanced Settings window appears.
2. Select **Enable modification**.

The options in the Show Advance Settings become selectable.



3. Make the appropriate changes. Table 86 on page 449 describes options in the Show Advanced Settings window.

Table 86 Options in the Show Advanced Settings dialog box.

Option	Description
Enable modification	Enables options in the Show Advanced Settings dialog box.
Restore Settings	
Restore Default Host/Credentials	Restores the original settings in the Credentials group box.
Host address	
Use the default repository server address	Sets the repository to the default.
Use the following server address	Enables you to specify another server as the repository.
Credentials	
Username	Specifies the username for the repository server.
Password	Specifies the password for the username.
Confirm Password	Verifies the password you type.

4. Click **Apply**.

Modifying the username or password

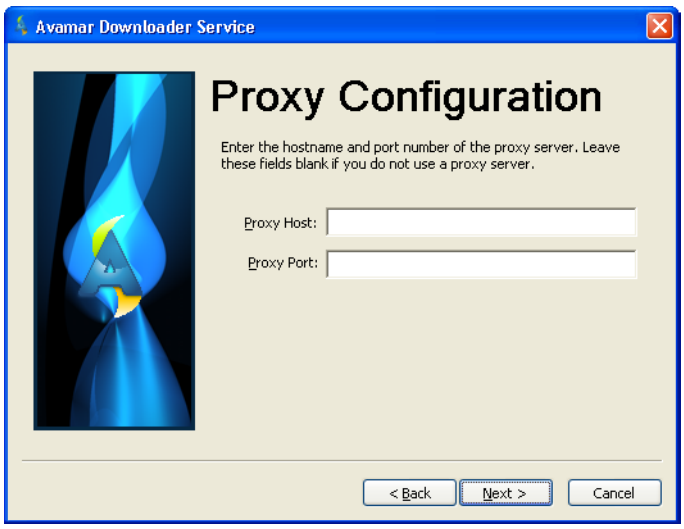
The following procedure modifies the username or password for the proxy host.

1. Click Avamar Downloader Service task tray icon.

   The Welcome! page appears.

2. Click **Next**.

   The Proxy Configuration page appears.



3. (Optional) Complete the settings for the **Proxy Configuration** page:

   a. For **Proxy Host**, type the hostname or the IP address for the proxy server (for example, proxy.example.com or 10.220.330.40).

   b. For the **Proxy Port**, type the port number for the proxy server.

   If the configuration does not use a proxy server, leave both fields blank.

4. Select the system from the Known Systems list and click **Modify**.

   The Avamar Downloader Service - Add Known Systems page appears.

5. Make the necessary changes and click **OK**.

6. Click **Next**.

   The Review Configuration page appears.

7. Review the configuration details, and then click **Finish**.

Removing an Avamar system from the Known Systems list

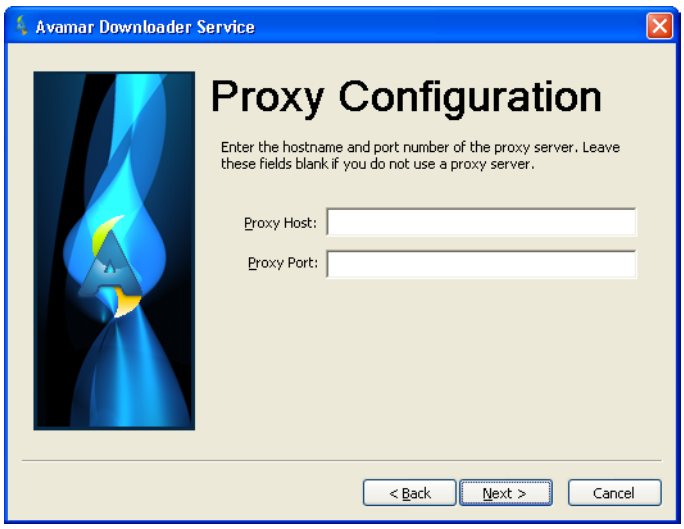
The following procedure removes an Avamar system from the Known Systems list.

1. Click Avamar Downloader Service task tray icon.

   The Welcome! page appears.

2. Click **Next**.

   The Proxy Configuration page appears.



3. (Optional) Complete the settings for the **Proxy Configuration** page:

   a. For **Proxy Host**, type the hostname or the IP address for the proxy server (for example, proxy.example.com or 10.220.330.40).

   b. For the **Proxy Port**, type the port number for the proxy server.

   If the configuration does not use a proxy server, leave both fields blank.

4. Select the system from the Known Systems list and click **Remove**.

   A confirmation dialog box appears.

5. Click **Yes** to remove the system from the Known Systems list.

6. Click **Next**.

   The Review Configuration page appears.

7. Review the configuration details, and then click **Finish**.

Viewing version and copyright information

The following procedure shows the version of the Avamar Downloader Service and copyright information.

1. Right-click the Avamar Downloader Service task tray icon and select **About**.

   The About dialog box appears.

2. Click **OK** to close the **About** dialog box.

Troubleshooting Avamar Downloader Service issues

This topic describes how to resolve common issues with the Avamar Downloader Service.

Not receiving files from the Avamar FTP site

After you click Check for New Packages, the Avamar Downloader Service writes the following error messages to AvamarDownloaderService.log:

```
6/1/2011 13:36:38 PM [380] FtpOpenFile failed (errno=12002)
   6/1/2011 13:36:38 PM [380] SendManifest failed
```

Microsoft Windows 7 security rules block port 21, which prevents the Avamar Downloader Service from requesting files from the Avamar FTP site (ftp.avamar.com).

To resolve this issue, define an inbound rule in the Windows Firewall with Advanced Security interface. "Defining an inbound rule for Microsoft Windows 7 hosts" on page 441 provides instructions.

Downloading a package fails

If the utility node or the single-node server cannot access the Windows host computer, a message similar to the following can appear when you try to download a package:

```
The selected package cannot be downloaded.
```

To correct this problem, add a new line to the /etc/hosts file on the utility node and enter the Windows computer's IP address, fully-qualified name, and short name. See the following sample entry:

```
10.6.172.50         avamar-1.example.com          avamar-1
```

Temporary IPv6 addresses cause package download to fail

The Avamar Downloader Service fails to download a package when temporary IPv6 addresses are in use on all operating systems. The download process fails with "connection refused" errors.

The connection refused errors are due to the use of temporary IPv6 addresses. Windows Vista, Windows 2008 Server, or later versions of Windows use temporay IPv6 addresses by default.

To work around this issue, block temporary IPv6 addresses on the system that runs the Avamar Downloader Service. Type the following `netsh` commands from the Command Prompt window:

```
netsh interface ipv6 set privacy state=disabled store=active
netsh interface ipv6 set privacy state=disabled store=persistent
netsh interface ipv6 set global randomizeidentifiers=disabled
 store=active
netsh interface ipv6 set global randomizeidentifiers=disabled
 store=persistent
```

Type each command on a single line.

Uninstalling the Avamar Downloader Service

The following procedure uninstalls the Avamar Downloader Service.

1. Exit any running applications.
2. Uninstall the software:
   - On Windows Server 2003, Windows XP, or Windows Vista, use **Add/Remove Programs**.
   - On Windows Server 2008 or Windows 7, use **Programs and Features**.

The uninstall process removes all files including file cache contents and configuration items.

Installing packages from System Maintenance

System Maintenance is an Avamar feature that extends Avamar Enterprise Manager functionality by enabling you to perform the following tasks:

- Download OS patches, hotfixes, and workflow packages to Avamar servers.
- Install OS patches, hotfixes, and workflow packages on Avamar servers.
- View history information for all packages installed on Avamar servers.
- Delete packages from Avamar servers after a successful installation.

Select System Maintenance from any other page in Avamar Enterprise Manager to view the System Maintenance page.

System Maintenance includes the following tabs:

- **Maintenance**—Downloads and installs workflow packages.
- **SW Updates**—Downloads and installs patches and hotfixes.
- **History**—Displays status information for all packages that have been installed.

Microsoft Windows browser requirements

On Microsoft Windows, the Microsoft Internet Explorer or Mozilla Firefox browser requires a minimum of 2 GB of RAM for the System Maintenance page.

EMC Customer Support account

System Maintenance provides a special password-protected account for EMC Customer Support. This account enables EMC Customer Support access to restricted installation packages for the Avamar server that only EMC Customer Support can install. The gray lock icon in the tab bar provides access to the EMC Customer Support account.

NOTICE

Only EMC Customer Support should access the EMC Customer Support account.

Maintenance and SW Updates tabs

The Maintenance and SW Updates tabs share the basic page layout described in Table 87 on page 454.

Table 87 Item and column descriptions

Item or column	Description	
	Indicates that packages are available for installation.	
Systems pane	Provides package availability and operational status about each Avamar server.	
AVP		Indicates that one or more packages are available to download and install on the Avamar server.
Status		Indicates that the Avamar Installation Manager is running on the Avamar server.
		Indicates one of the following: • The Avamar server is running a version of the Avamar server software before 6.0. • The installation process has encountered an issue and requires the user's response.
		Indicates that an Avamar package installation is in progress.
System	Displays the Fully Qualified Domain Name for the Avamar server.	
Version	Displays the version of the Avamar server software.	
Package List pane	Displays all available installation packages for the Avamar server.	
Grouping list	Enables you to group packages by type: Show All or Hotfix.	
Sort by list	Enables you to sort the packages by title, status, or priority.	
Download button	Indicates that a package is available to download to the local repository. Clicking Download disables the button until the download transfer completes. Then the button changes to Install. **Notice:** You can download multiple packages simultaneously, but install only one package at a time. You can also install a package while you are downloading packages.	
Install button	Starts the installation process. The Install button appears only after the package has been downloaded to the local repository.	
Monitor button	Displays the Installation Progress page.	
Delete button	Deletes the package from the local repository.	
Continue button	Indicates that a package is in the initial installation phase (deployed but not yet started). Clicking Continue displays the Installation Setup page.	

NOTICE

If you accidently close the browser during the installation of a package, the installation does not stop. To resume the installation, open a new browser window and log in to the Avamar Enterprise Manager. The installation continues from the point it was when the browser window closed.

Installing workflow packages from the Maintenance tab

The Avamar Enterprise Manager displays the Maintenance tab only when workflow packages are available for installation. Otherwise, the Avamar Enterprise Manager does not display the Maintenance tab.

The following procedure installs workflow packages.

1. Open a web browser and log in to Avamar Enterprise Manager:
   a. In the web browser, type the following command:

      http://*Avamar-server***/em**

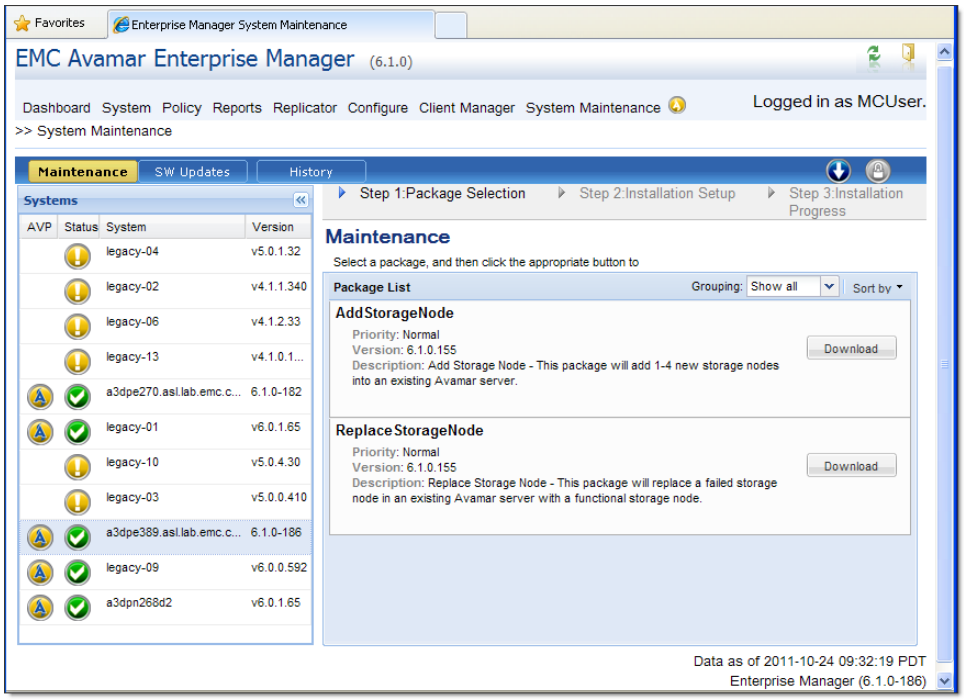
      where *Avamar-server* is the hostname of the Avamar server.

      The EMC Avamar Enterprise Manager login page appears.
   b. Type the Avamar administrator user account in the **User Name** field and the password in the **Password** field.
   c. Click **Log On**.

      The EMC Avamar Enterprise Manager dashboard page appears.
2. Click **System Maintenance**.

   The System Maintenance page appears.

The Maintenance tab appears if workflow packages are available for any Avamar server in the configuration.



3. Click **Maintenance**.
4. Select a system from the **Systems** list.

   Workflow packages that are available for the system you selected appear in the Package List.
5. Install a workflow package:

   a. If the workflow package is not yet in the local repository, a **Download** button appears. Click **Download** to download the package to the local repository. Otherwise, continue to step b.

      After the download completes, the user interface:

      – Replaces the **Download** button with the **Install** button.

      – Provides a help button, which contains installation information specific to the workflow package.

      NOTICE

      Not all workflow packages include a help button.

   b. To view help information for the workflow package, click the help button.

   c. To start the installation, click **Install**.

      The background color for the package changes to yellow and the initialization begins.

      When the initialization process finishes, the Installation Setup page appears.

6. Provide installation setup information.

   Some packages do not require setup information.

7. Click **Continue**.

   The Installation Progress page appears. The following figure shows the installation progress for the add storage node workflow package.

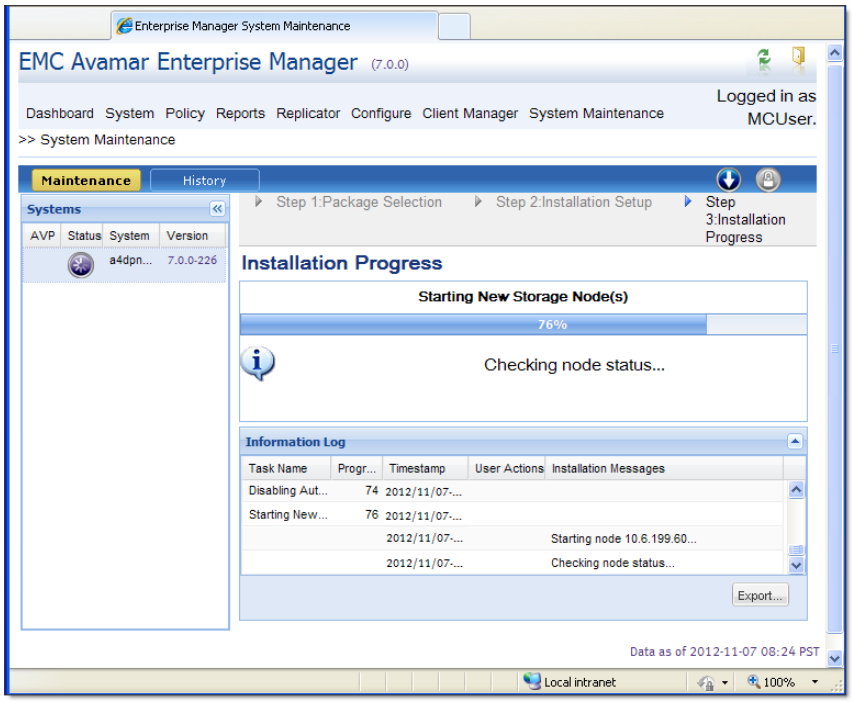


Table 88 on page 457 describes the Installation Progress page.

Table 88 Installation Progress page item descriptions

Item	Description
Progress bar	Displays the installation's progress as a percentage for each task.
Status Messages	Displays the name of the current task 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. • Displays action buttons relevant to the problem. For example: Skip This Task, Undo This Task, Undo All Changes, or Call EMC support.
Information Log table	Provides details about each installation task.
Export	Click **Export** to save log information to a file. The Export as dialog box appears. 1. Select one of command buttons: **Excel** or **PDF**. 2. Follow the prompts to save the log information to a file.

8. Respond to all installation prompts.

   After the installation completes, the user interface performs the following tasks:

   - Replaces the **Install** button with the **Run** button.

     The Run button enables you to run the workflow package again.

   - Adds a **Delete** button. "Deleting packages" on page 459 provides more information about the use of the **Delete** button.

Installing patch and hotfix packages from the SW Updates tab

The following procedure installs patch and hotfix packages.

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Click **System Maintenance**.

   The System Maintenance page appears.
3. Click **SW Updates**.

   The SW Updates page appears.
4. Select an Avamar server from the **Systems** list.

   If packages are available, they appear in the Package List.
5. (Optional) Filter the list of packages by selecting one of the options from the **Show** list.
6. Select a package.
7. Install the package on the Avamar server:

   a. If a package is not yet in the local repository, a **Download** button appears. Click **Download** to download the package to the local repository. Otherwise, continue to step b.

      After the download completes, the **Download** button changes to the **Install** button.

   b. Click the **Install** button to start the installation.

      The background color for the package changes to yellow and the initialization begins.

      When the initialization process finishes, the Installation Setup page appears.
8. Provide installation setup information, if requested.

   NOTICE

   Installation setup requirements are specific to the type of package. Some packages do not require any installation setup.

9. Provide advanced settings, if required:
   a. Select **Show advanced settings** to view optional settings.
   b. Provide the requested information.

   NOTICE

   Advanced settings are specific to the type of package. Some packages do not have any advanced settings.

10. Click **Continue**.

    The Installation Progress page appears. Table 89 on page 459 describes this page.

Table 89 Installation Progress page item descriptions

Item	Description
Progress bar	Displays the installation's progress as a percentage.
Status Messages	Displays the name of the current task in progress 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. • Displays action buttons relevant to the problem. For example: Skip This Task, Undo This Task, Undo All Changes, or Call EMC support.
Installation Logs table	Provides details about each installation task.
Export	Click **Export** to save log information to a file. The Export as dialog box appears. 1. Select one of command buttons: **Excel** or **PDF**. 2. Follow the prompts to save the log information to a file.

11. Respond to all installation prompts.

Deleting packages

After you successfully install a package, you can delete the package from Package List. After a successful installation, the AvInstaller service automatically deletes the package from the packages folder on the Avamar system.

NOTICE

Only EMC Customer Support can delete restricted packages.

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Click **System Maintenance**.

   The System Maintenance page appears.

3. Click the appropriate tab.
   - Click **SW Updates** to show hotfix and patch packages.
   - Click **Maintenance** to show workflow packages.

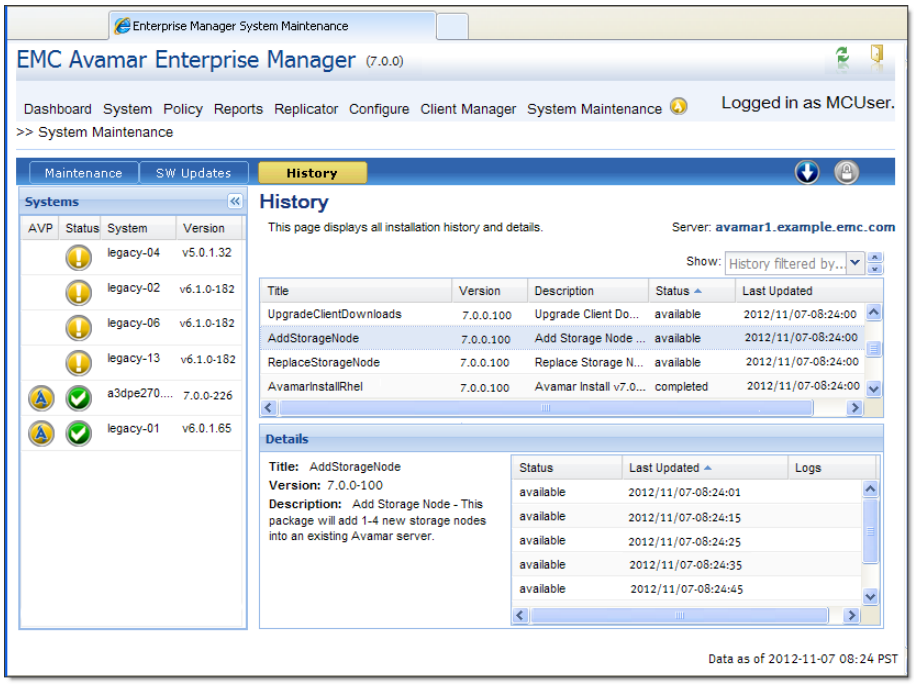
     The **Maintenance** tab only appears if one or more workflow packages are available for the Avamar servers in the configuration.
4. Select a system from the **Systems** list.

   If packages are available for deletion, a Delete button appears.
5. Click **Delete** to delete the package.

   A Confirmation dialog box appears.
6. In the **Confirmation** dialog box, click **Yes** to confirm the package deletion.

Viewing installation history information

The History page displays a table that contains installation history for all packages. The default sort order of the table is ascending order based on the date in the Last Updated column. The most recently installed package is listed as the last item in the table.



From the History page you can perform the following tasks:

- Toggle the sort order from ascending to descending by clicking on the heading in any column.

  An up-arrow or down-arrow icon appears next to the heading to indicate the column's sort order.

- Filter the history information in the table by selecting a filter option from the Show list box (upper right corner).

- Show or hide column headings by clicking the arrow icon in a column heading to open the menu, and then by selecting or clearing column headings from the Columns menu option.

Table 90 on page 461 describes the column headings in the History table.

Table 90 History table column information

Column heading	Description
Title	The name of the package.
Version	Version of Avamar server software.
Description	A brief description of the package.
Status	The current status of the package: • Available—The package is in the manifest and is available to download. • Completed—The package installation completed. • Processing—A package installation is in progress. • Ready—The package is ready to install. • Removed—The package has been deleted from the Avamar grid.
Last Updated	The date and time of the last status update.

To view the History page:

1. Open a web browser and log in to Avamar Enterprise Manager.
2. Click **System Maintenance**.

   The System Maintenance page appears.
3. Click **History**.

   The History page appears.
4. Select a system from the **Systems** list.

   All packages for the selected system appear in the History table.

   NOTICE

   To view a subset of packages for a system, you can set a filter. Click the arrow next to the **Show** list box and select a filter option.
5. Click a row in the **History** table to view more details about a specific package.

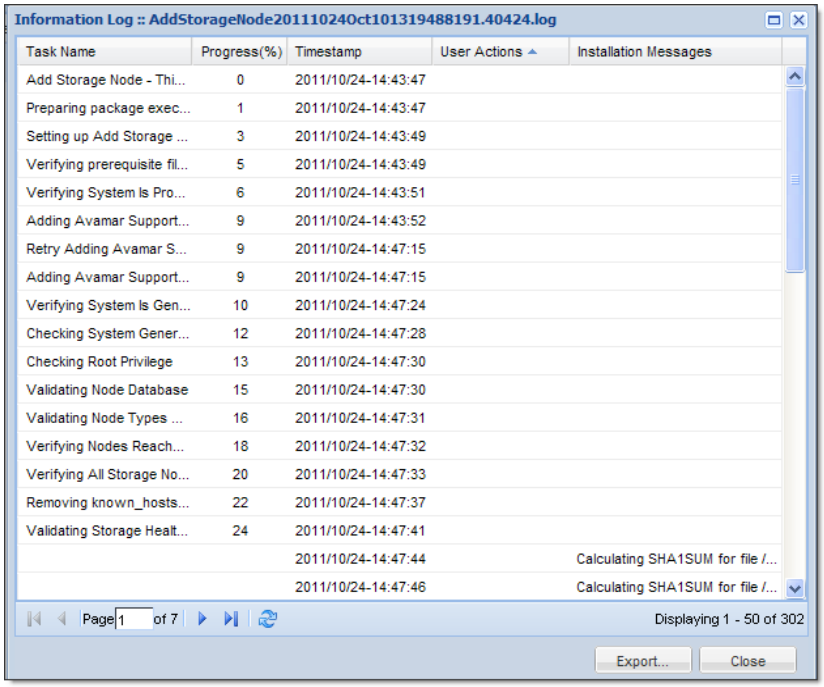
Table 91 on page 462 describes the column headings in the Details table.

Table 91 Detail table column descriptions

Column heading	Description
Status	Status details for a package: • Available—The package is in the manifest and is available to download. • Ready—The package is ready to install. • Deployed—The start of the installation initialization. • Deploying—The start of the package deployment. • Processing—The start of the package installation. • Completed—The completion of the package installation. • Removed—The removal of the package.
Last Updated	The corresponding date and time of the package status message.
Logs	Displays a Logs button for packages with a processing status. Clicking **Logs** opens a pop-up windows that provides details about the tasks performed to install the package.

6. In the **Details** table, click **Logs** to view log information about specific tasks.

   A dialog box appears. The following figure shows example log information.



   To enlarge the window, click the icon (upper right corner).

7. To save the log information to a file, click **Export**.

   The Export as dialog box appears.

8. Click one of format buttons:
   - Click **Excel** to open or save the file in Microsoft Excel format.
   - Click **PDF** to view the file in Adobe Acrobat Reader as a PDF file.
9. Return to the **Export** window and click **Close**.

CHAPTER 18
Client System Recovery

The following topics describe how to restore a supported Windows, Red Hat Linux, CentOS Linux, SUSE Linux, or Oracle Solaris client system back to its original system state:

- Windows client system recovery 466
- Red Hat and CentOS Linux system recovery 466
- SUSE Linux system recovery 474
- Oracle Solaris system recovery 482

Windows client system recovery

The following table lists the locations of client system recovery information for Windows operating systems.

Table 92 Windows client system recovery publications

Topic	Publication
Windows Server 2008 and Windows 7 disaster recovery	*EMC Avamar for Windows Server User Guide*
Windows Server 2003 disaster recovery	*EMC Avamar for Windows Server User Guide*
Windows Server 2003 System Recovery using NT Backup	*Restoring Windows Server 2003 System State Using NTBackup and Avamar Technical Note*
Windows XP and 2000 System Recovery using NT Backup	*EMC Avamar for Windows Server User Guide*

Red Hat and CentOS Linux system recovery

This procedure describes how to restore a Red Hat or CentOS Linux client system to its original system state.

Prerequisites

Ensure that the environment meets the following prerequisites before you perform system recovery for a Red Hat or CentOS Linux client:

- A complete and recent Avamar backup of the original client local file system must exist on the Avamar server.
- The recovery destination disk must be connected to the recovery target client.
- A minimal installation of a compatible operating system must have been performed on the recovery target client.

Reconstruct partition table

Before proceeding any further, you must reconstruct the partition table used in the original Avamar backup by executing an **avtar --showlog** mounts command on a temporary client computer, then examining the output to determine the number and size of partitions to create during the target recovery client minimal operating system installation.

1. Locate the backup to use for the system state recovery:
   a. In Avamar Administrator, click the **Backup & Restore** launcher button.

      The Backup, Restore and Manage window appears.

   b. Click the **Restore** tab.
   c. In the clients tree, select the original Linux client.
   d. Find the full system backup to use to recover the system state.

e. Note the backup label number.

f. Leave Avamar Administrator open for the remainder of the system state recovery procedure.

2. On a temporary client computer with network connectivity to the Avamar server, open a command shell and log in as root.

3. Type:

```
/usr/local/avamar/bin/avtar --avamaronly --showlog mounts
--server=AVAMARSERVER --id=USERNAME --ap=PASSWORD
--path=/DOMAIN/MyClient --labelnumber=LABEL-NUM
```

where:

- AVAMARSERVER is the Avamar server IP address or fully qualified hostname as defined in DNS.
- /DOMAIN/MyClient is the full location of the original Linux client on the Avamar server.
- USERNAME and PASSWORD are the login credentials for a user account with a sufficient role and privileges to perform a restore operation.
- LABEL-NUM is a label number of the backup to use for the system state recovery.

4. Examine the command output to locate entries beginning with **mount_decision**.

For example:

```
mount_decision: reason="starting_point" fstype="ext3" path="/"
mount_decision: reason="default_backup" fstype="ext3" path="/boot"
mount_decision: reason="default_backup" fstype="ext3" path="/home"
```

These are entries for the mount points on the original system. Earlier in the output, there are entries for each of these mount points.

For example:

```
mount: status="user_directed_backup" path="/" hdev="/dev/root"
kind="ext3" blksize=4096 freeblks=1189334 maxblks=2405872
freefiles=2259654 maxfiles=2432000 dev=2050

mount: status="default_backup" path="/boot" hdev="/dev/sda1"
kind="ext3" blksize=1024 freeblks=183371 maxblks=194442
freefiles=50167 maxfiles=50200 dev=2049

mount: status="default_backup" path="/home" hdev="/dev/sdb1"
kind="ext3" blksize=4096 freeblks=1027161 maxblks=5158925
freefiles=2530548 maxfiles=2621440 dev=2065
```

These entries contain mount point size and path information.

5. Calculate the original file system size or each mount point in bytes by multiplying the blksize value by the maxblks.

NOTICE

Multiplying the blksize value by the maxblks value calculates the free space used on the original device. However, you should create the root partition with an additional 2 GB to 3 GB of free space to ensure sufficient space for the minimal install used for the restore process.

6. Note which paths are mounted from separate file systems.

   This information is required later in the restore process.

Recovery target client preparation

To prepare the new recovery target client before you restore a system from an Avamar backup:

1. Perform a minimal installation of a compatible operating system.

   For purposes of this procedure:

   - Minimal installation means that desktop environment entries such as Desktop - Gnome, should not be selected for installation.
   - In the Customize Now dialog box Base System category, the Base option should be selected. All other options in all other categories should be disabled.
   - Compatible operating system means the same version. For example, if the original client backup on the Avamar server was taken from an RHEL3 client, then RHEL3 must be installed on the recovery target client.
   - Use the information gathered during "Reconstruct partition table" on page 466 to create as many partitions as necessary to replicate the original configuration.

2. (Optional) Following the minimal operating system installation, consider saving a copy of the /etc/fstab file so that it can be compared to the restored /etc/fstab file.
3. Install the Avamar Client for Linux software as described in the *EMC Avamar Backup Clients User Guide*.

Recovery procedure

1. Ensure that the recovery target client has been prepared as described in "Recovery target client preparation" on page 468.
2. Start the recovery target client from the install media (first CD/DVD):
   - If you are running Red Hat or CentOS 4 or 5, then type at the command prompt:

     ```
     linux rescue
     ```

   - If you are running Red Hat or CentOS versions 6.0 and higher, select the **Rescue installed system** option.
3. Follow the onscreen instructions.

   Be sure to enable networking by providing IP address, network mask, default gateway, and DNS server values when prompted. You can use a temporary hostname and IP, or the original information from the machine that you are restoring.
4. Allow the installer to search for installations and mount the /mnt/sysimage file system as read-write.

   This is the target of the restore, and is also referred to as the "recovery destination disk."

Note: You cannot restore the root file system directly to /mnt/sysimage because there is currently no method to restrict the restore operation to only the local partition without traversing network mount points. Therefore, a restore directly to /mnt/sysimage might copy files from all the partitions, and /mnt/sysimage could fill up before all required files were restored.

5. Ensure that /lib, /lib64, /usr/lib, /usr/lib64, /mnt/sysimage/lib, /mnt/sysimage/lib64, and /mnt/sysimage/usr/local/avamar/lib are all present in the LD_LIBRARY_PATH system variable.
6. If any directories are missing from LD_LIBRARY_PATH, add them to the LD_LIBRARY_PATH variable.
7. Create a temporary /tmp/avtar.cmd flag file with a UNIX text editor.

   For example:

   ```
   cd /tmp
   vi avtar.cmd
   --bindir=/mnt/sysimage/usr/local/avamar/bin
   --vardir=/mnt/sysimage/usr/local/avamar/var
   --sysdir=/mnt/sysimage/usr/local/avamar/etc
   --server=AVAMARSERVER
   --account=/DOMAIN/MyClient
   --id=USERNAME
   --ap=PASSWORD
   --target=.
   ```

   where:

   - AVAMARSERVER is the Avamar server IP address or fully qualified hostname as defined in DNS.
   - /DOMAIN/MyClient is the full location of the original Linux client on the Avamar server.
   - USERNAME and PASSWORD are the login credentials for a user account with sufficient role and privileges to perform the restore operation.

8. Restore most of the directories that originally existed under root (/):

   NOTICE

   Do not restore files located on file systems other than the root file system at this time. These directories and files are restored later in this procedure.

   a. Create a temporary restore directory under the client /mnt/sysimage directory and change directory to it by typing:

      For example:

      ```
      mkdir /mnt/sysimage/restore
      cd /mnt/sysimage/restore
      ```

   b. Restore the contents of the root file system from the backup by typing the following command on a single command line:

      ```
      /mnt/sysimage/usr/local/avamar/bin/avtar.bin -x
      --flagfile=/tmp/avtar.cmd --labelnumber=LABEL-NUM
      [--exclude=./boot --exclude=./home] /
      ```

      where LABEL-NUM is the label number of the backup to use for the system state recovery.

      Use **--exclude=PATH** options to exclude paths that were identified as separate mount points during "Reconstruct partition table" on page 466. These directories and files are separately restored later in this procedure.

      The first two **--exclude** options in the previous command are included as an example. These must be replaced with options appropriate to the machine being restored. Exclude options must be specified relative to the root of the original backup. For example, **--exclude=./boot** instead of **--exclude=/boot**.

   c. For each directory that was restored, delete the original directory from /mnt/sysimage, and move the restored directory from the /mnt/sysimage/restore directory to /mnt/sysimage.

      For example:

      ```
      rm -rf /mnt/sysimage/etc
      mv /mnt/sysimage/restore/etc /mnt/sysimage/etc
      ```

   d. Repeat step c for each directory successfully restored to /mnt/sysimage/restore.

9. Restore individual files in the root (/) directory:

   a. Change directory to /mnt/sysimage/restore by typing.

      ```
      cd /mnt/sysimage/restore
      ```

   b. Restore the individual files in the root (/) directory by typing:

      ```
      mv ./* /mnt/sysimage
      mv ./.* /mnt/sysimage
      ```

10. Restore other mount points:

    a. Check that file systems are mounted as expected by typing the following on the command line:

       ```
       df -h
       ```

    b. Compare the output to the expected set of mounted file systems.

    c. If there are discrepancies, mount the devices onto the appropriate mount points, as determined during "Reconstruct partition table" on page 466.

    d. Change directory into each mount point.

       For example:

       ```
       cd /mnt/sysimage/home
       ```

    e. Create a temporary restore directory, then change directory into it:

       For example:

       ```
       mkdir ./restore
       cd ./restore
       ```

    f. Restore the contents of the mount point by typing the following:

       ```
       /mnt/sysimage/usr/local/avamar/bin/avtar.bin -x
       --flagfile=/tmp/avtar.cmd --labelnumber=LABEL-NUM /home
       ```

       where:

       – LABEL-NUM is the label number noted in "Reconstruct partition table" on page 466.

       – /home is an example mount point.

    g. Return to the mount point directory, and delete all the files besides the restore directory.

       For example:

       ```
       alias ls=/usr/bin/ls
       cd /mnt/sysimage/home; rm -rf `ls --hide restore`
       rm -rf ./.*
       ```

    h. Change directory to the restore directory, then move the contents into the appropriate place in the mount point by typing:

       ```
       cd ./restore;mv `ls -A ./` ..
       ```

    i. Remove the restore directory by typing:

       ```
       cd ..
       rmdir restore
       ```

    j. Repeat steps d—i for each remaining mount point.

11. Perform final check and reboot:

    a. Inspect /mnt/sysimage/etc/fstab, and verify that there are valid statements for each file system to be mounted on the new system.

       There are three ways that devices might be listed in the fstab file: device path, volume label, and Universally Unique Identifier (UUID).

       You can determine this information about the file systems by typing:

       /mnt/sysimage/lib/udev/vol_id DEVICE_PATH

       where DEVICE_PATH is the /dev path to the device.

       If that program is not present on the system, type:

       /mnt/sysimage/sbin/blkid DEVICE_PATH

       If you had to manually recreate partitions during the minimal-system install, the device UUIDs might have changed. Update the device UUIDs in /mnt/sysimage/etc/fstab. If some volumes are missing expected labels, set the label by typing:

       /mnt/sysimage/sbin/e2label DEVICE_PATH LABEL

       where:

       – DEVICE_PATH is the /dev path for the device.
       – LABEL is the desired label.

    b. Re-examine the fstab carefully at this point.

       The restored system does not boot properly if the fstab entries do not exactly match the storage device configuration, and the rescue system on the install media has difficulty discovering which file systems to mount to /mnt/sysimage.

       Note: If you saved a reference copy of the fstab file during "Recovery target client preparation" on page 468, you can probably find the disk information in that file. For systems with few manual modifications to their restored fstab file, it might be possible to use the reference fstab file instead of the restored copy of the file.

    c. Verify that no more files are present in /mnt/sysimage/restore by typing:

       ls -al /mnt/sysimage/restore

    d. If the directory is empty, remove it by typing:

       rmdir /mnt/sysimage/restore

    e. If the command fails because the directory is not empty, there might be directories that you failed to move in step 8.

    f. If so, ensure that they get moved to their proper restore locations by performing steps 8—9.

12. Exit the command shell and reboot the system by typing:

    exit

    If rebooting a Red Hat or CentOS 6 system, a menu appears.

13. Select **reboot**, then **OK** and press **Enter**.

    The system restarts.

14. Eject the CD and boot normally.

15. Confirm correct client operation.

Troubleshooting

If the restored system does not boot at the end of the restore procedure, then the version of GRUB installed by the minimal OS might be too dissimilar to the version previously used on the machine. To resolve this issue:

1. Boot into the restore environment as described in steps 2—4 of the "Recovery procedure" on page 468.
2. If the startup process cannot find the restored OS, then its fstab is probably misconfigured. Mount the partitions manually, and correct the contents of the file, as described in step 11of the "Recovery procedure" on page 468.
3. Reinstall GRUB by typing:

   ```
   chroot /mnt/sysimage
   grub-install DEVICE
   ```

   where DEVICE is the boot device (for example,/dev/sda).

4. Exit the chroot environment by typing:

   exit

5. Exit the command shell and reboot the system by typing:

   exit

   If rebooting a Red Hat or CentOS 6 system, a menu appears.

6. Select **reboot**, then **OK** and press **Enter**.

   The system restarts.

7. Eject the CD and boot normally.

If the OS detects that you have restored the system to new hardware, it might revert the network settings to defaults (for example, DHCP name resolution instead of static IP).

You can recover the previous network settings by manually reconfiguring the settings.

You can examine the previous settings by opening the .bak files in /etc/sysconfig/network-scripts in a text editor.

These files contain useful information, but should not be used in the current configuration in an unmodified form, since they include MAC address information from the previous hardware.

SUSE Linux system recovery

This procedure describes how to restore a SUSE Linux client system to its original system state.

Prerequisites

Ensure that the environment meets the following prerequisites before you perform system recovery for a SUSE Linux client:

- A complete and recent Avamar backup of the original client local file system must exist on the Avamar server.
- The recovery destination disk must be connected to the recovery target client.
- A minimal installation of a compatible operating system must have been performed on the recovery target client.

Reconstruct partition table

Before proceeding any further, you must reconstruct the partition table used in the original Avamar backup. This is accomplished by executing an **avtar --showlog** mounts command on a temporary client, then examining the output to determine the number and size of partitions to create during the target recovery client minimal operating system installation.

1. Locate the backup to use for the system state recovery:
   a. In Avamar Administrator, click the **Backup & Restore** launcher button.

      The Backup, Restore and Manage window appears.

   b. Click the **Restore** tab.
   c. In the clients tree, select the original Linux client.
   d. Find the full system backup to use to recover the system state.
   e. Note the backup label number.
   f. Leave Avamar Administrator open for the remainder of the system state recovery procedure.
2. Open a command shell and log in as root.

3. Type:

   ```
   /usr/local/avamar/bin/avtar --avamaronly --showlog mounts
   --server=AVAMARSERVER --id=USERNAME --ap=PASSWORD
   --path=/DOMAIN/MyClient --labelnumber=LABEL-NUM
   ```

   where:

   - AVAMARSERVER is the Avamar server IP address or fully qualified hostname as defined in DNS.
   - /DOMAIN/MyClient is the full location of the original Linux client on the Avamar server.
   - USERNAME and PASSWORD are the login credentials for a user account with sufficient role and privileges to perform a restore operation.
   - LABEL-NUM is a label number of the backup to use for the system state recovery.

4. Examine the command output to locate entries beginning with **mount_decision**.

   For example:

   ```
   mount_decision: reason="starting_point" fstype="ext3" path="/"
   mount_decision: reason="default_backup" fstype="ext3" path="/boot"
   mount_decision: reason="default_backup" fstype="ext3" path="/home"
   ```

   These are entries for the mount points on the original system. Earlier in the output, there are entries for each of these mount points.

   For example:

   ```
   mount: status="user_directed_backup" path="/" hdev="/dev/root"
   kind="ext3" blksize=4096 freeblks=1189334 maxblks=2405872
   freefiles=2259654 maxfiles=2432000 dev=2050
   mount: status="default_backup" path="/boot" hdev="/dev/sda1"
   kind="ext3" blksize=1024 freeblks=183371 maxblks=194442
   freefiles=50167 maxfiles=50200 dev=2049
   mount: status="default_backup" path="/home" hdev="/dev/sdb1"
   kind="ext3" blksize=4096 freeblks=1027161 maxblks=5158925
   freefiles=2530548 maxfiles=2621440 dev=2065
   ```

   These entries contain mount point size and path information.

5. Calculate the original file system size or each mount point in bytes by multiplying the blksize value by the maxblks.

   NOTICE

   Multiplying the blksize value by the maxblks value calculates the free space used on the original device. However, you should create the root partition with an additional 2 GB to 3 GB of free space to ensure sufficient space for the minimal install used for the restore process.

6. Note which paths are mounted from separate file systems. This information is required later in the restore process.

Recovery target client preparation

Before restoring system from the Avamar backup, prepare the new recovery target client by performing the following:

1. Perform a minimal installation of a compatible operating system.

   For purposes of this procedure:

   - Minimal installation means that only Base System and Minimal System (Appliances) packages are installed from the Software selection page. All other packages should be deselected so that they are not installed.
   - Compatible operating system means the same version. For example, if the original client backup on the Avamar server was taken from an SLES10 client, then SLES10 must be installed on the recovery target client.
   - Use the information gathered during "Reconstruct partition table" on page 474 to create as many partitions as necessary to replicate the original configuration.

2. (Optional) Following the minimal operating system installation, consider saving a copy of the /etc/fstab file so that it can be compared to the restored /etc/fstab file.
3. Install the Avamar Client for Linux software, as described in the *EMC Avamar Backup Clients User Guide*.

Recovery procedure

1. Ensure that the recovery target client has been prepared as described in "Recovery target client preparation" on page 476.
2. Start the recovery target client from the install media and select **Rescue System**.
3. Open a command shell on the recovery target client and log in as root.
4. Mount the root partition created in the minimal install to /mnt by typing:

   ```
   mount /dev/sda# /mnt
   ```

   where /dev/sda# is the device containing the root file system.

   Note: If the drive was configured to use Linux Logical Volume Management, the root device might be in the form of /dev/VolGroup##/LogVol##.

5. Rebind the pseudo-file systems into the /mnt tree by typing:

   ```
   mount --rbind /proc /mnt/proc
   mount --rbind /sys /mnt/sys
   mount --rbind /dev /mnt/dev
   ```

6. Change the current file system root by typing:

   ```
   chroot /mnt
   ```

7. Start the network as configured in the prerequisites by typing:

   ```
   rcnetwork start
   ```

8. Mount the auto-mount file systems and verify that the correct file systems were mounted by typing:

   ```
   mount -a;df -h
   ```

9. If any file systems are missing (for example, if /boot is not set to auto-mount), manually mount them to their correct locations using additional mount commands.
10. Exit the chroot environment by typing:

    ```
    exit
    ```

11. Copy the network name resolution file from the chroot environment into the working restore environment by typing:

    ```
    cp /mnt/etc/resolv.conf /etc/resolv.conf
    ```

12. Ensure that /lib, /lib64, /usr/lib, /usr/lib64, /mnt/lib, /mnt/lib64, and /mnt/usr/local/avamar/lib are all present in the LD_LIBRARY_PATH system variable.
13. If any directories are missing from LD_LIBRARY_PATH, add them to the LD_LIBRARY_PATH variable.
14. Create a temporary /tmp/avtar.cmd flag file with a UNIX text editor such as vi or Emacs.

    For example:

    ```
    cd /tmp
    vi avtar.cmd
    --bindir=/mnt/usr/local/avamar/bin
    --vardir=/mnt/usr/local/avamar/var
    --sysdir=/mnt/usr/local/avamar/etc
    --server=AVAMARSERVER
    --account=/DOMAIN/MyClient
    --id=USERNAME
    --ap=PASSWORD
    --overwrite=always
    --target=.
    ```

    where:

    - AVAMARSERVER is the Avamar server IP address or fully qualified hostname as defined in DNS.
    - /DOMAIN/MyClient is the full location of the original Linux client on the Avamar server.
    - USERNAME and PASSWORD are the login credentials for a user account with sufficient role and privileges to perform the restore operation.

15. Restore most of the directories that originally existed under root (/):

    NOTICE

    Do not restore files located on file systems other than the root file system at this time. These directories and files are restored later in this procedure.

    a. Create a temporary restore directory under the client /mnt directory and change directory to it by typing:

    ```
    mkdir /mnt/restore
    cd /mnt/restore
    ```

    b. Restore the contents of the root file system from the backup by typing the following command on a single command line:

    ```
    /mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd
    --labelnumber=LABEL-NUM [--exclude=./boot --exclude=./home] /
    ```

    where LABEL-NUM is the label number noted in "Reconstruct partition table" on page 474.

    Use **--exclude=PATH** options to exclude paths that were identified as separate mount points during "Reconstruct partition table" on page 474. These directories and files are separately restored later in this procedure.

    The first two **--exclude** options in the previous command are included as an example. These must be replaced with options appropriate to the machine being restored. Exclude options must be specified relative to the root of the original backup. For example, **--exclude=./boot** instead of **--exclude=/boot**.

    c. For each directory that was restored, delete the original directory from /mnt, and move the restored directory from the /mnt/restore directory to /mnt.

    For example:

    ```
    rm -rf /mnt/etc
    mv /mnt/restore/etc /mnt/etc
    ```

    d. Repeat step c for each directory successfully restored to /mnt/restore.

16. Restore individual files in the root (/) directory:

    a. Change directory to /mnt/restore by typing.

    ```
    cd /mnt/restore
    ```

    b. Restore the individual files in the root (/) directory by typing:

    ```
    mv ./* /mnt
    mv ./.* /mnt
    ```

17. Restore other mount points:

    a. Check that file systems are mounted as expected by typing:

    ```
    df -h
    ```

    b. Compare the output to the expected set of mounted file systems.

    c. If there are discrepancies, mount the devices onto the appropriate mount points, as determined during "Reconstruct partition table" on page 474.

d. Change directory to each mount point.

   For example:

   ```
   cd /mnt/home
   ```

e. Create a temporary restore directory, then change to that directory:

   ```
   mkdir ./restore
   cd ./restore
   ```

f. Restore the contents of the mount point by typing:

   ```
   /mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd
   --labelnumber=LABEL-NUM /home
   ```

   where:

   – LABEL-NUM is a label number of the backup to use for the system state recovery.

   – /home is an example mount point.

g. Return to the mount point directory, then delete all files except for the restore directory.

   For example:

   ```
   alias ls=/bin/ls
   cd /mnt/home; rm -rf `ls --hide restore`
   rm -rf ./.*
   ```

h. Change directory to the restore directory, then move the contents into the appropriate place in the mount point by typing:

   ```
   cd ./restore;mv `ls -A ./` ..
   ```

i. Remove the restore directory by typing:

   ```
   cd ..
   rmdir restore
   ```

j. Repeat steps d through i for the remaining mount points.

18. Perform a final check and reboot:

    a. Inspect /mnt/etc/fstab, and verify that there are valid statements for each file system to be mounted on the new system.

       There are three ways that devices might be listed in the fstab file: device path, volume label, and Universally Unique Identifier (UUID).

       You can determine this information about the file systems by typing:

       ```
       /mnt/lib/udev/vol_id DEVICE_PATH
       ```

       where DEVICE_PATH is the /dev path to the device.

If you had to manually re-create partitions during the minimal-system install, the device UUIDs might have changed. Update the device UUIDs in /mnt/etc/fstab. If some volumes are missing expected labels, set the label by typing:

/mnt/sbin/e2label DEVICE_PATH LABEL

where:

- DEVICE_PATH is the /dev path for the device.
- LABEL is the desired label.

b. Re-examine the fstab carefully at this point.

The restored system does not boot properly if the fstab entries do not exactly match the storage device configuration, and the rescue system on the install media has difficulty discovering which file systems to mount to /mnt.

Note: If you saved a reference copy of the fstab file during "Recovery target client preparation" on page 476, you can probably find the disk information in that file. For systems with few manual modifications to their restored fstab file, it might be possible to use the reference fstab file instead of the restored copy of the file.

---

c. Verify that no more files are present in /mnt/restore by typing:

ls -al /mnt/restore

d. If the directory is empty, remove it by typing:

rmdir /mnt/restore

e. If the command fails because the directory is not empty, there might be directories that you failed to move in step 15.

f. If so, perform steps 15 and 16 to move the directories to the proper restore location.

19. Reboot the system by typing:

reboot

20. Eject the CD and boot normally.

21. Confirm correct client operation.

Troubleshooting

If the restored system does not boot at the end of the restore procedure, then the version of GRUB installed by the minimal OS might be too dissimilar to the version previously used on the machine.

To resolve this issue:

1. Boot into the restore environment as described in step 2 through step 8 of "Recovery procedure" on page 476.
2. Reinstall GRUB by typing:

   grub-install DEVICE

   where DEVICE is the boot device (for example,/dev/sda).
3. Exit the chroot environment by typing:

   exit
4. Reboot the system by typing:

   reboot
5. Eject the CD and boot normally.

   If the OS detects that you have restored the system to new hardware, it might revert the network settings to defaults (for example, DHCP name resolution instead of static IP).

   You can recover the previous network settings by manually reconfiguring the settings.

   You can examine the previous settings by opening the .bak files in /etc/sysconfig/network-scripts in a text editor.

   These files contain useful information, but should not be used in the current configuration in an unmodified form, since they include MAC address information from the previous hardware.

Oracle Solaris system recovery

This procedure describes how to restore a Oracle Solaris client system to its original system state.

Prerequisites

Ensure that the environment meets the following prerequisites before you perform Solaris client system recovery.

Backup containing critical system files

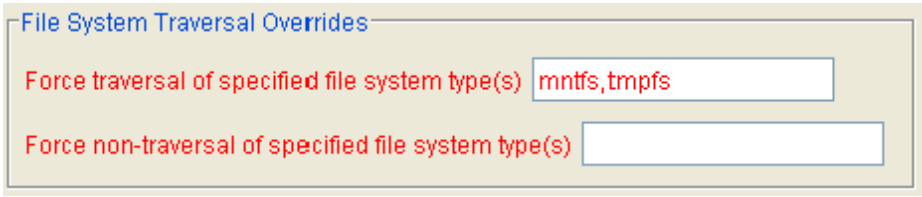
To successfully restore a Oracle Solaris client system to its original system state, there must be an Avamar backup containing the entire local file system and the following critical system files and virtual file systems. This is accomplished by forcing traversal of the targets listed in the following table during a backup.

Table 93 Target locations

Target	Description
mntfs	/etc/svc/volatile
tmpfs	/etc/mnttab

To ensure that these targets are included in a backup:

- In Avamar Administrator, explicitly add these targets in an on-demand backup or dataset by specifying **mntfs,tmpfs** in the **Force traversal of the specified file system type(s)** box in the plug-in options, as shown in the following figure:



- Specify **--forcefs="mntfs,tmpfs"** on the **avtar** command line.

You can also optionally include any of the following other system directories and virtual file systems in a backup by forcing traversal of the targets in the following table.

Table 94 Other system directories and virtual file systems (page 1 of 2)

Target	Description
cachefs	Solaris Cache File System.
fdfs	Solaris File Descriptor File System.
fifofs	Solaris FIFO File System.
lofs	Solaris Loopback File System (local NFS).
namefs	Solaris Name File System.
proc	Solaris /proc directory.
procfs	Solaris Process Access File System.

Table 94 Other system directories and virtual file systems (page 2 of 2)

Target	Description
specfs	Solaris Device Special File System.
swapfs	Solaris Swap File System.
tfs	Solaris Translucent File System.

Available /var and /opt file systems

If the client you are attempting to recover previously used network mounted /var and /opt file systems, make every effort to mount and use those same network mounted /var and /opt file systems during system recovery.

If this is not possible, install a minimal version of Solaris on the client hard disk drive to create local /var and /opt directories.

Other file systems

If you are using zfs or any other add-on file system, ensure that these file systems are properly re-created and mounted before beginning system recovery.

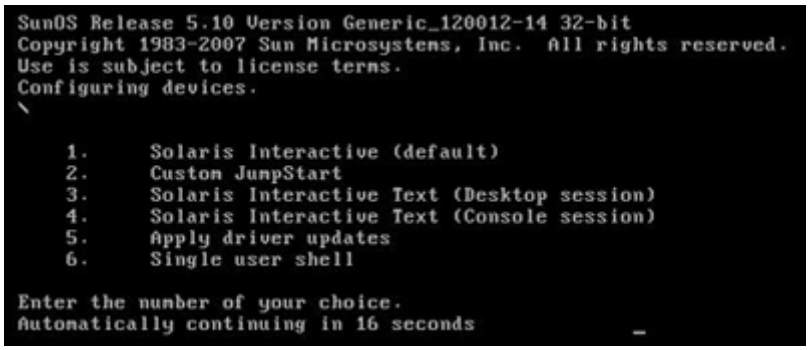
Procedure

To recover a Oracle Solaris client system:

1. Boot from CDROM by typing:

   reboot -- cdrom

2. (Solaris 11 and 10 only) If you are restoring a Solaris 11 or 10 client, at the boot options menu, select either option **3. Solaris Interactive Text (Desktop session)** or option **4. Solaris Interactive Text (Console session)**.



3. Proceed through the prompts, providing the client hostname, IP address, default gateway, and corporate DNS server name when prompted to do so.

4. Do one of the following:
   - If you are restoring a Solaris 8 client, the following appears in the command shell:

     ```
     Solaris Web Start will assist you in installing software for
     Solaris (! to quit)
     ```

     Press **!** to quit and return to a shell prompt.
   - If you are restoring a Solaris 11 or 10 client:
     a. When prompted to select an installation type, press **F5** to exit.
     b. Press **F2** to confirm the exit and return to a shell prompt.
5. Mount the old / partition under /a by typing:

   `mount /dev/dsk/c1t0d0s0 /a`

   Use the correct site-specific disk partition and mount parameters for the root volume.

   This is the target of the restore.
6. Mount the old /opt partition under /opt by typing:

   `mount /dev/dsk/c1t0d0s5 /opt`

   Use the correct site-specific disk partition and mount parameters for the /opt volume.
7. Mount the old /var partition under /var by typing:

   `mount /dev/dsk/c1t0d0s4 /var`

   Use the correct site-specific disk partition and mount parameters for the /var volume.
8. If a previous version of Avamar Client for Solaris software exists in /opt/AVMRclnt, uninstall it according to instructions found in the *EMC Avamar Backup Clients User Guide*, then reboot from CDROM to continue.
9. Install the proper version Avamar Client for Solaris software according to instructions in the *EMC Avamar Backup Clients User Guide*.

   The correct install package for each version of Solaris is listed below:
   - Solaris 10 or 11 X86_64bit—AvamarClient-solaris10-x86_64-VERSION.pkg
   - Solaris 10 or 11 SPARC—AvamarClient-solaris10-sparc-VERSION.pkg
   - Solaris 10 X86—AvamarClient-solaris10-x86-VERSION.pkg
   - Solaris 8 or 9—AvamarClient-solaris8-sparc-VERSION.pkg

   where VERSION is the version of Avamar client software.

   NOTICE

   The installation program displays a warning about root (/) having 0 free bytes, as well as errors related to read-only file systems when trying to create /etc/init.d/avagent and various links in /usr/bin and /etc/rc.d/rcX.d. However, despite these warnings, all the binaries are correctly installed in /opt/AVMRclnt/bin.

10. Restore /etc to /a/etc by typing:

    ```
    mkdir /a/etc; cd /a/etc
    /opt/AVMRclnt/bin/avtar -x --server=AVAMARSERVER --id=USERNAME
    --password=PASSWORD --account=/DOMAIN/CLIENT-NAME --target=. /etc
    ```

    where:

    - AVAMARSERVER is the hostname or IP address of the Avamar server
    - USERNAME and PASSWORD are the Avamar login credentials

      Note: These login credentials must be assigned a role (described in "Understanding users, authentication, and roles" on page 76) that allows access to the backups for this client on the Avamar server.

    - DOMAIN and CLIENT-NAME is the Solaris client to restore

    Note this information for use in the remainder of this procedure.

    NOTICE

    You cannot restore the root file system directly to /a, because there is currently no way to restrict the restore operation to only the local partition without traversing network mount points. A restore directly to /a might copy files from all partitions, causing /a to fill up before all required files are restored.

11. Inspect /a/etc/vfstab to verify the original mount points for the local file system.
12. Remove any mount points in the list of directories to restore from the Avamar backup.
13. In Avamar Administrator, click the **Backup & Restore** launcher button.

    The Backup, Restore and Manage window appears.
14. Click the **Restore** tab.
15. In the clients tree, select the original Solaris client.
16. Find and select the backup to use for the restore.
17. Examine the directories and files that originally existed under root (/).
18. For each directory that originally existed under root (/), perform the following steps:
    a. Manually create an empty directory with the same name under /a.
    b. Change directory to that directory.
    c. From the command line, restore the contents of the directory from the backup.

       For example, consider the following commands to restore /dev:

       ```
       mkdir /a/dev; cd /a/dev
       /opt/AVMRclnt/bin/avtar -x --server=AVAMARSERVER --id=USERNAME
       --password=PASSWORD --account=/DOMAIN/CLIENT-NAME
       --overwrite=always --restoresystem --target=. /dev
       ```

       The **--overwrite=always** option forces existing files to be overwritten and the **--restoresystem** option causes system files, such as devices and named pipes, to be restored.
19. Reboot the client normally and confirm correct operation.

CHAPTER 19
Avamar Client Manager

The following topics describe Avamar Client Manager, which is a web-based management application that provides centralized Avamar client administration capabilities for larger businesses and enterprises:

- Capabilities 488
- Starting Avamar Client Manager 488
- General information 489
- Global tools 494
- Overview page 503
- Clients page 507
- Policies page 527
- Queues page 532
- Logs page 534

Capabilities

Avamar Client Manager facilitates the management of large numbers of Avamar clients.

NOTICE

Avamar Client Manager works with Avamar clients on a supported native operating system and Avamar clients on a supported operating system running in a VMware virtual machine. Avamar Client Manager cannot work with Avamar clients through virtual center, virtual machine, or virtual proxy configurations. The Avamar Client Manager UI displays supported Avamar clients and hides all unsupported clients.

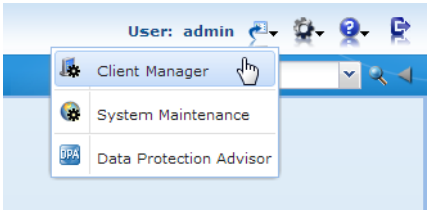
Starting Avamar Client Manager

Avamar Client Manager is started from either Backup & Recovery Manager or Avamar Enterprise Manager.

Starting from Backup & Recovery Manager

To start Avamar Client Manager from Backup & Recovery Manager:

1. Log in to Backup & Recovery Manager.
2. On the Backup & Recovery Manager banner bar, click **Launch**.
3. On the **Launch** menu, click **Client Manager**.

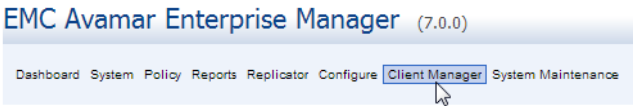


Avamar Client Manager appears in a new tab or window and opens the **Overview** page.

Starting from Avamar Enterprise Manager

To start Avamar Client Manager from Avamar Enterprise Manager:

1. Log in to Avamar Enterprise Manager.
2. On the Avamar Enterprise Manager menu bar, click **Client Manager**.



Avamar Client Manager appears in a new tab or window and opens the **Overview** page.

General information

The following topics provide general information about Avamar Client Manager:

- "Connection security" on page 489
- "Apache web server authentication" on page 489
- "Editing the session time-out period" on page 489
- "Increasing the JavaScript time-out period" on page 490
- "Configuration properties" on page 491

Connection security

To secure data transmissions between a computer and the Avamar server, a secure connection is created using HTTPS. This form of the HTTP protocol encrypts messages before they are sent and decrypts them when they are received. HTTPS is used for all login transmissions and for all transmission of data during registration and activation operations.

All attempts to access the Avamar server through the UI over standard HTTP protocol are redirected to HTTPS to prevent plain text transmissions.

Apache web server authentication

To protect user security, web browsers display an authentication warning when accessing a secure web page, unless the web server provides a trusted public key certificate with the page. The Avamar Client Manager UI uses only secure web pages, and this warning is seen in browsers that access those pages. To avoid the warning, install a trusted public key certificate on the Apache web server provided with Avamar.

The *EMC Avamar Product Security Guide* describes how to obtain and install a trusted public key certificate for the Apache web server.

Editing the session time-out period

To protect the security of the assets accessible through Avamar Client Manager, sessions time out after 72 hours (4,320 minutes) of inactivity. When a session has been running for 72 hours or more without any interaction between the web browser and the Avamar Client Manager server, Avamar Client Manager ends the session. Avamar Client Manager does not end a session while a commit task is in progress.

When Avamar Client Manager ends a session, close the web browser window or tab in which the session was running, and restart Avamar Client Manager.

You can increase or decrease the time-out period.

To edit the session time-out period:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Stop the Apache Tomcat server by typing:

   /usr/local/avamar/bin/emwebapp.sh --stop

4. Open the following file for editing:

   /usr/local/avamar-tomcat/webapps/aam/WEB-INF/web.xml

5. Change the value of the session-timeout tag to a new value, in minutes.

   For example, the default section is:

   ```
   <session-config>
         <session-timeout>4320</session-timeout>
   </session-config>
   ```

   To change the time-out value to 1 hour, edit the section to:

   ```
   <session-config>
         <session-timeout>60</session-timeout>
   </session-config>
   ```

6. Restart the Apache Tomcat server by typing:

   /usr/local/avamar/bin/emwebapp.sh --start

Increasing the JavaScript time-out period

The Avamar Client Manager UI uses JavaScript to perform many of its tasks. Sometimes an Avamar Client Manager UI script requires more time to finish than is permitted by a web browser's default script time-out value.

When this happens, a message appears and the script is stopped. You can click continue to allow the script to finish its work.

To avoid seeing this message, increase the script time-out period.

Increasing the JavaScript time-out period in Internet Explorer

To increase the script time-out period for Internet Explorer on Windows:

1. Open a registry editor, such as Regedt32.exe.
2. Open the key:

   HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Styles

   If the key does not exist, create it.
3. Create a DWORD value called "MaxScriptStatements" under this key
4. Set the value of the DWORD to 20,000,000.

   This number represents the number of script statements.
5. Restart the browser.

Increasing the JavaScript time-out period in Firefox

To increase the script time-out period for Firefox:

1. In the browser address bar, type:

   about:config

   The about:config warning appears.
2. Click **I'll be careful, I promise!**.

   The preferences window opens.
3. In **Filter**, type:

   dom.max_script_run_time

   The script runtime preference appears.
4. Double-click the preference.

   The Enter integer value dialog box appears.
5. Type **30** and click **OK**.
6. Restart the browser.

Configuration properties

Avamar Client Manager normally does not require any changes to its default configuration. However, some properties can be adjusted to suit a particular deployment requirement.

Avamar Client Manager properties are in the following file:

`/usr/local/avamar/etc/acm.properties`

The following table provides information about the properties.

Table 95 Avamar Client Manager properties (page 1 of 2)

Property	Description	Default value
activation.retry.attempts	The number of client activation attempts made before activation fails.	24
activation.retry.frequency.minutes	The number of minutes between client activation attempts.	120
move.getactivities.retry.attempts	The number of checks to determine whether a client is inactive (so that it can be moved).	7
move.getactivities.frequency.seconds	The number of seconds between checks to determine whether a client is inactive (so that it can be moved).	5

Table 95 Avamar Client Manager properties (page 2 of 2)

Property	Description	Default value
move.queue.error.codes	Sets a comma-separated list of error codes that determine whether a move task failure is added to the queue. A move is only added to the queue if its failure generates one of these error codes. The value 'none' can be used to prevent all failed move tasks from being added to the queue. The value 'empty' can be used to add all failed move tasks to the queue.	22271, 22280, 22282, 22295, 30006, 30012, 30016, 30017, 30019
move.retry.attempts	Sets the number of times a failed move task will be retried.	24
move.retry.frequency.minutes	Sets the span of time, in minutes, between retry attempts.	120
toolbar.displaytime.client	Determines whether time displayed within Avamar Client Manager uses the time zone of the web browser's host computer or time zone of the Avamar server. The default value uses the time zone of the web browser's host computer.	true
orgu.name.append.domain	Determines whether clients displayed in the Client Information area of the UI are listed using only the client's hostname or using their FQDN. The default value displays the FQDN for each client.	true

Changing a configuration property

To change an Avamar Client Manager configuration property:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Client Manager properties file, acm.properties, in a text editor such as vi or Emacs.
5. Edit the value of the property.
6. Save and close the file.
7. Restart the Avamar Enterprise Manager service:

   ```
   dpnctl stop ems
   dpnctl start ems
   ```

Support for version 5.x servers

Software changes and additions have enabled new features in Avamar Client Manager. Some of the features that are fully supported when working with clients activated to an Avamar 6.x or 7.0 have limited support when working with clients activated to an Avamar 5.x server. The following features have limited support on Avamar 5.x server:

- Move clients to a new server
- Move clients to a new domain
- Retire clients
- Delete clients
- Upgrade
- Username search
- Client details
- Dataset, retention policy, and schedule details

Move clients to a new server

When you move a client to a new server the original server must release the client's activation before the new server can activate the client. The ability to respond to a remote command to release an activation became available in Avamar server version 5.0.1.31.

The following table describes the support for moving clients to a new server in Avamar Client Manager. Support is based on the source server version, and is limited by the target server version.

Table 96 Limitations for moving clients to a new server

Source server version	Move permitted?	Limitations
Version 5.x prior to version 5.0.1.31	No	N/A
Version 5.x from 5.0.1.31	Yes[1]	Target server must be version 5.0.1.31 or newer.
Version 6.0 or newer	Yes	Target server must be version 6.0 or newer.

1. Moving clients to a new server from an Avamar server version 5.0.1.31 or newer fails when attempted immediately after the MCS is restarted and while it is still initializing. Wait until initialization is complete before using the Move Clients to New Server feature. Waiting for MCS initialization is not required for clients activated to Avamar server version 6.x.

Move clients to a new domain

Moving clients to a new domain is not supported for clients activated to Avamar server version 5.x.

Retire clients

Clients activated to an Avamar server older than version 5.0.1.31 cannot be retired using Avamar Client Manager. Clients activated to Avamar server version 5.0.1.31 or newer can be retired using Avamar Client Manager, however the task fails when attempted immediately after the MCS is restarted and while it is still initializing. Wait until initialization is complete before using the Retire Clients feature.

Waiting for MCS initialization is not required for clients activated to Avamar server version 6.x.

Delete clients

Clients activated to an Avamar server older than version 5.0.1.31 cannot be deleted using Avamar Client Manager. Clients activated to Avamar server version 5.0.1.31 or newer can be deleted using Avamar Client Manager, however the task fails when attempted immediately after the MCS is restarted and while it is still initializing. Wait until initialization is complete before using the Delete Clients feature.

Waiting for MCS initialization is not required for clients activated to Avamar server version 6.x.

Upgrade

Avamar Client Manager cannot be used to upgrade clients activated to Avamar server version 5.x. The remote upgrade process requires methods that are only available on Avamar server version 6.0 and newer.

Username search

Username search, as described in "Searching by name" on page 495, is not available for clients activated to Avamar server version 5.x. The method required to obtain account information for users of a specific client became available in Avamar server version 6.0.

Client details

For clients activated to Avamar server version 5.x, the Client Details window provides no information in the **Users on this Client** field. The method required to obtain account information for users of a specific client became available in Avamar server version 6.0.

Dataset, retention policy, and schedule details

For clients activated to Avamar server version 5.x, the dataset details, retention policy details, and schedule details windows may display some empty fields.

Global tools

Avamar Client Manager provides several tools that you can use with more than one section of the application. Use these tools to help with the following tasks:

- Selecting a server to work with
- Filtering a page's summary view
- Viewing context relevant details
- Exporting information from a page
- Enabling tool tips

Selecting a server

Use the server selection field to display, and work with, information for a specific server.

Expand the **Navigation** panel on the left side of the UI so that the server selection field is visible at the top of the panel. Navigate to a page that displays the server selection field in an active, selectable, state.

1. On the server selection field, click the arrow icon.

   When the server selection field is not visible, expand the **Navigation** panel on the left side of the UI. When the server selection field is not relevant to the current page view it appears in a dimmed state, that is, it is not active and selectable.

2. From the list of servers, select a server.

   The page view refreshes. Information about the server and its tasks appears.

Filters

Avamar Client Manager offers you a wide range of filters.

Use a filter to determine which objects appear in the list on the current page. Filters work with a variety of objects. The type of object and the available filters depend on the page's context.

In Avamar Client Manager you can filter the following types of objects:

- Servers
- Clients
- Policies
- Groups
- Tasks
- Log entries

Filters that apply to the current context appear on the **Filters** bar at the top of the page.

Searching by name

To find objects by comparing a search string to object names, use the search field.

Before you begin, navigate to a view that has one of the following search-enabled fields on the **Filters** bar:

- User name
- Client name
- Group name
- Domain name

Use search to limit the list to objects with the same and similar names.

1. Click the arrow next to the search-enabled field.

   A text entry box appears.

2. In the text entry box, type a search string.

   Avamar Client Manager compares the search string you type to the names of objects and includes matching objects on the list. Objects match when a portion of the name contains the search string.

3. Click the search button.

Avamar Client Manager refreshes the list. The results include only matching objects. (Optional) To remove the search string and to display all objects, click **X** next to the text entry field.

Example 1 Searching by username

To include all clients that have a user with the characters "eng" in their username, type **`*eng*`** in the text entry field.

Search string rules

A search string is one or more characters that you type into a name search field. Avamar Client Manager compares the search string with all object names. When the search string matches all or part of an object's name, Avamar Client Manager adds the object's name to the results.

The following rules apply to a search string:

- No more than 24 characters
- Can use an asterisk (*) character to represent zero or more characters
- Cannot start with a period character
- Cannot include any of the following characters: `/:?"<>\,~!@#$%^|&'(){}_`

Using the activity type filter

Use the activity type filter to limit a list to one type of activity.

Before you begin, navigate to a view that includes **Activity Type** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Activity Type**.

   A selection list appears, with the values: **Backup** and **Restore**.

2. Select a value.

   Select **Backup** to include only backup tasks in the list. Select **Restore** to only include restore tasks in the list.

Avamar Client Manager filters the results using the activity type you selected.

Example 2 Filtering idle clients

In the **Idle Clients** section of the Clients page, select **Backup** on the **Activity Type** filter. Avamar Client Manager limits the list to clients without any backup activity during the defined period.

Using the client status filter

Use the client status filter to add clients with the specified client status to the list.

Before you begin, navigate to a view that includes **Client Status** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Client Status**.

   A selection list of the client statuses for all clients in that context appears.

2. Select a status.
3. (Optional) Repeat the steps to select additional statuses.

Avamar Client Manager refreshes the list. Only entries with the selected client statuses appear on the list.

Example 3 Filtering by failed activation

In the **Add Clients** section of the Clients page, select **Activation Failure** on the **Client Status** filter. Avamar Client Manager limits the list to registered computers with at least one unsuccessful activation attempt.

Client status values

The following table describes the values available on the client status filter.

Table 97 Descriptions of client status values

Value	Description
Activate	Includes activated clients.
Activation failure	Includes registered clients that have failed to activate within the time limit.
Pending response	Includes registered clients that have not responded to activation and did not exceed the time limit for activation.
Selected	Includes the computers selected in Add Clients that you have not attempted to activate.

Using the failure criteria filter

Use the failure criteria filter to define which clients Avamar Client Manager includes in a list of failed clients.

Before you begin, navigate to a view that includes **Failure Criteria** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Failure Criteria**.

   A selection list appears, with the values:

   - At least one activity failed
   - All activities failed
   - Last activity failed

2. Select a value.

   The value you select determines which clients Avamar Client Manager includes in the list of failed clients. Avamar Client Manager includes only clients that match the selected activity status.

Avamar Client Manager refreshes the list. Only clients with an activity status that matches the selected value appear on the list.

Example 4 Filtering for clients with failed last activity

In the **Failed Clients** section of the Clients page, select **Last activity failed** on the **Failure Criteria** filter. Avamar Client Manager refreshes the list and includes clients only when their most recent activity failed. The failed activity can be either a backup or a restore.

Using the OS filter

Use the OS filter to limit a list to clients with specific operating systems.

Before you begin, navigate to a view that includes **OS** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **OS**.

   A list of the OS versions of all clients in that context appears.

2. Select an OS version.
3. (Optional) Repeat the steps to select additional OS versions.

Avamar Client Manager refreshes the list. Only clients with the selected OS version appear on the list.

Using the period filter

Use the period filter to define the calendar date boundaries of the displayed results.

Before you begin, navigate to a view that includes **Period** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Period**.

   A selection list appears, with the values: **Before**, **After**, and **On**.

2. Select a value.
3. Click the arrow next to the selected value.

   A date entry field and a small calendar icon appear.

4. Click the calendar icon, navigate to a specific date, and then click the date.

   Alternatively, in the date entry field, type a date with the format m/d/yy, and click the search button.

5. (Optional) Further refine the results by repeating these steps using the other values.

Avamar Client Manager refreshes the list. Only entries within the specified period appear on the list.

Using the status filter

Use the status filter to limit a list to entries with specific statuses.

Before you begin, navigate to a view that includes **Status** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Status**.

   A selection list of all statuses for all entries in that context appears.

2. Select a status.

3. (Optional) Repeat the steps to select additional statuses.

Avamar Client Manager refreshes the list. Only entries with the selected statuses appear on the list.

Using the status code filter

Use the status code filter to limit a list to entries with specific status codes.

Before you begin, navigate to a view that includes **Status Code** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Status Code**.

   A selection list of the status codes for all entries in that context appears.

2. Select a status code.

3. (Optional) Repeat the steps to select additional status codes.

Avamar Client Manager refreshes the list. Only entries with the selected status codes appear on the list.

Status Codes

Status codes appear in log entries.

The following table describes some of the status codes you can see when activating clients.

Table 98 Descriptions of client activation status codes (page 1 of 2)

Status Code	Description
22271	Invitation failed–The Avamar server cannot contact the Avamar client software
22237	Activation failed–Client previously activated or cannot communicate with Avamar server

Table 98 Descriptions of client activation status codes (page 2 of 2)

Status Code	Description
22280	Client reconnect error–Hostname mismatch
22282	Client reconnect error–Unknown ID
22295	Client registration error–Server not available

Using the success criteria filter

Use the success criteria filter to define which clients Avamar Client Manager includes in a list of successful clients.

Before you begin, navigate to a view that includes **Success Criteria** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Success Criteria**.

   A selection list appears, with the values:

   - At least one activity successful
   - All activities successful
   - Last activity successful

2. Select a value.

   The value you select determines which clients Avamar Client Manager includes in the list of successful clients. Avamar Client Manager only includes clients that match the selected activity status.

Avamar Client Manager refreshes the list. Only clients with an activity status that matches the selected value appear on the list.

Example 5 Filtering for clients with a successful last activity

In the **Activated Clients** section of the Clients page, select **Last activity successful** on the **Success Criteria** filter. Avamar Client Manager refreshes the list and only includes the clients with a successful last activity, either a backup or a restore.

Using the version filter

Use the version filter to limit a list to clients with specific versions of the Avamar client software.

Before you begin, navigate to a view that includes **Version** on the **Filters** bar.

1. On the **Filters** bar, click the arrow next to **Version**.

   A selection list of the Avamar client software versions for all clients in that context appears.

2. Select a version.
3. (Optional) Repeat the steps to select additional software versions.

Avamar Client Manager refreshes the list. Only clients with the selected software versions appear on the list.

Viewing details

Use the **Details** panel to view context relevant details.

Before you begin, navigate to a view that includes the **Details** panel or **Details** bar on the right-side.

1. On the right-side of the page, click the **Details** bar.

   The **Details** panel expands.

2. In **Summary**, select an object.

   The page context determines the object type. An object can be a client or a group. You can select more than one object.

   Detailed information for the selected object appears in the **Details** panel.

3. (Optional) When you select more than one object, use the paging controls at the bottom of the **Details** panel to view information for each selected object.

Details panel fields

The following table describes the fields that appear on the **Details** panel when you select a client.

Table 99 Descriptions of Details panel fields for clients

Field	Description
Name	The name of the selected client computer.
Domain	The Avamar domain of the selected client.
Groups	A comma-separated list of the client's Avamar groups.
Version	The version of Avamar client software installed on the client computer. Avamar Client Manager can only determine this for activated clients.
OS	The operating system running on the client computer.
Status	The state of a client's activation with an Avamar server, either: Active or Activation Failure.

The following table describes the fields that appear on the **Details** panel when you select a group.

Table 100 Descriptions of Details panel fields for groups (page 1 of 2)

Field	Description
Name	The name of the selected group.
Domain	The Avamar domain of the selected group.
Activated Clients	Number of activated clients assigned to the group.
Dataset	Dataset assigned to the group.

Table 100 Descriptions of Details panel fields for groups (page 2 of 2)

Field	Description
Retention	Retention policy assigned to the group.
Schedule	Back up schedule assigned to the group.
Enable	Displays True for groups with scheduled backups enabled. Displays False for groups with scheduled backups disabled.

Exporting data

Use export to download the selected summary as an Excel spreadsheet.

Before you begin, navigate to a page view that includes **Export** on the page bar.

1. On the page bar, click **Export**.

   Avamar Client Manager includes all information from the summary in the exported data.

   The web server pushes an Excel file containing the summary information to the browser.

2. Save the file to your computer.
3. Use an application that can read the Excel-formatted spreadsheets to open the file.

Setting the entries per page limit

Increase the limit on the number of entries displayed in summary lists.

By default, Avamar Client Manager limits its summary lists to 25 entries per page. When there are more entries than the current entries per page limit, the entries appear on 2 or more pages. You can increase the entries per page limit to make it easier to work with many entries.

1. On the status bar at the bottom of Avamar Client Manager, click **Entries Per Page**. The list of choices appears.
2. Click a number on the list.

Avamar Client Manager sets the selected number as the new limit and refreshes the page.

Viewing tool tips

Enable and display tool tips to view concise help messages for various elements of the UI.

1. On the status bar at the bottom of Avamar Client Manager, select **Show Tooltips**.
2. Hover the pointer over a user interface element that has a tool tip. The following elements may have tool tips:

   - Dashboard chart sections
   - Controls
   - Column headings

The tool tip for the selected element appears.

Overview page

Avamar Client Manager's **Overview** page provides access to high level information about the management of an enterprise's Avamar clients.

From the left-side menu of the **Overview** page, select:

- **Server Summary** for information about a selected Avamar server.
- **Dashboard** for information about client backups.

Server Summary

The **Server Summary** section provides columns of information about the Avamar servers that you have registered with Enterprise Manager.

Filter this information by using the filters available on the **Filters** bar. Change the sorting method used for the list by clicking on a column heading.

In each of the following columns, nonzero values are linked to a more detailed report about that column's information:

- Active Clients
- Idle Clients
- Successful Clients
- Failed Clients

Example 6 Viewing more information about a server's idle clients

One of your servers has **6** in the Idle Clients column. Click **6**. The Idle Clients summary for that server opens and information about the six idle clients appears.

Server Summary columns

The following table describes the columns in the **Server Summary** section.

Table 101 Descriptions of the columns on the Server Summary section

Column	Description
Server	Hostname or IP address of the Avamar server. Only servers registered in Enterprise Manager are visible in Avamar Client Manager.
Total Clients	Total number of clients registered with the Avamar server. Does not include retired clients.
Active Clients	Total number of clients with activity (backup or restore) during the specified period.
Idle Clients	Total number of clients with no backup activity during the specified period.
Successful Clients	Total number of clients with a backup status that matches the value set in the Successful Backups filter. Also includes the average amount of time for those backups.
Failed Clients	Total number of clients with failed backups during the specified period.
Clients with Restore	Total number of clients with restore activity (successful or unsuccessful) during the specified period.

Dashboard

The **Dashboard** section provides a graphical snapshot view of a selected server.

The dashboard provides information in panels that you can expand, collapse, or delete to create the view you need.

Usage tips:

- Collapse or expand a panel by clicking the arrow icon in the panel's title bar.
- Delete a panel by clicking the **X** in the panel's title bar.
- Return the dashboard to its default view by reloading the page in your web browser.

Setting a panel's period

Set a panel's period to define the number of days of data in the display.

Before you begin, navigate to the **Dashboard** section with any of the following panels displayed: **Analyze**, **Backup Report**, and **Backup Trend**.

1. On a panel, in the period field, click the arrow icon.

   The period field is available on the following panels:

   - Analyze
   - Backup Report
   - Backup Trend

   The period list appears.

2. Select a period.

   The available choices are:

   - Last 24 hours
   - Last 7 days
   - Las 30 days

Avamar Client Manager refreshes the panel with data for the selected period.

Client panel

The **Client** panel uses a pie chart to represent the total number of potential clients for the selected server. Colors represent the percentage of the total for:

- Activated
  Green represents the percentage of clients that the selected server has activated.
- Not activated
  Red represents the percentage of clients that the selected server has registered, but not activated.
- Free
  Gray represents the percentage of unused client connections available on the selected server.

Server panel

The **Server** panel provides a grid view of information about the selected server.

The following table describes the columns in the grid view.

Table 102 Descriptions of the columns in the Server panel grid

Column	Description
Node Type	Specifies the server's node type: Single or Multi.
Active Backup	Number of running backups.
Backup in Queue	Number of backups in the server's queue waiting to run.
Replication	Current state of the replication cron job: • Running • Not running
Status	Current state of the server's Management Console Server (MCS) system: • Active • Down

Backup Trend panel

The **Backup Trend** panel is a line chart that shows the size of data backed up at specific points in time over a defined period. The x-axis represents points in time over the selected period. The y-axis represents the size of data in the backup at each point in time.

The line drawn between the plotted points represents the backup trend, which is the change in backed up data over time.

Client Type panel

The **Client Type** panel uses a bar chart to represent the number of activated clients of each category that a server has:

- Regular
  All activated clients that do not fit into one of the other three categories.
- vMachine
  Guest clients; the virtual computers backed up through Avamar client software running on the host computer.
- Proxy
  Proxy virtual machine clients; clients that use Avamar for VMware image backup and restore.
- vCenter
  Avamar clients that protect vCenter management infrastructure by backing up vCenter hosts.

Analyze panel

The **Analyze** panel uses a bar chart to represent the number of clients that are in each of the following states during the selected period:

- Successful
  Clients with at least one successful backup.
- Failed
  Clients with backup activity but no successful backups.
- Idle
  Clients with no backup activity.

Backup Report panel

For backups attempted during the selected period, the Backup Report panel uses a bar chart to represent the number of each of the following results:

- Successful
  Successfully completed backups; with or without errors.
- Failed
  Backups that failed to complete.
- Canceled
  Backups canceled before completion.

Client Queues panel

The Client Queues panel uses a bar chart to display the number of clients in each of the following queues:

- Upgrade
- Move to server
- Activation

Storage Capacity panel

The Storage Capacity panel uses a pie chart to represent the total storage capacity of the selected server. Colored slices represent the following:

- Used
  Red represents the portion of storage that contains data.
- Free Capacity
  Green represents the portion of storage that is unused and available.

Backup Health panel

The Backup Health panel uses a bar chart to represent the number of clients that have retained backup data for specific periods of time. The panel uses the periods: 1 day, 30 days, 60 days, and 90 days.

On the bar chart, the x-axis represents the period that Avamar has retained the data and the y-axis represents the number of clients.

Clients page

Avamar Client Manager's **Clients** page provides information and tools for working with Avamar clients.

From the **Clients** page you can:

- Select the computers in your enterprise's domain and add them as Avamar clients
- View detailed information about individual clients
- Move, retire, and delete clients
- Change a client's group associations
- Upgrade the Avamar software on the client

To navigate between the sections of the Clients page, select from the choices in the left-side menu.

Client and server tools

Avamar Client Manager provides several tools to help manage Avamar clients and Avamar servers.

A tool only appears when it is relevant to the context. Changes made by the tool apply to the selected client and the selected server. Launch a tool by clicking its command button.

Creating an Avamar domain

Create an Avamar domain to add a new branch to an Avamar server's administrative hierarchy.

Before you begin, navigate to a view that includes **Create Domain**: either the **Add New Clients** dialog box or the **Client Move** dialog box.

1. In the **Domain Selection** pane, select the location for the new domain.

   To locate the new domain directly beneath the root domain, select the server icon. To locate the new domain beneath another domain, select that domain.

2. Click **Create Domain**. The **New domain** dialog box appears.
3. In **New Domain Name**, type a name for the domain.

   Avamar does not allow the following characters in a domain name:
   `=~!@$^%(){}[]|,` ;#\/:*?<>'"&+`
4. (Optional) Type information in the **Contact**, **Phone**, **Email**, and **Location** fields.
5. Click **OK**.

Avamar Client Manager adds the new domain to the selected server and the new domain appears on the **Domain Selection** pane.

Viewing a client's group associations

To determine the policies that apply to a client, view the client's group associations.

Before you begin, navigate to a view that includes **Group Associations** on the **Actions** bar. A client's group associations determine the client's backup dataset, the client's backup schedule, and the client's backup retention period.

1. Select a client.
2. Click **Group Associations**.

The **Groups for Client** dialog box appears and lists the client's groups.

Columns shown on group associations lists

The following table describes the columns that appear on group associations lists.

Table 103 Descriptions of columns on group associations lists

Column	Description
Name	Label assigned to the group in Avamar.
Domain	Avamar domain of the group.
Dataset	Name of the dataset assigned to the group. Click the name to view the dataset's policy details.
Schedule	Name of the schedule assigned to the group. Click the name to view the schedule's policy details.
Retention	Name of the retention policy assigned to the group. Click the name to view the retention policy's details.
Enable	Scheduled backup setting. If Yes, backups run according to the group's schedule. If No, scheduled backups do not run.

Adding group associations to a client

To apply the policies of a group to a client, add the group association to the client.

Before you begin, navigate to a view that includes **Group Associations** on the **Actions** bar.

This task results in an association between a client and a group. The Avamar server applies the group's policies to the client.

1. Select a client.
2. Click **Group Associations**.
3. On the **Groups for Client** dialog box, click **Add Groups**.

   The **Add Groups for Client** dialog box appears.
4. Select a group.

   You can select more than one group.
5. Click **Add**.

Avamar Client Manager adds the group associations to the client.

Creating a group

To make a new set of policies available for assignment to clients, create a group with the policies. The **Create Group** command is available when adding a client to a group, and when moving a client to a new domain or to a new server.

Before you begin, navigate to a view that includes **Create Group**: either the **Add Groups** dialog box or the **Client Move** dialog box.

1. Click **Create Group**.

   On the **Client Move** dialog box selecting a domain enables the button.

   The **Create Group in Domain** dialog box appears.

2. In **Group Name**, type a name for the new group.

   Avamar does not allow the following characters in a group's name:
   =~!@$^%(){}[]|,`;#\/:*?<>'"&+

3. (Optional) Select **Enable** to enable scheduled backups of clients that you assign to the group.

   Clear this checkbox to disable scheduled backups of clients that you assign to the group.

4. In **Dataset**, select a dataset for the group.

5. In **Schedule**, select a schedule for the group.

6. In **Retention Policy**, select a retention policy for the group.

7. Click **OK**.

Avamar Client Manager creates the new group in the selected domain.

Removing group associations from a client

To stop applying a group's policies to a client, remove the group association from the client.

Before you begin, navigate to a view that includes **Group Associations** on the **Actions** bar.

This task removes the association between a client and a group. When you complete the task the group's policies no longer apply to the client.

1. Select a client.

2. Click **Group Associations**.

3. On the **Groups for Client** dialog box, select a group.

   You can select more than one group.

4. Click **Remove**.

Avamar Client Manager removes the association between the client and the selected groups.

Overriding group policy settings for a client

To modify the policies applied to a client, override the policies of its group.

Before you begin, navigate to a view where **View/Edit Details** appears on the **Actions** bar and the client appears in the clients list.

1. Select a client.
2. On the **Actions** bar, click **View/Edit Details**.

   The **Client Details** dialog box appears.
3. Select the **Advanced** tab.

   The policy override settings appear with the client's current state shown.
4. Make changes to the client's current state by selecting or clearing settings.
5. Click **OK**.

Avamar Client Manager changes the group policy settings for the client.

Group policy override settings

To modify a policy applied to a client, use one of the policy override settings.

The following table describes the policy override settings on the **Advanced** tab of the **Client Details** dialog box.

Table 104 Descriptions of the group policy override settings (page 1 of 2)

Setting	Description
Override group dataset	Permits you to assign to a client a dataset that is different from the group dataset. After selecting this option, assign a dataset by selecting it from the **Select an existing dataset** list.
Select an existing dataset	List of available dataset choices that you can assign to a client. To use this list, first select **Override group dataset**.
Override group retention	Permits you to assign to a client a retention setting that is different from the group setting. After selecting this option, assign a retention setting by selecting it from the **Select an existing retention policy** list.
Select an existing retention policy	List of available retention settings that you can assign to a client. To use this list, first select **Override group retention**.
Disable all backups	Disables all backups of the client. Users can still restore data.
Activated	Places a registered client in an activated state. When you clear this setting, users cannot perform backups or restores.
Allow client-initiated backups	Permits users to begin backups from the client.
Allow file selection for client-initiated backups	Permits users to select files to include in backups started from the client. The **Exclude** list for the group's dataset does not apply.

Table 104 Descriptions of the group policy override settings (page 2 of 2)

Setting	Description
Allow client to add to dataset	Permits users to add folders to the datasets of the client's groups. The following rules apply to this setting: • The Avamar server filters the added data with the group's **Exclude** list and **Include** list. • The added data is in every scheduled and on-demand backup for each group assigned to the client. • User must have access to the Avamar client web UI to add folders or remove folders.
Allow client to override daily group schedules	Permits users to select a start time for scheduled backups that is different from the start time assigned by the group. Prerequisites: • Add time entries to the Avamar server's **Override** schedule. • Assign a daily schedule to the client's group. • Provide users access to the Avamar client web UI to allow them to select a new schedule.
Allow client to override retention policy on client-initiated backups	Assigns the retention policy specified in Select an existing retention policy to client-initiated backups. Prerequisites: • Enable **Override group retention** • Enable **Allow client-initiated backups**

Viewing summary information about a client

Use **Client Details** to see information about a client and its users.

Before you begin, navigate to a view where **View/Edit Details** appears on the **Actions** bar and the client appears in the clients list.

1. Select a client.
2. On the **Actions** bar, click **View/Edit Details**.

   The **Client Details** dialog box appears.
3. Select the **Summary** tab.

Information about the client appears. Also, a list of users associated with the client appears.

Summary information fields

The following table describes the information fields on the **Summary** tab of the **Client Details** dialog box.

Table 105 Descriptions of the summary information fields (page 1 of 2)

Field	Description
Client Name	Name that the Avamar server uses to reference the client.
Domain	Avamar domain of the client.
OS	Operating system information provided by the client.

Table 105 Descriptions of the summary information fields (page 2 of 2)

Field	Description
Version	Version of Avamar client installed on the client.
Last backup	Date and time of the last successful backup of the client.
Users	List of local and domain user accounts on the client.

Changing a client's name on the server

When you change a computer's name, you must also change its client name on the Avamar server.

Change the name of the computer hosting the Avamar client, both locally and in DNS, before performing this task. Navigate to a view where **View/Edit Details** appears on the **Actions** bar and the client appears in the clients list.

1. Select a client.
2. On the **Actions** bar, click **View/Edit Details**.

   The **Client Details** dialog box appears.
3. Select the **Summary** tab.
4. In **Client name**, type the new name for the client.
5. Click **OK**.

Avamar Client Manager changes all references on the server to the new client name.

Viewing a client's backup history

To determine whether an Avamar server has backed up a client as expected, view the client's backup history.

Before you begin, navigate to a view where **View/Edit Details** appears on the **Actions** bar and the client appears in the clients list.

1. Select a client.
2. On the **Actions** bar, click **View/Edit Details**.

   The **Client Details** dialog box appears.
3. Select the **Backups** tab.
4. In **From**, select the earliest date of the period to view.
5. In **To**, select the latest date of the period to view.
6. (Optional) Select **On-demand backups**.

   Select this choice to include user-initiated backups in the results. Clear this choice to exclude those backups.
7. (Optional) Select **Scheduled backups**.

   Select this choice to include backups initiated by a group schedule in the results. Clear this choice to exclude those backups.

A list of the client's backups that match the filter settings appears.

Columns on the Backups tab

The following table describes the columns on the **Backups** tab of the **Client Details** dialog box.

Table 106 Descriptions of the columns on the Backups tab

Column	Description
Label	Unique name assigned to the backup.
Plug-in	Plug-ins used during the backup.
Size	Total size of the client's data in the backup.
Started	Date and time that the backup started.
Expired	Date that retention of the backup ends.

Viewing a client's installed plug-ins

View the Avamar plug-ins installed on an Avamar client to help determine the types of data in its backups.

Before you begin, navigate to a view where **View/Edit Details** appears on the **Actions** bar and the client appears in the clients list.

1. Select a client.
2. On the **Actions** bar, click **View/Edit Details**.

   The **Client Details** dialog box appears.
3. Select the **Plug-ins** tab.

A list of the plug-ins installed on the client appears.

Columns on the Plug-ins tab

The following table describes the columns on the **Plug-ins** tab of the **Client Details** dialog box.

Table 107 Descriptions of the columns on the Plug-ins tab

Column	Description
Name	Name of the plug-in.
Version	Version number assigned to the plug-in.
Build	Build number assigned to the plug-in.
Last Backup	Date and time that the last successful backup with the plug-in finished.

Deleting a client from a server

To remove a client's records and backups from an Avamar server, delete the client from the server.

Before you begin, navigate to a view where the client appears in the client list and Delete appears on the Actions bar.

NOTICE

When Avamar Client Manager deletes a client from an Avamar server it stops all activity with that client, deletes the client's backups, and removes all record of the client from the server's database.

1. Select a client.
2. On the **Actions**, bar, click **Delete**.
3. On the **Confirm** dialog box, type your password.

   Use the password of the account logged into Avamar Client Manager.
4. Click **OK**.

   The **Alert** dialog box appears.
5. Click **OK**.

Avamar Client Manager runs a background process that removes all the client's information and data from the server.

Add Clients section

The **Add Clients** section provides information and tools to register and activate your enterprise computers as Avamar clients.

Use the **Add Clients** section to import information about the computers in your enterprise. You can import the information from your LDAP v.3-compliant naming system or from a CSV file.

After import, you can filter the information by client status and client name to help in the selection of prospective Avamar clients.

You can use Avamar Client Manager to register and activate the selected computers to an Avamar server. Completion of the activation process requires installation of the Avamar client software on the computers and access to that software from the server. The normal workflow is to install the client software on a computer before you select it for activation.

Directory service information

You can use your enterprise's directory service to provide Avamar Client Manager with information about the computers that are potential Avamar clients.

Any LDAP v.3-compliant directory service can be used, such as Microsoft Active Directory.

When you use this method, Avamar Client Manager queries your enterprise's directory service to obtain information about clients and, if available, directory service organizational units, such as directory domains, and directory groups.

Before using the directory service method, complete LDAP server configuration for Avamar Enterprise Manager as described in "Configuring directory service information" on page 412.

This method also requires the following:

- TCP/IP access to your enterprise's LDAP v.3-compliant directory service from the server that is running Avamar Enterprise Manager.
- Account information for a user account with read access to the directory service.
- The name of the directory service domain for the computers that you want to import.

Importing information from a directory service

To prepare to add computers as Avamar clients, import information about the computers from the directory service.

Before you begin, do the following:

- Ensure access to your enterprise's LDAP v.3-compliant directory service from the server that is running Avamar Enterprise Manager.
- Obtain a username, and its associated domain and password for an account with read access to the directory service.
- Have available the name of the directory service domain of the computers.

1. In the left-side menu, click **Clients** › **Add Clients**.
2. On the **Actions** bar, click **New Clients**.

   The **Client Information Source** dialog box appears.
3. Select **Active Directory**.
4. In **User Domain**, select the domain of the account you are using to access the directory service.

   To add directory service domains to this list, refer to the administration guide.
5. In **User Name**, type the name of the account.
6. In **Password**, type the password of the account.
7. In **Directory Domain**, select the name of the directory service domain for the computer information you are importing.
8. Click **OK**.

Avamar Client Manager imports the information from the directory service.

After you finish this task, use the imported computer information to select and activate computers as clients of an Avamar server.

CSV file information

You can use a comma-separated values (CSV) file to provide Avamar Client Manager with information about the computers that are potential Avamar clients.

You can create the CSV file manually or you can create it by using the output of a Systems management tool such as the Microsoft System Center Configuration Manager or the Microsoft Systems Management Server.

When a Systems management tool creates the CSV file by using a push install of the Avamar client software, only those clients that have the software successfully installed appear in Avamar Client Manager.

During the upload of a CSV file, Avamar Client Manager checks the file for correct formatting, and cancels the upload when it finds a problem.

CSV file format

A correctly formatted CSV file complies with the following rules:

- At least two rows.
- Values separated by a comma only.
- The first row of the file must consist of the literal names for each type of value.

  The name for the first value is **Hostname**. The name for the second value is **Group**.
- The second row, and all subsequent rows, must have at least one value and no more than two values.
- The formatting rules require a first value that is a valid hostname for a computer and a trailing comma.
- The second value is optional, but when you include it, it must be the directory service logical group name for the computer.

  When you do not provide the second value for a computer, Avamar Client Manager lists the computer at the root level in the hierarchical display.
- In the second value, use a forward slash ('/') to separate the hierarchical levels of the directory service logical group name.

If you use spreadsheet software to create or edit the client list, do not add a comma along with the value to try to create comma separated values. This can result in an incorrectly formatted file. When you save the client list in the editor as a CSV file-type, the editor adds the comma separators as part of the file conversion process. To check the formatting, open the client list in a plain text editor.

Example 7 Correctly formatted CSV file

In a plain text editor, a correctly formatted client list file looks like the following example.

```
Hostname,Group
User1-desktop.Acme.corp.com,acme.corp/USA/MA
User1-laptop.Acme.corp.com,acme.corp/USA/CA/SFO
User2-desktop.Acme.corp.com,acme.corp/Engineering
User3-desktop.Acme.corp.com,
User4-desktop.Acme.corp.com
```

The first line lists the literal names of each type of value.

The second line contains the hostname "User1-desktop.Acme.corp.com", the separating comma, and the group "acme.corp/USA/MA".

The third line contains the hostname "User1-laptop.Acme.corp.com", the separating comma, and the group "acme.corp/USA/CA/SFO".

The fourth line contains the hostname "User2-desktop.Acme.corp.com", the separating comma, and the group "acme.corp/Engineering".

The fifth and sixth lines contain only the hostnames "User3-desktop.Acme.corp.com" and "User4-desktop.Acme.corp.com", each followed by a comma. The formatting rules require a comma, even without a group. The lines do not list groups, so both hostnames appear at the root level of the hierarchical display.

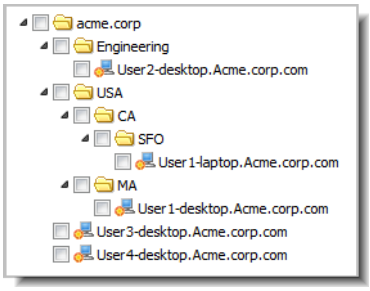


Figure 15 View after uploading the CSV file described in Example 7 on page 516

Uploading information in a CSV file

To prepare to add computers as Avamar clients, upload information about the computers in a comma-separated values (CSV) file.

Before you begin, generate or create a correctly formatted CSV file and have a copy available on the web browsing computer.

1. In the left-side menu, click **Clients** › **Add Clients**.
2. On the **Actions** bar, click **New Clients**.

   The **Client Information Source** dialog box appears.
3. Select **CSV File**.
4. Click **Browse**.

   The **Choose File to Upload** dialog box appears.
5. Navigate to your CSV file, select it, and click **Open**.
6. On the **Client Information Source** dialog box, click **OK**.

Avamar Client Manager uploads the information from the CSV file.

After you finish this task, use the uploaded computer information to select and activate computers as clients of an Avamar server.

Activation

Activation consists of changing the relationship between a computer and an Avamar server to enable the server to manage backups of the computer.

The relationship moves through three states:

- No relationship
  The computer is unknown to the server. Computers in this state appear in Add Clients, when you first add the computer information to Avamar Client Manager.
- Registered
  Avamar Client Manager entered the information about the computer into the Avamar server's database. Computers in this state appear in Registered Clients after Avamar Client Manager starts the activation process and completes registration with the Avamar server. The changed state of these computers also appears in Add Clients.
- Activated
  The computer has Avamar client software installed and running. The client software and the server are in communication and have exchanged an encrypted key to verify their identities. Computers in this state appear in Activated Clients after activation is complete. The changed state of these computers also appears in Add Clients and Registered Clients.

A computer that is in the activation process appears on the Queues page, in Activation. Avamar Client Manager attempts to activate a computer every 2 hours until it succeeds or until it reaches the limit of 24 attempts. When the process completes, Avamar Client Manager removes the computer from this view and adds an entry on the Logs page, in Activation.

Activating your computers

To enable backup management of a client, activate it with an Avamar server.

Before you begin, install Avamar client software on the computers being activated and import information about the computers from either your directory service or a CSV file.

1. On the left-side menu, click **Clients** › **Add Clients**.

   A hierarchical view of the computers in your enterprise appears. Avamar Client Manager generates this view from the information that you imported.

2. Browse or search the hierarchy to find the computers to activate.
3. Select each computer to activate.
4. To select all computers in a folder, expand the folder to show the computers, then select the folder.
5. Click **Activate**.

   The **Server - Domain Selection** dialog box appears.

6. Expand the listing for a server, and select an Avamar domain.

   Avamar Client Manager assigns the computers to the selected server and domain during activation.

7. Click **Next**.

   The **Server - Group Selection** dialog box appears.

8. Select a group or multiple groups.

   Avamar Client Manager assigns the computers to the selected group or groups during activation.

9. Click **Finish**.

Avamar Client Manager sends the activation task to the queue.

After you finish this task, check the **Activation** section of the **Queues** page to determine the status of the activation process. After the process completes, check the **Activation** section of the **Logs** page to determine its final status.

Registered Clients section

Clients that have registered with an Avamar server but not been activated appear in the **Registered Clients** section.

Use this section to select clients and perform the following client-related tasks:

- Activate
- Delete
- Associate with groups
- View and edit details
- Add and remove group override settings

Activating a registered client

To enable backup management of a registered client that failed to activate when registered, activate it from the **Registered Clients** section.

Before you begin, install Avamar client software on the computers you want to activate.

When activation of a computer as a client of an Avamar server fails, Avamar Client Manager still registers the computer with the server. You can correct any problems that prevented the activation and retry it.

1. On the left-side menu, click **Clients** › **Registered Clients**.
2. Select each client to activate.
3. Click **Activate**.

Avamar Client Manager sends the activation task to the queue.

After you finish this task, check the **Activation** section of the **Queues** page to determine the status of the activation process. After the process completes, check the **Activation** section of the **Logs** page to determine its final status.

Activated Clients section

Activated clients of the selected Avamar server appear in the **Activated Clients** section.

Use the **Activated Clients** section to perform the following tasks:

- Move client to a different server
- Move client to a different Avamar domain
- Retire a client
- Delete a client
- Manage a client's group associations
- View and edit a client's details
- Add and remove group override settings

Moving a client to a new server

To use a new Avamar server to manage an Avamar client, move the client's registration, activation, and backups to the new server.

To allow at least one of the client's backups to be replicated to the new server, Avamar Client Manager prevents you from moving the client in the following situations:

- Some of the client's backups are stored on a Data Domain server, and you select **All** in **Replicate Existing Backups**.
- The client's last backup is stored on a Data Domain server, and you select **Last** in **Replicate Existing Backups**.

Before you begin, do the following:

- Select a client activated to a server with Avamar server software version 5.0.1.31 or newer.
- For a client activated with an Avamar server older than version 6.x, fully initialize the MCS process on that server.

1. On the left-side menu, click **Clients** › **Activated Clients**.
2. Select a client.
3. On the **Actions** bar, click **Move**.

   The **Domain Selection** pane of the **Client Move** dialog box appears.
4. At the top of the **Domain Selection** pane, from the server selection list, select the Avamar server that is the target of the move.

   The target server's domains appear in the **Domain Selection** pane.
5. In the **Domain Selection** pane, select the target domain.
6. Click **Next**.

   The **Group Selection** pane of the **Client Move** dialog box appears.
7. Select a target group.

8. You can optionally select more than one target group.

   Avamar Client Manager adds the client to all selected groups.

9. In **Replicate Existing Backups** at the bottom of the **Group Selection** pane, select a value:

   - **All**

     Replicate all the client's backups to the target server.

   - **Last**

     Replicate only the last backup.

   - **None**

     Replicate none of the backups.

   Replication makes the backups available from the target server.

10. (Optional) In **Delete From Source**:

    - Select to remove all the client's backups from the source server.
    - Clear to move the source server's registration of the client to the source server's MC_RETIRED domain and retain copies of the client's backups on the source server.

11. Click **Finish**.

    The **Confirm Replication Authentication** dialog box appears.

12. In **Source Server**, type the password for the replonly account on the source server.

13. In **Target Server**, type the password for the replonly account on the target server.

14. Click **OK**.

In a background process, Avamar Client Manager moves the client to the selected target.

Moving a client to a different Avamar domain

To change the administrative relationship between an Avamar client and an Avamar server you can move the client to a different Avamar domain.

Before you begin, select a client activated to a server with Avamar server software version 6.x or newer.

1. On the left-side menu, click **Clients** › **Activated Clients**.
2. Select a client.
3. On the **Actions** bar, click **Move**.

   The **Client Move** dialog box appears.

4. In the **Domain Selection** pane of the **Client Move** dialog box, select the target domain.
5. Click **Next**.

   The **Group Selection** pane appears on the **Client Move** dialog box.

6. Select a target group.

   You can optionally select more than one target group. Avamar Client Manager adds the client to all the selected groups.

7. Click **Finish**.

   An alert box appears.

8. Click **OK**.

In a background process, Avamar Client Manager moves the client to the selected target.

Retiring a client

When you no longer need to run backups of a client, retire it. Avamar Client Manager retains backups that exist at the time of retirement so that you can restore data when necessary.

1. On the left-side menu, click **Clients** › **Activated Clients**.
2. Select a client.

   You can select more than one client. The retention policy setting you select applies to all selected clients.

3. On the **Actions** bar, click **Retire**. The **Retire Client** dialog box appears.
4. In **Select Retention Policy**, select one of the options.

Table 108 Select Retention Policy options

Option	Description
Retire client and retain backups with existing expiration date	The Avamar server retains the backups for the existing retention period.
Retire client and retain all backups indefinitely	The Avamar server retains the backups until you manually delete them
Retire client and reset backup expiration date	The Avamar server retains the backups until the date set in New Expiration Date

5. If you select **Retire client and reset backup expiration date** in the previous step then, in **New Expiration Date**, select a date.

   The **Confirm** dialog box appears.

6. Click **Yes**.

   The **Alert** dialog box appears.

7. Click **OK**.

In a background process, Avamar Client Manager retires the selected client.

Failed Clients section

Clients that have unsuccessful backup or restore activity appear in the Failed Clients section.

Use the Failed Clients section to perform the following tasks:

- Delete a client
- Manage a client's group associations
- View and edit a client's details
- Add and remove group override settings

When working with failed clients, use the filters described in the following table.

Table 109 Descriptions of filters used when working with failed clients

Filter	Description
Period	Specifies the period that Avamar Client Manager examines.
Activity Type	Specifies the type of activity that Avamar Client Manager examines.
Failure Criteria	Defines the failure threshold used by Avamar Client Manager.

Idle Clients section

Clients activated with an Avamar server that do not have activity during a specified period appear in the **Idle Clients** section.

When working with idle clients, use the **Period** filter to specify the period that Avamar Client Manager examines for activity, and the **Activity Type** filter to specify the type of activity.

Use the **Idle Clients** section to perform the following tasks:

- Delete a client
- Manage a client's group associations
- View and edit a client's details
- Add and remove group override settings

"Client and server tools" on page 507 describes these tasks.

Upgrade Clients section

The **Upgrade Clients** section provides information and tools you can use to apply upgrades and hotfixes to Avamar clients.

Use the **Upgrade Clients** section to perform the following tasks:

- Download an upgrade package to a server
- Select an upgrade package
- Apply the package to selected clients
- Remove an upgrade package from a server

Upgrade Clients section requirements

Before using the Avamar Client Manager **Upgrade Clients** section, do the following:

- For each client or plug-in, install the minimum client version as described in the following table.

Table 110 Client version support for client and plug-in upgrades

Client/Plug-in Upgrade	Avamar client version 6.0 and newer	Avamar client version 7.0 and newer
Avamar NDMP Accelerator	Not supported	Supported
Debian Linux	Not supported	Supported
Mac OS X	Not supported	Supported
Red Hat Linux	Supported	Supported
Solaris	Not supported	Supported
SuSE Linux Enterprise Server	Supported	Supported
Ubuntu	Not supported	Supported
Windows[1]	Supported	Supported

1. Use of the Upgrade Clients feature to upgrade Avamar client software on Windows cluster nodes is not supported. The *Avamar for Windows Servers Guide* describes how to upgrade Avamar client software on Windows cluster nodes.

- Install Avamar server version 6.0 and newer on the Avamar servers associated with the clients and plug-ins selected for upgrade.
- Install, configure, and run the Avamar Downloader Service.

  The Avamar Downloader Service obtains the client packages and plug-in packages required by the upgrade feature. This service pulls the packages from EMC and pushes them onto the Avamar data server subsystem (GSAN). After the packages are updated in GSAN, the packages appear in Avamar Client Manager's **Select Package** window, and upgrades can be performed.

For information about how to obtain packages without using the Avamar Downloader Service refer to the technical note *Client-Only System Upgrades* available through the EMC online support web site at https://support.emc.com/products.

Multiple system deployments

For Avamar deployments that involve more than one Avamar system, Avamar Client Manager running on one of the Avamar systems (managing system) can be used to manage clients associated with other Avamar systems (managed systems).

The managed systems must meet the following requirements:

- Managed system is added to Enterprise Manager on the managing system.

  Adding managed systems to Enterprise Manager on the managing system provides the managing system with the information it needs to support client upgrades on the managed systems. "Monitoring other systems" on page 348 describes how to add systems to Enterprise Manager.

- Managed system is running the same version of Avamar software as the managing system.

The same version requirement ensures that all packages required by clients on the managed systems are available for deployment through the managing system.

To provide full client upgrade support for clients associated with Avamar systems that do not meet the same version requirement, run Avamar Client Manager on those systems.

Downloading upgrade and hotfix packages

Use Avamar Client Manager to download upgrade and hotfix packages to an Avamar server.

Before you begin, do the following:

- Install and configure the Avamar Downloader Service and the AvInstaller service. Refer to the administration guide for information about these tasks.
- Select an Avamar server.

Before applying an upgrade or hotfix package to an Avamar client, download the package to the Avamar server associated with the Avamar client.

1. On the left-side menu, click **Clients** › **Upgrade Clients**.
2. On the **Actions** bar, click **Select Package**.

   The **Upgrade Client** dialog box appears.
3. In the **Status** column for the package, click **Download**.

   The status of the package must be "Available".

Avamar Client Manager begins the download. A progress bar appears. After the download finishes, Avamar Client Manager updates the package status, in sequence, to each of the following values: Waiting, Processing, and Ready.

Package status values

The **Upgrade Client** dialog box provides information about the availability of upgrade packages and hotfix packages in the **Status** column.

The following table describes the values that can appear in the **Status** column of the **Upgrade Client** dialog box.

Table 111 Descriptions of package status values

Value	Description
Available	The package is available in the EMC package repository. The status entry includes a Download link. Use this link to begin the download of the file to the selected Avamar server.
Downloading	Avamar Client Manager is downloading the package to the selected Avamar server. Avamar Client Manager depicts the progress of the download using a progress bar.
Download failed	Avamar Client Manager could not download the package to the selected Avamar server. This status value appears for 3 seconds and then Avamar Client Manager resets the value to Available.
Waiting	Avamar Client Manager is waiting for the selected Avamar server to begin entering the downloaded package's information into the Avamar data server.
Processing	Avamar Client Manager is waiting for the selected Avamar server to finish entering the downloaded package's information into the Avamar data server.
Ready	The package is available on the selected Avamar server and Avamar Client Manager can apply it to eligible clients.

Selecting an upgrade package

Select an upgrade package or hotfix package to apply to Avamar clients.

Before you begin, do the following:

- Install and configure the Avamar Downloader Service and the AvInstaller service. Refer to the administration guide for information about these tasks.
- Select an Avamar server.
- Download the upgrade or hotfix package to the selected Avamar server.

1. On the left-side menu, click **Clients** › **Upgrade Clients**.
2. On the **Actions** bar, click **Select Package**.

   The **Upgrade Client** dialog box appears.
3. Select a package.

   Before you can select a package, the package must have a Ready status.
4. Click **Select**.

   The **Upgrade Client** dialog box closes.

The Avamar clients that are eligible for the upgrade or the hotfix appear.

After you finish this task, select clients and apply the upgrade or hotfix package to them.

Applying the upgrade package

Select Avamar clients and apply the upgrade package or hotfix package.

Before you begin, select an upgrade package or hotfix package. View the list of Avamar clients that are eligible for the selected package.

1. From the list of Avamar clients that are eligible for the upgrade or the hotfix, select a client.

   You can select more than one client.

2. On the **Actions** bar, click **Upgrade**.

Avamar Client Manager starts upgrading the selected clients. The upgrade runs in the background.

After you finish this task, track the progress of the upgrade in the **Upgrade** section of the **Queues** page. View the final status of the upgrade in the **Upgrade** section of the **Logs** page.

Deleting upgrade and hotfix packages

Use Avamar Client Manager to delete upgrade and hotfix packages from an Avamar server.

Before you begin, select an Avamar server that has an unneeded upgrade or hotfix package.

1. On the left-side menu, click **Clients** › **Upgrade Clients**.
2. On the **Actions** bar, click **Select Package**.

   The **Upgrade Client** dialog box appears.

3. Select a package.

   You can only delete packages that have a Ready status.

4. Click **Delete**.

Avamar Client Manager removes the selected package from the Avamar server.

Policies page

Avamar Client Manager's **Policies** page provides access to group policies and to group members.

The **Policies** page includes a summary view of the policies for the groups on the selected Avamar server.

Use the **Policies** page to perform the following tasks:

- Add clients to a group
- Remove clients from a group
- View the details of a group's dataset policy, retention policy, and schedule policy

Columns on the Policies page summary view

The following table describes the columns that appear in the **Policies** page summary view.

Table 112 Descriptions of the columns on the Policies page summary view

Column	Description
Name	Label assigned to the group in Avamar.
Domain	Avamar domain of the group.
Activated Clients	Number of activated clients associated with the group.
Dataset	Name of the dataset policy assigned to the group. Click the name to view the group's dataset policy.
Schedule	Name of the schedule policy assigned to the group. Click the name to view the group's schedule policy.
Retention	Name of the retention policy assigned to the group. Click the name to view the group's retention policy.

Adding clients to a group

To apply the policies of a group to clients, add the clients to the group.

This task results in an association between a client and a group. The Avamar server applies the group's policies to the client.

1. Click **Policies** › **Groups**.
2. Select a group.
3. Click **Edit Group Members**.

   The **Edit Group Members** dialog box appears.
4. Click **Add**.

   The **Add Clients to Group** dialog box appears.
5. Select a client.

   You can select more than one client.
6. Click **Add**.

Avamar Client Manager adds the clients to the group.

Removing clients from a group

To remove the policies of a group from clients, remove the clients from the group.

This task removes the association between a client and a group. When you complete the task the group's policies no longer apply to the client.

1. Click **Policies** › **Groups**.
2. Select a group.
3. Click **Edit Group Members**.

   The **Edit Group Members** dialog box appears.
4. Select a client.

   You can select more than one client.
5. Click **Remove**.

Avamar Client Manager removes the clients from the group.

Viewing a group's dataset policy

Use a group's entry on the **Policies** page to view details of the group's dataset policy.

1. Click **Policies** › **Groups**.

   A summary view of the groups on the selected server appears.
2. On a group's entry, in the **Dataset** column, click the name of the dataset policy.

The selected group's dataset policy details appear in a dialog box.

Dataset policy details

In determining a group's dataset the following logical processing steps are used:

1. Avamar creates an initial dataset consisting of the data specified in Source.
2. Avamar removes the data in the dataset that matches a rule in Excludes.
3. Avamar adds back the data removed from the dataset by Excludes when it matches a rule in Includes.

The following table describes the attributes that appear in the dataset policy dialog box.

Table 113 Descriptions of the attributes displayed in the dataset policy dialog box

Attribute	Description
Source	A hierarchical view of the data that is the source for backups. This data is from at least one Avamar plug-in and, for each plug-in, consists of a defined file system hierarchy, either the entire file system or selected folders.
Excludes	Folders and file types in the dataset specified by Source that Avamar excludes from the final dataset.
Includes	Folders and file types that Avamar includes back into the final dataset.

Viewing a group's retention policy

Use a group's entry on the **Policies** page to view details of the group's retention policy.

1. Click **Policies** › **Groups**.

   A summary view of the groups on the selected server appears.

2. On a group's entry, in the **Retention** column, click the name of the retention policy.

The selected group's retention policy details appear in a dialog box.

Retention policy details

The following table describes the attributes that appear in the retention policy dialog box.

Table 114 Descriptions of the attributes displayed in the retention policy dialog box

Attribute	Description
Name	Label assigned to the retention policy.
Domain	Avamar domain of the retention policy.
Override	Displays the current state of the retention policy setting Override basic retention policy for scheduled backups: • Yes The setting is selected. The basic retention policy is ignored for scheduled backups. • No The setting is not selected. The basic retention policy is applied for scheduled backups.
Basic Expiration Date	The length of time that the Avamar server retains a backup's root hash for untagged backups.
Keep days of daily	The number of days that the Avamar server retains a backup's root hash for backups tagged as a daily retention type.
Keep weeks of weekly	The number of weeks that the Avamar server retains a backup's root hash for backups tagged as a weekly retention type.
Keep months of monthly	The number of months that the Avamar server retains a backup's root hash for backups tagged as a monthly retention type.
Keep years of yearly	The number of years that the Avamar server retains a backup's root hash for backups tagged as a yearly retention type.

Viewing a group's schedule policy

Use a group's entry on the **Policies** page to view details of the group's schedule policy.

1. Click **Policies** › **Groups**.

   A summary view of the groups on the selected server appears.

2. On a group's entry, in the **Schedule** column, click the name of the schedule policy.

The selected group's schedule policy details appear in a dialog box.

Schedule policy details

The following table describes the attributes that appear in the schedule policy dialog box.

Table 115 Descriptions of the attributes displayed in the schedule policy dialog box

Attribute	Description
Name	Label assigned to the schedule policy.
Domain	Avamar domain of the schedule policy.
Native Timezone	Time zone of the schedule policy's Avamar server.
Daylight Savings Adjustment	Indicates whether a DST adjustment is in effect on the Avamar server. • Yes DST adjustment is in effect. • No DST adjustment is not in effect.
Next Run Time (Native)	Expected date and time of the next scheduled backup, expressed in the Avamar server's time zone.
Next Run Time (Local)	Expected date and time of the next scheduled backup, expressed in the web browser's time zone.
Backup Window Duration	Number of hours after the start time that the backup can run.
Repeat	Recurrence type: • Daily • Weekly • Monthly
Hours of Day AM	(Daily schedules only) Specifies the hours of the day between midnight and noon, when the group's backups start.
Hours of Day PM	(Daily schedules only) Specifies the hours of the day between noon and midnight, when the group's backups start.
Days of Week	(Weekly schedules only) Specifies the days of the week when the group's backups start.
Days of Month	(Monthly schedules only) Specifies the day of the month when the group's backups start.
Delay Start Until (Local)	Start date and time of the group's first backup, in the web browser's time zone.
End Policy (Local)	Effective period of the schedule policy: • No End Date The schedule policy runs indefinitely. • End After *end_date* The schedule policy terminates after *end_date*, where *end_date* is a date value and a time value.
Description	Descriptive text assigned to the schedule policy.

Queues page

Avamar Client Manager's **Queues** page provides access to the Avamar Client Manager activity queues.

The **Queues** page provides a summary view of active and pending Avamar Client Manager tasks for the selected Avamar server. Tasks appear in separate sections based on the type of task, as follows:

- Activation

  Click **Queues** › **Activation** to view active and pending tasks related to client activation.

- Delete

  Click **Queues** › **Delete** to view active and pending tasks related to the removal of clients from Avamar servers.

- Move

  Click **Queues** › **Move** to view active and pending tasks related to moving clients from one Avamar server to another.

- Retire

  Click **Queues** › **Retire** to view active and pending tasks related to retiring Avamar clients.

- Upgrade

  Click **Queues** › **Upgrade** to view active and pending tasks related to upgrading the software on Avamar clients.

Use the **Queues** page to perform the following tasks:

- View the details of active and pending tasks
- Cancel tasks

Columns on the Queues page summary view

The following table describes the columns that appear in the **Queues** page summary view.

Table 116 Descriptions of the columns displayed on the Queues page summary view

Column	Description
Client	Name of the Avamar client.
Status	Current status of the event.
Status Code	Numeric code assigned to the current status.
Description	Brief description of the event.
User	Login name of the person who started the event.
Date	Date and time that the event started.

Activation queue descriptions

Avamar Client Manager provides information about the current state of an activation task in the Activation queue's summary.

The following table provides information about some of the entries that can appear in the Description field of the Activation queue summary.

Table 117 Descriptions of entries in the Description field of the Activation queue summary

Entry format	Description
Activation at commit failed. Client scheduled for 24 retries. *message*	Entry that appears in the queue after the first failure of a client activation, where *message* describes the cause of the failure.
(*n*/24) - Activation failed - *message*	Second and subsequent entries that appear in the queue for failed client activations, where: • *n* is an integer. The integer is initially 1, and increases by 1 after each try. • *message* describes the cause of the failure.
Invitation failed. - *message*	Final entry that appears in the queue for a failed client activation, displayed after 24 attempts fail, where *message* describes the cause of the failure.

Canceling a task

Cancel a pending task to prevent it from running.

You can stop a task from running by canceling it while it is in the pending state.

1. On the left-side menu, click **Queues** › *task_queue*, where *task_queue* is the **Queues** page section for the type of task you are canceling.

   For example to cancel a client activation, click **Queues** › **Activation**.
2. Select a task.
3. Click **Cancel**.

   A confirmation dialog box appears.
4. Click **OK**.

Avamar Client Manager removes the task from the queue, cancels the task, and adds an entry to the log.

Logs page

Avamar Client Manager's **Logs** page provides access to the Avamar Client Manager logs.

The **Logs** page provides a summary view of Avamar Client Manager logs. Log entries appear in separate sections based on the type of task that generated the entry, as follows:

- Activation

  Click **Logs** › **Activation** to view log entries related to client activation.

- Delete

  Click **Logs** › **Delete** to view log entries related to the removal of clients from Avamar servers.

- Move

  Click **Logs** › **Move** to view log entries related to moving clients from one Avamar server to another.

- Retire

  Click **Logs** › **Retire** to view log entries related to retiring Avamar clients.

- Upgrade

  Click **Logs** › **Upgrade** to view log entries related to upgrading the software on Avamar clients.

Use the **Logs** page to perform the following tasks:

- View log entries
- View the client log for upgrades
- Clear all log entries in a section

Columns on the Logs summary view

The following table describes the columns that appear in the logs summary view.

Table 118 Descriptions of the columns displayed in the logs summary view

Column	Description
Client	Name of the Avamar client.
Status	Final status of the event.
Status Code	Numeric code assigned to the final status.
Description	Brief description of the event.
User	Login name of the person who started the event.
Date	Date and time the event ended.

Viewing the client log after upgrading an Avamar client

View the Avamar client's local log after a completed upgrade attempt.

Before you begin, use Avamar Client Manager to apply an upgrade package or hotfix to an Avamar client.

Viewing the Avamar client's local log can provide details about the reasons for an unsuccessful client upgrade.

1. On the left-side menu, click **Logs** › **Upgrade**.
2. On the right-side of the page, click the **Details** bar.

   The **Details** panel expands.
3. In **Summary**, select a client upgrade log entry.

   Detailed information for the selected log entry appears in the **Details** panel.
4. On the **Details** panel, in **Log**, click **View Log**.

The **Upgrade Log** window opens and the client's local log appears in the window.

(Optional) After you finish this task, select and copy information from the client's local log. Paste the copied information into a text editor.

Clearing all log entries in a section

Avamar Client Manager provides a method for you to remove all log entries from a task section of the **Logs** page.

Before you begin, complete at least one task that results in a log entry in one of the task sections of the **Logs** page.

1. On the left-side menu, click **Logs** › **task_log**, where **task_log** is a **Logs** page section.

   For example, to clear all upgrade entries, click **Logs** › **Upgrade**.
2. Click **Clear All**.

   The **Alert** dialog box appears.
3. Click **Yes**.

Avamar Client Manager removes all log entries for the selected section.

CHAPTER 20
Avamar Desktop/Laptop

Avamar Desktop/Laptop is a version of the Avamar client software that adds enhanced features for enterprise desktop and laptop computers.

The Avamar Desktop/Laptop features are designed to improve functionality of Avamar client for Windows and Macintosh desktops and laptops. Many of the features are also supported on qualifying Linux computers.

The following topics provide information about Avamar Desktop/Laptop:

- Features 538
- Environment requirements 539
- User authentication 542
- Apache web server authentication 549
- Web UI port change 549
- Secure token time-out value 551
- Alternate file browsing method for clients 552
- Rebranding the web UI 552
- Checking the status of Avamar Desktop/Laptop server 553
- Stopping and starting Avamar Desktop/Laptop server 554
- User selectable backup start times 554
- On-demand backups 555
- Source data additions 558
- Selectable backup sets 558
- Restore of replicated backups 559
- Restore from an alternate computer 559
- Server-class clients 562
- Restore data size limit 565
- Restore queue limit 566
- Avamar client software installation 567
- Remove the Avamar client software 571
- Client log locations 571

Features

Single-click and interactive on-demand backups — Users can start an on-demand backup with a single-click on the client menu, or open the web browser UI for an interactive on-demand backup.

Web browser UI — Restore by search, restore by browse, on-demand backup, and activity history are all available through a convenient web browser user interface. This UI is available for Avamar clients on Windows, Mac, and qualifying Linux computers.

User authentication and data security options — Authenticate users through the enterprise's Active Directory or OpenLDAP-compliant directory service, with or without Kerberos encryption. Alternatively, authenticate users using built-in Avamar authentication, or a combination of Avamar authentication and LDAP authentication. Optionally, use NIS to authenticate users.

Transparent login — Enable users to access the web UI without using the login screen. A secure message mechanism is used to authenticate users based on information from the client computer. This also gives administrators the ability to allow non-domain users to restore files to their local account on the computer.

User selectable backup schedules — Avamar domains can be configured to enable users to select from a list of available backup schedules. The system runs the backup as soon as possible after the selected time.

Restore of folders and files to the original location — Users can restore folders and files to the original location. The same name can be used or, to avoid overwriting a file, a new name can be generated.

Restore of files to an alternate location — Users can restore files to an alternate location on their computer.

Restore files from other computers — Domain users can restore files from any Windows or Mac computer on which they have a user profile to the Windows or Mac computer they are logged in to.

Creation of a restore set by search or directory tree browse — Users can use search or can browse a backup directory tree to create a set of folders and files to restore. Files can be restored to their original location or to a new location.

Activity history — Users can view a 14-day history of the status of restore and backup tasks, and listings of the folders and files backed up during that period.

Deploy Avamar clients using common systems management tools — In a corporate environment, Avamar Desktop/Laptop can be push installed on Windows and Macintosh desktop and laptop computers using systems management tools such as Microsoft Systems Management Server 2003 (SMS).

Manage using Avamar Client Manager — Activate, upgrade, analyze, and manage clients using the Avamar Client Manager web browser UI.

Environment requirements

The Avamar Desktop/Laptop environment must meet the requirements in the following topics:

- "Computer requirements" on page 539
- "Network requirements" on page 540
- "LDAP authentication requirements" on page 540
- "Avamar system requirements" on page 541

Computer requirements

Avamar client computers using Avamar Desktop/Laptop must meet the minimum requirements in the following table.

Table 119 Minimum requirements for client computers using Avamar Desktop/Laptop

Category	Requirement
Operating system	Windows, Mac, or Linux operating system that is supported for use with Avamar client. **Note:** Windows Server, Mac OS X Server, and Linux computers that meet the requirements specified in the EMC Avamar Backup Clients User Guide are supported as server-class clients, as described in "Server-class clients" on page 562.
CPU	1 GHz
RAM	1 GB
Hard drive space	250 MB permanent hard drive space minimum for software installation. **Note:** Additional space may be required by snapshot technology and to back up system state.
Network interface	Either of the following: • 10BaseT or higher, configured with the latest drivers for the platform • IEEE 802.11a/b/g, configured with the latest drivers for the platform
Ports	TCP data port must allow bidirectional communication with the Avamar server.
Web browser	JavaScript-enabled web browser. On Windows: • Windows Internet Explorer • Mozilla Firefox • Google Chrome On Macintosh: • Apple Safari On Linux: • Mozilla Firefox The browser must be configured to be launched by a call to one of the following environment variables: • (For KDE) kfmclient • (For GNOME) gnome-open • (Others) BROWSER

Network requirements

The networks must meet the requirements in the following table.

Table 120 Network requirements

Category	Requirement
Protocol	TCP/IP.
Routers	Must permit TCP packet routing between the Avamar server and each client computer.
Firewalls	Must allow bidirectional communication between the Avamar server and each client computer using TCP data port 28002.
Naming system	Must facilitate connections between each client and the Avamar server, including situations where IP address changes are caused by DHCP and VPN access.

LDAP authentication requirements

To use LDAP authentication the environment must meet the minimum requirements in the following table.

Table 121 LDAP authentication requirements

Category	Requirement
Directory service	LDAP v.3 compliant systems, such as Microsoft Active Directory and OpenLDAP.
Domain components	The configuration of the Avamar Desktop/Laptop server must correctly describe any domain components used to segregate authentication. Also, the Kerberos realm for LDAP user authentication from Macintosh computers must be the default Kerberos realm.
User accounts	• Users must log in to the client computer using a domain account authenticated through a domain directory service. **Note:** A local account is permitted when local user access is enabled. • The root account on a Mac cannot be used to restore files from backups.

Avamar authentication requirements

To use Avamar authentication the environment must meet the minimum requirements in the following table.

Table 122 Avamar authentication requirements

Category	Requirement
Naming system	Client computers must have a static, resolvable, fully qualified domain name.
User accounts	Users must have a local or domain login account for the client computer. Users must also have an account on the Avamar server domain associated with the client computer.

NIS authentication requirements

To use NIS authentication the environment must meet the minimum requirements in the following table.

Table 123 NIS support requirements

Category	Requirement
NIS domain name	Client computers must all use the same static, resolvable, fully qualified NIS domain name.
NIS domain	Users must have properly configured user accounts in the NIS domain.

Avamar system requirements

You should work with an EMC field sales representatives when deciding on the characteristics of the Avamar system deployment that work best to support an enterprise's desktop and laptop clients.

Due to the wide range of differences in each enterprise's desktop and laptop topology, a description of the requirements for an Avamar system to support desktops and laptops at any one enterprise is beyond the scope of this guide.

NOTICE

Avamar Desktop/Laptop supports backup and restore using Avamar file system plug-ins on Windows, Mac, and Linux computers. Avamar Desktop/Laptop does not support other Avamar plug-ins.

User authentication

Avamar Desktop/Laptop protects backed up data by authenticating users and enforcing access rights. Avamar Desktop/Laptop uses a separate server process running on the Avamar system to facilitate authentication through both internal and external methods. Every Avamar system installation includes the Avamar Desktop/Laptop server process.

Avamar Desktop/Laptop provides user authentication through the methods described in these sections:

- "Pass-through authentication" on page 542
- "LDAP authentication" on page 544
- "NIS authentication" on page 546
- "Avamar authentication" on page 547

Pass-through authentication

Pass-through authentication uses encrypted channels to access user credentials from a client computer and associate the credentials with file ownership properties. The client computer's operating system obtains the user's credentials during log in to the computer or through common access card (CAC) technology.

Avamar Desktop/Laptop performs pass-through authentication transparently. Users can back up and restore files without seeing the Avamar Desktop/Laptop login screen.

Avamar Desktop/Laptop enables pass-through authentication by default. It is limited to users on Windows computers and Mac computers. Also, Windows users with local administrator privileges can restore files owned by anyone on the computer without additional login.

Pass-through authentication requires information that is attached to backups generated by Avamar client, version 6.x and later. Pass-through authentication users can view and restore only their data that is contained in backups generated by Avamar client, version 6.x and later.

Compatibility with other methods

Pass-through authentication can be used with LDAP authentication. "LDAP authentication" on page 544 describes how to configure Avamar Desktop/Laptop to use LDAP authentication.

Pass-through authentication can be used with NIS authentication. Users on Linux computers can be authenticated by your enterprise's NIS. "NIS authentication" on page 546 describes how to configure Avamar Desktop/Laptop to use NIS authentication.

Pass-through authentication can be used with Avamar authentication. Avamar Desktop/Laptop determines if the client computer is in one of the specified Avamar domains. It authenticates users of those computers through Avamar authentication. It authenticates other users through pass-through authentication. "Avamar authentication" on page 547 describes how to configure Avamar Desktop/Laptop to use Avamar authentication.

Enabling local user access

Optionally, configure Avamar Desktop/Laptop to allow local user access through pass-through authentication. A local user is one who is authenticated through a local computer account instead of a domain account.

With local user access enabled, local users can access the Avamar client web UI to restore data they own on the authenticating computer.

Local user access requires pass-through authentication on a Windows computer or a Mac computer. By default local user access is disabled.

NOTICE

Before enabling local user access carefully consider its security implications within the context of the organization. Local user authentication is inherently less secure than domain authentication.

To enable local user access:

1. Enable pass-through authentication.

   For more information, see "Pass-through authentication" on page 542.

2. Open a command shell and log in:

   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.

3. Switch user to root by typing:

   ```
   su -
   ```

   The following change applies to all clients and backups associated with the server.

4. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

5. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor, such as vi or Emacs.

6. Uncomment the local user key and set its value to true.

   Change:

   ```
   #allowLocalUsers=false
   ```

   To:

   ```
   allowLocalUsers=true
   ```

7. Save and close the file.

Disabling pass-through authentication

You can disable pass-through authentication and require that all users log in through the Avamar Desktop/Laptop login screen. When pass-through authentication is disabled, configure one of other methods of authentication for Windows users and Mac users.

To disable pass-through authentication:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Create or edit the value of the userLoginRequired key:

   Change:

   ```
   userLoginRequired=false
   ```

   to:

   ```
   userLoginRequired=true
   ```

6. Save and close the file.

LDAP authentication

You can configure Avamar Desktop/Laptop to use an LDAP v.3-compliant directory service to authenticate users with their directory service username and password. The authentication process uses Kerberos in a Simple Authentication and Security Layer (SASL) Bind by default. You can configure it to use plaintext in a Simple Bind.

To increase the security of user data, Avamar Desktop/Laptop obtains the domain username of a Windows user or Mac user from their computer and enters it in a read-only field on the Avamar Desktop/Laptop login screen.

Compatibility with other methods

SASL Bind LDAP authentication can be used with pass-through authentication. Plaintext LDAP is not compatible with pass-through authentication. "Pass-through authentication" on page 542 describes pass-through authentication.

LDAP authentication can be used with NIS authentication. Users on Linux computers are authenticated by your enterprise's NIS. "NIS authentication" on page 546 describes how to configure Avamar Desktop/Laptop to use NIS authentication.

LDAP authentication can be used with Avamar authentication. Avamar Desktop/Laptop determines if the client computer is in one of the specified Avamar domains. It authenticates users of those computers through Avamar authentication. It authenticates

other users through pass-through authentication. It authenticates the remaining users through LDAP authentication. "Avamar authentication" on page 547 describes how to configure Avamar Desktop/Laptop to use Avamar authentication.

Configuring LDAP authentication with Kerberos

To configure Avamar Desktop/Laptop to authenticate users through an LDAP v.3-compliant directory service with an SASL Bind:

1. Configure Avamar with information about the directory service, as described in "Providing LDAP information" on page 413.
2. Return to the **LDAP Management** tab.
3. Click **Edit LDAP file**.
4. In the text area, find the following key:

   user-login-module=*MODULE*

   where *MODULE* is the value for a module type.

   If the key does not exist, type it on a separate line as shown in step 5.
5. Change the key's value by replacing *MODULE* with **kerberos**:

   user-login-module=kerberos

   Kerberos is the default value. Avamar Desktop/Laptop assumes this value when the user-login-module key is missing.
6. Click **Save**.
7. Click **Close**.

Avamar Desktop/Laptop applies the setting and enables LDAP authentication with an SASL Bind.

Changing the specified Kerberos encryption type

The encryption type used by the LDAP with Kerberos authentication method can optionally be changed to a different type. The default configuration of krb5.conf specifies the use of MIT Kerberos encryption type "DES cbc mode with CRC-32" to communicate with LDAP servers. This encryption type may conflict with a key distribution center (KDC) in the Active Directory environment. If that occurs, the message "KDC has no support for encryption type" appears.

A possible solution to this conflict is to remove the specified encryption type from krb5.conf, thereby permitting the KDC to select the encryption type.

To remove the specified Kerberos encryption type:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
2. Click **Edit KRB5 file**.
3. In the text area, find the following entries:

```
[libdefaults]
default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

4. Comment out the entries as shown here:

```
#[libdefaults]
# default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
# default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

5. Click **Save**.
6. Click **Close**.

Avamar Desktop/Laptop removes the encryption type specifications.

Configuring LDAP authentication with plaintext

To configure Avamar Desktop/Laptop to authenticate users through an LDAP v.3-compliant directory service with a Simple Bind:

1. Configure Avamar with information about the directory service, as described in "Providing LDAP information" on page 413.
2. Return to the **LDAP Management** tab.
3. Click **Edit LDAP file**.
4. In the text area, find the following key:

   user-login-module=*MODULE*

   where *MODULE* is the value for a module type.

   If the key does not exist, type it on a separate line as shown in step 5.
5. Change the key's value by replacing *MODULE* with **ldap**:

   user-login-module=ldap
6. Click **Save**.
7. Click **Close**.

Avamar Desktop/Laptop applies the setting and enables LDAP authentication with a Simple Bind.

NIS authentication

You can configure Avamar Desktop/Laptop to authenticate Linux users through your enterprise's NIS.

Compatibility with other methods

NIS authentication is compatible with all other authentication methods. After you enable it, Avamar Desktop/Laptop uses NIS to authenticate any user who is logged in to a Linux computer.

Configuring NIS authentication

To configure Avamar Desktop/Laptop to authenticate Linux users through NIS, complete the task described in "Providing NIS information" on page 414.

Avamar authentication

You can configure Avamar Desktop/Laptop to authenticate users through Avamar authentication. In this method Avamar Desktop/Laptop uses internal Avamar domain information.

When you enable Avamar authentication, Avamar Desktop/Laptop compares username/password combinations with user records that have been entered into the Avamar server.

To add user records for Avamar authentication refer to "Adding a user to a client or domain" on page 90.

Avamar authentication works with users who authenticate at the Avamar root level, Avamar domain levels, or Avamar subdomain levels. The mechanism first checks at the subdomain level. If the username is found at that level, then authentication proceeds. If the username is not found, then the next level up is checked. This continues until the username is found, or the Avamar root is reached without finding the username.

For example, if the login computer, 123abc.example.com, is activated with the /clients/mountain Avamar subdomain, then the mechanism makes checks in the following order until the username is found:

1. /clients/mountain (activation subdomain)
2. /clients (next level up)
3. / (root)

Avamar roles

Avamar Desktop/Laptop applies the role assigned by a user's Avamar user account when it grants access through Avamar authentication. User roles are described in "User roles" on page 83.

Avamar Desktop/Laptop permits users to perform only those operations that are allowed by their role. The one exception is that users with the Restore only operator role can launch a backup from Avamar Desktop/Laptop.

Compatibility with other methods

Avamar authentication is compatible with all other authentication methods. Avamar Desktop/Laptop uses the following sequence for authentication:

1. Uses Avamar authentication to authenticate users on a client assigned to one of the specified Avamar domains.
2. When pass-through authentication is enabled, authenticates qualified users, who are not logged in to a client assigned to a specified Avamar domain, using pass-through authentication.
3. When NIS authentication configured, authenticates all Linux users, who are not logged in to a client assigned to a specified Avamar domain, through NIS.
4. When mixed authentication is enabled and LDAP is configured, authenticates users, who are not logged in to a client assigned to a specified Avamar domain, through LDAP.

You can configure Avamar Desktop/Laptop to use Avamar authentication in the following configurations:

- With all other configured authentication methods
- With all other configured authentication methods, except LDAP

Configuring Avamar authentication with all other methods

To configure Avamar Desktop/Laptop to use Avamar authentication and all other configured and enabled authentication methods:

1. Add Avamar user records to domain-level lists as described in "Adding a user to a client or domain" on page 90.
2. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
3. Click **Edit LDAP file**.
4. In the text area, find the following key:

   `user-login-module=`*`MODULE`*

   where *MODULE* is the value for a module type.

   If the key does not exist, type it on a separate line as shown in step 5.
5. Change the key's value by replacing *MODULE* with **mix**:

   `user-login-module=mix`
6. In the text area, type the following key/value pair:

   `avamar-authentication-domains=`*`DOMAIN1,DOMAIN2,DOMAIN3,...`*

   where *DOMAIN1,DOMAIN2,DOMAIN3,...* is a comma-separated list of Avamar domains.

   Avamar Desktop/Laptop uses Avamar authentication to authenticate users who are logged in to a client assigned to one of the specified Avamar domains.
7. Click **Save**.
8. Click **Close**.

Avamar Desktop/Laptop applies the setting and enables Avamar authentication and all other configured and enabled authentication methods.

Configuring Avamar authentication with all other methods, except LDAP

To configure Avamar Desktop/Laptop to use Avamar authentication and all other configured and enabled authentication methods, except LDAP:

1. Add Avamar user records to domain-level lists as described in "Adding a user to a client or domain" on page 90.
2. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 412.
3. Click **Edit LDAP file**.

4. In the text area, find the following key:

   user-login-module=*MODULE*

   where *MODULE* is the value for a module type.

   If the key does not exist, type it on a separate line as shown in step 5.

5. Change the key's value by replacing *MODULE* with **avamar**:

   user-login-module=avamar

6. In the text area, type the following key/value pair:

   avamar-authentication-domains=*DOMAIN1,DOMAIN2,DOMAIN3,...*

   where *DOMAIN1,DOMAIN2,DOMAIN3,...* is a comma-separated list of Avamar domains.

   Avamar Desktop/Laptop uses Avamar authentication to authenticate users who are logged in to a client assigned to one of the specified Avamar domains.

7. Click **Save**.

8. Click **Close**.

Avamar Desktop/Laptop applies the setting and enables Avamar authentication and all other configured and enabled authentication methods, except LDAP.

Apache web server authentication

To protect user security, web browsers display an authentication warning when accessing a secure web page unless the web server provides a trusted public key certificate with the page. The Avamar Desktop/Laptop UI uses only secure web pages, and this warning is seen in browsers that access those pages. To avoid the warning, install a trusted public key certificate on the Apache web server provided with Avamar.

The *EMC Avamar Product Security Guide* describes how to obtain and install a trusted public key certificate for the Apache web server.

Web UI port change

Access to the web UI involves HTTPS communication between the Avamar server and the client's web browser. When a user requests a back up or restore by using the Avamar client menu, the default web browser on the client is instructed to contact the Avamar server on port 443, the standard HTTPS port. On the Avamar server, this initial request to port 443 is redirected to port 8443, the HTTPS port for the web UI.

The initial contact port can be changed. This change involves a configuration file command on the client and changes to the Apache SSL configuration file on the server.

Changing the port on the client

To change the initial contact port on Avamar client:

1. Open the avscc configuration file in a plain text editor.

   This file is located in the Avamar var directory on the client.

Table 124 Path to avscc.cfg

OS	Path
Windows	%SystemDrive%\Program Files\avs\var\avscc.cfg
All others	/usr/local/avamar/var/avscc.cfg

   If avscc.cfg does not exist at this location then create it.

2. Add the following line to avscc.cfg:

   --port=*n*

   where *n* is the new initial contact port.

3. Save and close avscc.cfg.
4. Restart the client

Changing the port on the server

To change the HTTPS listening port on Avamar server:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   su -

3. Open the Apache SSL configuration file in a plain text editor.

Table 125 Path to Apache SSL configuration file

OS	Path
Red Hat Enterprise Linux	/etc/httpd/conf.d/ssl.conf
SuSE Linux Enterprise Server	/etc/apache2/vhosts.d/vhost-ssl.conf

4. Find and change the HTTPS port listening directive.

   Change:

   `Listen 443`

   to

   `Listen n`

   where *n* is the new initial contact port.

5. Save and close the file.
6. Restart the Apache server daemon, httpd, using **apachectl**:

   ```
   apachectl restart
   ```

Secure token time-out value

Avamar Desktop/Laptop includes a secure token as part of the URL it uses to begin a backup session or restore session in a client's web browser. The secure token is valid for a short time and then expires. A backup or restore session cannot be opened with an expired token.

The client's web browser must establish an HTTPS connection with the Avamar server within the time-out period of the token or the session is rejected. By default, the time-out value is 20 seconds. This value can be changed.

Changing the secure token time-out value

To change the time that a secure token is valid:

1. Open a command shell and log in using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server:
     a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

        ```
        ssh-agent bash
        ssh-add ~admin/.ssh/admin_key
        ```

     b. When prompted, type the admin_key passphrase and press **Enter**.
2. Stop the Management Console Server (mcs) service by typing:

   ```
   dpnctl stop mcs
   ```

3. Change the working directory by typing:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Open mcserver.xml in a plain text editor.
5. Find the dtlt node, as shown here:

   ```
   <node name="dtlt">
      <map>
         <entry key="expire_data_after_secs" value="20" />
      </map>
   </node>
   ```

6. Change the value of the entry with key="expire_data_after_secs" to a new time-out value:

```
<node name="dtlt">
   <map>
      <entry key="expire_data_after_secs" value="SS" />
   </map>
</node>
```

   where *SS* is the new time-out value, in seconds.

7. Save the change and close the editor.
8. Restart mcs by typing:

   dpnctl start mcs

9. Close the command shell.

Alternate file browsing method for clients

The Avamar client web UI uses a file manager interface for several of its tasks. This interface allows users to select local files and folders to backup or restore. Normally, Avamar client web UI uses the client computer's OS-specific file browsing services to provide the file management interface. However, if these services are not available, an alternate file browsing method is offered.

Possible reasons for the unavailability of the default browsing services are:

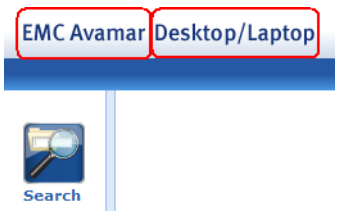
- Port 28002 on the client is blocked by a firewall rule
- The client is behind a NAT

The alternate method uses a Java applet to provide file browsing services. When the default services are unavailable, and the user elects to permit the alternate method, the Java applet is loaded. During loading of the applet the user may see authentication warnings about the web site certificate of the Avamar server and the Java applet's digital signature. These warnings must be affirmatively acknowledged or the applet will not load.

After the applet loads, the web page is automatically refreshed to allow the Avamar client web UI to use the applet. The user must restart the task after the page is refreshed.

Rebranding the web UI

Rebrand the Avamar client web UI by replacing the two logo graphics located at the top left corner of the UI.



To replace the logo graphics:

1. Create the two replacement graphics. The graphics should meet the following requirements:
   - Portable Network Graphic (png) format
   - Transparent background to allow the background gradient to be seen behind the graphic text and images
   - Named ProductNameAvamar.png and ProductNameDTLT.png
   - 97 px wide and 18 px tall for ProductNameAvamar.png, and 128 px wide and 18 px tall for ProductNameDTLT.png
2. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
3. Switch user to root by typing:

   ```
   su -
   ```

4. Change the working directory by typing:

   ```
   cd /usr/local/avamar-dtlt-tomcat/webapps/dtlt/images/banner
   ```

5. Make backup copies of the original graphics by typing:

   ```
   cp ProductNameAvamar.png ProductNameAvamar.png_orig
   cp ProductNameDTLT.png ProductNameDTLT.png_orig
   ```

6. Move the new logos into the current working directory as "ProductNameAvamar.png" and "ProductNameDTLT.png".

   In some web browsers, with certain cache settings, the new graphic may not appear right away.
7. To view the new graphic on those browsers, follow the browser instructions for deleting cached copies of previously viewed files and refresh the page.

Checking the status of Avamar Desktop/Laptop server

To check the status of Avamar Desktop/Laptop server:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Use dpnctl to obtain status information about the Avamar Desktop/Laptop server:

   ```
   dpnctl status dtlt
   ```

Stopping and starting Avamar Desktop/Laptop server

When you restart the Avamar utility node, the Avamar Desktop/Laptop server restarts automatically. However, you also can manually stop and start the Avamar Desktop/Laptop server.

To stop and start Avamar Desktop/Laptop:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. To stop Avamar Desktop/Laptop, type:

   ```
   dpnctl stop dtlt
   ```

4. To start Avamar Desktop/Laptop, type:

   ```
   dpnctl start dtlt
   ```

User selectable backup start times

With Avamar Desktop/Laptop you can allow users to select a different start time for their backups. Users select from a list of available times that you create. Selections are made through the web UI Backup page. A selection overrides the start time assigned through group policy.

Requirements

The user selectable backup start time feature is available to a user when each of the following is true:

- User's client group uses a Daily schedule.
- Override group schedules setting is enabled for the user's client, as described in "Allowing users to add to source data" on page 182.
- Time entries have been added to the Override Daily Schedule, as described in "Editing the Override Daily Schedule" on page 145.

Available start time list

The available alternative start times appear on the web UI Backup page. The times that appear are defined by editing the Override Daily Schedule, as described in "Editing the Override Daily Schedule" on page 145.

When an entry is removed from the Override Daily Schedule after a user has selected it, the client continues to use the time specified by that entry as its backup start time. This continues until the user next logs into the web UI. At that time the user is prompted to select an new time from the list.

When a client is removed from a group, any record of an alternative start time for that client is also removed.

Time zone

The server's time zone is used when editing the Override Daily Schedule, as described in "Editing the Override Daily Schedule" on page 145.

The client's time zone is used to display the list of available start times on the web UI Backup page.

On-demand backups

Avamar Desktop/Laptop enables on-demand backup functionality by default. This means that authenticated users of an Avamar client can initiate an on-demand backup whenever they choose.

Avamar client users can initiate an on-demand backup through the:

- System tray or menu bar icon (single-click backup)
- Client backup reminder (single-click backup)
- Web UI (interactive backup)

The dataset used by an on-demand backup is determined by the operating system of the computer.

Table 126 Operating systems and associated datasets used by on-demand backups

Operating system	Data backed up
Non-server-class computers	Dataset for each assigned group
Server-class computers	Dataset assigned to the individual computer

To enable users to choose the folders and files included in an interactive on-demand backup, enable selectable backup sets, which is discussed in "Selectable backup sets" on page 558.

On-demand backup limit

Avamar client users do not normally have a specific limit on the number of on-demand backups that they can run from a computer. This default setting relies on the following practical limitations of on-demand backups:

- Only one backup task from a client is allowed in the task queue
- Another backup cannot be started during the time required to successfully back up the client

When these practical limitations are not enough to ensure that the number of on-demand backups do not exceed a specific maximum value, set an on-demand backup limit.

The on-demand backup limit is set using the restrictBackupsPerDay key in dtlt.properties. This setting:

- Applies to all clients activated to an Avamar server
- Counts all successfully completed on-demand backups from a computer towards the total
- Combines on-demand backups from all users that share a computer towards the total

The possible values for the restrictBackupsPerDay key are described in the following table.

Table 127 Possible values for limiting on-demand backups

Value	Description
false	No specific limit on the number of on-demand backups that can be successfully run in a day. This is the default setting.
0	On-demand backups cannot be run by any user.
n	No more than *n* on-demand backups can be run in a day, where *n* is any positive integer less than or equal to 100, and a day is defined as midnight to midnight using the Avamar server's time zone. Unsuccessful backups do not count towards the total.

Setting an on-demand backup limit

To set an on-demand backup limit:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Edit the value of the restrictBackupsPerDay key:

   Change:

   ```
   restrictBackupsPerDay=false
   ```

   To:

   ```
   restrictBackupsPerDay=n
   ```

   where *n* is any positive integer less than or equal to 100, or *n* is **0**.
6. Save and close the file.

Retention policy

The retention of data from on-demand backups is controlled by the End User On Demand Retention policy, described in "Creating a retention policy" on page 150. By default, this policy retains data from on-demand backups for 60 days.

You can change the End User On Demand Retention policy on an Avamar server using Avamar Administrator. The change applies to all on-demand backups initiated by a client activated with that server. However, the change only applies to on-demand backups that occur after the change.

Changing the retention policy

To change the End User On Demand Retention policy on an Avamar server:

1. In Avamar Administrator, select **Tools** › **Manage Retention Policies**.

   The Manage All Retention Policies window appears.

2. Select **End User On Demand Retention** from the list and click **Edit**.

   The Edit Retention dialog box appears.

3. In **Retention period**, enter a number and select a unit of time (**days**, **weeks**, **months**, or **years**).

4. Click **OK**.

Disabling on-demand backups

You can disable on-demand backup capability for one or more clients. Users on a client for which this capability is disabled cannot initiate a backup from the client system tray or menu bar icon or from the web UI.

To disable on-demand backups for a single client:

1. In Avamar Administrator, click the **Policy** launcher button.

   The **Policy** window appears.

2. Click the **Clients** tab.

3. Select the client and click **Edit**.

   The **Edit Client** dialog box appears.

4. Clear **Allow client initiated backups**.

5. Click **OK**.

To disable on-demand backups for multiple clients:

1. In Avamar Administrator, click the **Policy** launcher button.

   The **Policy** window appears.

2. Click the **Clients** tab.

3. Select the clients and click **Edit**.

   The **Edit Multiple Clients** dialog box appears.

4. In **Allow client initiated backups**, select **No**.

5. In **Allow client initiated backups**, select **Apply Change**.

6. Click **OK**.

Source data additions

Avamar Desktop/Laptop allows you to permit users to add folders to the source data defined by their client's groups. When this is enabled, users see the **Add Data** button on the backup page of the web UI. By clicking this button they can select folders to add.

When this feature is enabled:

- Group exclusions and inclusions apply to the additions
- Additions are combined with both automatic and on-demand backups
- Additions are combined with the source data for every group assigned to the client

"Allowing users to add to source data" on page 182 describes how to enable and administer this feature.

Selectable backup sets

Avamar Desktop/Laptop provides the ability to permit users to create sets of folders and files to back up through on-demand backups. When this feature is allowed, users can:

- Specify the folders and files to include in a backup set
- Create multiple backup sets
- Save backup sets for reuse
- Manually start a back up of the folders and files in the backup sets they create

Automatic backup of clients according to their group policies is not affected by this feature.

Enabling this feature for Windows, Mac, and Linux clients that use Avamar Desktop/Laptop requires the completion of two tasks:

- Enable the Avamar Administrator setting **Allow file selection on client initiated backups**, as described in "Allowing users to select data source for on-demand backups" on page 175.
- Change a value in dtlt.properties, as described in "Enabling selectable backup sets" on page 558.

Enabling selectable backup sets

To enable selectable backup sets for Avamar Desktop/Laptop clients:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.

5. Edit the value of the **allowUserInititedBackupsFileSelection** key:

   Change:

   ```
   allowUserInititedBackupsFileSelection=false
   ```

   To:

   ```
   allowUserInititedBackupsFileSelection=true
   ```

6. Save and close the file.

Restore of replicated backups

An Avamar client can be moved to a new server, either by using Avamar Client Manager, or by using Enterprise Manager's replication commands. When a client is moved, its backups are replicated on the new server.

Avamar Desktop/Laptop must index replicated backups before they are available to browse or search in the web UI. Indexing is initiated by a user, after logging in to the web UI.

When a user logs in, the **Replicated Backups Available** dialog appears. The user can choose to initiate indexing of the replicated backups from this dialog, or dismiss the dialog without initiating indexing. When the dialog is dismissed, an alert icon appears on the web UI banner bar. Indexing can also be initiated from the alert icon.

Indexing is a one-time task for a computer that has been moved to a new server. It runs in the same session in which it is initiated. When it is completed, Avamar Desktop/Laptop sends the user's web browser a refresh command and the data from the replicated backups appears in the web UI.

Restore from an alternate computer

The Avamar Desktop/Laptop enhancements allow restores from an alternate computer. This capability permits a user to log in to a computer (target) and restore backups from another computer (source).

To use restore from an alternate computer, the requirements in the following table must be met.

Table 128 Requirements for restoring from an alternate computer (page 1 of 2)

Category	Requirement
Operating system	• Windows operating system • Mac operating system **Note:** Restores between Windows and Mac computers are supported.
Account type	Domain
Profile	Both source and target computers have a local profile for the user's domain account. **Note:** A local profile for a domain account is created automatically at a user's first login on the computer.

Table 128 Requirements for restoring from an alternate computer (page 2 of 2)

Category	Requirement
Avamar client	Version 6.0 or later is installed on both source and target.
Avamar server	Both source and target are activated with the same Avamar server and the server is running Avamar 6.0 or later.
Backup	There is at least one qualifying backup. **Note:** A qualifying backup is one completed successfully after both: • Avamar Desktop/Laptop 6.0 or later is installed on the source computer. • A local profile for the user's domain account is created on the source computer.

When these requirements are met, users can restore files that they own from the source computer to the target computer.

Users with local administrator rights on a Windows source computer at the time of a backup can restore any file from that source computer to a target computer, regardless of ownership. To disable this functionality, see "Restricting file access for Windows administrators" on page 562.

Restoring from an alternate computer

To restore from an alternate computer:

1. Right-click the Avamar system tray icon.

   The client menu opens.

2. Click **Restore**.

   The Search page opens.

3. In the computer list box, select the source computer.

   The list box displays only computers that have at least one qualifying backup for the user logged in to the target computer.

4. Use the Search page or Browse page to select and restore files from the backups of the source computer to the target computer.

Viewing history for an alternate computer

To view the backup and restore history for an alternate computer:

1. Right-click the Avamar system tray icon.

   The client menu opens.

2. Click **Restore**.

   The Search page opens.

3. On the left-side menu, click **History**.

   The History page opens.

4. In the computer list box, select the alternate computer.

   Backup history information for the alternate computer appears.

Disabling restore from an alternate computer

The restore from an alternate computer feature can be turned off. This is a global property and affects all clients.

To disable restore from an alternate computer:

1. Open a command shell and log in:

   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.

2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.

5. Create or edit the value of the **disableRestoreFromAlternateComputer** key:

   Change:

   ```
   disableRestoreFromAlternateComputer=false
   ```

   to:

   ```
   disableRestoreFromAlternateComputer=true
   ```

6. Save and close the file.

Restricting file access for Windows administrators

By default, users with local administrator rights on a Windows source computer at the time of a backup can restore any file from that source computer to a target computer, regardless of file ownership. You can change this behavior to restrict their access to only files that they own.

To restrict file access by Windows administrators:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Create or edit the value of the **checkAlternateComputerOwnership** key:

   Change:

   ```
   checkAlternateComputerOwnership=false
   ```

   to:

   ```
   checkAlternateComputerOwnership=true
   ```

6. Save and close the file.

Server-class clients

In addition to support for traditional desktop and laptop computers, Avamar client also supports server-class computers. A server-class computer is one that is running a supported version of any of the following operating systems:

- Linux
- Windows Server
- Mac OS X Server

Generally, the Avamar Desktop/Laptop enhancements function the same for server-class computers as for desktop and laptop computers. The *differences* are described in the following topics:

- "Back up now dataset" on page 563
- "Backup of large number of files" on page 563
- "Backup on battery power" on page 563
- "Disable restores" on page 564

Back up now dataset

On a server-class computer, clicking **Back Up Now** on the Client menu or on the Backup reminder launches a backup of the dataset assigned individually to the computer.

Viewing or editing a server-class computer's assigned dataset

To view or edit the dataset assigned to a server-class computer:

1. In Avamar Administrator, click the **Policy** launcher button.

   The **Policy** window appears.
2. Click the **Policy Management** tab.
3. Click the **Clients** tab.
4. Select a client.
5. Click **Edit**.

   The **Edit Client** window appears.
6. Click the **Dataset** tab.
7. View or edit the value in **Select an Existing Dataset**.

Backup of large number of files

To accommodate server-class clients with backups that have a large number of files and directories, changes are made to the web UI when a threshold number of file and directory entries is reached. These changes automatically occur when the number of files and directories in a backup exceeds approximately 4 million. The exact number of files that causes these changes is based on the available memory on the Avamar server.

There is no upper limit to the number of files and directories that can be in a backup.

When the threshold is reached, the following changes occur:

- Search page is removed from the web UI.
- History page is removed from the web UI.
- File versions are not available on the Browse page.
- Restore is only allowed for users with local administrator rights on the computer. Non-administrator users cannot restore any files, including those that they own locally on the server-class computer.
- Restore data size limits, described in "Restore data size limit" on page 565, are not enforced.

Backup on battery power

The Avamar Desktop/Laptop enhancements provide a setting that can be used to enable and disable backups for computers running on battery power. This feature is not available for server-class computers. Backups are always enabled on these computers.

Disable restores

You can disable locally initiated restores on both Windows and Macintosh server-class computers with the Avamar Desktop/Laptop enhancements installed by editing the dtlt.properties file. When server-class computer restores are disabled, a restore can only be initiated from Avamar Administrator, as described in "Backup, Restore, and Backup Management" on page 95.

Setting this option has the following impact:

- Prevents locally initiated restores
- Removes the Search and Browse pages from the web UI
- Hides previous versions
- Displays Backup and History pages
- Enables restores of its backups to another computer that is not a server-class computer

To restore to an alternate computer, users must have local administrative rights on the server-class computer. "Restore from an alternate computer" on page 559 provides details.

NOTICE

Disabling restores for server-class computers does not remove the Restore item from the Avamar system tray or Menu bar icon. However, the Restore item's action is blocked.

Disabling restores for server-class computers

To disable restores on server-class computers:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Edit the value of the **allowServerRestores** key:

   Change:

   ```
   allowServerRestores=true
   ```

   To:

   ```
   allowServerRestores=false
   ```

6. Save and close the file.

Restore data size limit

Avamar client users do not normally have a limit on the amount of data that is restored in a single task. This default setting allows a user to restore up to the entire backup in a single task. Very large restore tasks can, in some instances, cause undesirable load on the network.

Set a restore data size limit to control the network load caused by these large restore tasks. When a limit is set, individual users cannot restore more than the limit in any one restore task. When files in excess of the limit are selected to be restored, the following message appears:

```
The selected files exceed the restore data size limit set by your
   administrator. Use multiple tasks to restore the files in smaller
   groups. Contact your administrator for help with a very large
   restore.
```

To restore files that exceed the limit the user must either:

- Restore the files in multiple tasks that do not exceed the limit.
- Have an administrator perform the restore.

NOTICE

By design the restore data size limit does not apply to server-class clients (those clients with a very large backup data set). This is described in "Server-class clients" on page 562.

Setting a restore data size limit

To set a restore data size limit:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```
3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```
4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Uncomment and edit the value of the **limitRestoreSize** key:

   Change:

   ```
   #limitRestoreSize=500
   ```

   To:

   ```
   limitRestoreSize=n
   ```

   where *n* is the data size limit in megabytes.
6. Save and close the file.

Restore queue limit

The Avamar client web UI minimizes network and server load by blocking restore requests for clients that already have a restore task in the queue. Users who attempt to start a new restore while one is pending receive a message and their request is blocked. After the pending task is complete, a new restore task can be initiated.

This behavior can be changed to allow users to start multiple restore tasks. The change applies to all clients of the Avamar server.

Removing the restore queue limit

To remove the restore queue limit:

1. Open a command shell and log in:
   - For a single-node server, log in to the server as root.
   - For a multi-node server, log in to the utility node as root.
2. Switch user to root by typing:

   ```
   su -
   ```

3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
5. Create or edit the value of the **disallowMultipleRestores** key:

   Change:

   ```
   disallowMultipleRestores=true
   ```

   to:

   ```
   disallowMultipleRestores=false
   ```

6. Save and close the file.

Avamar client software installation

The recommended method for installing the Avamar client software on large numbers of Windows or Mac computers is to use a Systems management tool. A Systems management tool can remotely push-install the software on large numbers of computers in a short amount of time.

Also, a Systems management tool can often generate a list of the computers where the software is successfully installed. This list can be used when you use Avamar Client Manager to register and activate computers.

Avamar client for Windows can be installed using several silent install options. These are described in "Windows install options" on page 568.

NOTICE

Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.

Supported systems management tools

Remote installation has been tested and approved using the following Systems management tools:

- Microsoft Systems Management Server 2003 (SMS) on Windows Computers
- SMS with Quest Software's Quest Management Xtensions for SMS on Macintosh computers

In addition, you may be able to use other Systems management tools to remotely push install the Avamar client software, including the following tools:

- Microsoft System Center Configuration Manager 2007
- IBM Tivoli Management Framework
- HP OpenView ServiceCenter
- Symantec Altiris
- Apple Remote Desktop

Systems management tools vary. The steps required to push software to a set of computers depend upon the tool. Consult the documentation for the tool to determine the steps required to perform these tasks.

Push installation on Windows computers

To push install Avamar client software on supported Windows computers:

1. Copy the Avamar client for Windows installer package to a location that is accessible to the Systems management tool.
2. Configure the Systems management tool to copy the correct installer package to each computer.
3. Designate the computers on which to install the software.

4. Provide an installation launch command, using the following format:

   msiexec /qn /I "*path_to_MSI_pkg***"**[**SERVER=***server*] [**DOMAIN=***domain_path*] [**GROUP="***group_paths***"**] [**UICOMPONENT=**{**0**|**1**}] [**PROGRESSBAR=**{**true**|**false**}] [**BALLOONMESSAGE=**{**true**|**false**}] [**BACKUPREMINDER=***days*]

   where *path_to_MSI_pkg* is the full path to the location of the installer package relative to the root of the computer file system and the bracketed arguments are optional, as described in "Windows install options" on page 568.

5. Launch the Systems management tool installation process.

Windows install options

The following table lists optional arguments that can be used with the msiexec installer either during remote push-installation or local command-line installation of Avamar client for Windows. Combinations of arguments can be used. Separate arguments by a space.

Table 129 Arguments to apply Windows install options (page 1 of 2)

Description	Argument
Set the Avamar server assigned to the client.	**SERVER=***server* where *server* is the IP address or FQDN of the Avamar server assigned to the client. When this argument is not provided or is incorrect the client is successfully installed but is not activated.
Set the Avamar domain path assigned to the client.	**DOMAIN=***domain_path* where *domain_path* is the full Avamar domain path assigned to the client. Path must start with a slash path character (Unicode 002F: /). Default value is "/clients".
Set the Avamar group path assigned to the client.	**GROUP=***group_paths* where group_paths is a comma-separated list of Avamar group paths assigned to the client. Each group path must start with a slash path character (Unicode 002F: /) and all paths must be double quoted. For example: **GROUP="/clients/text,/clients/admin"** Default value is "/Default Group".
Enable Avamar client with the standard GUI or as an agent process with no user interface.	**UICOMPONENT=**{**0**|**1**} where 0 enables Avamar client with no user interface and 1 enables Avamar client with the standard GUI. The default value is 1. **Note:** When UICOMPONENT is set to **0** all additional options are ignored.
Set the initial state of client's progress window.	**PROGRESSBAR=**{**true**|**false**} The default value is **true**. When state is **true** the progress window is shown during tasks. When state is **false** the progress window is hidden.

Table 129 Arguments to apply Windows install options (page 2 of 2)

Description	Argument
Set the initial state of balloon messages on the client.	**BALLOONMESSAGE=**{**true**|**false**} The default value is **true**. When state is **true** balloon messages are shown. When state is **false** balloon messages are hidden.
Set the initial time value of the client's backup reminder.	**BACKUPREMINDER=***days* Where *days* is the number of days after the last backup before a backup reminder is shown. The possible values for *days* are: **1**, **2**, **3**, **4**, **5**, **6**, **7**, and **Never**. The default value is **3**.

The values set by the following arguments can be changed by subsequent user modifications or different settings specified during an upgrade:

- UICOMPONENT
- PROGRESSBAR
- BALLOONMESSAGE
- BACKUPREMINDER

Push installing on Macintosh computers

To push install Avamar client software on supported Macintosh computers:

1. Copy the Avamar client for Macintosh installer package to a location that is accessible to the Systems management tool.
2. Configure the Systems management tool to copy the correct installer package to each computer.
3. Designate the computers on which to install the software.
4. Provide the installation launch command:

   /usr/sbin/installer -pkg "*path_to_install_pkg*" -target *install_location*

   where *path_to_install_pkg* is the full path to the location of the installer package relative to the root of the computer file system and *install_location* is the location in which to install the software.

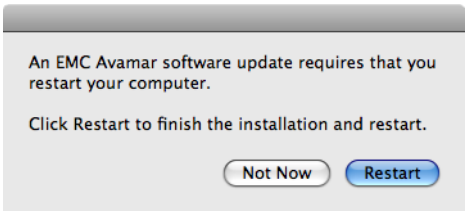
   Normally, *install_location* is the root (/), but any local volume is allowed.
5. Launch the Systems management tool installation process.

Post-install task on some Macintosh computers

After installation of the Avamar client for Macintosh, a restart of some clients may be required.

This is caused by a change to the process data size setting that is made on those computers. During installation, the installer determines if the process data size is less than 96 MB. A minimum process data size of 96 MB is required for optimal performance of the Avamar client for Macintosh. If the process data size is less than 96 MB, then the installer changes it to 96 MB and displays a restart reminder.

If a restart is required, a message appears.



Choose when to restart the computer:

- To restart the computer immediately and complete the process data size change, click **Restart**.
- To hide the reminder for 2 hours and restart at a later time, click **Not Now**.

If you do not click either button within 30 seconds, then the reminder is hidden and appears again in 2 hours. If you click **Restart** but the restart process is interrupted for any reason, then the reminder does not appear again. You must remember to restart the computer to complete the process data size change.

Local installation of the client

The Avamar Desktop/Laptop software can also be installed locally. This method launches a graphical installation interface. At the conclusion of the installation, the computer is ready to register and activate with an Avamar server.

To perform a local installation, you can download the client installer using the downloads link, which is discussed in "Avamar client software installation" on page 567. If the downloads link is disabled, the client installer must be transferred to the computer by some other file transfer method.

The disadvantages of using local installation are:

- It is very time consuming when performed individually on thousands of computers.
- It does not provide a list that can be used to register and activate groups of computers using Avamar Client Manager.

Local installation, upgrading, and uninstalling of Avamar Desktop/Laptop is described in the *EMC Avamar Backup Clients User Guide*.

Remove the Avamar client software

The following topics explain how to remove the Avamar client software.

Removing the software on Windows

To remove the Avamar client software from a Windows computer:

1. Open the Windows **Add or Remove Programs** applet.
2. In the list of currently installed programs, select **EMC Avamar for Windows**.
3. Click **Remove**.

   A confirmation message appears.
4. Click **Yes**.

Removing the software on Macintosh

To remove the Avamar client software from a Macintosh computer:

1. Open a Terminal (shell) session.
2. Log in as an administrator.

   The uninstall command requires root (super-user) permissions. The **sudo** command is used to run the command with root permissions. An administrator account or another account listed in sudoers is required by **sudo**.
3. Run the uninstall script:

   ```
   sudo /usr/local/avamar/bin/avuninstall.sh
   ```

Client log locations

Local logs on client computers provide information about backup and restore operations and UI functionality. The available logs are:

- Workorder

  The workorder log is named *workorder_name*.log, where *workorder_name* is the full name of a particular task. These logs provide detailed information about the specific task.
- Agent

  The agent log is named avagent.log. This log provides information about the status of all backup and restore activity on the computer.
- Console

  The console log is named avscc.log. A console log is created for each user on a computer. It provides information about the performance of the UI.

While these logs are readily accessible through the client UI you can also access them directly.

On Windows computers the logs are available through the paths in the following table.

Table 130 Paths to logs on Windows computers

Log	Path
Workorder	%SystemDrive%\Program Files\avs\var\clientlogs\
Agent	%SystemDrive%\Program Files\avs\var\
Console	%APPDATA%\Avamar\

On Linux computers and Mac computers the logs are available through the paths in the following table.

Table 131 Paths to logs on Linux computers and Mac computers

Log	Path
Workorder	/usr/local/avamar/clientlogs
Agent	/var/avamar/
Console	$HOME/.avamardata/

CHAPTER 21
Data Domain Systems

The following topics provide details on how to integrate Data Domain systems with Avamar:

- Introduction to Avamar and Data Domain system integration 574
- Architecture overview 575
- Backup support 576
- Backup 578
- Restore 578
- VMware Instant Access 579
- Replication 579
- Monitoring and reporting 579
- Security 580
- Data migration 580
- Pre-integration requirements 580
- Preparing the Data Domain system for Avamar integration 583
- Adding Data Domain systems to Avamar 585

Introduction to Avamar and Data Domain system integration

EMC Data Domain deduplication storage systems are typically implemented to back up large high-change rate databases. Avamar is typically implemented to back up file systems, virtual servers, low change rate databases, remote offices, and desktop/laptops. Before Avamar 6.0, managing Data Domain systems and Avamar servers required two separate user interfaces. Beginning with Avamar 6.0, Avamar and Data Domain systems are integrated through a single user interface, Avamar Administrator, as shown in Figure 16.

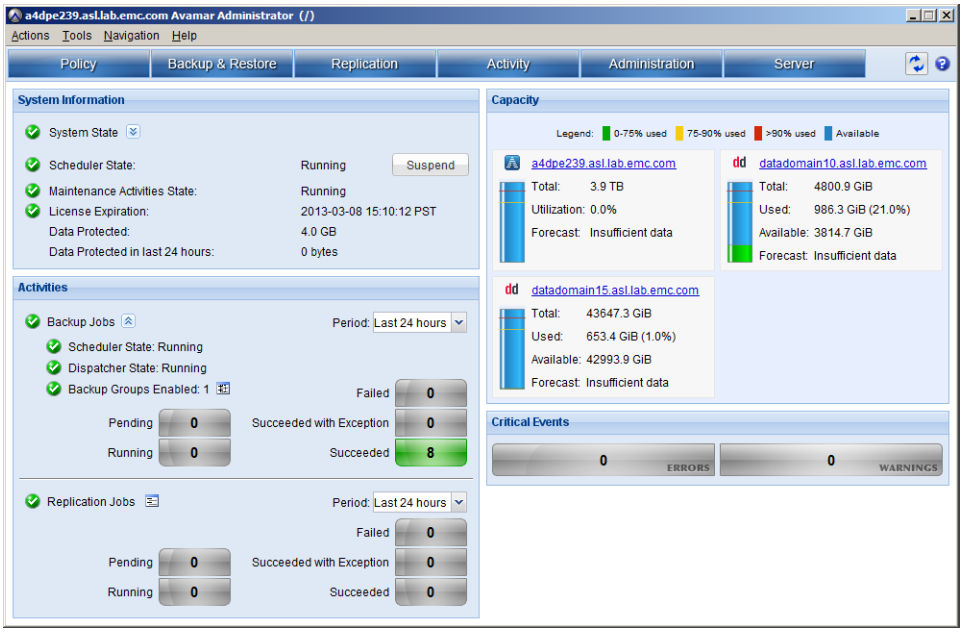


Figure 16 Avamar Administrator user interface

Avamar and Data Domain system integration enables:

- Data Domain systems to be a backup target for Avamar backups
- One or more Data Domain systems to be managed by Avamar
- Avamar clients to use the EMC Data Domain Boost software option to use Data Domain systems as backup targets
- The target destination of backup data, which is set by a backup policy at the dataset level
- Transparent user interaction to the backup target (Avamar or Data Domain)

New features for Data Domain system integration

The following new features have been added for Avamar 7.0 and Data Domain system integration support:

- Support for file system backups. "File system support" on page 577 provides additional information.
- Support for NDMP backups. "NDMP support" on page 578 provides additional information.

- VMware Instant Access allows the backup administrator to boot up a lost or corrupted VMware virtual machine almost instantly from an VMware image backup stored on Data Domain system. "VMware Instant Access" on page 579 provides additional information.
- Checkpoint Backups to Data Domain enable Disaster Recovery for single node Avamar Server by creating periodic checkpoint backups to an attached Data Domain system. This feature is only available on Single Node Avamar servers and requires target Data Domain system with DD OS 5.3 or later. "Avamar checkpoint backup support" on page 578 provides additional information.
- SharePoint backups support backing up Remote Blob Storage (RBS).
- The Avamar Plug-in for Lotus Domino is supported.
- Exchange logs are backed up to a Data Domain system instead of to the Avamar server.

Architecture overview

A Data Domain system performs deduplication through DD OS software. Avamar source-based deduplication to a Data Domain system is facilitated through the use of the Data Domain Boost library.

Avamar uses the DD Boost library through API-based integration to access and manipulate directories, files, and other items contained on the Data Domain File System. The DD Boost API gives Avamar visibility into some of the properties and capabilities of the Data Domain system. This enables Avamar to control backup images stored on Data Domain systems. It also enables Avamar to manage maintenance activities and to control replication to remote Data Domain systems.

DD Boost is installed on the backup clients and on the Avamar utility node or an Avamar single node system.

Figure 17 depicts a high-level architecture of the combined Avamar and Data Domain solution. With Avamar and Data Domain integration you can specify whether specific datasets in an Avamar backup policy target an Avamar server or a Data Domain system.

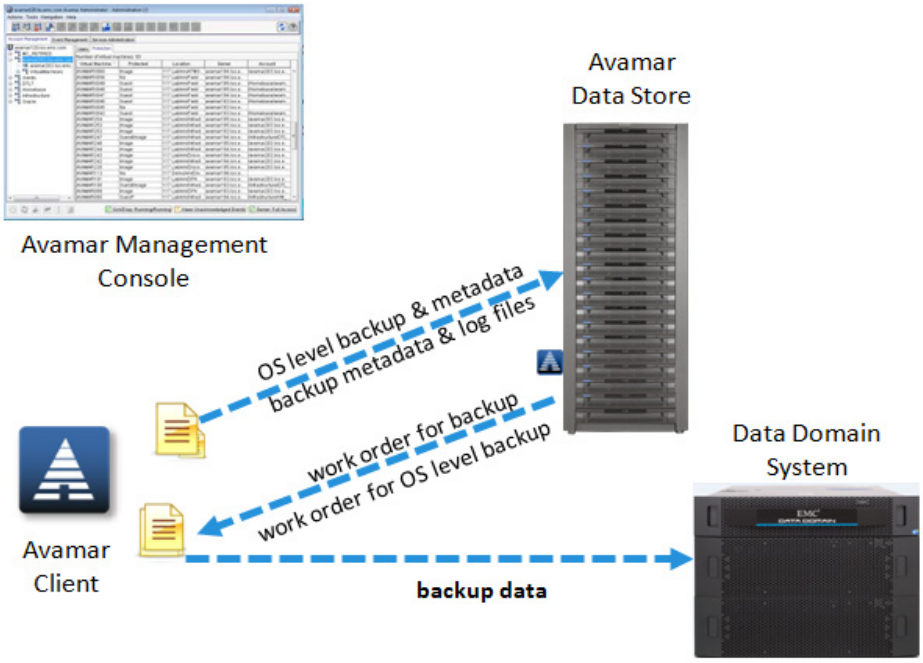


Figure 17 Avamar and Data Domain system workflow

When you select an Avamar server as the backup target, the Avamar client on each host perfroms deduplication segment processing. Data and metadata sent from the client are stored on the Avamar server.

When you select a Data Domain system as the backup target, backup data is transferred to the Data Domain system. The related metadata generated by the Avamar client software is simultaneously sent to the Avamar server for storage. The metadata enables the Avamar management system to perform restore operations directly from the Data Domain system without first going through the Avamar server.

The *EMC Avamar Metadata Capacity Reporting and Monitoring Release 7.0 Technical Note* provides more information about metadata capacity for backups stored on Data Domain systems. This technical note is available from EMC online support (https://support.emc.com).

Backup support

Avamar and Data Domain integration provides the following backup support:

- "File system support" on page 577
- "Avamar client support" on page 577
- "NDMP support" on page 578
- "Avamar checkpoint backup support" on page 578

Note: Up-to-date client compatibility information is available in the EMC Avamar Compatibility and Interoperability Matrix on EMC Online Support at https://support.EMC.com.

File system support

The following operating systems include file system backup and restore support for Avamar and Data Domain integration. Only 64-bit operating systems are supported:

- Avamar Client for Windows
  - Windows Server 2012
  - Windows 8
  - Windows Server 2008 R2 SP1 or later
  - Windows Server 2008 SP2 or later
  - Windows Server 2003 SP2 or later

Note: You cannot back up Windows System State data to a Data Domain system through Avamar integration.

  - Avamar Client for AIX 6.1, 7.1
  - Avamar Client for HP-UX 11.31
    - IA-64, no support for RISC
    - Requires ONCPlus (requires Library revision 11.31.06 or later)
  - Avamar Client for Solaris (Solaris 10 x64 and Solaris 10 on SPARC)

    Note: For Solaris 10 on SPARC, client side deduplication is disabled and deduplication is performed on the Data Domain system.

  - Avamar Client for Linux
    - RHEL 5 and 6
    - SLES 10 and 11

Note: There is no file system support for desktop/laptop backups.

Avamar client support

Avamar and Data Domain system integration supports the following Avamar plug-ins:.

- Avamar Plug-in for DB2
- Avamar Plug-in for Exchange VSS
- Avamar Plug-in for Hyper-V VSS
- Avamar Plug-in for Lotus Domino
- Avamar Plug-in for Oracle
- Avamar Plug-in for SAP with Oracle
- Avamar Plug-in for SharePoint VSS
- Avamar Plug-in for Sybase
- Avamar Plug-in for SQL Server
- Avamar VMware Image Backup/FLR Appliance

NDMP support

Avamar supports Data Domain systems as the backup target for Network Data Management Protocol (NDMP) backup through the Avamar NDMP Accelerator.

The following items are related to NDMP support:

- NDMP support is available for VNX, Celerra, and NetApp
- Incremental backups must be based on a backup from the same storage device

Avamar checkpoint backup support

Avamar checkpoint backup support allows Avamar checkpoints to be stored on a Data Domain system (that uses DD OS 5.3 or later). These checkpoints are then used if disaster recovery is required.

The backup option for Avamar checkpoint support is only available on a single node Avamar server or Avamar Virtual Edition (AVE). You configure this option through the Avamar Administrator. The restore option is only available through EMC Professional Services.

The use cases for this option are:

- Disaster Recovery for a single node Avamar server or AVE
- For configurations that do not have a secondary Avamar server and Data Domain system for replication
- For environments which perform backups mainly to Data Domain systems

Backup

During a backup, the Avamar server sends a backup request to the Avamar client. If the backup request includes the option to use a Data Domain system as the target, backup data is stored on the Data Domain system. Metadata is stored on the Avamar server.

Restore

The process of data recovery is transparent to the backup administrator. The backup administrator uses the same Avamar recovery processes that are native to current Avamar implementations.

VMware Instant Access

VMware Instant Access is used to boot up a lost or corrupted virtual machine almost instantly from an image backup stored on a Data Domain system.

VMware Instant Access works through the following processes:

1. A virtual machine image backup is staged to a temporary location on the Data Domain system.
2. The virtual machine is exported to a temporary location as a secure NFS share.
3. The share is mounted as a NFS datastore on an ESX/ESXi host.

Note: When VMware Instant Access is used, the virtual machine should not be left running on the Data Domain system for extended periods. When the virtual machine runs on the Data Domain system, performance might degrade because of the workflow. To move the VMware Instant Access from the Data Domain system to the VMware production environment, use vMotion.

Note: An alternative to VMware Instant Access is to restore a virtual machine back to the production environment. The Avamar software's ability to leverage Changed Block Tracking (CBT) dramatically speeds the recovery process.

See the *EMC Avamar for VMware User Guide* for additional information on performing VMware Instant Access.

Replication

Replication between primary and replica Data Domain systems is integrated into the Avamar management feature set. This is configured in Avamar Administrator through the Avamar replication policies applied to each dataset. All typical Avamar replication scenarios are supported for datasets that use a Data Domain system as a target, including:

- Many-to-one, one-to-many, cascading replication
- Extension of data retention times
- Root-to-root

Monitoring and reporting

Avamar can collect and display data for health monitoring, system alerts, and capacity reporting on a Data Domain system by using Simple Network Management Protocol (SNMP). This enables you to monitor Data Domain activities, events, capacity, and system status in the same way that you monitor activities, events, capacity, and system status for the Avamar server. You can also run reports to analyze the system.

Security

The following topics provide details on security in an Avamar environment with Data Domain for encryption and user access.

Encryption

The connection between the Avamar client and the Data Domain system is not encrypted. The DD Boost library does not support data encryption between the client and the Data Domain system. Backups from the Avamar client to the Avamar server are always compressed and encrypted.

User access

Use caution when granting users access to the Data Domain system. A user should not be able to directly access the Data Domain system and manually delete data.

Data migration

You cannot migrate backup data directly from the Avamar server to the Data Domain system.

To start using the Data Domain system as the backup target for an Avamar client instead of the Avamar server, edit the dataset to use the Data Domain system, and start performing backups to the Data Domain system. When you change the backup target to the Data Domain system, you must perform a full backup.

After you successfully perform a backup to the Data Domain system, you can delete the earlier backups from the Avamar server.

Pre-integration requirements

Before you integrate a Data Domain system with Avamar, review the following topics:

- "Network throughput" on page 581
- "Network configuration" on page 581
- "NTP configuration" on page 581
- "Licensing" on page 581
- "Port usage and firewall requirements" on page 582
- "Capacity" on page 582
- "Data Domain system streams" on page 582
- "Existing backup products in use with Data Domain" on page 583

Note: This chapter assumes the Avamar server and the Data Domain system(s) are installed and configured.

Network throughput

The Avamar server and all Data Domain systems must be on the same local network. Do not connect the Avamar server and Data Domain systems over a Wide Area Network (WAN). Configurations that use a WAN are not supported.

You can use Avamar replication over a WAN to replicate data from source Avamar servers and Data Domain systems to target Avamar servers and Data Domain systems.

Before integrating a Data Domain system with an Avamar server, ensure that enough network bandwidth is available. To obtain the maximum throughput available on a Data Domain system (for restores, level zero backups, and subsequent incremental backups after a level-zero backup), verify that the network infrastructure provides more bandwidth than the bandwidth required by the maximum throughput of the Data Domain system.

Network configuration

Configure (or verify) the following network configuration:

- Assign a Fully Qualified Domain Name (FQDN) to each Data Domain system.
- Do not use IP addresses in place of hostnames when registering a Data Domain system. This can limit the ability to route optimized duplication traffic exclusively through a registered interface.
- Ensure that DNS on the Data Domain system is properly configured.
- Ensure forward and reverse DNS lookups work between the following systems:
  - Avamar server
  - Data Domain system
  - Backup and restore clients
- Use Hosts files to resolve hostnames to non-routable IP addresses.
- Do not create secondary hostnames to associate with alternate or local IP interfaces.

NTP configuration

Configure the Avamar server and Data Domain system to use the same Network Time Protocol (NTP) Server.

Licensing

Ensure that the environment meets the licensing requirements in Table 132.

Table 132 Licensing requirements

Product	Licensing requirement
Avamar	Standard Avamar licensing requirements apply.
Data Domain	The DD Boost license must be installed on the Data Domain system. For replication from one Data Domain system to another, a replication license must be installed.

Port usage and firewall requirements

To enable communication between Avamar and the Data Domain systems, review and implement the port usage and firewall requirements in the following documents:

- *EMC Avamar Product Security Guide*
- "Port Requirements for Allowing Access to Data Domain System Through a Firewall," available on the Data Domain Support Portal at:

  `https://my.datadomain.com`

Capacity

Carefully assess your backup storage needs when evaluating how much data to store on the Data Domain system and the Avamar server. Include estimates from data that is sent to the Data Domain system from any other servers. Review the capacity management information in the *EMC Avamar Administration Guide*.

When the Data Domain system reaches its maximum storage capacity, no further backups to the Data Domain system occur until additional capacity is added or old backups are deleted.

"Data Domain capacity monitoring" on page 60 provides details on how to monitor capacity.

The *EMC Avamar Metadata Capacity Reporting and Monitoring Release 7.0 Technical Note* provides more information about metadata for backups stored on Data Domain systems.

Data Domain system streams

Each Data Domain system has a soft limit to the maximum number of connection and data streams that can be sustained simultaneously while maintaining performance. The number of streams varies depending on the Data Domain system model. For example, the EMC Data Domain DD990 can support 540 backup streams, while the EMC Data Domain DD620 can support 20 backup streams. You configure the maximum number of streams Avamar can use when you add a Data Domain system to the Avamar server.

The Avamar server uses the backup stream value to limit the number of concurrent backup or restore jobs. If the Data Domain system is fully dedicated to the Avamar server, the stream value entered in Avamar Administrator could potentially be the maximum number of streams supported by the Data Domain system model. In cases where the Data Domain system is shared with other third-party applications or another Avamar server, then a subset of the number of streams should be allocated.

Each Avamar backup client (that supports multi-stream backups) can be configured to use the appropriate number of streams (typically based on the number of databases) through multi-streaming configuration when the Avamar backup job is configured. The streams are released when the backup/restore operation completes. The number of streams allocated should depend on the number and type of Avamar clients that backs up data at about the same time.

Existing backup products in use with Data Domain

Data Domain systems can use other third-party backup and archiving software. The Avamar server does not assume it has sole ownership of the Data Domain system. Ensure that proper sizing is evaluated if the system is shared with other software products. The Avamar server makes no use of the native Data Domain system snapshot and replication features. Replication occurs through the DD Boost SDK library by using copying and cloning. However, other third party products may make use of the native Data Domain system snapshot and replication features. In this case, a snapshot of an entire Data Domain system or a replication of an entire Data Domain system includes the Avamar data.

Preparing the Data Domain system for Avamar integration

To support Avamar and Data Domain integration, ensure the environment meets the Data Domain system requirements listed in Table 133:

Table 133 Data Domain requirements (page 1 of 2)

Data Domain feature or specification	Requirement for use with Avamar
Data Domain Operating System (DD OS)	Avamar integration requires DD OS 5.3.*x*./ DD OS 5.4.*x*
DD Boost	Avamar integration requires DD Boost 2.6.*x* DD Boost software enables backup servers to communicate with storage systems without the need for Data Domain systems to emulate tape. There are two components to DD Boost: one component that runs on the backup server and another that runs on the Data Domain system. In the context of Avamar, the component that runs on the backup server (DD Boost libraries) is integrated into the Avamar Client. DD Boost software is an optional product that requires a license to operate on the Data Domain system.

Table 133 Data Domain requirements (page 2 of 2)

Data Domain feature or specification	Requirement for use with Avamar
Data Domain device type	Avamar supports any Data Domain system that supports the execution of the required DD OS version.
Data Domain File System	Enable Data Domain File System using either the Data Domain System Manager or CLI. After you enable file system operations, it may take as up to 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is using the DD Extended Retention option. Do not perform backups, restores, or system maintenance operations until the status appears correctly in Avamar Administrator. Otherwise, the backups, restores, or system maintenance operations may fail.
DD Boost user account	The DD Boost library uses a unique login account name created on the Data Domain system, this account name is known as the DD Boost account. Only one DD Boost account exists per Data Domain system. If the account is renamed and/or the password is changed, these changes must be immediately updated on the Avamar system by editing the Data Domain configuration options. Failure to update the DD Boost account information could potentially yield integrity check errors and/or backup/restore problems. The DD Boost account must have administrator privileges.

Note: When you enable DD Boost on the Data Domain device, DD Boost becomes the preferred method of connectivity for any clients that are enabled for DD Boost. While this method is acceptable for clients that can take advantage of DD Boost features, it can result in performance degradation for other clients. Proper due diligence and effective data gathering are keys to avoiding such interactions, especially during upgrades.

Before you can add a Data Domain system to the Avamar configuration, prepare the Data Domain system by enabling DD Boost and creating a DD Boost user account for the Avamar server to use to access the Data Domain system for backups and restores (and replication, if applicable).

To prepare the Data Domain system:

1. Disable DD Boost on the Data Domain system by logging into the Data Domain CLI as an administrative user and typing:

   ```
   ddboost disable
   ```

2. Create a DD Boost account and password:

   a. Create the user account with admin privileges by typing:

      ```
      user add USER role admin
      ```

      where USER is the username for the new account.

b. Set the new account as the DD Boost user by typing:

```
ddboost set user-name USER
```

where USER is the username for the account.

3. Enable DD Boost to allow the changes to take effect by typing the following command:

```
ddboost enable
```

IMPORTANT

If you change the DD Boost account name or password, make sure to edit the Data Domain system configuration in Avamar Administrator. Otherwise all backups, restores and maintenance activities fail.

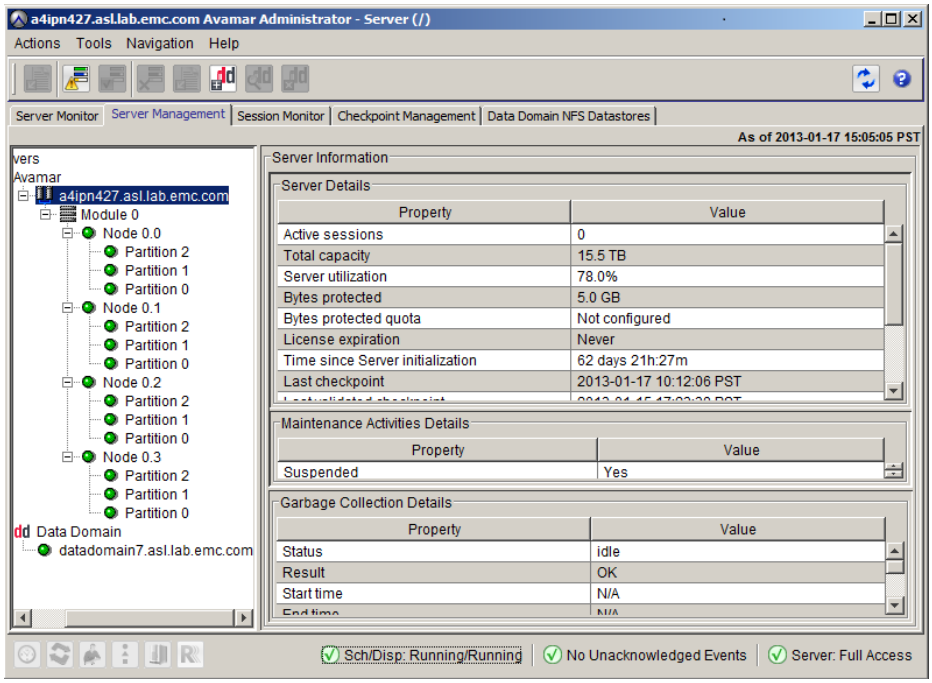
Adding Data Domain systems to Avamar

To add a Data Domain system to the Avamar server configuration:

1. In **Avamar Administrator**, click the **Server** tab.

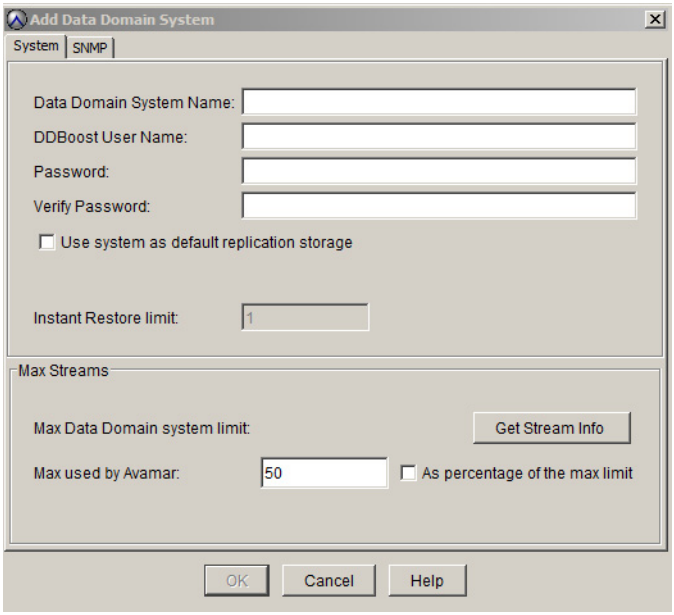
   The **Avamar Server** window appears.

2. Click the **Server Management** tab.



3. Select **Actions** › **Add Data Domain System**.

   The **Add Data Domain System** dialog box appears.



4. On the **System** tab, specify Data Domain system information:

   a. In the **Data Domain System Name** box, type the fully qualified domain name of the Data Domain system to add.

   Note: Do not use an IP address or a secondary hostname that associates with alternative or local IP interfaces. It may limit the ability of Avamar to route optimized deduplication traffic.

   b. In the **DDBoost User Name** box, type the username of the DD Boost account for Avamar to use to access the Data Domain system for backups, restores, and replication.

   c. In the **Password** box, type the password for the account that Avamar should use to access the Data Domain system for backups, restores, and replication.

   d. In the **Verify Password** box, type the password again to verify it.

   e. If you have more than one Data Domain system associated with Avamar, you can specify one Data Domain system to be the default replication storage. Check the **Use system as default replication storage** if this system is the default replication storage.

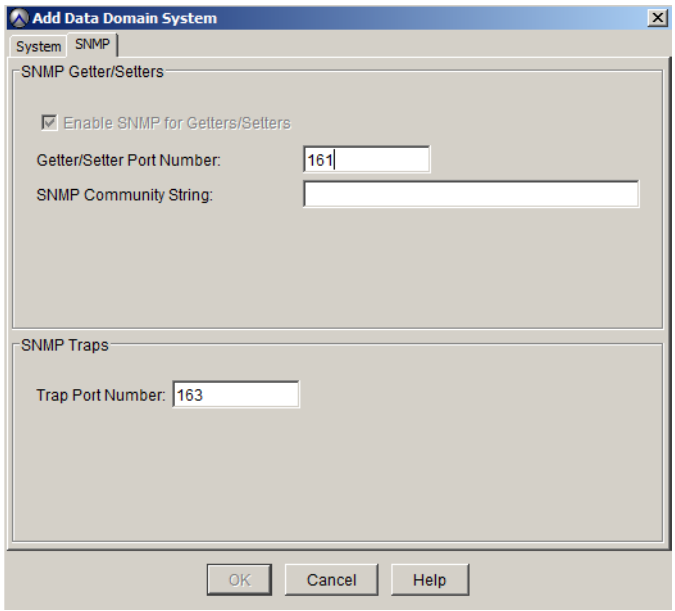
   f. To view the number of supported streams (based on the target Data Domain system, click the **Get Stream Info** button in the bottom right corner of the dialog box.

g. In the **Max used by Avamar** box, type the maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores.

Consider both the maximum number of streams that the Data Domain system supports (listed next to Max Streams Limit), as well as whether other applications are using streams to send data to and receive data from the Data Domain system.

If the processes writing to and reading from the Data Domain system use all available streams, then Avamar queues backup or restore requests until one or more streams become available.

5. To configure SNMP , click the **SNMP** tab.



The SNMP options to configure for Avamar and Data Domain system integration include:

- The **Getter/Setter Port Number** text box lists the port on the Data Domain system from which to receive and on which to set SNMP objects. The default value is 161.
- The **SNMP Community String** text box lists the community string Avamar uses for read-only access to the Data Domain system.
- The **Trap Port Number** text box lists the trap port on the Avamar server. The default value is 163.

SNMP configuration enables Avamar to collect and display data for system health monitoring, system alerts, and capacity reporting.

6. Click **OK**.

The **Add Data Domain System** progress dialog box appears.

7. After the addition is complete, click **Close.**

Note: When you add a Data Domain system to the Avamar configuration, Avamar creates a MTree on the Data Domain system for the Avamar server. The MTree refers to the directory created within the DD Boost path. Data Domain systems support a maximum of 100 MTrees. If you reach the limit, then you cannot add the Data Domain system to the Avamar configuration.

For additional information on backups, replication, monitoring, and troubleshooting Avamar and Data Domain system integration, see the *EMC Avamar and EMC Data Domain System Integration Guide*.

APPENDIX A
Command Shell Server Logins

The following topics describe the command shell server logins:

- User accounts 590
- Starting command shell sessions 590
- Switching user IDs 590
- Using sudo 591

User accounts

The following user accounts are commonly used for system administration and maintenance tasks:

- root
- admin
- dpn

The admin and dpn user accounts require authentication by way of Secure Shell (SSH).

Starting command shell sessions

This example procedure describes how to log in to an Avamar server or utility node as user admin through SSH.

To start a command shell session, open a command shell and log in using one of the following methods:

- To log in to a single-node server, log in to the server as admin.
- To log in to a multi-node server:
  a. Log in to the utility node as admin, and then load the admin OpenSSH key by typing:

     ```
     ssh-agent bash
     ssh-add ~admin/.ssh/admin_key
     ```

  b. When prompted, type the admin_key passphrase and press **Enter**.

Switching user IDs

You can switch to user root by typing **su**, and switch back to the previous login ID by typing **exit**.

To switch to the dpn user account:

1. Switch user to the dpn user account and login shell by typing:

   ```
   su - dpn
   ```

2. When prompted for a password, type the dpn password and press **Enter**.
3. Load the dpn OpenSSH key by typing:

   ```
   ssh-agent bash
   ssh-add ~dpn/.ssh/dpnid
   ```

   NOTICE

   To determine the active user account (login ID) of a shell session, type **whoami**.

Using sudo

On Gen4 and later Avamar Data Stores, the admin and dpn user accounts are automatically added to the sudoers file. This enables admin and dpn users to execute a limited set of commands that would otherwise require operating system root permission.

Prefixing commands with sudo

Instead of switching user to root with the **su** command, admin and dpn users can directly issue commands normally requiring root permissions by prefixing each command with **sudo**. For example, the following command installs MyPackage.rpm:

```
sudo rpm -ivh MyPackage.rpm
```

If prompted for a password, type the password and press **Enter**.

You might be periodically prompted to retype the admin or dpn password when prefixing other commands with **sudo**. This is normal.

Spawning a sudo Bash subshell

If you need to execute several commands that normally require root permissions, you can spawn a persistent sudo Bash subshell by typing **sudo bash**.

Commands that normally require root permissions can now be typed directly with no additional modifications to the command line syntax. For example:

```
sudo bash
rpm -ivh MyPackage1.rpm
rpm -ivh MyPackage2.rpm
rpm -ivh MyPackage3.rpm
exit
```

APPENDIX B
Plug-in Options

The following topics provide information about backup and restore plug-in options:

- How to set plug-in options 594
- Backup options 594
- Restore options 597

How to set plug-in options

Plug-in options enable you to control specific actions for on-demand backups, restores, and scheduled backups. The plug-in options that are available depend on the type of operation and plug-in.

You specify plug-in options for on-demand backup or restore operations, or when you create a dataset for a scheduled backup. You can set options by using the graphical controls and by typing options and values in the Enter Attribute and Enter Attribute Value fields.

NOTICE

No error checking or validation is performed on free text entries. In addition, free text entries override settings made using the graphical controls.

Detailed instructions on how to access and set plug-in options during a backup or restore are available in Chapter 4, "Backup, Restore, and Backup Management."

Backup options

The backup options that appear depend on the type of plug-in. The table in this topic lists the backup options for the following plug-ins:

- AIX file system
- FreeBSD file system
- HP-UX file system
- Linux file system
- Macintosh file system
- NetWare file system
- SCO OpenServer file system

Backup options for the Avamar Plug-in for Microsoft Windows are available in the *EMC Avamar for Windows Server User Guide*. Backup options for application plug-ins, such as SQL Server, SharePoint VSS, and so on, are available in the user guide for the plug-in.

The following options are available when you perform an on-demand backup or when you configure a dataset for scheduled backups for the file system plug-ins listed in this topic.

Table 134 Backup plug-in options (page 1 of 3)

Option	Description
Backup label	Assigns this descriptive label to the backup.
(NetWare only) SMS Authentication	
Server login ID	(NetWare only) Specifies the SMS login username. For example, CN=admin.O=HOSTNAME_CTX.
Server password	(NetWare only) Specifies the password for the SMS login username.
Snapshot stored-on pool	(NetWare only) Specifies the snapshot stored-on pool name.

Table 134 Backup plug-in options (page 2 of 3)

Option	Description
Logging	
List backup contents	Specifies how much information about the backup contents to include in the log files. One of the following: • No file listing • List file names • List files and dates
Informational message level	Specifies how many informational messages to include in the log files. One of the following: • No informationals—Suppresses all informational messages, but includes errors and warnings in the log files. • Some informationals—Includes some informational messages in the log files. • Many informationals—Includes additional status information in the log files. • All informationals—Provides maximum information. Includes all informational messages, errors, and warnings in the log files.
Report advanced statistics	Specifies whether to write advanced timing and deduplication statistics to the log files.
Enable debugging messages	Specifies whether to write maximum information to log files, which creates very large log files.
File System Traversal	
Do not traverse any mounts	Specifies whether to traverse mount points during the backup.
Traverse fixed-disk mounts	Specifies whether to traverse only fixed-disk file system mount during the backup.
Traverse fixed-disk and remote network mounts	Specifies whether to traverse both fixed-disk and NFS network mount points during the backup.
Force traversal of specified file system type(s)	Accepts a comma-separated list of one or more file system types (for example, nfs, ext2, jfs, xfs) that should be traversed during the backup.
Force non-traversal of specified file system type(s)	Accepts a comma-separated list of one or more file system types (for example, nfs, ext2, jfs, xfs) that should not be traversed during this backup.
Pre-Script	
Run user-defined script at beginning of backup	Runs a user-defined script at the beginning of the backup session. The script must be located in /usr/local/avamar/etc/scripts.
Abort backup if script fails	Specifies whether to stop the backup if the script returns a non-zero status code.
Post-Script	
Run user-defined script at end of backup	Runs a user-defined script at the end of the backup session. The script must be located in /usr/local/avamar/etc/scripts.
Exit process with script failure exitcode	Specifies whether **avtar** should exit with the exit code of the script instead of a standard **avtar** exit code.

Table 134 Backup plug-in options (page 3 of 3)

Option	Description
Client Cache Options	
Check client-side caches and report inconsistencies	If selected, a backup does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server.
Check and repair client-side caches	If selected, a backup does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server, and repairs inconsistencies.
Maximum client file cache size (MBs)	Specifies the maximum client file cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of physical RAM should be allocated to the client file cache.
Maximum client hash cache size (MBs)	Specifies the maximum client hash cache size in MB. A negative value indicates a fraction of RAM. For example, -8 specifies that no more than 1/8th of physical RAM should be allocated to the client hash cache.
Advanced Options	
Client-side flag file	Specifies the path to a flag file on the client that contains additional option settings.
Network usage throttle (Mbps)	Specifies a setting that reduces network usage to a specified rate, expressed as megabits/second. For example, 0 = unrestricted, 50% of a T1 = 0.72.
Directly connect to all server nodes	Specifies whether to establish multiple connections to the server. This can improve backup performance under certain circumstances.

Restore options

The restore options that are available depend on the type of plug-in. The table in this topic lists the restore options for the following plug-ins:

- AIX file system
- FreeBSD file system
- HP-UX file system
- Linux file system
- Macintosh file system
- NetWare file system
- SCO OpenServer file system

Restore options for the Avamar Plug-in for Microsoft Windows are available in the *EMC Avamar for Windows Server User Guide*. Restore options for application plug-ins, such as SQL Server, SharePoint VSS, and so on, are available in the user guide for the plug-in.

The following options are available when you perform a restore using the file system plug-ins listed in this topic.

Table 135 Restore plug-in options (page 1 of 2)

Option	Description
Overwrite existing files	Controls behavior when the file to be restored already exists. One of the following: • Never • Always • Generate New Name • If Modified • If Newer
(NetWare only) SMS Authentication	
Server login ID	(NetWare only) Specifies the SMS login username. For example, CN=admin.O=HOSTNAME_CTX.
Server password	(NetWare only) Specifies the password for the SMS login username.
Logging	
List backup contents	Specifies how much information about the backup contents to include in the log files. One of the following: • No file listing • List file names • List files and dates
Informational message level	Specifies how many informational messages to include in the log files. One of the following: • No informationals—Suppresses all informational messages, but includes errors and warnings in the log files. • Some informationals—Includes some informational messages in the log files. • Many informationals—Includes additional status information in the log files. • All informationals—Provides maximum information. Includes all informational messages, errors, and warnings in the log files.

Table 135 Restore plug-in options (page 2 of 2)

Option	Description
Report advanced statistics	Specifies whether to write advanced timing and deduplication statistics to the log files.
Enable debugging messages	Specifies whether to write maximum information to log files, which creates very large log files.
Pre-Script	
Run user-defined script at beginning of restore	Runs a user-defined script at the beginning of the restore session. The script must be located in /usr/local/avamar/etc/scripts.
Abort restore if script fails	Specifies whether to stop the restore if the script returns a non-zero status code.
Post-Script	
Run user-defined script at end of restore	Runs a user-defined script at the end of the restore session. The script must be located in /usr/local/avamar/etc/scripts.
Exit process with script failure exitcode	Specifies whether **avtar** should exit with the exit code of the script instead of a standard **avtar** exit code.
Client Cache Options	
Check client-side caches and report inconsistencies	If selected, a restore does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server.
Check and repair client-side caches	If selected, a restore does not occur. Instead, Avamar performs a validation check of the client-side cache with the Avamar server, and repairs inconsistencies.
Rebuild client-side caches from most recent backup	Does not restore data. If selected, Avamar uses the contents of the last backup to re-create the client-side file cache.
Advanced Options	
Do not descend into subdirectories	Specifies whether to restore only the specified top-level directory and not any subdirectories.
Recreate original path beneath target directory	Specifies whether to re-create the original path to files and directories beneath the specified target directory. For example, if you restore /usr/MyDir/MyFile to /tmp and you select this option, then the full path to the restored file is /tmp/usr/MyDir/MyFile.
Directly connect to all server nodes	Specifies whether to establish multiple connections to the server. This can improve restore performance under certain circumstances.

APPENDIX C
MCS and EMS Database Views

When creating reports, review the information in the following topics on each MCS and EMS database view and the columns within each view:

- Data types 600
- MCS database views 600
- EMS database views 642

Data types

Each column in a database view stores one of the data types listed in the following table.

Table 136 Database view data types

Type	Description
bool	Logical Boolean value (true or false).
date	Specific calendar date (year, month, day).
float8	8-byte floating-point number.
int2	Signed 2-byte integer (whole number).
int4	Signed 4-byte integer (whole number).
int8	Signed 8-byte integer (whole number).
numeric	Exact numeric value with selectable precision.
text	Variable-length character string.
time	Specific time of day.
timestamp	Specific calendar date and time of day.
varchar	Variable-length character string.

MCS database views

The following topics describe the columns in each MCS database view.

v_activities

The v_activities view contains a record for each backup, restore, or validation activity that has taken place.

NOTICE

Beginning with version 4.0, use of this database view is deprecated in favor of "v_activities_2" on page 603. Official support for this database view is likely to be discontinued in a future release.

Table 137 MCS database v_activities view (page 1 of 4)

Column	Type	Description
axionsystemid	varchar	Avamar system ID.
bytes_excluded	float8	Number of bytes intentionally excluded. Not relevant for replication activities.
bytes_modified_sent	float8	Not relevant for replication activities.
bytes_modified_not_sent	float8	Not relevant for replication activities.
bytes_new	float8	Number of bytes processed after data deduplication.

Table 137 MCS database v_activities view (page 2 of 4)

Column	Type	Description
bytes_overhead	float8	Number of bytes of overhead. Not relevant for replication activities.
bytes_scanned	float8	Number of bytes processed. Not relevant for replication activities.
bytes_skipped	float8	Number of bytes unintentionally skipped (errors and so forth).
cid	varchar	Client ID.
client_name	varchar	Client name.
client_os	varchar	Client operating system.
client_ver	varchar	Avamar client software version.
completed_date	date	Completed or terminated date.
completed_time	time	Completed or terminated time.
completed_ts	timestamp	Completed or terminated date and time.
createtime	numeric	Avamar server timestamp for when backup was created.
dataset	varchar	Dataset used to perform this backup (applies to group-based backups only).
dataset_override	bool	True if a client dataset was used instead of a group dataset to perform this backup.
display_name	varchar	VMware client display name.
domain	varchar	Client domain.
effective_expiration	varchar	Expiration of the backup as calculated at the time of the backup.
effective_expiration_ts	timestamp	Expiration of the backup as calculated at the time of the backup.
effective_path	varchar	Dataset used in the backup (applies to group-based backups only).
encryption_method	varchar	Encryption method used. Valid values are: • proprietary • ssl
error_code	int4	Numeric activity status completion code.
error_code_summary	varchar	If the activity did not successfully complete, a short summary of the error code.
expiration	text	Current expiration date.
expiration_ts	timestamp	Current expiration timestamp.
group_name	varchar	Group name (applies to group-based backups only).
initiated_by	varchar	Activity initiated by (applies to on-demand backup only).

Table 137 MCS database v_activities view (page 3 of 4)

Column	Type	Description
num_files_skipped	float8	Number of files unintentionally skipped (errors and so forth). Not relevant for replication activities.
num_of_files	float8	Number of files processed. Can be zero for replication activities. Not relevant for replication activities.
plugin_name	varchar	Name of the plug-in used to perform this activity.
plugin_number	int4	Numeric plug-in ID.
recorded_date	date	Date the activity was recorded.
recorded_date_time	timestamp	Date and time the activity was recorded.
recorded_time	time	Time the activity was recorded.
retention_policy	varchar	Retention policy used to perform this backup (applies to group-based backups only).
retention_policy_override	bool	True if a client retention policy was used instead of a group retention policy to perform this backup.
schedule	varchar	Schedule used for scheduled backups.
schedule_recurrence	varchar	Recurrence interval, either daily, weekly, yearly, or monthly.
scheduled_end_date	date	Expected end date of the activity.
scheduled_end_time	time	Expected end time of the activity.
scheduled_end_ts	timestamp	Expected end date and time of the activity.
scheduled_start_date	date	Scheduled start date.
scheduled_start_time	time	Scheduled start time.
scheduled_start_ts	timestamp	Scheduled start date and time.
session_id	varchar	Unique identifier for this activity.
snapup_label	varchar	Backup label. Blank for replication activities.
snapup_number	varchar	Backup number. Blank for replication activities.
started_date	date	Start date of the activity.
started_time	time	Start time of the activity.
started_ts	timestamp	Start date and time of the activity.

Table 137 MCS database v_activities view (page 4 of 4)

Column	Type	Description
status_code	int4	Last known status code of the activity.
status_code_summary	varchar	Short summary of this status code.
type	varchar	Type of activity. Valid values are: • On-Demand Snapup • Scheduled Snapup • Restore • Validate **Note:** Value "Archive Source" deprecated in version 3.7.

v_activities_2

The v_activities_2 view contains a record for each non-replication activity (that is, backup, restore, or validation) that has taken place. Replication activities are stored in "v_repl_activities" on page 633.

Table 138 MCS database v_activities_2 view (page 1 of 4)

Column	Type	Description
axionsystemid	varchar	Avamar system ID.
bytes_excluded	float8	Number of bytes intentionally excluded.
bytes_modified_sent	float8	Number of bytes modified and sent.
bytes_modified_not_sent	float8	Number of bytes modified but not sent.
bytes_new	float8	Number of bytes processed after data deduplication.
bytes_overhead	float8	Number of bytes of overhead.
bytes_scanned	float8	Number of bytes processed.
bytes_skipped	float8	Number of bytes unintentionally skipped (errors and so forth).
cid	varchar	Client ID.
client_name	varchar	Client name.
client_os	varchar	Client operating system.
client_ver	varchar	Avamar client software version. **Note:** If this activity is a VMware image backup or restore, this is the Avamar client software version running on the proxy server.
completed_date	date	Completed or terminated date.
completed_time	time	Completed or terminated time.
completed_ts	timestamp	Completed or terminated date and time.

Table 138 MCS database v_activities_2 view (page 2 of 4)

Column	Type	Description
createtime	numeric	Avamar server timestamp for when the backup was created.
dataset	varchar	Dataset used to perform this backup (applies to group-based backups only).
dataset_override	bool	True if a client dataset was used instead of a group dataset to perform this backup.
ddr_hostname	varchar	If the server column value is DD, then this is the Data Domain system name.
display_name	varchar	VMware client display name.
domain	varchar	Client domain.
effective_expiration	varchar	Expiration of the backup as calculated at the time of the backup.
effective_expiration_ts	timestamp	Expiration of the backup as calculated at the time of the backup.
effective_path	varchar	Dataset used in the backup (applies to group-based backups only).
encryption_method	varchar	Encryption method used for client/server data transfer. Choices are: • proprietary • ssl
encryption_method2	varchar	Encryption method used for client/server data transfer. Choices are: • High—Strongest available encryption setting for that specific client platform. • Medium—Medium strength encryption. • None—No encryption. The exact encryption technology and bit strength used for any given client-server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides information.
encrypt_method2_sa	bool	True if the mcserver.xml encrypt_server_authenticate preference is set to true. Otherwise, false.
error_code	int4	Numeric activity status completion code.
error_code_summary	varchar	If the activity did not successfully complete, a short summary of the error code.
expiration	text	Current expiration date.
expiration_ts	timestamp	Current expiration timestamp.
group_name	varchar	Group name (applies to group-based backups only).
initiated_by	varchar	Activity initiated by (applies to On-Demand Backup only).

Table 138 MCS database v_activities_2 view (page 3 of 4)

Column	Type	Description
num_files_skipped	float8	Number of files unintentionally skipped (errors and so forth).
num_of_files	float8	Number of files processed.
plugin_name	varchar	Name of the plug-in used to perform this activity.
plugin_number	int4	Numeric plug-in ID.
proxy_cid	varchar	VMware proxy client unique ID.
recorded_date	date	Date the activity was recorded.
recorded_date_time	timestamp	Date and time the activity was recorded.
recorded_time	time	Time the activity was recorded.
retention_policy	varchar	Retention policy used to perform the backup (applies to group-based backups only).
retention_policy_override	bool	True if a client retention policy was used instead of a group retention policy to perform this backup.
server	varchar	Specifies the destination Data Domain system for backups, or source Data Domain system for restores. Valid values are: • Avamar—Avamar server • DD—Data Domain system
schedule	varchar	Schedule used for scheduled backups.
schedule_recurrence	varchar	Recurrence interval, either daily, weekly, yearly, or monthly.
scheduled_end_date	date	Expected end date of the activity.
scheduled_end_time	time	Expected end time of the activity.
scheduled_end_ts	timestamp	Expected end date and time of the activity.
scheduled_start_date	date	Scheduled start date.
scheduled_start_time	time	Scheduled start time.
scheduled_start_ts	timestamp	Scheduled start date and time.
session_id	varchar	Unique identifier for this activity.
snapup_label	varchar	Backup label. Blank for replication activities.
snapup_number	varchar	Backup number. Blank for replication activities.
started_date	date	Start date of the activity.
started_time	time	Start time of the activity.
started_ts	timestamp	Start date and time of the activity.
status_code	int4	Last known status code of the activity.

Table 138 MCS database v_activities_2 view (page 4 of 4)

Column	Type	Description
status_code_summary	varchar	Short summary of this status code.
type	varchar	Type of activity. Valid values are: • On-Demand Backup • Scheduled Backup • Restore • Validate **Note:** Value "Archive Source" deprecated in version 3.7.
wid	varchar	Unique workorder identifier for this activity.

v_activity_errors

The v_activity_errors view contains a record that stores the total number of times a specific event code is encountered during a specific activity.

Table 139 MCS database v_activity_errors view

Column	Type	Description
cid	varchar	Client ID.
cnt	int4	Count of the number of times that this event code occurred.
code	int4	Event code.
pid_number	int4	Plug-in number.
session_id	varchar	Session ID.

v_audits

The v_audits view contains a record for each audit log entry.

Table 140 MCS database v_audits view (page 1 of 3)

Column	Type	Description
audit_id	int4	Internally generated unique ID for this audit entry.
date_time	timestamp	Date and time of the event.
domain	varchar	Domain associated with this event.
ecode	int4	Event code.
product	varchar	Values include: • EM • EMS • END_USER • MCCLI • MCGUI • MCS • SNMP_SUB_AGENT • WEB_RESTORE

Table 140 MCS database v_audits view (page 2 of 3)

Column	Type	Description
role	varchar	Values include: • Administrator • Activity Operator • Restore Only Operator
object	varchar	Values include: • ACTIVITY • AGENT • BACKUP • CLIENT • CP • CPV • CRG • CRON • DATASET • DOMAIN • EMS • EVENT • GC • GROUP • HFSCHECK • MCS • PLUGIN • PROFILE • REPL • REPORT • RETENTION • SCHEDULE • SNMP_SUB_AGENT • SNMPD • SYSLOGD • USER

Table 140 MCS database v_audits view (page 3 of 3)

Column	Type	Description
operation	varchar	Values include: • ACK • ACTIVATE • ADD • AUTH • BACKUP • BROWSE • CANCEL • COPY • DELETE • DISABLE • EDIT • ENABLE • EXPORT • LOGON • RESTART • RESUME • RETIRE • RUN • START • STOP • SUSPEND • VALIDATE
user_name	varchar	User ID that initiated this action.

v_client_backups_users

The v_client_backups_users view contains a record of disk capacity data for each disk on each node.

Table 141 MCS database v_client_backups_users view

Column	Type	Description
activitiesid	bigint	Unique activity identifier.
backup_number	varchar	Numerical backup identifier.
cid	varchar	Client ID.
name	varchar	Name of the backup user.
sid	varchar	User Security Identifier (SID).
userid	bigint	Unique backup user identifier.

v_clientperftrack

The v_clientperftrack view contains a record for client performance statistical data, to be included in High Profile Events.

Table 142 MCS database v_clientperftrack view

Column	Type	Description
axionsystemid	varchar	Avamar system ID.
bytes_excluded	float8	Number of bytes intentionally excluded.
bytes_modified_not_sent	float8	Number of bytes modified but not sent.
bytes_modified_sent	float8	Number of bytes modified and sent.
bytes_new	float8	Number of bytes processed after data deduplication.
bytes_overhead	float8	Number of bytes of overhead.
bytes_reduced_comp	float8	Number of bytes reduced by compression.
bytes_scanned	float8	Number of bytes processed.
bytes_skipped	float8	Number of bytes unintentionally skipped (errors and so forth).
cid	varchar	Client ID.
client_os	varchar	Client operating system.
client_ver	varchar	Avamar client software version.
completed_ts	timestamp	Completed or terminated date and time.
effective_path	varchar	Dataset used in the backup (applies to group-based backups only).
failure_event_code	integer	Failure event code.
num_files_skipped	float8	Number of file unintentionally skipped (errors and so forth).
num_mod_files	float8	Number of files modified.
num_of_files	float8	Number of files processed.
operation	varchar	Type of activity reported by this entry.
pid_number	int4	Plug-in number.
scheduled_start_ts	timestamp	Scheduled start date and time.
server	varchar	Specifies the destination Data Domain system for backups, or source Data Domain system for restores. Valid values are: • Avamar—Avamar server • DD—Data Domain system
session_id	varchar	Unique identifier for this activity.
started_ts	timestamp	Start date and time of the activity.
wid	varchar	Unique workorder identifier for this activity.

v_clients

The v_clients view contains a record for each client known to the MCS.

NOTICE

Beginning with version 4.0, use of this database view is deprecated in favor of "v_clients_2" on page 612. All official support for this database view is likely to be discontinued in a future release.

Table 143 MCS database v_clients view (page 1 of 2)

Column	Type	Description
agent_version	varchar	Version of the agent installed.
allow_overtime	bool	True if the client can ignore the scheduling window end time. See also "overtime_option" on page 611.
allow_userinit_snapup_file_sel	varchar	Allow file selection on user initiated backups.
allow_userinit_snapups	varchar	Allow user initiated backups.
backed_up_ts	timestamp	Last backup date and time.
can_page	bool	True if MCS can call out to the client.
checkin_ts	timestamp	Last checkin date and time.
cid	varchar	Client ID.
client_addr	varchar	Client IP address.
client_name	varchar	Client name.
client_type	varchar	Client type. One of the following: • REGULAR • VCENTER • VMACHINE • VPROXY • VREGULAR
contact_email	varchar	Contact email address.
contact_location	varchar	Contact location.
contact_name	varchar	Person to contact regarding issues with this client.
contact_notes	varchar	Contact notes.
contact_phone	varchar	Contact phone number.
created	date	Creation date.
ds_override	bool	True if the client can override the group dataset.
enabled	bool	True if the client can generate activities.
full_domain_name	varchar	Fully qualified client location.
has_snapups	bool	True if the client has backups.

Table 143 MCS database v_clients view (page 2 of 2)

Column	Type	Description
modified	date	Date that client information was last modified.
os_type	varchar	Client OS type.
override_userinit_retpol	varchar	Override standard retention policy on user initiated backups.
overtime_option	varchar	One of the following: • ALWAYS—Scheduled group backups are always allowed to run past the schedule duration setting. • NEXT—Only the next scheduled group backup is allowed to run past the schedule duration setting. • NEXT_SUCCESS—Scheduled group backups are allowed to run past the schedule duration setting until a successful backup is completed. • NEVER—Scheduled group backups are never allowed to run past the schedule duration setting. • This value is automatically set to NEXT_SUCCESS when the client initially registers, and is cleared after one backup successfully completes.
page_addr	varchar	IP address used to contact this client.
page_port	varchar	Data port used to contact this client.
pageadr_locked	bool	True if the address cannot be updated automatically by MCS.
plugin_for_last_backup	varchar	Plug-in used for the last backup.
rc_override	bool	True if the client can override the group retry count setting.
registered	bool	True if the client has checked in to MCS.
registered_ts	timestamp	Registered date and time.
restore_only	bool	True if the client can only do restores.
retry_cnt	int4	Connection retry count.
rp_override	bool	True if the client can override the group retention policy.
timeout	int4	Connection time-out value.
tp_override	bool	True if the client can override the group time-out period setting.

v_clients_2

The v_clients_2 view contains a record for each client known to the MCS.

Table 144 MCS database v_clients_2 view (page 1 of 2)

Column	Type	Description
agent_version	varchar	Version of the agent installed.
allow_overtime	bool	True if the client can ignore the scheduling window end time. See also "overtime_option" on page 613.
allow_userinit_snapup_file_sel	varchar	Allow file selection on user initiated backups.
allow_userinit_snapups	varchar	Allow user initiated backups.
backed_up_ts	timestamp	Last backup date and time.
can_page	bool	True if MCS can call out to the client.
checkin_ts	timestamp	Last checkin date/time.
cid	varchar	Client ID.
client_addr	varchar	Client IP address.
client_name	varchar	Client name.
client_type	varchar	Client type. One of the following: • REGULAR • VCENTER • VMACHINE • VPROXY • VREGULAR
contact_email	varchar	Contact email address.
contact_location	varchar	Contact location.
contact_name	varchar	Person to contact regarding issues with this client.
contact_notes	varchar	Contact notes.
contact_phone	varchar	Contact phone number.
created	date	Creation date.
display_client_name	varchar	Virtual machine displayable node name.
display_full_domain	varchar	Fully qualified domain and client display name.
ds_override	bool	True if the client can override the group dataset.
enabled	bool	True if the client can generate activities.
full_domain_name	varchar	Fully qualified client location.
has_snapups	bool	True if the client has backups.
modified	date	Date that client information was last modified.
os_type	varchar	Client OS type.

Table 144 MCS database v_clients_2 view (page 2 of 2)

Column	Type	Description
override_userinit_retpol	varchar	Override standard retention policy on user initiated backups.
overtime_option	varchar	One of the following: • ALWAYS—Scheduled group backups are always allowed to run past the schedule duration setting. • NEXT—Only the next scheduled group backup is allowed to run past the schedule duration setting. • NEXT_SUCCESS—Scheduled group backups are allowed to run past the schedule duration setting until a successful backup is completed. • NEVER—Scheduled group backups are never allowed to run past the schedule duration setting. This value is automatically set to NEXT_SUCCESS when the client initially registers, and is cleared after one backup successfully completes.
page_addr	varchar	IP address used to contact this client.
page_port	varchar	Data port used to contact this client.
pageadr_locked	bool	True if the address cannot be updated automatically by MCS.
plugin_for_last_backup	varchar	Plug-in used for the last backup.
rc_override	bool	True if the client can override the group retry count setting.
registered	bool	True if the client has checked in to MCS.
registered_ts	timestamp	Registered date and time.
restore_only	bool	True if the client can only do restores.
retry_cnt	int4	Connection retry count.
rp_override	bool	True if the client can override the group retention policy.
timeout	int4	Connection time-out value.
tp_override	bool	True if the client can override the group time-out period setting.

v_compatibility

The v_compatibility view stores MCS database compatibility information.

Table 145 MCS database v_compatibility view

Column	Type	Description
component	varchar	Subsystem component. One of the following: • db_schema_version_init • db_schema_version • db_views_schema_version
version	varchar	Specific version number of the component.

v_datasets

The v_datasets view contains a record for each dataset known to the MCS.

Table 146 MCS database v_datasets view

Column	Type	Description
all_data	bool	True if the dataset saves all data.
domain	varchar	Avamar domain associated with the dataset.
is_link	bool	True if the dataset is a pointer to another dataset.
is_read_only	bool	True if the dataset cannot be modified.
link_name	varchar	Name of the dataset if is_link is true.
name	varchar	Name of the dataset.

v_ddr_node_space

The v_ddr_node_space view tracks Data Domain system utilization and capacity.

Table 147 MCS database v_ddr_node_space view

Column	Type	Description
date	date	Date.
time	time	Time.
date_time	timestamp	Date and time.
ddr_id	varchar	Unique Data Domain system ID.
ddr_hostname	varchar	Data Domain system hostname.
utilization	numeric	/backup: post-comp percentage of space utilized.
capacity_gib	float8	/backup: post-comp size in GiB.

v_dpnsummary

The v_dpnsummary view contains a record for each backup, restore, or validation activity on a client-by-client basis.

Table 148 MCS database v_dpnsummary view

Column	Type	Description
clientver	varchar	Version of agent software running on the client.
host	varchar	Client name.
mod_sent	float8	Bytes modified and sent.
modnotsent	float8	Bytes modified but not sent.
numfiles	float8	Number of files processed.
nummodfiles	float8	Number of files modified.
operation	varchar	Type of activity reported by this entry.
os	varchar	Client operating system.
overhead	float8	Number of bytes of overhead sent and stored on the storage subsystem.
pcntcommon	int4	Percentage of data deduplication.
reduced	float8	Bytes reduced by compression.
root	varchar	Dataset used in the backup (applies to group-based backups only).
seconds	float8	Completed or terminated date and time.
sessionid	varchar	Unique identifier for the client to storage subsystem session for this activity.
starttime	timestamp	Date and time the job was dispatched to the client by Avamar Administrator. **Note:** Start time in the client log might be slightly later due to communication and job setup latency.
startvalue	float8	Scheduled start date and time, expressed as elapsed time (in seconds) since the beginning of the UNIX epoch.
status	varchar	Success or failure result of this activity.
totalbytes	float8	Number of bytes processed.
workorderid	varchar	Unique workorder identifier for this activity.

v_dpn_stats

The v_dpn_stats view contains a record for Avamar server statistics.

Table 149 MCS database v_dpn_stats view

Column	Type	Description
data_protected_mb	float8	Megabytes protected.
date	date	Date.
date_time	timestamp	Date and time.
dpn_name	varchar	Avamar server name.
time	time	Time.

v_ds_commands

The v_ds_commands view contains a record for each optional plug-in command defined for each dataset.

Table 150 MCS database v_ds_commands view

Column	Type	Description
command_name	varchar	Name of the command.
dataset_name	varchar	Name of the dataset.
domain	varchar	Domain.
plugin_name	varchar	Name of the plug-in.
type	varchar	Type of optional plug-in command.
value	varchar	Value associated with the command name.

v_ds_excludes

The v_ds_excludes view contains a record for each exclude definition defined for each dataset.

Table 151 MCS database v_ds_excludes view

Column	Type	Description
dataset_name	varchar	Name of the dataset.
domain	varchar	Domain.
plugin_name	varchar	Name of the plug-in.
value	varchar	Exclude value for the dataset or plug-in.

v_ds_includes

The v_ds_includes view contains a record for each include definition defined for each dataset.

Table 152 MCS database v_ds_includes view

Column	Type	Description
dataset_name	varchar	Name of the dataset.
domain	varchar	Domain.
plugin_name	varchar	Name of the plug-in.
value	varchar	Include value for the dataset or plug-in.

v_ds_targets

The v_ds_targets view contains a record for each source target defined for each dataset.

Table 153 MCS database v_ds_targets view

Column	Type	Description
dataset_name	varchar	Name of the dataset.
domain	varchar	Domain.
plugin_name	varchar	Name of the plug-in.
value	varchar	Target value for the dataset or plug-in.

v_dtlt_dataset_targets

The v_dtlt_dataset_targets view contains a record of client selected targets to add to its group dataset.

Table 154 MCS database v_dtlt_dataset_targets view

Column	Type	Description
cid	varchar	Client ID.
client_name	varchar	Client name.
full_domain_name	varchar	Fully qualified client location.
plugin_number	int4	Numeric plug-in ID.
target	varchar	Target path.

v_dtlt_sched_override

The v_dtlt_sched_overrideview contains a record of each client selected time to override daily group schedules.

Table 155 MCS database v_dtlt_sched_override view

Column	Type	Description
cid	varchar	Client ID.
client_name	varchar	Client name.
full_domain_name	varchar	Fully qualified client location.
gid	varchar	Group ID.
group_name	varchar	Group name.
group_domain	varchar	Group domain.
timezone	varchar	Time zone where the schedule was created or last modified.
hour	integer	Hour.
minutes	integer	Minutes.

v_ev_catalog

The v_ev_catalog view contains a record for each event code in the events catalog.

Table 156 MCS database v_ev_catalog view (page 1 of 3)

Column	Type	Description
category	varchar	Event category.
code	int4	Event code.
name	varchar	Event name.

Table 156 MCS database v_ev_catalog view (page 2 of 3)

Column	Type	Description
object	varchar	Values include: • ACTIVITY • AGENT • BACKUP • CLIENT • CP • CPV • CRG • CRON • DATASET • DOMAIN • EMS • EVENT • GC • GROUP • HFSCHECK • MCS • PLUGIN • PROFILE • REPL • REPORT • RETENTION • SCHEDULE • SNMP_SUB_AGENT • SNMPD • SYSLOGD • USER
operation	varchar	Values include: • ACK • ACTIVATE • ADD • AUTH • BACKUP • BROWSE • CANCEL • COPY • DELETE • DISABLE • EDIT • ENABLE • EXPORT • LOGON • RESTART • RESUME • RETIRE • RUN • START • STOP • SUSPEND • VALIDATE

Table 156 MCS database v_ev_catalog view (page 3 of 3)

Column	Type	Description
severity	varchar	Event severity.
summary	varchar	Single-line event description.
swSource	varchar	Software modules generating the event.
type	varchar	Event type.

v_ev_cus_body

The v_ev_cus_body view contains a record listing the attachments for each custom events profile.

Table 157 MCS database v_ev_cus_body view

Column	Type	Description
attachments	varchar	String of attachment data.
epid	varchar	Unique ID for this events profile.

v_ev_cus_cc_list

The v_ev_cus_cc_list view contains a record listing the email cc recipients for each custom events profile.

Table 158 MCS database v_ev_cus_cc_list view

Column	Type	Description
cc_list	varchar	List of email cc recipients.
epid	varchar	Unique ID for this events profile.

v_ev_cus_codes

The v_ev_cus_codes view contains a record for each event code that should be included in a custom events profile.

Table 159 MCS database v_ev_cus_codes view

Column	Type	Description
code	int4	Event code to monitor.
cur_value	bool	True if the code triggers email and syslog notification.
default_value	bool	Original default setting for the email and syslog notification.
epid	varchar	Unique ID for this events profile.

v_ev_cus_prof

The v_ev_cus_prof view contains a record for each custom events profile.

Table 160 MCS database v_ev_cus_prof view

Column	Type	Description
active	bool	True if the profile is enabled.
connectemc_channel	varchar	ConnectEMC configuration channel used for this profile.
connectemc_notify_enabled	bool	True if ConnectEMC Notification is enabled for this profile.
domain	varchar	Profile domain.
email_notify_enabled	bool	True if email notification should occur.
epid	varchar	Unique ID for this events profile.
include_logs	bool	True if logs are included in the email.
include_nodelist	bool	True if nodelist is included in the email.
inline_email_attachments	bool	True if email attachments are included in the body of the email.
log_dir	varchar	Directory location of log files.
name	varchar	Name of the custom profile.
read_only	bool	True if you cannot edit the profile.
sched_id	varchar	Email schedule.
snmp_notify_enabled	bool	True if snmp notification should be enabled.
subject	varchar	Email subject header string.
syslog_notify_enabled	bool	True if syslog notification should occur.
timestamp	numeric	Date and time of the last email check, expressed as elapsed time in seconds since the beginning of the UNIX epoch.

v_ev_cus_prof_params

The v_ev_cus_prof_params view contains event code-specific parameters for custom event profiles.

Table 161 MCS database v_ev_cus_prof_params view

Column	Type	Description
ecode	int4	Event code.
epid	varchar	Profile ID.
param	varchar	Parameter.
value	varchar	Value.

v_ev_cus_rpt

The v_ev_cus_rpt view contains a record for each report emailed with an event profile.

Table 162 MCS database v_ev_cus_rpt view

Column	Type	Description
enabled	bool	True if the option to email the report was set.
epid	varchar	Profile ID.
output_csv	bool	True if the report was emailed in Comma-Separated Values (CSV) format.
output_txt	bool	True if the report was emailed in plain text format.
output_xml	bool	True if the report was emailed in XML format.
rptid	varchar	Report ID.
since_count	int4	Number of days, weeks, or months since the last email was sent, or 0 if since_option is last_notified.
since_option	varchar	Unit of measure for since_count, as one of the following values: • day • week • month • last_notified

v_ev_cus_snmp_contact

The v_ev_cus_snmp_contact view contains a record for the snmp trap configuration for each profile.

Table 163 MCS database v_ev_cus_snmp_contact view

Column	Type	Description
community	varchar	Name of the snmp community as which to send traps.
epid	varchar	Profile ID.
snmp_host	varchar	Host to which to send snmp traps.
snmp_port	varchar	Data port to send snmp traps to. The default is 162.

v_ev_cus_syslog_contact

The v_ev_cus_syslog_contact view contains a record for each custom event profile that uses syslog as the notification mechanism.

Table 164 MCS database v_ev_cus_syslog_contact view

Column	Type	Description
epid	varchar	Unique ID for this events profile.
facility	int4	Syslog facility. Valid values are: • 1—user • 16—local0 • 17—local1 • 18—local2 • 19—local3 • 20—local4 • 21—local5 • 22—local6 • 23—local7
format	int4	Output format. Valid values are: • 1—XML • 2—Plain text
syslog_host	varchar	Default value is localhost.
syslog_port	int4	Default value is port 514.

v_ev_cus_to_list

The v_ev_cus_to_list view contains a record listing the email recipients for each custom events profile.

Table 165 MCS database v_ev_cus_to_list view

Column	Type	Description
epid	varchar	Unique ID for this events profile.
to_list	varchar	List of email recipients.

v_ev_unack

The v_ev_unack view contains a record for each unacknowledged event logged by the MCS.

Table 166 MCS database v_ev_unack view

Column	Type	Description
audience	varchar	Intended audience of the event.
category	varchar	Event category. Valid values are: • APPLICATION • SECURITY • SYSTEM • USER
code	int4	Event code.
data	varchar	Event data.
date	date	Date of the event.
description	varchar	Long event description.
domain	varchar	Domain associated with the event.
event_id	int4	Internally-generated event ID.
notes	varchar	Event notes text.
remedy	varchar	Event remedy text.
severity	varchar	Event severity. Valid values are: • NODE • NODE_FATAL • OK • PROCESS • PROCESS_FATAL • SYSTEM_FATAL • USER • USER_FATAL
software_source	varchar	Software modules generating the event.
source	varchar	Host generating the event.
summary	varchar	Single-line event description.
time	time	Time of the event.
timestamp	numeric	Date and time of the event, expressed as the elapsed time in seconds since the beginning of the UNIX epoch.
type	varchar	Event type. Valid values are: • INTERNAL • ERROR • WARNING • INFORMATION • DEBUG

v_events

The v_events view contains a record for each event logged by the MCS.

Table 167 MCS database v_events view

Column	Type	Description
audience	varchar	Intended audience of the event.
category	varchar	Event category. Valid values are: • APPLICATION • SECURITY • SYSTEM • USER
code	int4	Event code.
data	varchar	Event data.
date	date	Date of the event.
description	varchar	Long event description.
domain	varchar	Domain associated with the event.
event_id	int4	Internally-generated event ID.
notes	varchar	Event notes text.
remedy	varchar	Event remedy text.
severity	varchar	Event severity. Valid values are: • NODE • NODE_FATAL • OK • PROCESS • PROCESS_FATAL • SYSTEM_FATAL • USER • USER_FATAL
software_source	varchar	Software modules generating the event.
source	varchar	Host generating the event.
summary	varchar	Single-line event description.
time	time	Time of the event.
timestamp	numeric	Date and time of the event, expressed as the elapsed time in seconds since the beginning of the UNIX epoch.
type	varchar	Event type. Valid values are: • INTERNAL • ERROR • WARNING • INFORMATION • DEBUG

v_gcstatus

The v_gcstatus view contains a record for each garbage collection (GC) operation.

Table 168 MCS database v_gcstatus view

Column	Type	Description
bytes_recovered	int8	Number of bytes recovered in this garbage collection operation.
chunks_deleted	int4	Number of chunks deleted in this garbage collection operation.
elapsed_time	int8	Total elapsed time in seconds for this garbage collection operation.
end_time	timestamp	Date and time this garbage collection operation ended.
gcstatusid	int8	Unique ID for this garbage collection operation.
indexstripes_processed	int4	Number of index stripes involved in this garbage collection operation.
indexstripes_total	int4	Number of index stripes.
node_count	int4	Number of nodes involved in this garbage collection operation.
result	varchar	String result code.
start_time	timestamp	Date and time this garbage collection operation started.

v_group_members

The v_group_members view contains a record for each client organized by group assignment. A client can be a member of more than one group.

Table 169 MCS database v_group_members view

Column	Type	Description
cid	varchar	Client ID.
client_name	varchar	Client name.
dataset_name	varchar	Dataset name.
enabled	bool	True if the client is enabled in the group.
full_client_name	varchar	Client domain and hostname.
group_name	varchar	Group name.
restore_only	bool	True if the client has been deleted and is available only for restore.
retention_name	varchar	Retention policy name.
use_client_ds	bool	True if the client dataset should be used.
use_client_retry	bool	True if the client retry should be used.
use_client_rp	bool	True if the client retention policy should be used.
use_client_timeout	bool	True if the client time-out should be used.

v_groups

The v_groups view contains a record for each group known to the MCS.

Table 170 MCS database v_groups view

Column	Type	Description
created	date	Creation date.
dataset_name	varchar	Dataset name.
dataset_domain	varchar	Dataset domain.
domain	varchar	Domain.
enabled	bool	True if the group is active and enabled.
failed_stop	bool	True if group backups should stop on a failed backup.
group_type	varchar	One of the following: • REGULAR • VCENTER
modified	date	Last modified date.
name	varchar	Group name.
priority	int4	Group priority.
read_only	bool	True if the group cannot be modified.
retention_name	varchar	Retention policy name.
retention_domain	varchar	Retention policy domain.
retry_cnt	int4	Retry count.
run_once	bool	True if running only one backup.
schedule_name	varchar	Schedule name.
schedule_domain	varchar	Schedule domain.
skip_next	bool	True if skipping the next scheduled backup.
target_dpn	varchar	Avamar server to be used for this group.
timeout_min	int4	Time-out in minutes.

v_node_space

The v_node_space view contains a record of disk capacity data retrieved or calculated per disk and per node.

Table 171 MCS database v_node_space view (page 1 of 2)

Column	Type	Description
capacity_mb	float8	Disk size.
date	date	Date.
date_time	timestamp	Date and time.

Table 171 MCS database v_node_space view (page 2 of 2)

Column	Type	Description
disk	int2	Disk number.
diskreadonly	int2	Value applied to normalize percent full.
node	varchar	Node number.
stripes_reserved_mb	float8	Bytes reserved for stripe usage.
stripes_used_mb	float8	Amount of reserved stripe bytes used.
time	time	Time.
used_mb	float8	Disk capacity used.
utilization	numeric	Percentage of storage space used.

v_node_util

The v_node_util view contains a record of node statistics retrieved or calculated per node at a particular date and time.

Table 172 MCS database v_node_util view

Column	Type	Description
cpu_sys_percentage	numeric	Percentage of node utilization by operating system.
cpu_user_percentage	numeric	Percentage of node utilization by user.
date	date	Date.
date_time	timestamp	Date and time.
disk_reads_per_sec	int4	Disk reads per second.
disk_writes_per_sec	int4	Disk writes per second.
diskreadonly	int2	Value applied to normalize percent full.
load_avg	numeric	Load average.
net_in_kbytes_per_sec	int4	Network received in KB/s.
net_out_kbytes_per_sec	int4	Network transmitted in KB/s.
net_ping	numeric	Node ping time.
node	varchar	Node ID.
state	varchar	Node state.
time	time	Time.
utilization	numeric	Percentage of storage space used.

v_plugin_can_restore

The v_plugin_can_restore view contains a record of allowable plug-in substitutions for restores. Each record is a one-to-one allowable substitution in which the original backup plug-in (build, version) is matched with an allowable substitute plug-in ID (can_restore_pid).

Table 173 MCS database v_plugin_can_restore view

Column	Type	Description
build	varchar	An exception to the plug-in version value if not ALL.
can_restore_pid	int4	PID of the plug-in which this plug-in can use to perform restores.
pid_number	int4	Numeric plug-in ID.
version	varchar	Plug-in version.

v_plugin_catalog

The v_plugin_catalog view contains a record for each known plug-in.

Table 174 MCS database v_plugin_catalog view

Column	Type	Description
content	varchar	Content description of the plug-in.
description	varchar	Descriptive name of the plug-in.
encryption_mode	varchar	Encryption method used. Valid values are: • proprietary • ssl
explicit_target_supported	bool	True if targets for the plug-in can be entered when creating or editing a dataset for the plug-in.
implicit_target_supported	bool	True if the concept of all systems for the plug-in is supported when creating or editing a dataset.
include_implicit_as_default	bool	True if the implicit target is included by default when creating or editing a dataset.
multiple_restore_targets_supported	bool	True if multiple restore targets can be entered when restoring a backup.
multiple_targets_supported	bool	True if multiple targets can be entered when creating or editing a dataset for the plug-in.
pid	varchar	Name of the plug-in.
pid_number	int4	Unique plug-in identification.
version	varchar	Plug-in version.

v_plugin_depends_upon

The v_plugin_depends_upon view contains a record for each known plug-in dependency. Each record is a one-to-one match of a plug-in ID (build, version) and the plug-in ID on which it is dependent (dependence_on_pid).

Table 175 MCS database v_plugin_depends_upon view

Column	Type	Description
build	varchar	An exception to the plug-in version value if not ALL.
dependence_on_pid	int4	PID of the plug-in that this plug-in depends upon.
pid_number	int4	Numeric plug-in ID.
version	varchar	Plug-in version.

v_plugin_flag_groups

The v_plugin_flag_groups view contains a record for each grouping of plug-in options.

Table 176 MCS database v_plugin_flag_groups view

Column	Type	Description
cgid	varchar	Control group ID.
description	varchar	Description.
group_order	int4	Order of group.
tooltip	varchar	Text shown when the cursor hovers over the plug-in.
type	varchar	One of the following: • logical • radio

v_plugin_flag_pulldown

The v_plugin_flag_pulldown view contains a record for each entry in a plug-in option list.

Table 177 MCS database v_plugin_flag_pulldown view (page 1 of 2)

Column	Type	Description
build	varchar	An exception to the plug-in version value if not ALL.
command	varchar	One of the following: • browse • restore • snapup • validate
description	varchar	Displayable value of the entry.
entry	varchar	Entry in the pulldown menu.
fid	varchar	Flag ID.

Table 177 MCS database v_plugin_flag_pulldown view (page 2 of 2)

Column	Type	Description
flag_order	int4	Order of the flag in the pulldown.
plugin_number	int4	Numeric plug-in ID.
version	varchar	Plug-in version.

v_plugin_flags

The v_plugin_flags view contains a record for each plug-in option available for backups and restores.

Table 178 MCS database v_plugin_flags view

Column	Type	Description
build	varchar	An exception to the plug-in version value if not ALL.
cgid	varchar	Control grouping.
command	varchar	One of the following: • restore • backup
description	varchar	Plug-in option label.
fid	varchar	Flag ID.
flag_order	int4	Order of group.
max	int4	Maximum value of the flag, if applicable.
min	int4	Minimum value of the flag, if applicable.
name	varchar	Plug-in option name.
plugin_number	int4	Numeric plug-in ID.
pidnum	int4	Plug-in number that this flag should be directed to.
tooltip	varchar	Text shown when the cursor hovers over the plug-in option.
type	varchar	One of the following: • boolean (checkbox) • integer (field) • string (field)
value	varchar	Default value of the flag.
version	varchar	Plug-in version.

v_plugin_options

The v_plugin_options view contains a record for each available plug-in option.

Table 179 MCS database v_plugin_options view

Column	Type	Description
build	varchar	An exception to the version if not ALL.
can_modify	bool	For disable options only. True if the option value is preserved on upgrades.
option_name	varchar	Valid values are: • browse_supported • disable_browse • disable_mc_adhoc_snapups • disable_restore disable_validate • disable_scc_adhoc_snapups • disable_scheduled_snapups • restore_supported • snapup_supported • snapup_supports_cl_options • snapup_supports_exclusion • snapup_supports_inclusion • validate_supports
option_value	bool	True or false.
pid_number	int4	Numeric plug-in ID.
version	varchar	Plug-in version.

v_plugin_state

The v_plugin_state view contains a record that stores the state of each plug-in.

Table 180 MCS database v_plugin_state view

Column	Type	Description
build	varchar	An exception to the plug-in version values if not ALL.
obsolete	bool	True if the plug-in is obsolete.
obsolete_comment	varchar	Comment as to why the plug-in became obsolete.
pid_number	int4	Numeric plug-in ID.
user_added	bool	True if the user added the build.
version	varchar	Plug-in version.

v_plugins

The v_plugins view contains a record for each plug-in installed on any client known to the MCS.

Table 181 MCS database v_plugins view

Column	Type	Description
backed_up_ts	timestamp	Last backup date using this plug-in.
build	varchar	Plug-in build.
cid	varchar	Client ID.
client_name	varchar	Name of the client.
full_client_name	varchar	Client domain and hostname.
installed_ts	timestamp	Date this plug-in type was first registered with MCS.
lastupdate_ts	timestamp	Date this current plug-in version was first registered with MCS.
name	varchar	Description of the plug-in.
pid_number	int4	Plug-in number.
plugin_name	varchar	Name of the plug-in.
version	varchar	Plug-in version.

v_repl_activities

The v_repl_activities view contains a record for each replication activity.

Table 182 MCS database v_repl_activities view (page 1 of 3)

Column	Type	Description
bytes_excluded	float8	Number of bytes intentionally excluded.
bytes_modified_sent	float8	Number of bytes modified and sent.
bytes_modified_not_sent	float8	Number of bytes modified but not sent.
bytes_new	float8	Number of bytes processed after data deduplication.
bytes_overhead	float8	Number of bytes of overhead.
bytes_reduced_comp	float8	Number of bytes reduced by compression.
bytes_scanned	float8	Number of bytes processed.
bytes_skipped	float8	Number of bytes unintentionally skipped (errors and so forth).
cid	varchar	Client ID.
client_name	varchar	Client name.
client_os	varchar	Client operating system.
client_ver	varchar	Avamar client software version.
completed_ts	timestamp	Date and time this replication operation ended.

Table 182 MCS database v_repl_activities view (page 2 of 3)

Column	Type	Description
ddr_hostname	varchar	If server column value is DD, then this is the Data Domain system name.
dpn_domain	varchar	Client domain.
encryp_method	text	Encryption method used for client/server data transfer. Choices are: • proprietary • ssl **Note:** This column is deprecated and exists for historical purposes only. Use encryp_method2 instead.
encryp_method2	varchar	Encryption method used for client/server data transfer. Choices are: • High—Strongest available encryption setting for that specific client platform. • Medium—Medium strength encryption. • None—No encryption. The exact encryption technology and bit strength used for any given client-server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides information.
encrypt_method2_sa	bool	True if server authentication was enforced at the time of the backup (that is, mcserver.xml encrypt_server_authenticate preference is set true).
error_code	int4	Numeric activity status completion code.
error_code_summary	varchar	Last known error code summary.
gid	varchar	Group ID.
group	varchar	Group that initiated the replication activity. One of the following: • If the activity was a scheduled replication, this is the replication group. • Admin On-Demand Group is shown for-demand replication activities.
hostname	varchar	Destination server hostname.
initiated_by	varchar	Activity initiated by this user or MCS.
num_files_skipped	float8	Number of file unintentionally skipped (errors and so forth).
num_mod_files	float8	Number of files modified.
num_of_files	float8	Number of files processed. Can be zero for replication activities.
plugin_name	varchar	Plug-in name.
plugin_number	int4	Plug-in number.
recorded_date	date	Date replication occurred.

Table 182 MCS database v_repl_activities view (page 3 of 3)

Column	Type	Description
retention_type	varchar	This replication activity included one or more of the following retention types: • D—Daily backups • W—Weekly backups • M—Monthly backups • Y—Yearly backups • N—Backups not tagged as having a specific retention type
server	varchar	Specifies the destination Data Domain system for backups, or source Data Domain system for restores. Valid values are: • Avamar—Avamar server • DD—Data Domain system
scheduled_end_ts	timestamp	Date and time this replication operation was scheduled to end.
scheduled_start_ts	timestamp	Date and time this replication operation was scheduled to occur.
session_id	varchar	Unique identifier for this activity.
started_ts	timestamp	Date and time this replication operation started.
status_code	int4	Numeric status code.
status_code_summary	varchar	Status code summary.
systemid	varchar	Avamar system ID.
type	varchar	Type of activity. Valid values are: • Replication Destination • Replication Source
wid	varchar	Unique workorder identifier for this activity.

v_repl_backups

The v_repl_backups view contains a record for each replicated backup.

Table 183 MCS database v_repl_backups view (page 1 of 2)

Column	Type	Description
bytes_excluded	float8	Number of bytes intentionally excluded from the original backup.
bytes_modified_not_sent	float8	Number of bytes in the original backup modified but not sent.
bytes_modified_sent	float8	Number of bytes in the original backup modified and sent.
bytes_new	float8	Number of bytes processed after data deduplication.
bytes_overhead	float8	Number of bytes of overhead in the original backup.

Table 183 MCS database v_repl_backups view (page 2 of 2)

Column	Type	Description
bytes_reduced_comp	float8	Number of bytes in the original backup reduced by compression.
bytes_scanned	float8	Number of bytes processed when the backup was taken.
bytes_skipped	float8	Number of bytes unintentionally skipped when the backup was taken.
cid	varchar	Client ID.
current_expiration	varchar	Current expiration date of the backup.
current_retention	varchar	Current backup retention type. One of the following: • D—Daily backup • W—Weekly backup • M—Monthly backup • Y—Yearly backup • N—Backup not tagged as having a specific retention type
date_time	timestamp	Date and time of the original backup.
dst_label_num	varchar	Numeric backup identifier (label) on destination system.
files_skipped	float8	Number of file unintentionally skipped when the backup was taken.
label	varchar	Backup label.
mod_files	float8	Number of files modified when the backup was taken.
num_of_files	float8	Number of files in backup.
original_expiration	varchar	Expiration date of the backup as calculated at the time of the backup.
original_retention	varchar	Original backup retention type. One of the following: • D—Daily backup • W—Weekly backup • M—Monthly backup • Y—Yearly backup • N—Backup not tagged as having a specific retention type
pid	int4	Numeric plug-in ID.
repl_end_ts	timestamp	Replication end date and time.
repl_start_ts	timestamp	Replication start date and time.
size	float8	Backup size in bytes.
src_label_num	varchar	Numeric backup identifier (label) on source system.
systemid	varchar	Avamar source system ID.
wid	varchar	Unique workorder identifier for this backup.

v_report_filter

The v_report_filter view contains a record for each report identifying its filter options.

Table 184 MCS database v_report_filter view

Column	Type	Description
filter_name	varchar	Filter name.
filter_value	varchar	Filter value.
rptid	varchar	Report ID.

v_reports

The v_reports view contains a record for each report.

Table 185 MCS database v_reports view

Column	Type	Description
adhoc_query	bool	True if a query statement is being used instead of filtering options.
domain	varchar	Report domain.
graphs_allowed	varchar	Not currently supported.
name	varchar	Report name.
readonly	bool	True if the report cannot be edited or deleted. Used for reports that are provided with the product.
rptid	varchar	Report ID.
sql	varchar	SQL statement if adhoc_query is true.
view_name	varchar	Database view used by this report.

v_retention_policies

The v_retention_policies view contains a record for each retention policy known to the MCS.

Table 186 MCS database v_retention_policies view (page 1 of 2)

Column	Type	Description
daily	int4	Advanced policy daily retention.
domain	varchar	Domain.
duration	numeric	Duration of retention.
enabled	bool	True if enabled.
expiration_date	numeric	Expiration date.
is_link	bool	True if this is a reference to another retention policy.
link_name	varchar	Name of the retention policy if is_link is true.
monthly	int4	Advanced policy monthly retention.

Table 186 MCS database v_retention_policies view (page 2 of 2)

Column	Type	Description
name	varchar	Name of the retention policy.
override	bool	True if the advanced policy is used for scheduled backups.
policy_no	int4	Policy number. Valid policy numbers are: • 0—Undefined • 1—Compute expiration date • 2—Static expiration date • 3—No expiration date
read_only	bool	True if the retention policy cannot be modified.
unit	int4	Duration unit. Valid duration units are: • 0—No expiration • 1—Days • 2—Weeks • 3—Months • 4—Years
weekly	int4	Advanced policy weekly retention.
yearly	int4	Advanced policy yearly retention.

v_sch_recurrence

The v_sch_recurrence view contains a record for each recurring schedule known to the MCS.

Table 187 MCS database v_sch_recurrence view (page 1 of 2)

Column	Type	Description
domain	varchar	Schedule domain.
modifier	text	Qualifies entries in the value column: • day—Indicates that this is a monthly schedule that runs on every numerical calendar day specified by the value column entry. • hour—Indicates that this is a daily schedule that runs on every hour of the day specified by the value column entry. • every—Indicates that this is a weekly schedule that runs on every day of the week specified by the value column entry. • first—Indicates that this is a monthly schedule that runs during the first week of the month on the day of the week specified by the value column entry. • second—Indicates that this is a monthly schedule that runs during the second week of the month on the day of the week specified by the value column entry. • third—Indicates that this is a monthly schedule that runs during the third week of the month on the day of the week specified by the value column entry. • fourth—Indicates that this is a monthly schedule that runs during the fourth week of the month on the day of the week specified by the value column entry. • last—Indicates that this is a monthly schedule that runs during the last week of the month on the day of the week specified by the value column entry.

Table 187 MCS database v_sch_recurrence view (page 2 of 2)

Column	Type	Description
name	varchar	Name of the schedule.
recur_interval	text	Recurrence interval. Valid recurrence intervals are: • DAILY • HOURLY • WEEKLY • MONTHLY • YEARLY
value	text	Recurrence value: • For DAILY schedules, this value is the hour of the day. • For WEEKLY schedules, this value is the day of week, such as Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, and Friday. • For MONTHLY schedules that repeat on a specific day of the month, this numerical value is the day of the month. • For MONTHLY schedules that repeat on a specific day of a specific week, this value is the day of week, such as Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, and Friday.

v_schedules

The v_schedules view contains a record for each schedule known to the MCS.

NOTICE

Beginning with version 4.0, use of this database view is deprecated in favor of "v_schedules_2" on page 640. Official support for this database view is likely to be discontinued in a future release.

Table 188 MCS database v_schedules view (page 1 of 2)

Column	Type	Description
description	varchar	Schedule description.
domain	varchar	Domain.
enabled	bool	True if the schedule is enabled and active.
end_policy	int4	Type of schedule termination setting. Valid values are: • 2—Never end • 3—Run N number of times • 4—End on a specific date
end_recur	numeric	End recurrence. This is a specific date or a count of the number of times the schedule should run or 0 if the schedule never ends. This value is related to the value of end_policy.
first_start	timestamp	First start.
is_link	bool	True if this is a reference to another schedule.
last_check	timestamp	Last check.
last_start	timestamp	Last started.
link_name	varchar	Schedule name if is_link is true.

Table 188 MCS database v_schedules view (page 2 of 2)

Column	Type	Description
min_interval	timestamp	Minimum interval.
name	varchar	Name of the schedule.
overtime	bool	True if the schedule end time can be overridden.
read_only	bool	True if the schedule cannot be modified.
recur_counter	numeric	Recurrence counter.
recur_interval	varchar	Recurrence interval. Valid recurrence intervals are: • DAILY • HOURLY • WEEKLY • MONTHLY • YEARLY
start_duration	timestamp	Duration of the start scheduling window.
start_time	timestamp	Start time for the scheduling window.
time_zone_id	varchar	Time zone where the schedule was created or last modified.
total_duration	timestamp	Total duration of the scheduling window.
type_enum	varchar	Type of schedule. The only valid schedule type is CALENDAR.

v_schedules_2

The v_schedules_2 view contains a record for each schedule known to the MCS.

Table 189 MCS database v_schedules_2 view (page 1 of 2)

Column	Type	Description
description	varchar	Schedule description.
domain	varchar	Domain.
enabled	bool	True if the schedule is enabled and active.
end_policy	int4	Type of schedule termination setting. Valid values are: • 2—Never end • 3—Run N number of times • 4—End on a specific date
end_recur	numeric	End recurrence. This is a specific date or a count of the number of times the schedule should run or 0 if the schedule never ends. This value is related to the value of end_policy.
first_start	timestamp	First start.
is_link	bool	True if this is a reference to another schedule.
last_check	timestamp	Last check.
last_start	timestamp	Last started.
link_name	varchar	Schedule name if is_link is true.
min_interval	timestamp	Minimum interval.

Table 189 MCS database v_schedules_2 view (page 2 of 2)

Column	Type	Description
name	varchar	Name of the schedule.
overtime	bool	True if the schedule end time can be overridden.
read_only	bool	True if the schedule cannot be modified.
recur_counter	numeric	Recurrence counter.
recur_interval	varchar	Recurrence interval. Valid recurrence intervals are: • DAILY • WEEKLY • MONTHLY • ADHOC
start_duration	timestamp	Duration of the start scheduling window.
start_time	timestamp	Start time for the scheduling window.
time_zone_id	varchar	Time zone where the schedule was created or last modified.
total_duration	timestamp	Total duration of the scheduling window.
type_enum	varchar	Type of schedule. The only valid schedule type is CALENDAR.

v_serial_numbers

The v_serial_numbers view stores a list of all Avamar server node serial numbers.

Table 190 MCS database v_serial_numbers view

Column	Type	Description
nodeid	varchar	Avamar logical node designation. For example, 0.0, 0.1, 0.s, and so forth.
serial_number	varchar	Avamar server node serial number.
serial_numbers_id	bigint	Unique Avamar server node ID.

v_systems

The v_systems view contains a record for each Avamar system.

Table 191 MCS database v_systems view (page 1 of 2)

Column	Type	Description
gsansystemid	varchar	Avamar server ID.
gsansystemname	varchar	User assigned name.
hfsaddr	varchar	IP address of the server.
hfsport	int4	Port address of the server.
lastupdate	timestamp	Last updated timestamp.

Table 191 MCS database v_systems view (page 2 of 2)

Column	Type	Description
local_hfsaddr	varchar	Local IP address of the server.
mcsport	int4	Port address of MCS for the server from axion_systems.
systemid	int8	Numeric system ID (automatically assigned by MCS).

EMS database views

The following topics describe each column in each EMS database view.

v_avamar_server

The v_avamar_server view contains a record for each Avamar server monitored by Avamar Enterprise Manager.

Table 192 EMS database v_avamar_server view

Column	Type	Description
adaurl	varchar	Universal Resource Locator (URL) for an optional Avamar Data Archive (ADA).
avamar_server_id	bigint	Unique Avamar server ID.
hfsport	integer	Avamar Hash File System (HFS) port number.
hostname	varchar	Avamar server hostname.
ip	varchar	Avamar server IP address.
lastcontact	timestamp	Time in UTC time that the Avamar system was last successfully polled.
local	boolean	True if this Avamar server is running on the same system as the Avamar Enterprise Manager server.
mcport	integer	Management Console Server (MCS) Remote Method Invocation (RMI) port number.
monitoring	boolean	True if monitoring this Avamar server.
note	varchar	Note about the Avamar server entered by administrator.
rollbacktime	bigint	UNIX time of the last rollback.
status	varchar	Current polling status.
statusdetails	varchar	Detailed polling status.
systemid	varchar	Avamar system ID.
systemname	varchar	Avamar system name.
version	varchar	Avamar server version.

v_compatibility

The v_compatibility view stores Avamar Enterprise Manager server database compatibility information.

Table 193 EMS database v_compatibility view

Column	Type	Description
component	varchar	
version	varchar	

GLOSSARY

This glossary contains terms related to Avamar systems. Many of these terms are used in this manual.

A

activation See *client activation* (page 646).

authentication system A username and password system that is used to grant user access to the Avamar server. Avamar supports its own internal authentication system (avs), as well as several external authentication systems (OpenLDAP, Windows Active Directory, NIS, and SMB).

Avamar Administrator Avamar Administrator is a graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or client computer.

Avamar client A computer or workstation that runs Avamar software and accesses the Avamar server over a network connection. Avamar client software comprises a client agent and one or more plug-ins.

Avamar Enterprise Manager Avamar Enterprise Manager is a multi-server management console application that provides centralized Avamar server administration capabilities for larger businesses and enterprises.

Avamar File System (AvFS) A browsable virtual file system view of the normally inaccessible Avamar HFS. The Avamar File System provides read-only accessibility to all backups stored on an Avamar server down to the individual file level. This allows an Avamar server to be used as an online long-term historical strategic enterprise information store in addition to a backup and restore repository.

Avamar Downloader Service A Windows-based file distribution system that delivers software installation packages to target Avamar systems.

Avamar Installation Manager A web interface that manages installation packages. A successful Avamar server software installation or upgrade embeds the Avamar Installation Manager functionality in the Avamar Enterprise Manager as the System Maintenance page.

Avamar server The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

Avamar Web Access A browser-based user interface that provides access to the Avamar server for the express purpose of restoring files to a client.

AvInstaller A backend service that executes and reports package installations.

B

backup A point-in-time copy of client data that can be restored as individual files, selected directories, or as entire file systems. Although more efficient than a conventional incremental backup, a backup is always a full copy of client data that can be restored immediately from an Avamar server.

C

client activation The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

client agent An Avamar client agent is a platform-specific software process that runs on the client and communicates with the MCS (page 169) and with any plug-ins installed on that client.

client registration The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during activation.

ConnectEMC A program that runs on the Avamar server and that sends information to EMC Technical Support. ConnectEMC is typically configured to send alerts for high priority events as they occur, as well as reports once daily.

D

dataset A policy that defines a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

DNS Domain Name Server. A dynamic and distributed directory service for assigning domain names to specific IP addresses.

domain A feature in Avamar Administrator that is used to organize large numbers of clients into named areas of control and management.

E

Email Home An optional feature that uses the High Priority Events profile and Notification schedule to regularly send server error and status messages to EMC Technical Support.

EMC repository A repository that contains server installation packages, client installation packages, and manifest files.

The repository is located on the EMC network. Each EMC customer has a download center that contains files available to them. These files are maintained by the EMC Subscribenet team. Outgoing communication from the Avamar Downloader Service to the EMC repository is encrypted with SSL over an HTTP connection.

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 MCS.

ESRS EMC Secure Remote Support.

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.

group policy The dataset, schedule, and backup retention policy attached to a group that is used by all clients in a group, unless these policy settings are overridden by an administrator at the client level.

H

HFS Hash File System. The content addressed storage area inside the Avamar server used to store client backups.

HFS check An Avamar Hash File System check (HFS check) is an internal operation that validates the integrity of a specific checkpoint. Once a checkpoint has passed an HFS check, it can be considered reliable enough to be used for a server rollback.

J

JRE Java Runtime Environment.

L

LAN Local Area Network.

local repository The /data01/avamar/repo/packages directory on the utility node or single-node server. This directory contains the most current manifest file from the EMC repository. The Avamar Downloader Service pushes packages from the EMC repository to the local repository. If a customer site does not allow Internet access, you can manually copy packages into the local repository.

LOFS Loopback File System.

M

MAC address Media Access Control Address. A unique hardware address, typically embedded at the lowest level in a hardware assembly, that uniquely identifies each device on a network.

Management Console Server (MCS) The MCS provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by the Avamar Administrator graphical management console.

manifest file An XML file listing all the server, client, and workflow packages currently available for download from the EMC repository. The Avamar Downloader Service automatically downloads the manifest file from the EMC repository once a day and determines if new download packages are available.

The Avamar Downloader Service sends the new manifest file to the local repository for each known Avamar system.

module Avamar 1.2.0 and earlier multi-node Avamar servers utilized a dual-module synchronous RAIN architecture in which nodes were equally distributed in two separate equipment cabinets on separate VLANs. The term "module" is a logical construct used to describe and support this architecture (older multi-node Avamar servers comprised a primary module and a secondary module). These legacy systems continue to be supported. However, newer multi-node Avamar servers use a single module architecture, and even though Avamar Administrator provides "module detail" information, a module is therefore logically equivalent to the entire server.

N

NAT Network Address Translation.

NDMP Network Data Management Protocol.

NDMP Accelerator Avamar NDMP Accelerator (accelerator) is a dedicated single-node Avamar client that, when used as part of an Avamar system, provides a complete backup and recovery solution for Network Appliance filers (filers) by way of the Network Data Management Protocol (NDMP).

NFS Network file system.

NIS Network Information Service. An external authentication system that can be used to log in to an Avamar server.

node A networked storage subsystem that consists of both processing power and hard drive storage, and runs Avamar software.

NTP Network Time Protocol. Controls the time synchronization of a client or server computer to another reference time source.

O

ODBC Open DataBase Connectivity. A standard database access method that makes it possible to access any data from any application, regardless of which database management system (DBMS) is handling the data.

OpenLDAP Open Lightweight Directory Access Protocol. An external authentication system that can be used to log in to an Avamar server.

P

packages Avamar software installation files, hotfix patches, and OS patches available from the EMC repository. Packages comprise three types:

- Client—A release of Avamar file system or application backup software.
- Server—A new release of Avamar server software, a service pack, or a patch for the operating system, MC, or GSAN.
- Workflow—A package that runs operations such as adding a node or replacing a node.

Package files use the file extension "avp."

PAM Pluggable Authentication Module. A Linux library that enables a local system administrator to define how individual applications authenticate users.

plug-in An Avamar plug-in is a software process that recognizes a particular kind of data resident on that client.

policy A set of defined rules for client backups that can be named and applied to multiple groups. Groups have dataset, schedule, and retention policies.

R

RAIN Redundant Array of Independent Nodes. A flexible, fault-tolerant architecture that enables an Avamar server to maintain availability and preserve data storage if single nodes fail in an Avamar module.

RDMS Relational Database Management System.

registration See *client registration* (page 646).

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 file systems, directories, files, or data objects from a backup and writes the data to a designated location.

retention The ability to control the length of time that backups are kept in an Avamar server before automated deletion. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

roles A setting in Avamar Administrator that controls which operations each user can perform in the Avamar server. Roles are assigned on a user-by-user basis.

S

schedule The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

system migration A planned operation that uses full "root-to-root" replication to copy all data residing on a source Avamar server to a new destination server. If global client IDs (global CIDs) are used, clients that formerly backed up to the source server can continue to operate transparently without reregistering with the new destination server.

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

storage node A node in the Avamar server that provides storage of data.

T

TFTP Trivial File Transfer Protocol. A version of the TCP/IP FTP protocol that has no directory or password capabilities.

U

utility node In scalable multi-node Avamar servers, a single utility node provides essential internal services for the server. These services include MCS, cronjob, Domain Name Server (DNS), External authentication, Network Time Protocol (NTP), and Web access. Because utility nodes are dedicated to running these essential services, they cannot be used to store backups.

V

VLAN Virtual Local Area Network.