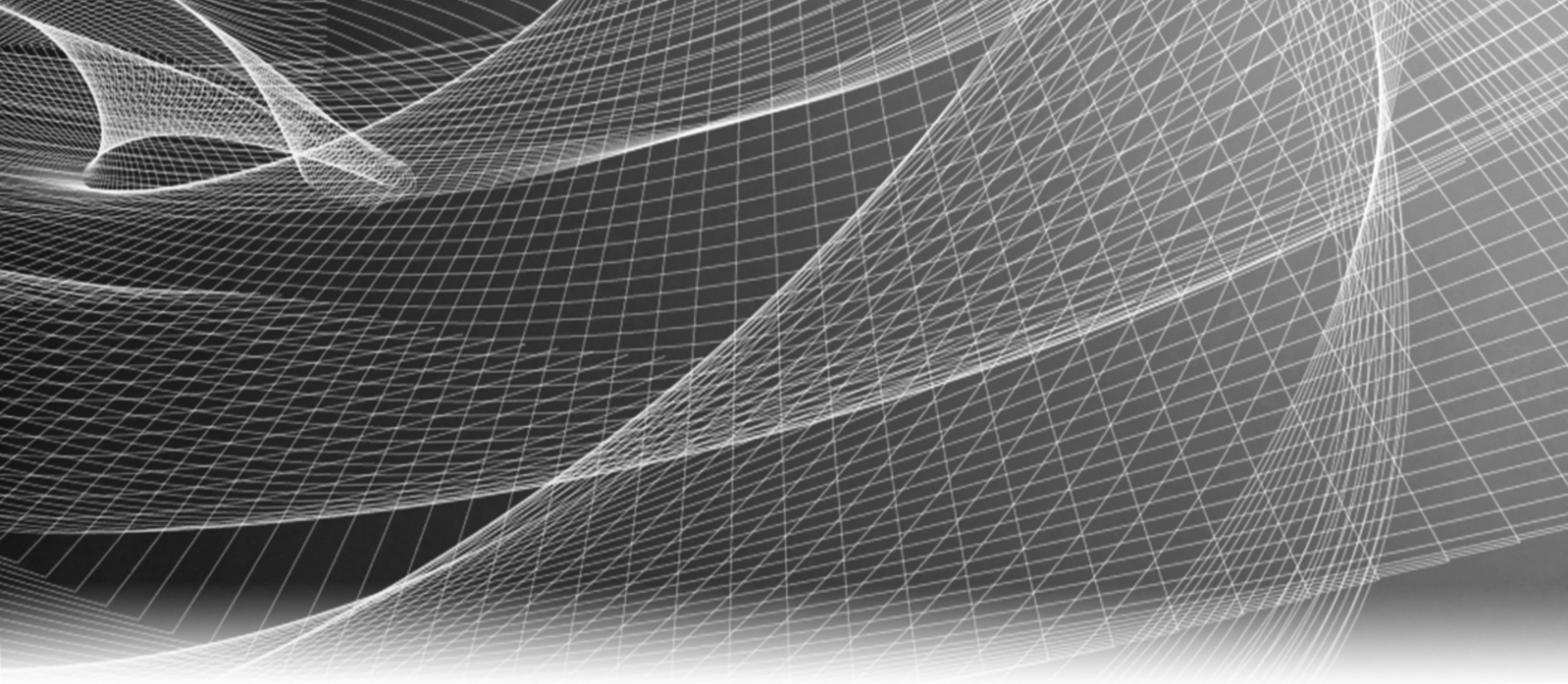


EMC® Avamar® 6.1

Administration Guide

P/N 300-013-345
REV 04

Copyright © 2001 - 2013 EMC Corporation. All rights reserved. Published in the USA.

Published April, 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.

EMC^2, EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

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.......... 28
Important terms and concepts 28
Avamar system.......... 28
Avamar server 29
Node 29
Hard disk storage.......... 29
Stripes 29
Object 29
Data deduplication.......... 30
Replication.......... 30
Functional overview 30
Avamar servers 30
Avamar clients 32
Avamar Administrator 33
Encryption.......... 33

Chapter 2 Avamar Administrator

Installing Avamar Administrator 36
Installing on Microsoft Windows.......... 36
Installing on Linux.......... 37
Upgrading Avamar Administrator.......... 39
Upgrading on Microsoft Windows.......... 39
Upgrading on Linux 39
Uninstalling Avamar Administrator.......... 39
Uninstalling on Microsoft Windows 39
Uninstalling on Linux.......... 39
Starting Avamar Administrator 40
Exploring the Avamar Administrator user interface 43
Status bar 43
Launcher shortcuts 43
Status messages.......... 44
Mouse shortcuts 46

Chapter 3 Domains, Clients, and Users

Domains 48
Understanding Avamar domains and subdomains 48
Creating a domain.......... 49
Editing domain information.......... 50
Deleting a domain.......... 51
Clients 52
Understanding Avamar clients.......... 52
Registering a single client 54
Batch client registration 55
Activating a client.......... 58

Editing client information 59
Viewing client properties 60
Enabling and disabling a client 61
Retiring a client 62
Moving a client to a new domain 63
Deleting a client 63
Editing client paging settings 64
Understanding users, authentication, and roles 67
Users 67
User authentication 68
Roles 69
Enabling user authentication 75
Enabling internal Avamar authentication 75
Enabling directory service authentication 75
Enabling selection of enterprise authentication 79
Managing user accounts 81
Adding a user to a client or domain 81
Editing user information 83
Deleting a user 84

Chapter 4 Backup, Restore, and Backup Management

Performing an on-demand backup 86
Restoring data from a backup 88
Finding a backup to restore 88
Restoring to the original location 93
Restoring to a different location 95
Restoring to multiple locations 99
Managing backups 103
Understanding backup expiration and deletion 103
Finding a backup to manage 103
Changing a backup expiration date 106
Changing backup retention types 107
Validating a backup 109
Viewing backup statistics 110
Deleting a backup 113
Monitoring backup, restore, or validation activities 113
Canceling a backup, restore, or validation 118

Chapter 5 Datasets, Schedules, and Retention Policies

Datasets 120
Understanding datasets 120
Dataset catalog 121
Creating a dataset 124
Editing a dataset 127
Copying a dataset 128
Deleting a dataset 129
Schedules 129
Understanding schedules 130
Schedule catalog 131
Creating a schedule 132
Editing a schedule 138
Copying a schedule 140
Deleting a schedule 140

Running a schedule now 141
Editing the override schedule 141
Retention policies 143
Basic retention settings 143
Advanced retention settings 144
Minimal retention 144
Last backup retention 145
Retention policy catalog 145
Creating a retention policy 146
Editing a retention policy 147
Copying a retention policy 148
Deleting a retention policy 148
Enabling the Minimal Retention policy 149
Disabling the Minimal Retention policy 150

Chapter 6 Groups and Group Policies

Important terms and concepts 152
Group members 152
Group policy 152
Default Group 152
Default Proxy Group 152
Default Virtual Machine Group 152
vCenter groups 153
Inheritance and client overrides 153
Policy window overview 153
Groups tab 154
Clients tab 155
Creating a group 156
Editing group properties 160
Editing a single group 160
Editing multiple groups 161
Copying a group 162
Enabling and disabling a group 162
Deleting a group 163
Viewing the Group Summary Reports 164
Viewing the Group Status Summary 165
Managing group membership 166
Adding and removing clients for a group 166
Adding and removing groups for a client 167
Overriding group policy settings 168
Assigning a different dataset to a client 168
Assigning a different retention policy to a client 169
Changing the client encryption method 170
Allowing scheduled backups to run overtime 171
Allowing users to select an alternative backup start time 173
Allowing users to add to source data 174
Allowing users to initiate backups 175
Allowing users to select data source for on-demand backups 179
Initiating on-demand group backups 181

Chapter 7 Events, Notifications, and Profiles

Important terms and concepts 184
Events 184
Audit logging 184
Customizing error events 185
Notifications 185
Profiles 187
Profile catalog 187
Editing system event profile properties 188
Creating a custom event profile 189
Editing custom event profile properties 197
Copying a custom event profile 198
Testing custom event profile notifications 199
Enabling and disabling a custom event profile 200
Deleting a custom event profile 200
Modifying “Email Home” configuration 200
Modify mcserver.xml Email Home settings 201
Monitoring the Avamar server using syslog 203
Configure a custom event profile 204
Configure local syslogd monitoring 205
Configure remote syslogd monitoring 206
Monitoring the Avamar server using SNMP 207
Prerequisite knowledge 207
SNMP requests 207
SNMP master agent 207
SNMP traps 208
Management Information Base (MIB) 208
Task list 208
Configuring the Net-SNMP agent 209
Configure a custom event profile 211
Managing ConnectEMC 213
EMC Secure Remote Support (ESRS) 213
User-configurable transports 213
Enabling and disabling ConnectEMC 214
Stopping and starting ConnectEMC 215
Editing Primary and Failover transports 216
Editing the Notification transport 219
Testing transports 221

Chapter 8 Reporting

Avamar reports 224
Predefined reports 224
Report templates 226
Creating a report 227
Editing a report 230
Running a report 231
Deleting a report 232
Viewing the Client Summary Report 232
Viewing the Activity Report 236
Viewing the Replication Report 240
Exporting displayed tabular data as CSV files 242
Activity Report 242
Replication Report 243
Client Summary Report 243

Event Management 243
Session Monitor 244
Support for third-party reporting tools 244
PostgreSQL 244
Crystal Reports templates 244
Setting up the PostgreSQL ODBC driver 245
Crystal Reports templates 247
Other third-party support 248

Chapter 9 Avamar Client Agent and Plug-in Management

Important terms and concepts 250
Disabling a version or build 250
Selective management of plug-in operations 250
Obsolete versions and builds 250
Agents Summary view 251
Plug-ins Summary view 252
Adding a build record 254
Editing version or build record settings 255
Deleting a build record 256
Enabling and disabling all client initiated activations 257
Enabling and disabling all client initiated backups 258

Chapter 10 Server Monitoring

Recommended daily server monitoring 260
Monitoring the server 260
Server Monitor tab 261
Server Management tab 264
Replication Storage Mapping tab 273
Session Monitor tab 273
Checkpoint Management tab 274
Domains/Clients tab 274
Verifying system integrity 275
Viewing system events 276
Filtering the Event Monitor display 278
Viewing the Audit Log 281
Filtering the Audit Log display 283
Viewing services information 286
Viewing a detailed client session log 287
Creating a Zip file for EMC Customer Service 289
Collecting and viewing log files 290

Chapter 11 Basic Server Administration

Avamar server functional block diagram 292
Data server 292
Management Console Server (MCS) 292
Enterprise Manager Server (EMS) 293
Avamar server maintenance activities and backup/maintenance windows 293
Maintenance activities 293
Backup/maintenance windows 294
Best practices 295
Acknowledging system events 296
Suspending and resuming backups and restores 297

Suspending and resuming scheduled operations 298
Enabling and disabling scheduled group backups 298
Suspending and resuming maintenance activities.................................. 299
Changing backup/maintenance window settings...................................... 300
Managing services 301
Canceling a client session 302
Resetting a client 303

Chapter 12 Server Shutdown and Restart

Shutting down the server 306
Restarting the server 307
Stopping the MCS 308
Starting the MCS 308
Getting MCS status 309

Chapter 13 Avamar Enterprise Manager

Capabilities and limitations 312
    Multi-system management 312
    Dashboard 312
    Only one Avamar Enterprise Manager server is required 312
    Monitoring multiple versions of Avamar systems................................ 312
    Use local MCS to authenticate Avamar Enterprise Manager logins 312
    Avamar Enterprise Manager compared with Avamar Administrator 312
    Web browser security settings.. 313
    Browser security settings may impact login 313
    Session time-out information 313
Shutting down the EMS... 313
Restarting the EMS... 314
Logging in to Avamar Enterprise Manager.. 314
Dashboard... 315
System.. 319
    Individual system information page 319
    All servers information (detailed dashboard) page 327
Capacity.. 328
Policy.. 328
Reports 329
    Running a report 330
    Exporting a report as a CSV File 330
Replicator 330
Configure 331
Client Manager... 332
System Maintenance... 332
Monitoring other systems.. 332
Suspending and resuming system monitoring....................................... 334
Removing a system from the systems list 335
Monitoring Avamar 4.1.x and 5.x systems 335
    Obtain and install the server hotfix... 335
    Configure MCS web services... 336
    Add the system to Avamar Enterprise Manager.................................. 337
Launching Avamar Administrator from Avamar Enterprise Manager............ 337

Chapter 14 Capacity Management

Limits and thresholds 342
100% — the “server read-only limit” 342
95% — the “health check limit” 342
80% — capacity warning issued 342
Obtaining basic utilization information 343
Avamar Administrator 343
Avamar Enterprise Manager 344
Capacity forecasting 345
Important limitation regarding capacity data after a rollback 346
Detailed utilization and forecasting 346
Customizing capacity limits and behavior 347
Avamar Administrator settings 347
Avamar Enterprise Manager settings 348
Updating Avamar application preference files 348
Server and client average daily change rates 349
Server data 350
Client data 351

Chapter 15 Replication

Overview 354
Efficient data transfers 354
Remote branch disaster recovery 354
Enterprise data center disaster recovery 354
Important terms and concepts 354
Normal replication 354
The REPLICATE domain 355
Full root-to-root replication 355
Source and destination servers 355
Normal replication is a scheduled event 356
Data that is replicated 356
Capabilities and limitations 356
Only static data is replicated 356
Replicating backups by retention type 356
Avamar Administrator manages only one server at a time 356
Time zones 357
Best practices 357
Avoid source and destination server incompatibilities 357
Use a large time-out setting initially 357
Schedule replication during periods of low backup activity 357
Managing replication with Avamar Administrator 358
Viewing replication statistics with Avamar Administrator 361
Managing replication with Avamar Enterprise Manager 362
Replicator setup page 362
Replicator status page 364
Configuring or modifying replication settings 365
Getting replication status 366
Starting and stopping daily replications 367

Chapter 16 Advanced Server Administration and Maintenance

Checkpoints ... 370
Creating a checkpoint ... 370
Validating a checkpoint ... 371
Deleting a checkpoint ... 372
Rolling back to a checkpoint ... 372
MCS configuration settings ... 373
Understanding MCS configuration settings ... 373
Backing up MCS data ... 374
Performing an on-demand MCS flush ... 375
Finding MCS backups in the system ... 375
Restoring MCS data ... 376
Reverting to default MCS preference settings ... 377
Configuring directory service information ... 378
Login requirements ... 378
Providing LDAP information ... 379
Providing NIS information ... 380
Testing an LDAP entry ... 380
Testing an NIS entry ... 381
Error messages for unsuccessful tests ... 381
Text editing of ldap.properties and krb5.conf ... 382
Changing the time-out value ... 384
Setting last backup retention ... 385
Manually changing Avamar Administrator client preferences ... 386
Updating server licensing ... 387
License installation road map ... 388
Generating a license key information file ... 388
Generating a permanent license key file ... 390
Installing and activating the license ... 390
Using the change-passwords utility with default user accounts ... 391
Changing single-node server network settings ... 398
Adding a custom security notification to web login pages ... 399
Manually updating the plug-in catalog ... 399
Configuring Avamar to use network address translation ... 400
Resolving NAT connection and configuration problems ... 402

Chapter 17 Server Updates and Hotfixes

Overview ... 404
Avamar Downloader Service ... 405
Avamar Downloader Service security ... 405
Avamar Downloader Service components ... 405
Avamar Downloader Service installation requirements ... 406
Installing the Avamar Downloader Service ... 406
Downloading the software ... 406
Installing the software ... 407
Defining an inbound rule for Microsoft Windows 7 hosts ... 408
Configuring the Avamar Downloader Service ... 409
Using the Avamar Downloader Service ... 411
Starting the Avamar Downloader Service configuration application ... 411
Monitoring Avamar Downloader Service status ... 411
Checking the EMC repository ... 412
Modifying the username or password ... 413
Removing an Avamar system from the Known Systems list ... 413
Checking the Avamar Downloader Service version ... 414

Troubleshooting Avamar Downloader Service issues 414
Not receiving files from the Avamar FTP site.. 414
Downloading a package fails.. 414
Uninstalling the Avamar Downloader Service... 415
Installing packages from System Maintenance 415
Microsoft Windows browser requirements... 415
EMC Customer Support account 415
Maintenance and SW Updates tabs... 416
Installing workflow packages from the Maintenance tab..................... 417
Installing patch and hotfix packages from the SW Updates tab........... 420
Deleting packages... 421
Viewing installation history information 422

Chapter 18 Client System Recovery

Windows client system recovery.. 428
Red Hat and CentOS Linux system recovery 428
Prerequisites.. 428
Reconstruct partition table 428
Recovery target client preparation 430
Recovery procedure.. 430
Troubleshooting... 435
SUSE Linux system recovery.. 436
Prerequisites.. 436
Reconstruct partition table 436
Recovery target client preparation 438
Recovery procedure.. 438
Troubleshooting... 443
Sun Solaris system recovery.. 444
Prerequisites.. 444
Procedure 445

Chapter 19 Avamar Client Manager

Capabilities 450
Starting Avamar Client Manager 451
General information 451
Connection security 451
Apache web server authentication 452
Editing the session time-out period.. 452
Increasing the JavaScript time-out period 453
Showing and hiding tooltips... 454
Refreshing the window.. 454
Process viewer 454
Activation log and Management log 455
Configuration properties 456
Support for version 4 and 5 servers... 457
Managing clients 459
Moving clients to a new server 460
Moving clients to a new domain 462
Retiring clients.. 463
Deleting clients... 464
Adding and removing groups for a client 465
Adding and removing clients in a group... 466
Working with individual clients 467

Analyzing client activity 471
    Server Summary report 471
    Successful Clients report 473
    Backup/Restore Summary by Client report 475
    Successful Backups report 476
    Failed Clients report 477
    Failed Backups report 478
    Idle Clients report 479
    Clients with Restore Activity report 480
    Restore Activities report 481
    Saving reports 482
Upgrading Avamar clients 483
    Requirements 483
    Obtaining client packages 484
    Upgrading Avamar client software 484
    Requirements for successful package downloads 486
    Downloading a client package to all servers 486
    Downloading a client package to selected servers 487
    Removing a client package 488
    Client Upgrade Status report 488
Activating clients 490
    Loading the list of clients for activation 490
    Searching for computers to activate 493
    Activating selected computers 494
    Activating computers by organizational unit 495
    Retrying activations 497
    Creating a domain 498
    Creating a group 498
    Viewing group information for a domain 498
    Viewing clients for a domain 499
    Searching for clients 499

Chapter 20 Avamar Desktop/Laptop

Features 502
Environment requirements 503
    Computer requirements 503
    Network requirements 504
    LDAP authentication requirements 504
    Avamar authentication requirements 504
    NIS authentication requirements 505
    Avamar system requirements 505
User authentication 506
    Pass-through authentication 507
    LDAP authentication 510
    Avamar authentication 513
    Mixed authentication 515
Apache web server authentication 518
Changing the default web UI port 518
    Client change 518
    Server changes 519
Alternate file browsing method for clients 519
Rebranding the web UI 520
Checking the status of Avamar Desktop/Laptop server 521
Stopping and starting Avamar Desktop/Laptop server 521

User selectable backup start times.. 521
    Requirements.. 521
    Available start time list... 522
    Time zone 522
On-demand backups... 522
    On-demand backup limit.. 523
    Retention policy 524
    Disabling on-demand backups... 525
Source data additions... 525
Selectable backup sets 526
    Enable selectable backup sets for Avamar Desktop/Laptop clients 526
Restore of replicated backups 527
Restore from an alternate computer 527
    Restoring from an alternate computer 528
    Viewing history for an alternate computer 528
    Disabling restore from an alternate computer...................................... 529
Server-class clients.. 529
    Back up now dataset.. 530
    Backup of large number of files... 530
    Backup on battery power.. 530
    Disable restores 531
Restore data size limit.. 532
Restore queue limit... 533
Downloads link 533
Installing the Avamar client software... 534
    Supported systems management tools 534
    Push install on Windows computers.. 535
    Push install on Macintosh computers.. 536
    Local installation of the client 537
Uninstalling the Avamar client software.. 538
    Uninstalling on Windows.. 538
    Uninstalling on Macintosh.. 538
Windows and Mac client log locations.. 539
Macintosh clients with Entourage.. 540
    Creating the dataset.. 540
    Client backup message 541

Chapter 21 Using Avamar with Data Domain

How Avamar and Data Domain work together.. 544
    Architecture of Avamar with Data Domain... 544
    Supported backup types 548
    System requirements 548
Managing Data Domain systems 549
    Preparing the Data Domain system... 549
    Adding a Data Domain system.. 550
    Editing a Data Domain system 552
    Deleting a Data Domain system... 553
Backup to a Data Domain system 554
Restore from a Data Domain system 556
System maintenance with Data Domain 556
    HFS check 557
    Checkpoints... 557
    Rollbacks 557
    Garbage Collection.. 557

Secure deletion 558
Replication with Data Domain 558
How replication works with Avamar and Data Domain 558
Configuring replication 562
Monitoring and reporting with Data Domain 565
Monitoring Data Domain with SNMP 565
Activity monitoring 565
Server monitoring 565
Event monitoring 565
Capacity monitoring 566
Replication monitoring 566
Reports 566
Troubleshooting Data Domain 567
Viewing detailed status information for troubleshooting 567
Data Domain status and resolutions 568
Monitoring status details 572

Chapter 22 Avamar File System (AvFS)

Capabilities and limitations 576
Samba is supported with limitations 576
NFS mounts not supported 576
Windows volume names 576
Data Domain Samba mounts not supported 576
Security recommendations 576
Installing and enabling AvFS 576
Shutting down AvFS 577
Configuring Samba for use with AvFS 578
Installing Samba on utility nodes with SLES 578
Configuring and starting Samba 579
Strengthening Samba security 581
Require a Samba username and password 581
Limit access to listed hosts and networks 581
Limit access to specific interfaces 582
Limit share visibility 582
Example Samba configuration file 583

Appendix A Command Shell Server Logins

User accounts 586
Starting command shell sessions 586
Switching user IDs 586
Using sudo 587
Prefixing commands with sudo 587
Spawning a sudo Bash subshell 587

Appendix B Plug-in Options

How to set plug-in options 590
Backup options 590
Restore options 592

Appendix C MCS and EMS Database Views

Data types 596
MCS database views 596
v_activities........ 596
v_activities_2........ 599
v_activity_errors........ 602
v_audits........ 602
v_client_backups_users........ 604
v_clientperftrack 605
v_clients 606
v_clients_2 608
v_compatibility 610
v_datasets 610
v_ddr_node_space........ 610
v_dpnsummary 611
v_dpn_stats 612
v_ds_commands........ 612
v_ds_excludes 612
v_ds_includes........ 613
v_ds_targets 613
v_dtlt_dataset_targets 613
v_dtlt_sched_override........ 614
v_ev_catalog........ 614
v_ev_cus_body 616
v_ev_cus_cc_list 616
v_ev_cus_codes........ 616
v_ev_cus_prof........ 617
v_ev_cus_prof_params 617
v_ev_cus_rpt........ 618
v_ev_cus_snmp_contact........ 618
v_ev_cus_syslog_contact........ 619
v_ev_cus_to_list 619
v_ev_unack........ 620
v_events 621
v_gcstatus 622
v_group_members 622
v_groups........ 623
v_node_space........ 623
v_node_util........ 624
v_plugin_can_restore........ 625
v_plugin_catalog........ 625
v_plugin_depends_upon........ 626
v_plugin_flag_groups........ 626
v_plugin_flag_pulldown........ 626
v_plugin_flags 627
v_plugin_options 628
v_plugin_state 628
v_plugins........ 629
v_repl_activities........ 629
v_repl_backups........ 631
v_report_filter 633
v_reports........ 633
v_retention_policies........ 633
v_sch_recurrence........ 634
v_schedules........ 635

v_schedules_2 ... 636
v_serial_numbers ... 637
v_systems ... 637
EMS database views ... 638
v_avamar_server ... 638
v_compatibility ... 639

Glossary

TABLES

	Title	Page
1	Revision history	21
2	Status bar icons	43
3	Scheduler and backup dispatching status messages	44
4	Status messages for unacknowledged events	44
5	Operational status messages for Avamar or Data Domain	45
6	Entry element attributes	56
7	Client properties summary	60
8	Methods to browse to a backup by file or folder	91
9	Backup Statistics dialog box tabs	111
10	Backup Statistics dialog box tabs	112
11	Activity Monitor tab columns	114
12	Directories excluded from Default Dataset backups	122
13	Directories excluded from Unix Dataset backups	122
14	Directories excluded from Windows Dataset backups	123
15	Dereference flag and folder wildcard examples	126
16	Schedule types	130
17	Schedule catalog	131
18	Basic retention settings	143
19	Types of retention policies	145
20	Buttons on the Policy window’s Groups tab	154
21	Buttons on the Policy window’s Clients tab	155
22	Group Status Summary information	165
23	Event information	184
24	Test methods for custom event profile notifications	199
25	Syslog field and Avamar Event data mappings	203
26	Syslog Notification screen settings	205
27	Avamar MIB definition file locations	208
28	Edit Primary Transport dialog box settings	217
29	Predefined Avamar reports	224
30	Report templates	226
31	Avamar report template descriptions	229
32	Client Summary report column descriptions	233
33	Activity report column descriptions	236
34	Replication report column descriptions	240
35	Avamar Crystal Reports templates	247
36	Avamar agents property descriptions	251
37	Avamar plug-in property descriptions	253
38	System monitoring tools and tasks	260
39	Server Monitor Avamar tab properties	261
40	Server Monitor Data Domain tab properties	263
41	Bytes Protected Summary properties on the Server Management tab	265
42	Server properties on the Server Management tab	265
43	Module properties on the Server Management tab	267
44	Node properties on the Server Management tab	267
45	Partition properties on the Server Management tab	269
46	Data Domain system properties on the Server Management tab	270
47	Session Monitor tab properties	273
48	Checkpoint Management tab properties	274
49	Event Monitor columns	276
50	Event Monitor filtering criteria	279

51 Audit Log column information 282
52 Audit Log filter criteria 284
53 Services Administration tab properties 286
54 Dashboard page information 316
55 Server status information 320
56 System activity information 327
57 Avamar system column information on the Configure page 331
58 MCS web service configuration settings 336
59 Secure Protocol settings 337
60 Avamar Administrator capacity management preferences 347
61 Avamar Enterprise Manager capacity management preferences 348
62 Replication cron job information 359
63 Avamar Enterprise Manager replication management 362
64 Replicator setup for Avamar systems 363
65 Replicator status for Avamar systems 364
66 Avamar server checkpoint states 370
67 MCS backup timestamp files 375
68 Error message information 381
69 KV pairs in ldap.properties 383
70 Common NAT connection and configuration problems and their solutions 402
71 Avamar Downloader Service components 405
72 Installation requirements for the Avamar Downloader Service 406
73 Avamar Downloader Service monitor status messages 411
74 Item and column descriptions 416
75 Installation Progress page item descriptions 419
76 Installation Progress page item descriptions 421
77 History table column information 423
78 Detail table column descriptions 424
79 Windows client system recovery publications 428
80 Target locations 444
81 Other system directories and virtual file systems 444
82 Process Viewer columns 454
83 Avamar Client Manager properties 456
84 Limitations for moving clients to a new server 458
85 Filters for available Avamar clients 463
86 Steps for selecting a backup retention policy 463
87 Client Details - Summary tab 467
88 Client Details - Backups tab 468
89 Client Details - Plugins tab 468
90 Client Details - Advanced tab 469
91 Avamar Client Manager reports 471
92 Server Summary report columns and linked reports 473
93 Successful Clients report columns 474
94 Backup/Restore Summary by Client report columns 475
95 Successful Backups report columns 476
96 Failed Clients report columns 478
97 Failed Backups report columns 478
98 Idle Clients report columns 479
99 Clients with Restore Activity report columns 481
100 Restore Activities report columns 481
101 Client Upgrade Status report columns 489
102 Client Upgrade Status report status types 489
103 Groups to which clients are added 492
104 Status codes and errors that put activation invitations in the queue 497
105 Entry formats for queued invitations 497

106 Client status descriptions........ 499
107 Minimum requirements for client computers using Avamar Desktop/Laptop 503
108 Network requirements........ 504
109 LDAP authentication requirements 504
110 Avamar authentication requirements 504
111 NIS support requirements 505
112 Avamar system requirements for supporting Avamar Desktop/Laptop........ 505
113 Avamar Desktop/Laptop user authentication methods........ 506
114 Authentication configuration factors that impact pass-through authentication 508
115 Path to avscc.cfg........ 518
116 Path to Apache SSL configuration file........ 519
117 Steps for deleting cached files by browser........ 520
118 Operating systems and associated datasets used by on-demand backups........ 522
119 Possible values for limiting on-demand backups........ 523
120 Requirements for restoring from an alternate computer........ 527
121 Arguments to apply Windows install options........ 535
122 Paths to logs on Windows computers........ 539
123 Paths to logs on Macintosh computers........ 539
124 Client backup message options........ 541
125 Status bar icons for troubleshooting Data Domain........ 567
126 Monitoring Status on the Server Management tab 568
127 Additional information below the Monitoring Status........ 572
128 Backup plug-in options 590
129 Restore plug-in options 593
130 Database view data types 596
131 MCS database v_activities view........ 596
132 MCS database v_activities_2 view........ 599
133 MCS database v_activity_errors view........ 602
134 MCS database v_audits view........ 602
135 MCS database v_client_backups_users view........ 604
136 MCS database v_clientperftrack view........ 605
137 MCS database v_clients view 606
138 MCS database v_clients_2 view 608
139 MCS database v_compatibility view 610
140 MCS database v_datasets view 610
141 MCS database v_ddr_node_space view........ 610
142 MCS database v_dpnsummary view 611
143 MCS database v_dpn_stats view........ 612
144 MCS database v_ds_commands view........ 612
145 MCS database v_ds_excludes view 612
146 MCS database v_ds_includes view........ 613
147 MCS database v_ds_targets view 613
148 MCS database v_dtlt_dataset_targets view 613
149 MCS database v_dtlt_sched_override view........ 614
150 MCS database v_ev_catalog view........ 614
151 MCS database v_ev_cus_body view 616
152 MCS database v_ev_cus_cc_list view........ 616
153 MCS database v_ev_cus_codes view........ 616
154 MCS database v_ev_cus_prof view........ 617
155 MCS database v_ev_cus_prof_params view 617
156 MCS database v_ev_cus_rpt view........ 618
157 MCS database v_ev_cus_snmp_contact view........ 618
158 MCS database v_ev_cus_syslog_contact view........ 619
159 MCS database v_ev_cus_to_list view 619
160 MCS database v_ev_unack view........ 620

161 MCS database v_events view 621
162 MCS database v_gcstatus view 622
163 MCS database v_group_members view 622
164 MCS database v_groups view 623
165 MCS database v_node_space view 623
166 MCS database v_node_util view 624
167 MCS database v_plugin_can_restore view 625
168 MCS database v_plugin_catalog view 625
169 MCS database v_plugin_depends_upon view 626
170 MCS database v_plugin_flag_groups view 626
171 MCS database v_plugin_flag_pulldown view 626
172 MCS database v_plugin_flags view 627
173 MCS database v_plugin_options view 628
174 MCS database v_plugin_state view 628
175 MCS database v_plugins view 629
176 MCS database v_repl_activities view 629
177 MCS database v_repl_backups view 631
178 MCS database v_report_filter view 633
179 MCS database v_reports view 633
180 MCS database v_retention_policies view 633
181 MCS database v_sch_recurrence view 634
182 MCS database v_schedules view 635
183 MCS database v_schedules_2 view 636
184 MCS database v_serial_numbers view 637
185 MCS database v_systems view 637
186 EMS database v_avamar_server view 638
187 EMS database v_compatibility view 639

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 representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on the EMC online support website. Check the EMC online support website 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
04	April 17, 2013	• Removed System Migration chapter. • Added "Data Domain Samba mounts not supported" on page 576.
03	October 25, 2012	Updates for release 6.1 Service Pack 1: • Changed: "Updating server licensing" on page 387. • Changed: "Upgrading Avamar client software" on page 484. • Added: "Requirements for successful package downloads" on page 486. • Changed: "Downloading a client package to all servers" on page 486. • Changed: "Downloading a client package to selected servers" on page 487 • Changed: "Pass-through authentication" on page 507.
02	July 31, 2012	Updated "Where to get help" on page 23 in the Preface.
A01	April 25, 2012	Initial release of Avamar 6.1

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:

⚠DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠CAUTION

CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

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:

Normal

Used in running (nonprocedural) text for:

- Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities
- URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications

Bold

Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages

Used in procedures for:

- Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
- What the user specifically selects, clicks, presses, or types

Italic

Used in all text (including procedures) for:

- Full titles of publications referenced in text
- Emphasis, for example, a new term
- Variables

`Courier`

Used for:

- System output, such as an error message or script
- URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

`Courier bold`

Used for specific user input, such as commands

`Courier italic`

Used in procedures for:

- Variables on the command line
- User input variables

< >

Angle brackets enclose parameter or variable values supplied by the user

[ ]

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 Service.

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.

Live chat

To engage EMC Customer Service 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 Service, 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 Service.

Your comments

Your suggestions will help us 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, A01)
- 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.. 28
- Important terms and concepts 28
- Functional overview 30

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 is backup and recovery software that 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.

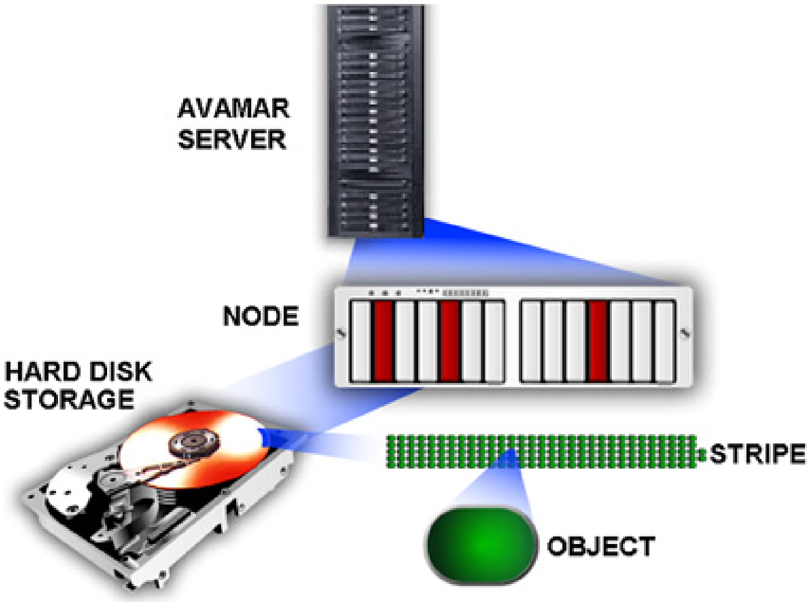
Avamar system

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.

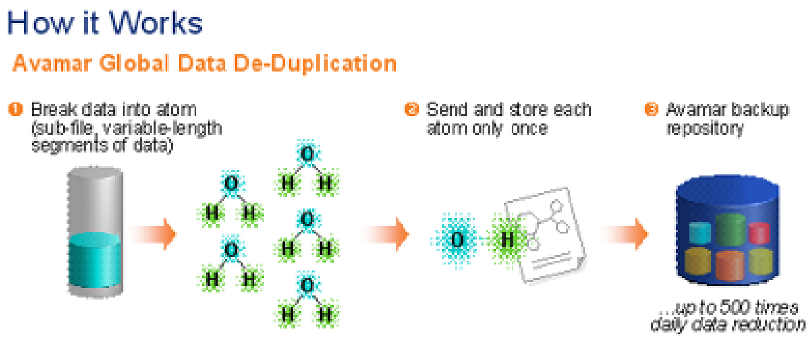
Object

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 filesystem and applies a data deduplication algorithm that identifies redundant data sequences and breaks the client filesystem 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.


How it Works
Avamar Global Data De-Duplication
1 Break data into atom (sub-file, variable-length segments of data)
2 Send and store each atom only once
3 Avamar backup repository
O
H
...up to 500 times daily data reduction

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 EMC Customer Service 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:

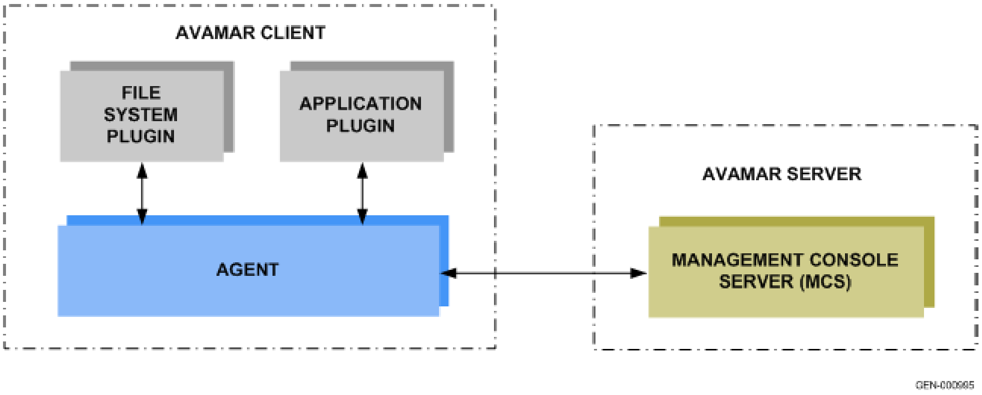
- Utility node — A utility node is dedicated to scheduling and managing background Avamar server jobs. In scalable multi-node Avamar servers, a single utility node provides essential internal services for the server (Management Console Server [MCS], cronjob, External authentication, Network Time Protocol [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.

Filesystem plug-ins

Filesystem plug-ins are used to browse, back up, and restore files or directories on a specific client filesystem. 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
- Sun 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.

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 36
- Upgrading Avamar Administrator.. 39
- Uninstalling Avamar Administrator 39
- Starting Avamar Administrator 40
- Exploring the Avamar Administrator user interface 43

Installing Avamar Administrator

You can install Avamar Administrator on either Microsoft Windows or on Linux.

Installing on Microsoft Windows

To install Avamar Administrator on Microsoft Windows:

1. Log in to the computer where the software will be installed.
2. Open a web browser and go to the following URL:

   ```
   http://AVAMARSERVER
   ```

   where AVAMARSERVER is the Avamar server network hostname (as defined in DNS) or IP address.

   You are automatically redirected to the Avamar secure web server.
3. If a security alert dialog box appears due to browser security settings, click **Yes** or **OK** to allow redirection to the Avamar secure web server.

   The Secure Log On page appears.
4. Scroll down until the **Documents and Downloads** hyperlink appears.
5. Click **Documents and Downloads**.

   The Downloads and Documentation page appears.
6. Click the operating system hyperlink for the computer.

   A directory listing appears.
7. If necessary, install Java Runtime Environment (JRE) 1.6 Update 12:
   a. Click the **jre-6u12-windows-i586-p** install package.
   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.
8. Click the **AvamarConsoleMultiple** install package.
9. Open the installation file, or download the installation file and then open it from the saved location.
10. If a security warning appears, click **Run**.

    The installation wizard appears.
11. Click **Accept** for the license agreement.

    The installation destination window appears.
12. (Optional) To change the installation directory, click **Browse** and select a different destination.

NOTICE

You can install multiple versions of Avamar Administrator on the same computer. Each version is identified by its full version number (for instance, 6.1.0.420). To ensure against inadvertently overwriting an existing version, select the destination folder carefully.

13. Click **Install**.

Installing on Linux

To install Avamar Administrator on Linux, download the install package from the Avamar server and then run the installation.

Downloading the install package

To download the install package:

1. Log in to the computer where the software will be installed.
2. Open a web browser and go to the following URL:

   ```
   http://AVAMARSERVER
   ```

   where AVAMARSERVER is the Avamar server network hostname (as defined in DNS) or IP address.

   You are automatically redirected to the Avamar secure web server.
3. If a security alert dialog box appears due to browser security settings, click **Yes** or **OK** to allow redirection to the Avamar secure web server.

   The Secure Log On page appears.
4. Scroll down until the **Documents and Downloads** hyperlink appears.
5. Click **Documents and Downloads**.

   The Downloads and Documentation page appears.
6. If necessary, install Java Runtime Environment (JRE) 1.6 Update 12:
   a. Click **Downloads › Red Hat Enterprise Linux 3** and download **jre-6u12-linux-amd64.rpm** to a temporary install directory on the system, such as /tmp.
   b. Run the installation program from a command shell.
   c. Follow the onscreen instructions to complete the JRE installation.
7. Click **Downloads › Linux**.

   Download the Avamar Administrator (AvamarConsole) install package to a temporary install directory on the system.

   NOTICE

   Use the Red Hat Enterprise Linux 3.0 installer for Red Hat Enterprise Linux 9.0.
8. Note the filename of the Avamar Administrator (AvamarConsole) install package.

Running the installation on Linux

To install Avamar Administrator on Linux:

1. Open a command shell and log in as root on the computer where the software will be installed.

2. Change directory to the temporary install directory. For example:

   ```
   cd /tmp
   ```

3. Type:

   ```
   rpm -ih AVAMARLINUXCONSOLE.rpm
   ```

   where AVAMARLINUXCONSOLE.rpm is the filename for the Avamar Administrator (AvamarConsole) install package.

   The following appears in the command shell:

   ```
   Please run /usr/local/avamar/6.1.0-nnn/bin/avsetup_mcc to configure
   MC Client
   ```

4. Type:

   ```
   /usr/local/avamar/VERSION/bin/avsetup_mcc
   ```

   where VERSION is the version of Avamar Administrator that you are installing.

   The following appears in the command shell:

   ```
   Enter the location of your JRE 1.5 installation
   [/usr/java/jre1.6u12]:
   ```

5. 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/6.1.0-nnn]:
   ```

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

   The following appears in the command shell:

   ```
   Avamar Administrator 6.1.0.nnn 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 39, and install the new software as described in "Installing on Linux" on page 37. 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.

Starting Avamar Administrator

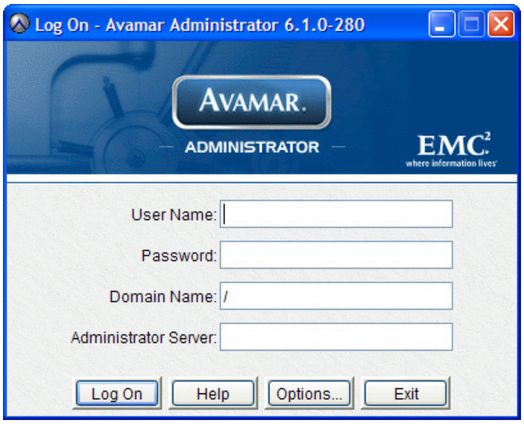
The following steps explain how to start Avamar Administrator when it is installed on the local computer. You also can launch Avamar Administrator from an Avamar Enterprise Manager session, as discussed in "Launching Avamar Administrator from Avamar Enterprise Manager" on page 337.

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.



Log On - Avamar Administrator 6.1.0-280

User Name:

Password:

Domain Name: /

Administrator Server:

2. In **User Name**, 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 69 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 backwards 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 through 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 75.

     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 384.

3. In **Password**, type the password for the user account.

4. In **Domain Name**, 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 48 provides details.

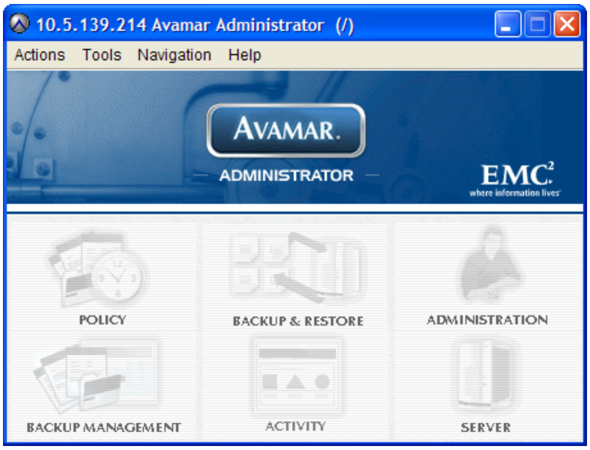
5. In **Avamar Server**, type the Avamar Administrator server name to log in to, as defined in the corporate Domain Name Server (DNS).

   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 launcher appears.



NOTICE

Full launcher functionality is only available to users assigned the role of Administrator. Other roles provide reduced functionality. "Understanding users, authentication, and roles" on page 67 provides details.

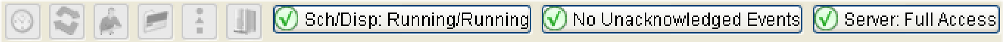
Each of the buttons invokes a different persistent window to perform specific tasks. You can invoke and switch among the windows using the Navigation menu or status bar shortcuts.

Exploring the Avamar Administrator user interface

The following topics discuss time-saving features and shortcuts in 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 2 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 and Restore	The Backup and Restore window is used to perform on-demand backups and restores. 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.
	Backup Management	The Backup Management window is used to change backup expiration dates, as well as validate backups or delete them from the system. "Changing a backup expiration date" on page 106, "Validating a backup" on page 109, and "Deleting a backup" on page 113 provide details.
	Activity	The Activity window is used to monitor backup and restore activity. "Monitoring backup, restore, or validation activities" on page 113 provides details.
	Server	The Server window is used to monitor server activity and client sessions. Chapter 16, "Advanced Server Administration and Maintenance," 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 3 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 296 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 298 provides details on re-enabling the scheduler. Chapter 14, "Capacity Management," and "Acknowledging system events" on page 296 provide details on resolving the system capacity issues and acknowledging the system event to resume backups.

Unacknowledged events

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

Table 4 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 display the Administration window Unacknowledged Events pane (tab). "Acknowledging system events" on page 296 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 5 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 297 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. "Data Domain status and resolutions" on page 568 provides details on the available detailed status messages.

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 pop-up 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 48
- Clients 52
- Understanding users, authentication, and roles 67
- Enabling user authentication 75
- Managing user accounts 81

Domains

The following topics provide details on Avamar domains:

- “Understanding Avamar domains and subdomains” on page 48
- “Creating a domain” on page 49
- “Editing domain information” on page 50
- “Deleting a domain” on page 51

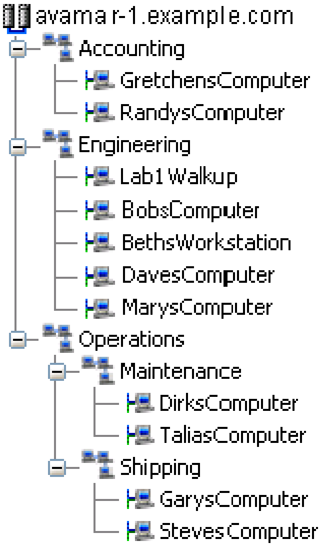
Understanding Avamar domains and subdomains

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 62. 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."

Domain and client name length limitation

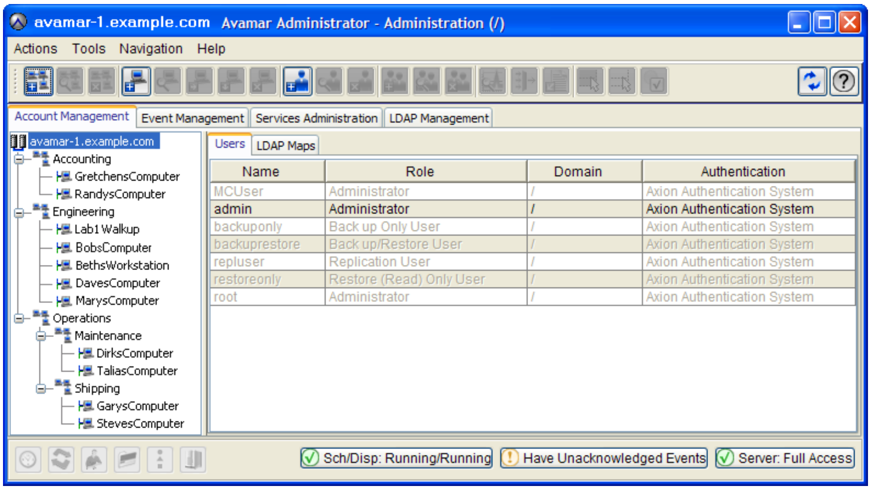
The sum of the characters in the domain, subdomain, and client names cannot exceed 63 characters. Therefore, it is best to use domain names that are short as practical.

Creating a domain

To create an Avamar domain:

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

   The Administration window appears.

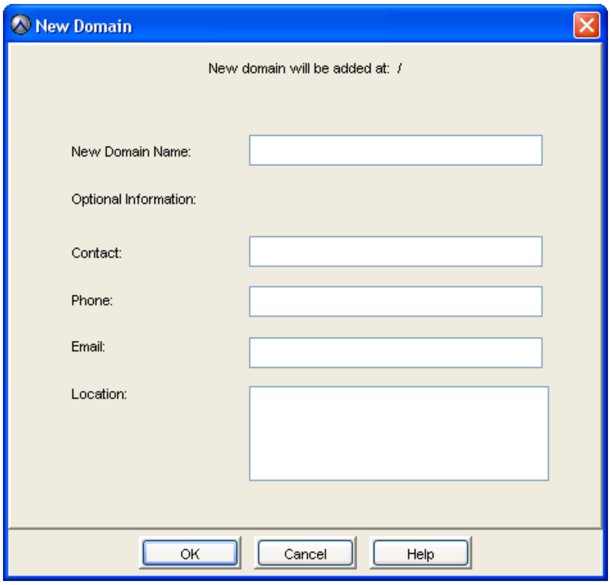


Name	Role	Domain	Authentication
MCUser	Administrator	/	Axion Authentication System
admin	Administrator	/	Axion Authentication System
backuponly	Back up Only User	/	Axion Authentication System
backuprestore	Back up/Restore User	/	Axion Authentication System
repluser	Replication User	/	Axion Authentication System
restoreonly	Restore (Read) Only User	/	Axion Authentication System
root	Administrator	/	Axion Authentication System

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.



New domain will be added at: /

   The complete client name and domain path cannot exceed 63 characters. When you create new domains, minimize the number of subdomains and keep domain names as short as practical.

5. In the **New Domain Name** box, type the name of the domain. Do not use any of the following characters in the domain name: ~!@$^%(){}[]|,`;#\/:*?<>'"&.
6. (Optional) In the **Contact** box, type the contact name.
7. (Optional) In the **Phone** box, type the contact telephone number.
8. (Optional) In the **Email** box, type the contact email address.
9. (Optional) In the **Location** box, 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:

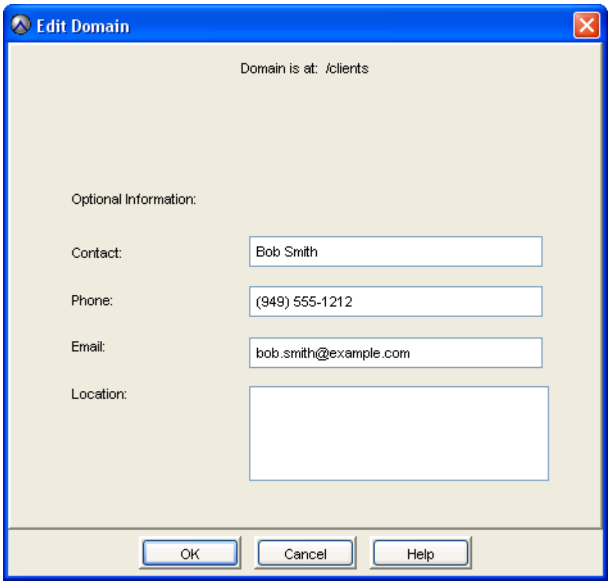
1. In Avamar Administrator, click the **Administration** launcher button.

   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.



Edit Domain

Domain is at: /clients

Optional Information:

Contact: Bob Smith

Phone: (949) 555-1212

Email: bob.smith@example.com

Location:

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 63.
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 52
- "Registering a single client" on page 54
- "Batch client registration" on page 55
- "Activating a client" on page 58
- "Editing client information" on page 59
- "Viewing client properties" on page 60
- "Enabling and disabling a client" on page 61
- "Retiring a client" on page 62
- "Moving a client to a new domain" on page 63
- "Deleting a client" on page 63
- "Editing client paging settings" on page 64

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:

- On a Windows client, install the Avamar Client for Windows and then initiate the registration process by right-clicking the Avamar server tray icon and selecting Activate.

- On a UNIX or Linux client, the Avamar client installation process prompts whether to register the client at that time.

Both client-side registration methods also activate 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 55 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 filesystem. There are two ways to activate a client:

- You can wait for the client to initiate activation. For example, right-click the Avamar system tray icon and select **Activate**.
- You can invite the client to activate with the server using Avamar Administrator. To do this, open the **Actions** menu and select **Account Management** › **Invite Client**.

For immediate activation using Avamar Administrator to succeed, the client must be present on the network, the Avamar client software must be installed and running, and the Avamar server must be able to resolve the hostname that was used to register the client. "Activating a client" on page 58 provides 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

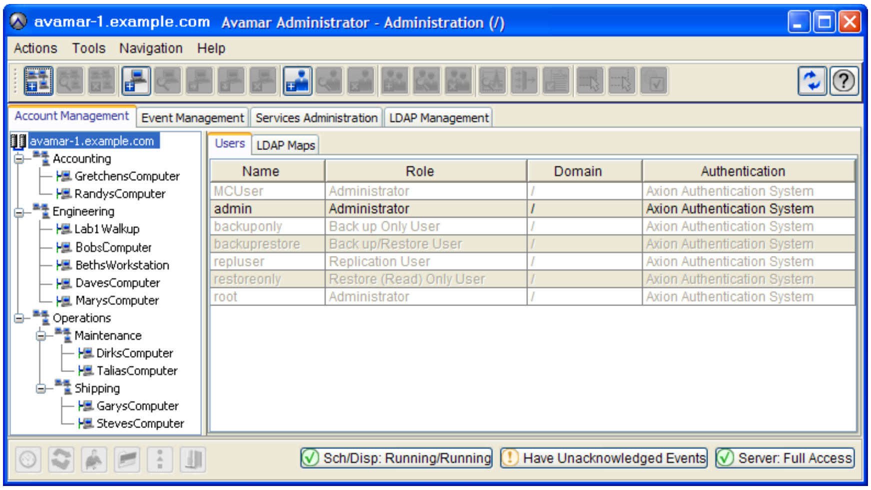
In Avamar Administrator, the client name must always be the client hostname. Furthermore, if you need to change the client name in Avamar Administrator because the client hostname changed, you must first shut down the Avamar software on the client computer, change the client name by editing the client information as described in "Editing client information" on page 59, 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.



Name	Role	Domain	Authentication
MCUser	Administrator	/	Axion Authentication System
admin	Administrator	/	Axion Authentication System
backuponly	Back up Only User	/	Axion Authentication System
backuprestore	Back up/Restore User	/	Axion Authentication System
repluser	Replication User	/	Axion Authentication System
restoreonly	Restore (Read) Only User	/	Axion Authentication System
root	Administrator	/	Axion Authentication System

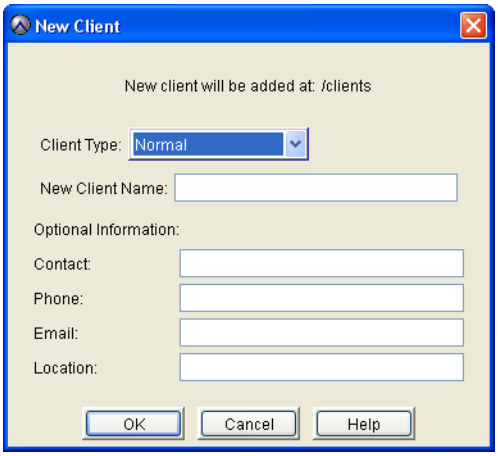
2. Click the **Account Management** tab.

   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.



New client will be added at: /clients

Client Type: Normal

New Client Name:

Optional Information:

Contact:

Phone:

Email:

Location:

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** box, type the client name.

   In Avamar Administrator, the client name must always be the client hostname. Additionally, the complete client name and domain path cannot exceed 63 characters.

7. (Optional) In the **Contact** box, type the contact name.
8. (Optional) In the **Phone** box, type the contact telephone number.
9. (Optional) In the **Email** box, type the contact email address.
10. (Optional) In the **Location** box, 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 53.

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 6 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 120 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 143 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.

NOTICE

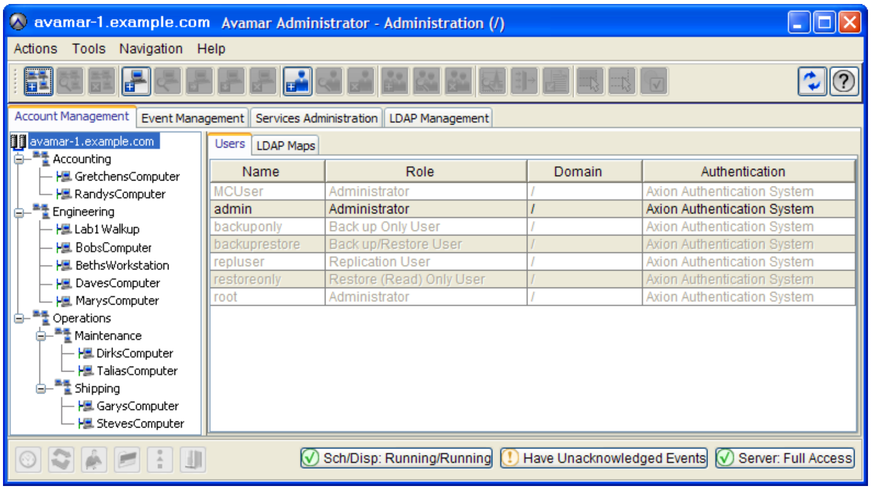
The previous clients definition file is shown for reference purposes only. Do not attempt to cut and paste this example into a clients definitions file. Invisible formatting characters will prevent you from successfully doing so.

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.



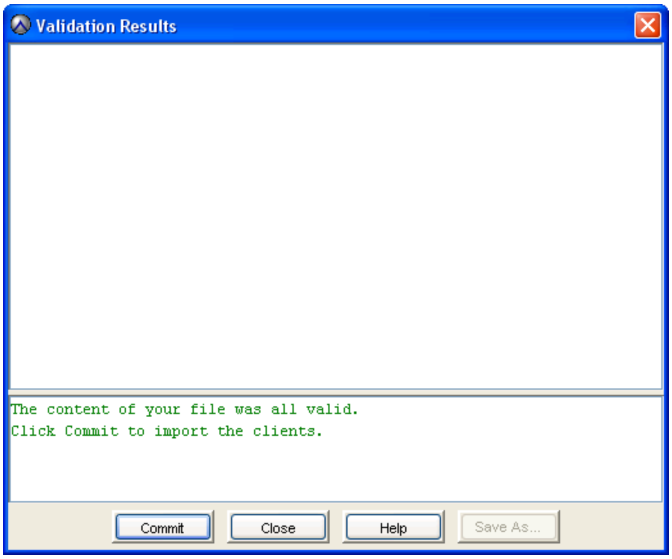
Name	Role	Domain	Authentication
MCUser	Administrator	/	Axion Authentication System
admin	Administrator	/	Axion Authentication System
backuponly	Back up Only User	/	Axion Authentication System
backuprestore	Back up/Restore User	/	Axion Authentication System
repluser	Replication User	/	Axion Authentication System
restoreonly	Restore (Read) Only User	/	Axion Authentication System
root	Administrator	/	Axion Authentication System

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

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

5. Click **Validate**.

   The Validation Results dialog box appears.



```
The content of your file was all valid.
Click Commit to import the clients.
```

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.

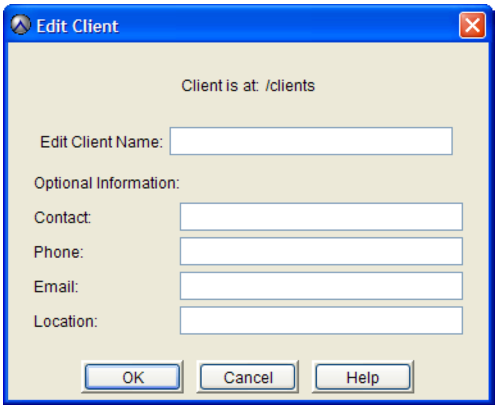
2. Click the **Account Management** tab.

   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.



Client is at: /clients

Edit Client Name:

Optional Information:

Contact:

Phone:

Email:

Location:

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

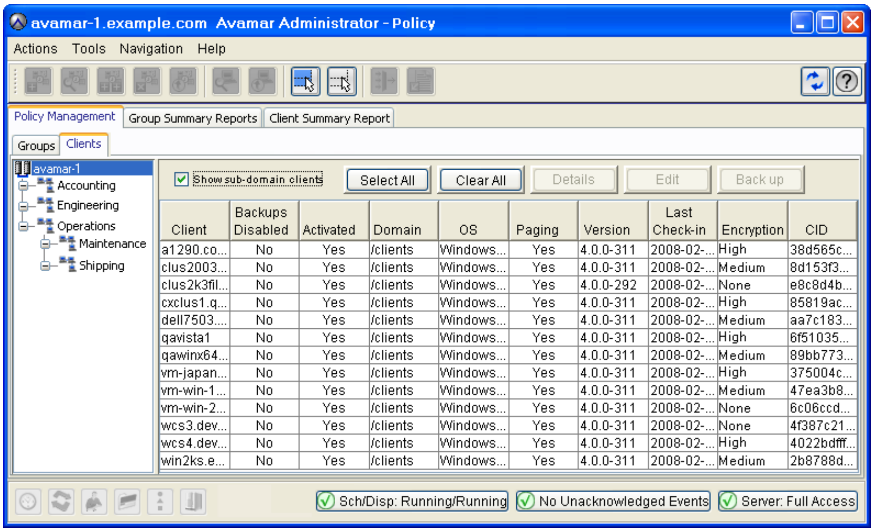
To view client properties:

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

   The Policy window appears.

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

3. Click the **Clients** tab.



☑ Show sub-domain clients

Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	CID
a1290.co...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	38d565c...
clus2003...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	8d153f3...
clus2k3fil...	No	Yes	/clients	Windows...	Yes	4.0.0-292	2008-02-...	None	e8c8d4b...
cxclus1.q...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	85819ac...
dell7503....	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	aa7c183...
qavista1	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	6f51035...
qawinx64...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	89bb773...
vm-japan...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	375004c...
vm-win-1...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	47ea3b8...
vm-win-2...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	6c06ccd...
wcs3.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	4f387c21...
wcs4.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	4022bdfff...
win2ks.e...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	2b8788d...

✓ Sch/Disp: Running/Running ✓ No Unacknowledged Events ✓ Server: Full Access

4. Select the client.

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

Table 7 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 filesystem 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.

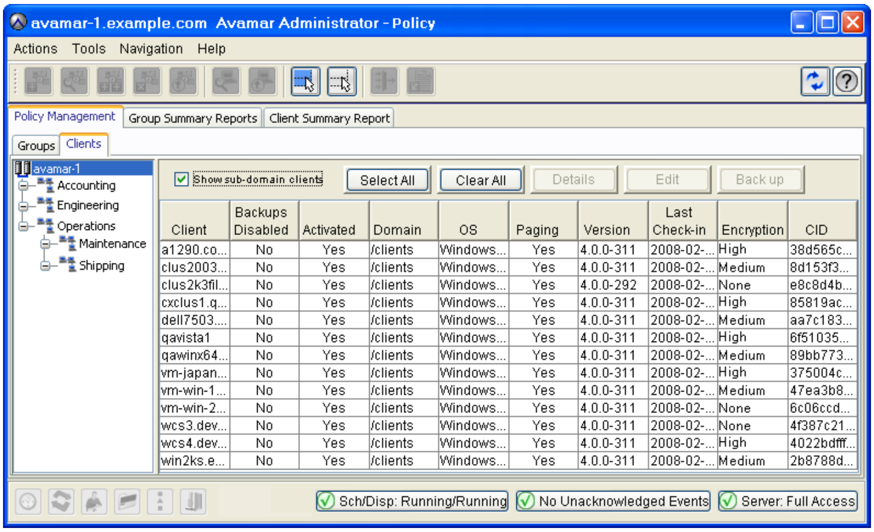
To disable and enable a client:

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

   The Policy window appears.

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

3. Click the **Clients** tab.



Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	CID
a1290.co...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	38d565c...
clus2003...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	8d153f3...
clus2k3fil...	No	Yes	/clients	Windows...	Yes	4.0.0-292	2008-02-...	None	e8c8d4b...
cxclus1.q...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	85819ac...
dell7503....	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	aa7c183...
qavista1	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	6f51035...
qawinx64...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	89bb773...
vm-japan...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	375004c...
vm-win-1...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	47ea3b8...
vm-win-2...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	6c06ccd...
wcs3.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	4f387c21...
wcs4.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	4022bdfff...
win2ks.e...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	2b8788d...

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.

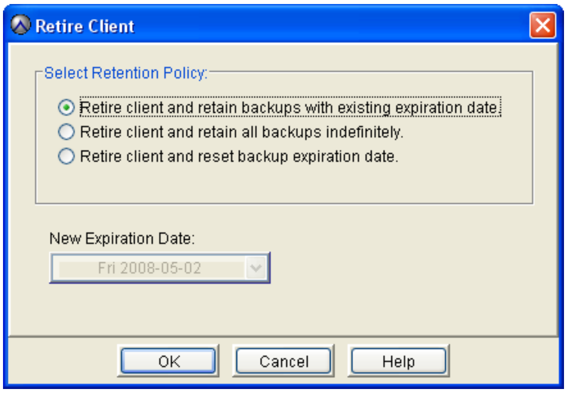
2. Click the **Account Management** tab.

   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.



Retire Client

Select Retention Policy:

● Retire client and retain backups with existing expiration date.
○ Retire client and retain all backups indefinitely.
○ Retire client and reset backup expiration date.

New Expiration Date: Fri 2008-05-02

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.

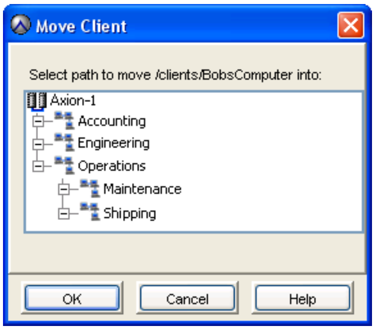
2. Click the **Account Management** tab.

   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.



Select path to move /clients/BobsComputer into:

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 62.

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.

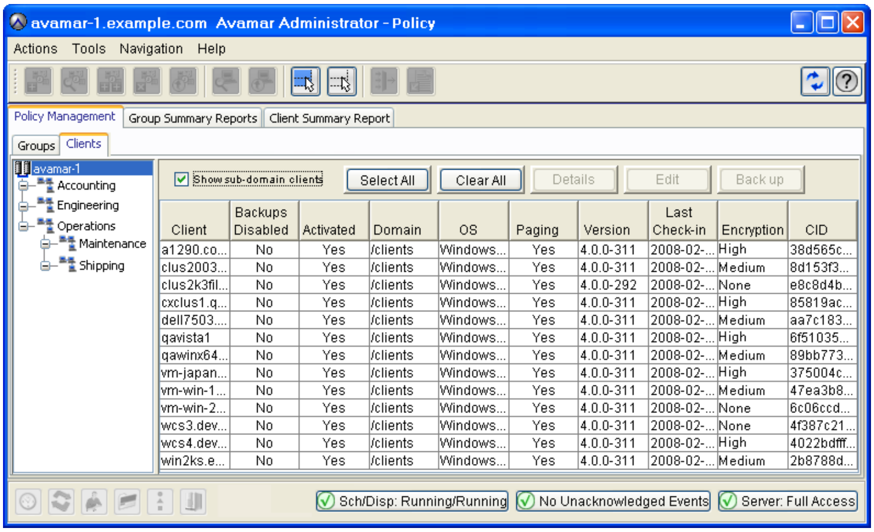
To edit client paging settings:

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

   The Policy window appears.

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

3. Click the **Clients** tab.



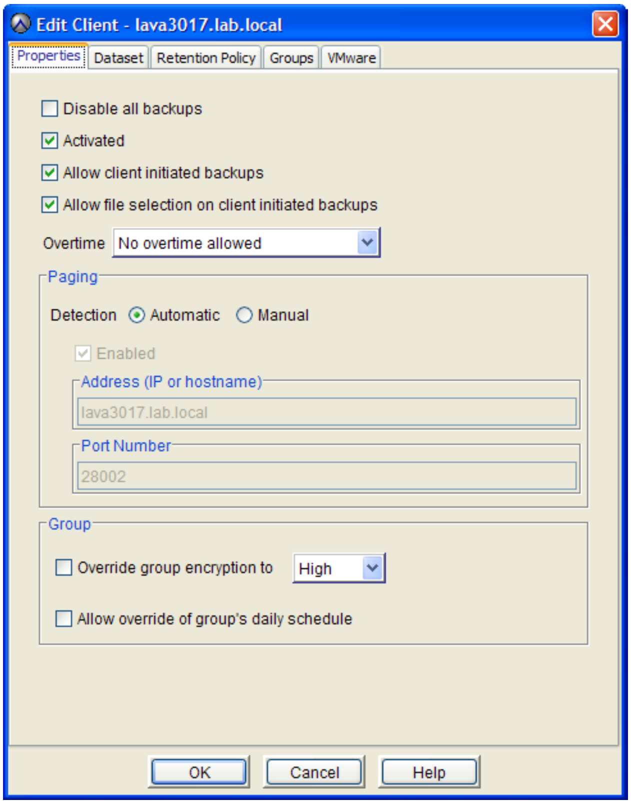
Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	CID
a1290.co...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	38d565c...
clus2003...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	8d153f3...
clus2k3fil...	No	Yes	/clients	Windows...	Yes	4.0.0-292	2008-02-...	None	e8c8d4b...
cxclus1.q...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	85819ac...
dell7503....	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	aa7c183...
qavista1	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	6f51035...
qawinx64...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	89bb773...
vm-japan...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	375004c...
vm-win-1...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	47ea3b8...
vm-win-2...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	6c06ccd...
wcs3.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	4f387c21...
wcs4.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	4022bdfff...
win2ks.e...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	2b8788d...

4. Select the client.

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

   The Edit Client window appears.

6. Click the **Properties** tab.



□ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

□ Override group encryption to: High

□ Allow override of group's daily schedule

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** box, 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 box. A hostname is probably not resolvable.

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

9. Click **OK**.

Understanding users, authentication, and roles

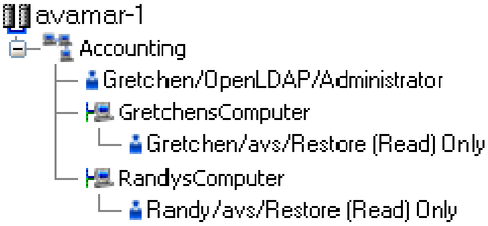
A user account in Avamar can administer a domain or client. The user account defines the authentication system that is used to grant users access to the Avamar server. It also defines the role for the user, which controls the operations that a user can perform. The following topics provide details:

- "Users" on page 67
- "User authentication" on page 68
- "Roles" on page 69

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:



```
avamar-1
  Accounting
    Gretchen/OpenLDAP/Administrator
    GretchensComputer
      Gretchen/avs/Restore (Read) Only
    RandysComputer
      Randy/avs/Restore (Read) Only
```

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 68 provides details on supported authenticaton systems.
- **Role** — Roles define the allowable operations for each user account. "Roles" on page 69 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 68
- "Directory service authentication" on page 68
- "Enterprise authentication" on page 68

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 75 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 79 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 69
- "Operator roles" on page 70
- "User roles" on page 74

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

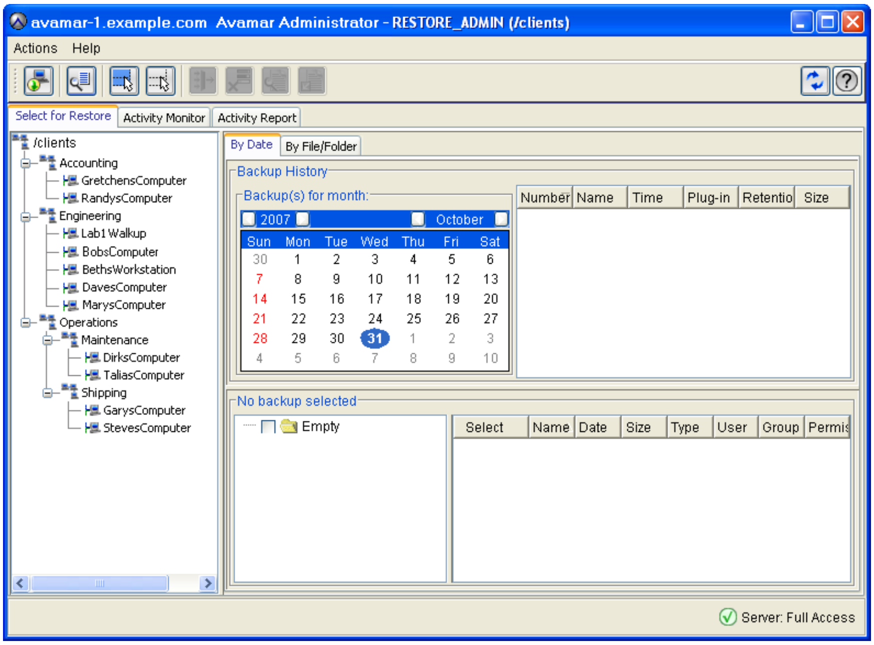
Users with an operator role do not have access to all features in Avamar Administrator. Instead, after login, they are presented with a single window that provides access to the features that they are allowed to use.

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.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

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 113.

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"
```

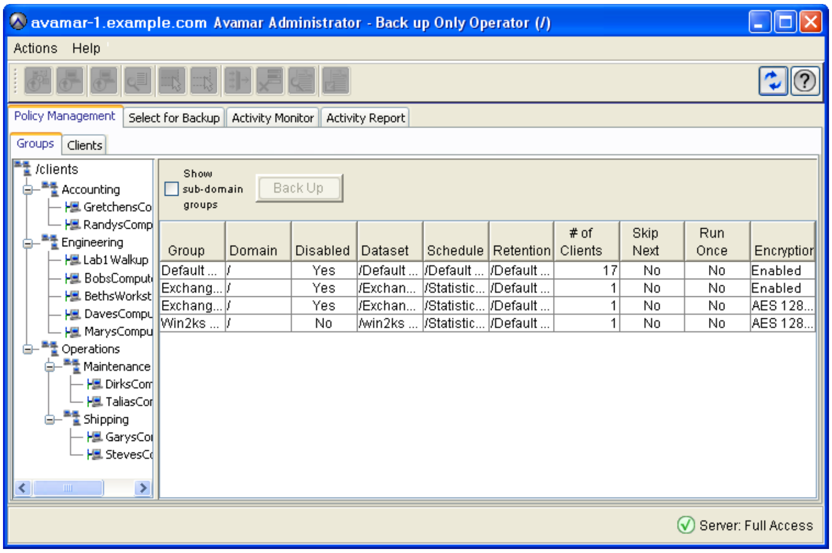
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user, and AUTH is the external authentication system used to authenticate the user.

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.



□ Show sub-domain groups

Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryption
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	Enabled
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Enabled
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	AES 128...
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	AES 128...

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 86.
- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 113.
- Initiate on-demand group backups as described in "Initiating on-demand group backups" on page 181.

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"
```

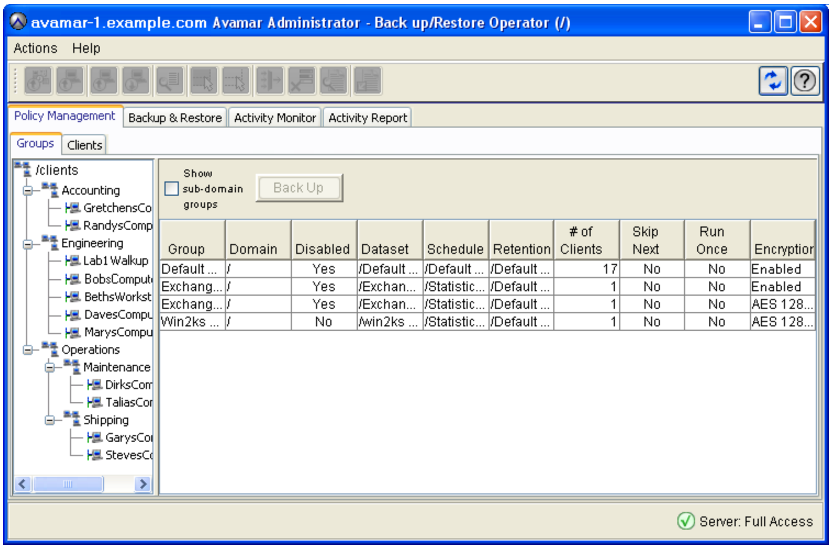
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user, and AUTH is the external authentication system used to authenticate the user.

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.



Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryptior
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	Enabled
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Enabled
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	AES 128...
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	AES 128...

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 86.
- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 113.
- Perform a restore as described in Chapter 4, "Backup, Restore, and Backup Management."
- Initiate on-demand group backups as described in "Initiating on-demand group backups" on page 181.

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"
```

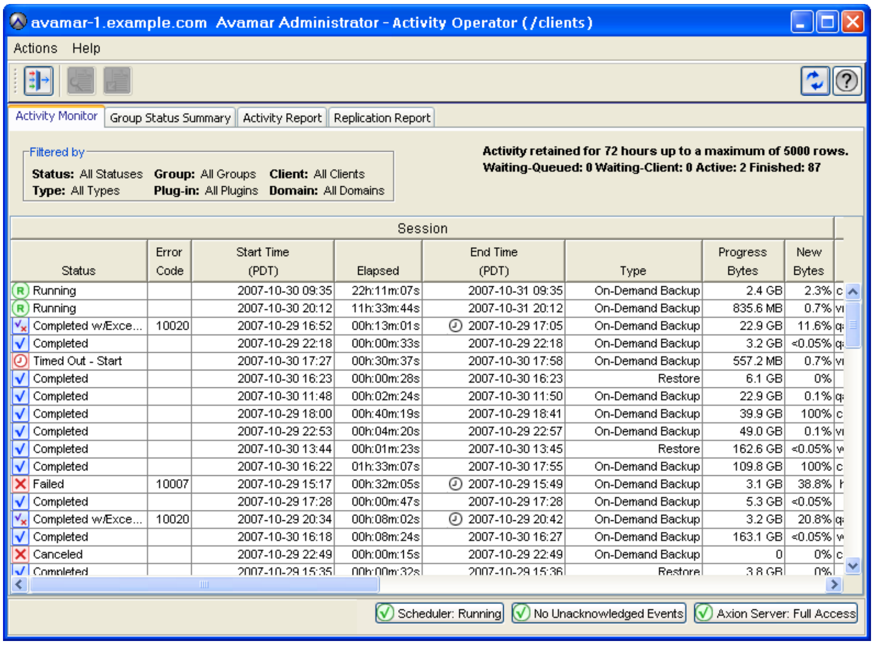
where LOCATION is the subdomain of the operator, NAME is the Avamar username of the user , and AUTH is the external authentication system used to authenticate the user.

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.



Filtered by
Status: All Statuses **Group:** All Groups **Client:** All Clients
Type: All Types **Plug-in:** All Plugins **Domain:** All Domains

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 2 Finished: 87

Session								
Status	Error Code	Start Time (PDT)	Elapsed	End Time (PDT)	Type	Progress Bytes	New Bytes	
Running		2007-10-30 09:35	22h:11m:07s	2007-10-31 09:35	On-Demand Backup	2.4 GB	2.3%	c
Running		2007-10-30 20:12	11h:33m:44s	2007-10-31 20:12	On-Demand Backup	835.6 MB	0.7%	vi
Completed w/Exce...	10020	2007-10-29 16:52	00h:13m:01s	2007-10-29 17:05	On-Demand Backup	22.9 GB	11.6%	q
Completed		2007-10-29 22:18	00h:00m:33s	2007-10-29 22:18	On-Demand Backup	3.2 GB	<0.05%	q
Timed Out - Start		2007-10-30 17:27	00h:30m:37s	2007-10-30 17:58	On-Demand Backup	557.2 MB	0.7%	vi
Completed		2007-10-30 16:23	00h:00m:28s	2007-10-30 16:23	Restore	6.1 GB	0%	
Completed		2007-10-30 11:48	00h:02m:24s	2007-10-30 11:50	On-Demand Backup	22.9 GB	0.1%	q
Completed		2007-10-29 18:00	00h:40m:19s	2007-10-29 18:41	On-Demand Backup	39.9 GB	100%	c
Completed		2007-10-29 22:53	00h:04m:20s	2007-10-29 22:57	On-Demand Backup	49.0 GB	0.1%	vi
Completed		2007-10-30 13:44	00h:01m:23s	2007-10-30 13:45	Restore	162.6 GB	<0.05%	w
Completed		2007-10-30 16:22	01h:33m:07s	2007-10-30 17:55	On-Demand Backup	109.8 GB	100%	c
Failed	10007	2007-10-29 15:17	00h:32m:05s	2007-10-29 15:49	On-Demand Backup	3.1 GB	38.8%	I
Completed		2007-10-29 17:28	00h:00m:47s	2007-10-29 17:28	On-Demand Backup	5.3 GB	<0.05%	
Completed w/Exce...	10020	2007-10-29 20:34	00h:08m:02s	2007-10-29 20:42	On-Demand Backup	3.2 GB	20.8%	q
Completed		2007-10-30 16:18	00h:08m:24s	2007-10-30 16:27	On-Demand Backup	163.1 GB	<0.05%	w
Canceled		2007-10-29 22:49	00h:00m:15s	2007-10-29 22:49	On-Demand Backup	0	0%	c
Completed		2007-10-29 15:35	00h:00m:32s	2007-10-29 15:36	Restore	3.8 GB	0%	

✓ Scheduler: Running ✓ No Unacknowledged Events ✓ Axion Server: Full Access

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

- Monitor activities as described in "Monitoring backup, restore, or validation activities" on page 113.
- View the group status summary as described in "Viewing the Group Status Summary" on page 165.
- View the Activity Report as described in "Viewing the Activity Report" on page 236.
- View the Replication Report as described in "Viewing the Replication Report" on page 240.

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 75
- "Enabling directory service authentication" on page 75
- "Enabling selection of enterprise authentication" on page 79

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 81.

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 378.

3. Create an LDAP map to associate the directory service group to Avamar user information, as discussed in “Adding an LDAP map” on page 77. An LDAP map is a database construct that ties a group of users to the following Avamar user information:

   - Authentication system
   - Domain or client 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

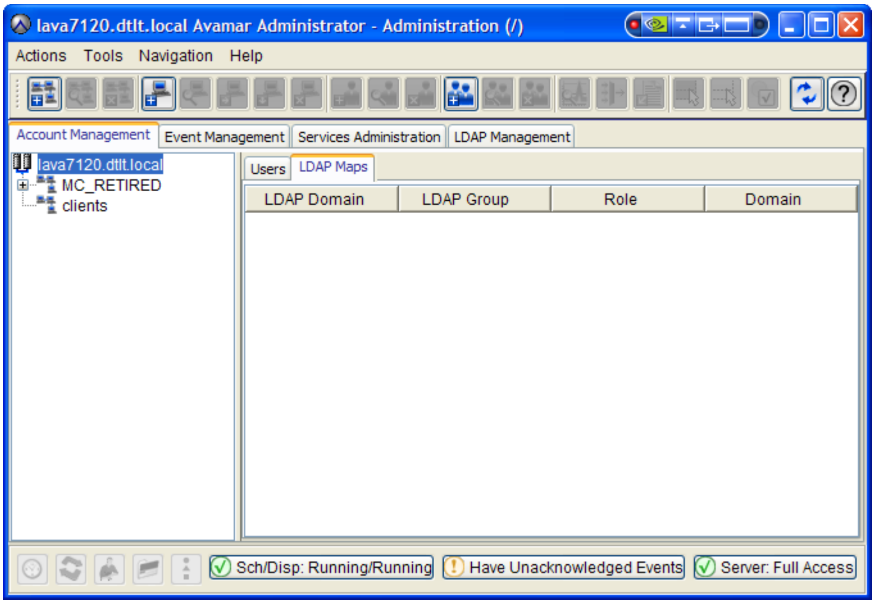
To add an LDAP map:

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.

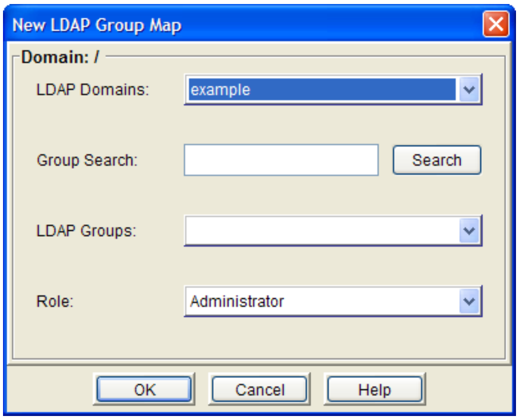


LDAP Domain	LDAP Group	Role	Domain

4. In the left-pane hierarchical tree, select the domain, subdomain, or client 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.



Domain: /

LDAP Domains: example

Group Search:

LDAP Groups:

Role: Administrator

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

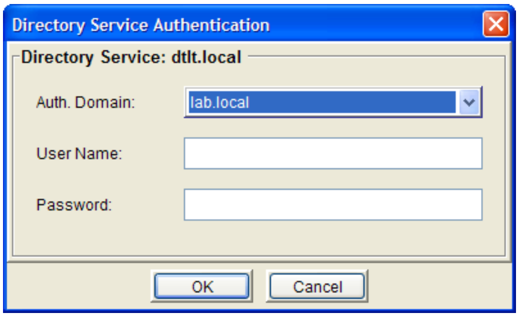
   If the list is empty, click Cancel to close the dialog box, configure directory service domains as described in "Configuring directory service information" on page 378, and then return to this task.

7. In the **Group Search** box, 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.



Directory Service Authentication

Directory Service: dtlt.local

Auth. Domain: lab.local

User Name:

Password:

   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** box, type a username for an account that has Read privileges for the domain.

11. In the **Password** box, 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 67.

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, subdomain, or client.

   The maps for the domain, subdomain, or client 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, subdomain, or client.

   The maps for the domain, subdomain, or client 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 mcserver.xml 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. 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 ldap node, as shown here:

   ```
   <node name="ldap">
      <map>
          <entry key="enable_new_user_authentication_selection"
   value="false" />
          <entry key="ldap_services_timeout_seconds" value="60" />
      </map>
   </node>
   ```

5. Change the value of the entry with key="enable_new_user_authentication_selection" to "true":

   ```
   <node name="ldap">
      <map>
          <entry key="enable_new_user_authentication_selection"
   value="true" />
          <entry key="ldap_services_timeout_seconds" value="60" />
      </map>
   </node>
   ```

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.

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 81
- "Editing user information" on page 83
- "Deleting a user" on page 84

Adding a user to a client or domain

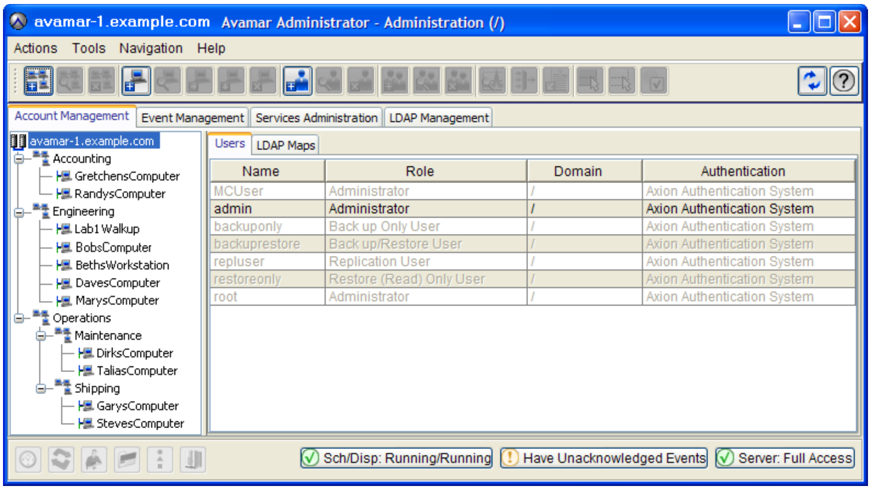
This topic describes how to add a user account to a client or domain when the user account is authenticated using Avamar internal authentication or the deprecated enterprise authentication system.

"Enabling directory service authentication" on page 75 provides details on adding a user that that uses an existing directory service for authentication.

To add a user to a client or domain:

1. Review "Roles" on page 69 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.



Name	Role	Domain	Authentication
MCUser	Administrator	/	Axion Authentication System
admin	Administrator	/	Axion Authentication System
backuponly	Back up Only User	/	Axion Authentication System
backuprestore	Back up/Restore User	/	Axion Authentication System
repluser	Replication User	/	Axion Authentication System
restoreonly	Restore (Read) Only User	/	Axion Authentication System
root	Administrator	/	Axion Authentication System

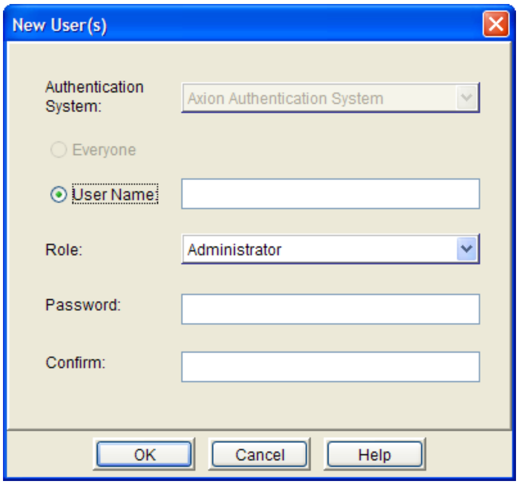
3. Click the **Account Management** tab.
4. Click the **Users** tab
5. In the left-pane hierarchical tree, select the domain or client for the new user.

   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 dialog box appears.



Authentication System: Axion Authentication System

○ Everyone

● User Name:

Role: Administrator

Password:

Confirm:

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 79.

   For a more robust alternative to enterprise authentication, use the method described in "Enabling directory service authentication" on page 75.

8. (Optional) If you select the enterprise authenticatno 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** box, type a password for the user.

    Passwords are case-sensitive and must:

    - Be 6–12 characters in length
    - Contain only alphanumeric, hyphen, period, or underscore characters
    - Contain at least one alphanumeric character

    This field is not used with enterprise authentication.

12. In the **Confirm** box, 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.

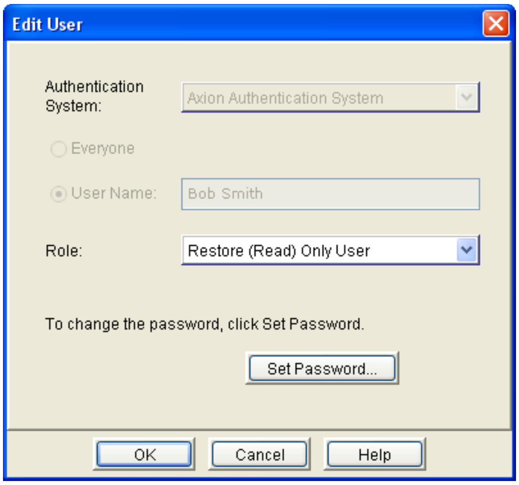
   In the Account Management tree, the icons for the clients indicate status. An x appears for disabled clients, a question mark appears for unregistered clients, and there is no special icon designation for active clients.

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.



Edit User

Authentication System: Axion Authentication System

○ Everyone

● User Name: Bob Smith

Role: Restore (Read) Only User

To change the password, click Set Password.

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** boxes.

   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 86
- Restoring data from a backup.. 88
- Managing backups... 103
- Monitoring backup, restore, or validation activities 113
- Canceling a backup, restore, or validation 118

NOTICE

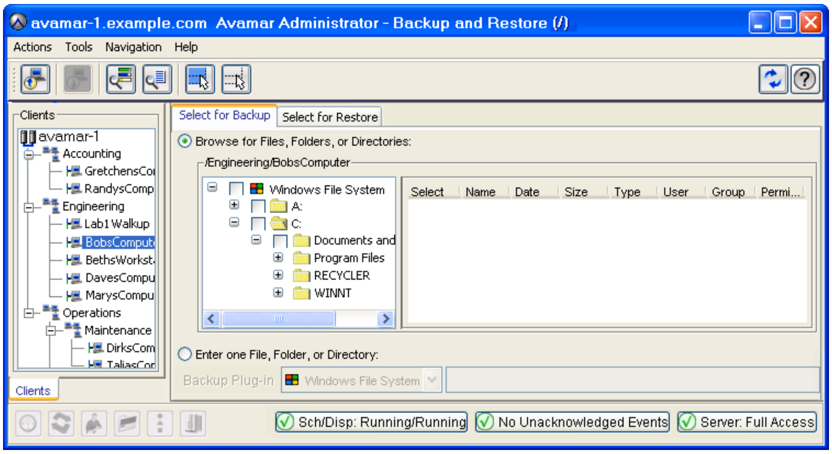
You can also automate backups by implementing a group policy to perform regularly scheduled backups for a group of clients. Chapter 6, “Groups and Group Policies,” provides details.

Performing an on-demand backup

To perform an on-demand client backup:

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

   The Backup and Restore window appears.



2. 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 filesystem 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.

3. Click the **Select for Backup** tab.

   A list of plug-ins installed on the selected client appears in the left pane of the Select for Backup tab.

4. Expand the node for the plug-in to use for the backup.

5. Browse to and select the data to back up.

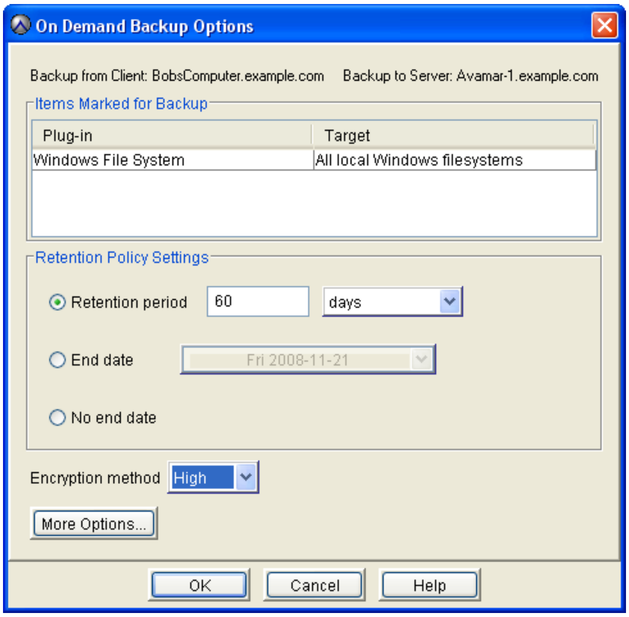
6. If you browse the client filesystem, specify a valid client username and password, then click **OK**.

   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.



On Demand Backup Options

Backup from Client: BobsComputer.example.com Backup to Server: Avamar-1.example.com

Items Marked for Backup

Plug-in	Target
Windows File System	All local Windows filesystems

Retention Policy Settings

● Retention period 60 days

○ End date Fri 2008-11-21

○ No end date

Encryption method High

9. Select the backup retention setting:

   - 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.**

10. Select the encryption method to use for client/server data transfer during this backup.

    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.

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 88
- "Restoring to the original location" on page 93
- "Restoring to a different location" on page 95
- "Restoring to multiple locations" on page 99

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 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 89
- "How to find a backup by date" on page 89
- "When to find a backup by file or folder" on page 90
- "How to find a backup by file or folder" on page 91

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 and Restore window appears.
2. 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.
3. Click the **Select for Restore** tab.
4. Click the **By Date** tab.
5. Select a backup from the calendar:

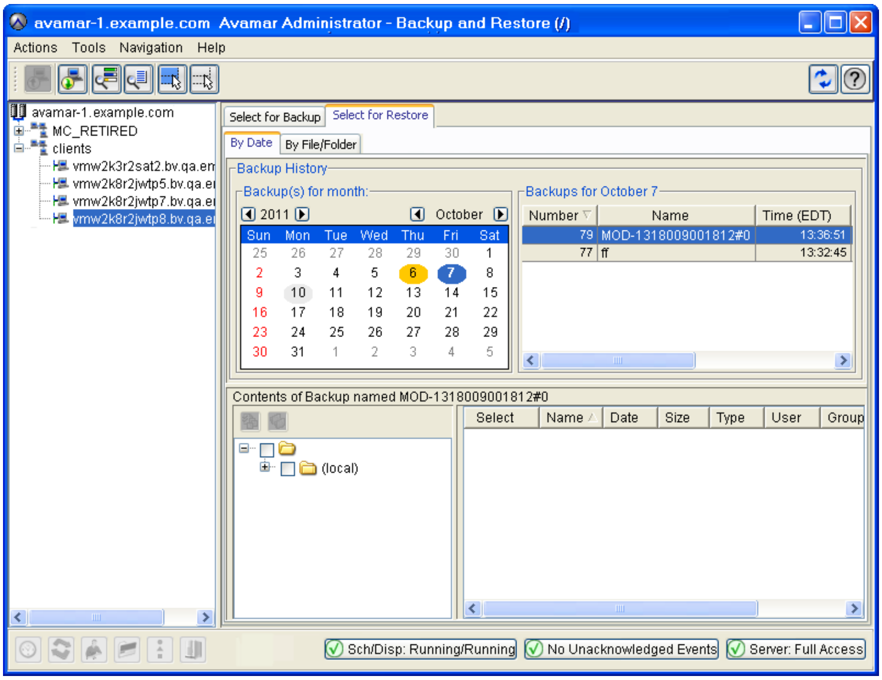
   a. Use the year and month navigational arrows to browse to a backup.

      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.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Number	Name	Time (EDT)
79	MOD-1318009001812#0	13:36:51
77	ff	13:32:45

7. Select the data to restore from the **Contents of Backup** pane at the bottom of the **Select for Restore** tab.

8. If you browse the client filesystem, 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 and Restore window appears.
2. 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.
3. Click the **Select for Restore** tab.
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 8 Methods to browse to a backup by file or folder

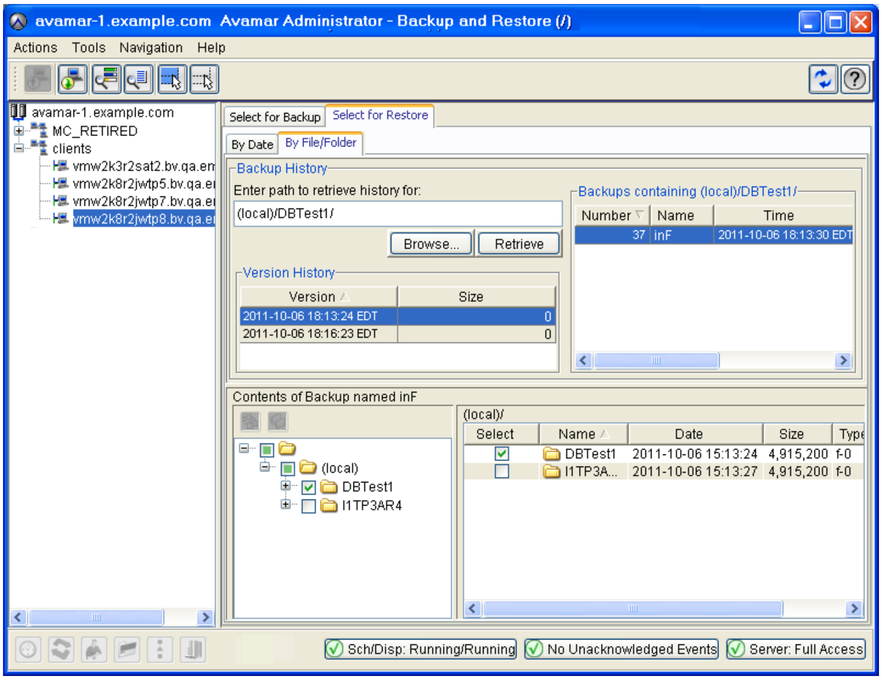
Method	Steps
Type the path to the file or folder	Type the full path to the client directory or file in the **Enter path to retrieve history for** text box.
Browse to the file or folder	1. Click **Browse**. The Select File or Folder window appears. 2. Select the client. 3. Select the plug-in. A list of 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.



Enter path to retrieve history for: (local)/DBTest1/

Backups containing (local)/DBTest1/

Number	Name	Time
37	inF	2011-10-06 18:13:30 EDT

Version	Size
2011-10-06 18:13:24 EDT	0
2011-10-06 18:16:23 EDT	0

(local)/

Select	Name	Date	Size	Type
☑	DBTest1	2011-10-06 15:13:24	4,915,200	f-0
□	I1TP3A...	2011-10-06 15:13:27	4,915,200	f-0

9. Select the data to restore from the **Contents of Backup** pane at the bottom of the **Select for Restore** tab.

10. If you browse the client filesystem, 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**.

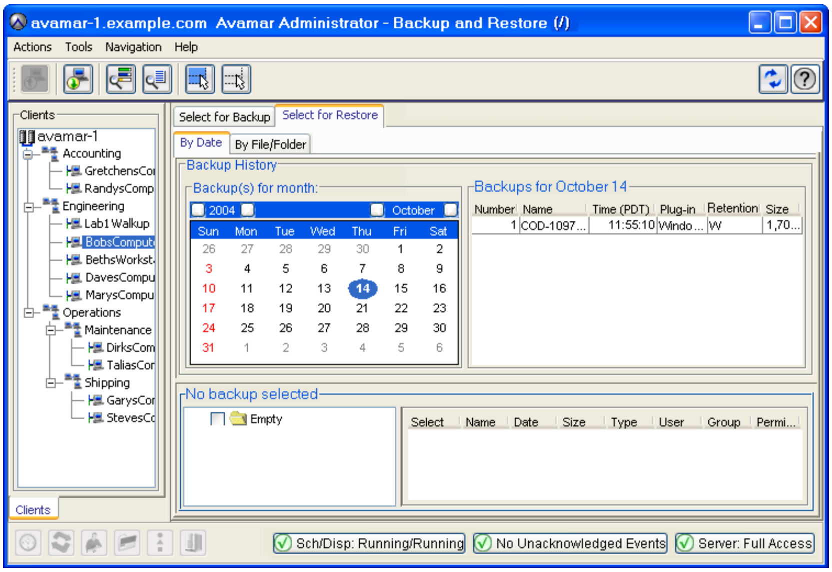
Restoring to the original location

To restore backup data to its original location:

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

   The Backup and Restore window appears.

2. Click the **Select for Restore** tab.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Number	Name	Time (PDT)	Plug-in	Retention	Size
1	COD-1097...	11:55:10	Windo...	W	1,70...

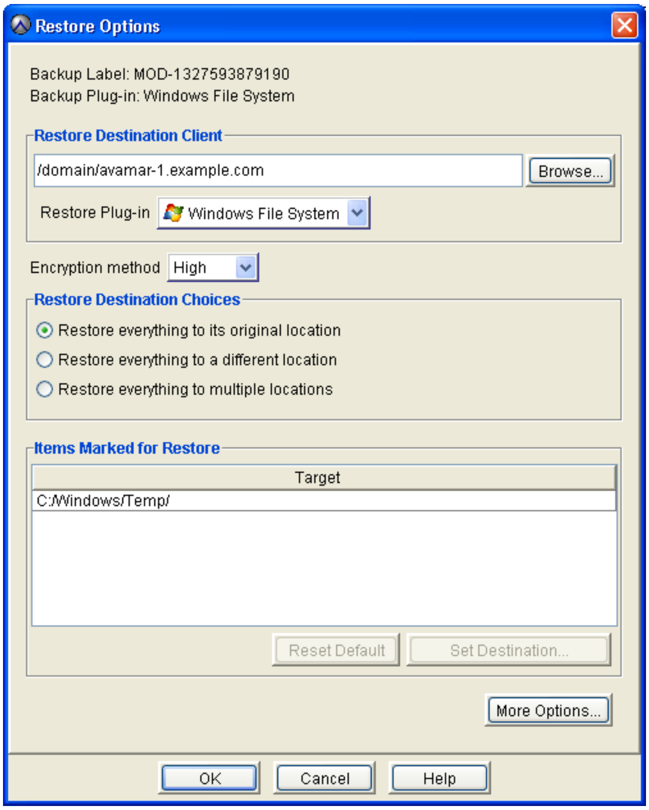
Select	Name	Date	Size	Type	User	Group	Permi...

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 89
   - “How to find a backup by file or folder” on page 91

4. Select **Actions › Restore Now.**

The Restore Options dialog box appears.



Restore Options

Backup Label: MOD-1327593879190
Backup Plug-in: Windows File System

Restore Destination Client

/domain/avamar-1.example.com

Restore Plug-in: Windows File System

Encryption method: High

Restore Destination Choices

● Restore everything to its original location
○ Restore everything to a different location
○ Restore everything to multiple locations

Items Marked for Restore

Target
C:/Windows/Temp/

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**.

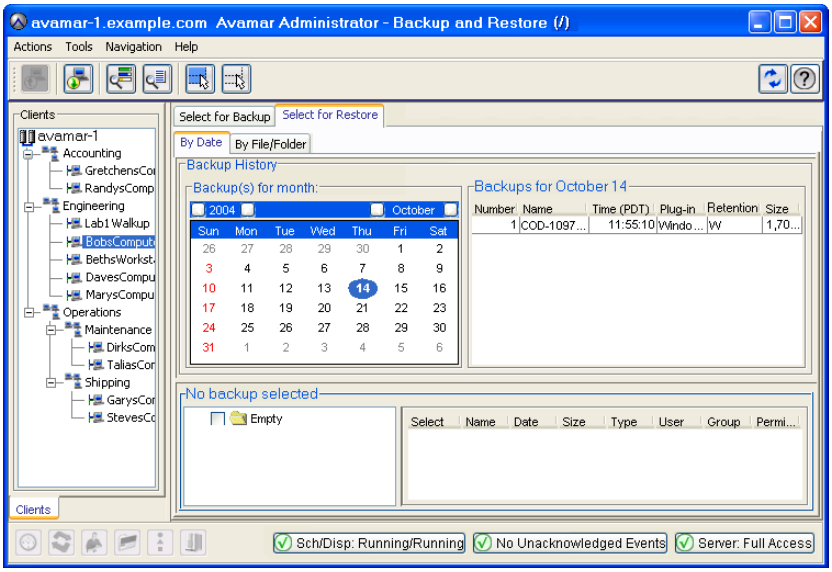
Restoring to a different location

To restore backup data to a single different location:

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

   The Backup and Restore window appears.

2. Click the **Select for Restore** tab.



avamar-1.example.com Avamar Administrator - Backup and Restore (/)

2004 October

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Backups for October 14

Number	Name	Time (PDT)	Plug-in	Retention	Size
1	COD-1097...	11:55:10	Windo...	W	1,70...

Select	Name	Date	Size	Type	User	Group	Permi...

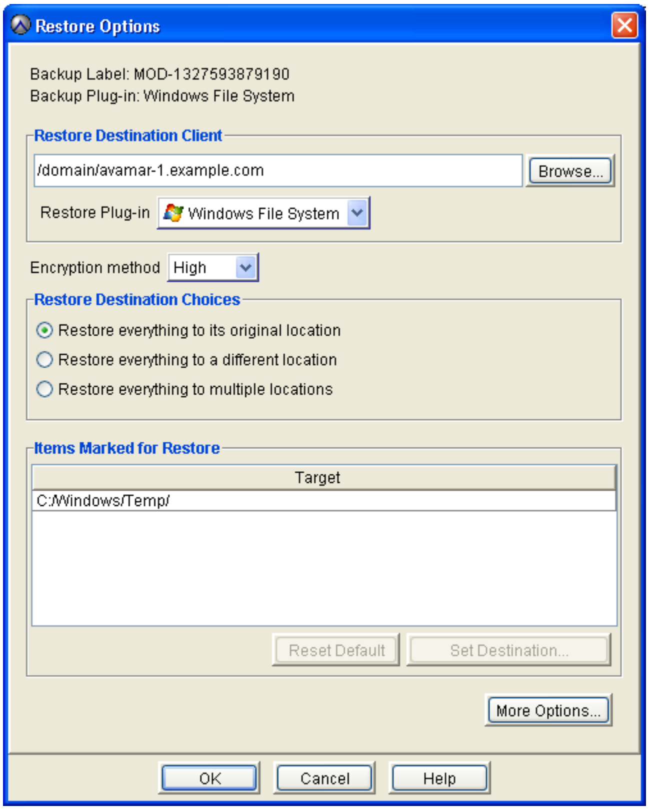
Sch/Disp: Running/Running
No Unacknowledged Events
Server: Full Access

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 89
   - "How to find a backup by file or folder" on page 91

4. Select **Actions › Restore Now.**

The Restore Options dialog box appears.



Backup Label: MOD-1327593879190
Backup Plug-in: Windows File System

/domain/avamar-1.example.com

Restore Plug-in: Windows File System

Encryption method: High

● Restore everything to its original location
○ Restore everything to a different location
○ Restore everything to multiple locations

C:/Windows/Temp/

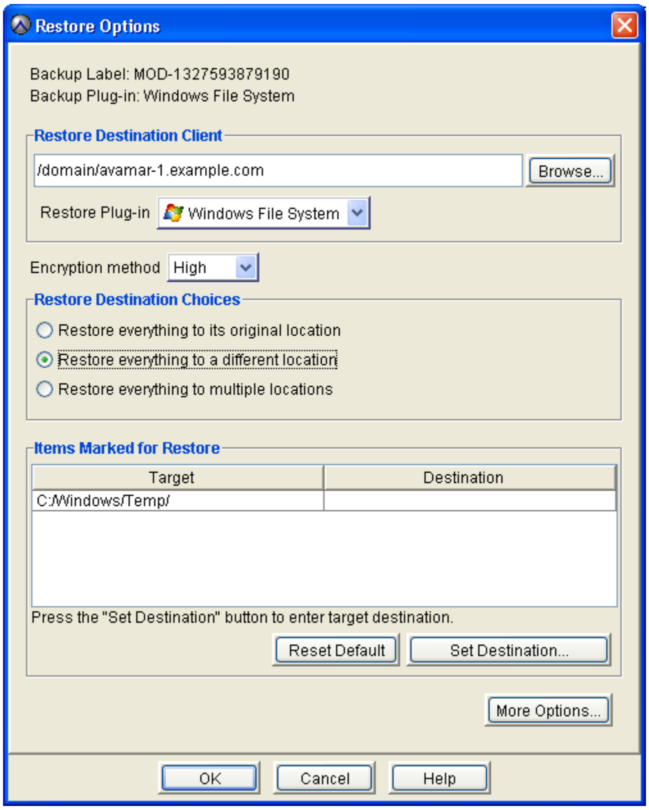
5. Select the destination client for the data to restore:
   - To restore to a different location on the same client, leave the default selection of the original client in the **Restore Destination Client** box.
   - To restore to a different client:
     a. Click the **Browse** button next to the **Restore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



Restore Options

Backup Label: MOD-1327593879190
Backup Plug-in: Windows File System

Restore Destination Client

/domain/avamar-1.example.com

Restore Plug-in: Windows File System

Encryption method: High

Restore Destination Choices

○ Restore everything to its original location
● Restore everything to a different location
○ Restore everything to multiple locations

Items Marked for Restore

Target	Destination
C:/Windows/Temp/	

Press the "Set Destination" button to enter target destination.

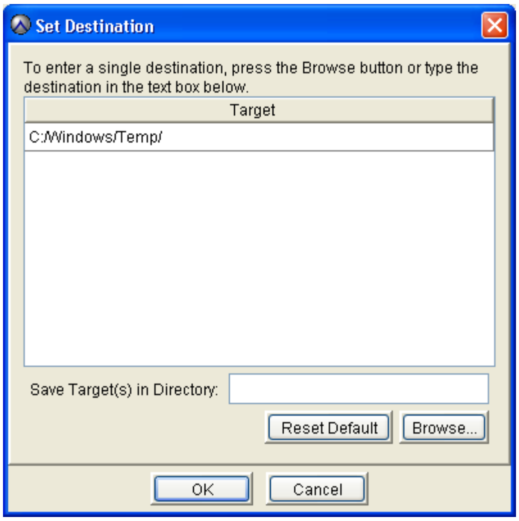
NOTICE

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.



Set Destination

To enter a single destination, press the Browse button or type the destination in the text box below.

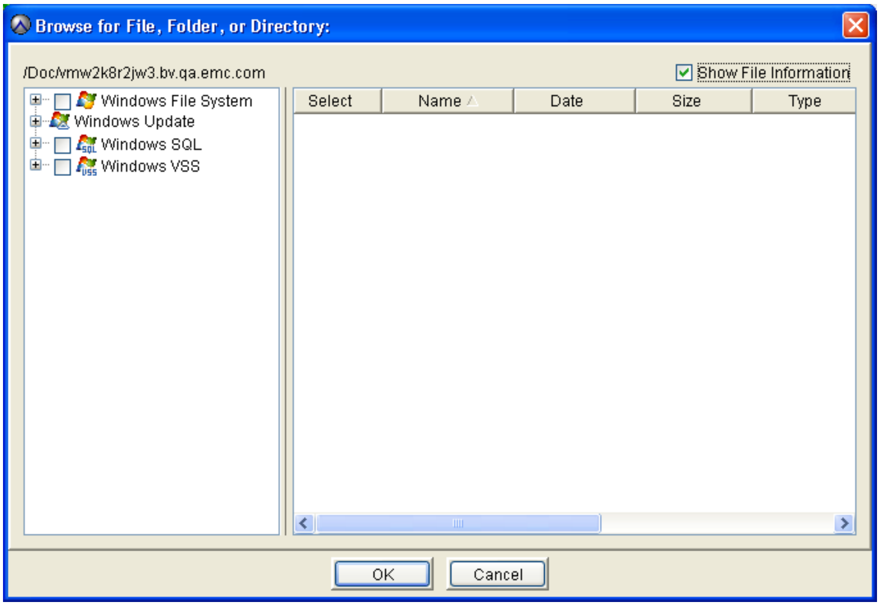
Target
C:/Windows/Temp/

Save Target(s) in Directory:

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.

NOTICE

If a file with the same name already exists in the path to which you are restoring a file, then 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**.

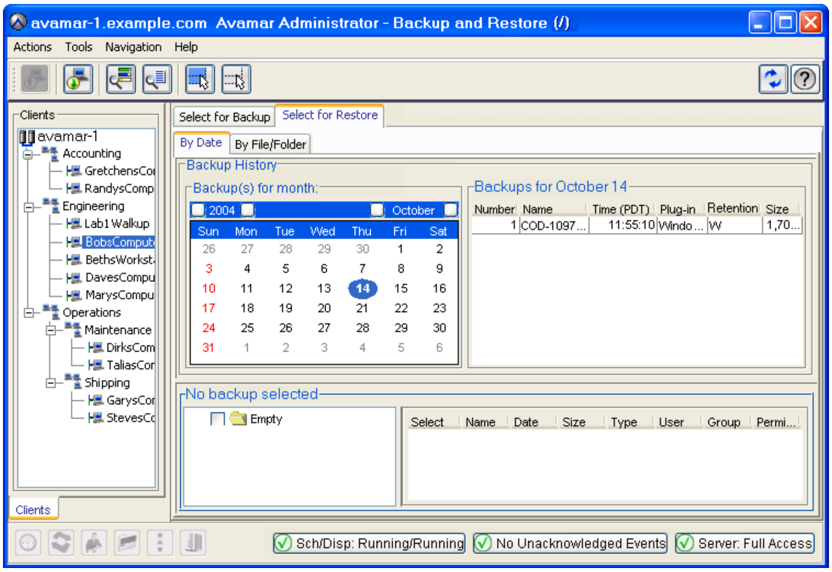
Restoring to multiple locations

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

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

   The Backup and Restore window appears.

2. Click the **Select for Restore** tab.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Number	Name	Time (PDT)	Plug-in	Retention	Size
1	COD-1097...	11:55:10	Windo...	W	1,70...

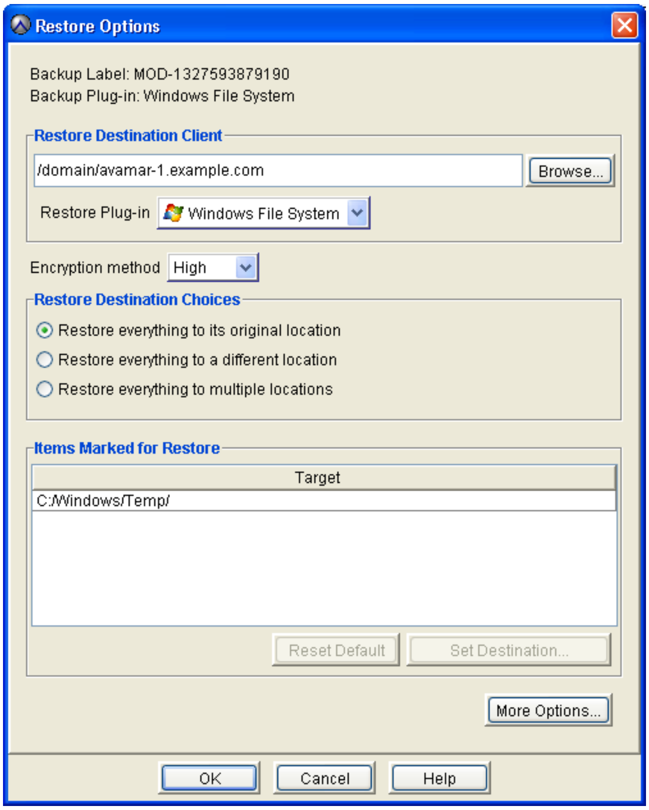
Select	Name	Date	Size	Type	User	Group	Permi...

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 89
   - “How to find a backup by file or folder” on page 91

4. Select **Actions › Restore Now.**

The Restore Options dialog box appears.



Backup Label: MOD-1327593879190
Backup Plug-in: Windows File System

Restore Destination Client

/domain/avamar-1.example.com

Restore Plug-in: Windows File System

Encryption method: High

Restore Destination Choices

● Restore everything to its original location
○ Restore everything to a different location
○ Restore everything to multiple locations

Items Marked for Restore

Target
C:/Windows/Temp/

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.

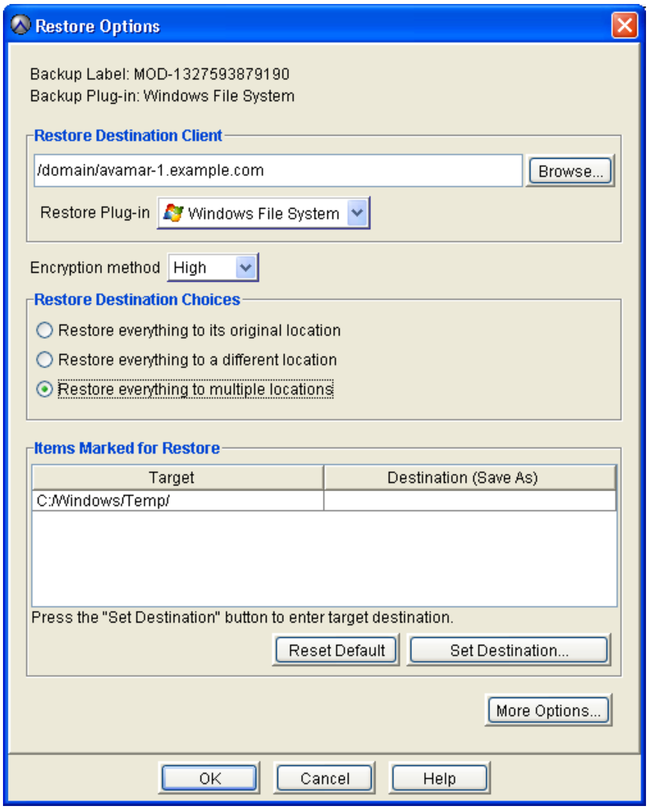
     c. Click **OK**.

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**.



Restore Options

Backup Label: MOD-1327593879190
Backup Plug-in: Windows File System

Restore Destination Client

/domain/avamar-1.example.com

Restore Plug-in: Windows File System

Encryption method: High

Restore Destination Choices

○ Restore everything to its original location
○ Restore everything to a different location
● Restore everything to multiple locations

Items Marked for Restore

Target	Destination (Save As)
C:/Windows/Temp/	

Press the "Set Destination" button to enter target destination.

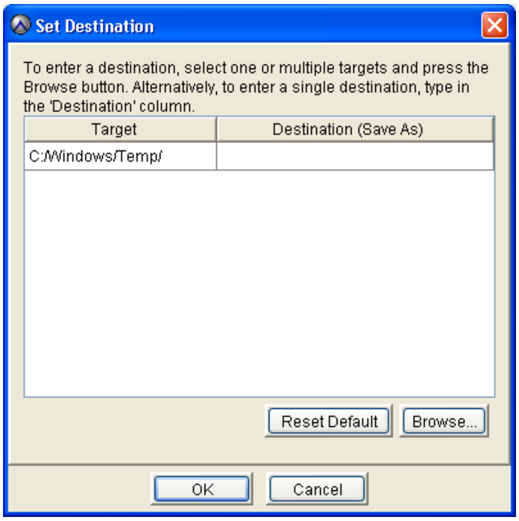
NOTICE

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.



Set Destination

To enter a destination, select one or multiple targets and press the Browse button. Alternatively, to enter a single destination, type in the 'Destination' column.

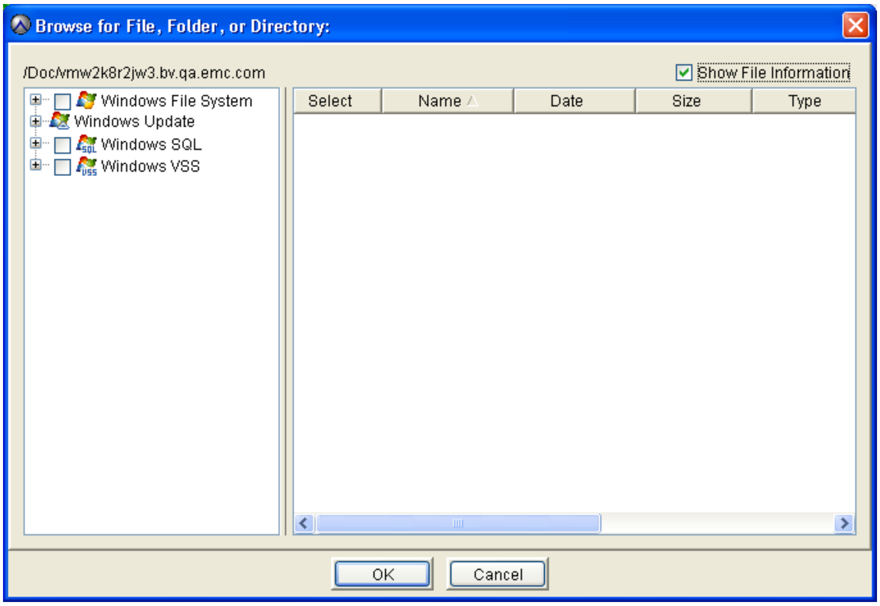
Target	Destination (Save As)
C:/Windows/Temp/	

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.

NOTICE

If a file with the same name already exists in the path to which you are restoring a file, then 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 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 103
- "Finding a backup to manage" on page 103
- "Changing a backup expiration date" on page 106
- "Changing backup retention types" on page 107
- "Validating a backup" on page 109
- "Viewing backup statistics" on page 110
- "Deleting a backup" on page 113

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 104
- "Finding a backup by date range" on page 105
- "Finding a backup by retention type" on page 106

NOTICE

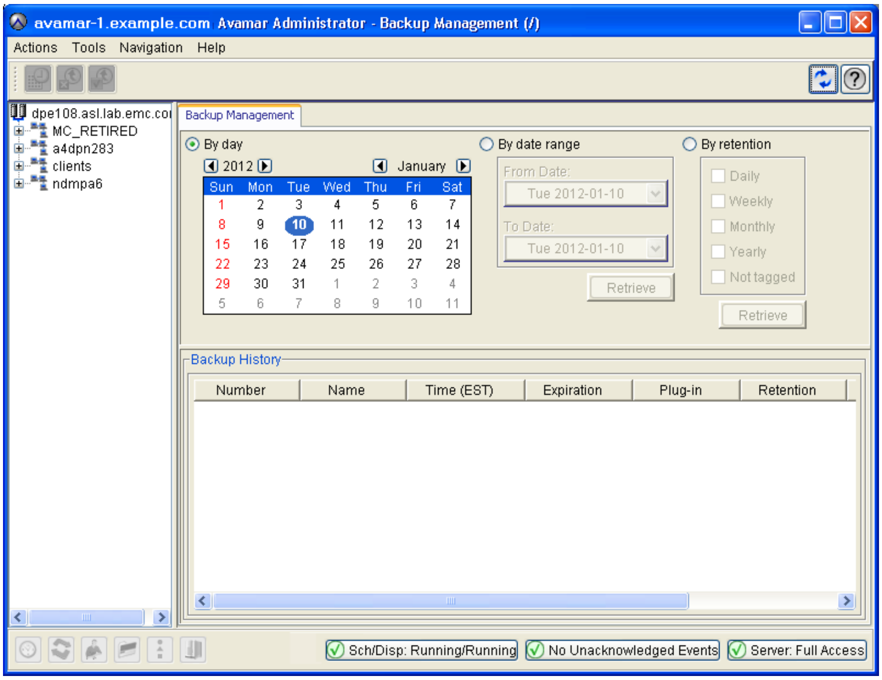
Avamar generally supports the use of specific supported international characters in directory, folder, and filenames. However, proper display of international language characters is contingent on the client computer Java locale and installed system fonts being compatible with the original language. If 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.

Finding a backup by calendar date

To find a backup on a specific calendar date:

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

   The Backup Management window appears.



● By day

2012 — January

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

○ By date range

From Date: Tue 2012-01-10

To Date: Tue 2012-01-10

○ By retention

□ Daily
□ Weekly
□ Monthly
□ Yearly
□ Not tagged

Number	Name	Time (EST)	Expiration	Plug-in	Retention

2. In the clients tree, browse to and select the client with the backups to manage.

3. On the **Backup Management** tab, select **By day**.

4. 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

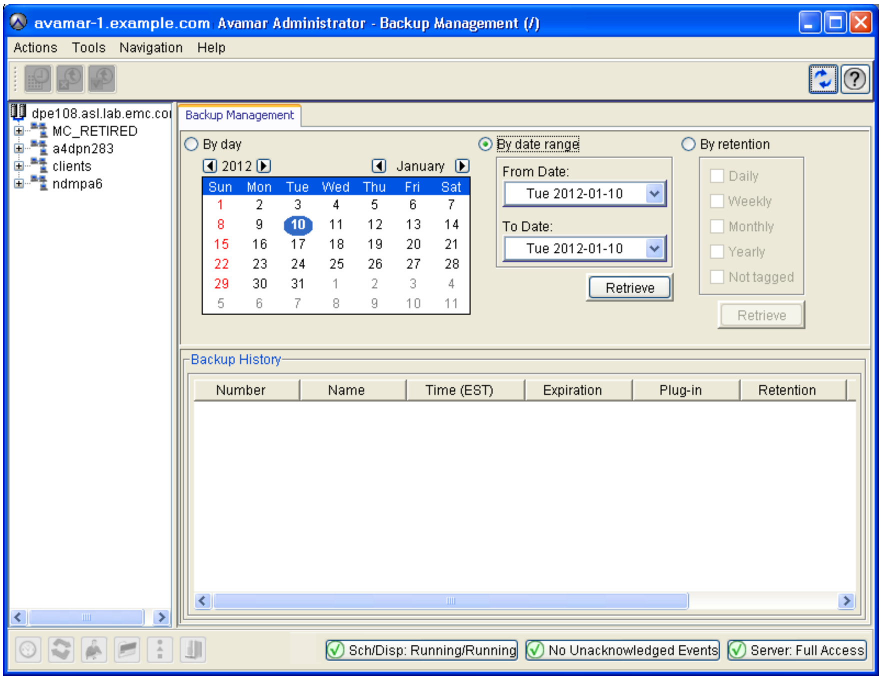
To find a backup within a range of dates:

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

   The Backup Management window appears.

2. In the clients tree, browse to and select the client with the backups to manage.

3. On the **Backup Management** tab, select **By date range**.



2012 January

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

From Date: Tue 2012-01-10

To Date: Tue 2012-01-10

Number	Name	Time (EST)	Expiration	Plug-in	Retention

4. Click the **From Date** list, and browse the calendar for the start date for the range.

5. Click the **To Date** list, and browse the calendar for the end date for the range.

6. Click **Retrieve**.

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

Finding a backup by retention type

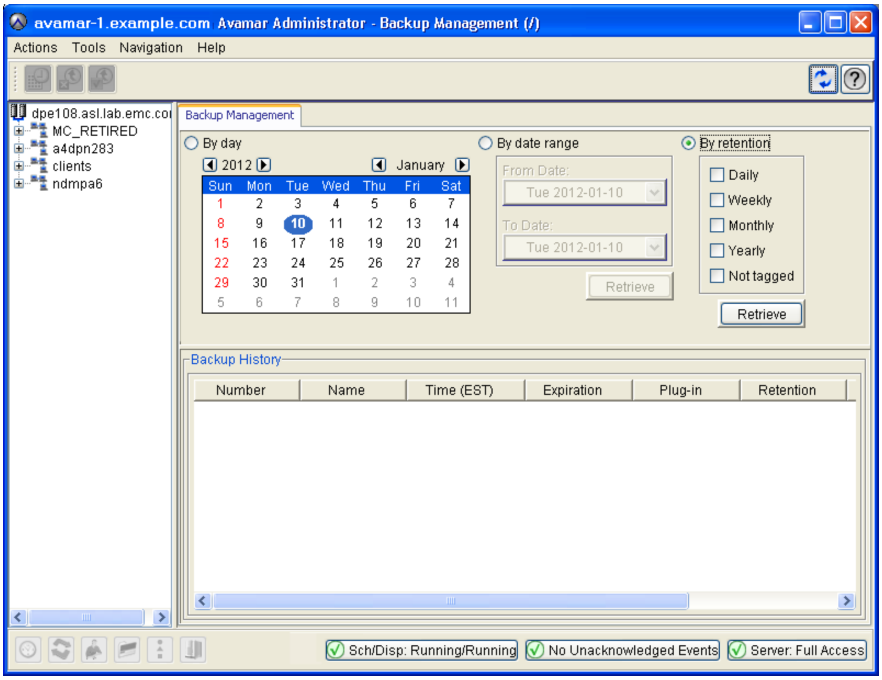
To find a backup with a certain retention type:

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

   The Backup Management window appears.

2. In the clients tree, browse to and select the client with the backups to manage.

3. On the **Backup Management** tab, select **By retention**.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Number	Name	Time (EST)	Expiration	Plug-in	Retention

4. Select the checkbox next to the retention type for the backup.

5. 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 Management** launcher button.

   The Backup Management window appears.

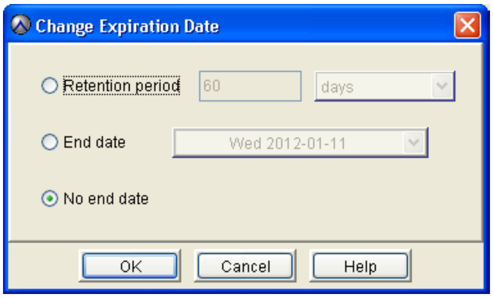
2. Find a backup to manage, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 104
   - "Finding a backup by date range" on page 105
   - "Finding a backup by retention type" on page 106.

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

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

The Change Expiration Date dialog box appears.



○ Retention period 60 days

○ End date Wed 2012-01-11

● No end date

5. 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**.

6. Click **OK**.

   A confirmation message appears.

7. Click **Yes**.

   An event code dialog box appears.

8. Click **OK**.

9. 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 Management** launcher button.

   The Backup Management window appears.

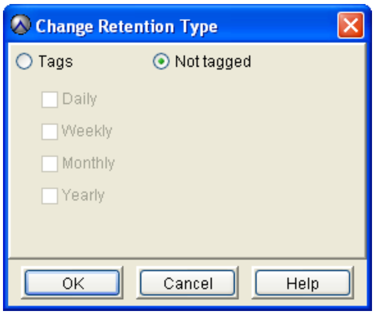
2. Find a backup to manage, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 104
   - "Finding a backup by date range" on page 105
   - "Finding a backup by retention type" on page 106.

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

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

   The Change Retention Type dialog box appears.



Change Retention Type

○ Tags ● Not tagged

□ Daily

□ Weekly

□ Monthly

□ Yearly

5. 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.

6. Click **OK**.

   A confirmation message appears.

7. Click **Yes**.

   A second confirmation message appears.

8. 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 filesystem.

To validate a backup:

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

   The Backup Management window appears.

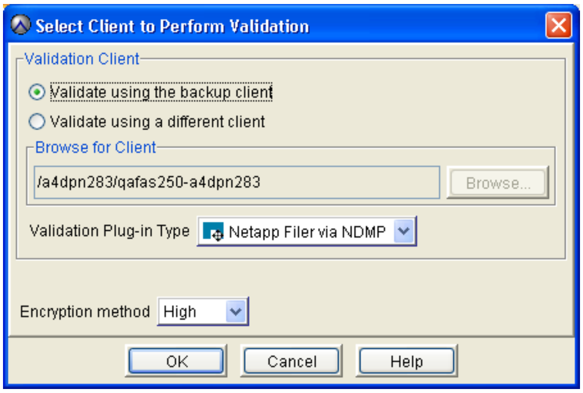
2. Find a backup to validate, as discussed in the following topics:

   - “Finding a backup by calendar date” on page 104
   - “Finding a backup by date range” on page 105
   - “Finding a backup by retention type” on page 106.

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.



Select Client to Perform Validation

Validation Client

● Validate using the backup client

○ Validate using a different client

Browse for Client

/a4dpn283/qafas250-a4dpn283

Validation Plug-in Type: Netapp Filer via NDMP

Encryption method: High

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.

   NOTICE

   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 Management** launcher button.

   The Backup Management window appears.

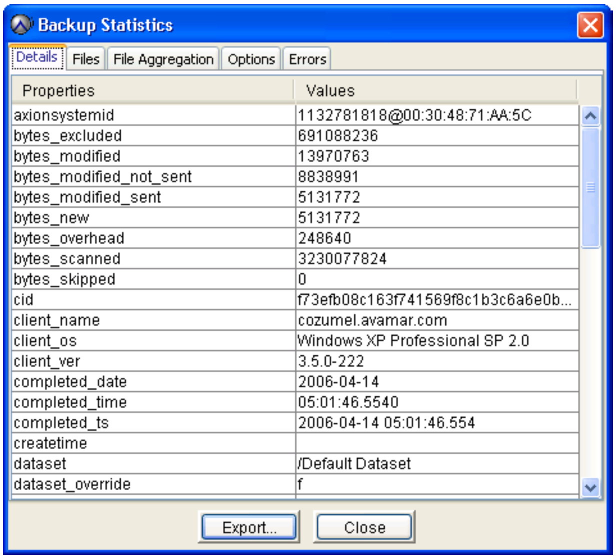
2. Find the backup, as discussed in the following topics:

   - "Finding a backup by calendar date" on page 104
   - "Finding a backup by date range" on page 105
   - "Finding a backup by retention type" on page 106.

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.



Properties	Values
axionsystemid	1132781818@00:30:48:71:AA:5C
bytes_excluded	691088236
bytes_modified	13970763
bytes_modified_not_sent	8838991
bytes_modified_sent	5131772
bytes_new	5131772
bytes_overhead	248640
bytes_scanned	3230077824
bytes_skipped	0
cid	f73efb08c163f741569f8c1b3c6a6e0b...
client_name	cozumel.avamar.com
client_os	Windows XP Professional SP 2.0
client_ver	3.5.0-222
completed_date	2006-04-14
completed_time	05:01:46.5540
completed_ts	2006-04-14 05:01:46.554
createtime	
dataset	/Default Dataset
dataset_override	f

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

Table 9 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 599.
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.

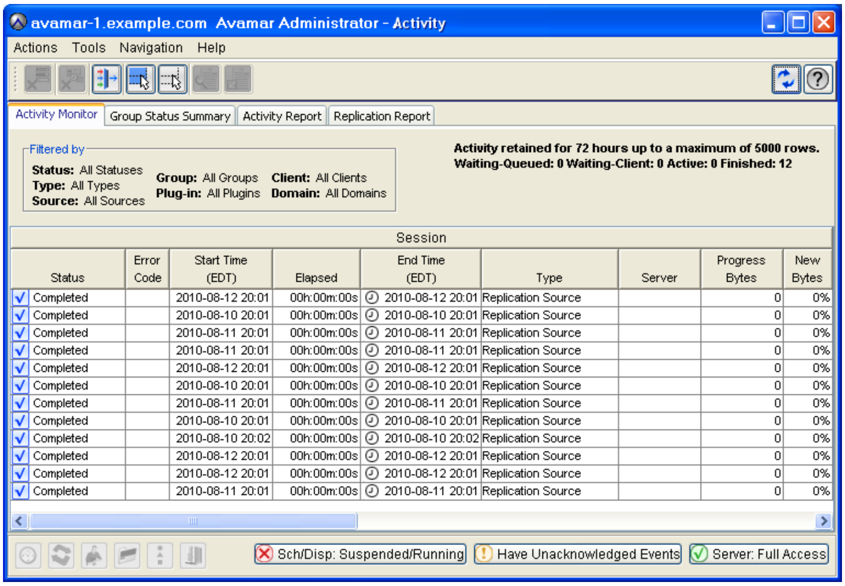
6. Click **Close**.

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.



Filtered by

Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

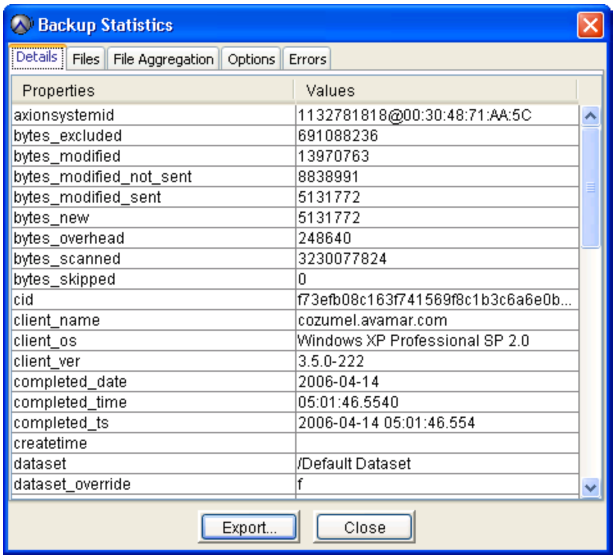
Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

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.



Properties	Values
axionsystemid	1132781818@00:30:48:71:AA:5C
bytes_excluded	691088236
bytes_modified	13970763
bytes_modified_not_sent	8838991
bytes_modified_sent	5131772
bytes_new	5131772
bytes_overhead	248640
bytes_scanned	3230077824
bytes_skipped	0
cid	f73efb08c163f741569f8c1b3c6a6e0b...
client_name	cozumel.avamar.com
client_os	Windows XP Professional SP 2.0
client_ver	3.5.0-222
completed_date	2006-04-14
completed_time	05:01:46.5540
completed_ts	2006-04-14 05:01:46.554
createtime	
dataset	/Default Dataset
dataset_override	f

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

Table 10 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 599.
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 Management** launcher button.

   The Backup Management window appears.

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

   - "Finding a backup by calendar date" on page 104
   - "Finding a backup by date range" on page 105
   - "Finding a backup by retention type" on page 106.

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

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

   A confirmation message appears.

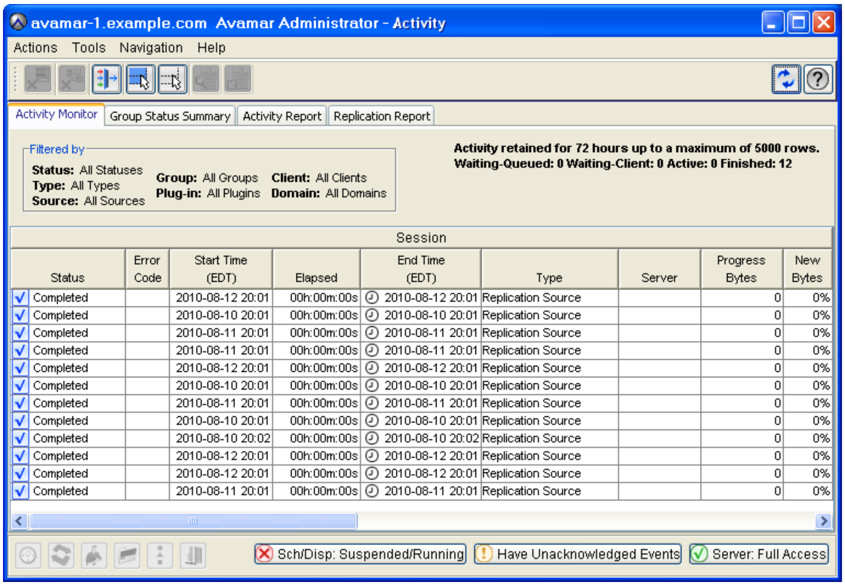
5. Click **OK**.

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.



Filtered by
Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

☒ Sch/Disp: Suspended/Running
! Have Unacknowledged Events
✓ Server: Full Access

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 11 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** — All client-initiated backups have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 249 provides details. • **Completed** — The activity successfully completed. • **Completed w/ Exception(s)** — The activity completed with minor errors or warnings. Double-click the entry to view the full error log, which contains the activity failure codes. • **Dropped Session** — The activity was successfully initiated, but because MCS could not detect any progress, the activity was forcefully canceled. • **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. • **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. • **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.

Table 11 Activity Monitor tab columns (page 2 of 4)

Column	Description
Status - continued	• **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** • **Plugin Disabled** — All operations have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 249 provides details. • **Restore Disabled** — All restore operations have been disabled for this plug-in. "Avamar Client Agent and Plug-in Management" on page 249 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 249 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 249 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.
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.

Table 11 Activity Monitor tab columns (page 3 of 4)

Column	Description
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.
Group	If the activity was a scheduled backup, this is the group that this client was a member of when this scheduled activity was initiated, since clients can be members of more than one group. On-demand is shown for all other activities.
Plug-in	Plug-in used for this activity.

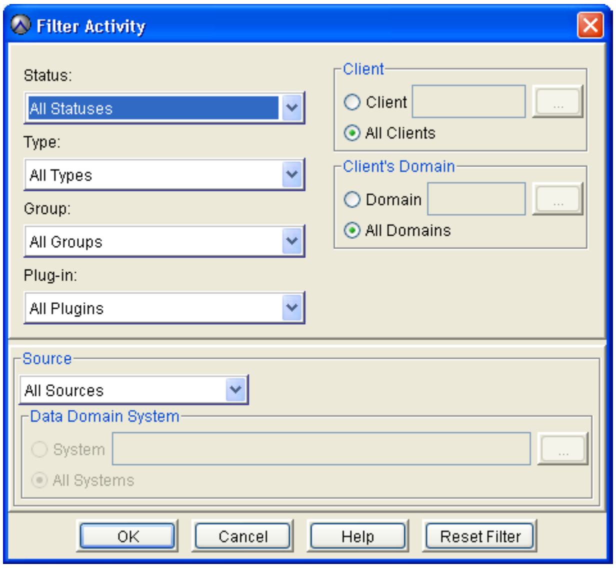
Table 11 Activity Monitor tab columns (page 4 of 4)

Column	Description
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 144 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.



Filter Activity

Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

Client

○ Client

● All Clients

Client's Domain

○ Domain

● All Domains

Source

All Sources

Data Domain System

○ System

● All Systems

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

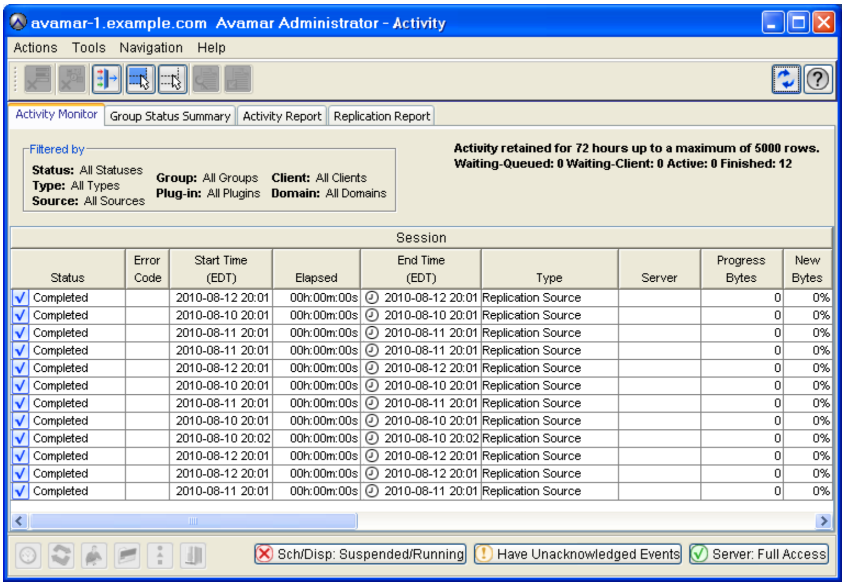
Canceling a backup, restore, or validation

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.



Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

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 120
◆ Schedules.. 129
◆ Retention policies 143

Datasets

When you perform an on-demand backup, the selection of directories and files in a client filesystem 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.

The following topics provide details on datasets:

- "Understanding datasets" on page 120
- "Dataset catalog" on page 121
- "Creating a dataset" on page 124
- "Editing a dataset" on page 127
- "Copying a dataset" on page 128
- "Deleting a dataset" on page 129

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 filesystem hierarchy, either the entire filesystem 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

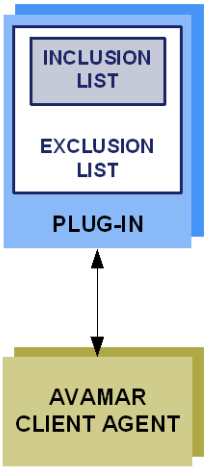
You cannot define inclusion and exclusion lists for VMware Image Backups.

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 152. 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" on page 168.

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 12 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 filesystem 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 13 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 filesystem 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 filesystem 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 14 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 152 and “vCenter groups” on page 153 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.

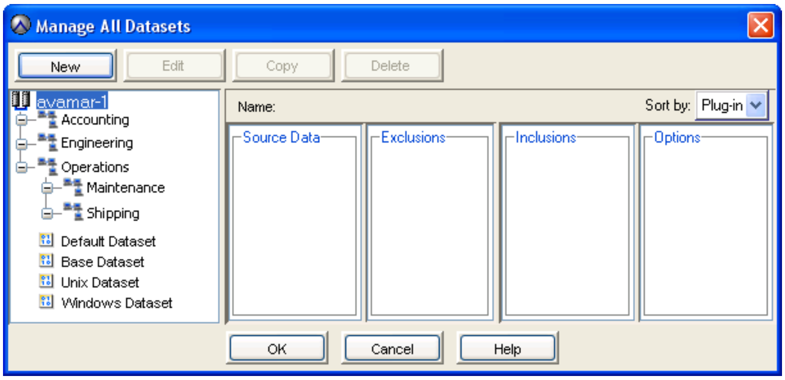
The *EMC Avamar for VMware User Guide* provides details on using the VMware Image Dataset to back up virtual machine data.

Creating a dataset

To create a dataset:

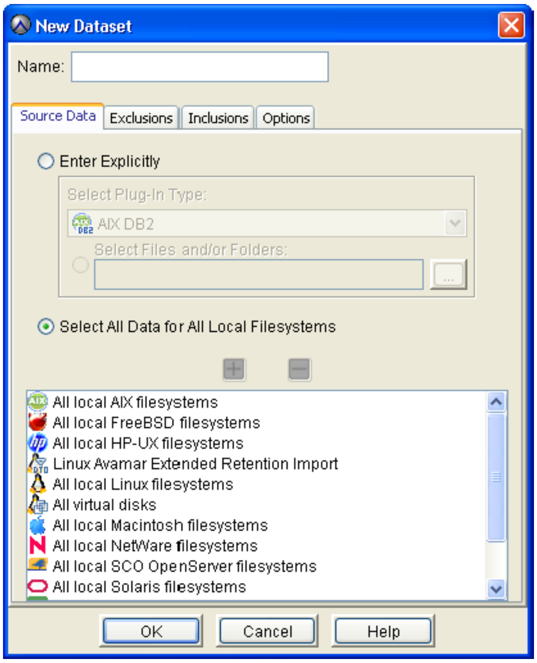
1. In Avamar Administrator, select **Tools › Manage Datasets**.

   The Manage All Datasets window appears.



2. Click **New**.

   The New Dataset dialog box appears.


New Dataset
Name:
Source Data
Exclusions
Inclusions
Options
○ Enter Explicitly
Select Plug-In Type:
AIX DB2
Select Files and/or Folders:
...
● Select All Data for All Local Filesystems
All local AIX filesystems
All local FreeBSD filesystems
All local HP-UX filesystems
Linux Avamar Extended Retention Import
All local Linux filesystems
All virtual disks
All local Macintosh filesystems
All local NetWare filesystems
All local SCO OpenServer filesystems
All local Solaris filesystems
OK
Cancel
Help

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 filesystems
   – All local FreeBSD filesystems
   – All local HP-UX filesystems
   – All local Linux filesystems
   – All local Macintosh filesystems
   – All local SCO OpenServer filesystems
   – All local Solaris filesystems
   – All local UnixWare filesystems
   – All local Windows filesystems

   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 filesystem 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 filesystems.

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 15 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 120 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.

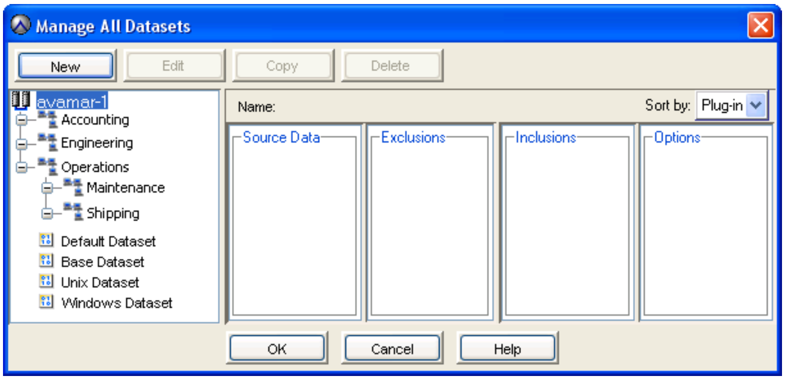
9. Click **OK**.

Editing a dataset

To edit a dataset:

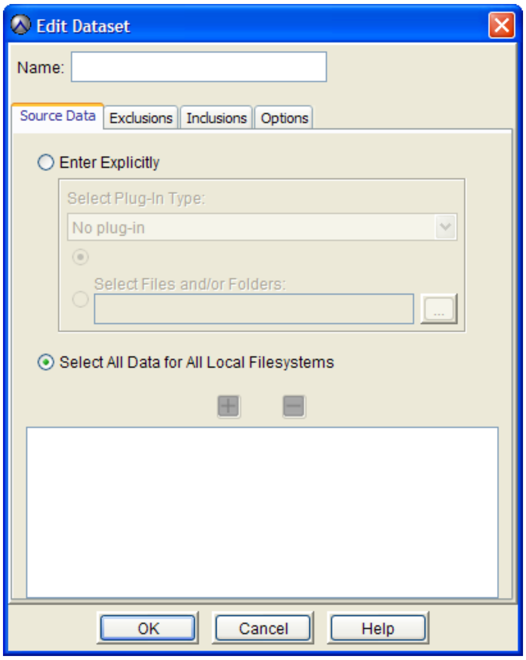
1. In Avamar Administrator, select **Tools › Manage Datasets**.

   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 124 provides details on dataset properties.

4. Click **OK**.

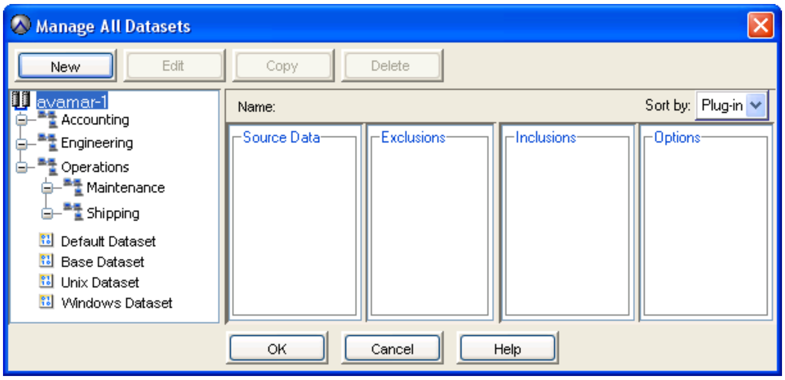
   Dataset changes take effect on the next scheduled backup. Backups that have already begun or have been completed are not affected.

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.

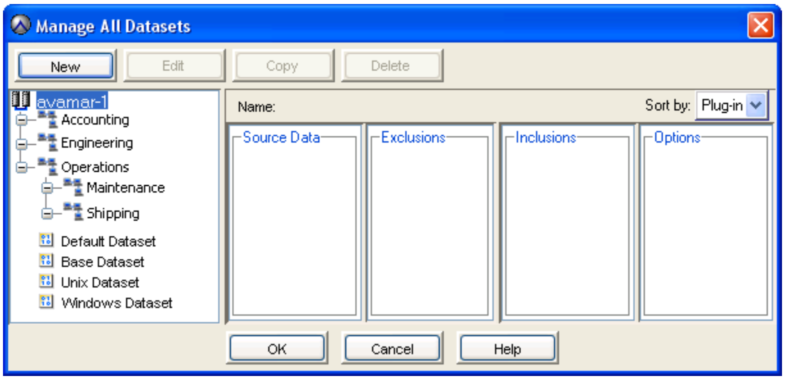
3. Type a name for the new dataset and click **OK**.

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
- Sending of custom event profile email notifications

The following topics provide details on schedules:

- "Understanding schedules" on page 130
- "Schedule catalog" on page 131
- "Creating a schedule" on page 132
- "Editing a schedule" on page 138
- "Copying a schedule" on page 140
- "Deleting a schedule" on page 140
- "Running a schedule now" on page 141
- "Editing the override schedule" on page 141

Understanding schedules

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

Table 16 Schedule types

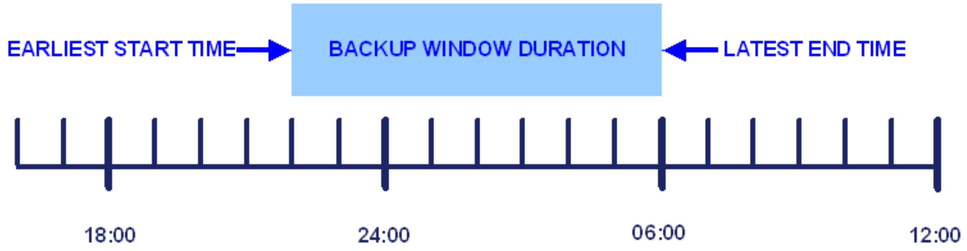
Schedule type	Description
Daily	Repeats a system activity every day at one or more times of the day. With daily schedules, you must also limit the duration of the activity to prevent job overlap.
Weekly	Repeats a system activity every week on one or more days of the week. With weekly schedules, you must 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. 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 17 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.
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 17 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

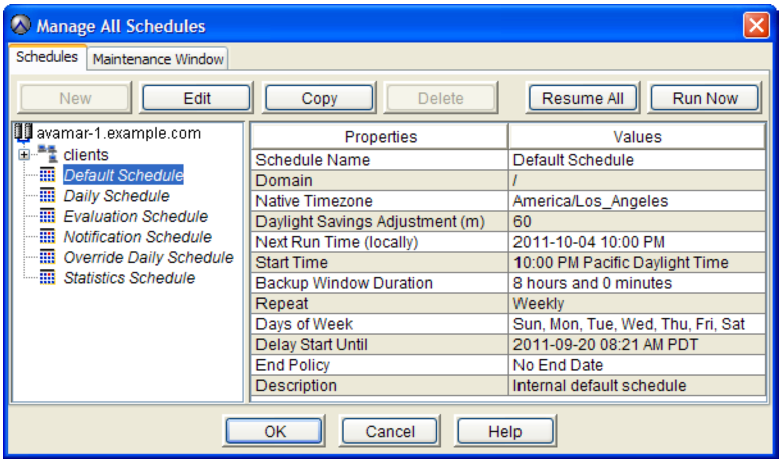
The steps to create a schedule depend on whether you are creating a daily, weekly, monthly, or on-demand schedule.

Creating a daily schedule

To create a daily schedule:

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

   The Manage All Schedules window appears.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

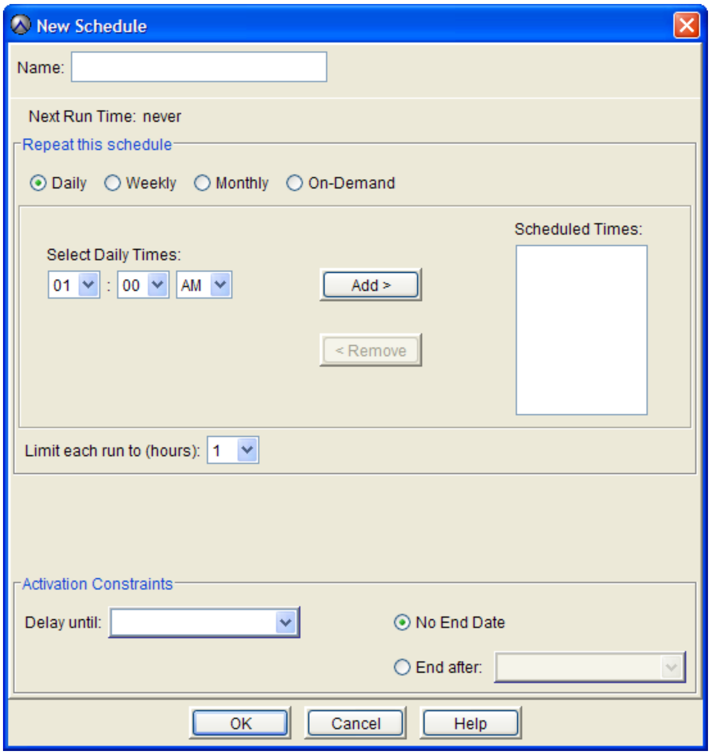
2. Click **New**.

   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**.



New Schedule

Name:

Next Run Time: never

Repeat this schedule

● Daily ○ Weekly ○ Monthly ○ On-Demand

Select Daily Times: 01 : 00 AM

Scheduled Times:

Limit each run to (hours): 1

Activation Constraints

Delay until:

● No End Date

○ End after:

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.

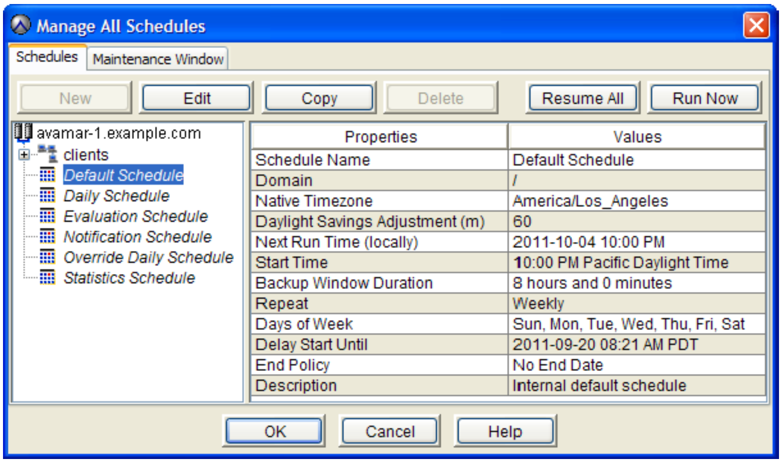
11. Click **OK**.

Creating a weekly schedule

To create a weekly schedule:

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

   The Manage All Schedules window appears.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

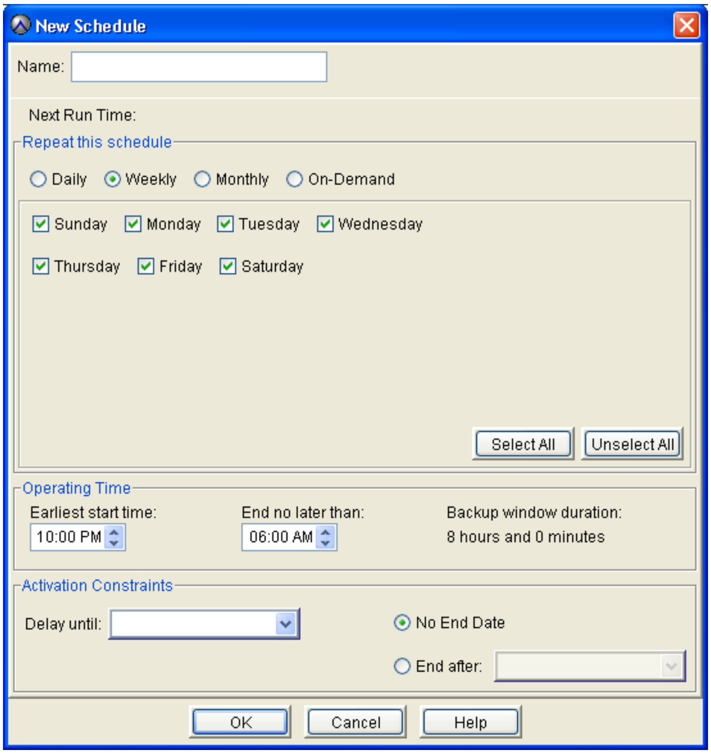
2. Click **New**.

   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**.



Name:

Next Run Time:

Repeat this schedule

○ Daily ● Weekly ○ Monthly ○ On-Demand

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

Operating Time

Earliest start time: 10:00 PM

End no later than: 06:00 AM

Backup window duration: 8 hours and 0 minutes

Activation Constraints

Delay until:

● No End Date

○ End after:

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.

   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.

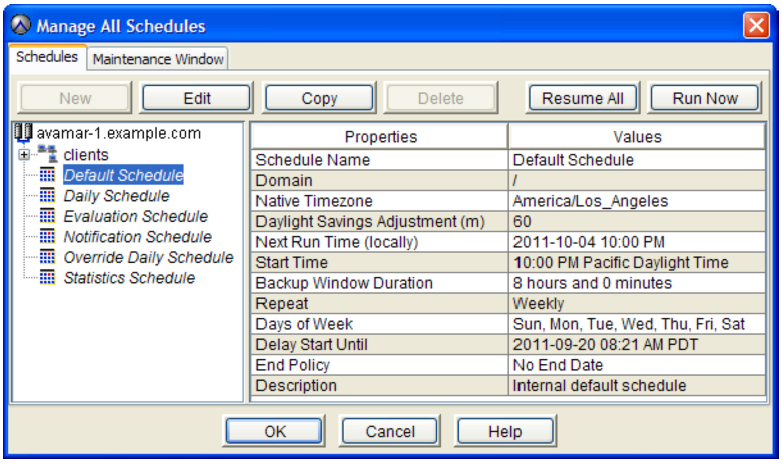
10. Click **OK**.

Creating a monthly schedule

To create a monthly schedule:

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

   The Manage All Schedules window appears.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

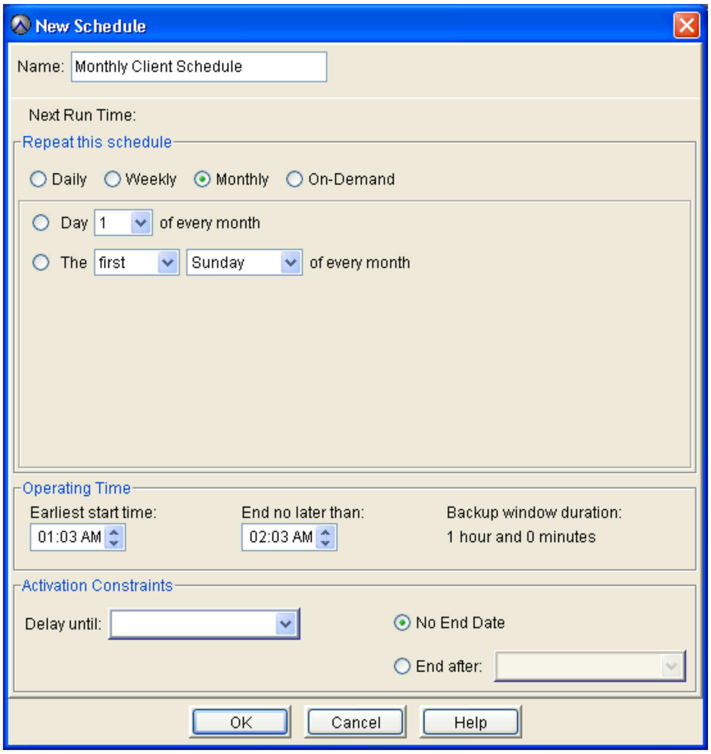
2. Click **New**.

   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.**



New Schedule

Name: Monthly Client Schedule

Next Run Time:

Repeat this schedule

○ Daily ○ Weekly ● Monthly ○ On-Demand

○ Day 1 of every month

○ The first Sunday of every month

Operating Time

Earliest start time: 01:03 AM

End no later than: 02:03 AM

Backup window duration: 1 hour and 0 minutes

Activation Constraints

Delay until:

● No End Date

○ End after:

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

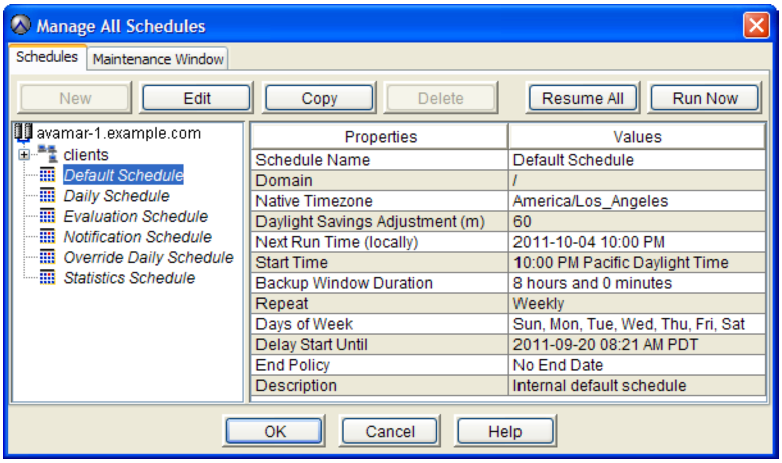
An on-demand schedule is useful in the following scenarios:

- 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.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

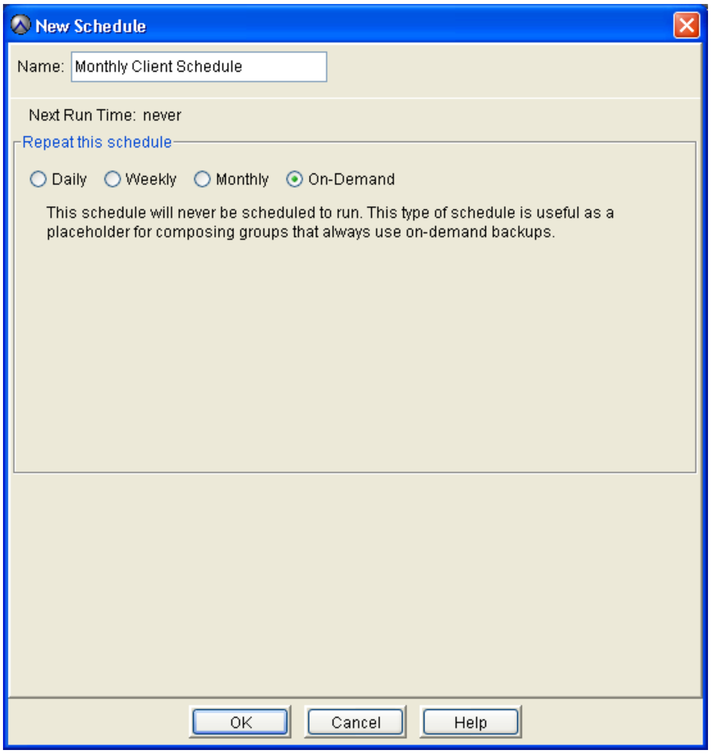
2. Click **New**.

   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**.



Name: Monthly Client Schedule

Next Run Time: never

Repeat this schedule

○ Daily ○ Weekly ○ Monthly ● On-Demand

This schedule will never be scheduled to run. This type of schedule is useful as a placeholder for composing groups that always use on-demand backups.

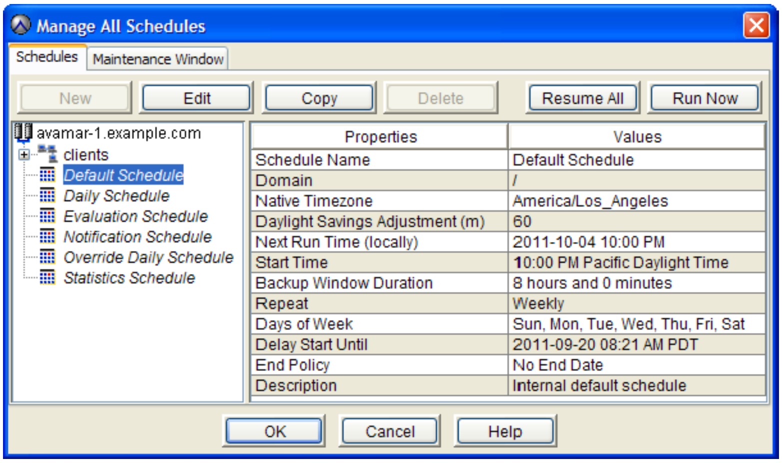
5. Click **OK**.

Editing a schedule

To edit a schedule:

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

   The Manage All Schedules window appears.

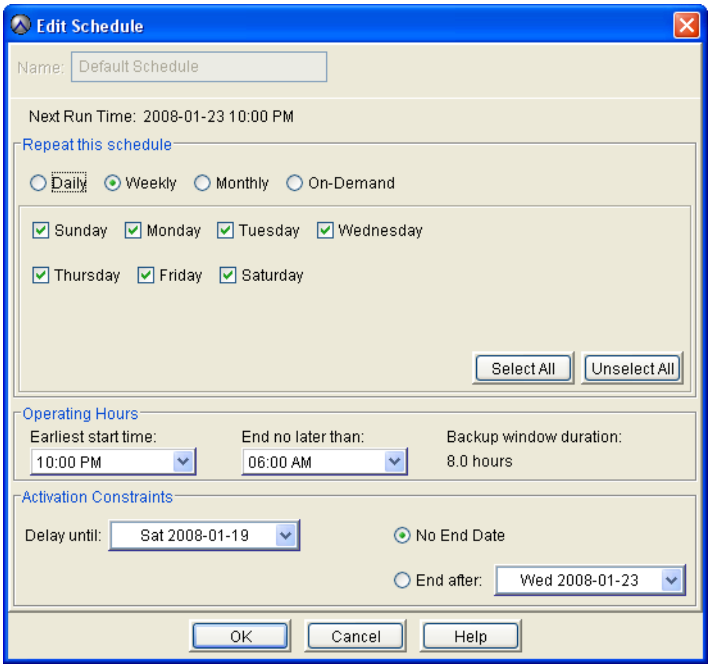


avamar-1.example.com
- clients
- Default Schedule
- Daily Schedule
- Evaluation Schedule
- Notification Schedule
- Override Daily Schedule
- Statistics Schedule

Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

2. Select a schedule from the list and click **Edit**.

The Edit Schedule dialog box appears.



Edit Schedule

Name: Default Schedule

Next Run Time: 2008-01-23 10:00 PM

Repeat this schedule

○ Daily ● Weekly ○ Monthly ○ On-Demand

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

Operating Hours

Earliest start time: 10:00 PM

End no later than: 06:00 AM

Backup window duration: 8.0 hours

Activation Constraints

Delay until: Sat 2008-01-19

● No End Date

○ End after: Wed 2008-01-23

3. Edit the schedule information.

   Details on schedule properties are available in the following topics:

   - “Creating a daily schedule” on page 132
   - “Creating a weekly schedule” on page 134
   - “Creating a monthly schedule” on page 135
   - “Creating an on-demand schedule” on page 137

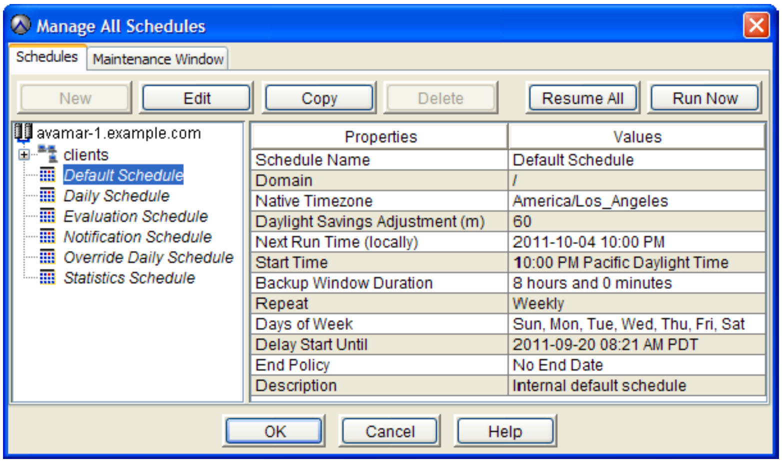
4. Click **OK**.

Copying a schedule

To copy a schedule:

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

   The Manage All Schedules window appears.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

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.**

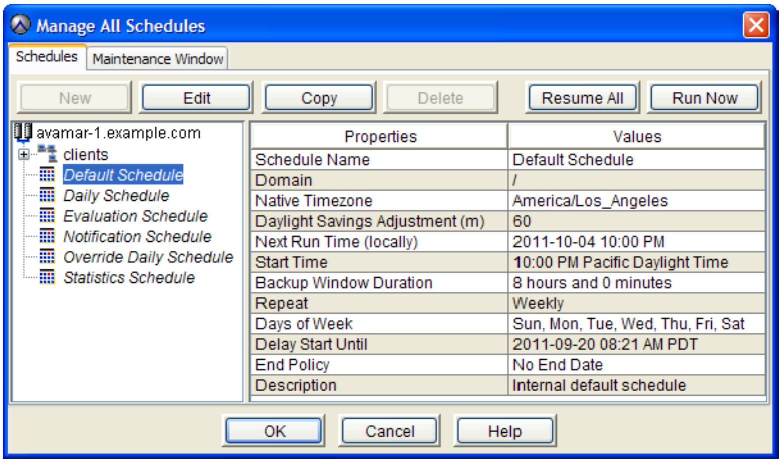
Deleting a schedule

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.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

3. Select the schedule from the list and click **Delete**.

   A confirmation message appears.

4. Click **Yes**.

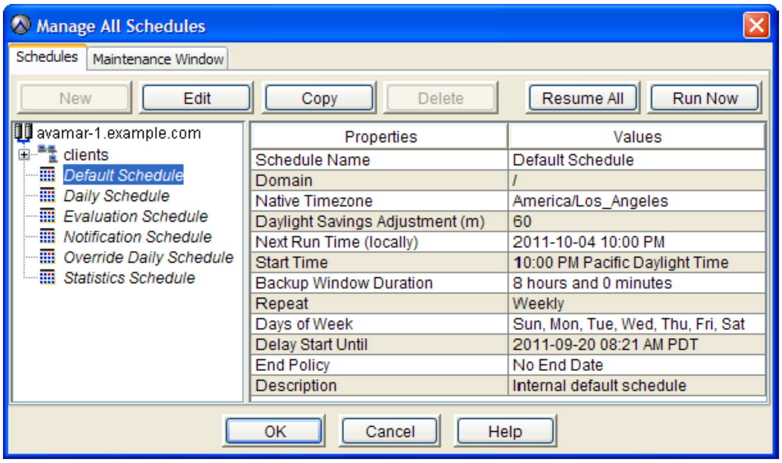
Running a schedule now

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.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

2. Select a schedule from the list and click **Run Now**.

Editing the override schedule

Use the override schedule to configure the start times that are available when you enable Override group schedules, as described in “Allowing users to select an alternative backup start time” on page 173. This schedule supplies the start times that users see and can select from when Override group schedules is enabled for their client.

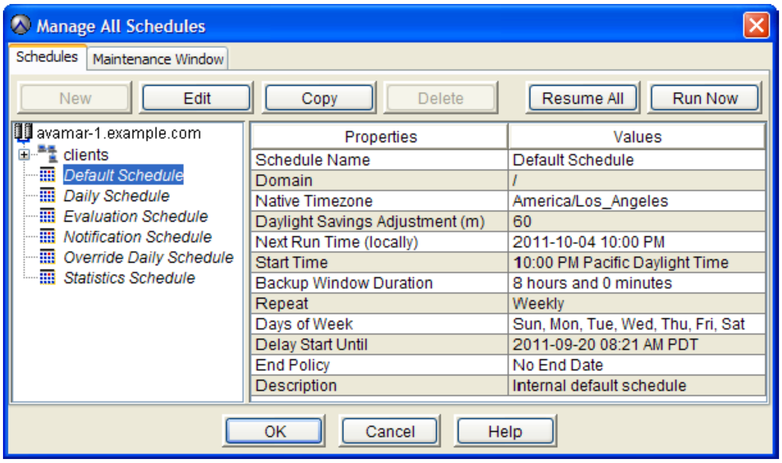
Users must have access to the web UI to view and select from the available start times. Access to the web UI is part of the enhanced features for enterprise desktop and laptop computers.

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.

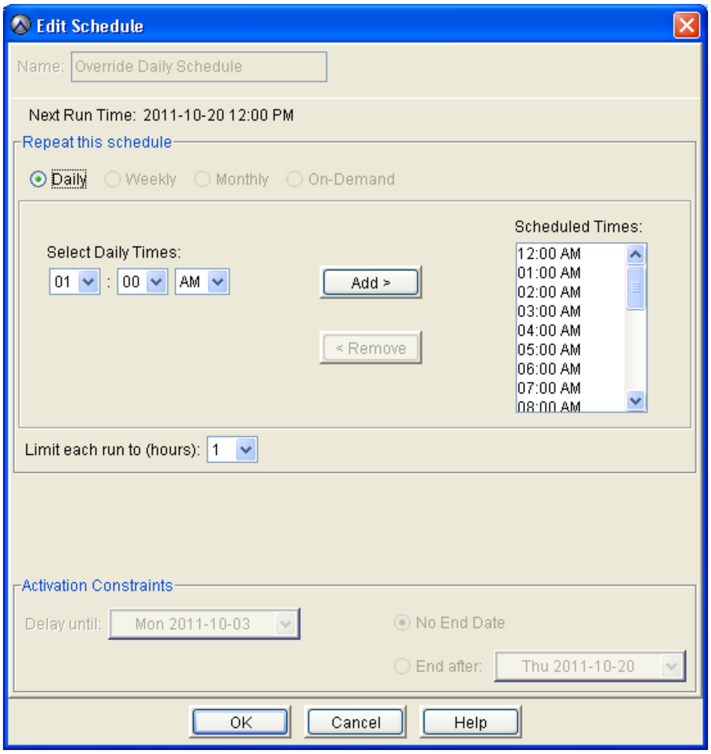


avamar-1.example.com
- clients
- Default Schedule
- Daily Schedule
- Evaluation Schedule
- Notification Schedule
- Override Daily Schedule
- Statistics Schedule

Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

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).



Name: Override Daily Schedule

Next Run Time: 2011-10-20 12:00 PM

● Daily ○ Weekly ○ Monthly ○ On-Demand

Select Daily Times: 01 : 00 AM

Scheduled Times:
12:00 AM
01:00 AM
02:00 AM
03:00 AM
04:00 AM
05:00 AM
06:00 AM
07:00 AM
08:00 AM

Limit each run to (hours): 1

Delay until: Mon 2011-10-03

● No End Date

○ End after: Thu 2011-10-20

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 106. 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 18 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 149 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.

"Setting last backup retention" on page 385 describes how to enable last backup retention.

Retention policy catalog

The retention policies in the following table are available by default.

Table 19 Types of retention policies

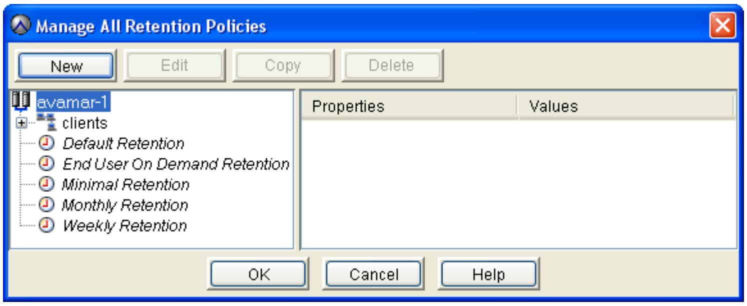
Retention policy type	Description
Minimal Retention	Controls the minimal retention feature, which is discussed in "Minimal retention" on page 144.
Default Retention	Defines backup retention settings for the Default Group. By default, the Default Retention policy assigns a retention period of 60 days 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:

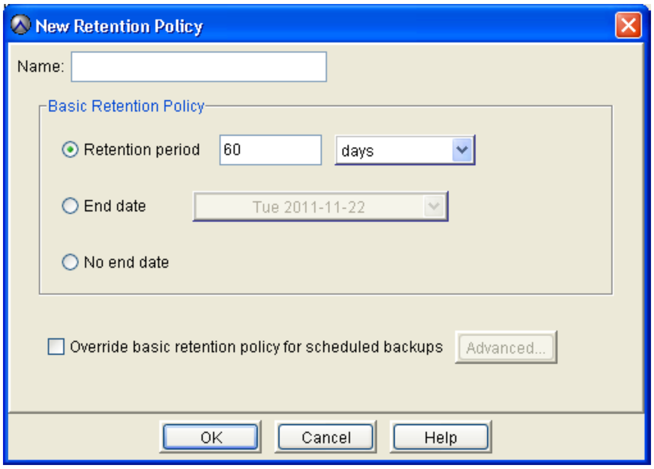
1. In Avamar Administrator, select **Tools › Manage Retention Policies**.

   The Manage All Retention Policies window appears.



2. Click **New**.

   The New Retention Policy dialog box appears.



Name:

● Retention period 60 days

○ End date Tue 2011-11-22

○ No end date

□ Override basic retention policy for scheduled backups

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**.

NOTICE

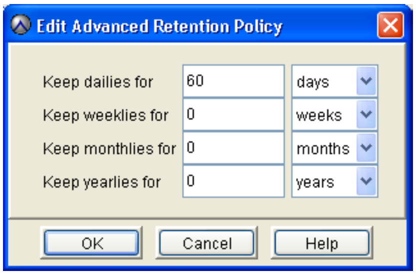
Best practices are to specify a retention that is greater than or equal to 14 days. When you create a retention policy for less than 14 days, an alert appears.

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.



Keep dailies for 60 days

Keep weeklies for 0 weeks

Keep monthlies for 0 months

Keep yearlies for 0 years

   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.

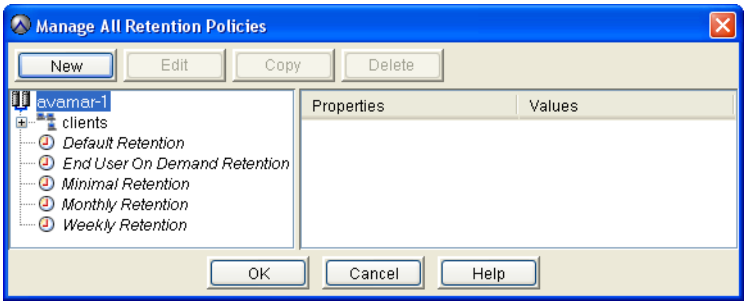
6. On the **New Retention Policy** dialog box, click **OK.**

Editing a retention policy

To edit a retention policy:

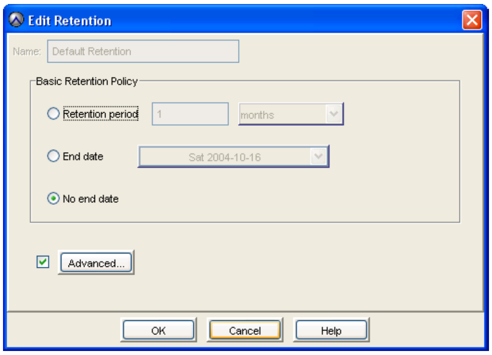
1. In Avamar Administrator, select **Tools › Manage Retention Policies.**

   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.



Name: Default Retention

Basic Retention Policy

○ Retention period 1 months

○ End date Sat 2004-10-16

● No end date

☑ Advanced...

3. Edit the retention policy information.

   "Creating a retention policy" on page 146 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.

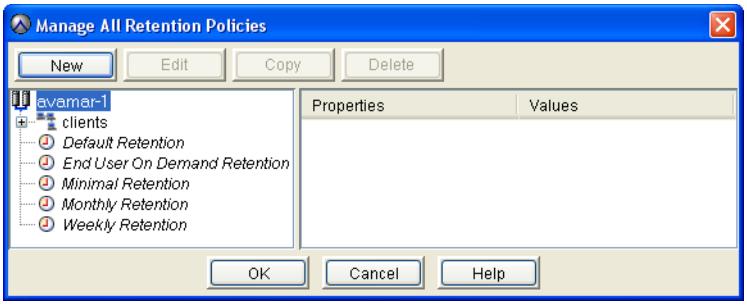
4. Click **OK**.

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**.

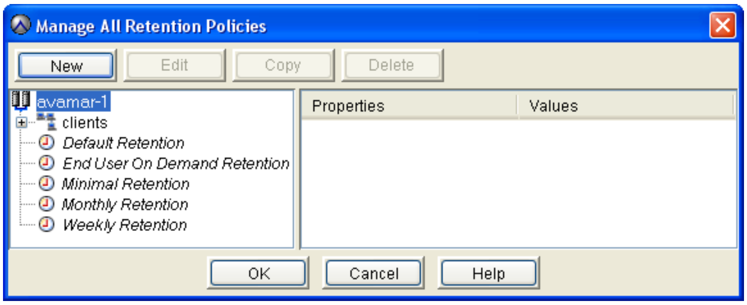
Deleting a retention policy

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.

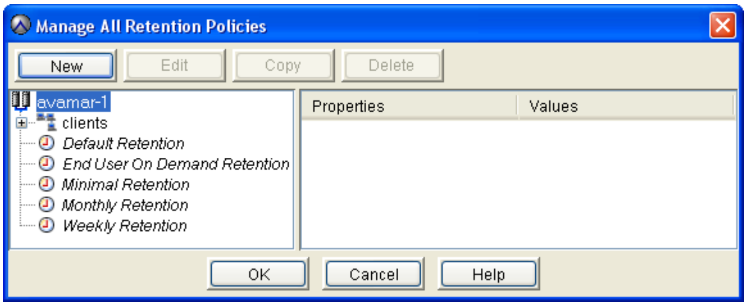
4. Click **Yes**.

Enabling the Minimal Retention policy

To enable the Minimal Retention policy:

1. In Avamar Administrator, select **Tools › Manage Retention Policies**.

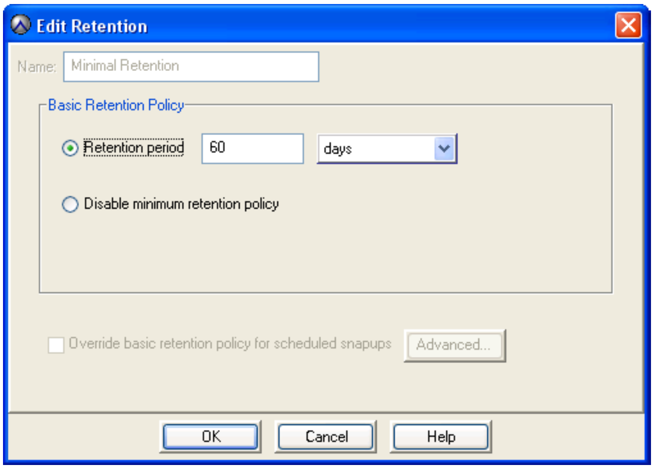
   The Manage All Retention Policies window appears.



2. Select the **Minimal Retention** policy and click **Edit.**

   The Edit Retention Policy dialog box appears.

3. Select **Retention period**.


Name: Minimal Retention

● Retention period 60 days

Edit Retention
Basic Retention Policy
○ Disable minimum retention policy
□ Override basic retention policy for scheduled snapups
Advanced...
OK
Cancel
Help

4. Specify the number of days, weeks, months, or years to ensure that backups are retained.

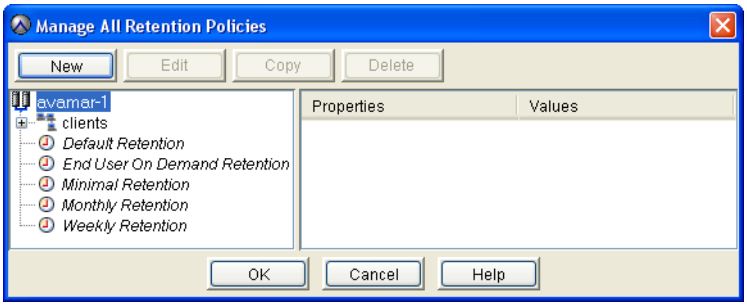
5. Click **OK**.

Disabling the Minimal Retention policy

To disable the Minimal Retention policy:

1. In Avamar Administrator, select **Tools › Manage Retention Policies**.

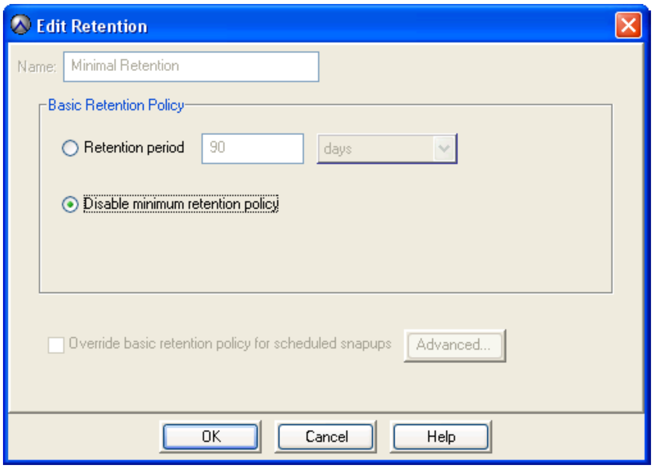
   The Manage All Retention Policies window appears.



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**.


Edit Retention

Name: Minimal Retention

Basic Retention Policy

○ Retention period 90 days

● Disable minimum retention policy

□ Override basic retention policy for scheduled snapups

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 152
- Policy window overview 153
- Creating a group........ 156
- Editing group properties........ 160
- Copying a group 162
- Enabling and disabling a group 162
- Deleting a group 163
- Viewing the Group Summary Reports 164
- Viewing the Group Status Summary 165
- Managing group membership 166
- Overriding group policy settings........ 168
- Initiating on-demand group backups........ 181

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 120
- "Schedules" on page 129
- "Retention policies" on page 143

These three objects comprise the "group policy." Group policy controls backup behavior for all members of the group unless you override these settings at the client level.

Default Group

Every client in the Avamar server is a member of at least one group. If you do not create any groups created, new clients are automatically 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.

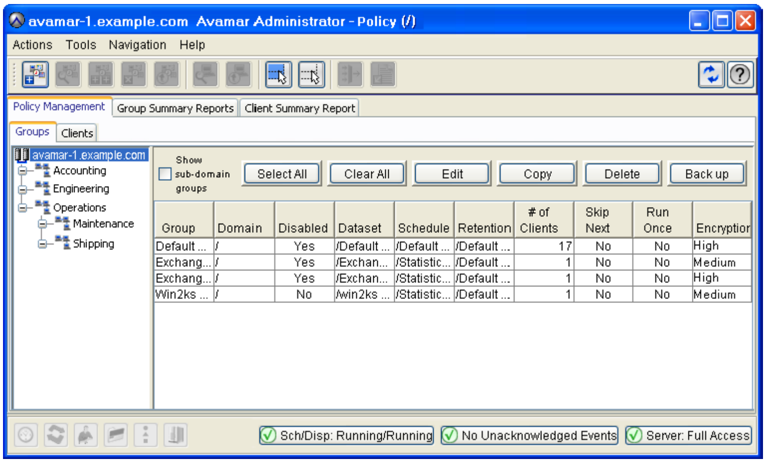
Inheritance and client overrides

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 to a client” on page 168 and “Assigning a different retention policy to a client” on page 169 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.



Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryptior
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	High
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Medium
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	High
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	Medium

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 20 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.

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 21 Buttons on the Policy window's Clients tab

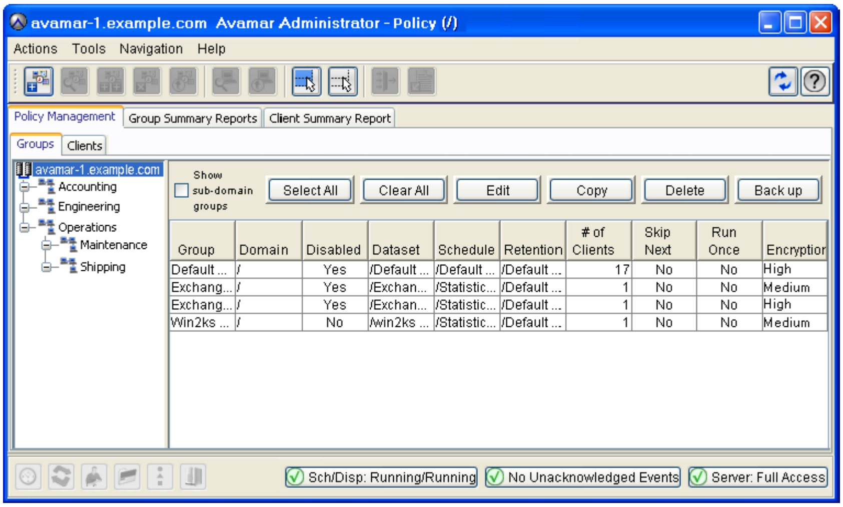
Button	Description
Select all	Click Select All to select all clients for edit.
Clear all	Click Clear All to clear the selection of all clients.
Details	Select a client and click Details to display the Client Details dialog box, which shows the properties of the client. You cannot view details for more than one client at a time. "Viewing client properties" on page 60 provides details on specific client properties.
Edit	Select one client and click Edit to display the Edit Client dialog box, which enables you to override various group policy settings on a client-by-client basis. Select multiple clients and click Edit to display the Edit Multiple Clients dialog box, which enables you to override various group policy settings for the selected group of clients. Use the Edit Client dialog box and the Edit Multiple Clients dialog box to override the following group policy settings: • Enable or disable all scheduled backups • Activate or deactivate a client • Allow or disallow client-initiated backups • Change the backup window overtime behavior • Change the encryption method • Allow or prevent users from making additions to source data
Back up	Select a client and click Back up to initiate an on-demand backup of that client.

Creating a group

To create a group:

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

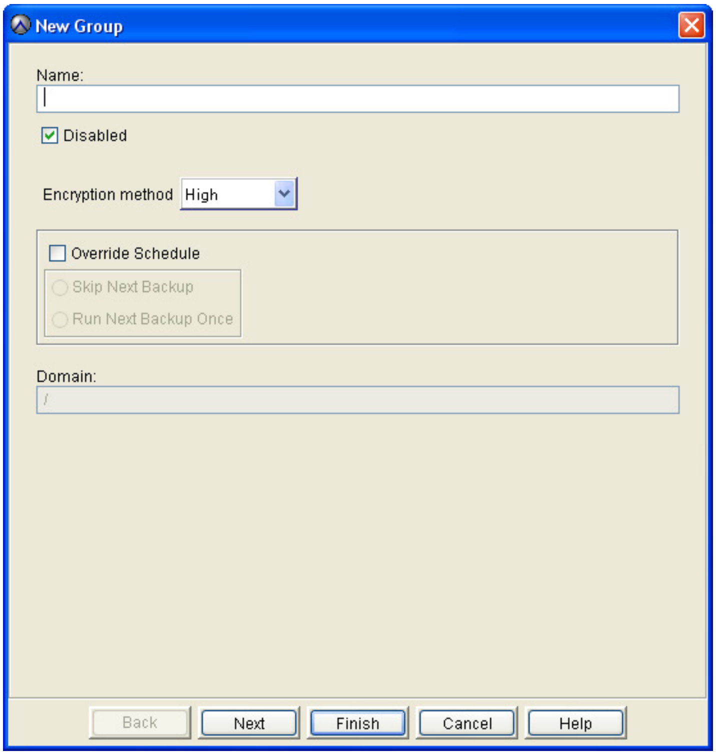
   The Policy window appears.



Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryption
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	High
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Medium
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	High
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	Medium

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.



Name:

☑ Disabled

Encryption method: High

□ Override Schedule

○ Skip Next Backup

○ Run Next Backup Once

Domain: /

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. From the **Encryption Method** list, select the encryption method used 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. Choose whether to use the assigned schedule for the group or override the assigned schedule:

   - To use the assigned schedule, leave the **Override Schedule** checkbox clear.
   - To override the schedule:

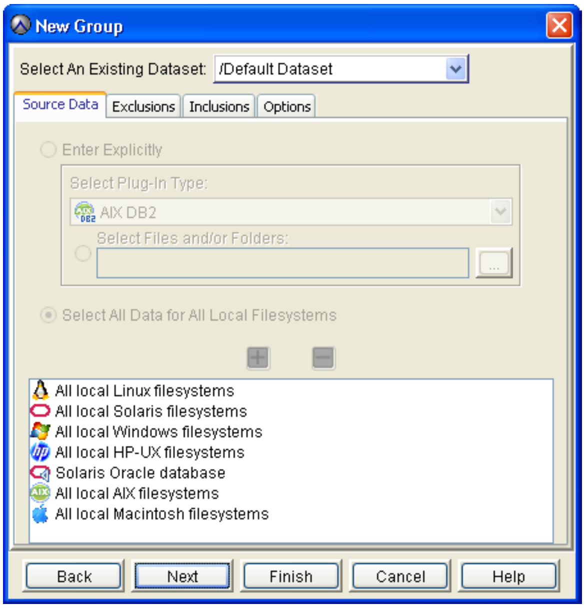
     a. Select **Override Schedule**.

        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.



New Group

Select An Existing Dataset: /Default Dataset

○ Enter Explicitly

Select Plug-In Type: AIX DB2

○ Select Files and/or Folders:

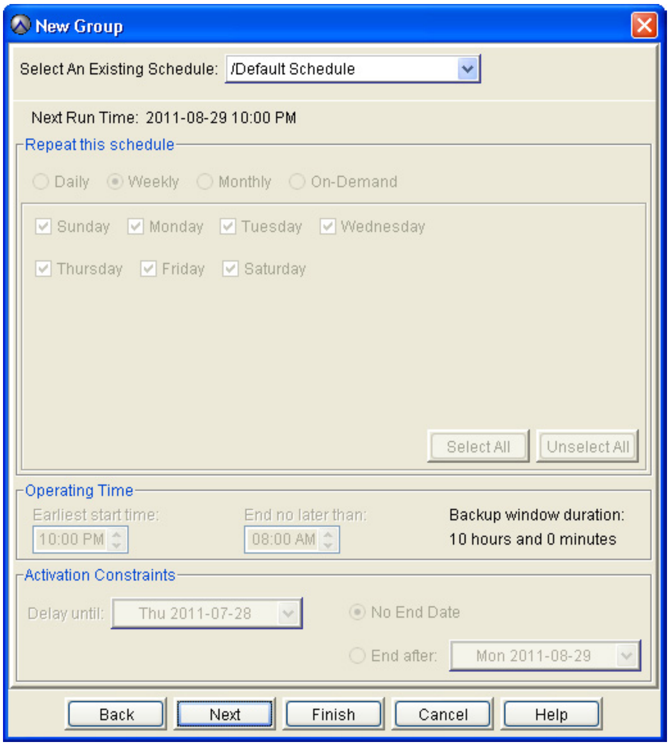
● Select All Data for All Local Filesystems

All local Linux filesystems
All local Solaris filesystems
All local Windows filesystems
All local HP-UX filesystems
Solaris Oracle database
All local AIX filesystems
All local Macintosh filesystems

10. From the **Select An Existing Dataset** list, select the dataset for the group.

11. Click **Next**.

    The next New Group wizard screen appears with schedule information.



New Group

Select An Existing Schedule: /Default Schedule

Next Run Time: 2011-08-29 10:00 PM

Repeat this schedule

○ Daily ● Weekly ○ Monthly ○ On-Demand

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

Operating Time

Earliest start time: 10:00 PM

End no later than: 08:00 AM

Backup window duration: 10 hours and 0 minutes

Activation Constraints

Delay until: Thu 2011-07-28

● No End Date

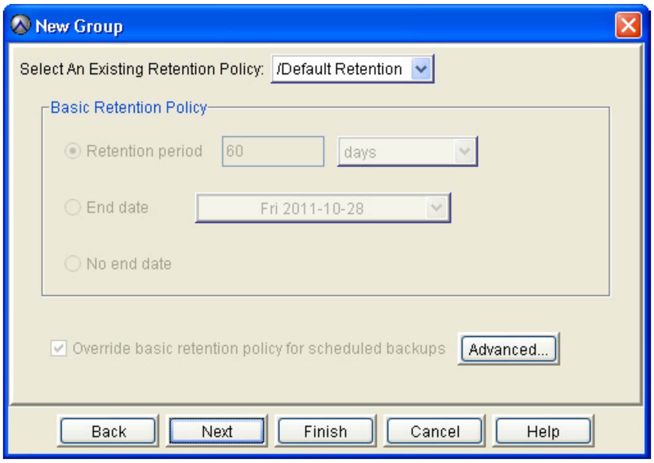
○ End after: Mon 2011-08-29

12. From the **Select An Existing Schedule** list, select a schedule for the group.

    You cannot edit schedules from this screen. Detailed schedule properties are shown so that you can review them prior to making a selection. The *EMC Avamar Administration Guide* provides additional information about editing schedule properties.

13. Click **Next**.

    The next New Group wizard screen appears with retention policy information.



New Group

Select An Existing Retention Policy: /Default Retention

Basic Retention Policy

● Retention period 60 days

○ End date Fri 2011-10-28

○ No end date

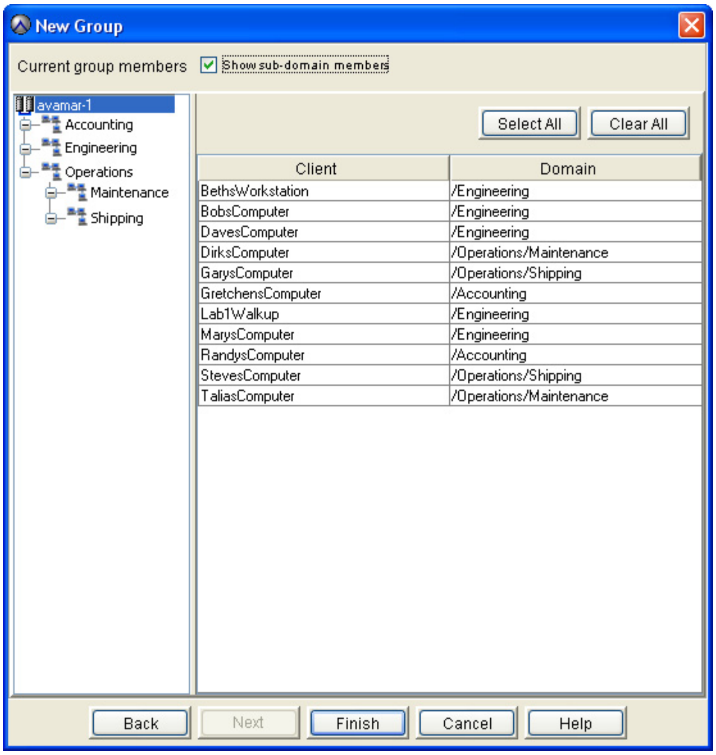
☑ Override basic retention policy for scheduled backups

14. From the **Select An Existing Retention Policy** list, select a retention policy for the group.

    You cannot edit retention policies from this screen. Detailed retention policy properties are shown so that you can review them prior to making a selection. The *EMC Avamar Administration Guide* provides additional information about editing retention policy properties.

15. Click **Next**.

    The final New Group wizard screen appears with a tree of domains and clients.



Current group members ☑ Show sub-domain members

Client	Domain
BethsWorkstation	/Engineering
BobsComputer	/Engineering
DavesComputer	/Engineering
DirksComputer	/Operations/Maintenance
GarysComputer	/Operations/Shipping
GretchensComputer	/Accounting
Lab1Walkup	/Engineering
MarysComputer	/Engineering
RandysComputer	/Accounting
StevesComputer	/Operations/Shipping
TaliasComputer	/Operations/Maintenance

16. Select one or more clients for the group. To select or clear the selection of all clients, click **Select All** or **Clear All**.

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

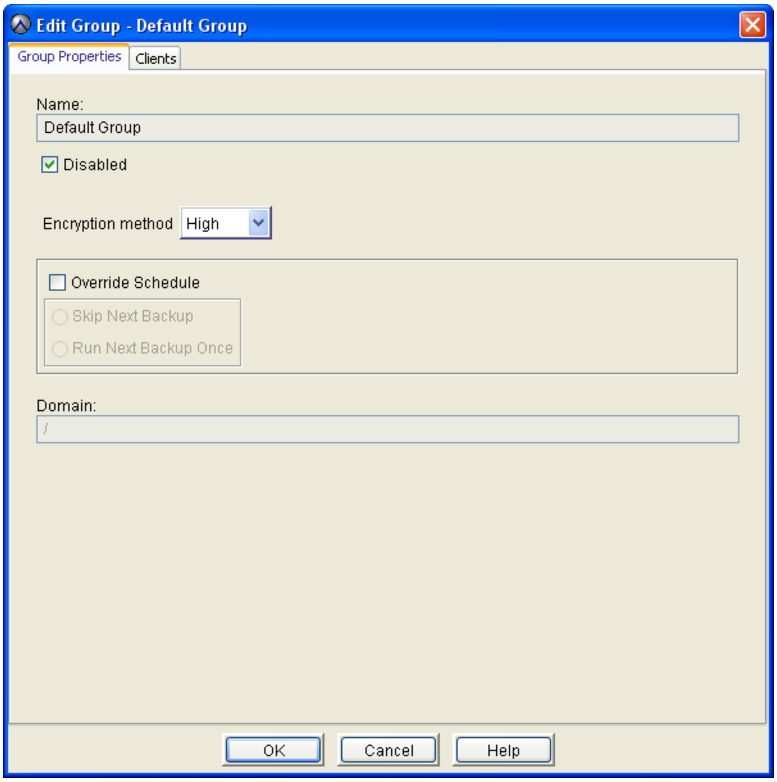
To edit a single group:

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. Open the **Actions** menu and select **Group › Edit Group**.

   The Edit Group dialog box appears.



Name:
Default Group

☑ Disabled

Encryption method High

□ Override Schedule
○ Skip Next Backup
○ Run Next Backup Once

Domain:
/

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

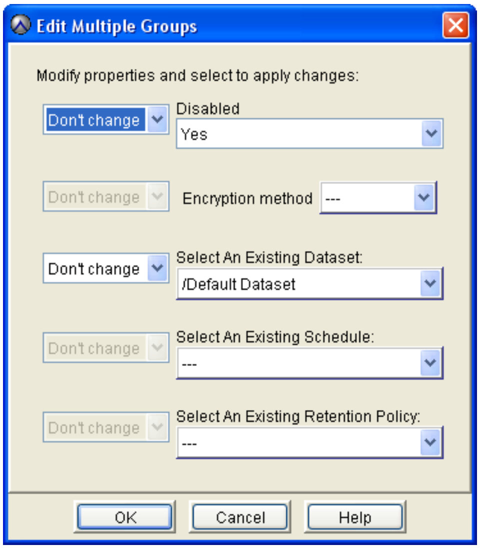
To edit multiple groups:

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. Open the **Actions** menu and select **Group › Edit Group**.

   The Edit Multiple Groups dialog box appears.



Edit Multiple Groups

Modify properties and select to apply changes:

Don't change — Disabled: Yes

Don't change — Encryption method: ---

Don't change — Select An Existing Dataset: /Default Dataset

Don't change — Select An Existing Schedule: ---

Don't change — Select An Existing Retention Policy: ---

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. Open the **Actions** menu and select **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. Right-click the group to disable, and then select **Disable Group**.

   When the group is disabled, a checkmark appears next to the option on the right-click menu. When the group is enabled, the checkmark next to the option on the right-click menu is cleared.

   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 59 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. Open the **Actions** menu and select **Group** › **Delete Group**.

   A confirmation message appears.

6. Click **Yes**.

   A second confirmation message appears.

7. Click **OK**.

Viewing the Group Summary Reports

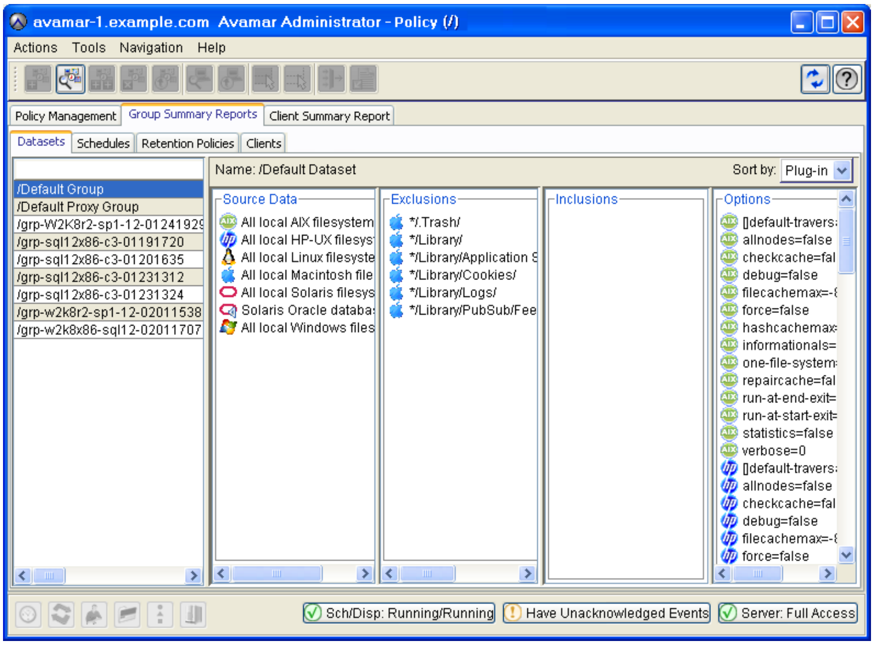
The Group Summary Reports are a combined “at a glance” view of all current group properties and settings, including group policy overrides. The reports also display the datasets, schedules, and retention policies assigned to various groups.

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.



/Default Group
/Default Proxy Group
/grp-W2K8r2-sp1-12-01241929
/grp-sql12x86-c3-01191720
/grp-sql12x86-c3-01201635
/grp-sql12x86-c3-01231312
/grp-sql12x86-c3-01231324
/grp-w2k8r2-sp1-12-02011538
/grp-w2k8x86-sql12-02011707

Name: /Default Dataset

Source Data:
All local AIX filesystem
All local HP-UX filesys
All local Linux filesyste
All local Macintosh file
All local Solaris filesys
Solaris Oracle databa
All local Windows files

Exclusions:
*/.Trash/
*/Library/
*/Library/Application S
*/Library/Cookies/
*/Library/Logs/
*/Library/PubSub/Fee

Options:
[]default-travers
allnodes=false
checkcache=fal
debug=false
filecachemax=-
force=false
hashcachemax
informationals=
one-file-system
repaircache=fal
run-at-end-exit=
run-at-start-exit=
statistics=false
verbose=0
[]default-travers
allnodes=false
checkcache=fal
debug=false
filecachemax=-
force=false

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

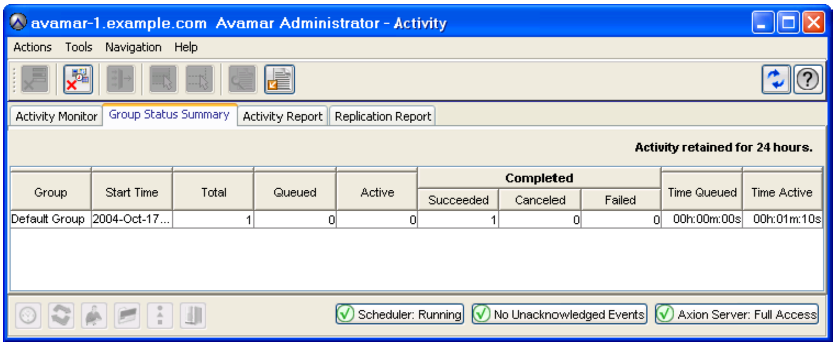
The Group Status Summary is a simplified presentation of all backup activity initiated as a result of group policies.

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.



Activity retained for 24 hours.

Group	Start Time	Total	Queued	Active	Completed			Time Queued	Time Active
					Succeeded	Canceled	Failed		
Default Group	2004-Oct-17...	1	0	0	1	0	0	00h:00m:00s	00h:01m:10s

The following table lists the information that appears on the Group Status Summary tab.

Table 22 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 add clients to or remove clients from a group in Avamar Administrator:

- **Group-centric** — You can select a group and then add or remove clients in the group, as discussed in "Adding and removing clients for a group" on page 166.
- **Client-centric** — You can select a client and then add or remove groups that the client belongs to, as discussed in "Adding and removing groups for a client" on page 167.

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 and removing clients for a group

To add or remove clients for a group:

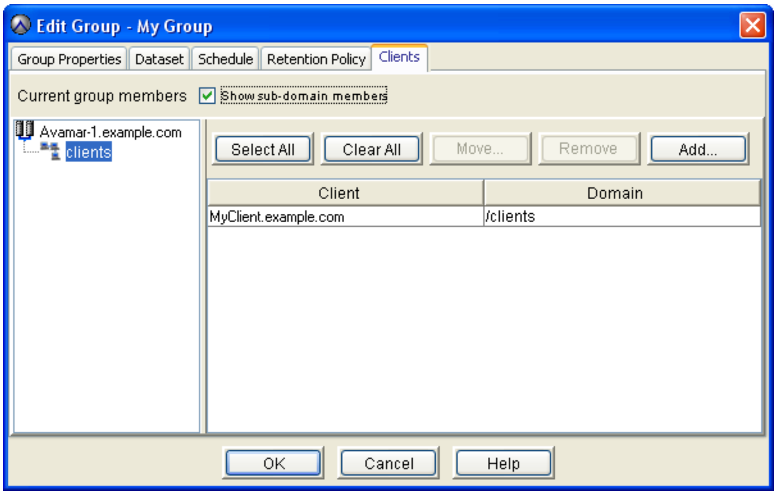
1. In Avamar Administrator, click the **Policy** launcher button.

   The Policy window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups tab**.
4. Select the group to edit.
5. Open the **Actions** menu and select **Group › Edit Group**.

   The Edit Group dialog box appears.

6. Click the **Clients** tab.



Edit Group - My Group

Current group members ☑ Show sub-domain members

Client	Domain
MyClient.example.com	/clients

7. Add and remove clients for the group:
   - To add clients, click **Add**, select the clients to add, and then click **OK**.
   - To remove clients, select the clients and click **Remove**.
8. On the **Edit Group** dialog box, click **OK**.

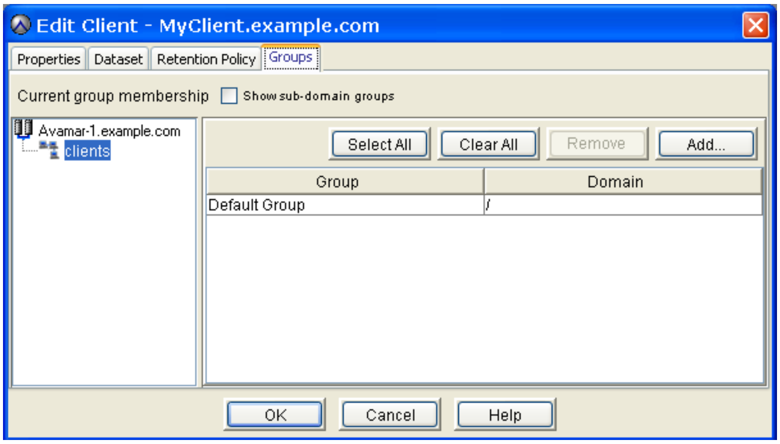
Adding and removing groups for a client

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. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client dialog box appears.
6. Click the **Groups** tab.



Group	Domain
Default Group	/

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

You can override the group policy settings by the following :

- “Assigning a different dataset to a client” on page 168
- “Assigning a different retention policy to a client” on page 169
- “Changing the client encryption method” on page 170
- “Allowing scheduled backups to run overtime” on page 171
- “Allowing users to select an alternative backup start time” on page 173
- “Allowing users to add to source data” on page 174
- “Allowing users to initiate backups” on page 175
- “Allowing users to select data source for on-demand backups” on page 179

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.

Assigning a different dataset to a client

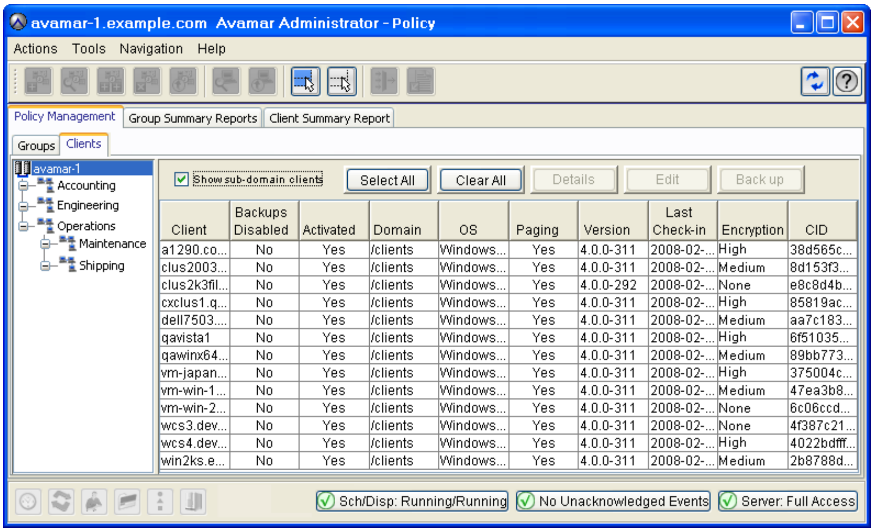
To assign a different dataset to a client:

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

   The Policy window appears.

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

3. Click the **Clients** tab.



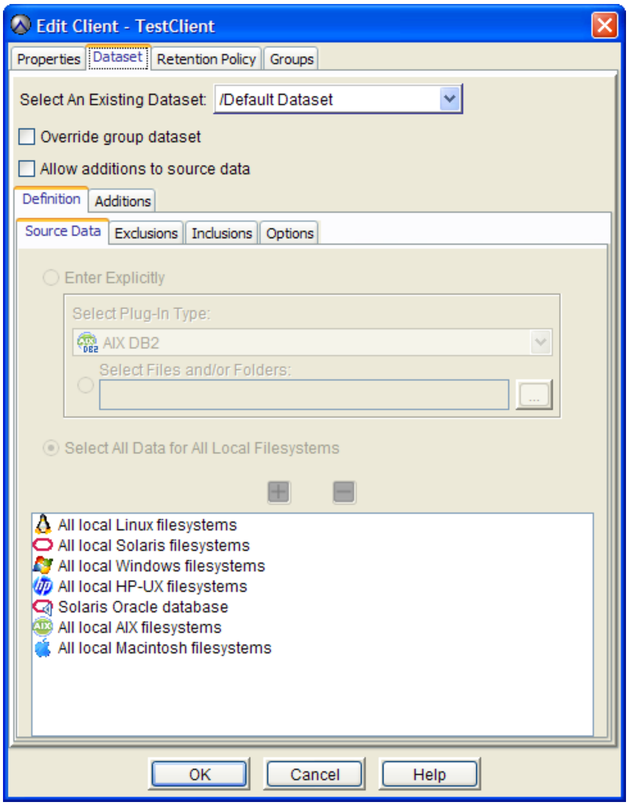
Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	CID
a1290.co...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	38d565c...
clus2003...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	8d153f3...
clus2k3fil...	No	Yes	/clients	Windows...	Yes	4.0.0-292	2008-02-...	None	e8c8d4b...
cxclus1.q...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	85819ac...
dell7503....	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	aa7c183...
qavista1	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	6f51035...
qawinx64...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	89bb773...
vm-japan...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	375004c...
vm-win-1...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	47ea3b8...
vm-win-2...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	6c06ccd...
wcs3.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	4f387c21...
wcs4.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	4022bdfff...
win2ks.e...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	2b8788d...

4. Select the client for which to override the dataset assignment.

5. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Dataset** tab.



Select An Existing Dataset: /Default Dataset

□ Override group dataset

□ Allow additions to source data

○ Enter Explicitly

Select Plug-In Type: AIX DB2

○ Select Files and/or Folders:

● Select All Data for All Local Filesystems

All local Linux filesystems
All local Solaris filesystems
All local Windows filesystems
All local HP-UX filesystems
Solaris Oracle database
All local AIX filesystems
All local Macintosh filesystems

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 127 provides details on how to edit dataset properties.

8. Select **Override group dataset**.

9. Click **OK**.

Assigning a different retention policy to a client

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 86 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.

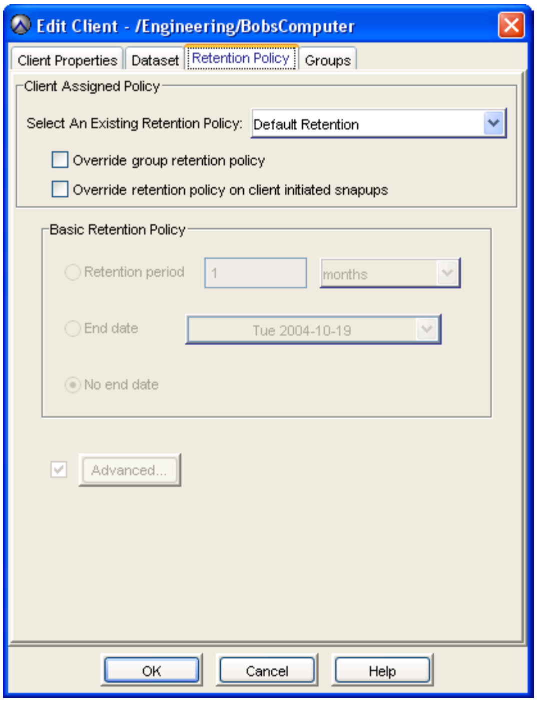
3. Click the **Clients** tab.

4. Select the client for which to override the retention policy assignment.

5. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Retention Policy** tab.



Client Assigned Policy

Select An Existing Retention Policy: Default Retention

□ Override group retention policy

□ Override retention policy on client initiated snapups

Basic Retention Policy

○ Retention period 1 months

○ End date Tue 2004-10-19

● No end date

☑ Advanced...

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 147 provides details on how to edit retention policy properties.

8. Select **Override group retention policy.**

9. Click **OK.**

Changing the client encryption method

To change the client encryption method:

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

   The Policy window appears.

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

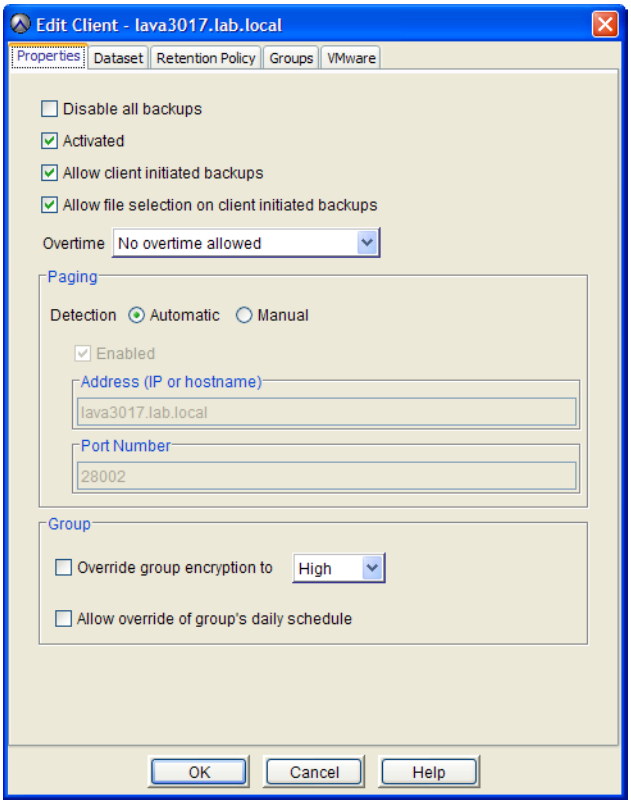
3. Click the **Clients** tab.

4. Select the client for which to change the encryption method.

5. Open the **Actions** menu and select **Client › Edit Client.**

   The Edit Client window appears.

6. Click the **Properties** tab.



Edit Client - lava3017.lab.local

Properties | Dataset | Retention Policy | Groups | VMware

□ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

□ Override group encryption to: High

□ Allow override of group's daily schedule

OK | Cancel | Help

7. Select the encryption method 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 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.

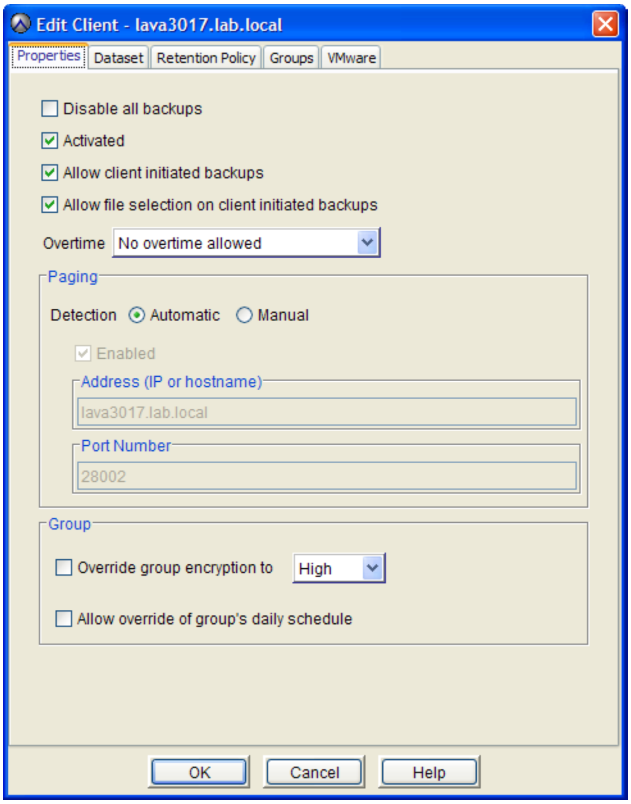
3. Click the **Clients** tab.

4. Select the client for which to allow overtime backups.

5. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Properties** tab.



☐ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

☐ Override group encryption to: High

☐ Allow override of group's daily schedule

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**.

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 schedule" on page 141.
- 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 521.

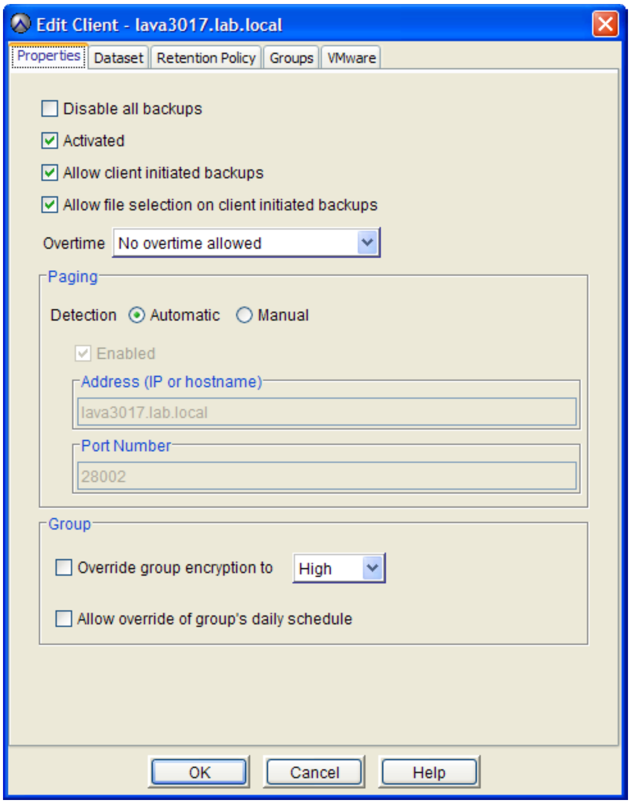
To allow users to select an alternative backup start time:

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. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Properties** tab.



□ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

□ Override group encryption to High

□ Allow override of group's daily schedule

7. Select **Allow override of group’s daily schedule**.

8. 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.

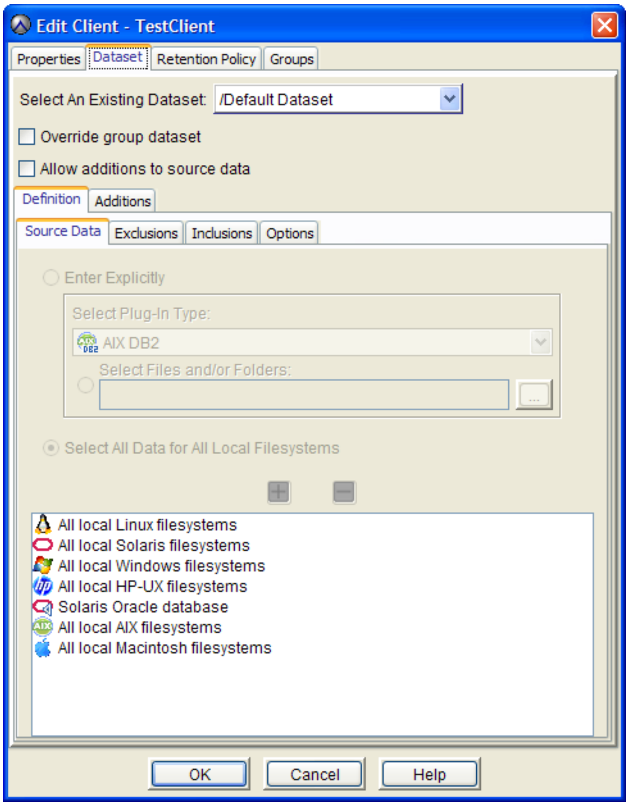
3. Click the **Clients** tab.

4. Select a client.

5. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Dataset** tab.



Select An Existing Dataset: /Default Dataset

☐ Override group dataset

☐ Allow additions to source data

○ Enter Explicitly

Select Plug-In Type: AIX DB2

Select Files and/or Folders:

● Select All Data for All Local Filesystems

All local Linux filesystems
All local Solaris filesystems
All local Windows filesystems
All local HP-UX filesystems
Solaris Oracle database
All local AIX filesystems
All local Macintosh filesystems

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**.

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.

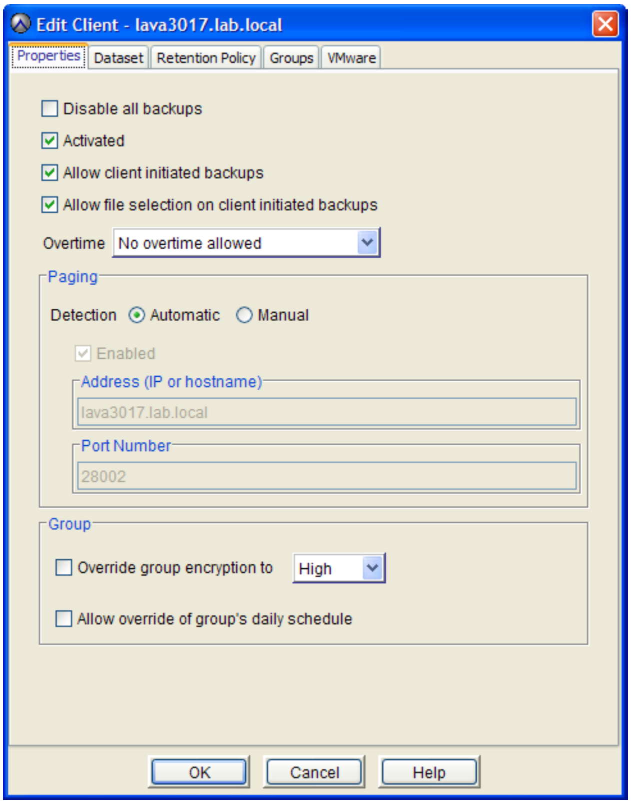
3. Click the **Clients** tab.

4. Select the client for which to allow users to initiate backups.

5. Open the **Actions** menu and select **Client › Edit Client**.

   The Edit Client window appears.

6. Click the **Properties** tab.



☐ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

☐ Override group encryption to: High

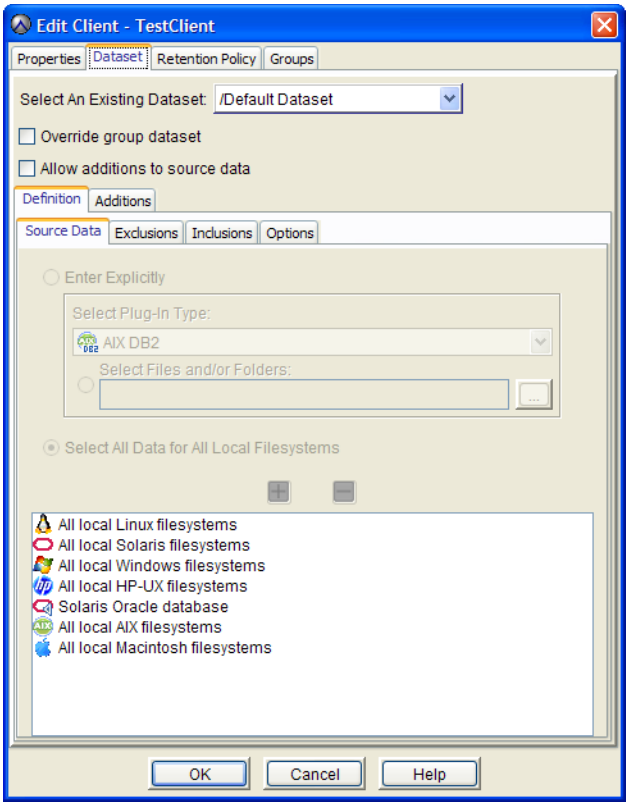
☐ Allow override of group's daily schedule

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 initiated. In addition, End User On-Demand Retention, described in "Creating a retention policy" on page 146, 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.



Select An Existing Dataset: /Default Dataset

□ Override group dataset

□ Allow additions to source data

○ Enter Explicitly

Select Plug-In Type: AIX DB2

○ Select Files and/or Folders:

● Select All Data for All Local Filesystems

- All local Linux filesystems
- All local Solaris filesystems
- All local Windows filesystems
- All local HP-UX filesystems
- Solaris Oracle database
- All local AIX filesystems
- All local Macintosh filesystems

   You cannot edit dataset properties in this window. Detailed dataset properties are shown so that you can review them before you make a selection.

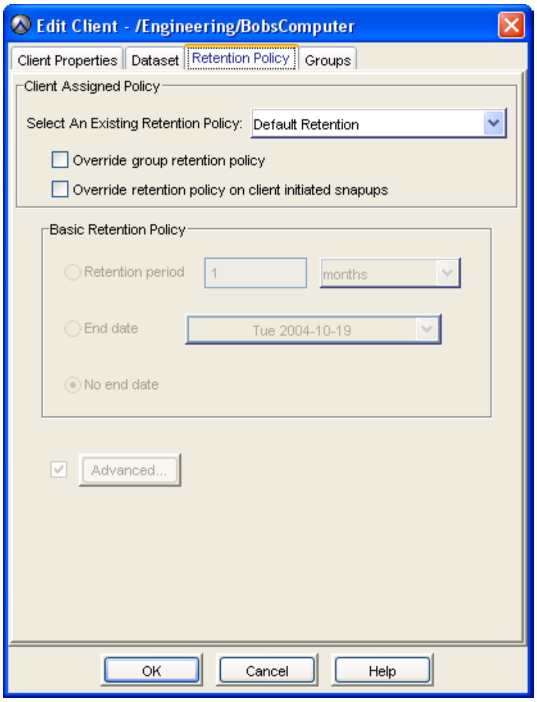
   b. Choose whether to use the group dataset or a different dataset for all client-initiated backups:

      – 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.



Client Assigned Policy

Select An Existing Retention Policy: Default Retention

□ Override group retention policy

□ Override retention policy on client initiated snapups

Basic Retention Policy

○ Retention period 1 months

○ End date Tue 2004-10-19

● No end date

☑ Advanced...

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 175.

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 526.

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.

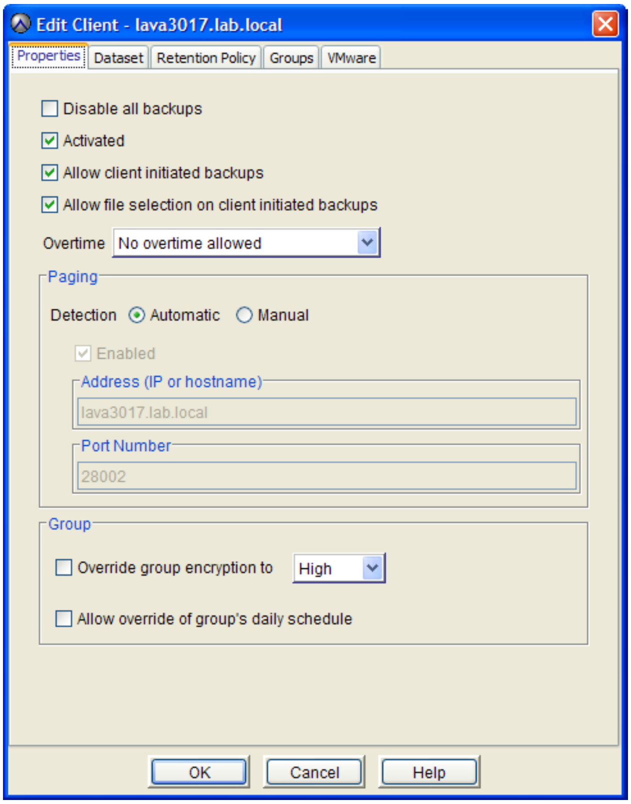
3. Click the **Clients** tab.

4. Select the client for which to allow users to initiate backups.

5. Select **Actions › Client › Edit Client.**

   The Edit Client window appears.

6. Click the **Properties** tab.



Edit Client - lava3017.lab.local

☐ Disable all backups

☑ Activated

☑ Allow client initiated backups

☑ Allow file selection on client initiated backups

Overtime: No overtime allowed

Paging

Detection ● Automatic ○ Manual

☑ Enabled

Address (IP or hostname): lava3017.lab.local

Port Number: 28002

Group

☐ Override group encryption to High

☐ Allow override of group's daily schedule

7. Select **Allow client initiated backups.**

8. Select **Allow file selection on client initiated backups.**

9. Click **OK.**

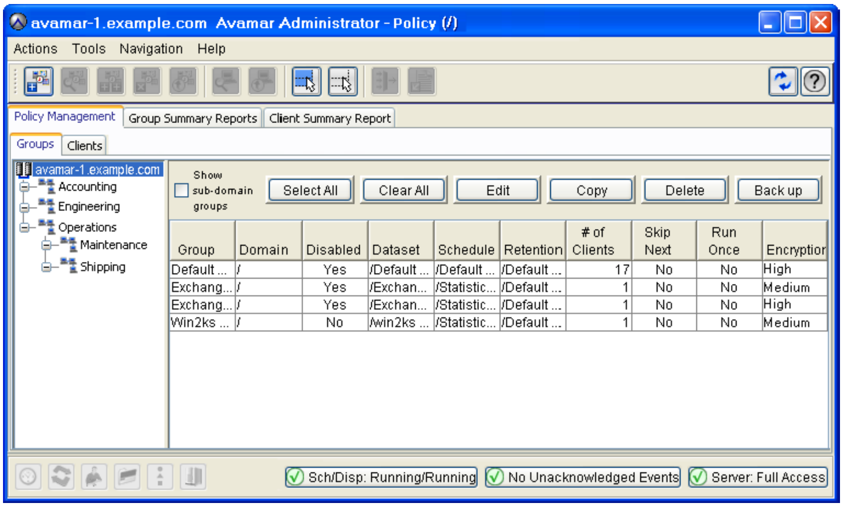
Initiating on-demand group backups

Occasionally, you may want to back up an entire group of clients 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.

To initiate an on-demand group backup:

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

   The Policy window appears.



Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryption
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	High
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Medium
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	High
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	Medium

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. Select the group and click **Back up**.

   A confirmation message appears.

5. Click **OK**.

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 184
- Editing system event profile properties 188
- Creating a custom event profile 189
- Editing custom event profile properties 197
- Copying a custom event profile 198
- Testing custom event profile notifications 199
- Enabling and disabling a custom event profile 200
- Deleting a custom event profile 200
- Modifying “Email Home” configuration 200
- Monitoring the Avamar server using syslog........ 203
- Monitoring the Avamar server using SNMP 207
- Managing ConnectEMC 213
- Enabling and disabling ConnectEMC 214
- Stopping and starting ConnectEMC 215
- Editing Primary and Failover transports 216
- Editing the Notification transport 219
- Testing transports 221

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 23 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.

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.

NOTICE

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.

NOTICE

You can increase or reduce the audit log retention period by manually editing the clean_db_audits_days preference in the /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml file, and then 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 203 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 207 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 following profiles.

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 224 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 Service (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 200 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 207 provides details.

Local Syslog profile

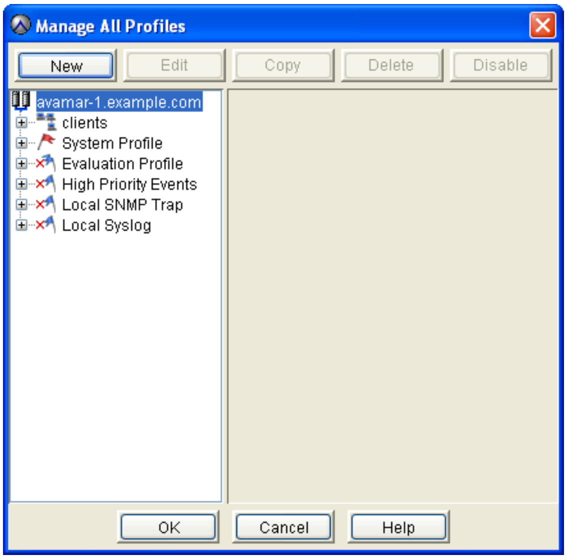
If enabled, the Local Syslog profile reports status by way of the local **syslogd** process on the Avamar server. "Monitoring the Avamar server using syslog" on page 203 provides details.

Editing system event profile properties

To edit system event profile properties:

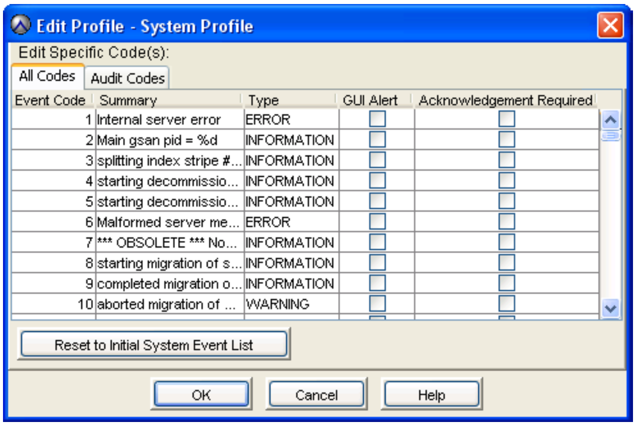
1. In Avamar Administrator, select **Tools › Manage Profiles**.

   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.


Edit Profile - System Profile
Edit Specific Code(s):
All Codes
Audit Codes
Reset to Initial System Event List
OK
Cancel
Help

Event Code	Summary	Type	GUI Alert	Acknowledgement Required
1	Internal server error	ERROR	□	□
2	Main gsan pid = %d	INFORMATION	□	□
3	splitting index stripe #...	INFORMATION	□	□
4	starting decommissio...	INFORMATION	□	□
5	starting decommissio...	INFORMATION	□	□
6	Malformed server me...	ERROR	□	□
7	*** OBSOLETE *** No...	INFORMATION	□	□
8	starting migration of s...	INFORMATION	□	□
9	completed migration o...	INFORMATION	□	□
10	aborted migration of ...	WARNING	□	□

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**.

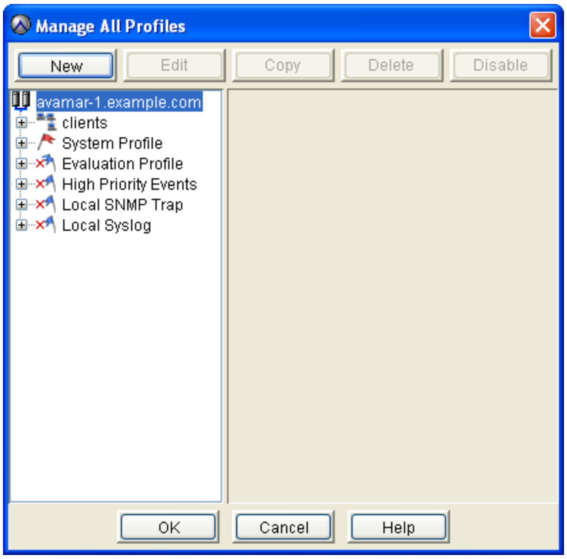
Creating a custom event profile

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**.

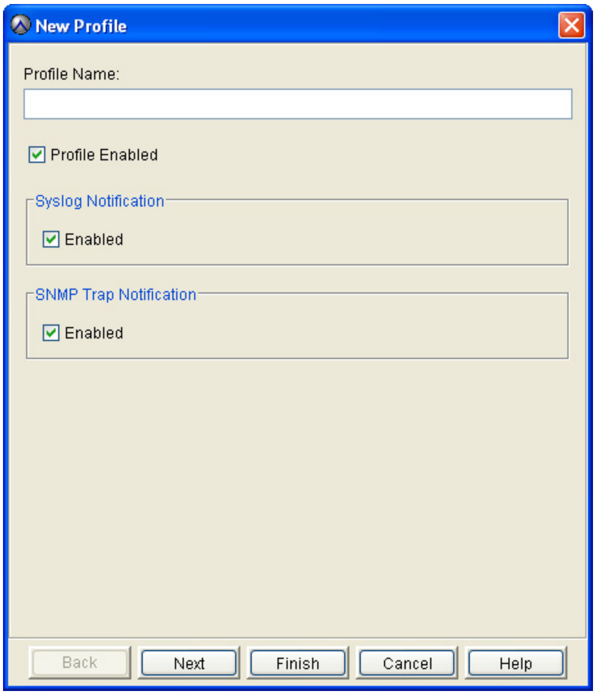
   The Manage All Profiles dialog box appears.



avamar-1.example.com
- clients
- System Profile
- Evaluation Profile
- High Priority Events
- Local SNMP Trap
- Local Syslog

2. In the tree, select the domain for the custom event profile and click **New**.

The New Profile wizard appears.



New Profile

Profile Name:

☑ Profile Enabled

Syslog Notification

☑ Enabled

SNMP Trap Notification

☑ Enabled

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.

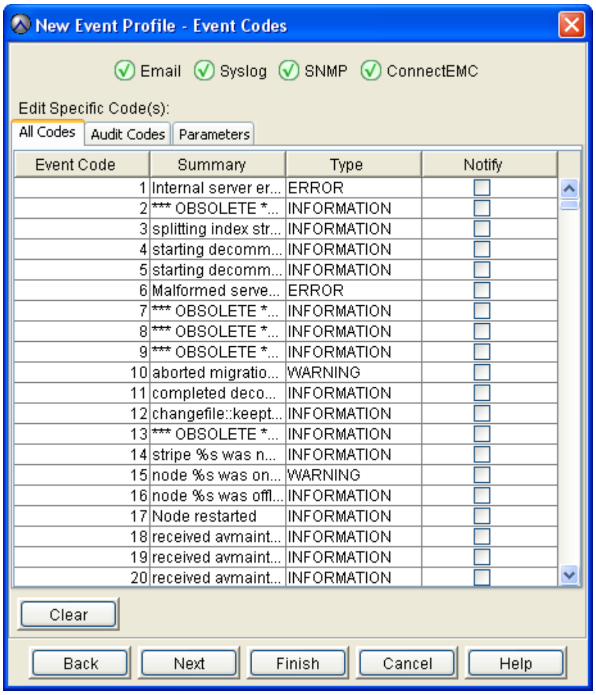
   c. Clear the **Syslog Notification – Enabled** option if you do not want to use the syslog notification feature with this profile,

   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.



Event Code	Summary	Type	Notify
1	Internal server er...	ERROR	□
2	*** OBSOLETE *...	INFORMATION	□
3	splitting index str...	INFORMATION	□
4	starting decomm...	INFORMATION	□
5	starting decomm...	INFORMATION	□
6	Malformed serve...	ERROR	□
7	*** OBSOLETE *...	INFORMATION	□
8	*** OBSOLETE *...	INFORMATION	□
9	*** OBSOLETE *...	INFORMATION	□
10	aborted migratio...	WARNING	□
11	completed deco...	INFORMATION	□
12	changefile::keept...	INFORMATION	□
13	*** OBSOLETE *...	INFORMATION	□
14	stripe %s was n...	INFORMATION	□
15	node %s was on...	WARNING	□
16	node %s was offl...	INFORMATION	□
17	Node restarted	INFORMATION	□
18	received avmaint...	INFORMATION	□
19	received avmaint...	INFORMATION	□
20	received avmaint...	INFORMATION	□

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.

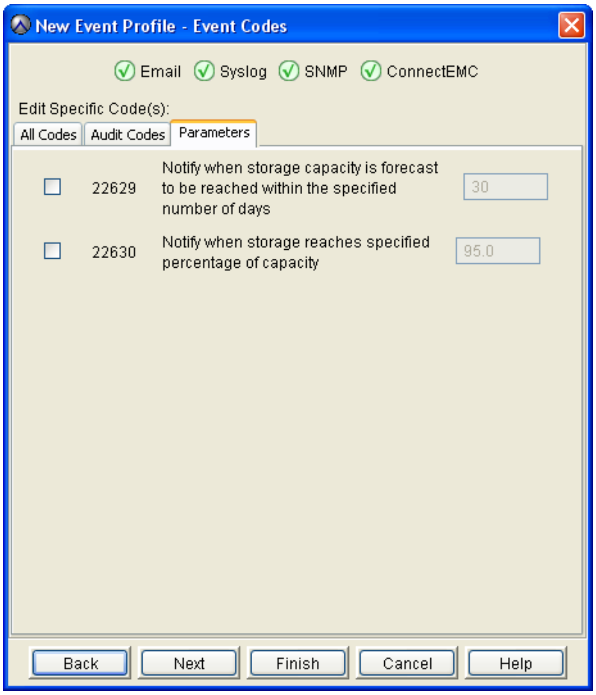
   b. Select the **Notify** option for one or more error codes.

   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.



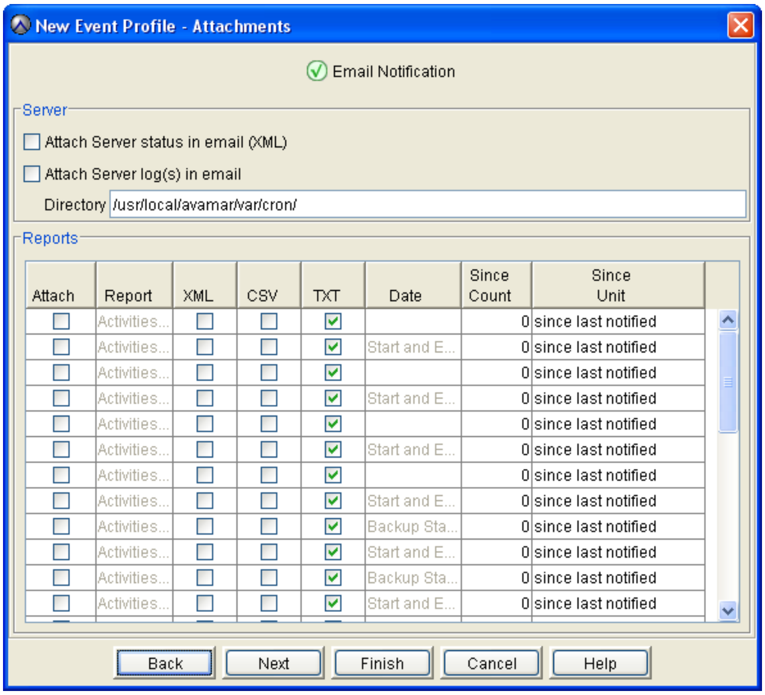
□	22629	Notify when storage capacity is forecast to be reached within the specified number of days	30
□	22630	Notify when storage reaches specified percentage of capacity	95.0

   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.



Server

☐ Attach Server status in email (XML)

☐ Attach Server log(s) in email

Directory /usr/local/avamar/var/cron/

Reports

Attach	Report	XML	CSV	TXT	Date	Since Count	Since Unit
☐	Activities...	☐	☐	☑		0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified
☐	Activities...	☐	☐	☑		0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified
☐	Activities...	☐	☐	☑		0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified
☐	Activities...	☐	☐	☑		0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified
☐	Activities...	☐	☐	☑	Backup Sta...	0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified
☐	Activities...	☐	☐	☑	Backup Sta...	0	since last notified
☐	Activities...	☐	☐	☑	Start and E...	0	since last notified

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

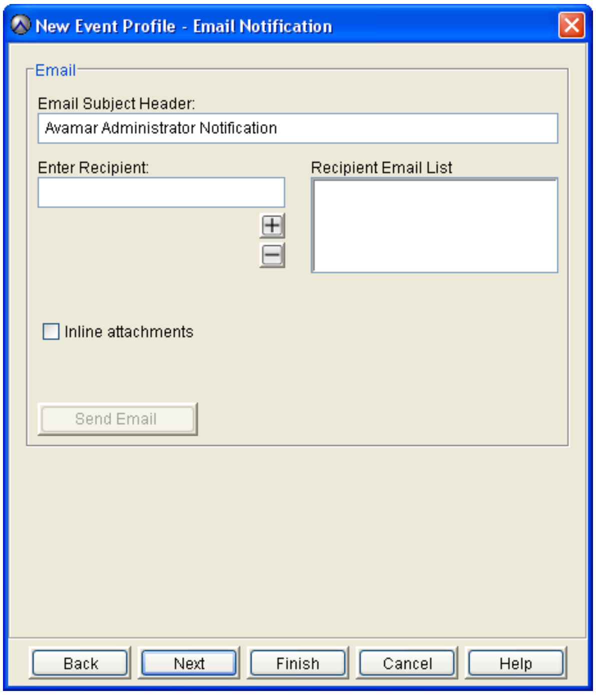
    c. Specify the number of historical reports of this type to send with each notification message using the **Since Count** and **Since Unit** fields. For example, send the past two months of these reports.

       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.



New Event Profile - Email Notification

Email Subject Header: Avamar Administrator Notification

☐ Inline attachments

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

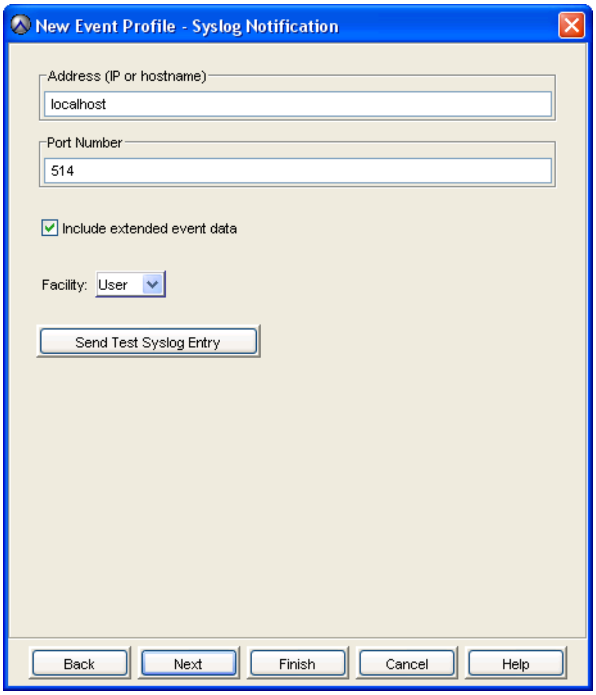
       When you insert the attachments, the email message may be very long.

    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.



Address (IP or hostname): localhost

Port Number: 514

☑ Include extended event data

Facility: User

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›

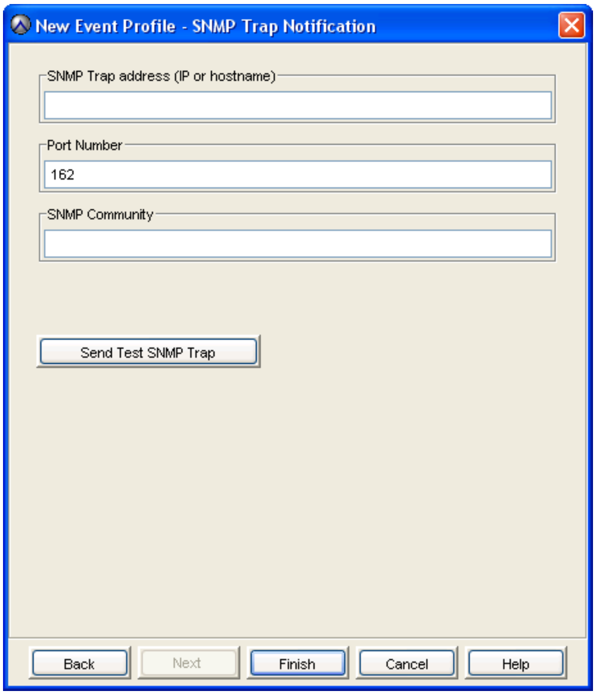
    d. From the **Facility** list, select one of the following: **user, local0, local1, local2, local3, local4, local5, local6,** or **local7**.

NOTICE

To test the syslog notification parameters, click **Send Test Syslog Entry**.

16. Click **Next**.

    The next wizard screen appears.



New Event Profile - SNMP Trap Notification

SNMP Trap address (IP or hostname):

Port Number: 162

SNMP Community:

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**.

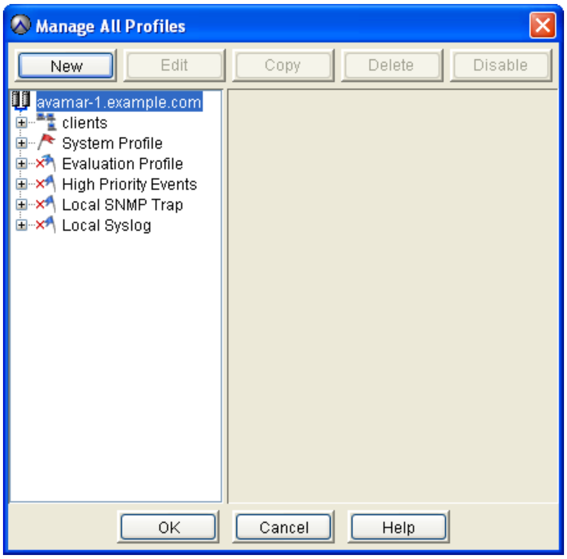
Editing custom event profile properties

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 189 provides details on custom event profile properties.

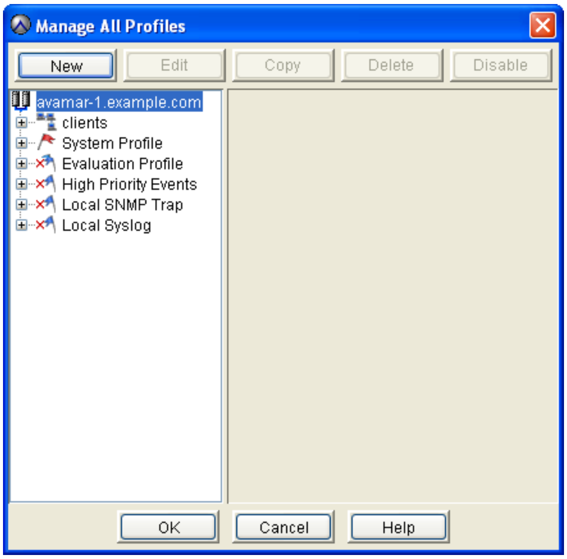
4. Click **OK.**

Copying a custom event profile

To copy a custom event profile:

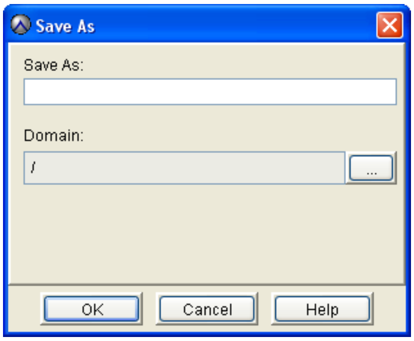
1. In Avamar Administrator, select **Tools › Manage Profiles.**

   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**.

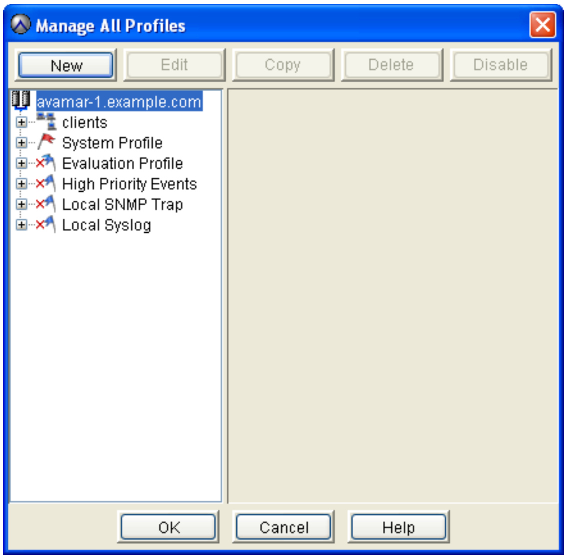
Testing custom event profile notifications

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 24 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 Service 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 129.

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 Service over the Internet.

- Administrative Mail Sender Address — For Email Home messages to be received by EMC Customer Service, 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 Service 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 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 feature called syslog that is used to collect system log messages and write them to a designated log file. Avamar servers can output Avamar server event codes in syslog format.

The service used to implement this feature is the syslog daemon (syslogd). This service can be hosted locally on the Avamar server or on a remote network host. "Configure local syslogd monitoring" on page 205 and "Configure remote syslogd monitoring" on page 206 provide details for configuring local or remote syslog monitoring, respectively.

The following table shows how Avamar event data is mapped to various syslog fields.

Table 25 Syslog field and Avamar Event data mappings

Syslog Field	Avamar Event Code Data
Facility	One of the following, set by way of the custom event profile Facility field: • user • local#, where # is a number from 0 to 7
Priority	One of the following, based on the Avamar event type: • 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

The following is an example Avamar server syslog message:

```
Feb 9 08:23:57 MyAvamar MCS: <Code> 22254 <Category> SYSTEM <Summary>
   Client Adhoc Backup Request Error - Unknown ID. <Data> Client =
   ivory
```

To monitor an Avamar server using syslog:

1. Configure a custom event profile that outputs designated Avamar server events to a local or remote syslogd process, as discussed in "Configure a custom event profile" on page 204.

2. Configure syslogd so that it can collect information from the Avamar server, as discussed in "Configure local syslogd monitoring" on page 205.

Configure a custom event profile

Local Syslog profile

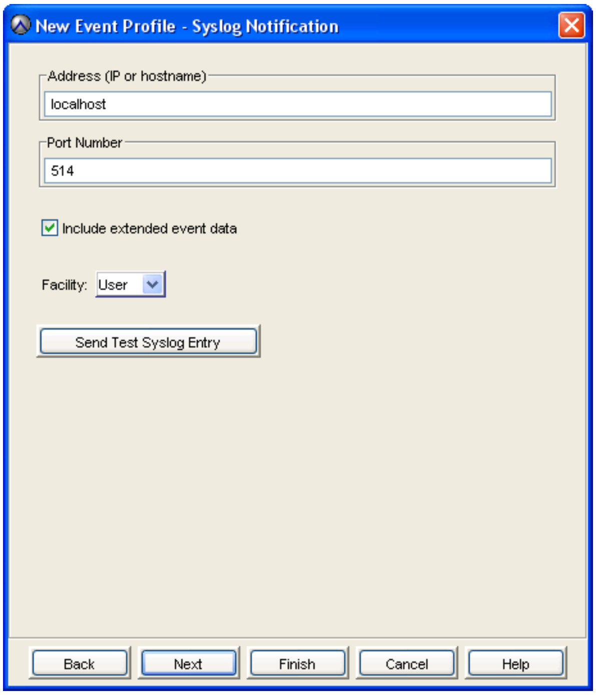
The default Avamar configuration includes a Local Syslog profile. If enabled, this profile outputs Avamar server event messages to the local syslogd process on the Avamar server.

The Local Syslog profile is read-only. You can enable it using the factory settings, but you cannot edit it. If you require custom Local Syslog profile settings, you must copy it and then edit the copy.

Using a custom event profile

If you create a custom event profile to support syslog monitoring, ensure that Syslog Notification **Enabled** option is selected on the first wizard screen. "Creating a custom event profile" on page 189 provides details on starting and proceeding through the wizard.

Continue through the wizard until the Syslog Notification screen appears.



New Event Profile - Syslog Notification

Address (IP or hostname): localhost

Port Number: 514

☑ Include extended event data

Facility: User

Complete the settings as described in the following table.

Table 26 Syslog Notification screen settings

Setting	Description
Address (IP or hostname)	IP address or hostname of the syslog server. This can be the local Avamar server or a remote network host that has been configured to listen for Avamar server syslogd messages over a LAN connection. "Configure local syslogd monitoring" on page 205 and "Configure remote syslogd monitoring" on page 206 provide details for configuring local or remote syslog monitoring, respectively.
Port Number	Port number used for syslog communication.
Include extended event data	If selected, additional (extended) event code information is included 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>
Facility	One of the following: • user • local#, where # is a number from 0 to 7

Configure local syslogd monitoring

To configure the syslog daemon (syslogd), edit the settings in the /etc/sysconfig/syslog configuration file. These settings implement various filtering rules and control where syslog messages are logged.

By default, Avamar writes to syslogd using localhost UDP port 514. To enable the local syslogd process to monitor these messages, edit the /etc/syslog.conf file to configure syslogd to listen on this data port.

The /etc/sysconfig/syslog file typically contains an entry similar to this:

```
SYSLOGD_OPTIONS="-m 0"
```

This entry line must be modified to add the **-r** parameter:

```
SYSLOGD_OPTIONS="-r -m 0"
```

After you edit /etc/sysconfig/syslog, restart the syslogd daemon using the following command:

```
kill -SIGHUP `cat /var/run/syslogd.pid`
```

A complete discussion of configuring local syslog monitoring is beyond the scope of this publication. The UNIX or Linux operating system documentation provides information.

Configure remote syslogd monitoring

This topic describes how to configure another network host to listen for Avamar server syslogd messages over a LAN connection.

These instructions are applicable to remote syslog servers running the SUSE Linux Enterprise Server (SLES) 10 operating system.

1. Open a command shell and log in to remote syslog server as root.
2. Uncomment the following line in /etc/syslog-ng/syslog-ng.conf.in:

   ```
   #
   # uncomment to process log messages from network:
   #
   udp(ip("0.0.0.0") port(514));
   ```

3. Initialize changes to the syslog-ng configuration by typing:

   ```
   SuSEconfig
   ```

4. Restart the syslog process by typing:

   ```
   /etc/init.d/syslog restart
   ```

5. 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
   ```

6. If you have a firewall enabled on the system, configure the firewall to allow UDP traffic on port 514.

A complete discussion of configuring remote syslog monitoring is beyond the scope of this publication. The UNIX or Linux operating system documentation provides information.

Monitoring the Avamar server using SNMP

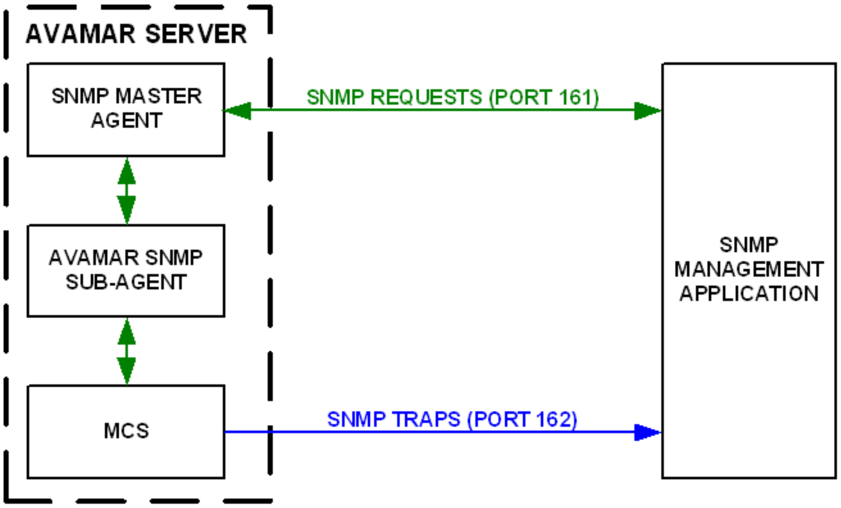
Simple Network Management Protocol (SNMP) is a protocol for communicating and monitoring event notification information between an application, hardware device, or software application and any number of monitoring applications or devices.

Prerequisite knowledge

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.

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 27 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 monitor an Avamar server 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 209.
   - 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 211.

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.

NOTICE

Run the **avsetup_snmp** utility from the /root directory as the root user.

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. 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]:
   ```

3. 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):
   ```

4. 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)
   :
   ```

5. 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):
   ```

6. 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):
```

7. 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.

8. 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]:
```

9. Press **Enter**.

   The following information appears in the command shell:

```
The OID that this community should be restricted to [RETURN for
no-restriction]:
```

10. Press **Enter**.

    The following information appears in the command shell:

```
Finished Output: rocommunity public MyCommunity
Do another rocommunity line? (default = y):
```

11. 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:
```

12. 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:
    ```

13. 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):
    ```

14. 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).

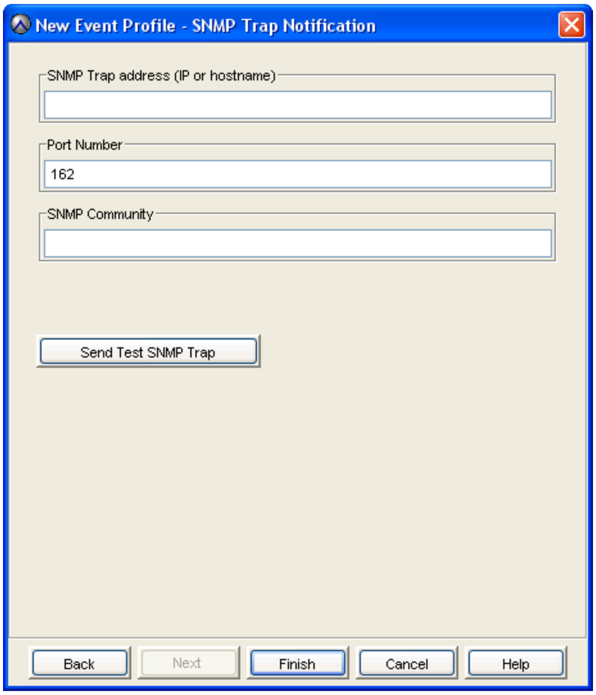
NOTICE

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 189, 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.



New Event Profile - SNMP Trap Notification

SNMP Trap address (IP or hostname)

Port Number: 162

SNMP Community

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 Service. 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.

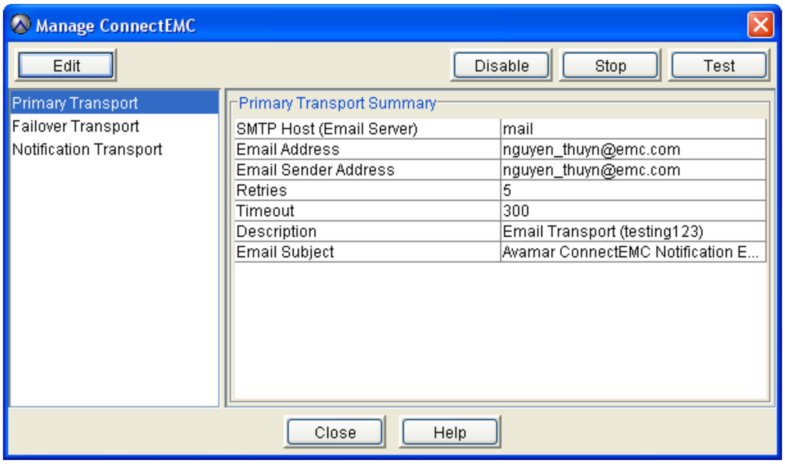
Enabling and disabling ConnectEMC

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.



Primary Transport Summary

SMTP Host (Email Server)	mail
Email Address	nguyen_thuyn@emc.com
Email Sender Address	nguyen_thuyn@emc.com
Retries	5
Timeout	300
Description	Email Transport (testing123)
Email Subject	Avamar ConnectEMC Notification E...

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**.

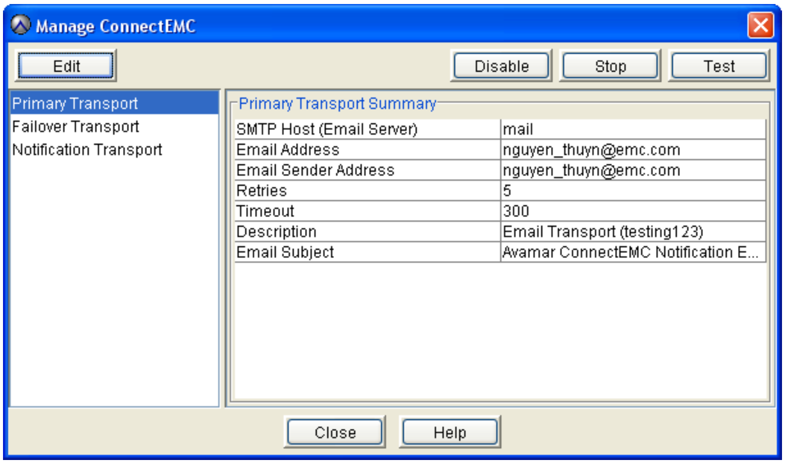
Stopping and starting ConnectEMC

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.



SMTP Host (Email Server)	mail
Email Address	nguyen_thuyn@emc.com
Email Sender Address	nguyen_thuyn@emc.com
Retries	5
Timeout	300
Description	Email Transport (testing123)
Email Subject	Avamar ConnectEMC Notification E...

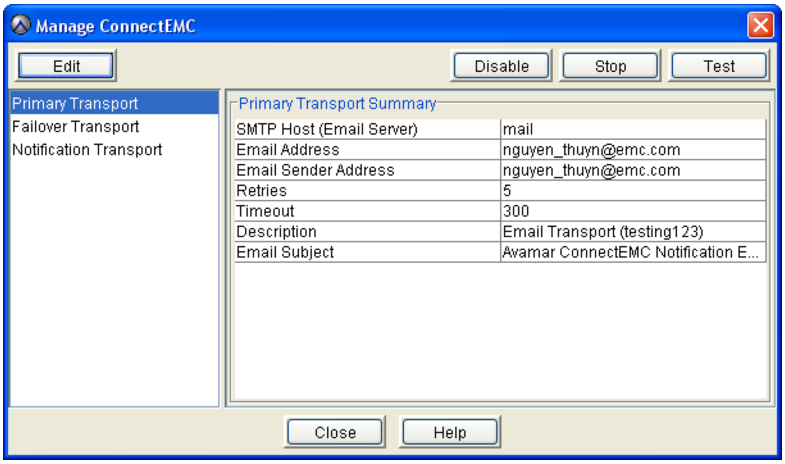
2. Click **Stop** or **Start** to stop or start the sending of ConnectEMC alerts, respectively.

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.



Primary Transport Summary

SMTP Host (Email Server)	mail
Email Address	nguyen_thuyn@emc.com
Email Sender Address	nguyen_thuyn@emc.com
Retries	5
Timeout	300
Description	Email Transport (testing123)
Email Subject	Avamar ConnectEMC Notification E...

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 28 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 Service. 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 Service. **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 28 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 Service. 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.

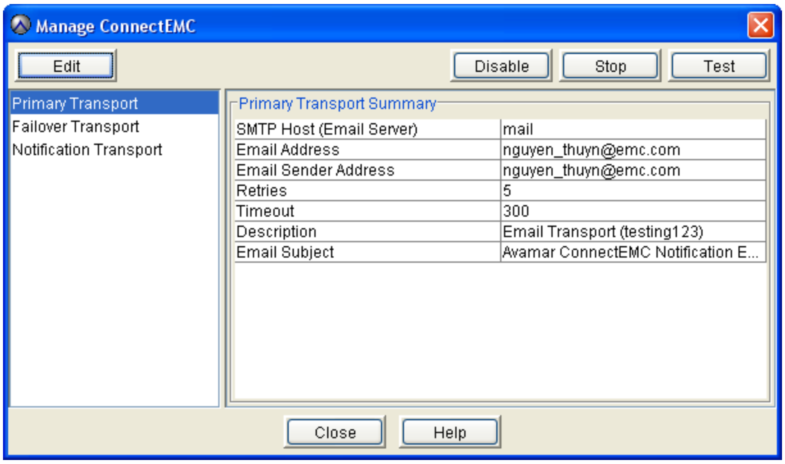
5. On the **Edit Primary Transport** dialog box, click **OK**.

Editing the Notification transport

To edit the Notification transport:

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

   The Manage ConnectEMC window appears.

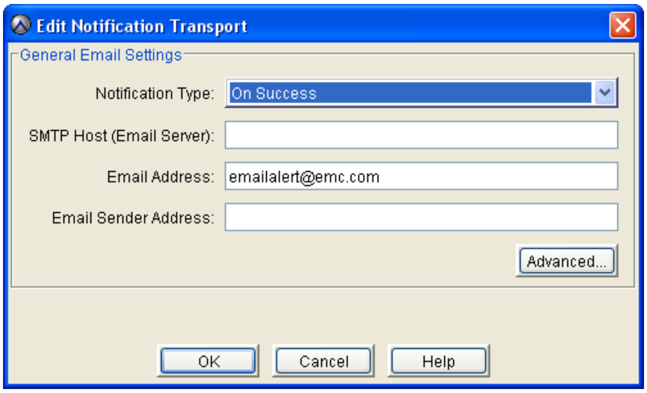


Primary Transport Summary

SMTP Host (Email Server)	mail
Email Address	nguyen_thuyn@emc.com
Email Sender Address	nguyen_thuyn@emc.com
Retries	5
Timeout	300
Description	Email Transport (testing123)
Email Subject	Avamar ConnectEMC Notification E...

2. Select the **Notification Transport** and click **Edit**.

   The Edit Notification Transport dialog box appears.



Notification Type: On Success

SMTP Host (Email Server):

Email Address: emailalert@emc.com

Email Sender Address:

3. From the **Notification Type** list, select one of the following types:

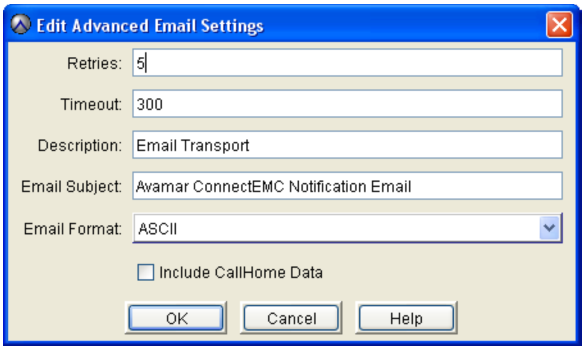
   - **On Success** — Notify recipients when an event file is successfully transferred to EMC.
   - **On Failure** — Notify recipients when an event file is not successfully transferred to EMC.
   - **On Success or Failure** — Notify recipients when an attempt is made to transfer an event file to EMC, regardless 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.



Edit Advanced Email Settings

Retries: 5

Timeout: 300

Description: Email Transport

Email Subject: Avamar ConnectEMC Notification Email

Email Format: ASCII

☐ Include CallHome Data

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 Service. 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.

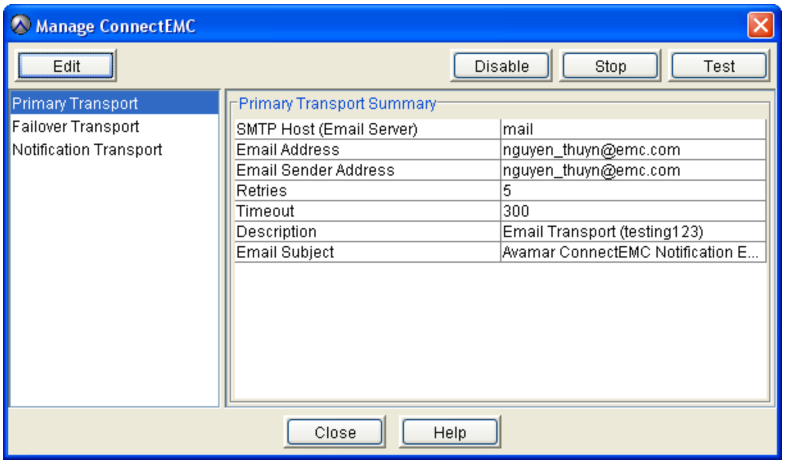
9. On the **Edit Notification Transport** dialog box, click **OK**.

Testing transports

To send test alerts and email messages:

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

   The Manage ConnectEMC window appears.



Primary Transport Summary

SMTP Host (Email Server)	mail
Email Address	nguyen_thuyn@emc.com
Email Sender Address	nguyen_thuyn@emc.com
Retries	5
Timeout	300
Description	Email Transport (testing123)
Email Subject	Avamar ConnectEMC Notification E...

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 224
- Creating a report 227
- Editing a report 230
- Running a report 231
- Deleting a report 232
- Viewing the Client Summary Report 232
- Viewing the Activity Report 236
- Viewing the Replication Report 240
- Exporting displayed tabular data as CSV files 242
- Support for third-party reporting tools 244
- Setting up the PostgreSQL ODBC driver 245
- Crystal Reports templates 247
- Other third-party support 248

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 29 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 29 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 29 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 187.

Report templates

In addition to predefined reports, you can create reports based on the templates in the following table.

Table 30 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.

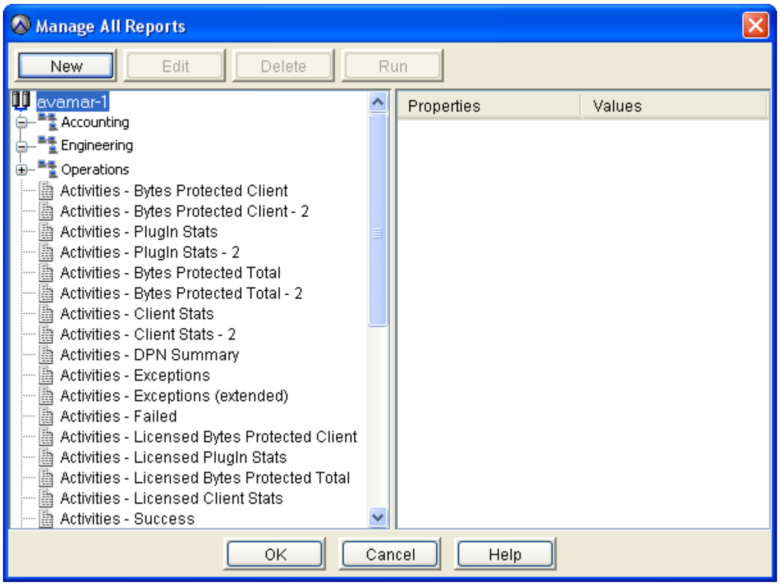
Creating a report

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 189 provides details.

To create a report:

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

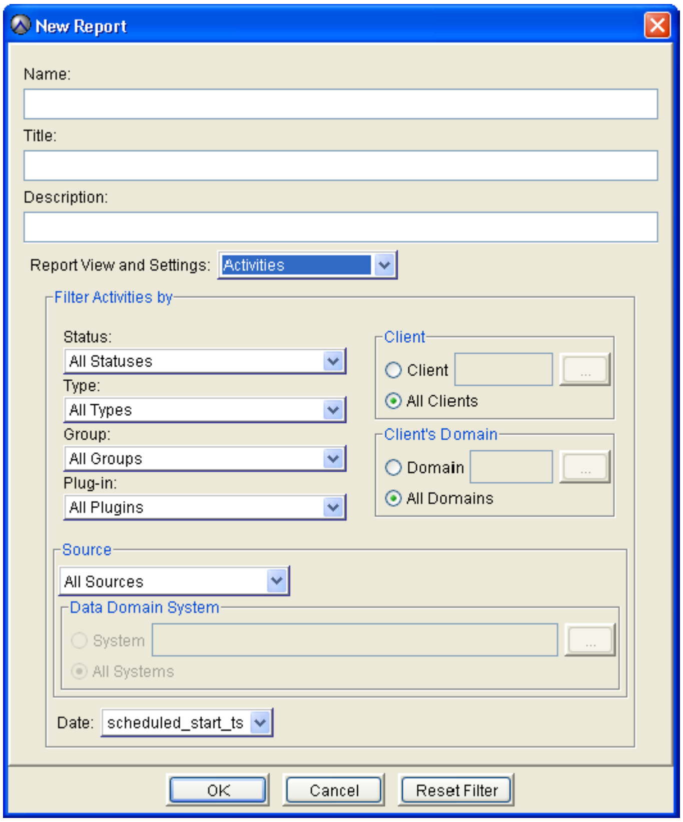
   The Manage All Reports dialog box appears.



avamar-1
Accounting
Engineering
Operations
Activities - Bytes Protected Client
Activities - Bytes Protected Client - 2
Activities - PlugIn Stats
Activities - PlugIn Stats - 2
Activities - Bytes Protected Total
Activities - Bytes Protected Total - 2
Activities - Client Stats
Activities - Client Stats - 2
Activities - DPN Summary
Activities - Exceptions
Activities - Exceptions (extended)
Activities - Failed
Activities - Licensed Bytes Protected Client
Activities - Licensed PlugIn Stats
Activities - Licensed Bytes Protected Total
Activities - Licensed Client Stats
Activities - Success

2. Select the domain for the report and click **New**.

The New Report dialog box appears.



New Report

Name:

Title:

Description:

Report View and Settings: Activities

Filter Activities by

Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

Client

○ Client

● All Clients

Client's Domain

○ Domain

● All Domains

Source

All Sources

Data Domain System

○ System

● All Systems

Date: scheduled_start_ts

3. Specify a name, display title, and optional short description for the report in the **Name**, **Title**, and **Description** fields.

4. From the **Report View and Settings** list, select a report template:

   - Activities
   - Clients
   - Replication Activities
   - Backend Capacity

   "Report templates" on page 226 provides details on each template.

5. Complete the settings that appear for the report template, as described in the following table.

Table 31 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 filesystem, 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.

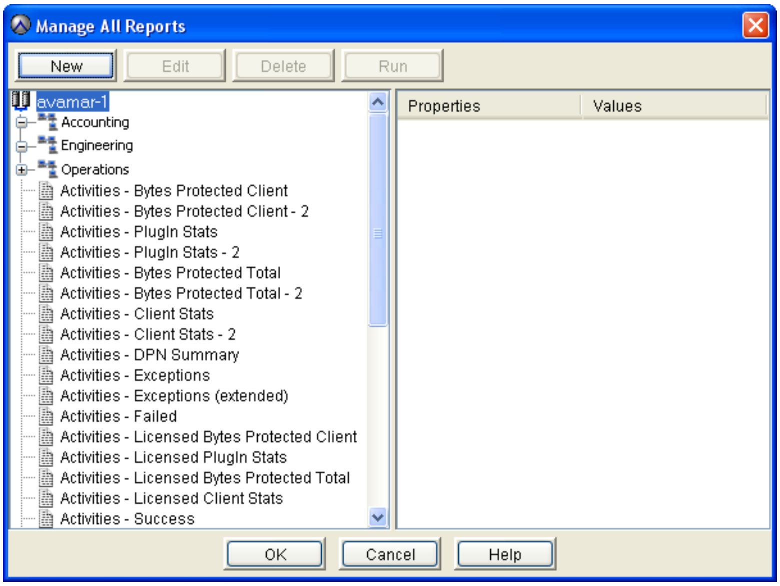
6. Click **OK**.

Editing a report

To edit a report:

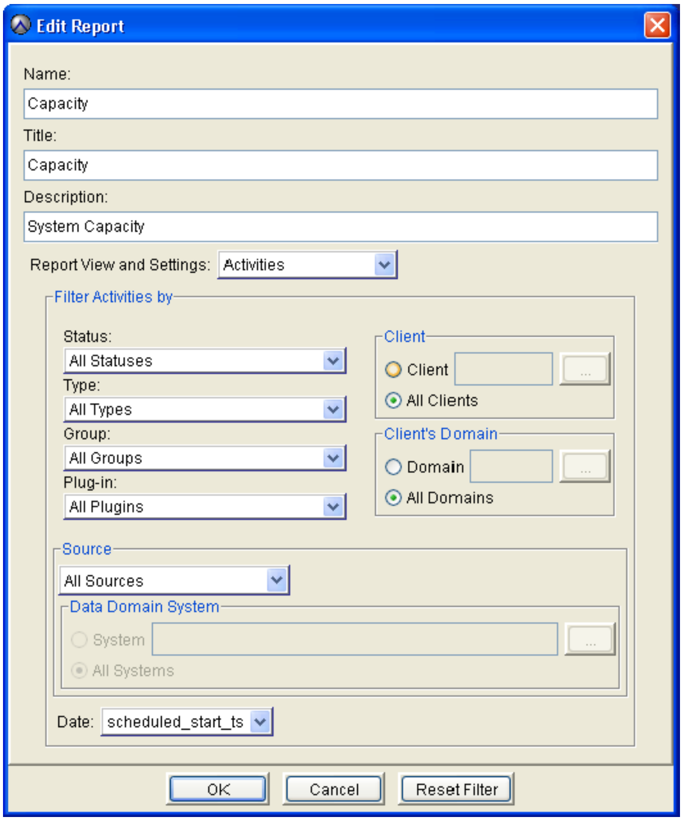
1. In Avamar Administrator, select **Tools › Manage Reports.**

   The Manage All Reports dialog box appears.


Manage All Reports
New
Edit
Delete
Run
avamar-1
Accounting
Engineering
Operations
Activities - Bytes Protected Client
Activities - Bytes Protected Client - 2
Activities - PlugIn Stats
Activities - PlugIn Stats - 2
Activities - Bytes Protected Total
Activities - Bytes Protected Total - 2
Activities - Client Stats
Activities - Client Stats - 2
Activities - DPN Summary
Activities - Exceptions
Activities - Exceptions (extended)
Activities - Failed
Activities - Licensed Bytes Protected Client
Activities - Licensed PlugIn Stats
Activities - Licensed Bytes Protected Total
Activities - Licensed Client Stats
Activities - Success
Properties
Values
OK
Cancel
Help

2. In the tree in the left pane, select the report and click **Edit.**

   The Edit Report dialog box appears.



Name: Capacity

Title: Capacity

Description: System Capacity

Report View and Settings: Activities

Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

○ Client

● All Clients

○ Domain

● All Domains

All Sources

○ System

● All Systems

Date: scheduled_start_ts

3. Edit the report settings, which are described in “Creating a report” on page 227.

4. Click **OK**.

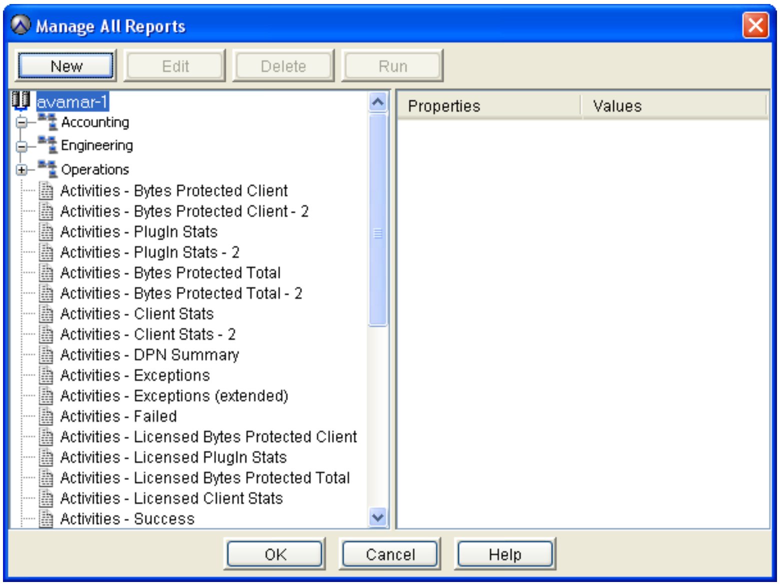
Running a report

Backend capacity reports are very resource intensive. Never run more than one backend capacity report at the same time. Whenever possible, avoid running backend capacity reports during the blackout window, described on page 294.

To run a report:

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

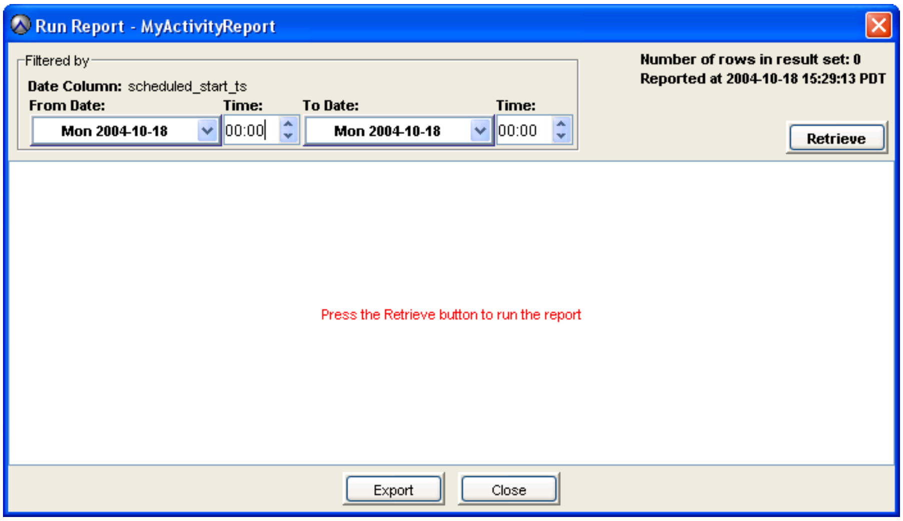
   The Manage All Reports dialog box appears.



avamar-1
- Accounting
- Engineering
- Operations
- Activities - Bytes Protected Client
- Activities - Bytes Protected Client - 2
- Activities - PlugIn Stats
- Activities - PlugIn Stats - 2
- Activities - Bytes Protected Total
- Activities - Bytes Protected Total - 2
- Activities - Client Stats
- Activities - Client Stats - 2
- Activities - DPN Summary
- Activities - Exceptions
- Activities - Exceptions (extended)
- Activities - Failed
- Activities - Licensed Bytes Protected Client
- Activities - Licensed PlugIn Stats
- Activities - Licensed Bytes Protected Total
- Activities - Licensed Client Stats
- Activities - Success

2. In the tree in the left pane, select the report and click **Run**.

   The Run Report dialog box appears.



Date Column: scheduled_start_ts

From Date: Mon 2004-10-18 Time: 00:00 To Date: Mon 2004-10-18 Time: 00:00

Number of rows in result set: 0
Reported at 2004-10-18 15:29:13 PDT

Press the Retrieve button to run the report

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.

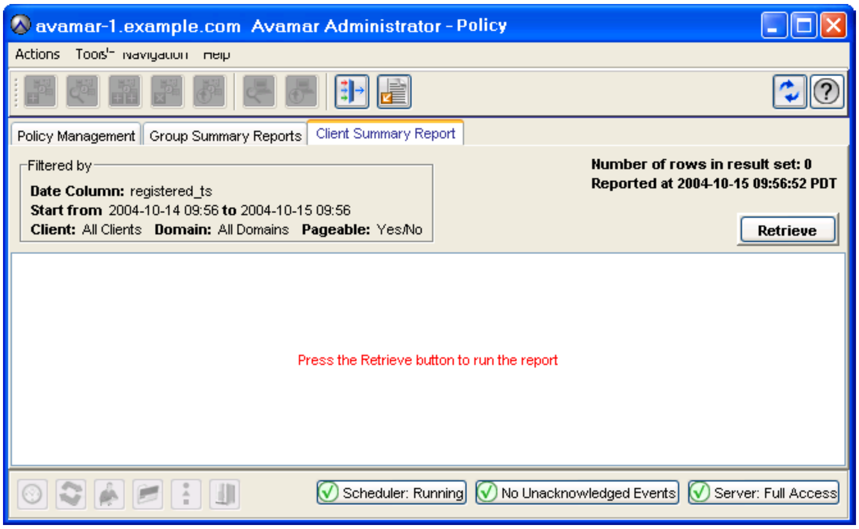
To view the Client Summary Report:

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.



avamar-1.example.com Avamar Administrator - Policy

Filtered by

Date Column: registered_ts
Start from 2004-10-14 09:56 **to** 2004-10-15 09:56
Client: All Clients **Domain:** All Domains **Pageable:** Yes/No

Number of rows in result set: 0
Reported at 2004-10-15 09:56:52 PDT

Press the Retrieve button to run the report

3. Click **Retrieve**.

   The client summary report displays the information in the following table for each client registered on the server.

Table 32 Client Summary report column descriptions (page 1 of 2)

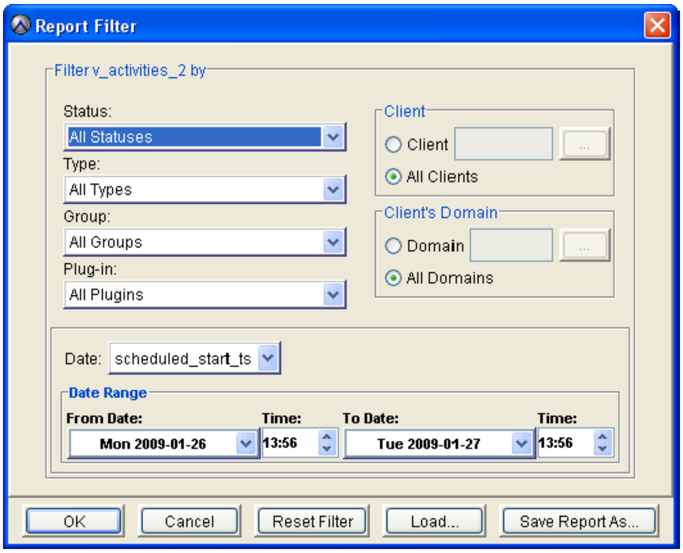
Column	Description
agent_version	Version of the agent that is installed.
allow_overtime	True if the client can ignore the scheduling window end time. See also overtime_option page 234.
allow_userinit_backup_file_sel	Allow file selection on user-initiated backups.
allow_userinit_backups	Allow user-initiated 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 32 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	
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.



Filter v_activities_2 by

Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

Client: ○ Client ● All Clients

Client's Domain: ○ Domain ● All Domains

Date: scheduled_start_ts

Date Range

From Date: Mon 2009-01-26 Time: 13:56 To Date: Tue 2009-01-27 Time: 13:56

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.

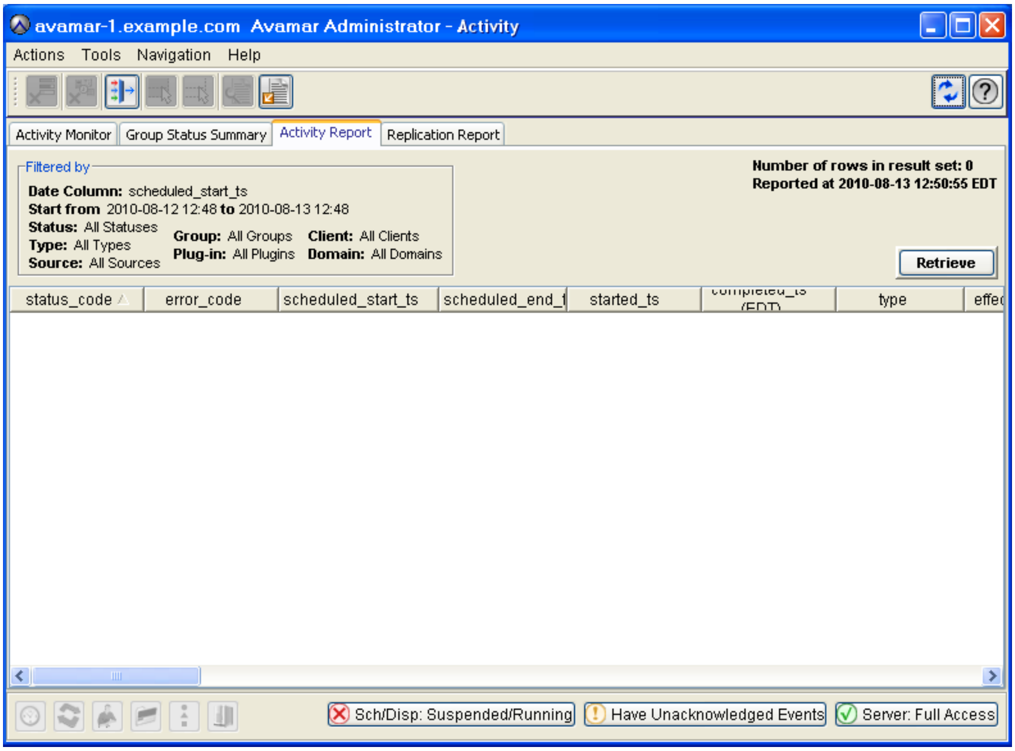
To view the Activity Report:

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.



Filtered by
Date Column: scheduled_start_ts
Start from 2010-08-12 12:48 **to** 2010-08-13 12:48
Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Number of rows in result set: 0
Reported at 2010-08-13 12:50:55 EDT

Sch/Disp: Suspended/Running
Have Unacknowledged Events
Server: Full Access

3. Click **Retrieve**.

   The activity report displays the information in the following table for each activity.

Table 33 Activity report column descriptions (page 1 of 3)

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 33 Activity report column descriptions (page 2 of 3)

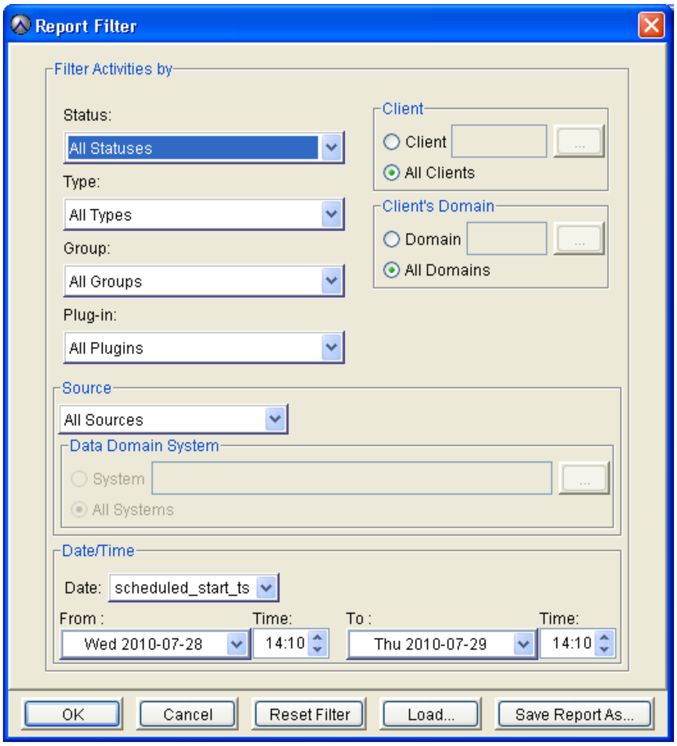
Column	Description
bytes_skipped	Total number of bytes unintentionally skipped (errors and so forth) during this activity.
cid	Client ID.
client_name	Avamar client name.
client_os	Client operating system.
client_ver	Avamar client software version.
completed_ts	Date and time that this activity ended, 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.
domain	Full location of the client in the Avamar server.
ddr_hostname	Hostname of the Data Domain system on which the activity occurred, if the activity occurred on a Data Domain system.
effective_expiration	Calendar date and time that this backup will expire.
effective_path	For group-based backups, the dataset used in 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.
encrypt_method2_sa	
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 33 Activity report column descriptions (page 3 of 3)

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.
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.
started_ts	Date and time that this activity started, adjusted for the prevailing time zone, which is shown in parentheses.
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.



Report Filter

Filter Activities by

Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

Client

○ Client

● All Clients

Client's Domain

○ Domain

● All Domains

Source

All Sources

Data Domain System

○ System

● All Systems

Date/Time

Date: scheduled_start_ts

From : Wed 2010-07-28 Time: 14:10

To : Thu 2010-07-29 Time: 14:10

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

Viewing the Replication Report

The Replication Report provides detailed information for recent replication operations.

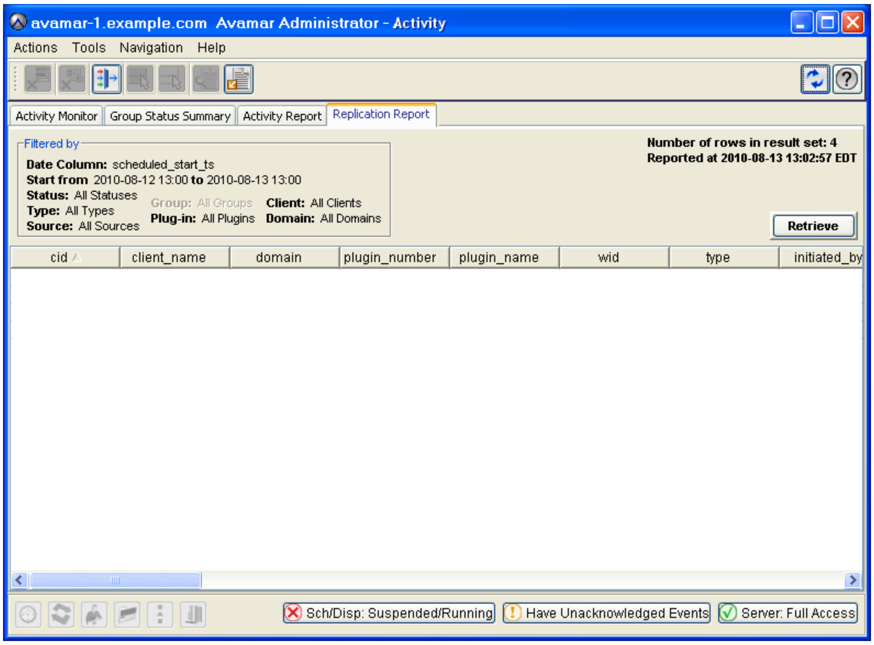
To view the Replication Report:

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.



Filtered by

Date Column: scheduled_start_ts
Start from 2010-08-12 13:00 **to** 2010-08-13 13:00
Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Number of rows in result set: 4
Reported at 2010-08-13 13:02:57 EDT

cid	client_name	domain	plugin_number	plugin_name	wid	type	initiated_by

3. Click **Retrieve**.

   The Replication report displays the information in the following table for each replication operation.

Table 34 Replication report column descriptions (page 1 of 2)

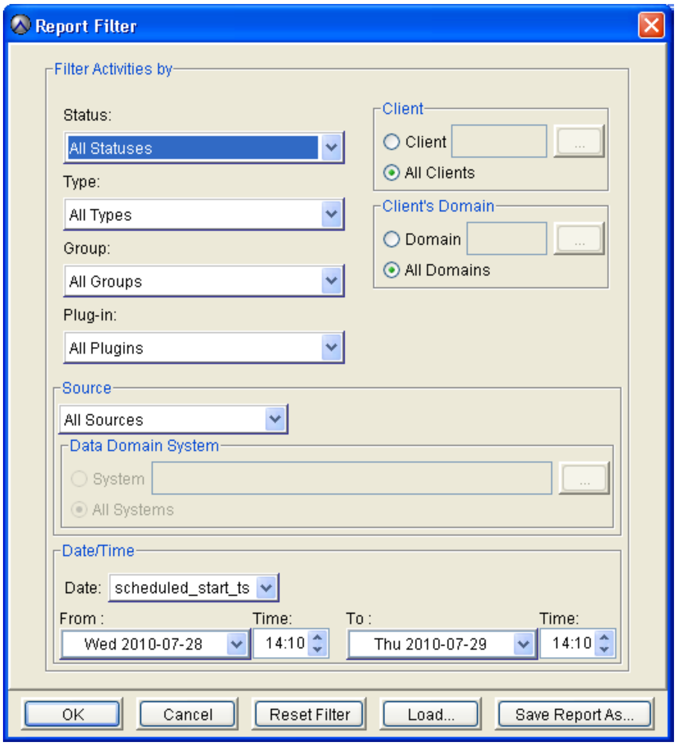
Column	Description
bytes_excluded	Total number of bytes intentionally excluded during this replication operation.
bytes_new	Total number of bytes processed during this replication operation after data deduplication.
bytes_overhead	Total number of overhead bytes.
bytes_scanned	Total number of bytes processed 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.
client_os	Client operating system.

Table 34 Replication report column descriptions (page 2 of 2)

Column	Description
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	
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.
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.
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.



Status: All Statuses

Type: All Types

Group: All Groups

Plug-in: All Plugins

○ Client

● All Clients

○ Domain

● All Domains

Source: All Sources

○ System

● All Systems

Date: scheduled_start_ts

From : Wed 2010-07-28 Time: 14:10 To : Thu 2010-07-29 Time: 14:10

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

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 242
- "Replication Report" on page 243
- "Client Summary Report" on page 243
- "Event Management" on page 243
- "Session Monitor" on page 244

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).

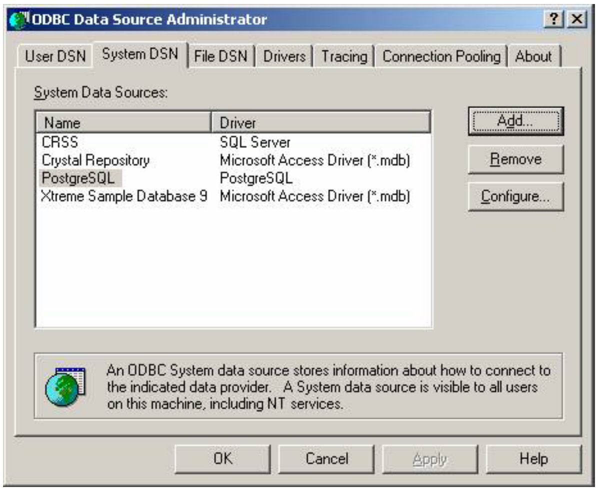
2. Open the Windows **Start** menu and select **Settings › Control Panel › Administrative Tools.**

   The Administrative Tools window appears.

3. Double-click **Data Sources (ODBC).**

   The ODBC Data Source Administrator appears.

4. Click the **System DSN** tab.



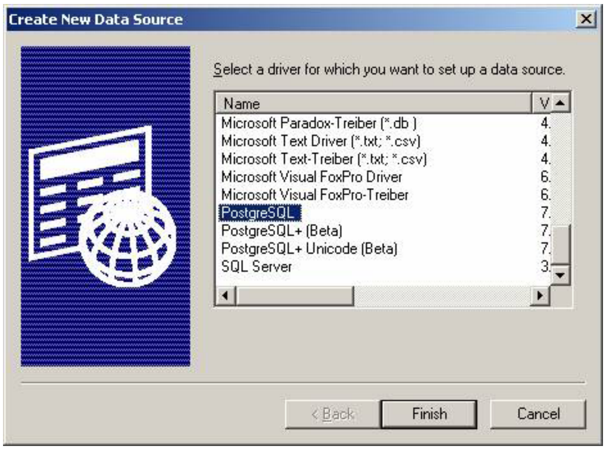
System Data Sources:

Name	Driver
CRSS	SQL Server
Crystal Repository	Microsoft Access Driver (*.mdb)
PostgreSQL	PostgreSQL
Xtreme Sample Database 9	Microsoft Access Driver (*.mdb)

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

5. Click **Add.**

   The Create New Data Source dialog box appears.

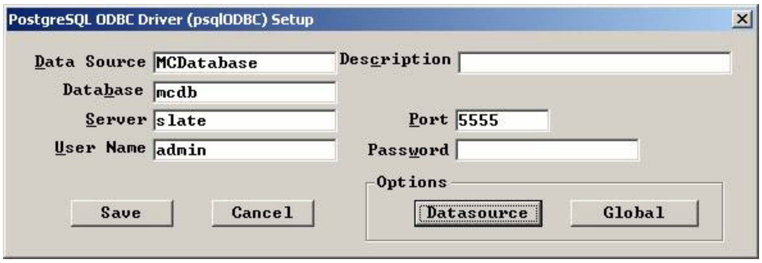


Select a driver for which you want to set up a data source.

Name	V
Microsoft Paradox-Treiber (*.db)	4.
Microsoft Text Driver (*.txt; *.csv)	4.
Microsoft Text-Treiber (*.txt; *.csv)	4.
Microsoft Visual FoxPro Driver	6.
Microsoft Visual FoxPro-Treiber	6.
PostgreSQL	7.
PostgreSQL+ (Beta)	7.
PostgreSQL+ Unicode (Beta)	7.
SQL Server	3.

6. Select the **PostgreSQL Driver** and click **Finish**.

   The PostgreSQL ODBC Driver (psqlODBC) Setup dialog box appears.



Data Source: MCDatabase
Description:
Database: mcdb
Server: slate
Port: 5555
User Name: admin
Password:

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.

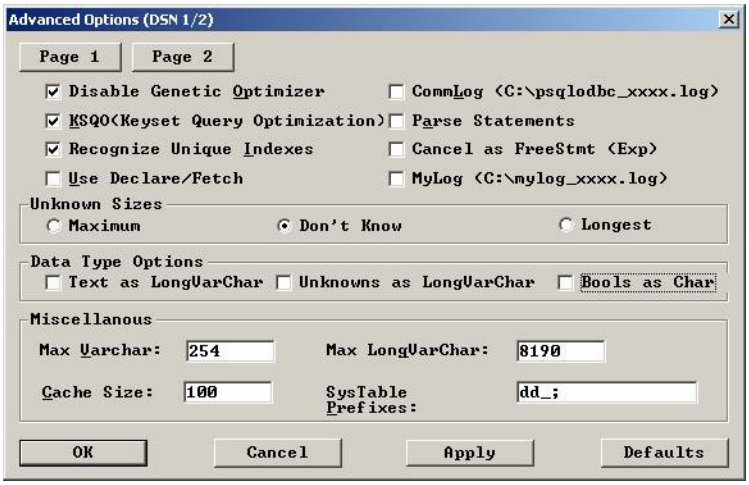
11. Leave the **Port** box set to 5555.

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.



☑ Disable Genetic Optimizer
☑ KSQO(Keyset Query Optimization)
☑ Recognize Unique Indexes
□ Use Declare/Fetch
□ CommLog (C:\psqlodbc_xxxx.log)
□ Parse Statements
□ Cancel as FreeStmt (Exp)
□ MyLog (C:\mylog_xxxx.log)

Unknown Sizes: ○ Maximum ● Don't Know ○ Longest

Data Type Options: □ Text as LongVarChar □ Unknowns as LongVarChar □ Bools as Char

Max Varchar: 254
Max LongVarChar: 8190
Cache Size: 100
SysTable Prefixes: dd_;

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 35 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 595 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 manage all client agents and plug-ins feature, which provides the mechanism for accomplishing this:

- Important terms and concepts 250
- Agents Summary view 251
- Plug-ins Summary view 252
- Adding a build record 254
- Editing version or build record settings 255
- Deleting a build record 256
- Enabling and disabling all client initiated activations 257
- Enabling and disabling all client initiated backups 258

"Avamar clients" on page 32 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 255 provides details.

Obsolete versions and builds

Any specific version (all builds) or build that is designated as obsolete is completely 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.

NOTICE

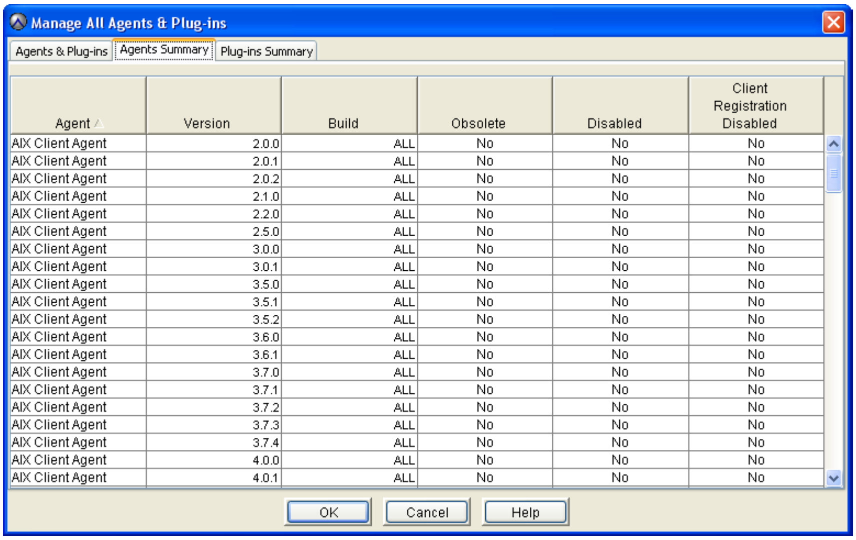
Agent versions and builds that are not supported by this version of Avamar server software are shown as obsolete. Clients with these versions or builds are completely denied access to the server and must upgrade before they can access this server. Please refer to the *EMC Avamar Compatibility and Interoperability Matrix*, available on the Avamar Support landing page: https://support.emc.com/products/Avamar.

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.



Agent	Version	Build	Obsolete	Disabled	Client Registration Disabled
AIX Client Agent	2.0.0	ALL	No	No	No
AIX Client Agent	2.0.1	ALL	No	No	No
AIX Client Agent	2.0.2	ALL	No	No	No
AIX Client Agent	2.1.0	ALL	No	No	No
AIX Client Agent	2.2.0	ALL	No	No	No
AIX Client Agent	2.5.0	ALL	No	No	No
AIX Client Agent	3.0.0	ALL	No	No	No
AIX Client Agent	3.0.1	ALL	No	No	No
AIX Client Agent	3.5.0	ALL	No	No	No
AIX Client Agent	3.5.1	ALL	No	No	No
AIX Client Agent	3.5.2	ALL	No	No	No
AIX Client Agent	3.6.0	ALL	No	No	No
AIX Client Agent	3.6.1	ALL	No	No	No
AIX Client Agent	3.7.0	ALL	No	No	No
AIX Client Agent	3.7.1	ALL	No	No	No
AIX Client Agent	3.7.2	ALL	No	No	No
AIX Client Agent	3.7.3	ALL	No	No	No
AIX Client Agent	3.7.4	ALL	No	No	No
AIX Client Agent	4.0.0	ALL	No	No	No
AIX Client Agent	4.0.1	ALL	No	No	No

The following table explains the properties for each client agent.

Table 36 Avamar agents property descriptions (page 1 of 2)

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.

Table 36 Avamar agents property descriptions (page 2 of 2)

Property	Description
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.

NOTICE

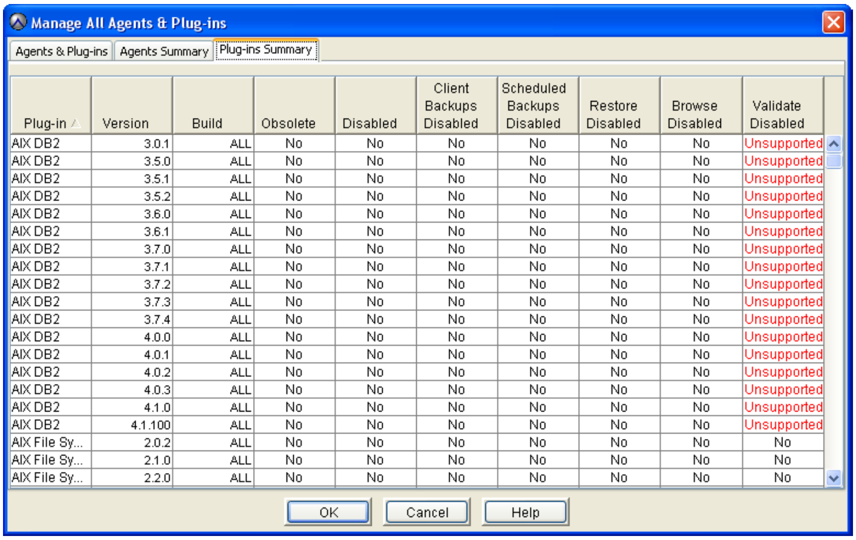
Specific plug-in versions and builds that are not supported by this version of Avamar server software are shown as obsolete. Clients with these versions or builds are completely denied access to the server and must upgrade before they can access this server. Please refer to the *EMC Avamar Compatibility and Interoperability Matrix*, available on the Avamar Support landing page: https://support.emc.com/products/Avamar.

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 37 Avamar plug-in property descriptions

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.
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.

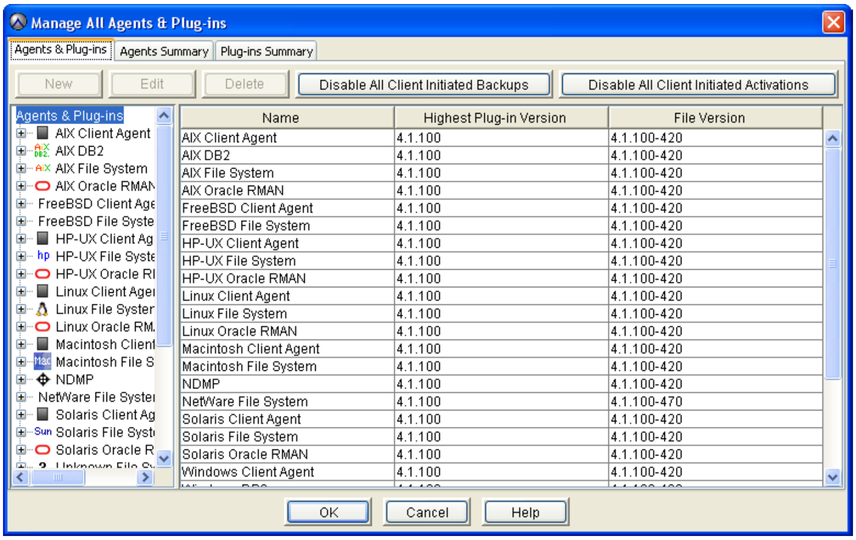
Adding a build record

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.

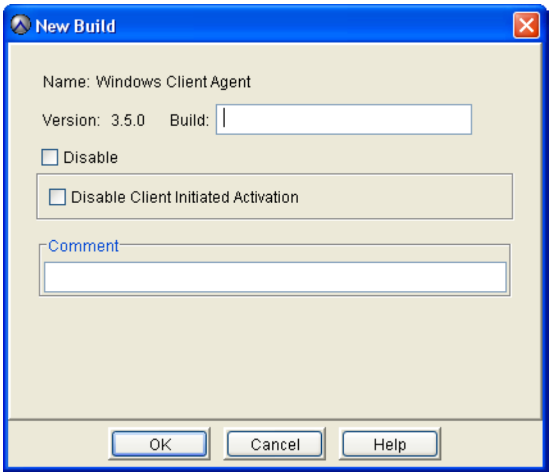


Name	Highest Plug-in Version	File Version
AIX Client Agent	4.1.100	4.1.100-420
AIX DB2	4.1.100	4.1.100-420
AIX File System	4.1.100	4.1.100-420
AIX Oracle RMAN	4.1.100	4.1.100-420
FreeBSD Client Agent	4.1.100	4.1.100-420
FreeBSD File System	4.1.100	4.1.100-420
HP-UX Client Agent	4.1.100	4.1.100-420
HP-UX File System	4.1.100	4.1.100-420
HP-UX Oracle RMAN	4.1.100	4.1.100-420
Linux Client Agent	4.1.100	4.1.100-420
Linux File System	4.1.100	4.1.100-420
Linux Oracle RMAN	4.1.100	4.1.100-420
Macintosh Client Agent	4.1.100	4.1.100-420
Macintosh File System	4.1.100	4.1.100-420
NDMP	4.1.100	4.1.100-420
NetWare File System	4.1.100	4.1.100-470
Solaris Client Agent	4.1.100	4.1.100-420
Solaris File System	4.1.100	4.1.100-420
Solaris Oracle RMAN	4.1.100	4.1.100-420
Windows Client Agent	4.1.100	4.1.100-420

2. In the tree, select the agent or plug-in version for the build.

3. Click **New.**

   The New Build dialog box appears.



Name: Windows Client Agent

Version: 3.5.0 Build:

□ Disable

□ Disable Client Initiated Activation

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.

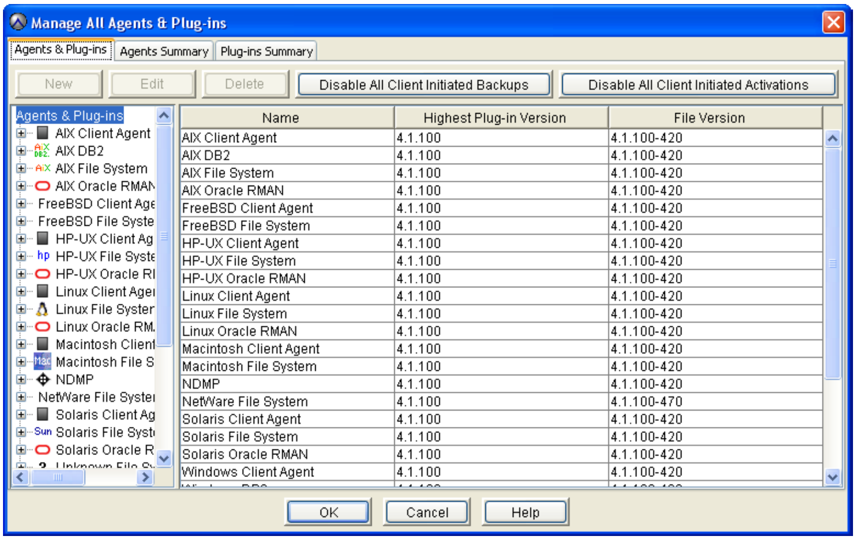
8. Click **OK**.

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.

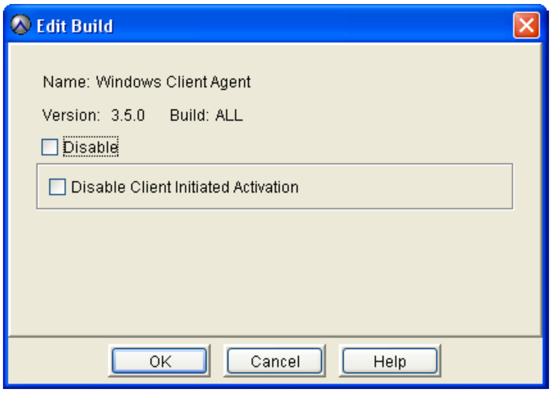


Name	Highest Plug-in Version	File Version
AIX Client Agent	4.1.100	4.1.100-420
AIX DB2	4.1.100	4.1.100-420
AIX File System	4.1.100	4.1.100-420
AIX Oracle RMAN	4.1.100	4.1.100-420
FreeBSD Client Agent	4.1.100	4.1.100-420
FreeBSD File System	4.1.100	4.1.100-420
HP-UX Client Agent	4.1.100	4.1.100-420
HP-UX File System	4.1.100	4.1.100-420
HP-UX Oracle RMAN	4.1.100	4.1.100-420
Linux Client Agent	4.1.100	4.1.100-420
Linux File System	4.1.100	4.1.100-420
Linux Oracle RMAN	4.1.100	4.1.100-420
Macintosh Client Agent	4.1.100	4.1.100-420
Macintosh File System	4.1.100	4.1.100-420
NDMP	4.1.100	4.1.100-420
NetWare File System	4.1.100	4.1.100-470
Solaris Client Agent	4.1.100	4.1.100-420
Solaris File System	4.1.100	4.1.100-420
Solaris Oracle RMAN	4.1.100	4.1.100-420
Windows Client Agent	4.1.100	4.1.100-420

2. In the tree, select the agent or plug-in version or build to edit.

3. Click **Edit**.

   The Edit Build dialog box appears.



Name: Windows Client Agent

Version: 3.5.0 Build: ALL

☐ Disable

☐ Disable Client Initiated Activation

4. Edit the build information.

   "Adding a build record" on page 254 provides details on agent and plug-in build settings.

5. Click **OK**.

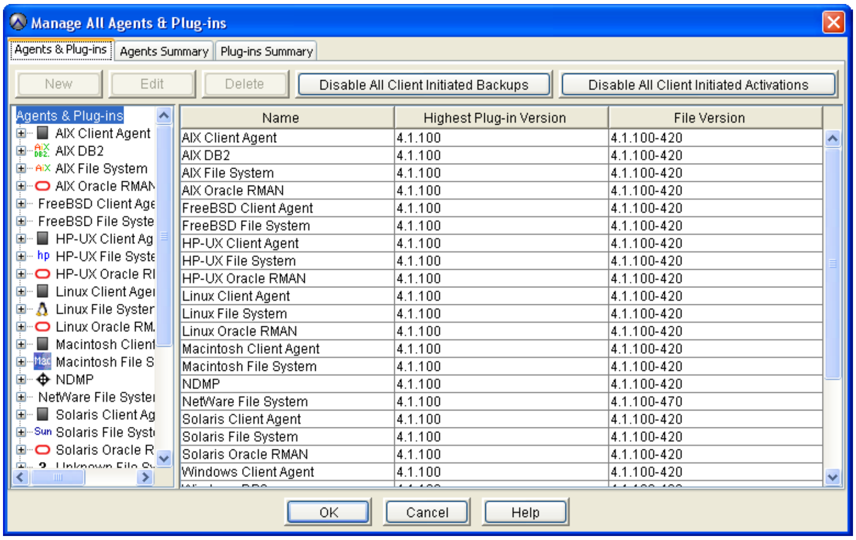
Deleting a build record

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.



Name	Highest Plug-in Version	File Version
AIX Client Agent	4.1.100	4.1.100-420
AIX DB2	4.1.100	4.1.100-420
AIX File System	4.1.100	4.1.100-420
AIX Oracle RMAN	4.1.100	4.1.100-420
FreeBSD Client Agent	4.1.100	4.1.100-420
FreeBSD File System	4.1.100	4.1.100-420
HP-UX Client Agent	4.1.100	4.1.100-420
HP-UX File System	4.1.100	4.1.100-420
HP-UX Oracle RMAN	4.1.100	4.1.100-420
Linux Client Agent	4.1.100	4.1.100-420
Linux File System	4.1.100	4.1.100-420
Linux Oracle RMAN	4.1.100	4.1.100-420
Macintosh Client Agent	4.1.100	4.1.100-420
Macintosh File System	4.1.100	4.1.100-420
NDMP	4.1.100	4.1.100-420
NetWare File System	4.1.100	4.1.100-470
Solaris Client Agent	4.1.100	4.1.100-420
Solaris File System	4.1.100	4.1.100-420
Solaris Oracle RMAN	4.1.100	4.1.100-420
Windows Client Agent	4.1.100	4.1.100-420

2. In the tree, select the agent or plug-in build to delete.

3. Click **Delete**.

Enabling and disabling all client initiated activations

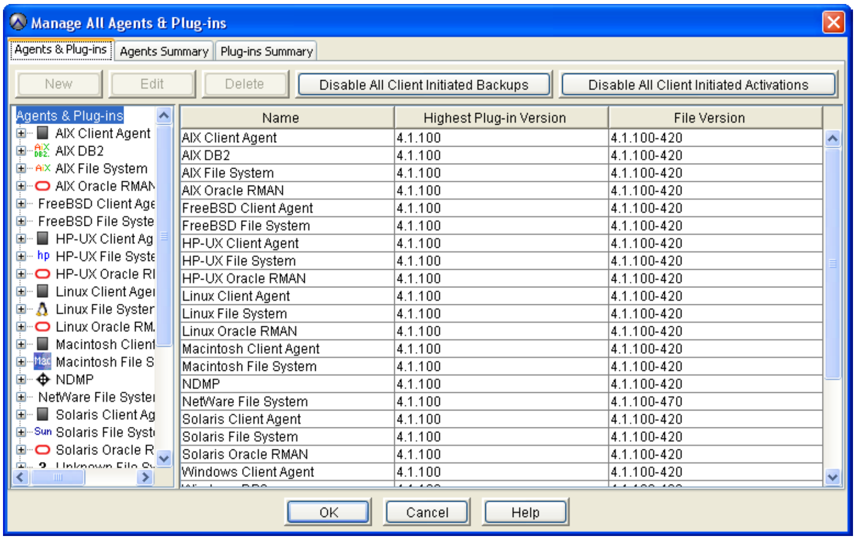
You can temporarily disable all new client initiated client activations. This is typically done to place the system in a state that supports various maintenance activities.

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.



Name	Highest Plug-in Version	File Version
AIX Client Agent	4.1.100	4.1.100-420
AIX DB2	4.1.100	4.1.100-420
AIX File System	4.1.100	4.1.100-420
AIX Oracle RMAN	4.1.100	4.1.100-420
FreeBSD Client Agent	4.1.100	4.1.100-420
FreeBSD File System	4.1.100	4.1.100-420
HP-UX Client Agent	4.1.100	4.1.100-420
HP-UX File System	4.1.100	4.1.100-420
HP-UX Oracle RMAN	4.1.100	4.1.100-420
Linux Client Agent	4.1.100	4.1.100-420
Linux File System	4.1.100	4.1.100-420
Linux Oracle RMAN	4.1.100	4.1.100-420
Macintosh Client Agent	4.1.100	4.1.100-420
Macintosh File System	4.1.100	4.1.100-420
NDMP	4.1.100	4.1.100-420
NetWare File System	4.1.100	4.1.100-470
Solaris Client Agent	4.1.100	4.1.100-420
Solaris File System	4.1.100	4.1.100-420
Solaris Oracle RMAN	4.1.100	4.1.100-420
Windows Client Agent	4.1.100	4.1.100-420

2. Click either **Enable All Client Initiated Activations** or **Disable All Client Initiated Activations.**

Enabling and disabling all client initiated backups

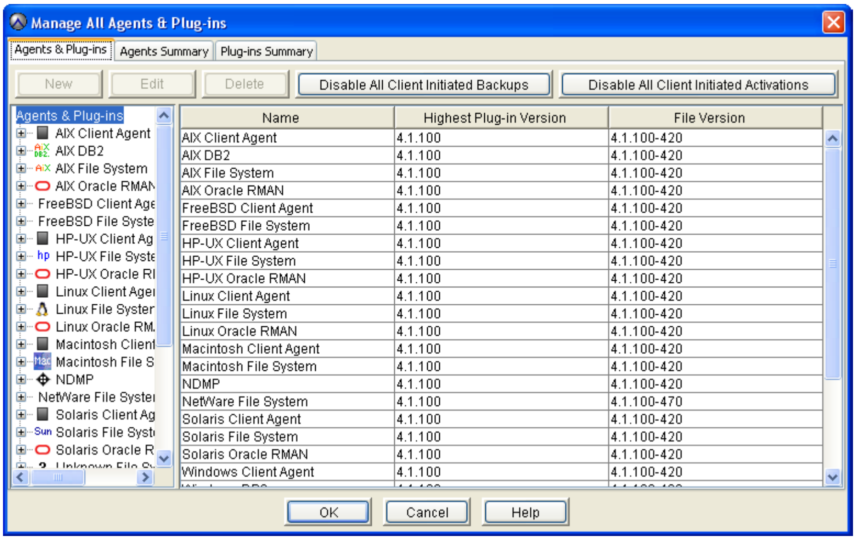
You can temporarily prevent Avamar clients from initiating on-demand backups. This is typically done to place the system in a state that supports various maintenance activities.

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.



Name	Highest Plug-in Version	File Version
AIX Client Agent	4.1.100	4.1.100-420
AIX DB2	4.1.100	4.1.100-420
AIX File System	4.1.100	4.1.100-420
AIX Oracle RMAN	4.1.100	4.1.100-420
FreeBSD Client Agent	4.1.100	4.1.100-420
FreeBSD File System	4.1.100	4.1.100-420
HP-UX Client Agent	4.1.100	4.1.100-420
HP-UX File System	4.1.100	4.1.100-420
HP-UX Oracle RMAN	4.1.100	4.1.100-420
Linux Client Agent	4.1.100	4.1.100-420
Linux File System	4.1.100	4.1.100-420
Linux Oracle RMAN	4.1.100	4.1.100-420
Macintosh Client Agent	4.1.100	4.1.100-420
Macintosh File System	4.1.100	4.1.100-420
NDMP	4.1.100	4.1.100-420
NetWare File System	4.1.100	4.1.100-470
Solaris Client Agent	4.1.100	4.1.100-420
Solaris File System	4.1.100	4.1.100-420
Solaris Oracle RMAN	4.1.100	4.1.100-420
Windows Client Agent	4.1.100	4.1.100-420

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 260
- Monitoring the server.. 260
- Verifying system integrity 275
- Viewing system events.. 276
- Filtering the Event Monitor display 278
- Viewing the Audit Log.. 281
- Filtering the Audit Log display 283
- Viewing services information.. 286
- Viewing a detailed client session log... 287
- Creating a Zip file for EMC Customer Service.. 289
- Collecting and viewing log files 290

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 38 System monitoring tools and tasks

Monitoring Tool	Monitoring Task
Activity Monitor, described on page 113	Investigate any abnormal client activity.
Server Monitor, described on page 260	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 276	Investigate any error or warning messages.
Unacknowledged Events list, described on page 296	Investigate and clear (acknowledge) any unacknowledged events.

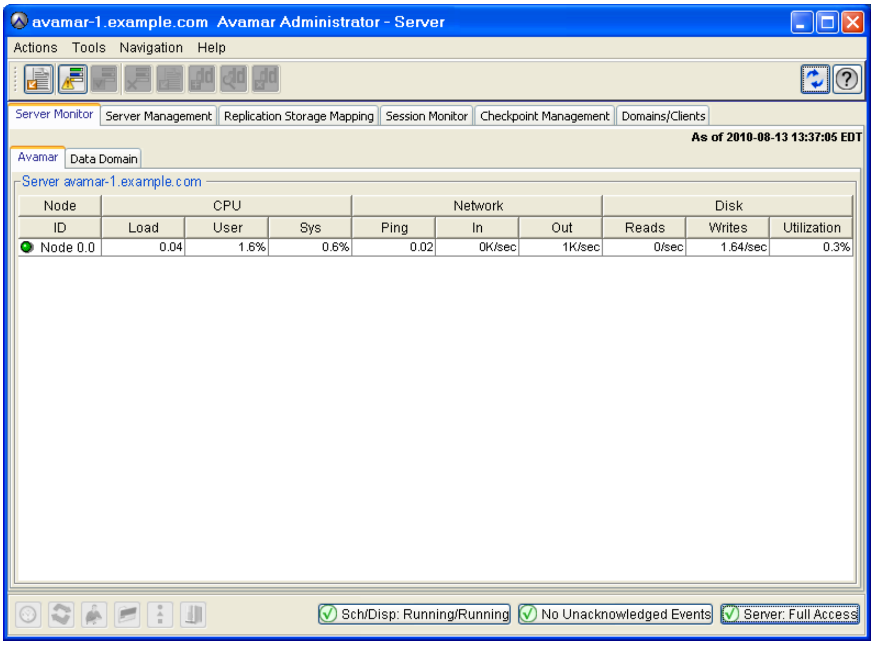
NOTICE

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 200 and "Managing ConnectEMC" on page 213 provide details.

Monitoring the server

To monitor the server, click the **Server** launcher button in Avamar Administrator.

The Server window appears.



As of 2010-08-13 13:37:05 EDT

Server avamar-1.example.com

Node	CPU			Network			Disk		
ID	Load	User	Sys	Ping	In	Out	Reads	Writes	Utilization
● Node 0.0	0.04	1.6%	0.6%	0.02	0K/sec	1K/sec	0/sec	1.64/sec	0.3%

✓ Sch/Disp: Running/Running
✓ No Unacknowledged Events
✓ Server: Full Access

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 39 Server Monitor Avamar tab properties (page 1 of 2)

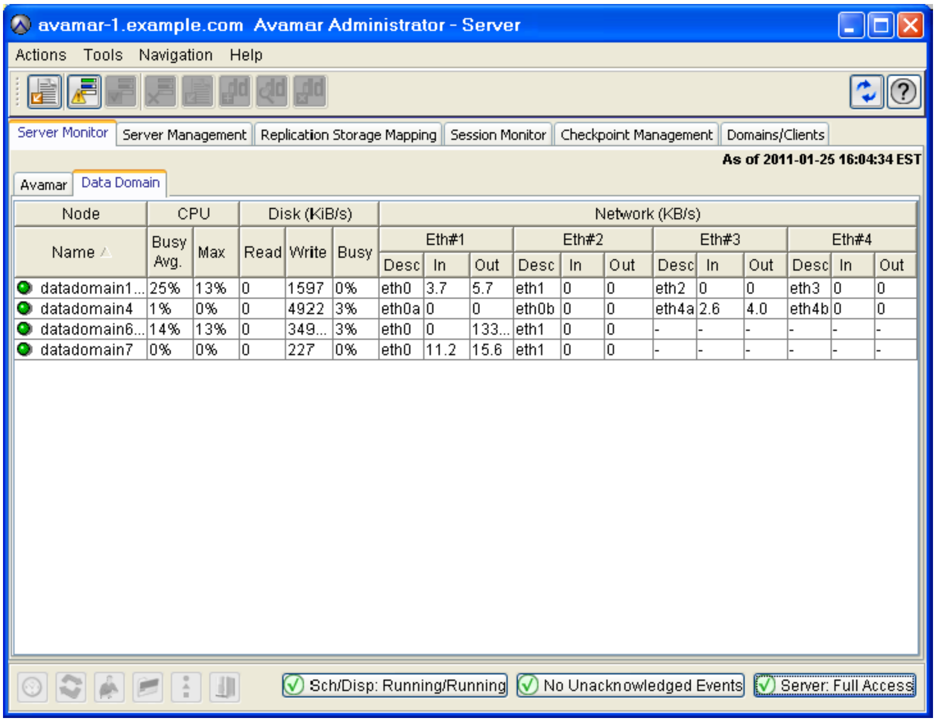
Property	Description
Node	
Status indicators	One of the following: 🟢 Online (green) — The node is functioning properly. 🔵 Read-Only (blue) — This status occurs normally as background operations are performed and when backups have been suspended. ⚪ Time-Out (gray) — MCS could not communicate with this 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. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
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.
Disk	

Table 39 Server Monitor Avamar tab properties (page 2 of 2)

Property	Description
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.

Data Domain tab

The Server Monitor Data Domain tab provides CPU, disk activity, and network activity for each node on the Data Domain system.



As of 2011-01-25 16:04:34 EST

Node	CPU		Disk (KiB/s)			Network (KB/s)											
						Eth#1			Eth#2			Eth#3			Eth#4		
Name	Busy Avg.	Max	Read	Write	Busy	Desc	In	Out	Desc	In	Out	Desc	In	Out	Desc	In	Out
● datadomain1...	25%	13%	0	1597	0%	eth0	3.7	5.7	eth1	0	0	eth2	0	0	eth3	0	0
● datadomain4	1%	0%	0	4922	3%	eth0a	0	0	eth0b	0	0	eth4a	2.6	4.0	eth4b	0	0
● datadomain6...	14%	13%	0	349...	3%	eth0	0	133...	eth1	0	0	-	-	-	-	-	-
● datadomain7	0%	0%	0	227	0%	eth0	11.2	15.6	eth1	0	0	-	-	-	-	-	-

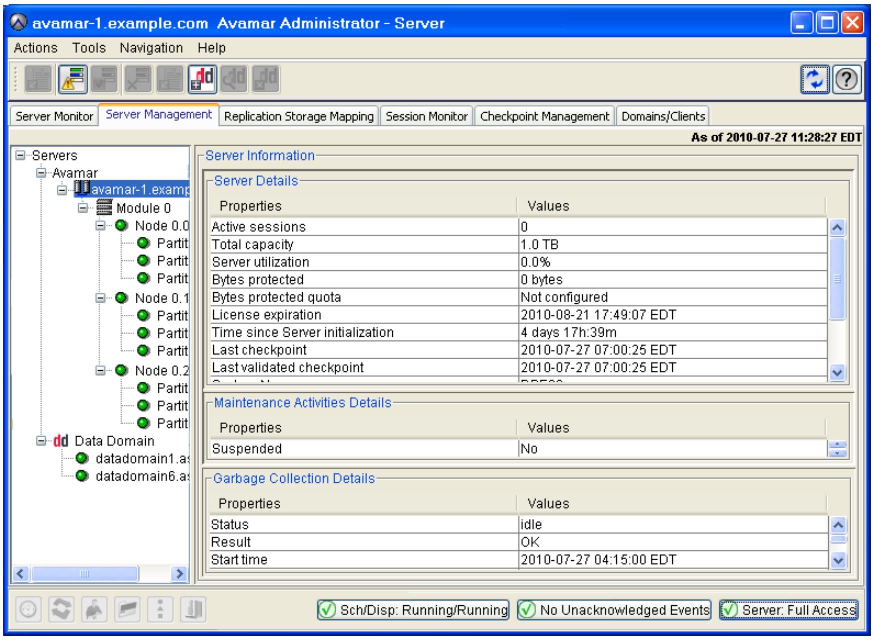
The following table describes the information available on the Server Monitor Data Domain tab.

Table 40 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. "Troubleshooting Data Domain" on page 567 provides 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.



As of 2010-07-27 11:28:27 EDT

Server Information

Server Details

Properties	Values
Active sessions	0
Total capacity	1.0 TB
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	2010-08-21 17:49:07 EDT
Time since Server initialization	4 days 17h:39m
Last checkpoint	2010-07-27 07:00:25 EDT
Last validated checkpoint	2010-07-27 07:00:25 EDT

Maintenance Activities Details

Properties	Values
Suspended	No

Garbage Collection Details

Properties	Values
Status	idle
Result	OK
Start time	2010-07-27 04:15:00 EDT

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, so “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 41 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 42 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 273 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 utilization. Actual utilization across all modules, nodes and drives might be slightly lower. "Avamar tab" on page 261 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 42 Server properties on the Server Management tab (page 2 of 2)

Property	Description
System ID	Unique identifier for this Avamar server.
HFSAddr	Hash Filesystem (HFS) address (Addr). This is the hostname or IP address that backup clients use to connect to this Avamar server.
HFSPort	Hash Filesystem (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 or blackout window). "Maintenance window" on page 295 and "Blackout window" on page 294 provide 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. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

Module information

The following table provides details on the Module properties on the Server Management tab.

Table 43 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 utilization. Actual utilization across all modules, nodes and drives might be slightly lower. "Avamar tab" on page 261 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 44 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.
Avamar server details	

Table 44 Node properties on the Server Management tab (page 2 of 3)

Property	Description
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 Filesystem (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.
Ping time (sec)	Time in seconds this node took to respond to a ping request.

Table 44 Node properties on the Server Management tab (page 3 of 3)

Property	Description
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. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
2. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

Partition information

The following table provides details on Partition properties on the Server Management tab.

Table 45 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.
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.

Table 45 Partition properties on the Server Management tab (page 2 of 2)

Property	Description
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. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
2. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

Data Domain system information

The following table provides details on the Data Domain system properties on the Server Management tab.

Table 46 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.
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.

Table 46 Data Domain system properties on the Server Management tab (page 2 of 3)

Property	Description
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. "Data Domain status and resolutions" on page 568 provides details on the available values.

Table 46 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:** “Monitoring status details” on page 572 provides 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. "Replication with Data Domain" on page 558 provides details.

Session Monitor tab

The Session Monitor tab shows a list of active client backup and restore sessions.

Table 47 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 filesystem 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 370 provides details on checkpoints. The following table provides details on the information shown on the Checkpoint Management tab.

Table 48 Checkpoint Management tab properties

Property	Description
Status indicators	One of the following: ✗ The checkpoint failed validation. ? The checkpoint has not yet been validated. R 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.

Domains/Clients tab

The Domains/Clients tab shows the nested domain structure on this server and all clients currently registered to this server. "Domains" on page 48 and "Clients" on page 52 provide details.

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 290, to ensure that no errors have occurred since that checkpoint was performed.

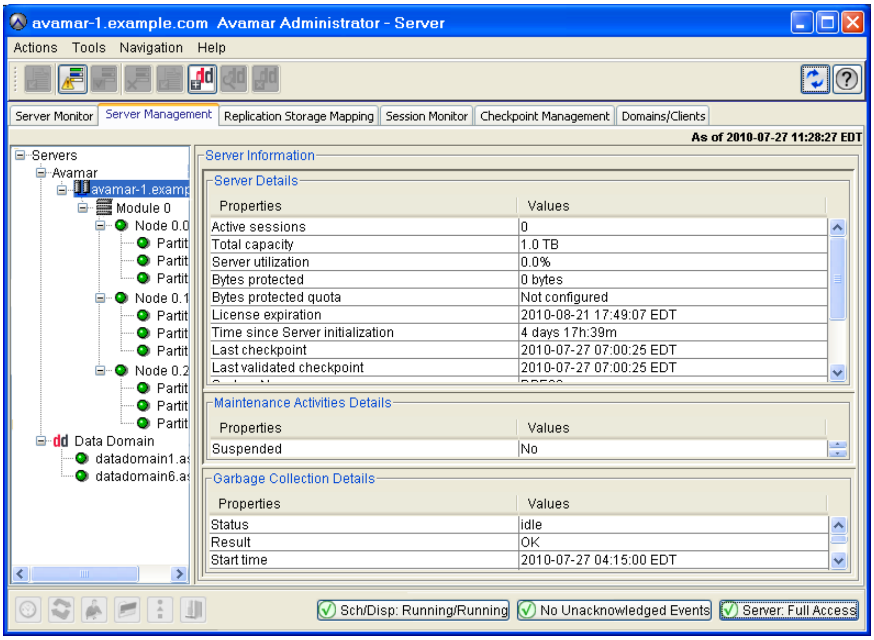
To very system integrity:

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.



As of 2010-07-27 11:28:27 EDT

Server Information

Server Details

Properties	Values
Active sessions	0
Total capacity	1.0 TB
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	2010-08-21 17:49:07 EDT
Time since Server initialization	4 days 17h:39m
Last checkpoint	2010-07-27 07:00:25 EDT
Last validated checkpoint	2010-07-27 07:00:25 EDT

Maintenance Activities Details

Properties	Values
Suspended	No

Garbage Collection Details

Properties	Values
Status	idle
Result	OK
Start time	2010-07-27 04:15:00 EDT

4. Verify that the **Last validated checkpoint** field shows a recent calendar date.

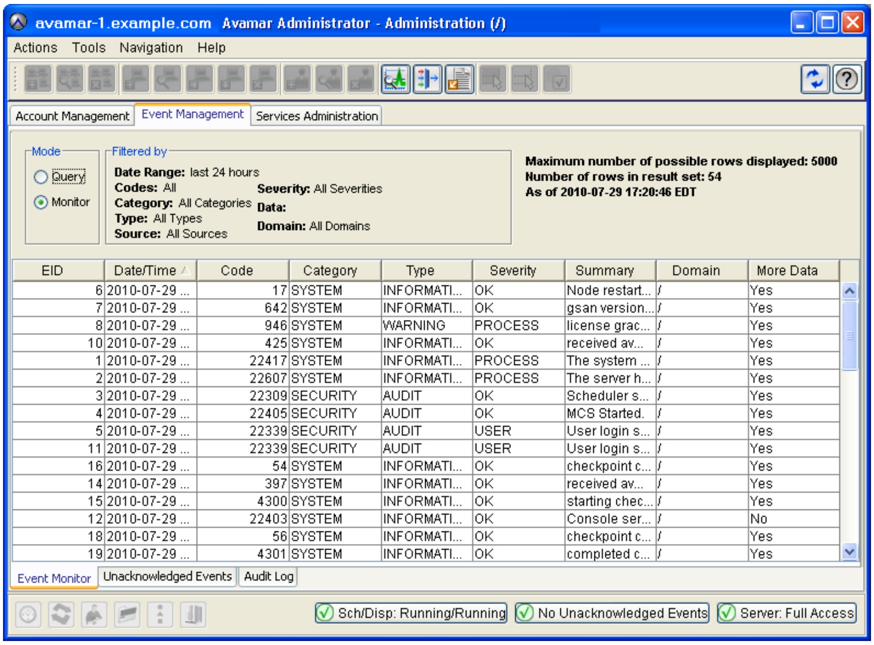
Viewing system events

To view system events:

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

   The Administration window appears.

2. Click the **Event Management** tab.



Mode
○ Query
● Monitor

Filtered by
Date Range: last 24 hours
Codes: All
Category: All Categories
Type: All Types
Source: All Sources
Severity: All Severities
Data:
Domain: All Domains

Maximum number of possible rows displayed: 5000
Number of rows in result set: 54
As of 2010-07-29 17:20:46 EDT

EID	Date/Time	Code	Category	Type	Severity	Summary	Domain	More Data
6	2010-07-29 ...	17	SYSTEM	INFORMATI...	OK	Node restart...	/	Yes
7	2010-07-29 ...	642	SYSTEM	INFORMATI...	OK	gsan version...	/	Yes
8	2010-07-29 ...	946	SYSTEM	WARNING	PROCESS	license grac...	/	Yes
10	2010-07-29 ...	425	SYSTEM	INFORMATI...	OK	received av...	/	Yes
1	2010-07-29 ...	22417	SYSTEM	INFORMATI...	PROCESS	The system ...	/	Yes
2	2010-07-29 ...	22607	SYSTEM	INFORMATI...	PROCESS	The server h...	/	Yes
3	2010-07-29 ...	22309	SECURITY	AUDIT	OK	Scheduler s...	/	Yes
4	2010-07-29 ...	22405	SECURITY	AUDIT	OK	MCS Started.	/	Yes
5	2010-07-29 ...	22339	SECURITY	AUDIT	USER	User login s...	/	Yes
11	2010-07-29 ...	22339	SECURITY	AUDIT	USER	User login s...	/	Yes
16	2010-07-29 ...	54	SYSTEM	INFORMATI...	OK	checkpoint c...	/	Yes
14	2010-07-29 ...	397	SYSTEM	INFORMATI...	OK	received av...	/	Yes
15	2010-07-29 ...	4300	SYSTEM	INFORMATI...	OK	starting chec...	/	Yes
12	2010-07-29 ...	22403	SYSTEM	INFORMATI...	OK	Console ser...	/	No
18	2010-07-29 ...	56	SYSTEM	INFORMATI...	OK	checkpoint c...	/	Yes
19	2010-07-29 ...	4301	SYSTEM	INFORMATI...	OK	completed c...	/	Yes

✓ Sch/Disp: Running/Running ✓ No Unacknowledged Events ✓ Server: Full Access

   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 278 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 278 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 49 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 49 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

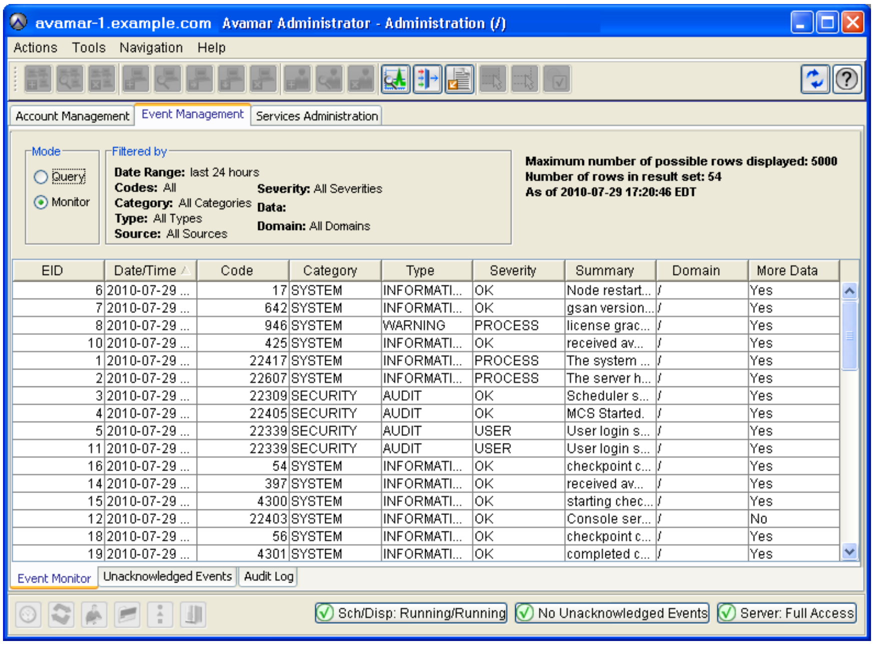
To filter the Event Monitor display:

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.



Mode
○ Query
● Monitor

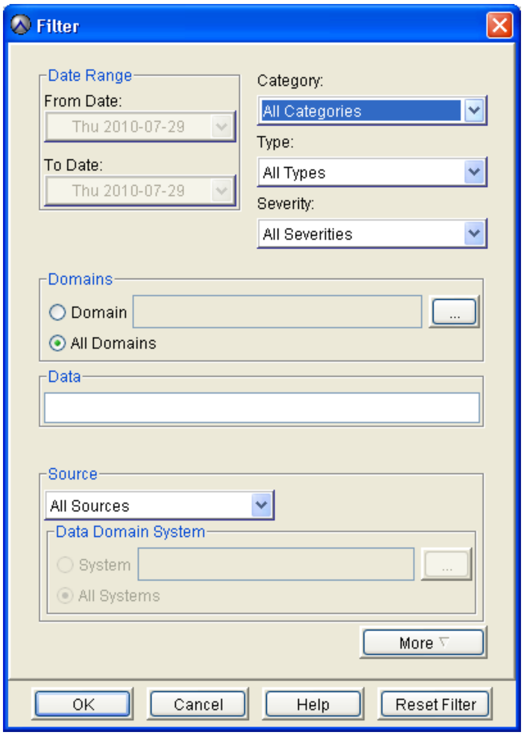
Filtered by
Date Range: last 24 hours
Codes: All
Category: All Categories
Type: All Types
Source: All Sources
Severity: All Severities
Data:
Domain: All Domains

Maximum number of possible rows displayed: 5000
Number of rows in result set: 54
As of 2010-07-29 17:20:46 EDT

EID	Date/Time	Code	Category	Type	Severity	Summary	Domain	More Data
6	2010-07-29 ...	17	SYSTEM	INFORMATI...	OK	Node restart...	/	Yes
7	2010-07-29 ...	642	SYSTEM	INFORMATI...	OK	gsan version...	/	Yes
8	2010-07-29 ...	946	SYSTEM	WARNING	PROCESS	license grac...	/	Yes
10	2010-07-29 ...	425	SYSTEM	INFORMATI...	OK	received av...	/	Yes
1	2010-07-29 ...	22417	SYSTEM	INFORMATI...	PROCESS	The system ...	/	Yes
2	2010-07-29 ...	22607	SYSTEM	INFORMATI...	PROCESS	The server h...	/	Yes
3	2010-07-29 ...	22309	SECURITY	AUDIT	OK	Scheduler s...	/	Yes
4	2010-07-29 ...	22405	SECURITY	AUDIT	OK	MCS Started.	/	Yes
5	2010-07-29 ...	22339	SECURITY	AUDIT	USER	User login s...	/	Yes
11	2010-07-29 ...	22339	SECURITY	AUDIT	USER	User login s...	/	Yes
16	2010-07-29 ...	54	SYSTEM	INFORMATI...	OK	checkpoint c...	/	Yes
14	2010-07-29 ...	397	SYSTEM	INFORMATI...	OK	received av...	/	Yes
15	2010-07-29 ...	4300	SYSTEM	INFORMATI...	OK	starting chec...	/	Yes
12	2010-07-29 ...	22403	SYSTEM	INFORMATI...	OK	Console ser...	/	No
18	2010-07-29 ...	56	SYSTEM	INFORMATI...	OK	checkpoint c...	/	Yes
19	2010-07-29 ...	4301	SYSTEM	INFORMATI...	OK	completed c...	/	Yes

4. Open the **Actions** menu and select **Event Management › Filter.**

The Filter dialog box appears.



From Date: Thu 2010-07-29

To Date: Thu 2010-07-29

Category: All Categories

Type: All Types

Severity: All Severities

○ Domain

● All Domains

All Sources

○ System

● All Systems

5. Define one or more of the filtering criteria described in the following table.

Table 50 Event Monitor filtering criteria (page 1 of 3)

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 50 Event Monitor filtering criteria (page 2 of 3)

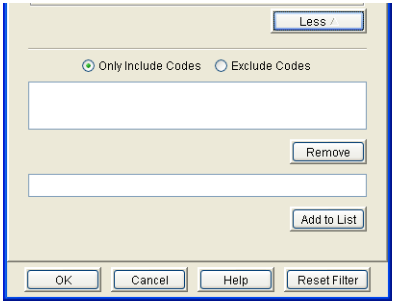
Setting	Description
Severity	Display events of the following severities: • All Severities • OK • USER • PROCESS • NODE • USER_FATAL • PROCESS_FATAL • NODE_FATAL • SYSTEM_FATAL
Domains	Select the All Domains option to display all events from all domains. To only show events from one domain, select the 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, as shown in the following figure.  Less ● Only Include Codes ○ Exclude Codes Remove Add to List OK Cancel Help Reset Filter 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).

Table 50 Event Monitor filtering criteria (page 3 of 3)

Setting	Description
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

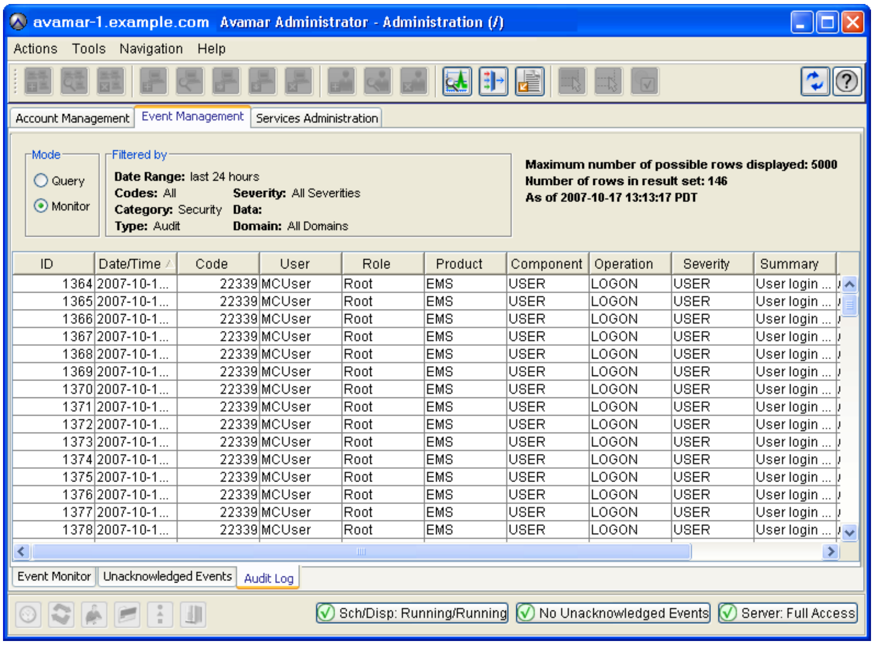
To view the Audit log:

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.



Mode

○ Query

● Monitor

Filtered by

Date Range: last 24 hours
Codes: All **Severity:** All Severities
Category: Security **Data:**
Type: Audit **Domain:** All Domains

Maximum number of possible rows displayed: 5000
Number of rows in result set: 146
As of 2007-10-17 13:13:17 PDT

ID	Date/Time	Code	User	Role	Product	Component	Operation	Severity	Summary
1364	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1365	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1366	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1367	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1368	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1369	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1370	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1371	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1372	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1373	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1374	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1375	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1376	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1377	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1378	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...

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 283 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 283 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 51 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.
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

Table 51 Audit Log column information (page 2 of 2)

Column	Description
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

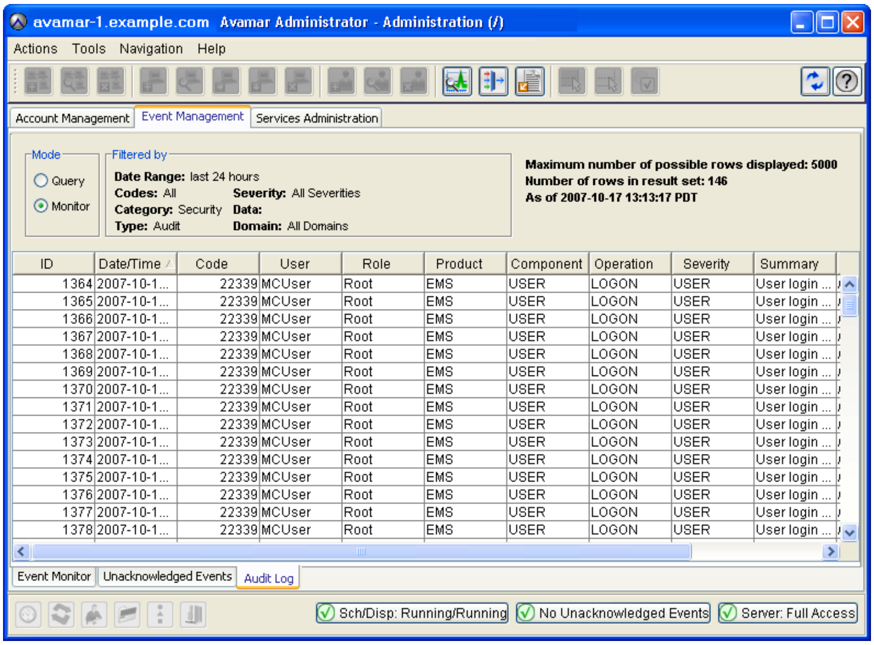
To filter the Audit Log display:

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.



Mode
○ Query
● Monitor

Filtered by
Date Range: last 24 hours
Codes: All **Severity:** All Severities
Category: Security **Data:**
Type: Audit **Domain:** All Domains

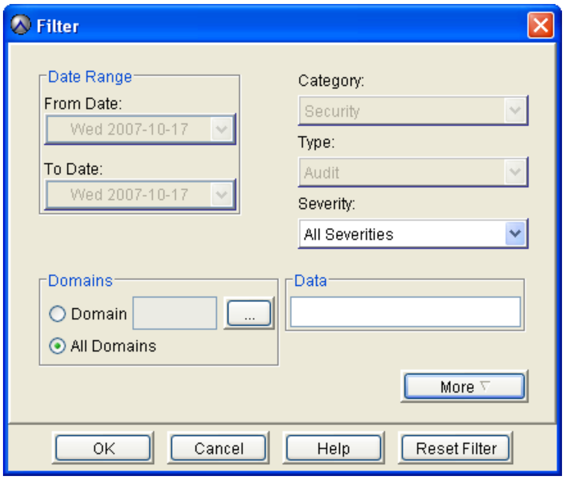
Maximum number of possible rows displayed: 5000
Number of rows in result set: 146
As of 2007-10-17 13:13:17 PDT

ID	Date/Time	Code	User	Role	Product	Component	Operation	Severity	Summary
1364	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1365	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1366	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1367	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1368	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1369	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1370	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1371	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1372	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1373	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1374	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1375	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1376	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1377	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...
1378	2007-10-1...	22339	MCUser	Root	EMS	USER	LOGON	USER	User login ...

✓ Sch/Disp: Running/Running ✓ No Unacknowledged Events ✓ Server: Full Access

4. Open the **Actions** menu and select **Event Management › Filter.**

The Filter dialog box appears.



From Date: Wed 2007-10-17

To Date: Wed 2007-10-17

Category: Security

Type: Audit

Severity: All Severities

○ Domain

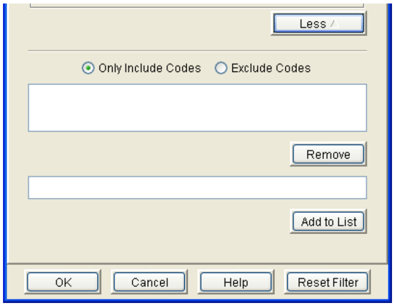
● All Domains

5. Define one or more of the filtering criteria listed in the following table.

Table 52 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).

Table 52 Audit Log filter criteria (page 2 of 2)

Setting	Description
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, as shown in the following figure.  Less Remove Add to List OK Cancel Help Reset Filter ● Only Include Codes ○ Exclude Codes 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).
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**.

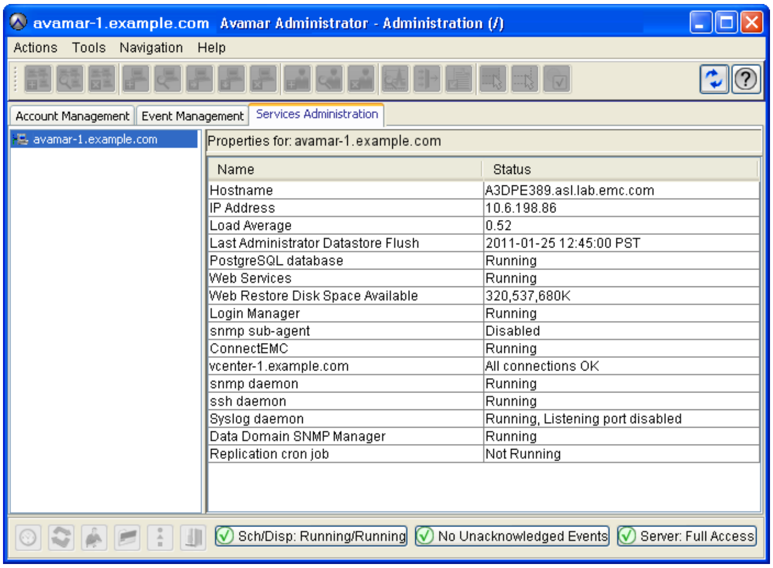
Viewing services information

To view services information:

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

   The Administration window appears.

2. Click the **Services Administration** tab.



Properties for: avamar-1.example.com

Name	Status
Hostname	A3DPE389.asl.lab.emc.com
IP Address	10.6.198.86
Load Average	0.52
Last Administrator Datastore Flush	2011-01-25 12:45:00 PST
PostgreSQL database	Running
Web Services	Running
Web Restore Disk Space Available	320,537,680K
Login Manager	Running
snmp sub-agent	Disabled
ConnectEMC	Running
vcenter-1.example.com	All connections OK
snmp daemon	Running
ssh daemon	Running
Syslog daemon	Running, Listening port disabled
Data Domain SNMP Manager	Running
Replication cron job	Not Running

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 53 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.
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.

Table 53 Services Administration tab properties (page 2 of 2)

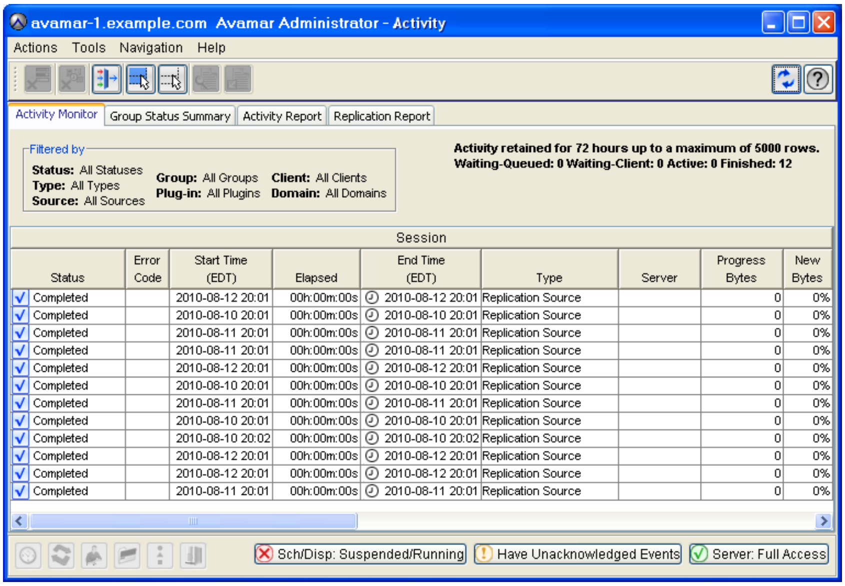
Service Name	Description
VMware vCenter Connection Monitor	Status of the VMware vCenter connections. This service is only present if a vCenter client has been added to the system. The *EMC Avamar for VMware User Guide* provides additional information.
snmp daemon	Status of the Avamar SNMP master agent 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 353 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.



Filtered by

Status: All Statuses **Group:** All Groups **Client:** All Clients
Type: All Types **Plug-in:** All Plugins **Domain:** All Domains
Source: All Sources

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

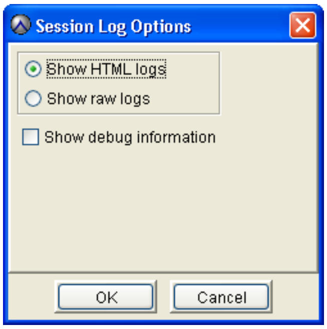
Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

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.

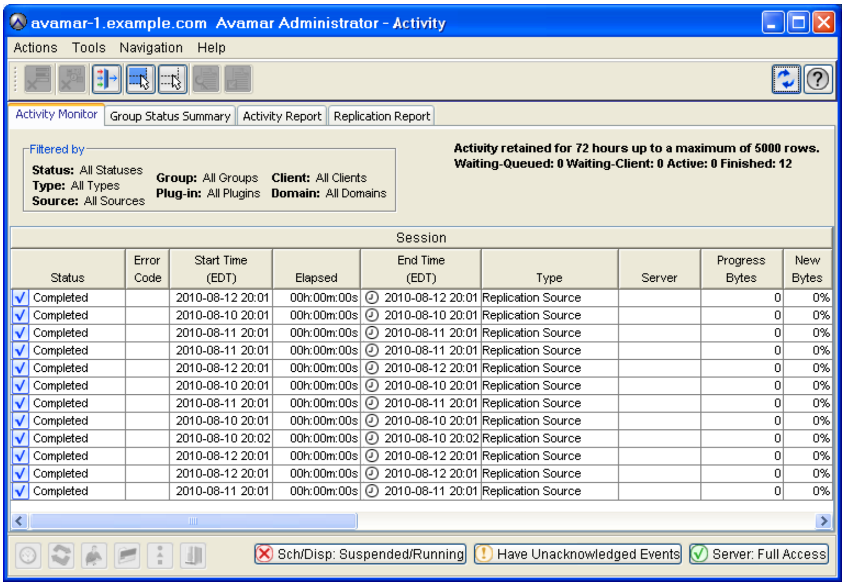
Creating a Zip file for EMC Customer Service

The **Activity** window enables you to create a Zip file for EMC Customer Service 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.



Status: All Statuses
Type: All Types
Source: All Sources
Group: All Groups
Plug-in: All Plugins
Client: All Clients
Domain: All Domains

Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

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 .

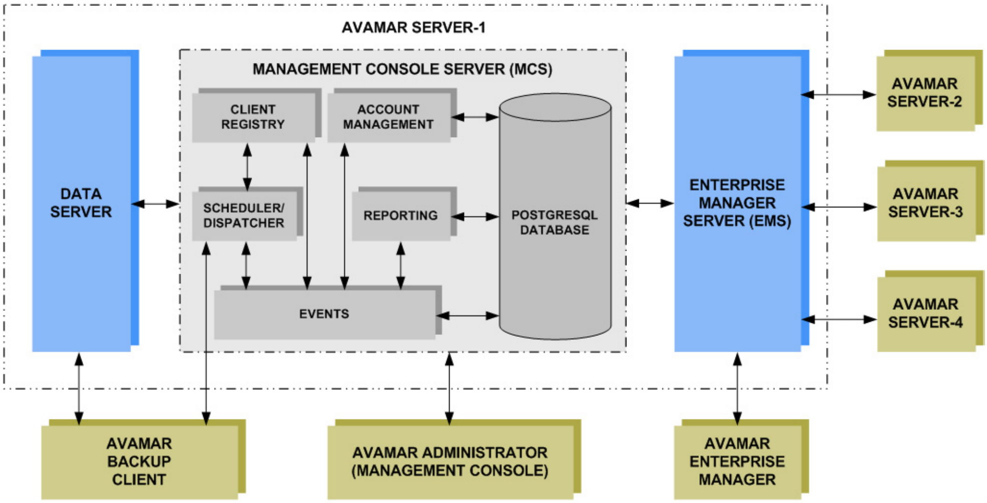
CHAPTER 11
Basic Server Administration

The following topics discuss basic Avamar server administrative concepts and tasks:

- Avamar server functional block diagram 292
- Avamar server maintenance activities and backup/maintenance windows 293
- Acknowledging system events........ 296
- Suspending and resuming backups and restores 297
- Suspending and resuming scheduled operations 298
- Enabling and disabling scheduled group backups 298
- Suspending and resuming maintenance activities........ 299
- Changing backup/maintenance window settings........ 300
- Managing services 301
- Canceling a client session 302
- Resetting a client 303

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 52 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 276 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 Service. 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 311 provides details.

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:

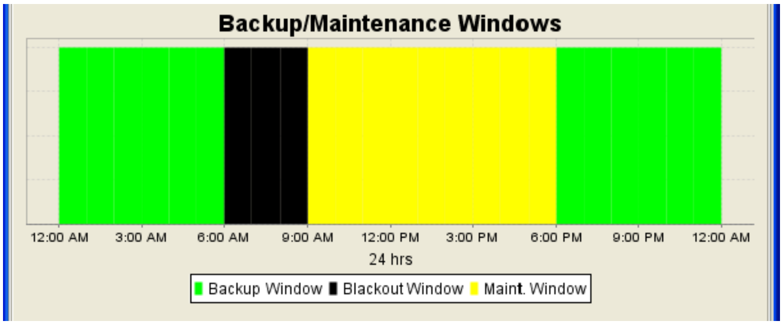
- **Checkpoint** — A checkpoint is a snapshot of the Avamar server taken for the express purpose of facilitating server rollbacks.
- **Checkpoint validation** (also known as HFS check) — A Hash Filesystem check (also known as HFS check) is an internal operation that validates the integrity of a specific 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 three operational windows, during which various system activities are performed:

- Backup window
- Blackout window
- Maintenance window

The following figure shows the default backup, blackout, and maintenance windows.



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 10 hours until 6 a.m. the following morning. You can customize the backup window start time and duration.

Blackout window

The blackout window is that portion of each day reserved to perform server maintenance activities, primarily Garbage Collection, that require unrestricted access to the server. No backup or administrative activities are allowed during the blackout window. You can, however, perform restores.

The default blackout window begins at 6 a.m. local server time and continues uninterrupted for 4 hours until 10 a.m. that same morning. You can customize the blackout window duration. However, any changes to the blackout window duration also affect maintenance window duration. For example, changing the blackout window duration from 4 hours to 3 hours extends the maintenance window duration 1 hour because it begins 1 hour earlier. The backup window is not affected.

NOTICE

Setting the blackout window duration too short might adversely impact the server's ability to recover storage space from deleted or expired backups. If you shorten the blackout window duration, closely monitor server capacity utilization and forecasting on a regular basis (at least weekly) to ensure that adequate garbage collection is taking place. "Capacity Management" on page 341 provides details.

Maintenance window

The maintenance window is that portion of each day reserved to perform routine server maintenance activities, primarily checkpoint creation and validation.There might be brief periods of time when backup or administrative activities are not allowed. Although backups can be initiated during the maintenance window, doing so impacts both the backup and maintenance activities. For this reason, minimize any backup or administrative activities during the maintenance window. You can, however, perform restores.

The default maintenance window begins at 10 a.m. local server time and continues uninterrupted for 10 hours until 8 p.m. Although you cannot directly customize the maintenance window, its start time and duration are derived from backup and blackout window settings (that is, it starts immediately after the blackout window and continues until the backup window start time).

Best practices

Review the following scheduling best practices:

- **Do not schedule backups close to or during the blackout window**

  To ensure that all morning maintenance activities complete in a timely manner, do not schedule any group backups close to or during the blackout window (6-10 a.m. local time for most systems).

- **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 (10 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.

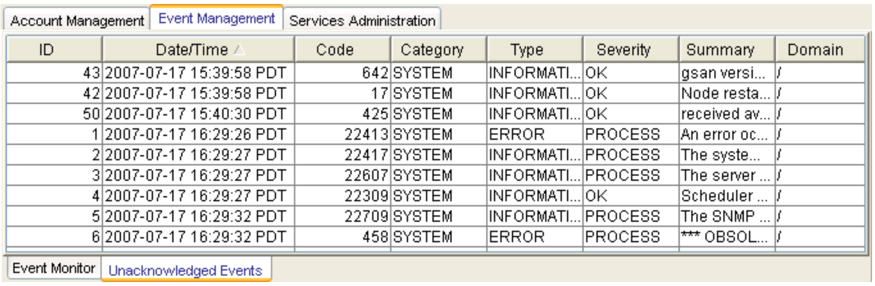
To acknowledge system events:

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.



ID	Date/Time	Code	Category	Type	Severity	Summary	Domain
43	2007-07-17 15:39:58 PDT	642	SYSTEM	INFORMATI...	OK	gsan versi...	/
42	2007-07-17 15:39:58 PDT	17	SYSTEM	INFORMATI...	OK	Node resta...	/
50	2007-07-17 15:40:30 PDT	425	SYSTEM	INFORMATI...	OK	received av...	/
1	2007-07-17 16:29:26 PDT	22413	SYSTEM	ERROR	PROCESS	An error oc...	/
2	2007-07-17 16:29:27 PDT	22417	SYSTEM	INFORMATI...	PROCESS	The syste...	/
3	2007-07-17 16:29:27 PDT	22607	SYSTEM	INFORMATI...	PROCESS	The server ...	/
4	2007-07-17 16:29:27 PDT	22309	SYSTEM	INFORMATI...	OK	Scheduler ...	/
5	2007-07-17 16:29:32 PDT	22709	SYSTEM	INFORMATI...	PROCESS	The SNMP ...	/
6	2007-07-17 16:29:32 PDT	458	SYSTEM	ERROR	PROCESS	*** OBSOL...	/

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.

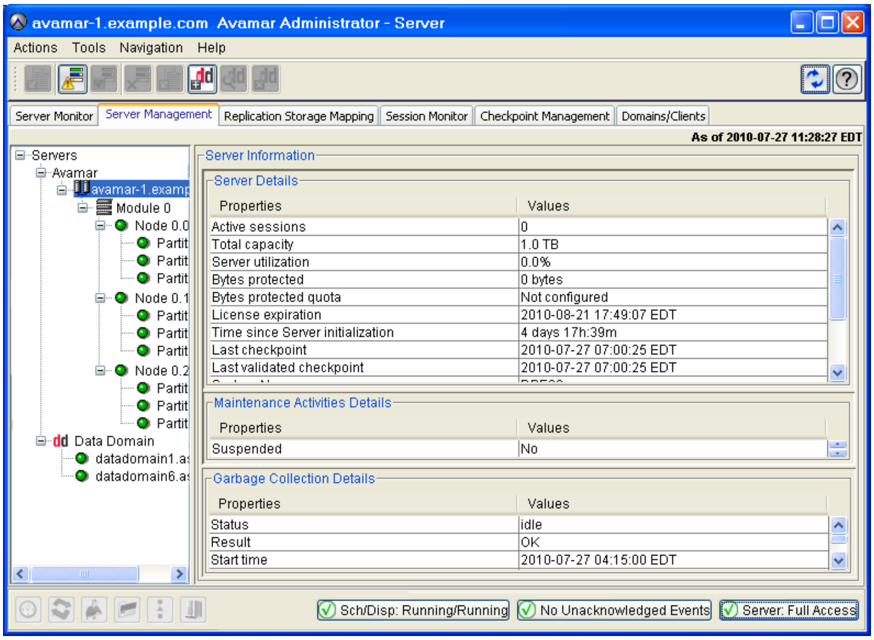
Suspending and resuming backups and restores

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.



As of 2010-07-27 11:28:27 EDT

Server Information

Server Details

Properties	Values
Active sessions	0
Total capacity	1.0 TB
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	2010-08-21 17:49:07 EDT
Time since Server initialization	4 days 17h:39m
Last checkpoint	2010-07-27 07:00:25 EDT
Last validated checkpoint	2010-07-27 07:00:25 EDT

Maintenance Activities Details

Properties	Values
Suspended	No

Garbage Collection Details

Properties	Values
Status	idle
Result	OK
Start time	2010-07-27 04:15:00 EDT

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.

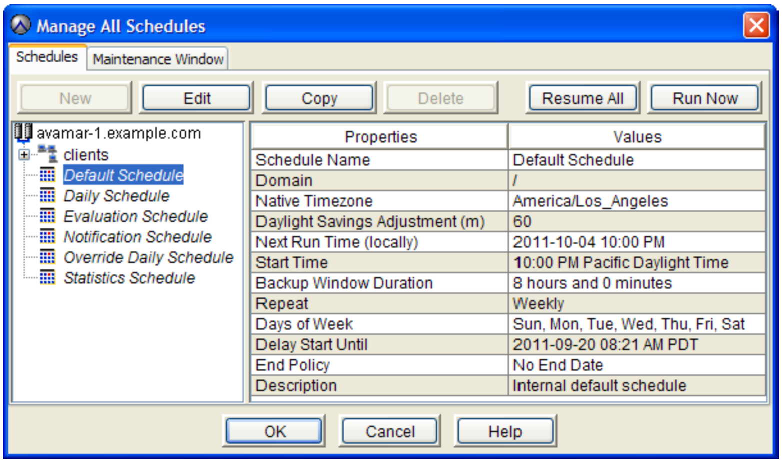
5. Click **Yes.**

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.



Properties	Values
Schedule Name	Default Schedule
Domain	/
Native Timezone	America/Los_Angeles
Daylight Savings Adjustment (m)	60
Next Run Time (locally)	2011-10-04 10:00 PM
Start Time	10:00 PM Pacific Daylight Time
Backup Window Duration	8 hours and 0 minutes
Repeat	Weekly
Days of Week	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Delay Start Until	2011-09-20 08:21 AM PDT
End Policy	No End Date
Description	Internal default schedule

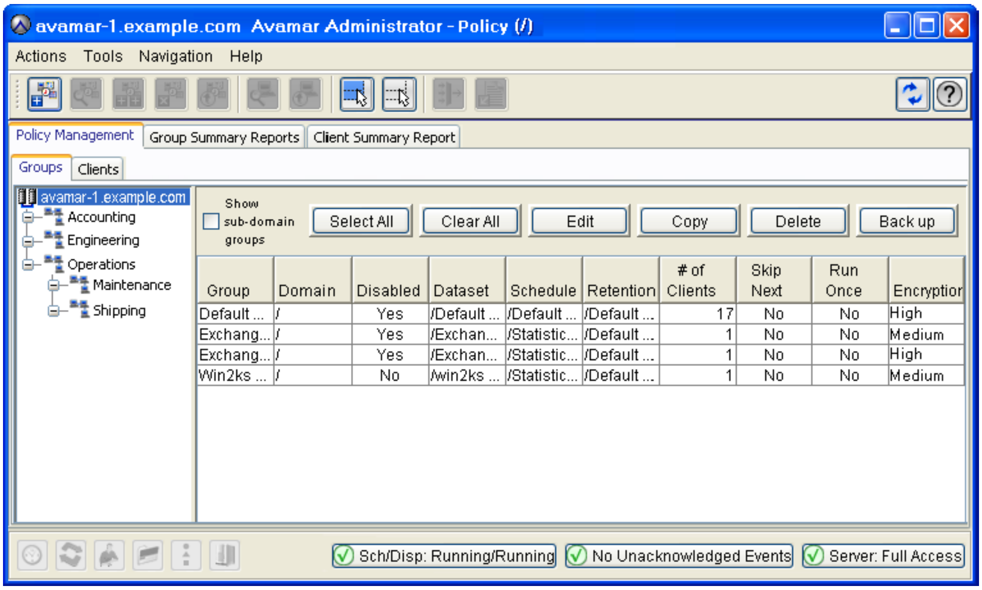
2. Click **Suspend All** or **Resume All.**

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.



Group	Domain	Disabled	Dataset	Schedule	Retention	# of Clients	Skip Next	Run Once	Encryption
Default ...	/	Yes	/Default ...	/Default ...	/Default ...	17	No	No	High
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	Medium
Exchang...	/	Yes	/Exchan...	/Statistic...	/Default ...	1	No	No	High
Win2ks ...	/	No	/win2ks ...	/Statistic...	/Default ...	1	No	No	Medium

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.

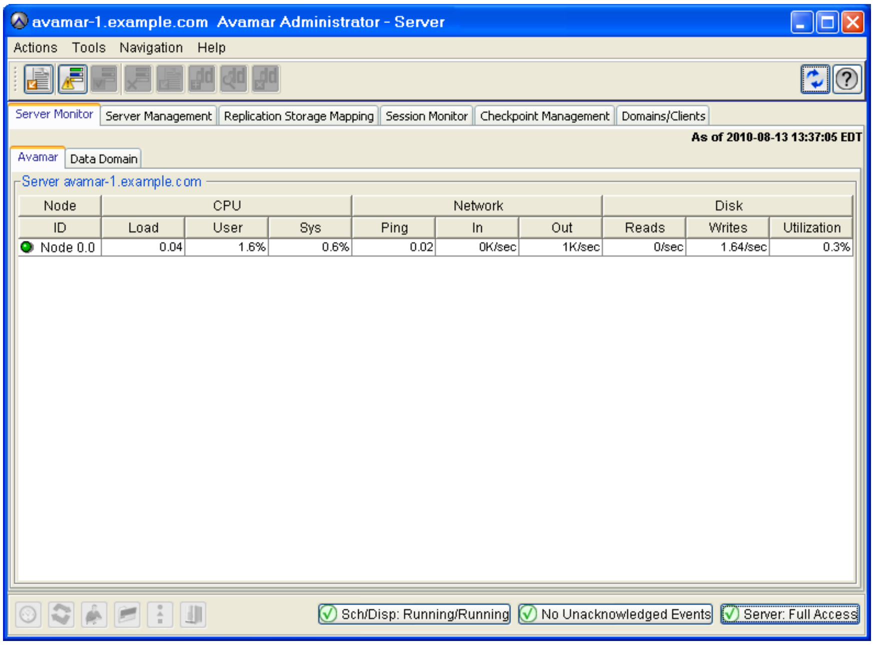
6. Click **Yes**.

Suspending and resuming maintenance activities

To suspend and resume maintenance activities:

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

   The Server window appears.



As of 2010-08-13 13:37:05 EDT

Server avamar-1.example.com

Node	CPU			Network			Disk		
ID	Load	User	Sys	Ping	In	Out	Reads	Writes	Utilization
● Node 0.0	0.04	1.6%	0.6%	0.02	0K/sec	1K/sec	0/sec	1.64/sec	0.3%

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
- Blackout window duration
- Time zone

Any changes to blackout window duration also affect maintenance window duration. For example, changing the blackout window duration from 4 hours to 3 hours extends the maintenance window duration 1 hour because it begins 1 hour earlier.

NOTICE

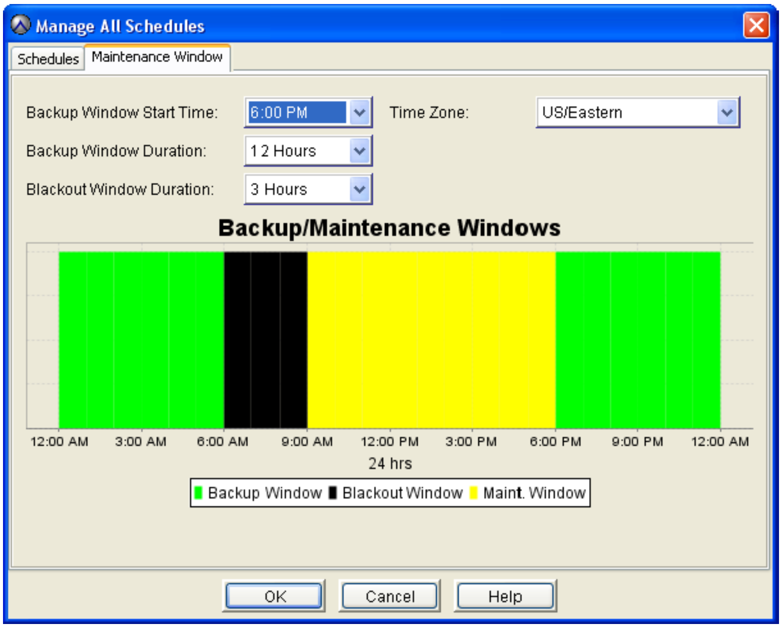
Setting the blackout window duration too short might adversely impact the server's ability to recover storage space from deleted or expired backups. If you shorten the blackout window duration, closely monitor server capacity utilization and forecasting on a regular basis (at least weekly) to ensure that adequate garbage collection is taking place. "Capacity Management" on page 341 provides details.

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.



Manage All Schedules

Backup Window Start Time: 6:00 PM

Time Zone: US/Eastern

Backup Window Duration: 12 Hours

Blackout Window Duration: 3 Hours

3. Change the backup window start time or duration, blackout window duration, or time zone by selecting a new value from the corresponding list.

4. Click **OK**.

Managing services

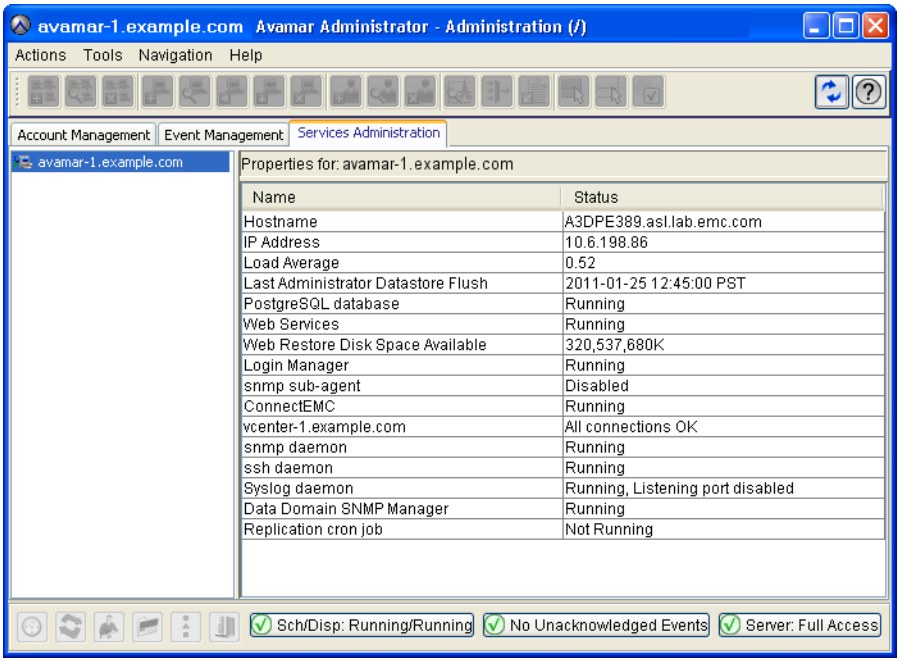
The Administration window Services Administration tab enables you to start, stop, suspend, or resume individual services.

To manage services:

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

   The Administration window appears.

2. Click the **Services Administration** tab.



Properties for: avamar-1.example.com

Name	Status
Hostname	A3DPE389.asl.lab.emc.com
IP Address	10.6.198.86
Load Average	0.52
Last Administrator Datastore Flush	2011-01-25 12:45:00 PST
PostgreSQL database	Running
Web Services	Running
Web Restore Disk Space Available	320,537,680K
Login Manager	Running
snmp sub-agent	Disabled
ConnectEMC	Running
vcenter-1.example.com	All connections OK
snmp daemon	Running
ssh daemon	Running
Syslog daemon	Running, Listening port disabled
Data Domain SNMP Manager	Running
Replication cron job	Not Running

3. Manage the servicez’

   - 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**.

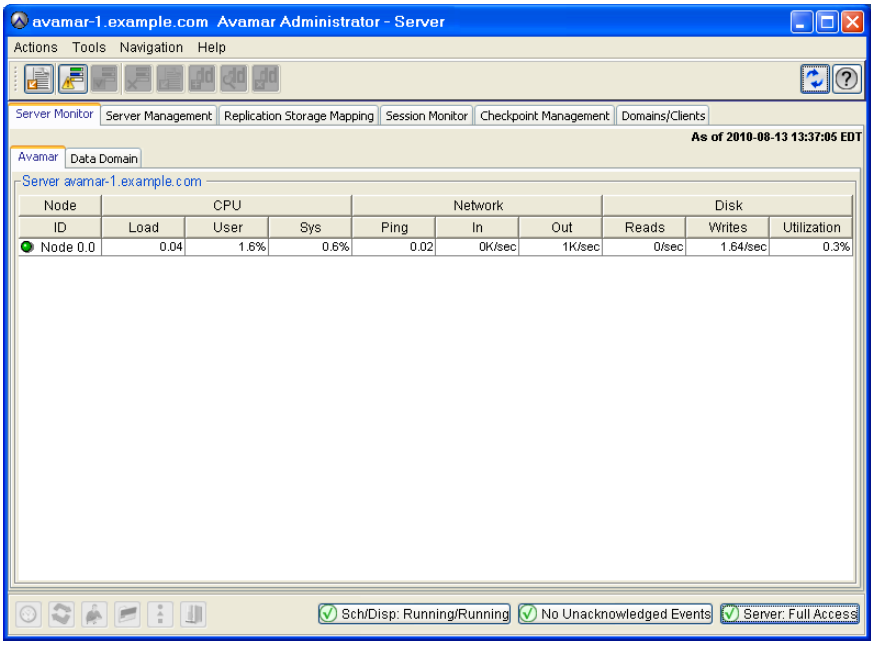
Canceling a client session

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.



As of 2010-08-13 13:37:05 EDT

Server avamar-1.example.com

Node	CPU			Network			Disk		
ID	Load	User	Sys	Ping	In	Out	Reads	Writes	Utilization
● Node 0.0	0.04	1.6%	0.6%	0.02	0K/sec	1K/sec	0/sec	1.64/sec	0.3%

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**.

NOTICE

If you cannot cancel this client session, you can reset the client to immediately and forcibly terminate any active **avtar** session on that client. "Resetting a client" on page 303 provides details.

Resetting a client

Resetting a client immediately and forcibly terminates any 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 302 provides details.

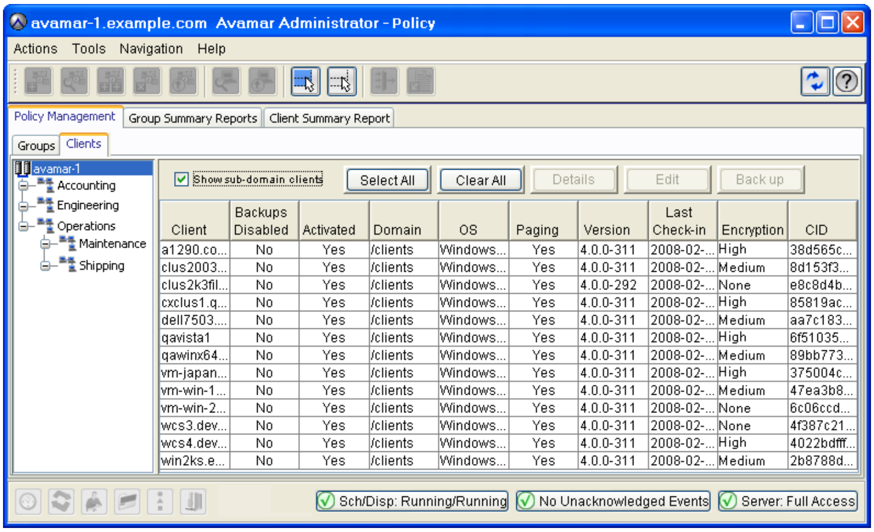
To reset a client:

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

   The Policy window appears.

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

3. Click the **Clients** tab.



☑ Show sub-domain clients

Client	Backups Disabled	Activated	Domain	OS	Paging	Version	Last Check-in	Encryption	CID
a1290.co...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	38d565c...
clus2003...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	8d153f3...
clus2k3fil...	No	Yes	/clients	Windows...	Yes	4.0.0-292	2008-02-...	None	e8c8d4b...
cxclus1.q...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	85819ac...
dell7503....	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	aa7c183...
qavista1	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	6f51035...
qawinx64...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	89bb773...
vm-japan...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	375004c...
vm-win-1...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	47ea3b8...
vm-win-2...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	6c06ccd...
wcs3.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	None	4f387c21...
wcs4.dev...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	High	4022bdfff...
win2ks.e...	No	Yes	/clients	Windows...	Yes	4.0.0-311	2008-02-...	Medium	2b8788d...

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 306
- Restarting the server 307
- Stopping the MCS 308
- Starting the MCS 308
- Getting MCS status 309

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 275.
- Create and validate a server checkpoint as discussed in "Creating a checkpoint" on page 370 and in "Validating a checkpoint" on page 371.

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.
4. Press **Enter**.

   Information similar to the following appears in the command shell:

   ```
   dpnctl: INFO: Suspending backup scheduler...
   dpnctl: INFO: Backup scheduler suspended.
   dpnctl: INFO: Suspending maintenance cron jobs...
   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 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:

   ```
   Identity added: /home/admin/.ssh/dpnid (/home/admin/.ssh/dpnid)
   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-7416
   dpnctl: INFO: Restarting gsan succeeded.
   dpnctl: INFO: gsan started.
   dpnctl: INFO: Updating MCS...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-mcs-update-output-7416
   dpnctl: INFO: MCS updated.
   dpnctl: INFO: Starting MCS...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-mcs-start-output-7416
   dpnctl: INFO: MCS started.
   dpnctl: INFO: Starting EMS...
   dpnctl: INFO: To monitor progress, run in another window: tail -f
   /tmp/dpnctl-ems-start-output-7416
   dpnctl: INFO: EMS started.
   dpnctl: INFO: Resuming scheduler...
   dpnctl: INFO: Scheduler resumed.
   dpnctl: INFO: Resuming maintenance cron jobs...
   dpnctl: INFO: Maintenance cron jobs resumed.
   ```

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 298.

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 312
- Shutting down the EMS 313
- Restarting the EMS 314
- Logging in to Avamar Enterprise Manager 314
- Dashboard 315
- System 319
- Capacity 328
- Policy 328
- Reports 329
- Replicator 330
- Configure 331
- Client Manager 332
- System Maintenance 332
- Monitoring other systems 332
- Suspending and resuming system monitoring 334
- Removing a system from the systems list 335
- Monitoring Avamar 4.1.x and 5.x systems 335
- Launching Avamar Administrator from Avamar Enterprise Manager 337

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 332 provides additional information.

Dashboard

The integrated dashboard, described on page 315, 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

Beginning with version 6.0, Avamar Enterprise Manager can manage Avamar 4.1.x, 5.x, or 6.0 systems. However, Avamar 4.1.x and 5.x systems require additional configuration and setup before monitoring them is possible. "Monitoring Avamar 4.1.x and 5.x systems" on page 335 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 good 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 315, and the replicator page, described on page 330, 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.

Shutting down the EMS

To perform an orderly shutdown of the 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

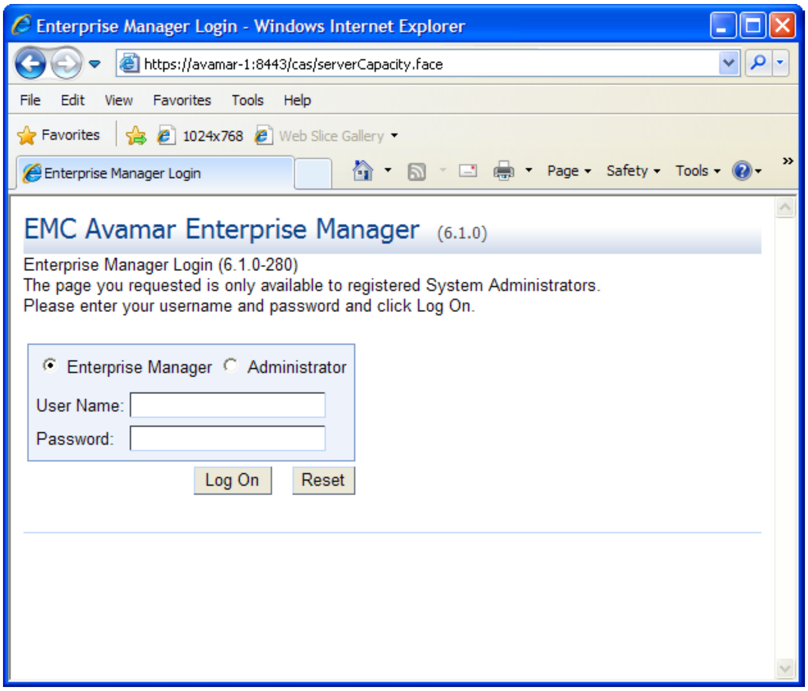
To log in to Avamar Enterprise Manager:

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.



EMC Avamar Enterprise Manager (6.1.0)

Enterprise Manager Login (6.1.0-280)
The page you requested is only available to registered System Administrators.
Please enter your username and password and click Log On.

● Enterprise Manager ○ Administrator

User Name:

Password:

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

   The account associated with this username must be assigned the Avamar role of Administrator. “Roles” on page 69 provides details about Avamar roles.

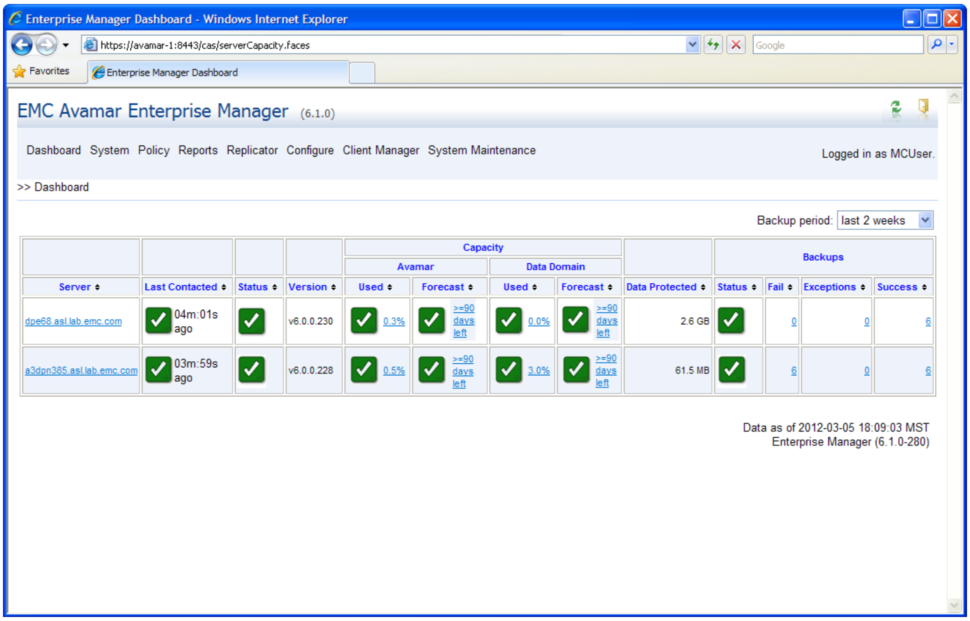
The username is checked against the internal user database first. If no match is found, then it is checked using Enterprise authentication. If that is not enabled, or no match is found, it is checked using directory service authentication. Each of these forms of authentication, is described in "Enabling user authentication" on page 75.

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.



Enterprise Manager Dashboard - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
Favorites
Enterprise Manager Dashboard

EMC Avamar Enterprise Manager (6.1.0)

Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance

Logged in as MCUser.

>> Dashboard

Backup period: last 2 weeks

				Capacity					Backups			
				Avamar		Data Domain						
Server ♦	Last Contacted ♦	Status ♦	Version ♦	Used ♦	Forecast ♦	Used ♦	Forecast ♦	Data Protected ♦	Status ♦	Fail ♦	Exceptions ♦	Success ♦
dpe68.asl.lab.emc.com	✓ 04m:01s ago	✓	v6.0.0.230	✓ 0.3%	✓ >=90 days left	✓ 0.0%	✓ >=90 days left	2.6 GB	✓	0	0	6
a3dpn385.asl.lab.emc.com	✓ 03m:59s ago	✓	v6.0.0.228	✓ 0.5%	✓ >=90 days left	✓ 3.0%	✓ >=90 days left	61.5 MB	✓	6	0	6

Data as of 2012-03-05 18:09:03 MST
Enterprise Manager (6.1.0-280)

Select Dashboard from any other page to view the Dashboard page.

The following table explains the information shown on the Dashboard page.

Table 54 Dashboard page information (page 1 of 3)

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 319 provides details.
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. State 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. X 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.

Table 54 Dashboard page information (page 2 of 3)

Information	Description
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 a problem with either the Avamar server, a configured Data Domain system, or both. However, backups and restores can continue. X There is a problem with either the Avamar server, a configured Data Domain system, or both, and 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.
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 state 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. X 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 346.
Capacity › Avamar › Forecast	Forecast state 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. X 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 346.

Table 54 Dashboard page information (page 3 of 3)

Information	Description
Capacity › Data Domain › Used	This column shows summary status of how storage capacity is being used on the configured Data Domain systems. Used state 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. X 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 346.
Capacity › Data Domain › Forecast	Forecast state 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. X 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 346.
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. State 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. X 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 329.
Backups › Fail	The number of failed backups. Click a backup status icon to view the Reports page, described in “Reports” on page 329.
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 329.
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 http://support.EMC.com and click Service Center to view existing SRs. Search the knowledgebase for Avamar Data Node offline solution esg118578, or consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

System

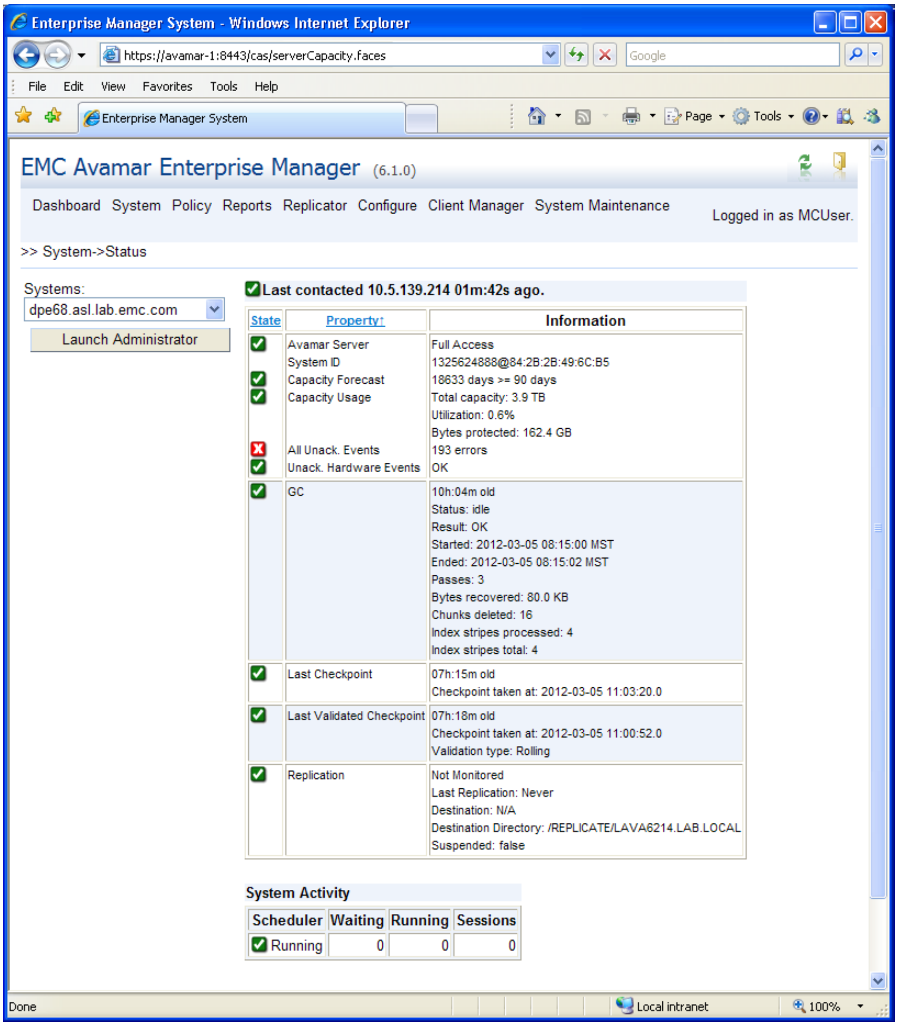
Avamar Enterprise Manager provides two kinds of system information pages:

- Individual system information pages, described in "Individual system information page" on page 319, 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 327, 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.


Enterprise Manager System - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager System
Page Tools
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> System->Status
Systems:
dpe68.asl.lab.emc.com
Launch Administrator
Done
Local intranet
100%

☑ Last contacted 10.5.139.214 01m:42s ago.

State	Property↑	Information
☑	Avamar Server	Full Access
	System ID	1325624888@84:2B:2B:49:6C:B5
☑	Capacity Forecast	18633 days >= 90 days
☑	Capacity Usage	Total capacity: 3.9 TB Utilization: 0.6% Bytes protected: 162.4 GB
☒	All Unack. Events	193 errors
☑	Unack. Hardware Events	OK
☑	GC	10h:04m old Status: idle Result: OK Started: 2012-03-05 08:15:00 MST Ended: 2012-03-05 08:15:02 MST Passes: 3 Bytes recovered: 80.0 KB Chunks deleted: 16 Index stripes processed: 4 Index stripes total: 4
☑	Last Checkpoint	07h:15m old Checkpoint taken at: 2012-03-05 11:03:20.0
☑	Last Validated Checkpoint	07h:18m old Checkpoint taken at: 2012-03-05 11:00:52.0 Validation type: Rolling
☑	Replication	Not Monitored Last Replication: Never Destination: N/A Destination Directory: /REPLICATE/LAVA6214.LAB.LOCAL Suspended: false

System Activity

Scheduler	Waiting	Running	Sessions
☑ Running	0	0	0

Server status

The following table explains server status information.

Table 55 Server status information (page 1 of 7)

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. State 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 315 provides additional information about refresh/polling intervals and associated status conditions. X 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.[1] – Avamar server hostname could not be resolved.[2] – Avamar server login credentials (username or password) were refused.[3] Investigate and remedy any red status condition immediately to ensure that server operation is not adversely affected.

Table 55 Server status information (page 2 of 7)

Information	Description
Avamar Server	The operational run level for the Avamar server. State 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 298 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).[3] **Node Offline** — One or more storage nodes has experienced a problem.[4] **Not available** — Avamar Enterprise Manager cannot obtain any information from this Avamar server. This might indicate communication problems or errors in retrieving data.[3] 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.[3] **Note:** 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 state 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 55 Server status information (page 3 of 7)

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 State 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. X Avamar server has used more than 95% of total storage capacity. No new backups are performed until you add capacity or delete old backups.[5]
All Unack. Events	This row shows whether there are any unacknowledged events on the Avamar server. State 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 296 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. X 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.

Table 55 Server status information (page 4 of 7)

Information	Description
Unack. Hardware Events	This row shows whether there are any unacknowledged hardware events on the Avamar server. State 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 296 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. X 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. Go to the EMC online support website, https://support.emc.com/products/Avamar, click the Advanced search link, select the Service Requests option from the Search list, and search for the Service Request. If you do not find the Service Request, search the knowledgebase at https://support.emc.com/products/Avamar, for the specific issue. If the required information is not found, use Live Chat to engage EMC Customer Service or create a Service Request as described in “Where to get help” on page 23.
Data Domain Server	The fully qualified domain name of the Data Domain system.
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. X The Data Domain system is experiencing problems, and backups and restores will not occur until the problem is resolved. “Data Domain status and resolutions” on page 568 provides details on the available status messages.
Capacity Forecast	Forecast state 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. X The Data Domain system is forecast to have less than 30 days of storage capacity.

Table 55 Server status information (page 5 of 7)

Information	Description
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 State 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. X 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.[5]
All Unack. Events	This row shows whether there are any unacknowledged events for the Data Domain system. State 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 296 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. X 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.
Unack. Hardware Events	This row shows whether there are any unacknowledged hardware events on the Data Domain system. State 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 296 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. X 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/.

Table 55 Server status information (page 6 of 7)

Information	Description
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 State 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. X 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. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
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 370 provides details on checkpoints. State 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. X More than 48 hours have elapsed since a checkpoint successfully completed on this Avamar server.

Table 55 Server status information (page 7 of 7)

Information	Description
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. State 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. X 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. State 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. X 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.[1] The optional replication management feature is discussed in “Replication” on page 353.

1. Consult the Administration link on the Avamar Support landing page, https://support.emc.com/products/Avamar, for additional troubleshooting information.
2. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
3. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
4. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.
5. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Search the knowledgebase for solution esg118578, or consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

System activity

The following table explains the System Activity information that appears on the System Status page in Avamar Enterprise Manager.

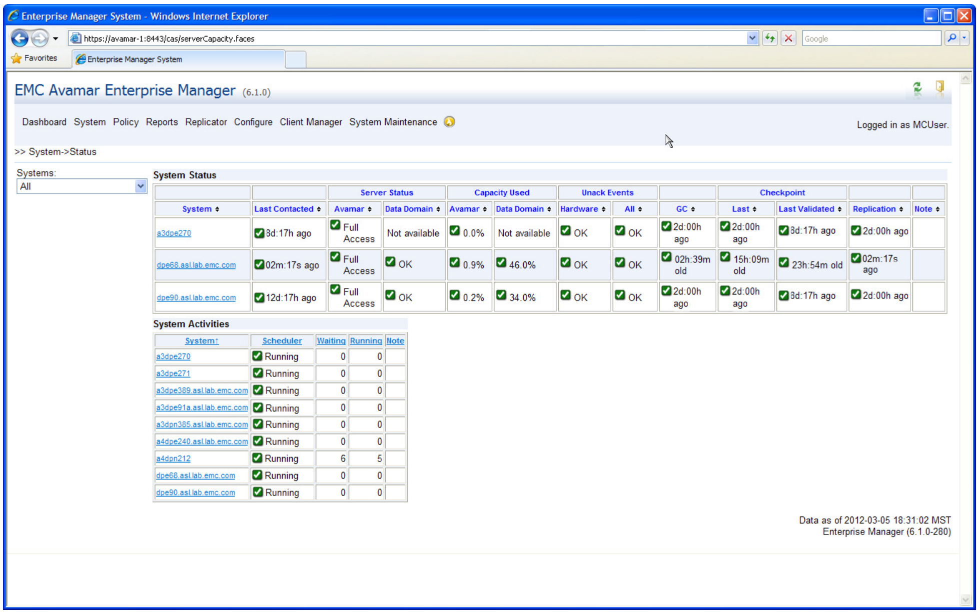
Table 56 System activity information

Information	Description
Scheduler	This column shows whether regularly scheduled server activities (for example, backups, maintenance activities) are enabled for this Avamar server. State 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 298 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 315, 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 319, to view the all systems information (detailed dashboard) page.


Enterprise Manager System - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Favorites
Enterprise Manager System
EMC Avamar Enterprise Manager (6.1.0)
Dashboard
System
Policy
Reports
Replicator
Configure
Client Manager
System Maintenance
Logged in as MCUser.
>> System->Status
Systems:
All

System Status

		Server Status		Capacity Used		Unack Events			Checkpoint			
System	Last Contacted	Avamar	Data Domain	Avamar	Data Domain	Hardware	All	GC	Last	Last Validated	Replication	Note
a3dpe270	✓ 8d:17h ago	✓ Full Access	Not available	✓ 0.0%	Not available	✓ OK	✓ OK	✓ 2d:00h ago	✓ 2d:00h ago	✓ 8d:17h ago	✓ 2d:00h ago	
dpe68.asl.lab.emc.com	✓ 02m:17s ago	✓ Full Access	✓ OK	✓ 0.9%	✓ 46.0%	✓ OK	✓ OK	✓ 02h:39m old	✓ 15h:09m old	✓ 23h:54m old	✓ 02m:17s ago	
dpe90.asl.lab.emc.com	✓ 12d:17h ago	✓ Full Access	✓ OK	✓ 0.2%	✓ 34.0%	✓ OK	✓ OK	✓ 2d:00h ago	✓ 2d:00h ago	✓ 8d:17h ago	✓ 2d:00h ago	

System Activities

System↑	Scheduler	Waiting	Running	Note
a3dpe270	✓ Running	0	0	
a3dpe271	✓ Running	0	0	
a3dpe389.asl.lab.emc.com	✓ Running	0	0	
a3dpe91a.asl.lab.emc.com	✓ Running	0	0	
a3dpn385.asl.lab.emc.com	✓ Running	0	0	
a4dpe240.asl.lab.emc.com	✓ Running	0	0	
a4dpn212	✓ Running	6	5	
dpe68.asl.lab.emc.com	✓ Running	0	0	
dpe90.asl.lab.emc.com	✓ Running	0	0	

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

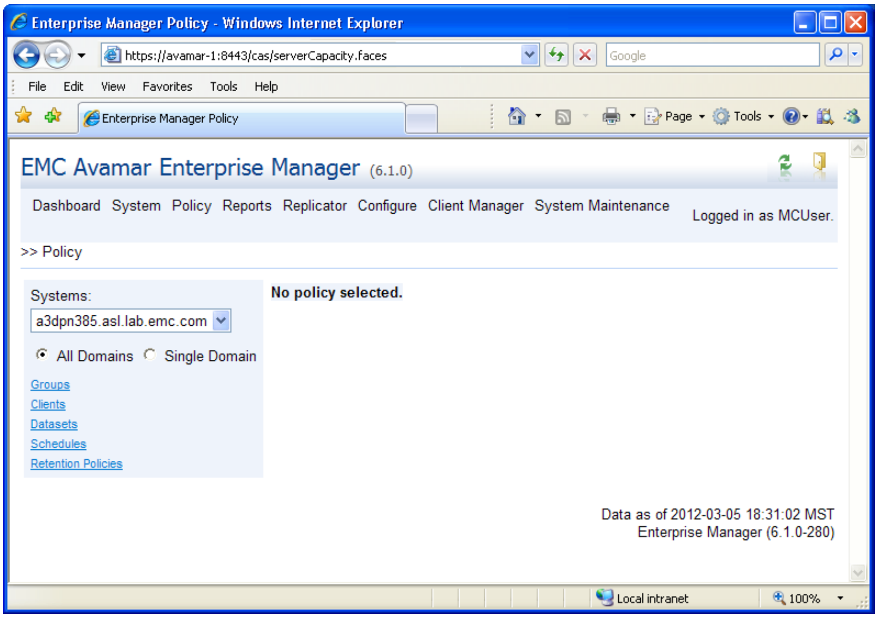
The information is the same as the information that appears for individual servers. "Individual system information page" on page 319 provides additional information.

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.


Enterprise Manager Policy - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager Policy
Page Tools
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Groups
Clients
Datasets
Schedules
Retention Policies
Local intranet
100%

Logged in as MCUser.

>> Policy

Systems: a3dpn385.asl.lab.emc.com

● All Domains ○ Single Domain

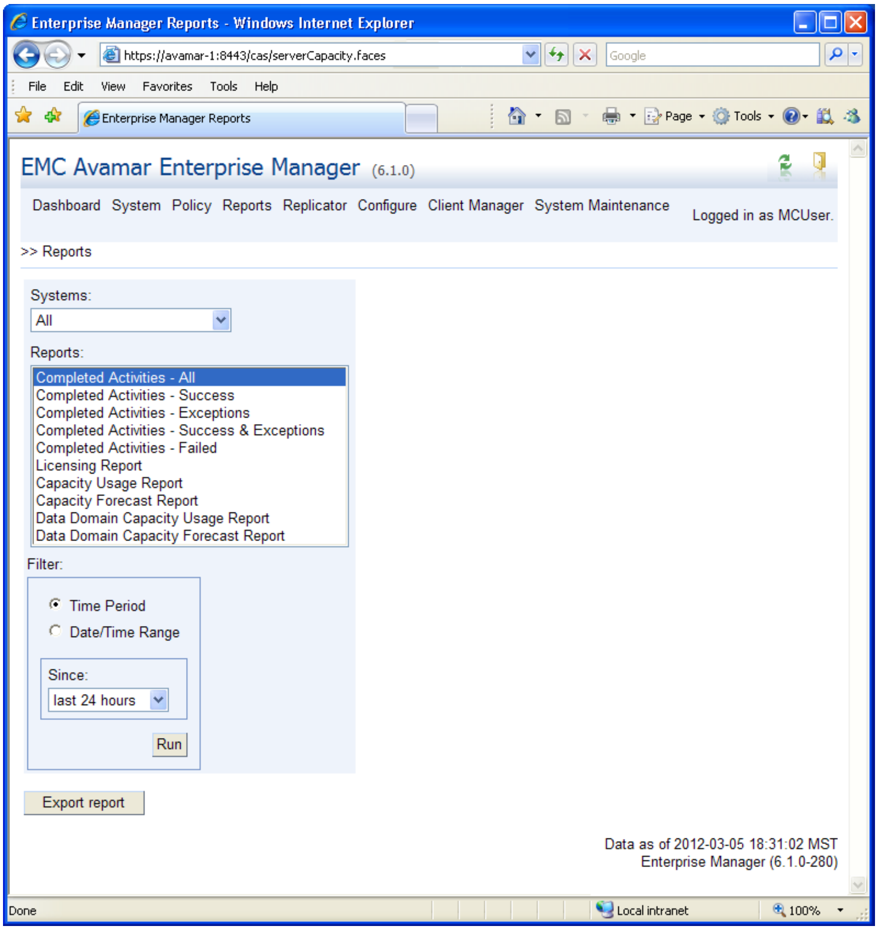
No policy selected.

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

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.


Enterprise Manager Reports - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager Reports
Page Tools
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> Reports
Systems:
All
Reports:
Completed Activities - All
Completed Activities - Success
Completed Activities - Exceptions
Completed Activities - Success & Exceptions
Completed Activities - Failed
Licensing Report
Capacity Usage Report
Capacity Forecast Report
Data Domain Capacity Usage Report
Data Domain Capacity Forecast Report
Filter:
● Time Period
○ Date/Time Range
Since:
last 24 hours
Run
Export report
Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)
Done
Local intranet
100%

“Avamar reports” on page 224 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 330.
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**.

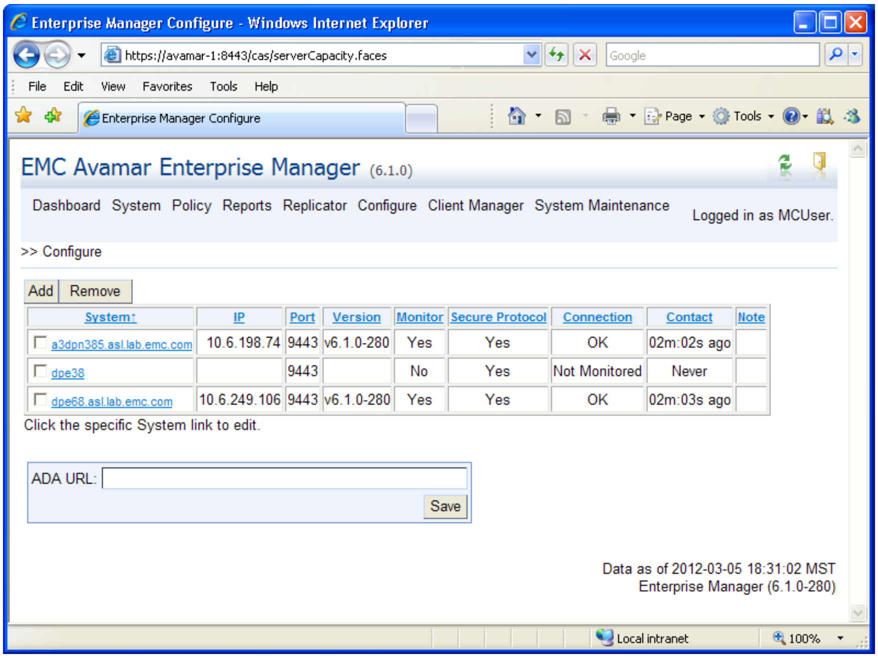
   The Save As dialog box appears.
4. Browse to the appropriate location and click **Save**.

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.



Enterprise Manager Configure - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager Configure
Page Tools

EMC Avamar Enterprise Manager (6.1.0)

Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.

>> Configure

System↑	IP	Port	Version	Monitor	Secure Protocol	Connection	Contact	Note
□ a3dpn385.asl.lab.emc.com	10.6.198.74	9443	v6.1.0-280	Yes	Yes	OK	02m:02s ago	
□ dpe38		9443		No	Yes	Not Monitored	Never	
□ dpe68.asl.lab.emc.com	10.6.249.106	9443	v6.1.0-280	Yes	Yes	OK	02m:03s ago	

Click the specific System link to edit.

ADA URL:

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

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 57 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.

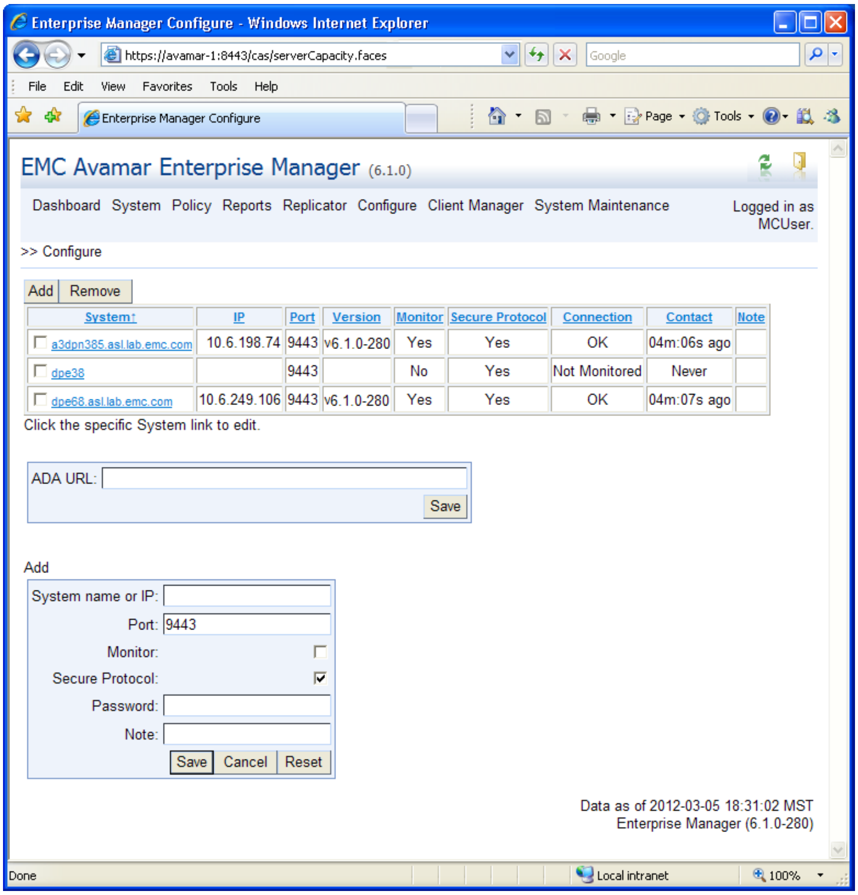
   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.

3. Click **Add**.

An Add block appears below the systems list.



Enterprise Manager Configure - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager Configure
Page
Tools
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> Configure
Add
Remove

System↑	IP	Port	Version	Monitor	Secure Protocol	Connection	Contact	Note
□ a3dpn385.asl.lab.emc.com	10.6.198.74	9443	v6.1.0-280	Yes	Yes	OK	04m:06s ago	
□ dpe38		9443		No	Yes	Not Monitored	Never	
□ dpe68.asl.lab.emc.com	10.6.249.106	9443	v6.1.0-280	Yes	Yes	OK	04m:07s ago	

Click the specific System link to edit.

ADA URL:

Add

System name or IP:

Port: 9443

Monitor: □

Secure Protocol: ☑

Password:

Note:

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

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 336 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.

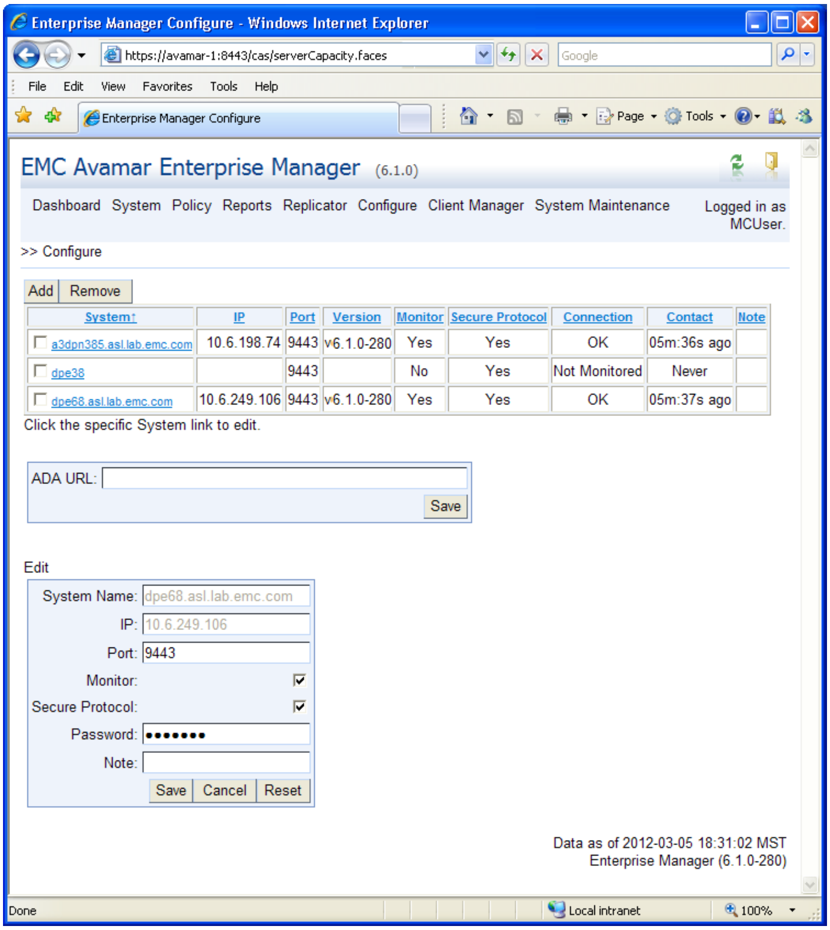
   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.

3. Click the server name.

   An Edit block appears below the systems list.


Enterprise Manager Configure - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File Edit View Favorites Tools Help
Enterprise Manager Configure
Page Tools
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> Configure
Add Remove
Done
Local intranet
100%

	System↑	IP	Port	Version	Monitor	Secure Protocol	Connection	Contact	Note
□	a3dpn385.asl.lab.emc.com	10.6.198.74	9443	v6.1.0-280	Yes	Yes	OK	05m:36s ago	
□	dpe38		9443		No	Yes	Not Monitored	Never	
□	dpe68.asl.lab.emc.com	10.6.249.106	9443	v6.1.0-280	Yes	Yes	OK	05m:37s ago	

Click the specific System link to edit.

ADA URL:

Save

Edit

System Name: dpe68.asl.lab.emc.com

IP: 10.6.249.106

Port: 9443

Monitor: ☑

Secure Protocol: ☑

Password: •••••••

Note:

Save Cancel Reset

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

4. Clear the **Monitor** checkbox to suspend monitoring, or select the checkbox to resume monitoring.

Removing a system from the systems list

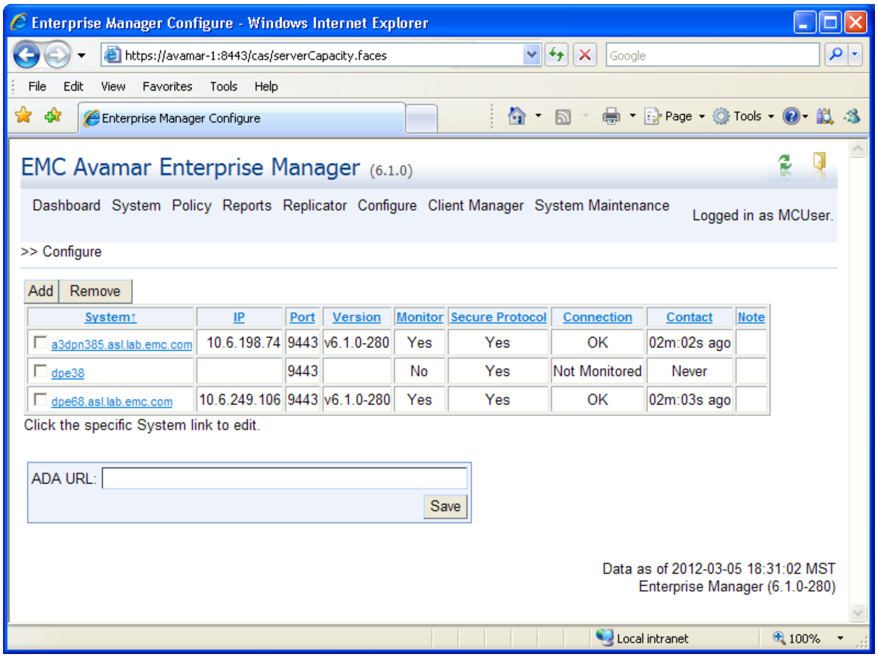
To remove a system from the list:

1. Open a web browser and log in to Avamar Enterprise Manager.

   The Dashboard page appears.

2. Select **Configure**.

   The Configure page appears.



Enterprise Manager Configure - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
File
Edit
View
Favorites
Tools
Help
Enterprise Manager Configure
Page
Tools

EMC Avamar Enterprise Manager (6.1.0)

Logged in as MCUser.

>> Configure

System↑	IP	Port	Version	Monitor	Secure Protocol	Connection	Contact	Note
□ a3dpn385.asl.lab.emc.com	10.6.198.74	9443	v6.1.0-280	Yes	Yes	OK	02m:02s ago	
□ dpe38		9443		No	Yes	Not Monitored	Never	
□ dpe68.asl.lab.emc.com	10.6.249.106	9443	v6.1.0-280	Yes	Yes	OK	02m:03s ago	

Click the specific System link to edit.

ADA URL:

Data as of 2012-03-05 18:31:02 MST
Enterprise Manager (6.1.0-280)

3. Select the checkbox next to the system.

4. Click **Remove**.

Monitoring Avamar 4.1.x and 5.x systems

To monitor Avamar 4.1.x or 5.x systems with Avamar Enterprise Manager 6.1, enable web services on those systems by performing the following configuration and setup tasks:

- "Obtain and install the server hotfix" on page 335
- "Configure MCS web services" on page 336
- "Add the system to Avamar Enterprise Manager" on page 337

Obtain and install the server hotfix

Obtain the correct hotfix for the Avamar server by contacting EMC Customer Service.

- Avamar 4.1.x systems require Hotfix 19759
- Avamar 5.x systems require Hotfix 19760

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 58 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 332.

Be sure to set the Secure Protocol as described in the following table.

Table 59 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:

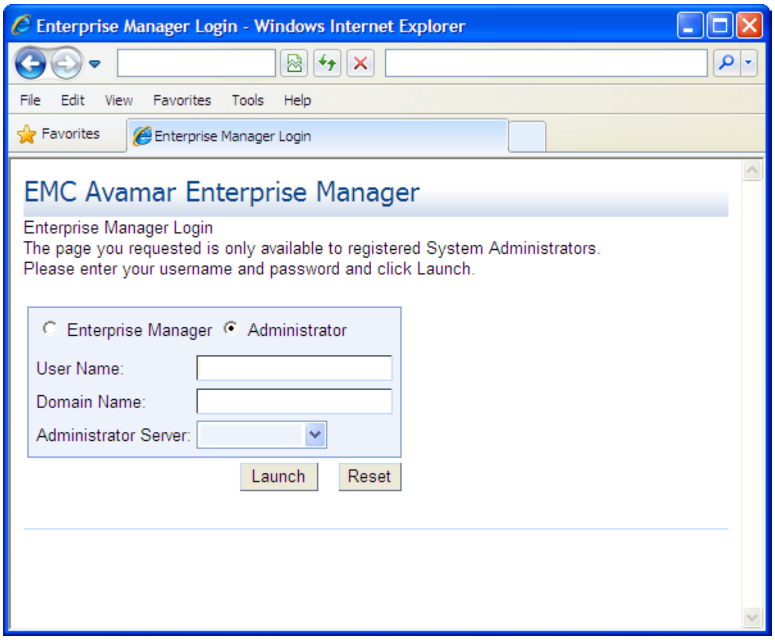
   ```
   http://AVAMARSERVER/em
   ```

   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.



EMC Avamar Enterprise Manager

Enterprise Manager Login
The page you requested is only available to registered System Administrators.
Please enter your username and password and click Launch.

○ Enterprise Manager ● Administrator

User Name:

Domain Name:

Administrator Server:

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.

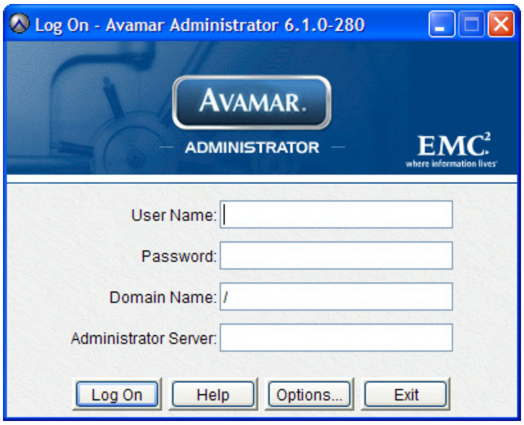
   You are redirected to a specific area of the Sun Microsystems website to download and install the correct version of the JRE.

   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.

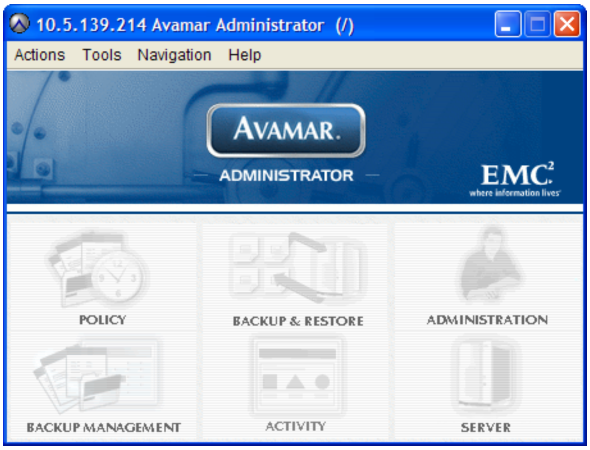
The Avamar Administrator login window appears.



10. Type the Avamar administrative user account password in the **Password** text box.

11. Click **Log On**.

    The Administrator launcher 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:

- Limits and thresholds 342
- Obtaining basic utilization information 343
- Capacity forecasting.. 345
- Detailed utilization and forecasting.. 346
- Customizing capacity limits and behavior... 347
- Server and client average daily change rates 349

Limits and thresholds

This topic describes how a server behaves as it crosses various consumed storage thresholds.

100% — the “server read-only limit”

When server 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. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578, or consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

95% — the “health check limit”

Although an Avamar server could be allowed to consume 100% of available storage capacity (that is, reach the server read-only limit), it is not a good practice to let that occur. Consuming all available storage can prevent certain server maintenance activities from running, which might otherwise free additional storage capacity for backups.

For that reason, a second limit is established called the “health check limit.” This is the amount of storage capacity that can be consumed and still have a “healthy” server.

This health check limit is derived by subtracting some percentage of server storage capacity from the server read-only limit. The default health check limit is 95%. You can customize this setting as discussed in “Customizing capacity limits and behavior” on page 347. However, setting this limit higher than 95% is not recommended.

When server utilization reaches the health check limit, backups that are in progress are allowed to complete, but all new backup activity is suspended. 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 future backup activity can resume. “Acknowledging system events” on page 296 provides details.

80% — capacity warning issued

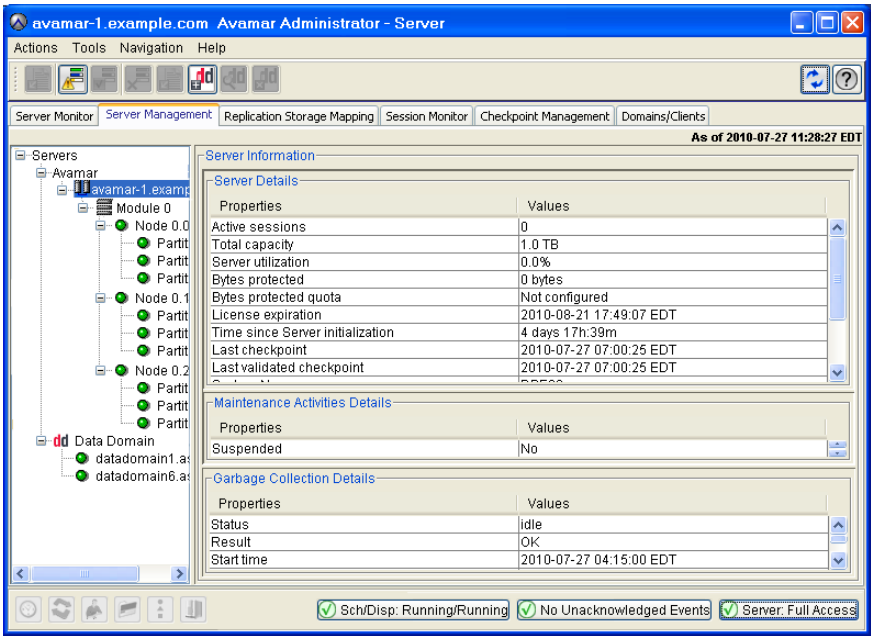
When server utilization reaches 80%, a pop-up notification informs you that the server has consumed 80% of its available storage capacity. Avamar Enterprise Manager capacity state icons are yellow.

Obtaining basic utilization information

Both Avamar Administrator and Avamar Enterprise Manager provide real-time basic capacity utilization information.

Avamar Administrator

In Avamar Administrator, basic capacity utilization information for a server is shown in the Server window on the Server Management tab when you select the Avamar server in the tree, as shown in the following example.



As of 2010-07-27 11:28:27 EDT

Server Information

Server Details

Properties	Values
Active sessions	0
Total capacity	1.0 TB
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	2010-08-21 17:49:07 EDT
Time since Server initialization	4 days 17h:39m
Last checkpoint	2010-07-27 07:00:25 EDT
Last validated checkpoint	2010-07-27 07:00:25 EDT

Maintenance Activities Details

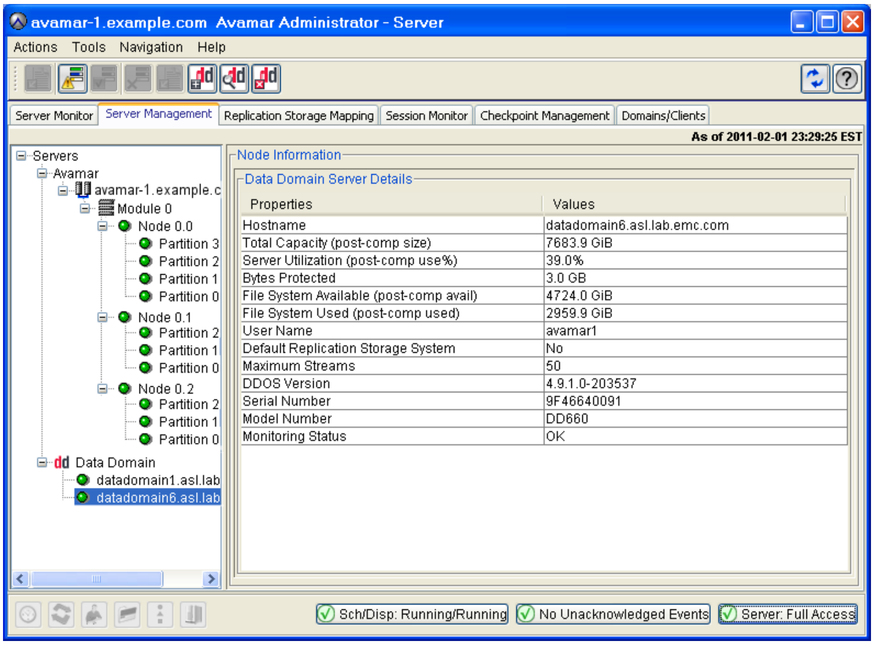
Properties	Values
Suspended	No

Garbage Collection Details

Properties	Values
Status	idle
Result	OK
Start time	2010-07-27 04:15:00 EDT

The Server Information table shows the total amount of server storage capacity and the percentage of total available server storage capacity currently used. "Monitoring the server" on page 260 provides information about the Server window.

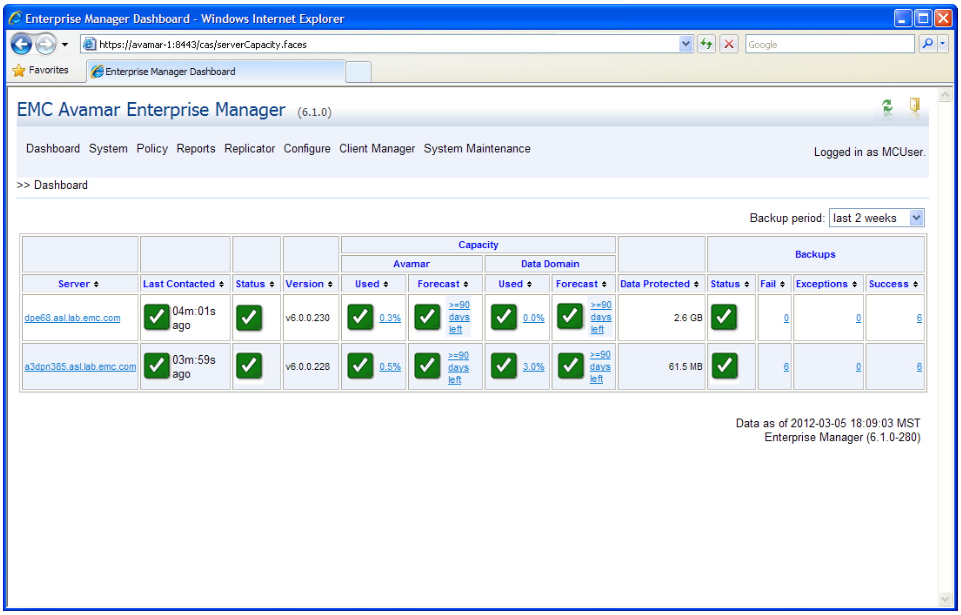
Similarly, if you select a Data Domain system from the tree, the total amount of storage capacity and the percentage of total available storage capacity in use is listed, as shown in the following example.



Properties	Values
Hostname	datadomain6.asl.lab.emc.com
Total Capacity (post-comp size)	7683.9 GiB
Server Utilization (post-comp use%)	39.0%
Bytes Protected	3.0 GB
File System Available (post-comp avail)	4724.0 GiB
File System Used (post-comp used)	2959.9 GiB
User Name	avamar1
Default Replication Storage System	No
Maximum Streams	50
DDOS Version	4.9.1.0-203537
Serial Number	9F46640091
Model Number	DD660
Monitoring Status	OK

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.


Enterprise Manager Dashboard - Windows Internet Explorer
https://avamar-1:8443/cas/serverCapacity.faces
Google
Favorites
Enterprise Manager Dashboard
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> Dashboard

Backup period: last 2 weeks

				Capacity					Backups			
				Avamar		Data Domain						
Server	Last Contacted	Status	Version	Used	Forecast	Used	Forecast	Data Protected	Status	Fail	Exceptions	Success
dpe68.asl.lab.emc.com	✓ 04m:01s ago	✓	v6.0.0.230	✓ 0.3%	✓ >=90 days left	✓ 0.0%	✓ >=90 days left	2.6 GB	✓	0	0	6
a3dpn385.asl.lab.emc.com	✓ 03m:59s ago	✓	v6.0.0.228	✓ 0.5%	✓ >=90 days left	✓ 3.0%	✓ >=90 days left	61.5 MB	✓	6	0	6

Data as of 2012-03-05 18:09:03 MST
Enterprise Manager (6.1.0-280)

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 state icons in the Capacity › Avamar › Used and Capacity › Data Domain › Used columns:

✓ The Avamar server or Data Domain systems have used less than 80% of total storage capacity.

! The Avamar server or Data Domain systems have used more than 80% but less than 95% of total storage capacity.

Consider adding capacity or deleting old backups.

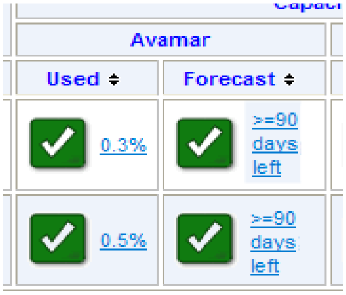
X The Avamar server or Data Domain systems have used more than 95% of total storage capacity. No new backups are allowed until you add capacity or delete old backups. If ConnectEMC has been enabled, a Service Request (SR) should have been logged. Go to the EMC online support website at http://support.EMC.com and click Service Center to view existing SRs. Search the knowledgebase for Avamar User and OS Capacity Management solution esg118578, or consult the Support by Product Page for Avamar Server at https://support.emc.com for additional troubleshooting information.

Capacity utilization information is also shown on the information page for each server. “Individual system information page” on page 319 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 315, shows capacity forecasting results in the Capacity Forecast column for the Avamar server, as shown in the following figure, and also for configured Data Domain systems.



Avamar			
Used ⇕		Forecast ⇕	
✓	0.3%	✓	>=90 days left
✓	0.5%	✓	>=90 days left

Capacity Forecast state 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.

X The Avamar server or Data Domain systems are forecast to have less than 30 days of storage capacity.

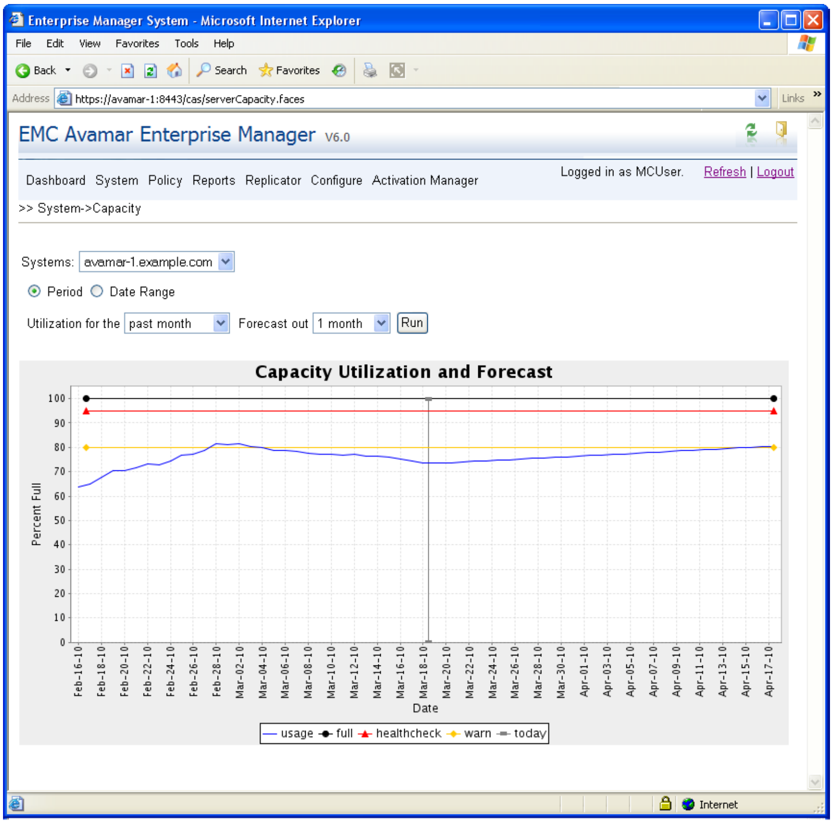
Important limitation regarding capacity data after a rollback

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.



Systems: avamar-1.example.com

● Period ○ Date Range

Utilization for the past month Forecast out 1 month Run

You can customize this 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 60 Avamar Administrator capacity management preferences

Preference	Description	Default Setting
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%
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 61 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

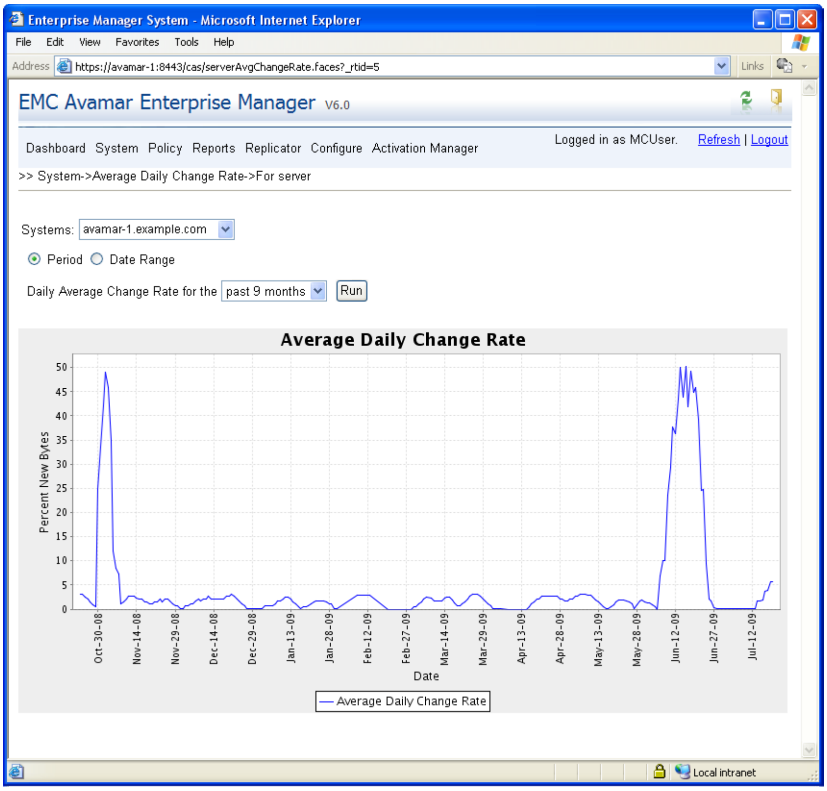
When managing server capacity, it is useful to know the average daily change rate for both the server and for individual clients.

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.


Enterprise Manager System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://avamar-1:8443/cas/serverAvgChangeRate.faces?_rtid=5
Links
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Configure Activation Manager
Logged in as MCUser.
Refresh | Logout
Run
Average Daily Change Rate
Percent New Bytes
50
45
40
35
30
25
20
15
10
5
0
Oct-30-08
Nov-14-08
Nov-29-08
Dec-14-08
Dec-29-08
Jan-13-09
Jan-28-09
Feb-12-09
Feb-27-09
Mar-14-09
Mar-29-09
Apr-13-09
Apr-28-09
May-13-09
May-28-09
Jun-12-09
Jun-27-09
Jul-12-09
Date
Average Daily Change Rate
Local intranet

>> System->Average Daily Change Rate->For server

Systems: avamar-1.example.com

● Period ○ Date Range

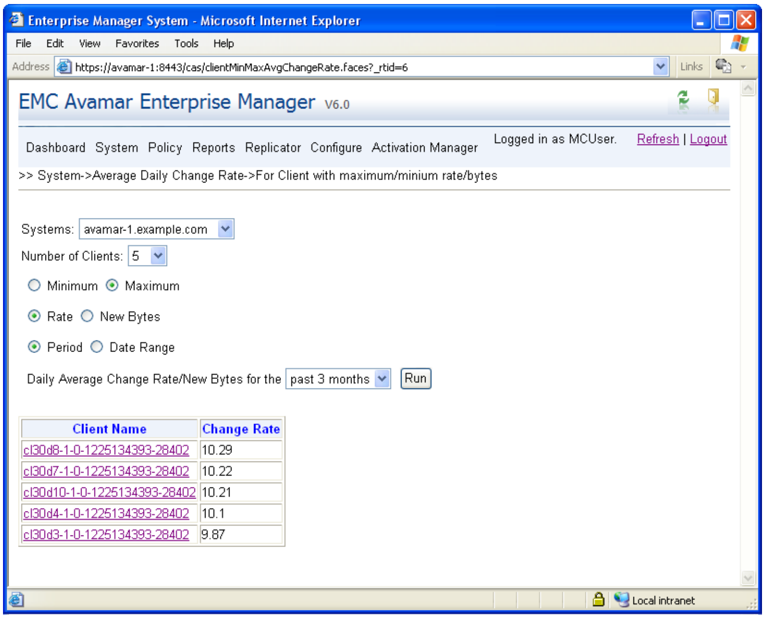
Daily Average Change Rate for the past 9 months

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.


Enterprise Manager System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Links
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Configure Activation Manager
Refresh | Logout
Run
Local intranet

https://avamar-1:8443/cas/clientMinMaxAvgChangeRate.faces?_rtid=6

Logged in as MCUser.

>> System->Average Daily Change Rate->For Client with maximum/minium rate/bytes

Systems: avamar-1.example.com

Number of Clients: 5

○ Minimum ● Maximum

● Rate ○ New Bytes

● Period ○ Date Range

Daily Average Change Rate/New Bytes for the past 3 months

Client Name	Change Rate
cl30d8-1-0-1225134393-28402	10.29
cl30d7-1-0-1225134393-28402	10.22
cl30d10-1-0-1225134393-28402	10.21
cl30d4-1-0-1225134393-28402	10.1
cl30d3-1-0-1225134393-28402	9.87

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.. 354
- Important terms and concepts 354
- Capabilities and limitations 356
- Best practices 357
- Managing replication with Avamar Administrator...................................... 358
- Viewing replication statistics with Avamar Administrator 361
- Managing replication with Avamar Enterprise Manager............................ 362

Overview

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

You can use either Avamar Administrator or Avamar Enterprise Manager to manage replication settings.

Efficient data transfers

Replication is accomplished by way of highly efficient, asynchronous Internet Protocol (IP) data transfers, which can be scheduled during off-peak hours to make optimum use of network bandwidth. Additionally, Avamar replication uses sophisticated data deduplication technology that finds and eliminates redundant sequences of data before it is sent to the destination server, thereby reducing network traffic and promoting efficient use of hard disk storage.

Remote branch disaster recovery

Replication enables the efficient replication of data stored in a single-node server to a multi-node server. Using replication, a distributed enterprise can centrally protect and manage multiple remote branch offices that use individual single-node servers for local backup and restore. The centralized multi-node server can then be used for disaster recovery, in the event of catastrophic data loss at any remote branch office.

Enterprise data center disaster recovery

Replication can also be used to replicate data stored in a multi-node server to any other multi-node server in the enterprise. In this manner, multi-node servers can provide peer-to-peer disaster recovery for each other.

Important terms and concepts

This topic discusses the basic concepts and fundamental principles of Avamar server replication.

There are two basic kinds of replication:

- Normal replication
- Full root-to-root replication

Normal replication

During normal replication, user data on the source Avamar server replicates to a destination Avamar server.

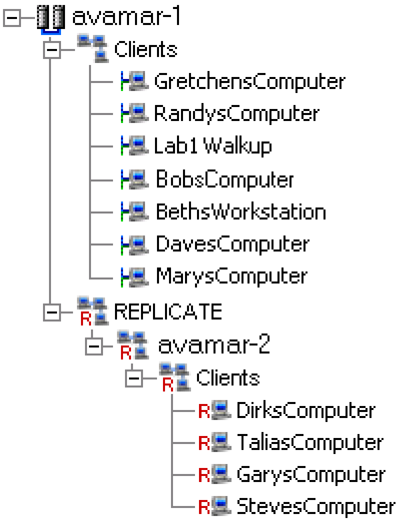
The REPLICATE domain

Replication automatically creates a REPLICATE domain on the destination server during the first replication operation. This domain contains a mirrored representation of the entire source server client tree on the destination server.

All data within the REPLICATE domain is read-only. The only operations allowed on these backups are:

- Redirecting restores to other clients not within the REPLICATE domain
- Changing a backup expiration date
- Validating backups on other clients not within the REPLICATE domain
- Viewing backup statistics
- Deleting a backup

In the following example figure, a destination server called avamar-1 contains both local clients and clients replicated from the avamar-2 source server.



Full root-to-root replication

Full root-to-root replication is a kind of replication that 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 can be changed on the destination server.

The remainder of this chapter deals exclusively with normal replication. "Avamar System Migration" on page 449 provides information on full root-to-root replication.

Source and destination servers

Replication always transfers data from a source Avamar server to a destination Avamar server. Furthermore, to maintain referential integrity on the source server, replicated data cannot be directly changed on the destination server. Replicated data is stored on the destination server only in case it is needed for future recovery.

Normal replication is a scheduled event

Once replication is set up and configured on the source server, normal replication occurs automatically at predetermined scheduled intervals.

Data that is replicated

To fully replicate an Avamar server, all of the following data must be copied from the source server to the destination server during each replication operation:

- Client backups
- Domains, clients, and users
- Groups, datasets, schedules, and retention policies
- State of the server (for example, contents of the activity monitor and server monitor databases at the time of the last MCS backup or “flush”)

Capabilities and limitations

The following topics discuss replication capabilities and limitations.

Only static data is replicated

Each replication operation transfers all static data resident on the source Avamar server. The concept of “static data” is especially important. 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.

Replicating backups by retention type

To enhance the flexibility of the retention feature, you can configure replication operations to replicate all backups from the source Avamar server to the destination Avamar server, or only replicate daily, weekly, monthly, or yearly backups.

Avamar Administrator manages only one server at a time

An important limitation of using Avamar Administrator to manage replication settings is that you are limited to managing one server at a time. If there is more than one Avamar system in the environment, you may prefer to use the Avamar Enterprise Manager multi-system management console 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 provide best practices for replication.

Avoid source and destination server incompatibilities

Although replication between different version servers 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.

Use a large time-out setting initially

If you specify an optional time-out 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 time-out 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 time-out 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 time-out 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, once you determine that the nightly replication window has normalized, you should optimize the length of the replication window accordingly.

The default time-out setting is 20 hours (72,000 seconds).

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.

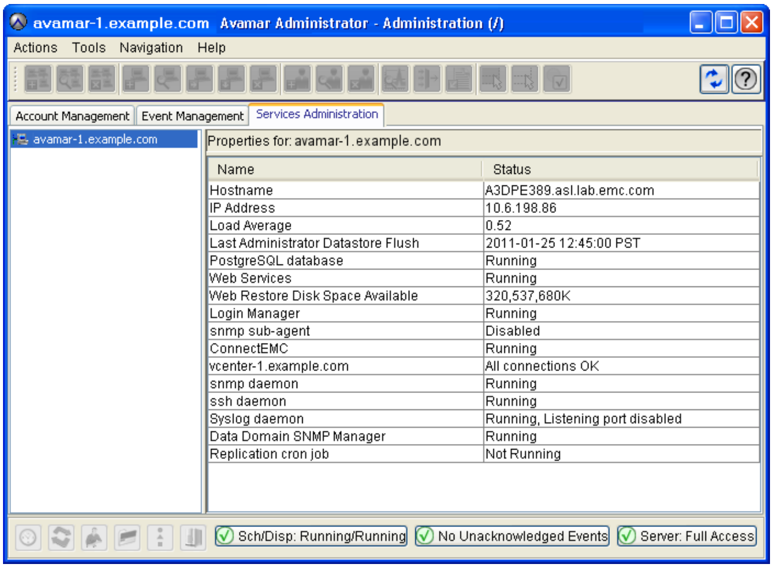
Managing replication with Avamar Administrator

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.

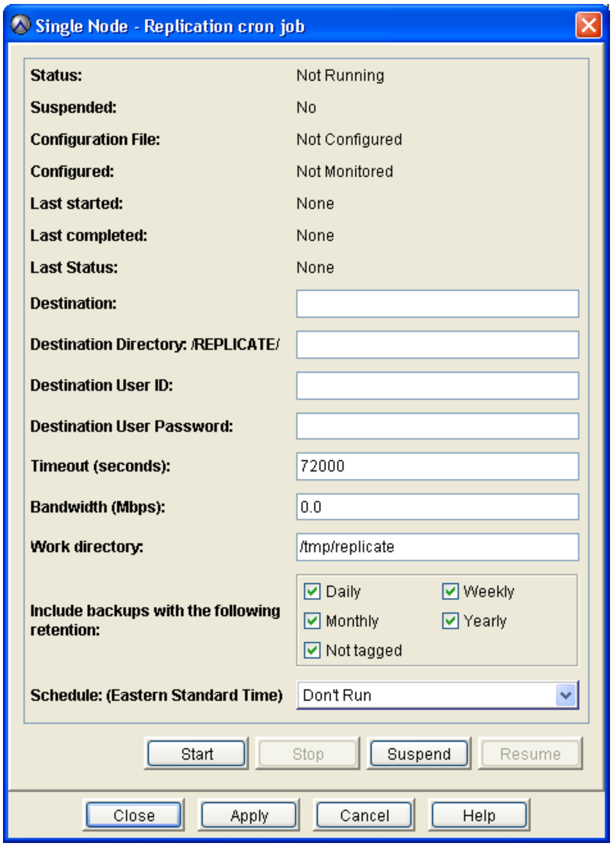


Properties for: avamar-1.example.com

Name	Status
Hostname	A3DPE389.asl.lab.emc.com
IP Address	10.6.198.86
Load Average	0.52
Last Administrator Datastore Flush	2011-01-25 12:45:00 PST
PostgreSQL database	Running
Web Services	Running
Web Restore Disk Space Available	320,537,680K
Login Manager	Running
snmp sub-agent	Disabled
ConnectEMC	Running
vcenter-1.example.com	All connections OK
snmp daemon	Running
ssh daemon	Running
Syslog daemon	Running, Listening port disabled
Data Domain SNMP Manager	Running
Replication cron job	Not Running

3. Double-click the **Replication cron job** entry in the properties table.

The Replication cron job dialog box appears.



Single Node - Replication cron job

Status:	Not Running
Suspended:	No
Configuration File:	Not Configured
Configured:	Not Monitored
Last started:	None
Last completed:	None
Last Status:	None
Destination:	
Destination Directory: /REPLICATE/	
Destination User ID:	
Destination User Password:	
Timeout (seconds):	72000
Bandwidth (Mbps):	0.0
Work directory:	/tmp/replicate
Include backups with the following retention:	☑ Daily ☑ Weekly ☑ Monthly ☑ Yearly ☑ Not tagged
Schedule: (Eastern Standard Time)	Don't Run

The Replication cron job dialog box displays the information described in the following table.

Table 62 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 62 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 113 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 (repluser) 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 (repluser).

   NOTICE

   If you change the password for the repluser 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.

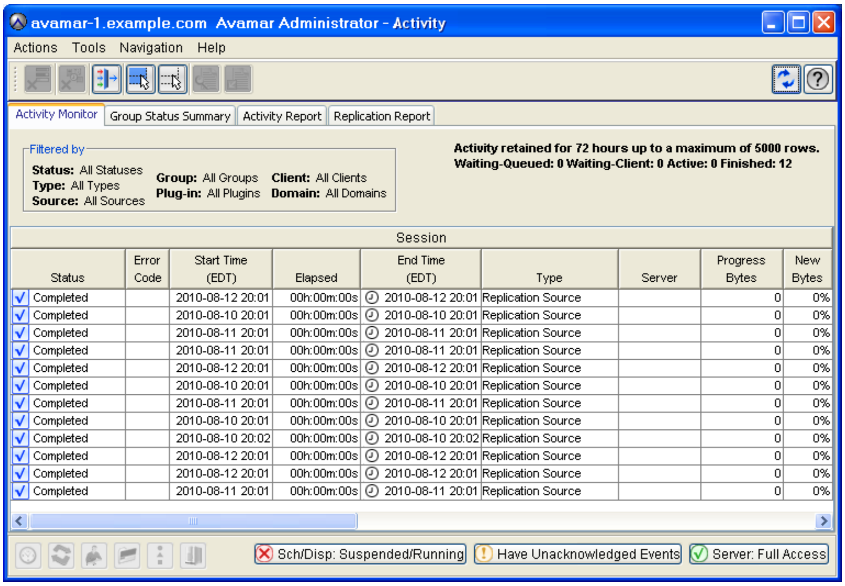
13. Click **OK**.

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.



Filtered by
Status: All Statuses **Type:** All Types **Source:** All Sources **Group:** All Groups **Plug-in:** All Plugins **Client:** All Clients **Domain:** All Domains

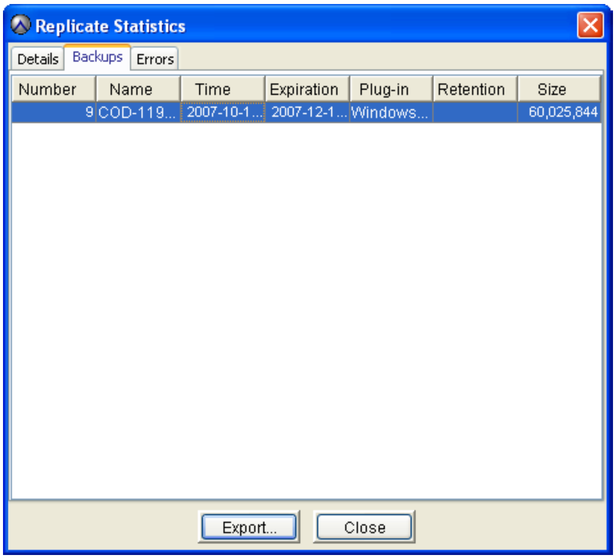
Activity retained for 72 hours up to a maximum of 5000 rows.
Waiting-Queued: 0 Waiting-Client: 0 Active: 0 Finished: 12

Session								
Status	Error Code	Start Time (EDT)	Elapsed	End Time (EDT)	Type	Server	Progress Bytes	New Bytes
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:01	00h:00m:00s	2010-08-10 20:01	Replication Source		0	0%
✓ Completed		2010-08-10 20:02	00h:00m:00s	2010-08-10 20:02	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-12 20:01	00h:00m:00s	2010-08-12 20:01	Replication Source		0	0%
✓ Completed		2010-08-11 20:01	00h:00m:00s	2010-08-11 20:01	Replication Source		0	0%

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.



Number	Name	Time	Expiration	Plug-in	Retention	Size
9	COD-119...	2007-10-1...	2007-12-1...	Windows...		60,025,844

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 629.
- **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 Avamar system at a time, the Avamar Enterprise Manager replication management feature can manage replication for multiple Avamar systems.

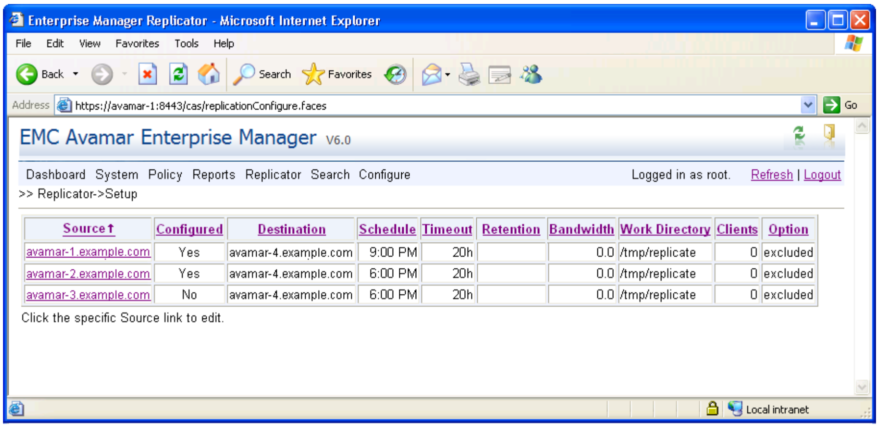
The following table describes the Avamar Enterprise Manager replication management pages

Table 63 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 select Status.
Replicator Setup	Used to configure replication	Place the mouse cursor over the Replicator menu until a sub-menu appears and 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.


Enterprise Manager Replicator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Search Configure
Logged in as root.
Refresh | Logout
Local intranet

https://avamar-1:8443/cas/replicationConfigure.faces

>> Replicator->Setup

Source↑	Configured	Destination	Schedule	Timeout	Retention	Bandwidth	Work Directory	Clients	Option
avamar-1.example.com	Yes	avamar-4.example.com	9:00 PM	20h		0.0	/tmp/replicate	0	excluded
avamar-2.example.com	Yes	avamar-4.example.com	6:00 PM	20h		0.0	/tmp/replicate	0	excluded
avamar-3.example.com	No	avamar-4.example.com	6:00 PM	20h		0.0	/tmp/replicate	0	excluded

Click the specific Source link to edit.

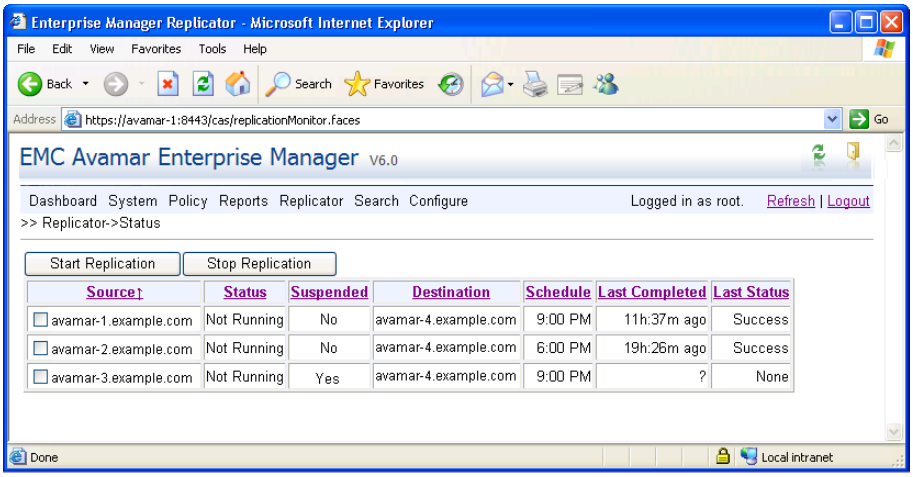
The following table lists the information that appears on the Replicator Setup page for each Avamar system in the Avamar Enterprise Manager configuration.

Table 64 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 334. • No — This Avamar system is not currently configured and enabled for replication operations. "Configuring or modifying replication settings" on page 365 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.


Enterprise Manager Replicator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://avamar-1:8443/cas/replicationMonitor.faces
Go
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Search Configure
Logged in as root.
Refresh | Logout
>> Replicator->Status
Start Replication
Stop Replication
Done
Local intranet

Source↑	Status	Suspended	Destination	Schedule	Last Completed	Last Status
□ avamar-1.example.com	Not Running	No	avamar-4.example.com	9:00 PM	11h:37m ago	Success
□ avamar-2.example.com	Not Running	No	avamar-4.example.com	6:00 PM	19h:26m ago	Success
□ avamar-3.example.com	Not Running	Yes	avamar-4.example.com	9:00 PM	?	None

The following table lists the information that appears on the Replicator Status page for each Avamar system.

Table 65 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.

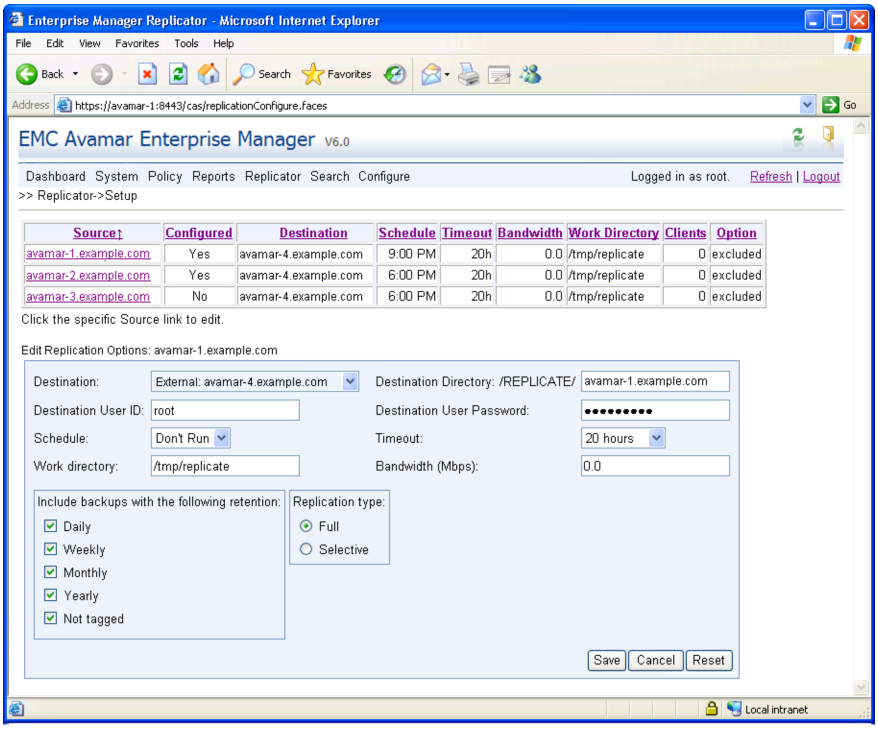
   The Dashboard page appears.

2. Place the mouse cursor over the **Replicator** menu until a sub-menu appears, 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.


Enterprise Manager Replicator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Search Configure
Logged in as root.
Refresh | Logout
Local intranet

Address: https://avamar-1:8443/cas/replicationConfigure.faces

>> Replicator->Setup

Source↑	Configured	Destination	Schedule	Timeout	Bandwidth	Work Directory	Clients	Option
avamar-1.example.com	Yes	avamar-4.example.com	9:00 PM	20h	0.0	/tmp/replicate	0	excluded
avamar-2.example.com	Yes	avamar-4.example.com	6:00 PM	20h	0.0	/tmp/replicate	0	excluded
avamar-3.example.com	No	avamar-4.example.com	6:00 PM	20h	0.0	/tmp/replicate	0	excluded

Click the specific Source link to edit.

Edit Replication Options: avamar-1.example.com

Destination:	External: avamar-4.example.com	Destination Directory: /REPLICATE/	avamar-1.example.com
Destination User ID:	root	Destination User Password:	●●●●●●●●●
Schedule:	Don't Run	Timeout:	20 hours
Work directory:	/tmp/replicate	Bandwidth (Mbps):	0.0

Include backups with the following retention:
☑ Daily
☑ Weekly
☑ Monthly
☑ Yearly
☑ Not tagged

Replication type:
● Full
○ Selective

Save Cancel Reset

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 repluser account.

7. In the **Destination User Password** box, type the password for the Avamar administrative user account ID (repluser).

   The password for the repluser 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 362 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

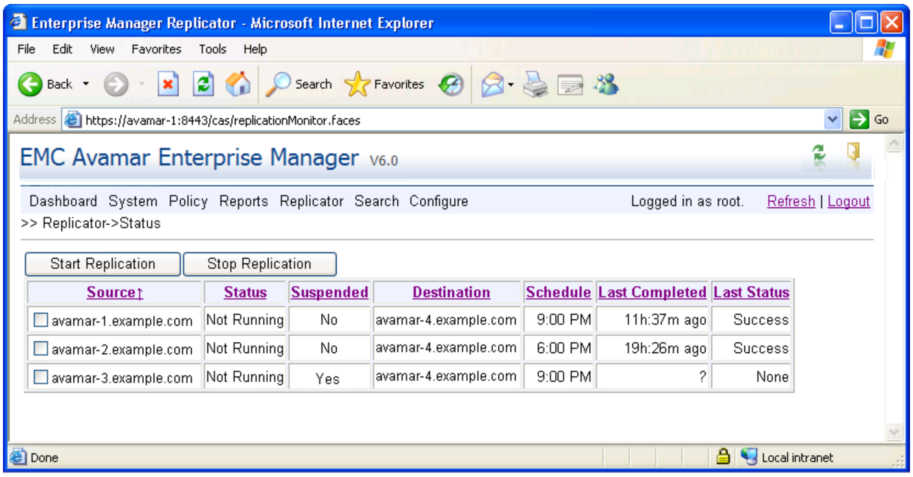
To view the status of replication operations for one or more Avamar servers:

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, then select **Status**.

The Replicator Status page appears.


Enterprise Manager Replicator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Search Configure
Logged in as root.
Refresh | Logout
>> Replicator->Status
Start Replication
Stop Replication
Done
Local intranet

https://avamar-1:8443/cas/replicationMonitor.faces

Source↑	Status	Suspended	Destination	Schedule	Last Completed	Last Status
□ avamar-1.example.com	Not Running	No	avamar-4.example.com	9:00 PM	11h:37m ago	Success
□ avamar-2.example.com	Not Running	No	avamar-4.example.com	6:00 PM	19h:26m ago	Success
□ avamar-3.example.com	Not Running	Yes	avamar-4.example.com	9:00 PM	?	None

The Replicator Status page shows consolidated daily replication status for each Avamar system that you are monitoring.

“Replicator status page” on page 364 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.

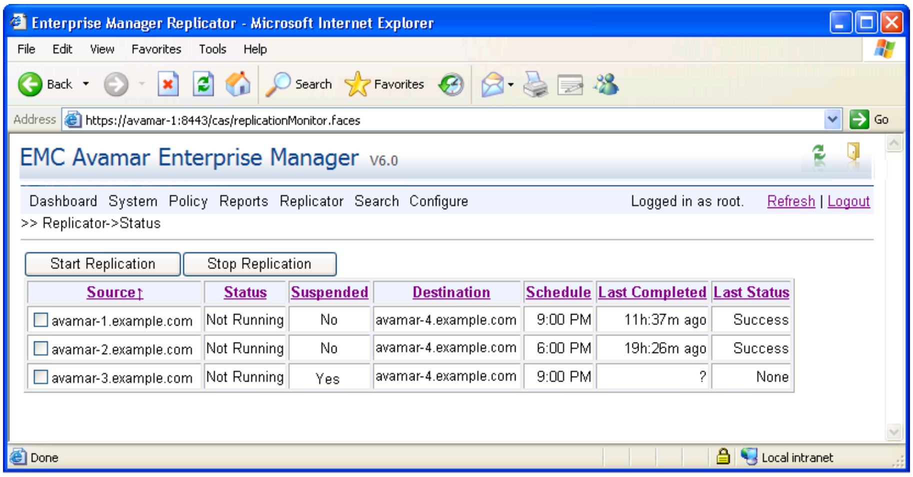
To start or stop daily replications:

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, then select **Status**.

The Replicator Status page appears.



Enterprise Manager Replicator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://avamar-1:8443/cas/replicationMonitor.faces
Go
EMC Avamar Enterprise Manager V6.0
Dashboard System Policy Reports Replicator Search Configure
Logged in as root.
Refresh | Logout
>> Replicator->Status
Start Replication
Stop Replication
Done
Local intranet

Source↑	Status	Suspended	Destination	Schedule	Last Completed	Last Status
□ avamar-1.example.com	Not Running	No	avamar-4.example.com	9:00 PM	11h:37m ago	Success
□ avamar-2.example.com	Not Running	No	avamar-4.example.com	6:00 PM	19h:26m ago	Success
□ avamar-3.example.com	Not Running	Yes	avamar-4.example.com	9:00 PM	?	None

3. Select the checkbox next to the server for which to stop or start replication, and click either **Start Replication** or **Stop Replication**.

CHAPTER 16
Advanced Server Administration and Maintenance

The following topics describe Avamar server administration and maintenance tasks:

- Checkpoints 370
- MCS configuration settings 373
- Configuring directory service information 378
- Setting last backup retention 385
- Manually changing Avamar Administrator client preferences 386
- Updating server licensing 387
- Using the change-passwords utility with default user accounts 391
- Changing single-node server network settings 398
- Adding a custom security notification to web login pages 399
- Manually updating the plug-in catalog 399
- Configuring Avamar to use network address translation 400

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 294.

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 66 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.

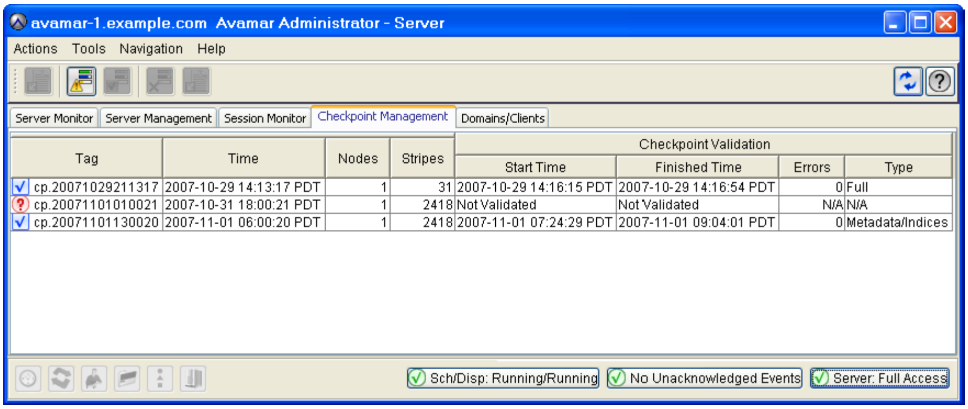
Creating a checkpoint

To create a checkpoint:

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

   The Server window appears.

2. Click the **Checkpoint Management** tab.



Tag	Time	Nodes	Stripes	Checkpoint Validation			
				Start Time	Finished Time	Errors	Type
✓ cp.20071029211317	2007-10-29 14:13:17 PDT	1	31	2007-10-29 14:16:15 PDT	2007-10-29 14:16:54 PDT	0	Full
? cp.20071101010021	2007-10-31 18:00:21 PDT	1	2418	Not Validated	Not Validated	N/A	N/A
✓ cp.20071101130020	2007-11-01 06:00:20 PDT	1	2418	2007-11-01 07:24:29 PDT	2007-11-01 09:04:01 PDT	0	Metadata/Indices

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

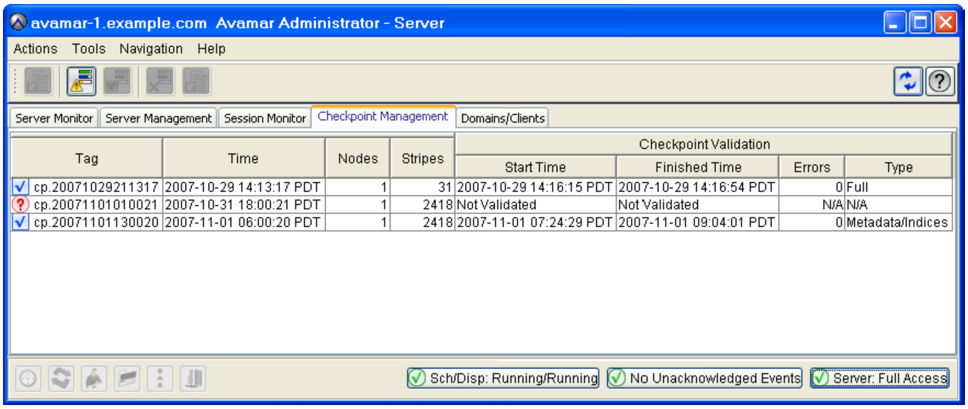
Checkpoint validations can take several hours to perform and only one checkpoint can be validated at a time.

To validate a checkpoint:

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

   The Server window appears.

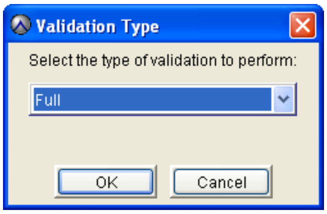
2. Click the **Checkpoint Management** tab.



Tag	Time	Nodes	Stripes	Checkpoint Validation			
				Start Time	Finished Time	Errors	Type
✓ cp.20071029211317	2007-10-29 14:13:17 PDT	1	31	2007-10-29 14:16:15 PDT	2007-10-29 14:16:54 PDT	0	Full
? cp.20071101010021	2007-10-31 18:00:21 PDT	1	2418	Not Validated	Not Validated	N/A	N/A
✓ cp.20071101130020	2007-11-01 06:00:20 PDT	1	2418	2007-11-01 07:24:29 PDT	2007-11-01 09:04:01 PDT	0	Metadata/Indices

3. Select an unvalidated checkpoint and select **Actions › Validate Checkpoint.**

   The Validation Type dialog box appears.



Select the type of validation to perform:

Full

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

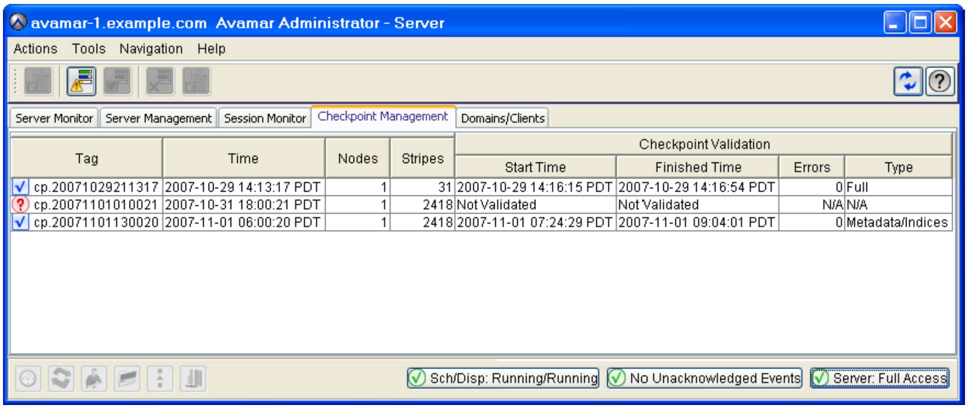
You can delete checkpoints to reclaim additional server storage capacity. Generally, it is best to delete unvalidated checkpoints before you delete validated checkpoints.

To delete a checkpoint:

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

   The Server window appears.

2. Click the **Checkpoint Management** tab.



Tag	Time	Nodes	Stripes	Checkpoint Validation			
				Start Time	Finished Time	Errors	Type
✓ cp.20071029211317	2007-10-29 14:13:17 PDT	1	31	2007-10-29 14:16:15 PDT	2007-10-29 14:16:54 PDT	0	Full
? cp.20071101010021	2007-10-31 18:00:21 PDT	1	2418	Not Validated	Not Validated	N/A	N/A
✓ cp.20071101130020	2007-11-01 06:00:20 PDT	1	2418	2007-11-01 07:24:29 PDT	2007-11-01 09:04:01 PDT	0	Metadata/Indices

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.

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.

MCS configuration settings

The following topics provide details on MCS configuration settings:

- “Understanding MCS configuration settings” on page 373
- “Backing up MCS data” on page 374
- “Performing an on-demand MCS flush” on page 375
- “Finding MCS backups in the system” on page 375
- “Restoring MCS data” on page 376
- “Reverting to default MCS preference settings” on page 377

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.

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 67 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 309.
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 375 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 298.

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. Rename /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml to old.mcserver.xml.
4. Copy the default server preferences file into the /usr/local/avamar/var/mc/server_data/prefs directory by typing:

   ```
   cp
   /usr/local/avamar/lib/mcserver.xml/usr/local/avamar/var/mc/server_d
   ata/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).
5. Restart the MCS by typing:

   ```
   dpnctl start mcs
   ```
6. Resume scheduled operations as discussed in "Suspending and resuming scheduled operations" on page 298.

Configuring directory service information

Avamar Administrator, Avamar Enterprise Manager, and the Avamar client web UI can use existing directory services to authenticate users. You can use multiple LDAP v.3-compliant directory services, such as Microsoft Active Directory Domain Services. Also, you can use a single Network Information Service (NIS) on its own or with the LDAP services.

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.

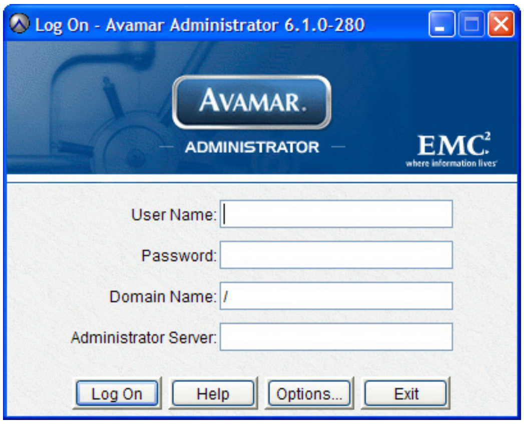
Login requirements

The interface for configuring Avamar to use directory services is only available to users that are assigned the Administrator role and are logged in to the root domain. These requirements are met during the Avamar Administrator log in process.

To log in to Avamar Administrator and use the directory service interface:

1. Launch Avamar Administrator:

   The login window appears.



User Name:

Password:

Domain Name: /

Administrator Server:

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 log in method is described in "Starting Avamar Administrator" on page 40.

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 launcher appears.

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

   The Administration window appears.

8. Click the **LDAP Management** tab.

   NOTICE

   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 378.

2. Click **Add a Directory Service.**

   The Add an Authentication Domain dialog appears.

3. Select **LDAP.**

4. In **Fully Qualified Domain Name,** type the fully qualified domain name (FQDN) of a directory server.

5. (Optional) Select **Make default domain.**

   Select this for the server that represents the organization's default directory service domain.

   NOTICE

   To enable user authentication for the client web UI from Macintosh computers, configure the LDAP server assigned to Macintosh users as the default server.

6. Click **OK.**

   A success dialog appears. If not, see "Error messages for unsuccessful tests" on page 381.

   The changes are immediately applied to the following services:

   - Management Console Server (mcs)
   - Enterprise Manager (em)
   - Desktop and Laptop (dtlt)

7. Click **Close** to close the dialog.

8. Repeat these steps to add any other authentication domains.

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 378.
2. Click **Add a Directory Service.**

   The Add an Authentication Domain dialog appears.
3. Select **NIS.**
4. In **NIS Domain Name,** type the NIS domain name assigned when the NIS domain was set up.
5. In **NIS Domain IP address,** type the IP address of the NIS server.
6. Click **OK.**

   A success dialog appears. If not, see "Error messages for unsuccessful tests" on page 381.
7. 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.**
8. Stop the services by typing:

   ```
   dpnctl stop mcs
   dpnctl stop ems
   dpnctl stop dtlt
   ```
9. Start the services by typing:

   ```
   dpnctl start mcs
   dpnctl start ems
   dpnctl start dtlt
   ```
10. Click **Close** to close the dialog.

Testing an LDAP entry

To test an LDAP entry:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 378.
2. Click **Test a Directory Service.**

   The Test an Authentication Domain dialog appears.
3. Select **LDAP.**

4. In **Fully Qualified LDAP Domain Name**, type the FQDN of an LDAP-compatible directory server to test.

5. In **Username**, type the username for an account that is authorized to read the LDAP database.

6. In **Password**, type the password associated with the username.

7. Click **OK**.

   The test results appear in a dialog. If the test is not a success, see "Error messages for unsuccessful tests" on page 381.

8. Click **Close** to close the dialog.

Testing an NIS entry

To test an NIS entry:

1. Launch Avamar Administrator, log in, and navigate to the **LDAP Management** tab, as described in "Login requirements" on page 378.

2. Click **Test a Directory Service**.

   The Test an Authentication Domain dialog appears.

3. Select **NIS**.

4. In **NIS Domain Name**, type an NIS domain name to test.

5. In **Username**, type the username for an account that is authorized to read the NIS database.

6. In **Password**, type the password associated with the username.

7. Click **OK**.

   The test results appear in a dialog.. If the test is not a success, see "Error messages for unsuccessful tests" on page 381.

8. Click **Close** to close the dialog.

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 68 Error message information (page 1 of 2)

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.

Table 68 Error message information (page 2 of 2)

Message	Description
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 378.
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.*r1.example.abc.com***=ldap://***dchost.r1.example.abc.com:389*

  where *r1.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=*dchost.example.abc.com*

  where *dchost.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 69 KV pairs in ldap.properties (page 1 of 2)

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.

Table 69 KV pairs in ldap.properties (page 2 of 2)

Key	Values	Description
support-nis-authentication	true false	Enables (false) or disables (true) 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 379 and "Providing NIS information" on page 380.
- Testing a directory service, as described in "Testing an LDAP entry" on page 380 and "Testing an NIS entry" on page 381.

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. 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 ldap node, as shown here:

```
<node name="ldap">
   <map>
      <entry key="enable_new_user_authentication_selection"
value="false" />
      <entry key="ldap_services_timeout_seconds" value="300" />
   </map>
</node>
```

5. Change the value of the entry with key="ldap_services_timeout_seconds" to a new time-out value in seconds:

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

6. Save the change and close the editor.

7. Restart the Management Console Server (mcs) service by typing:

```
dpnctl stop mcs
dpnctl start mcs
```

8. 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.

To change the default behavior and always retain the last backup:

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.

After this change, the last backup is retained for all clients. When a new backup runs, the new backup becomes the “last backup” and the previous “last backup” is treated according to its retention policy.

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.

The assigned license keys for standard Avamar products are available 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.

The assigned license keys for Avamar products that the EMC Backup Software suite models include, are available from Powerlink. To access Powerlink, type the login credentials provided in the EMC License Authorization (LAC) email sent to you from licensingnorthamerica@emc.com, licensingemea@emc.com, or licensingapj@emc.com.

If you cannot find the email:

1. Send an email to licensing@emc.com to request the EMC License Authorization email be resent.
2. Include the EMC product SO number in the email.

The following is an example of an assigned license key:

EMC Avamar Software License Key Information
Avamar System Customer Account ID: CN-10062734404
Avamar System Asset ID: A-2010014578

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 388.

   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 388.

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 390.

3. Install the license on the Avamar server as described in "Installing and activating the license" on page 390.

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 390, 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.

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

IMPORTANT

After using this utility to change the password for the MCUser account, use dpnctl to restart the Avamar Desktop/Laptop service, dtlt, as described in "Stopping and starting Avamar Desktop/Laptop server" on page 521. If the service is not restarted, Avamar client users will encounter session expired messages when they log into the web UI.

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 Technical Note*. All Avamar documentation, including this technical note, is available from the Avamar Support landing page at https://support.EMC.com/products/Avamar.

The part number for this technical note is 300-007-53.

Adding a custom security notification to web login pages

Avamar Enterprise Manager and the Avamar Web Access features enable you to include a custom security notification to users on their login pages. These notifications typically explain that only authorized users are permitted access. They also list the penalties for unauthorized access.

To implement these notifications, add the following plain-text files to the /usr/local/avamar/var/em/server_data/ directory:

- `disclaimer_EM.txt`
- `disclaimer_Web_Restore.txt`

The disclaimer_EM.txt file stores the custom security notification for the Avamar Enterprise Manager login page. The disclaimer_Web_Restore.txt file stores the custom security notification for the Avamar Web Access login page.

To customize security notification language, create these files in a text editor, add content and save them to the /usr/local/avamar/var/em/server_data/ directory. Either file can contain plain text or HTML content.

To discontinue the display of the additional security notifications, remove these files. It is also permissible for these files to be empty.

Manually updating the plug-in catalog

Beginning with Avamar 4.1, you can add new clients to an operational Avamar system without a system upgrade. When you add the new clients, Avamar 4.1 systems automatically update the consolidated plug-in catalog.

However, if you add new clients to an Avamar 4.0.x or earlier system, you must manually update the consolidated plug-in catalog for those clients to be recognized by the system.

To manually update the plug-in catalog:

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. Go to the directory that contains the plugin_catalog.xml file and rename it by typing:

   ```
   cd /usr/local/avamar/lib
   mv plugin_catalog.xml plugin_catalog.xml.old
   ```

3. Obtain the updated consolidated plug-in catalog.

   In most cases, EMC Customer Service provides this for you.
4. Copy the updated consolidated plug-in catalog to the /usr/local/avamar/lib directory.

5. Ensure that the updated plugin_catalog.xml file has the correct ownership and permissions by typing:

   ```
   ls -l plugin_catalog.xml
   ```

   Correct ownership and permissions are:

   ```
   304 -rw-r--r-- 1 root admin 305578 Jun 3 14:21 plugin_catalog.xml
   ```

6. If ownership and permissions are not correct, set them by typing:

   ```
   chmod 644 plugin_catalog.xml
   chown root:admin plugin_catalog.xml
   ```

7. Stop and then restart the MCS to enable the MCS to read the updated plugin_catalog.xml by typing:

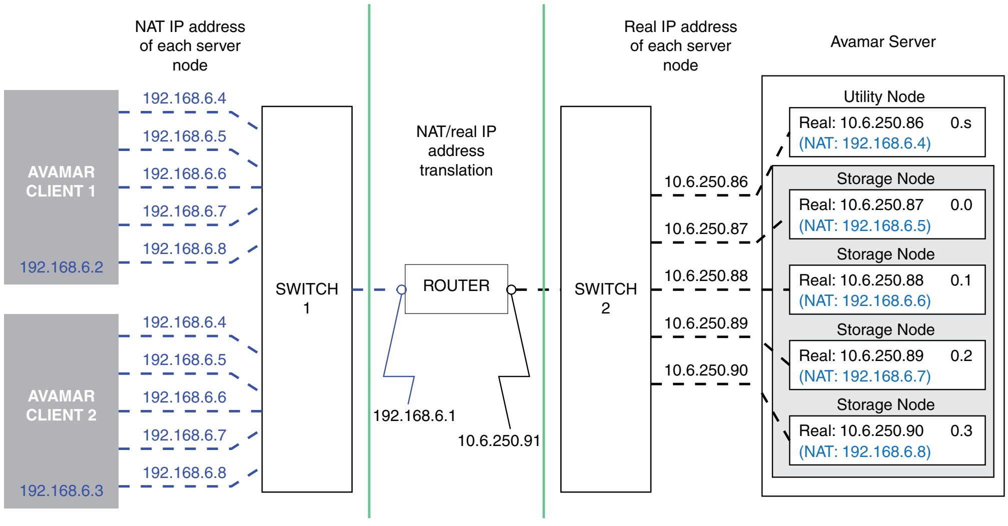
   ```
   dpnctl stop mcs
   dpnctl start mcs
   ```

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 52 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 70 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.. 404
- Avamar Downloader Service.. 405
- Installing the Avamar Downloader Service.. 406
- Configuring the Avamar Downloader Service 409
- Using the Avamar Downloader Service 411
- Troubleshooting Avamar Downloader Service issues 414
- Uninstalling the Avamar Downloader Service... 415
- Installing packages from System Maintenance 415
- Viewing installation history information 422

Overview

As part of an Avamar 6.1 server software installation or upgrade, EMC Customer Service installs:

- 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:

- 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 that contains:
  - Avamar Downloader Service Configuration
  - Start Avamar Downloader Service Monitor
- Desktop shortcut to the Avamar Downloader Service configuration application.

The AvInstaller manages:

- 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. 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 site prohibits access to the Internet, you can manually copy packages to the /data01/avamar/repo directory, and then move them to the /packages directory on the utility node or single-node server instead of using the Avamar Downloader Service.

Avamar Downloader Service components

The following table describes the components of the Avamar Downloader Service.

Table 71 Avamar Downloader Service components

Component	Description
AvamarDownloaderService 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
A	Task tray icon for the Avamar Downloader Service application. Moving the mouse over this icon displays status messages from the Avamar Downloader Service monitor. “Monitoring Avamar Downloader Service status” on page 411 provides more information. Right-clicking this icon displays three options: • Configure Avamar Downloader Service — Opens the Avamar Downloader Service configuration application. • Open Download Repository — Opens the local file cache directory on the Windows server: C:\Program Files\EMC\Avamar Downloader Service\repository • Close Notification Display — Closes the task tray application.

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. The following table provides the installation requirements for the Avamar Downloader Service.

Table 72 Installation requirements for the Avamar Downloader Service

Software/hardware	Requirement
Operating system	• Microsoft Windows Server 2003 SP1 • Microsoft Windows Server 2003 SP2 • Microsoft Windows Vista • Microsoft Windows 7 • Microsoft Windows Server 2008 • Microsoft Windows XP SP3 **Note:** The Avamar Downloader Service does not support R2 versions for Microsoft Windows Server.
Filesystem	Any filesystem
Hard drive space	Minimum of 12 MB
RAM	Minimum of 20 MB

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

To download the 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://AVAMARSERVER
   ```

   where AVAMARSERVER is the Avamar system network hostname (as defined in DNS) or IP address.

   The Avamar Web Restore page appears.
3. Click **Download and Documents.**

   The Avamar Web Documents and Downloads page appears.
4. Click the correct operating system hyperlink for the Windows computer.

   A directory listing appears.

5. Click the **AvamarDownloaderService-windows-PLATFORM-VERSION.exe** hyperlink.

   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.

6. Click **Save** to save the file to a directory on the computer.

Installing the software

To install the 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 Select Installation 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 **Browse.**

      The Browse for Folder dialog box appears.

   b. Navigate to a folder to use for the installation.

   c. Click **OK** to accept the folder and to close the dialog box.

      The Folder text box displays the new folder.

   d. Click **Next** to continue.

   The Confirm Installation page appears.

4. Click **Next.**

   The Installing Avamar Downloader Service page appears, which displays a progress bar as the installation proceeds.

   After the installation completes, the Installation Complete page appears.

5. Click **Close.**

   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 408 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.

To define 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**.

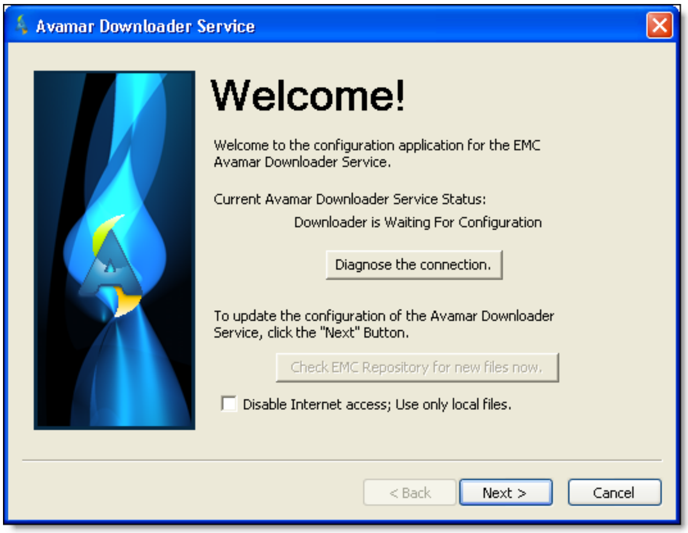
5. In the **Windows Firewall with Advanced Security** interface verify that the **Inbound Rules** list contains the **Avamar Downloader Service Program from EMC** entry.

Configuring the Avamar Downloader Service

To configure the Avamar Downloader Service:

1. Click (Avamar Downloader Service task tray icon).

   The Welcome! page appears.



Avamar Downloader Service

Welcome!

Welcome to the configuration application for the EMC Avamar Downloader Service.

Current Avamar Downloader Service Status:
Downloader is Waiting For Configuration

To update the configuration of the Avamar Downloader Service, click the "Next" Button.

□ Disable Internet access; Use only local files.

NOTICE

The first time you run the Avamar Downloader Service application, the Current Avamar Downloader Service Status is “Downloader is Waiting For Configuration.”

2. Click **Next**.

   The EMC FTP Credentials page appears.

NOTICE

Do not change the FTP username and password credentials. If you change the FTP username or password, you must reinstall the Avamar Downloader Service to recover these credentials.

3. Accept the default FTP username and password, and then click **Next**.

   The Proxy Configuration page appears.

4. (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 11.2.345.67).

   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.

5. Click **Next**.

   The Avamar Systems page appears.

6. Click **Add**.

   The Avamar Downloader Service - Add Known System dialog box appears.

7. 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**.

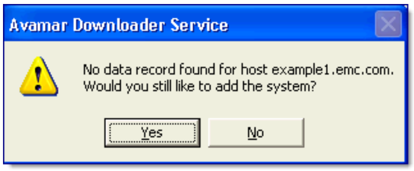
   c. In the **Password** field, type the root password.

   d. In the **Confirm Password** field, retype the root password.

8. Click **OK**.

   The system is added to the Known Systems list.

   If the hostname cannot be resolved, the following informational dialog box appears:

   No data record found for host example1.emc.com.
   Would you still like to add the system?

   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.

9. Repeat step 6 through step 8 to add all remaining Avamar systems.

10. Click **Next**.

    The Review Configuration page appears.

11. Review the configuration details, and then click **Finish**.

    The status from the Avamar Downloader Service changes to OK.

Using the Avamar Downloader Service

This topic describes how to use the Avamar Downloader Service to:

- Start the Avamar Downloader Service configuration application
- Monitor status messages
- Configure Avamar Downloader Service settings
- Check the EMC repository for new files
- Add new Avamar systems to the Known Systems list
- Modify an Avamar system’s username and password
- Remove an Avamar system from the Known Systems list

Starting the Avamar Downloader Service configuration application

To start the Avamar Downloader Service configuration application, use one of the following methods:

- From the **Start** menu, select **Programs** › **EMC** › **Avamar** › **Avamar Downloader Service Configuration.**
- Click the task tray icon.
- Double-click the Avamar Downloader Service desktop 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.

The following table lists Avamar Downloader Service monitor status messages.

Table 73 Avamar Downloader Service monitor status messages (page 1 of 2)

Status message	Description
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.

Table 73 Avamar Downloader Service monitor status messages (page 2 of 2)

Status message	Description
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.

To manually start the monitor, click **Start** and select **Programs** › **EMC** › **Avamar** › **Avamar Downloader Service** › **Start Avamar Downloader Service Monitor**.

Stopping the monitor

To stop the monitor, right-click the Avamar Downloader Service task tray icon, and then select **Close Notification Display**.

Checking the EMC repository

You can check the EMC repository for updates at any time.

To check the EMC repository for new updates:

1. Click A (Avamar Downloader Service task tray icon).

   The Welcome! page appears.

2. Click **Check EMC Repository for new files now**.

   The Avamar Downloader Service:

   - 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 time period is 30 days.

   NOTICE

   You cannot click **Check EMC Repository for new files now** if the status of the Avamar Downloader Service is anything other than OK or “waiting for new files.”

3. Click **Cancel** to exit the configuration application.

Modifying the username or password

To modify the username or password:

1. Click A (Avamar Downloader Service task tray icon).

   The Welcome! page appears.

2. Click **Next**.

   The EMC Credentials page appears. The program automatically fills in the username and password fields.

3. Type the password in the **Confirm Password** field, and then click **Next**.

   The EMC FTP Credentials page appears. The program automatically fills in the username and password fields.

4. Type the password in the **Confirm Password** field, and then click **Next**.

   The Avamar Systems page appears.

5. Select the system from the Known Systems list and click **Modify**.

   The Avamar Downloader Service - Add Known Systems page appears.

6. Make the necessary changes and click **OK**.

7. Click **Next**.

   The Review Configuration page appears.

8. Review the configuration details, and then click **Finish**.

Removing an Avamar system from the Known Systems list

To remove an Avamar system from the Known Systems list:

1. Click A (Avamar Downloader Service task tray icon).

   The Welcome! page appears.

2. Click **Next**.

   The EMC Credentials page appears. The program automatically fills in the username and password fields.

3. Type the password in the **Confirm Password** field, and then click **Next**.

   The EMC FTP Credentials page appears. The program automatically fills in the username and password fields.

4. Type the password in the **Confirm Password** field, and then click **Next**.

   The Avamar Systems page appears.

5. Select the system from the Known Systems list and click **Remove**.

   A confirmation dialog box appears.

6. Click **Yes** to remove the system from the Known Systems list.

7. Click **Next**.

   The Review Configuration page appears.

8. Review the configuration details, and then click **Finish**.

Checking the Avamar Downloader Service version

To check the version of the Avamar Downloader Service:

1. Click A (Avamar Downloader Service task tray icon).

2. Click About

   The About box appears.

3. Review the contents, and click OK.

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 EMC Repository for new files now, the Avamar Downloader Service writes the following error messages to the 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 408 provides instructions.

Downloading a package fails

If the utility node or single-node server cannot access the Windows host computer, a message similar to the following might appear when you attempt 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
```

Uninstalling the Avamar Downloader Service

To uninstall the Avamar Downloader Service:

1. Exit any running applications.
2. From the **Start** menu, select **Settings** › **Control Panel** › **Add or Remove Programs**.

   The Add or Remove Programs window appears.

3. Select Avamar Downloader Service from the list of currently installed programs, and then click **Remove**.

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:

- 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 Service. This account enables EMC Customer Service access to restricted installation packages for the Avamar server that must be installed only by EMC Customer Service. The gray lock icon in the tab bar provides access to the EMC Customer Support account.

NOTICE

Only EMC Customer Service 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 the following table.

Table 74 Item and column descriptions

<table>
<tr><th>Item or column</th><th colspan="2">Description</th></tr>
<tr><td>⬆</td><td colspan="2">Indicates that packages are available for installation.</td></tr>
<tr><td>Systems pane</td><td colspan="2">Provides package availability and operational status about each Avamar server.</td></tr>
<tr><td>AVP</td><td>A</td><td>Indicates that one or more packages are available to download and install on the Avamar server.</td></tr>
<tr><td rowspan="3">Status</td><td>✓</td><td>Indicates that the Avamar Installation Manager is running on the Avamar server.</td></tr>
<tr><td>!</td><td>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.</td></tr>
<tr><td>✱</td><td>Indicates that an Avamar package installation is in progress.</td></tr>
<tr><td>System</td><td colspan="2">Displays the Fully Qualified Domain Name for the Avamar server.</td></tr>
<tr><td>Version</td><td colspan="2">Displays the version of the Avamar server software.</td></tr>
<tr><td>Package List pane</td><td colspan="2">Displays available installation packages for the Avamar server.</td></tr>
<tr><td>Grouping list</td><td colspan="2">Enables you to group packages by type: Show All or Hotfix.</td></tr>
<tr><td>Sort by list</td><td colspan="2">Enables you to sort the packages by title, status, or priority.</td></tr>
<tr><td>Download button</td><td colspan="2">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.
Note: You can download multiple packages at the same time, but install only one package at a time. You can also install a package while you are downloading packages.</td></tr>
<tr><td>Install button</td><td colspan="2">Starts the installation process. The Install button appears only after the package has been downloaded to the local repository.</td></tr>
<tr><td>Monitor button</td><td colspan="2">Displays the Installation Progress page.</td></tr>
<tr><td>Delete button</td><td colspan="2">Deletes the package from the local repository.</td></tr>
<tr><td>Continue button</td><td colspan="2">Indicates that a package is in the initial installation phase (deployed but not yet started).
Clicking Continue displays the Installation Setup page.</td></tr>
</table>

NOTICE

If you accidently close the browser during the installation of a patch, update, or upgrade package, the installation is not stopped. 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 terminated.

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.

To install workflow packages:

1. Open a web browser and log in to Avamar Enterprise Manager:

   a. In the web browser, type:

      `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.

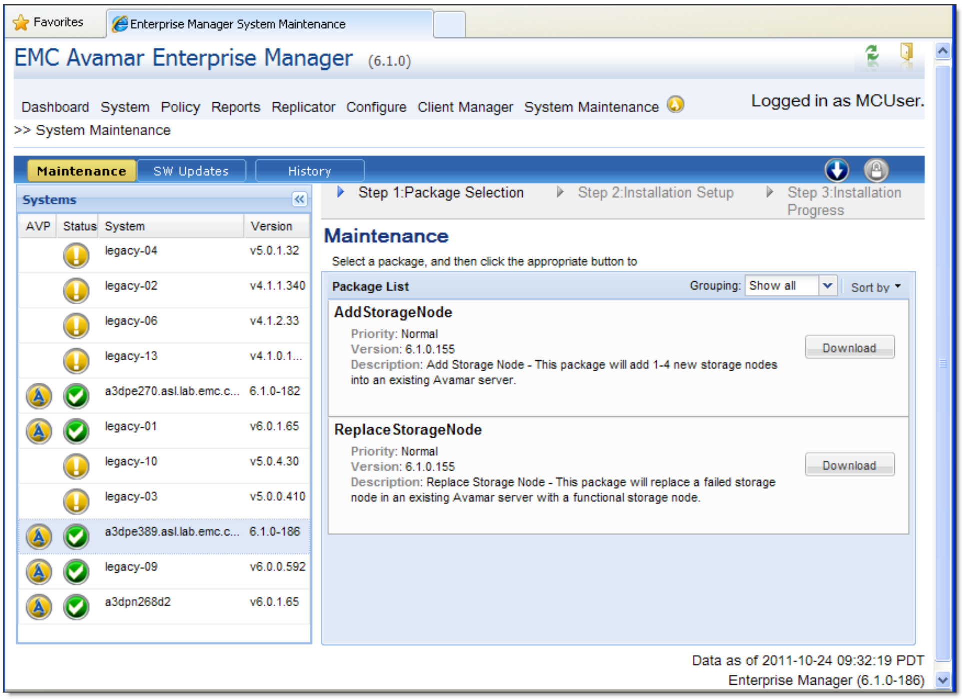
   c. Click **Log On**.

      The EMC Avamar Enterprise Manager dashboard page appears.

2. Click **System Maintenance**.

   The System Maintenance page appears.

If workflow packages are available for any Avamar server in the configuration, the Maintenance tab appears.



Systems

AVP	Status	System	Version
	!	legacy-04	v5.0.1.32
	!	legacy-02	v4.1.1.340
	!	legacy-06	v4.1.2.33
	!	legacy-13	v4.1.0.1...
A	✓	a3dpe270.asl.lab.emc.c...	6.1.0-182
A	✓	legacy-01	v6.0.1.65
	!	legacy-10	v5.0.4.30
	!	legacy-03	v5.0.0.410
A	✓	a3dpe389.asl.lab.emc.c...	6.1.0-186
A	✓	legacy-09	v6.0.0.592
A	✓	a3dpn268d2	v6.0.1.65

Maintenance

Select a package, and then click the appropriate button to

Package List Grouping: Show all Sort by

AddStorageNode
Priority: Normal
Version: 6.1.0.155
Description: Add Storage Node - This package will add 1-4 new storage nodes into an existing Avamar server.

ReplaceStorageNode
Priority: Normal
Version: 6.1.0.155
Description: Replace Storage Node - This package will replace a failed storage node in an existing Avamar server with a functional storage node.

Data as of 2011-10-24 09:32:19 PDT
Enterprise Manager (6.1.0-186)

3. Click **Maintenance**.

4. Select a system from the **Systems** list.

   Workflow packages available for the system you selected appear in the Package List.

5. To 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 ? .

   c. Click **Install** to start the installation.

      The background color for the package changes to yellow and the initialization begins.

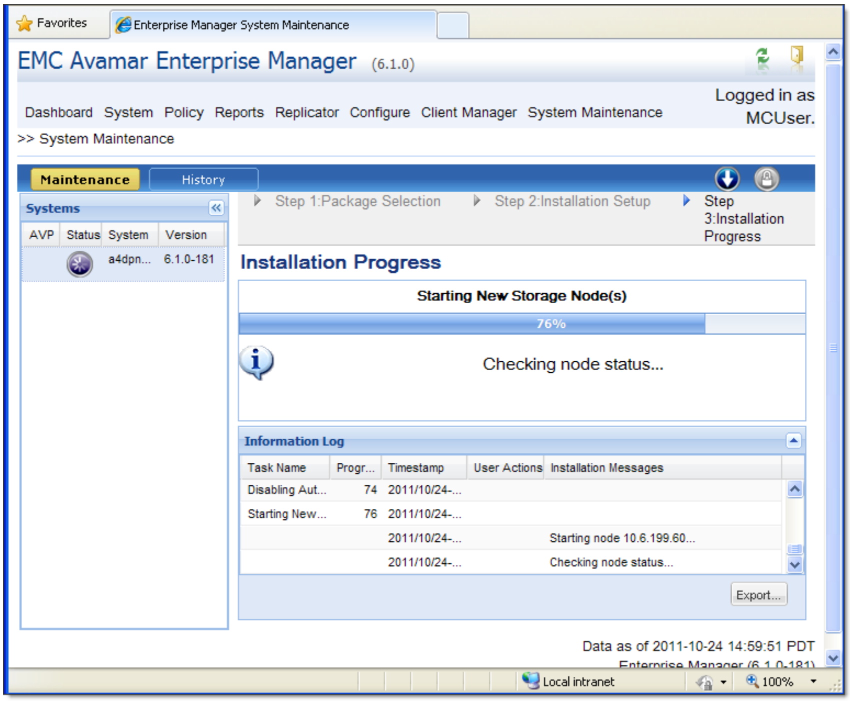
      When the initialization process finishes, the Installation Setup page appears.

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.



Starting New Storage Node(s)

Checking node status...

Task Name	Progr...	Timestamp	User Actions	Installation Messages
Disabling Aut...	74	2011/10/24-...		
Starting New...	76	2011/10/24-...		
		2011/10/24-...		Starting node 10.6.199.60...
		2011/10/24-...		Checking node status...

Data as of 2011-10-24 14:59:51 PDT

Enterprise Manager (6.1.0-181)

The following table describes the Installation Progress page.

Table 75 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:

   - 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 421 provides more information about the use of the **Delete** button.

Installing patch and hotfix packages from the SW Updates tab

To install 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. If requested, provide installation setup information.

   NOTICE

   Installation setup requirements are specific to the type of package. Some packages do not require any installation setup.

9. If available, provide advanced settings:

   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, which is described in the following table, appears.

Table 76 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 hotfix, patch, or workflow 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 Service can delete restricted packages.

To delete 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.

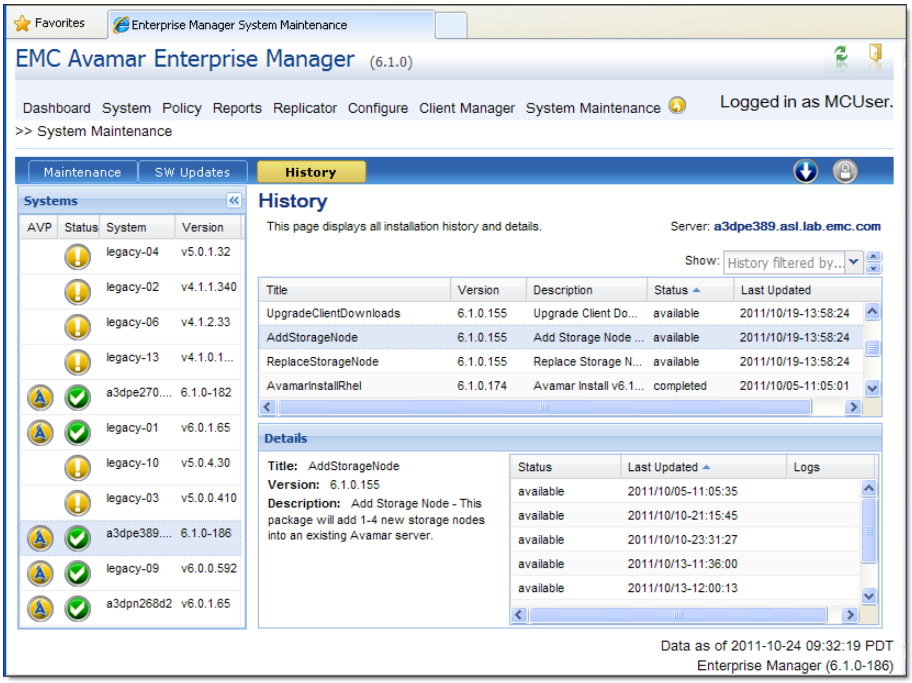
     The **Maintenance** tab only appears if one or more workflow packages are available for the Avamar servers in the configuration.
4. Select a system from the **Systems** list.

   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, therefore, is listed as the last item in the table.


Favorites
Enterprise Manager System Maintenance
EMC Avamar Enterprise Manager (6.1.0)
Dashboard System Policy Reports Replicator Configure Client Manager System Maintenance
Logged in as MCUser.
>> System Maintenance
Maintenance
SW Updates
History
Systems
Show:
History filtered by...
Details

AVP	Status	System	Version
	!	legacy-04	v5.0.1.32
	!	legacy-02	v4.1.1.340
	!	legacy-06	v4.1.2.33
	!	legacy-13	v4.1.0.1...
A	✓	a3dpe270....	6.1.0-182
A	✓	legacy-01	v6.0.1.65
	!	legacy-10	v5.0.4.30
	!	legacy-03	v5.0.0.410
A	✓	a3dpe389....	6.1.0-186
A	✓	legacy-09	v6.0.0.592
A	✓	a3dpn268d2	v6.0.1.65

History

This page displays all installation history and details.

Server: a3dpe389.asl.lab.emc.com

Title	Version	Description	Status ▲	Last Updated
UpgradeClientDownloads	6.1.0.155	Upgrade Client Do...	available	2011/10/19-13:58:24
AddStorageNode	6.1.0.155	Add Storage Node ...	available	2011/10/19-13:58:24
ReplaceStorageNode	6.1.0.155	Replace Storage N...	available	2011/10/19-13:58:24
AvamarInstallRhel	6.1.0.174	Avamar Install v6.1...	completed	2011/10/05-11:05:01

Title: AddStorageNode
Version: 6.1.0.155
Description: Add Storage Node - This package will add 1-4 new storage nodes into an existing Avamar server.

Status	Last Updated ▲	Logs
available	2011/10/05-11:05:35	
available	2011/10/10-21:15:45	
available	2011/10/10-23:31:27	
available	2011/10/13-11:36:00	
available	2011/10/13-12:00:13	

Data as of 2011-10-24 09:32:19 PDT
Enterprise Manager (6.1.0-186)

From the History page you can:

- Toggle the sort order from ascending to descending by clicking on the heading in any column.

  An up 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 (top 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.

The following table describes the column headings in the History table.

Table 77 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 currently 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.

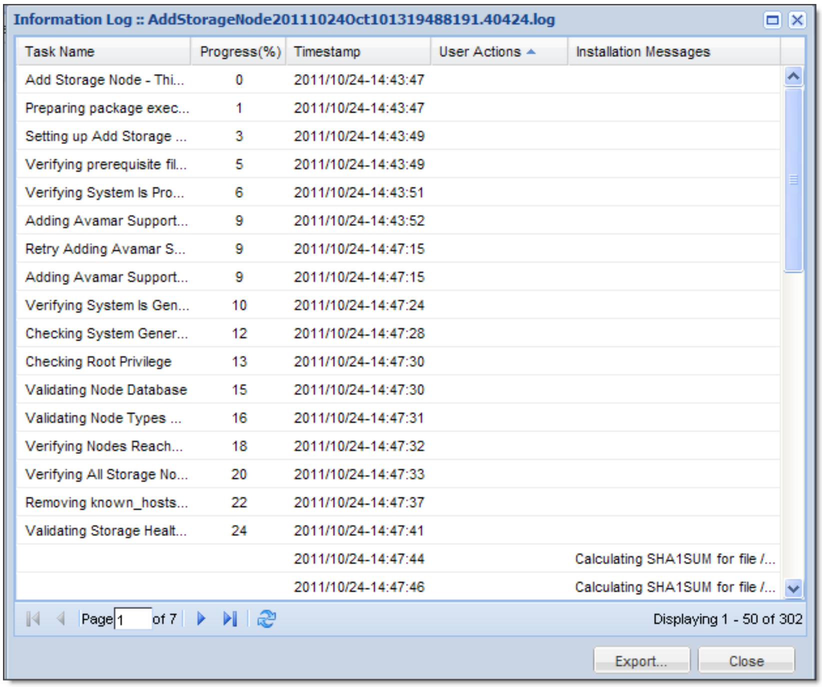
The following table describes the column headings in the Details table.

Table 78 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 pop-up window appears. The following figure shows example log information.



Information Log :: AddStorageNode20111024Oct101319488191.40424.log

Task Name	Progress(%)	Timestamp	User Actions	Installation Messages
Add Storage Node - Thi...	0	2011/10/24-14:43:47		
Preparing package exec...	1	2011/10/24-14:43:47		
Setting up Add Storage ...	3	2011/10/24-14:43:49		
Verifying prerequisite fil...	5	2011/10/24-14:43:49		
Verifying System Is Pro...	6	2011/10/24-14:43:51		
Adding Avamar Support...	9	2011/10/24-14:43:52		
Retry Adding Avamar S...	9	2011/10/24-14:47:15		
Adding Avamar Support...	9	2011/10/24-14:47:15		
Verifying System Is Gen...	10	2011/10/24-14:47:24		
Checking System Gener...	12	2011/10/24-14:47:28		
Checking Root Privilege	13	2011/10/24-14:47:30		
Validating Node Database	15	2011/10/24-14:47:30		
Validating Node Types ...	16	2011/10/24-14:47:31		
Verifying Nodes Reach...	18	2011/10/24-14:47:32		
Verifying All Storage No...	20	2011/10/24-14:47:33		
Removing known_hosts...	22	2011/10/24-14:47:37		
Validating Storage Healt...	24	2011/10/24-14:47:41		
		2011/10/24-14:47:44		Calculating SHA1SUM for file /...
		2011/10/24-14:47:46		Calculating SHA1SUM for file /...

NOTICE

To enlarge the window, click the ▭ icon (top right corner).

NOTICE

If you use the Mozilla Firefox 3.x browser, it may become sluggish when scrolling through a log table that contains more that 200 lines or when the system has limited RAM available. The Internet Explorer 7 or 8 browser does not have this problem.

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 Sun Solaris client system back to its original system state:

- Windows client system recovery 428
- Red Hat and CentOS Linux system recovery 428
- SUSE Linux system recovery 436
- Sun Solaris system recovery 444

Windows client system recovery

The following table lists the locations of client system recovery information for Windows operating systems.

Table 79 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 filesystem 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 and Restore window appears.

   b. Click the Select for 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 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.

Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

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 filesystem 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 filesystems.

   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 428 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 430.
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 filesystem 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 filesystem directly to /mnt/sysimage because there is currently no method that restricts 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 filesystems other than the root filesystem 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 filesystem 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 428. 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.

Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

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 Note: 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 filesystems are mounted as expected by typing the following on the command line:

    ```
    df -h
    ```

    b. Compare the output to the expected set of mounted filesystems.

    c. If there are discrepancies, mount the devices onto the appropriate mount points, as determined during “Reconstruct partition table” on page 428.

    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 428.

    – /home is an example mount point.

    Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

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 step d — step 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 filesystem 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 filesystems 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 filesystems to mount to /mnt/sysimage.

   Note: If you saved a reference copy of the fstab file during "Recovery target client preparation" on page 430, 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.Note:.

f. If so, ensure that they get moved to their proper restore locations by performing step 8.Note: through step 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 step 2 through step 4 of the "Recovery procedure" on page 430.

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 11 of the "Recovery procedure" on page 430.

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 filesystem 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 and Restore window appears.

   b. Click the **Select for 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.

   Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

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 filesystem 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 filesystems. 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 436 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 438.
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 filesystem.

   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-filesystems 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 filesystem root by typing:

   ```
   chroot /mnt
   ```

7. Start the network as configured in the prerequisites by typing:

   ```
   rcnetwork start
   ```

8. Mount the auto-mount filesystems and verify that the correct filesystems were mounted by typing:

   ```
   mount -a;df -h
   ```

9. If any filesystems 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 filesystems other than the root filesystem 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 filesystem 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 436.

    Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

    Use --**exclude=PATH** options to exclude paths that were identified as separate mount points during "Reconstruct partition table" on page 436. 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 filesystems are mounted as expected by typing:

    ```
    df -h
    ```

    b. Compare the output to the expected set of mounted filesystems.

    c. If there are discrepancies, mount the devices onto the appropriate mount points, as determined during “Reconstruct partition table” on page 436.

    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.

    Note: Space limitations in this guide cause the previous command example to continue to more than one line. You must type the command on a single command line with no line feeds or returns.

    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 step d — step 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 filesystem 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 filesystems 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 filesystems to mount to /mnt.

    Note: If you saved a reference copy of the fstab file during "Recovery target client preparation" on page 438, 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 438.
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.

Sun Solaris system recovery

This procedure describes how to restore a Sun 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

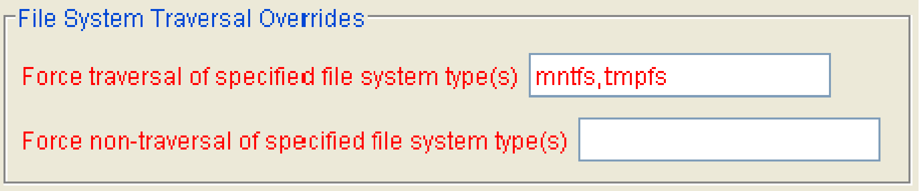
To successfully restore a Sun Solaris client system to its original system state, there must be an Avamar backup containing the entire local filesystem and the following critical system files and virtual filesystems. This is accomplished by forcing traversal of the targets listed in the following table during a backup.

Table 80 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:



File System Traversal Overrides

Force traversal of specified file system type(s): mntfs,tmpfs

Force non-traversal of specified file system type(s):

- Specify **--forcefs=”mntfs,tmpfs”** on the **avtar** command line.

You can also optionally include any of the following other system directories and virtual filesystems in a backup by forcing traversal of the targets in the following table.

Table 81 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 81 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 filesystems

If the client you are attempting to recover previously used network mounted /var and /opt filesystems, make every effort to mount and use those same network mounted /var and /opt filesystems 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.

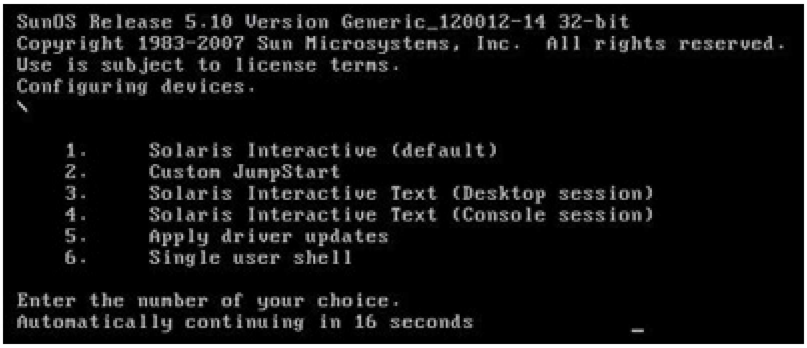
Procedure

To recover a Sun Solaris client system:

1. Boot from CDROM by typing:

   ```
   reboot -- cdrom
   ```

2. (Solaris 10 only) If you are restoring a Solaris 10 client, at the boot options menu, select either option **3. Solaris Interactive Text (Desktop session)** or option **4. Solaris Interactive Text (Console session)**.



```
SunOS Release 5.10 Version Generic_120012-14 32-bit
Copyright 1983-2007 Sun Microsystems, Inc.  All rights reserved.
Use is subject to license terms.
Configuring devices.
\

    1.     Solaris Interactive (default)
    2.     Custom JumpStart
    3.     Solaris Interactive Text (Desktop session)
    4.     Solaris Interactive Text (Console session)
    5.     Apply driver updates
    6.     Single user shell

Enter the number of your choice.
Automatically continuing in 16 seconds
```

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 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.

   This is so that **pkgadd** and **pkgrm** commands do not quit with errors such as:

   ```
   nonexistent admin file or bad device (/var/sadm/pkg) specified
   ```

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 8 or 9 — AvamarClient-solaris8-sparc-VERSION.pkg
   - Solaris 10 SPARC — AvamarClient-solaris10-x86-VERSION.pkg
   - Solaris 10 X86 — AvamarClient-solaris10-x86-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 filesystems 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=USER
    --password=PASSWORD --account=/DOMAIN/CLIENT-NAME --target=. /etc
    ```

    where:

    - AVAMARSERVER is the hostname or IP address of the Avamar server
    - USER and PASSWORD are the Avamar login credentials
    - DOMAIN and CLIENT-NAME is the Solaris client to restore

    Note this information for use in the remainder of this procedure.

NOTICE

These login credentials must be assigned a role (described in "Understanding users, authentication, and roles" on page 67) that allows access to the backups for this client on the Avamar server.

NOTICE

You cannot restore the root filesystem 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 filesystem.
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 and Restore window appears.
14. Click the **Select for 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 /.
18. For each directory that originally existed under / (and therefore needs to be restored from the Avamar backup), 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=USER
       --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 the Avamar Client Manager, which is a web-based management application that provides centralized Avamar client administration capabilities for larger businesses and enterprises:

- Capabilities 450
- Starting Avamar Client Manager 451
- General information 451
- Managing clients 459
- Analyzing client activity........ 471
- Upgrading Avamar clients 483
- Activating clients 490

Capabilities

Avamar Client Manager is designed to facilitate 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.

Management tasks — Avamar Client Manager enables you to work with large numbers of clients when performing the following tasks:

- Moving clients to a new server
- Moving clients to a new domain
- Retiring clients
- Deleting clients
- Modifying the associations between clients and groups

Analysis tasks — Using Avamar Client Manager reports, you can quickly determine the status of large numbers of clients in the following areas:

- Backup and restore summaries by client
- Successful backups
- Clients with successful backups
- Clients with failed backups
- Restore activities
- Clients with restore activity
- Failed backups
- Idle clients

You can filter the information in the reports by searching for a computer using all or part of a computer name or username. This enables you to focus the reports on specific computers.

Upgrade tasks — Avamar Client Manager enables you to remotely change the Avamar software on large numbers of Avamar client computers:

- Upgrade
- Downgrade
- Apply a hotfix

Activation tasks — Avamar Client Manager enables you to perform the following activation-related tasks for large numbers of computers:

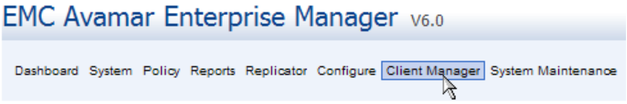
- Search for computers
- Activate selected computers
- Activate computers by organizational unit
- Create an Avamar domain
- Create an Avamar group
- Show all Avamar groups
- Show all Avamar clients
- Search for Avamar clients

Starting Avamar Client Manager

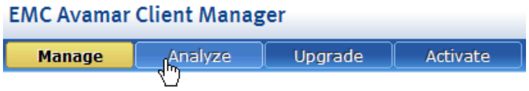
Avamar Client Manager is started from the Avamar Enterprise Manager menu bar.

To start Avamar Client Manager:

1. Log in to Avamar Enterprise Manager.
2. In the Avamar Enterprise Manager interface, click **Client Manager**.



The Avamar Client Manager opens, starting with the Manage page.



General information

The following topics provide general information about Avamar Client Manager:

- "Connection security" on page 451
- "Apache web server authentication" on page 452
- "Editing the session time-out period" on page 452
- "Increasing the JavaScript time-out period" on page 453
- "Showing and hiding tooltips" on page 454
- "Refreshing the window" on page 454
- "Process viewer" on page 454
- "Activation log and Management log" on page 455
- "Support for version 4 and 5 servers" on page 457

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, the session times out. However, Avamar Client Manager does not time out while a commit task is in progress.

When a session times out, close the web browser window or tab in which the session was running, and restart Avamar Client Manager.

To edit the session time-out value:

1. Log in as root on the Avamar server utility node.
2. Stop the Apache Tomcat server by typing:

   ```
   /usr/local/avamar/bin/emwebapp.sh --stop
   ```

3. Open the following file for editing:

   ```
   /usr/local/avamar-tomcat/webapps/aam/WEB-INF/web.xml
   ```

4. 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>
   ```

5. 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.

Showing and hiding tooltips

To show or hide global tooltips in Avamar Client Manager:

1. On the Avamar Client Manager banner bar, click ⚙.
2. Select **Options**.
3. Select or clear **Show Tooltips**.

Refreshing the window

Click the refresh icon, ↻, to update the information in a window or log view.

Process viewer

Process Viewer displays information about background processes, including move and activation tasks.

To open Process Viewer:

1. On the Avamar Client Manager banner, click ⚙.
2. Click **Process Viewer**.

   Process Viewer provides the information listed in the following table.

Table 82 Process Viewer columns

Column	Description
Description	Type of task that started the process
User	Login ID that started the process
Status	Current state of the process: • Success - The task completed without error. • Failure - The task could not be completed. • Partial Success - The task succeeded for at least one client and failed for at least one client. • Active - The task is in progress. • Queued - At least one of the activations associated with the client move task is in the retry queue.
Start time	Date and time that the process started
End time	Date and time that the process finished

3. (Optional) To filter the information to show only process entries for selected processes, in the **Process** section of the **Process Filter** pane, select the processes.

   The process list in this section is dynamically generated based on all processes currently tracked by Process Viewer.

4. (Optional) To filter the information to show only process entries for specified client status types, in the **Client Status** section of the **Process Filter** pane, select the status types.

   The client status list in this section is dynamically generated based on the status types for all processes currently tracked by Process Viewer.

5. (Optional) To filter the information to show only process entries for processes started by a specific username:

   a. In the **Username** section of the **Process Filter** pane, type a search string.

      The search string is used to match all or part of a username. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

      – No more than 24 characters
      – Cannot start with a period character
      – Cannot contain any of the following characters: `/:?"<>,~!@#$%^|&’(){}_`

   b. Click the button next to the text box.

6. (Optional) To clear all entries from Process Viewer, click **Clear All** and click **Yes**.

   All entries are cleared from Process Viewer, and the Avamar system database row for each entry is marked with a deletion flag (soft delete).

7. Click **Close**.

Activation log and Management log

The Activation log and Management log provide the status and result of client management and activation tasks. These logs are stored in the Avamar system database.

Viewing the Activation log or Management log

To view the Activation log or Management log:

1. Click **View Log** on either the **Manage** or **Activate** page.

2. (Optional) Filter the log entries:

   - To view only log entries for certain servers, select the checkbox next to the server names in the **Server** pane.

   - To view only log entries for clients with a certain status, select the checkbox next to the status in the **Client Status** pane.

     In the Activation log, one or more of the following types is listed:

     – Selected for Registration
     – Pending Client Response
     – Activation Failure
     – Activated Client

     In the Management log, one of more of the following types is listed:

     – Success
     – Pending
     – Failure

   - To view only log entries with a certain status code, select the status codes in the **Status Code pane**.

   - To search for log entries, select the log field by which to search in the **Search** pane, type a search string in the text box, and then click the button next to the text box.

3. Close the log window.

Exporting the Activation log or Management log

To export a log as a CSV file, click 🖨. The formatted file, named View_Log.xls, is sent to a web browser.

Deleting the Activation log or Management log

To delete the entries in the Activation log or Management log:

1. In either the Activation log or Management log, click 🗑.

   The Confirm window appears.

2. Click **Yes**.

   All entries are cleared from the log, and the Avamar system database row for each entry is marked with a deletion flag (soft delete).

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 83 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
move.queue.error.codes	Sets a comma-separated list of error codes that detemine 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

Table 83 Avamar Client Manager properties (page 2 of 2)

Property	Description	Default value
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. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Client Manager properties file, acm.properties, in a text editor such as vi or Emacs.
4. Edit the value of the property.
5. Save and close the file.
6. Restart the Avamar Enterprise Manager service:

   ```
   dpnctl stop ems
   dpnctl start ems
   ```

Support for version 4 and 5 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 server version 6.0 have limited support when working with clients activated to an Avamar server version 4.1.x or 5.x. The following features have limited support on Avamar server versions 4.1.x or 5.x:

- 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, as described in "Moving clients to a new server" on page 460, 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 84 Limitations for moving clients to a new server

Source server version	Move permitted?	Limitations
Version 4.1.x and 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.x	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, as described in "Moving clients to a new domain" on page 462, is not supported for clients activated to Avamar server version 4.1.x or 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 4.1.x or 5.x. The remote upgrade process, as described in "Upgrading Avamar client software" on page 484, requires methods that are only available on Avamar server version 6.0 and newer.

Username search

Username search, as described in "Managing clients" on page 459 and "Upgrading Avamar clients" on page 483, is not available for clients activated to Avamar server version 4.1.x or 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 4.1.x or 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 4.1.x or 5.x, the dataset details, retention policy details, and schedule details windows may display some empty fields.

Managing clients

Avamar Client Manager enables you to perform the following client management tasks for large numbers of clients:

- "Moving clients to a new server" on page 460
- "Moving clients to a new domain" on page 462
- "Retiring clients" on page 463
- "Deleting clients" on page 464
- "Adding and removing groups for a client" on page 465
- "Adding and removing clients in a group" on page 466

You can also view summary information and override group policy settings for individual clients. "Working with individual clients" on page 467 describes these topics.

Moving clients to a new server

NOTICE

Avamar Client Manager does not support moving clients to a new Avamar server if the client has any backups on a Data Domain server. An attempt to move such a client is prevented to preserve the client's access to its backups on the Data Domain server.

To move an activated client to a different Avamar server:

1. On the **Home** window of the **Manage** page, click **Move clients to a new server.**

   The Move clients to a new server window appears.

2. Filter the available Avamar clients:

   - In **Server,** select the servers with clients to include in the task.
   - In **OS,** select the type of operating system for clients to include in the task.
   - In **Client by Name/Username,** type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection in **Server** than only clients for the first server in the sorted list appear. If you do not make a selection or entry in **OS** or **Client by Name/Username,** then all values in the category are included.

3. In the **Move clients to a new server** pane, select the clients to move.

   Limit client moves to no more than five clients at one time. This reserves sufficient system resources for other processes.

4. Click **Server.**

   The Move client to Server window appears with the selected clients listed in the Source Client(s) pane.

5. In the server selection box on the **Target Server Information** pane title bar, select the target Avamar server.

6. In the **Target Server Information** pane, select a target domain, or click **Create Domain** to create a domain as described in "Creating a domain" on page 498.

7. Click **Next.**

   The groups available in the selected domain, and all domains above it, appear.

8. Select groups for the clients.

   To select all groups on the current page, select the box at the top of the selection column. To create a group, click **Create Group,** and complete that task as described in "Creating a group" on page 498.

9. In **Replicate Existing Backups**, select the client backups to replicate to the new server:
   - Select **All** to replicate all backups for the client.
   - Select **Last** to replicate only the last backup for the client.
   - Select **None** to not replicate any of the backups for the client.
10. Choose whether to delete or retain a client and its backups on the original server by selecting or clearing the **Delete From Source** checkbox.

    To retain the existing backups on a client's original server, clear **Delete From Source**. This causes the client on the original server to be moved to the MC_RETIRED domain on the original server and retains its backups. A new instance of the client is created on the target server and replication of existing backups to the target server is determined by the selection made in Replicate Existing Backups.
11. Click **Finish**.

    If you are replicating backups for the client to the new server, the Confirm Replication Authentication dialog box appears. Otherwise, the move is initiated as a background process.
12. On **Confirm Replication Authentication**, in **Source Server**, type the password for the source server's repluser or MCUser account.

    The specific account is determined by Avamar Client Manager and the **Username** field is populated with the correct username for the replication role. The **Username** value is determined based on the server version. Avamar server version 4.x uses the MCUser account for replication. Avamar server versions 5.x and newer use the repluser account for this role.
13. On **Confirm Replication Authentication**, in **Target Server**, type the password for the target server's repluser or MCUser account.

    The specific account is determined by Avamar Client Manager and the **Username** field is populated with the correct username for the replication role. The **Username** value is determined based on the server version. Avamar server version 4.x uses the MCUser account for replication. Avamar server versions 5.x and newer use the repluser account for this role.
14. Click **OK**.

    Move tasks are initiated as background processes. To check the status of the processes, use the "Analyzing client activity" on page 471. To check the status of the tasks, use the Management Log, as described in "Activation log and Management log" on page 455.

When activation of the client on the new server fails, the client is, by design, left registered with the new server. This ensures that its replicated backups are associated with it on the new server.

Move tasks that generate specific error codes are added to a queue to be retried. The error codes, number of retry attempts, and retry interval can be configured. The default values for these properties, and the steps required to change them, are described in "Configuration properties" on page 456.

Moving clients to a new domain

To move an activated client to a different Avamar domain on the same server:

1. On the **Home** window of the **Manage** page, click **Move clients to a new domain.**

   The Move clients to a new domain window appears.

2. Filter the available Avamar clients:

   - In **Server,** select the server with clients to include in the task.
   - In **OS**, select the type of operating system for clients to include in the task.
   - In **Client by Name/Username,** type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection in **Server** than only clients for the first server in the sorted list appear. If you do not make a selection or entry in **OS** or **Client by Name/Username**, then all values in the category are included.

3. In the **Move clients to a new domain** pane, select the clients to move.

4. Click **Domain.**

   The Move client to Domain window appears with the selected clients listed in the Source Client(s) pane.

5. In the **Target Server Information** pane, select a target domain, or click **Create Domain** to create a domain as described in "Creating a domain" on page 498.

6. Click **Next.**

   The groups available in the selected domain, and all domains above it, appear.

7. Select groups for the clients.

   To select all groups on the current page, select the box at the top of the selection column. To create a group, click **Create Group**, and complete that task as described in "Creating a group" on page 498.

8. Click **Finish.**

   Move tasks are initiated as background processes. To check the status of the processes, use the "Analyzing client activity" on page 471. To check the status of the tasks, use the Management Log, as described in "Activation log and Management log" on page 455.

Retiring clients

To transfer an activated Avamar client to retired status:

1. On the **Home** window of the **Manage** page, click **Retire clients**.

   The Retire clients window appears.

2. Filter the available Avamar clients as described in the following table.

Table 85 Filters for available Avamar clients

Filter	Clients displayed
Server	Clients associated with the selected server. When no selection is made, only clients for the first server in the sorted list appear.
OS	Clients running a selected OS. When no selection is made, the client display is not limited by this filter.
Client by Name/Username	Clients that have a hostname or username that matches the text string that is typed. When no text is entered, the client display is not limited by this filter.
Last Check-in	Clients that have a last check-in that is within the selected time range: • More than 7 days • More than 2 weeks • More than 1 month • More than 3 months When Unfiltered is selected, the client display is not limited by this filter. The "last check-in" for an Avamar client is the last time it contacted the server to get a new work order.

3. In the **Retire** clients pane, select the clients to retire.

4. Click **Retire**.

   The Retire Client window appears.

5. Select the retention policy for the backups for the retired clients, as described in the following table.

Table 86 Steps for selecting a backup retention policy

Retention policy	Steps to select the policy
Current retention period set for the backups	In **Select Retention Policy**, select **Retire client and retain backups with existing expiration date.**
Until the backups are manually deleted	In **Select Retention Policy**, select **Retire client and retain all backups indefinitely.**
Until a certain date	In **Select Retention Policy**, select **Retire client and reset backup expiration date**, and then specify the date in **New Expiration Date.**

6. Click **OK**.

   A confirmation message appears.

7. Click **Yes**.

   Retire client tasks are initiated. To check the status of the tasks, use the Management Log, as described in "Activation log and Management log" on page 455.

Deleting clients

To remove an activated Avamar client and all of the backups for the client from the associated Avamar server:

1. On the **Home** window of the **Manage** page, click **Delete clients**.

   The Delete clients window appears.

2. Filter the available Avamar clients:

   - In **Server**, select the servers with clients to include in the task.
   - In **OS**, select the type of operating system for clients to include in the task.
   - In **Client by Name/Username**, type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection in **Server** than only clients for the first server in the sorted list appear. If you do not make a selection or entry in **OS** or **Client by Name/Username**, then all values in the category are included.

3. In the **Delete** clients pane, click ⊗ next to the client name.

   The first confirmation dialog appears.

   NOTICE

   Client deletion removes the client, its backups, and its backup history from the server. To help avoid inadvertent deletions and loss of valuable data a two-step confirmation process is used

4. Click **Yes**.

   The second confirmation dialog appears.

5. Type the password used to log in to Avamar Enterprise Manager for the current session.

   The user account must have the Avamar role of Root Administrator or Administrator for the client's domain. "Understanding users, authentication, and roles" on page 67 provides details.

6. Click **OK**.

   Tasks to delete the client and all of its backups are initiated. To check the status of the tasks, use the Management Log, as described in "Activation log and Management log" on page 455.

Adding and removing groups for a client

To add or remove groups associated with a client:

1. On the **Home** window of the **Manage** page, click **Modify client and group associations.**

   The Modify client and group associations window appears.

2. Click the **Client** tab.

3. Filter the available Avamar clients:

   - In **Server,** select the servers with clients to include in the task.
   - In **OS,** select the type of operating system for clients to include in the task.
   - In **Client by Name/Username,** type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection in **Server** than only clients for the first server in the sorted list appear. If you do not make a selection or entry in **OS** or **Client by Name/Username,** then all values in the category are included.

4. In the **Client** pane, click ⚙ next to the client being changed.

   The Edit Client window appears.

   To view information about the client, click the client name in the Client column.

5. Remove a group for the client by selecting the group and clicking **Remove.**

   This removes the association between the client and the selected group but does not remove or delete the group.

   At least one group must be associated with a client.

6. Add groups for the client:

   a. Click **Add Groups.**

      The Add Groups for Client window appears.

   b. Select additional groups to associate with the client.

      To select all groups on the current page, select the box at the top of the selection column. To create a group, click **Create Group,** and complete that task as described in "Creating a group" on page 498.

   c. Click **Add.**

      The client association tasks are initiated.

   d. Click **Close** on the **Add Groups for Client** window.

7. Click **Close** on the **Edit Client** window.

Adding and removing clients in a group

To add and remove the clients associated with a group:

1. On the **Home** window of the **Manage** page, click **Modify client and group associations.**

   The Modify client and group associations window appears.

2. Click the **Group** tab.

3. Filter the available Avamar clients:

   - In **Server**, select the servers with clients to include in the task.
   - In **OS**, select the type of operating system for clients to include in the task.
   - In **Client by Name/Username**, type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection in **Server** than only clients for the first server in the sorted list appear. If you do not make a selection or entry in **OS** or **Client by Name/Username**, then all values in the category are included.

4. In the **Group** pane, click ⚙ next to the group being changed.

   The Edit Group window appears.

   You can view group information by clicking a link in any of the following columns:

   - Activated Clients
   - Dataset
   - Retention
   - Schedule

5. Remove a client from the group by selecting the client and clicking **Remove**.

6. Add clients to the group:

   a. Click **Add Clients**.

      The Add Clients for Group window appears.

   b. Select clients to add to the group.

      To select all clients on the current page, select the box at the top of the selection column.

   c. Click **Add**.

      The group association tasks are initiated.

7. Click **Close** on the **Edit Group** window.

Working with individual clients

Click the hyperlinked name of any Avamar client displayed in Avamar Client Manager to open the Client Details window for that client. This window provides access to information about the client and allows you to configure group policy overrides for the client.

Client information

The Summary, Backups, Plugins, and Advanced tabs on the Client Details window provide Avamar client information.

Summary tab

The following table describes the client information available on the Summary tab of the Client Details window.

Table 87 Client Details - Summary tab

Label	Description
Client Name	Name of the client. This is an editable field and can be used to change the name of the client in the Avamar server's database. It does not change the hostname of the client. Use this function to update the client name in Avamar when a client's hostname is changed. To rename the client in Avamar: 1. Change the name in Client Name to match the new hostname of the client computer. 2. Click **OK**. **Notice:** An incorrect value in Client Name breaks the association between the client and its backups and its group. To reestablish these connections, change the value in Client Name to match the hostname of the client.
Domain	Domain on the Avamar server to which the client is assigned.
OS	Operating system installed on the client.
Version	Avamar client version installed on the client.
Last Backup	Date and time of the last successful backup of the client.
‹OS› users on ‹HOSTNAME›	List of all non-system users associated with backed up data from the client, where ‹OS› is the OS assigned to the client and ‹HOSTNAME› is the hostname of the client.

Backups tab

The following table describes the client information available on the Backups tab of the Client Details window.

Table 88 Client Details - Backups tab

Label	Description
From	Earliest date used to define the list of displayed backups.
To	Latest date used to define the list of displayed backups.
On-Demand Backups	Select to display on-demand backups.
Scheduled Backups	Select to display scheduled backups.
Label	Reference name assigned to backup.
Plugin	Name of Avamar plugin used during backup.
Size	Size of all data scanned during the backup.
Started	Date and time backup started.
Expiration	Date retention of the backup expires.

Plugins tab

The following table describes the client information available on the Plugins tab of the Client Details window.

Table 89 Client Details - Plugins tab

Label	Description
Name	Name of plugin assigned.
Version	Version of plugin assigned.
Build	Build of plugin assigned.
Last Backup	Date and time of last backup that used the plugin.

Advanced tab

The following table describes the client information available on the Advanced tab of the Client Details window.

Table 90 Client Details - Advanced tab (page 1 of 2)

Label	Description
Override group dataset	Permits you to assign a dataset that is different from the group dataset. After selecting this option, assign a dataset by selecting it from the drop down list. For a description of the Avamar Administrator setting, see "Assigning a different dataset to a client" on page 168.
Override group retention	Permits you to assign a retention setting that is different from the group setting. After selecting this option, assign a retention setting by selecting it from the drop down list. For a description of the Avamar Administrator setting, see "Assigning a different retention policy to a client" on page 169.
Disable all backups	Disables all backups for the client. For a description of the Avamar Administrator setting, see "Enabling and disabling a client" on page 61.
Activated	Clear this setting to change the state of a client from activated to nonactivated. Select this to change a client that has been placed in a nonactivated state back to an activated state. **Notice:** This setting does not initiate activation of a client. It only changes the state of a client that has been previously activated.
Allow client initiated backups	Select to allow users to initiate on-demand backups. For a description of the Avamar Administrator setting, see "Allowing users to initiate backups" on page 175.
Allow file selection on client initiated backups	Select to allow users to create sets of folders and files to back up through an on-demand backup. **Notice:** Folders and files selected through this feature are not subject to group dataset source limits, exclusions, or inclusions. For a description of the Avamar Administrator setting, see "Allowing users to select data source for on-demand backups" on page 179.

Table 90 Client Details - Advanced tab (page 2 of 2)

Label	Description
Allow client to add to dataset	Select this to allow users to add folders to the source data for the group datasets assigned to their client. 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. • User must have access to the Avamar client web UI from the client to make or remove additions. For a description of the Avamar Administrator setting, see "Allowing users to add to source data" on page 174.
Allow client to override all daily group schedule	Select this to allow users to select a start time for scheduled backups that is different from the start time assigned through their group. This setting is equivalent to the Allow override of group's daily schedule setting in Avamar Administrator and is subject to the same set of additional requirements: • Time entries must be added to the override schedule as described in the administration guide. • 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. For a description of the Avamar Administrator setting, see "Allowing users to select an alternative backup start time" on page 173.
Allow client to override retention policy on client initiated backups	Select to use retention setting from Override group retention with on-demand backups of the client. To use this setting: 1. Enable Override group retention and select a retention policy. 2. Enable Allow client initiated backups. 3. Enable this setting.

Group policy overrides

Use the Advanced tab on the Client Details window to set group policy overrides for a client. Many of the settings are equivalent to the Avamar Administrator settings described in "Overriding group policy settings" on page 168. Settings made in Avamar Administrator appear in this window and settings made in this window appear in the equivalent Avamar Administrator fields for the client.

To use Avamar Client Manager to set group policy overrides for a client:

1. In any Avamar Client Manager view that shows Avamar clients, click the client name.

   The Client Details window for that client opens.

2. Click the **Advanced** tab.
3. Select a group policy override setting.
4. Click **OK**.

Analyzing client activity

Avamar Client Manager provides several reports that enable you to view summary and detailed information about the performance of the Avamar servers, and about backup and restore activity on Avamar clients.

Table 91 Avamar Client Manager reports

Report	Description
"Server Summary report" on page 471	Provides general client information for all available Avamar servers and serves as a springboard to more detailed information related to the data categories it contains.
"Backup/Restore Summary by Client report" on page 475	Provides summary information about the backup and restore activity of active clients on a selected server.
"Successful Backups report" on page 476	Provides information about successful backup workorders of selected clients for a specific Avamar server and time period.
"Successful Clients report" on page 473	Lists clients of a specific Avamar server that meet the selected definition of a successful client.
"Restore Activities report" on page 481	Provides information about restore workorders of selected clients for a specific Avamar server and time period.
"Clients with Restore Activity report" on page 480	Lists clients on a specific Avamar server that have any restore activity during a specified time period.
"Failed Clients report" on page 477	Lists clients on a specific Avamar server that do not meet the selected definition of a successful client during the specified time period.
"Failed Backups report" on page 478	Provides information about failed backup workorders of selected clients for a specific Avamar server and time period.
"Idle Clients report" on page 479	Lists the clients on an Avamar server that have no backup activity during the specified time period.

Server Summary report

The Server Summary report provides general client information for all available Avamar servers. It also serves as a springboard to more detailed information related to the data categories it contains. Where a report containing more detailed information about a particular data category is available, the number in the column for that category acts as a link to the report.

For example, to view the Backup/Restore Summary by Client report for a particular server, click the number in the Active Clients column for that server.

Data that is linked to another report appears as a blue hyperlink. When the number is black, no additional report is available.

Viewing the Server Summary report

To view the Server Summary report:

1. On the Avamar Client Manager button bar, click **Analyze**.

   The Analyze page appears and displays the Filters and the Server Summary report.

2. (Optional) Filter the data in the report:

   a. Choose whether to filter the data by a certain time period or range:

      - To view data for a certain time period, select **Period** and then select a value from the **Past** list.

        The minimum value is 1 day and the maximum is 3 months. The current date is the end of the time period that is defined by the value selected. For example, selecting 1 month defines a time period starting 1 month before the current date and ending on the current date.

      - To view data for a certain time range, select **Range** and then select a start and end date for the range.

        The maximum range is 3 months.

   b. Filter the report by the local hostname of a client by typing a search string in **Client** and clicking the button next to the text entry field.

      The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

      - No more than 24 characters
      - Cannot start with a period character
      - Cannot contain any of the following characters:
        `/:?"<>\,~!@#$%^|&’(){}_`

   c. Filter the report by the username on a client by typing a search string in **Username** and clicking the button next to the text entry field.

      The search string must meet the same requirements as the client search string, except that the \ character can be used.

   d. Filter the report by Avamar server by selecting the server from the **Server** list or select **All Servers** from the list to view data for all servers.

   These filters also apply to detailed reports that you launch from the Server Summary report.

3. Select the definition to use for a successful client by clicking ⚙ **› Successful Clients,** and then selecting an option to define a successful client:

   - At least one successful backup
   - All backups successful
   - Last backup successful

4. (Optional) To set the maximum number of report rows, select ⚙ **› Entries Per Page,** and then select a number.

5. View detailed reports by clicking data that appears in blue.

Server Summary report details

The Server Summary report contains the information listed in the following table.

Table 92 Server Summary report columns and linked reports

Column	Description	Linked Report
Server	Hostname or IP address of the Avamar server. The server must be registered in Enterprise Manager.	None
Total Clients	Total number of clients registered with the server. Does not include retired clients.	None
Active Clients	Total number of clients with backup and/or restore activity during the specified time period.	Backup/Restore Summary by Client
Idle Clients	Total number of clients with no backup activity during the specified time period.	Idle Clients
Successful Clients	Total number of clients that meet the selected definition of a successful client during the specified time period, and the average amount of time for the backups of those clients.	Successful Clients
Failed Clients	Total number of clients that do not meet the selected definition of a successful client during the specified time period.	Failed Clients
Clients with Restore	Total number of clients with restore activity during the specified time period, including successful and failed workorders.	Clients with Restore Activity

Successful Clients report

The Successful Clients report lists clients of a specific Avamar server that meet the selected definition of a successful client during a specified time period. It also provides information about the backup activity on each client.

Viewing the Successful Clients report

To view the Successful Clients report:

1. Open the Server Summary report and optionally filter the data in the report, as discussed in "Viewing the Server Summary report" on page 472.

   The report filters you set in the Server Summary report are used in the initial view of the Successful Clients report. These filters can be changed on the Successful Clients report itself.

2. (Optional) Click ⚙ on the Server Summary report menu bar, click **Successful Clients,** and select one of the definitions of a successful client:

   - At least one successful backup (default)
   - All backups successful
   - Last backup successful

3. Identify the report row for the server with the clients for which to view the report.

4. In the row, click the number in the **Successful Clients** column.

   When the number in the Successful Clients column is 0, the server does not have a report for the specified view.

5. (Optional) Filter the report data further by the local hostname of a client or the username on a client by typing a search string in the **Client** or **Username** boxes and clicking the button next to the box.

   The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

   - No more than 24 characters
   - Cannot start with a period character
   - Cannot contain any of the following characters: `/:?"<>,~!@#$%^|&’(){}_`

Successful Clients report detail

The Successful Clients report contains the information listed in the following table.

Table 93 Successful Clients report columns

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Successful Backups	• Total number of backups of the client during the specified time period. • Includes any of the following: • Successful backups • Backups with exceptions • Backups with errors Does not include failed backups.
Last Successful Backup	Date and time of the end of the last successful backup of the client. This value is not limited by the selected time period.
Average Backup Duration	Average amount of time required to complete a backup of the client.
Total Size	Sum, in bytes, of all data processed in all of the successful backups of the client during the specified time period.

Backup/Restore Summary by Client report

The Backup/Restore Summary by Client report provides a summary view of the backup and restore activity for each client on a selected server. The report can also be used to view reports for selected clients.

Viewing the Backup/Restore Summary by Client report

To view the Backup/Restore Summary by Client report:

1. Open the Server Summary report and optionally filter the data in the report, as discussed in "Viewing the Server Summary report" on page 472.

   The report filters you set in the Server Summary report apply to the Backup/Restore Summary by Client report.

2. Identify the report row for the server with the clients for which to view the report.
3. In the row, click the number in the **Active Clients** column.

   When the number in the Active Clients column is 0, the server does not have a report for the specified view.

4. (Optional) Filter the report data further by the local hostname of a client or the username on a client by typing a search string in the **Client** or **Username** boxes and clicking the button next to the box.

   The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

   - No more than 24 characters
   - Cannot start with a period character
   - Cannot contain any of the following characters: `/:?"<>,~!@#$%^|&’(){}_`

Backup/Restore Summary by Client report details

The Backup/Restore Summary by Client report contains the information listed in the following table.

Table 94 Backup/Restore Summary by Client report columns (page 1 of 2)

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Successful Backups	Total number of backups of the client during the specified time period. Includes any of the following: • Successful backups • Backups with exceptions • Backups with errors Does not include failed backups.
Failed Backups	Total number of failed backup attempts for the client during the specified time period.

Table 94 Backup/Restore Summary by Client report columns (page 2 of 2)

Column	Description
Restores	Total number of restore workorders during the specified time period. Includes successful and failed workorders.
Last Successful Backup	Date and time of the end of the last successful backup of the client. **Note:** This date is not limited by the specified time period.
Average Backup Duration	Average amount of time to complete a backup of the client.

Successful Backups report

The Successful Backups report lists information about successful backup workorders for a specific Avamar server and time period.

Viewing the Successful Backups report

To view the Successful Backups report:

1. Open either the Successful Clients report or the Backup/Restore Summary by Client report for the time period being analyzed. The following topics provide details:
   - "Viewing the Successful Clients report" on page 473
   - "Viewing the Backup/Restore Summary by Client report" on page 475
2. Specify clients for the Successful Backups report by selecting the checkbox next to the client names.
3. Click **Successful Backup**.

Successful Backups Report details

The Successful Backups report contains the information listed in the following table.

Table 95 Successful Backups report columns

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Plug-in	Plug-in type used for the workorder.
Dataset	Dataset used for the workorder.
Type	Type of backup, either On-Demand or Scheduled.
Start	Date and time that the workorder started.
End	Date and time that the workorder ended.
Elapsed Time	Total time required to complete the workorder.
Data Size	Size of all data transferred during the backup.
Changed	Size of the data that changed since the last successful backup.

Failed Clients report

The Failed Clients report lists clients on a specific Avamar server that do not meet the selected definition of a successful client during a specified time period.

Viewing the Failed Clients report

To view the Failed Clients report:

1. Open the Server Summary report and optionally filter the data in the report, as discussed in "Viewing the Server Summary report" on page 472.

   The report filters you set in the Server Summary report are used in the initial view of the Failed Clients report. These filters can be changed on the Failed Clients report itself.

2. (Optional) Click ⚙ on the Server Summary report menu bar, click **Successful Clients,** and select one of the definitions of a successful client:

   - At least one successful backup (default)
   - All backups successful
   - Last backup successful

   Failed clients are those clients that do not qualify under the selected definition of a successful client.

3. Identify the report row for the server with the clients for which to view the report.

4. In the row, click the number in the **Failed Clients** column.

   When the number in the Failed Clients column is 0, the server does not have a report for the specified view.

5. (Optional) Filter the report data further by the local hostname of a client or the username on a client by typing a search string in the **Client** or **Username** boxes and clicking the button next to the box.

   The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

   - No more than 24 characters
   - Cannot start with a period character
   - Cannot contain any of the following characters: `/:?"<>,~!@#$%^|&'(){}_`

Failed Clients report details

The Failed Clients report contains the information listed in the following table.

Table 96 Failed Clients report columns

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Failed Backups	Total number of failed backups for the client during the specified time period.
Last Successful Backup	Date and time of the end of the last successful backup of the client. This value is not limited by the selected time period.

Failed Backups report

The Failed Backups report lists information about failed backup workorders for a specific Avamar server and time period.

Viewing the Failed Backups report

To view the Failed Backups report for selected clients:

1. Open either the Backup/Restore Summary by Client report or the Failed Clients report for the time period being analyzed. The following topics provide details:
   - "Viewing the Backup/Restore Summary by Client report" on page 475
   - "Viewing the Failed Clients report" on page 477
2. Specify clients for the Failed Backups report by selecting the checkbox next to the client names.
3. Click **Failed Backup**.

Failed Backups report details

The Failed Backups report contains the information listed in the following table.

Table 97 Failed Backups report columns (page 1 of 2)

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Plug-in	Plug-in type used for the workorder.
Dataset	Dataset used for the workorder.
Type	Type of backup, either On-Demand or Scheduled.
Start	Date and time that the workorder started.

Table 97 Failed Backups report columns (page 2 of 2)

Column	Description
End	Date and time that the workorder ended.
Status Code	Backup workorder status code. Click the status code to view additional information.
Error Code	Avamar server error code for the failed workorder. Click the error code to view additional information.

Idle Clients report

The Idle Clients report lists the clients on an Avamar server that have no backup activity during the specified time period.

Viewing the Idle Clients report

To view the Idle Clients report:

1. Open the Server Summary report and optionally filter the data in the report, as discussed in "Viewing the Server Summary report" on page 472.

   The report filters you set in the Server Summary report apply to the Idle Clients report.

2. Identify the report row for the server with the clients for which to view the report.

3. In the row, click the number in the **Idle** column.

   When the number in the Idle column is 0, the server does not have a report for the specified view.

4. (Optional) Filter the report data further by the local hostname of a client or the username on a client by typing a search string in the **Client** or **Username** boxes and clicking the button next to the box.

   The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

   - No more than 24 characters
   - Cannot start with a period character
   - Cannot contain any of the following characters: / : ? " < > , ~ ! @ # $ % ^ | & ’ ( ) { } _

Idle Clients report details

The Idle Clients report contains the information listed in the following table.

Table 98 Idle Clients report columns

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.

Clients with Restore Activity report

The Clients with Restore Activity report lists clients on a specific Avamar server that have any restore activity during a specified time period. It also provides information about the restore activity on each client.

Clients are included on the Clients with Restore Activity report if they have at least one of the following:

- Successful restores
- Restores with exceptions
- Restores with errors
- Failed Restores

Viewing the Clients with Restore Activity report

To view the Clients with Restore Activity report:

1. Open the Server Summary report and optionally filter the data in the report, as discussed in "Viewing the Server Summary report" on page 472.

   The report filters you set in the Server Summary report apply to the Clients with Restore Activity report.

2. Identify the report row for the server with the clients for which to view the report.

3. In the row, click the number in the **Clients with Restore** column.

   When the number in the Clients with Restore column is 0, the server does not have a report for the specified view.

4. (Optional) Filter the report data further by the local hostname of a client or the username on a client by typing a search string in the **Client** or **Username** boxes and clicking the button next to the box.

   The search string is used to match all or part of the local hostname of clients. Use an asterisk (*) to represent zero or more characters. The search string must comply with the following rules:

   - No more than 24 characters
   - Cannot start with a period character
   - Cannot contain any of the following characters: `/:?"<>,~!@#$%^|&’(){}_`

Clients with Restore Activity report details

The Clients with Restore Activity report contains the information listed in the following table.

Table 99 Clients with Restore Activity report columns

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Successful	Total number of the restore workorders for the client that did not fail during the specified time period. Includes any of the following: • Successful restores • Restores with exceptions • Restores with errors
Failed	Total number of restore workorders for the client that failed during the specified time period.
Total Size	Sum total of all data included in restore workorders for the client during the specified time period. This value includes the data in both successful and failed restore workorders.

Restore Activities report

The Restore Activities report lists information about restore workorders for a specific Avamar server and time period.

Viewing the Restore Activities report

To view the Restore Activities report for selected clients on an Avamar server:

1. Open either the Backup/Restore Summary by Client report or the Clients with Restore Activity report. The following topics provide details:
   - "Viewing the Backup/Restore Summary by Client report" on page 475
   - "Viewing the Clients with Restore Activity report" on page 480
2. Specify clients for the Restore Activities report by selecting the checkbox next to the client names.
3. Click **Restore Activity**.

Restore Activities report details

The Restore Activities report contains the information listed in the following table.

Table 100 Restore Activities report columns (page 1 of 2)

Column	Description
Client	Name of the client.
Domain	Domain on the Avamar server to which the client is assigned.
Plug-in	Plug-in type used for the workorder.
Start	Date and time that the workorder started.

Table 100 Restore Activities report columns (page 2 of 2)

Column	Description
End	Date and time that the workorder ended.
Elapsed Time	Total time required to complete the workorder.
Status Code	Restore workorder status code. For unsuccessful workorders, the status code is a link. Click the link to view additional information.
Error Code	Avamar server error code for the restore workorder. For unsuccessful workorders, the error code is a link. Click the link to view additional information.
Files	Total number of files in the restore.
Data Size	Total size of the data restored in the workorder.

Saving reports

To save a report, you can export it as a CSV-formatted file.

To export a report, click 💾.

The report is sent to the web browser as a CSV-formatted file.

Save options for the Server Summary report

You can print the Server Summary report directly from a web browser, or export the report as either a PDF or a CSV-formatted file. When you export the report as a PDF, the report is limited to a maximum of 50,000 records.

To print the Server Summary report, click 🖨.

The report is sent to the web browser as a PDF that you can print or save.

To export the Server Summary report:

1. On the Server Summary report tool bar, click 💾.

   The Export Options dialog appears.

2. In **Select Export Type**, choose **PDF File** or **CSV File**.
3. (PDF only) In **PDF Orientation**, choose **Landscape** or **Portrait**.
4. Click **OK**.

   The exported report is sent to your web browser.

Upgrading Avamar clients

Avamar Client Manager enables you to change the version of Avamar client that is installed on client computers to either a newer version or a hotfix. You also can downgrade the installed software, download a client package to all associated Avamar servers, and remove client packages from Avamar servers.

The following topics provide details:

- "Requirements" on page 483
- "Obtaining client packages" on page 484
- "Upgrading Avamar client software" on page 484
- "Downloading a client package to all servers" on page 486
- "Removing a client package" on page 488
- "Client Upgrade Status report" on page 488

Requirements

The Avamar Client Manager upgrade feature requires one of the following clients:

- Avamar client version 6.0 and newer for Windows computers

  NOTICE

  Use of this 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.

- Avamar client version 6.0 and newer for Linux computers

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), if the managed systems meet the following requirements:

- 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 332 describes how to add systems to Enterprise Manager.

- 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.

Compatibility with older versions of Avamar server

The upgrade feature is not compatible with older version of Avamar server. Avamar Client Manager cannot be used to upgrade clients activated to Avamar server version 4.1.x or 5.x. The upgrade process requires methods that are only available on Avamar server version 6.0 and newer.

Obtaining client packages

Client packages are obtained using the Avamar Downloader Service. This service pulls the packages from EMC and pushes them onto the Avamar data server subsystem (GSAN).

"Server Updates and Hotfixes" on page 403 describes the installation, configuration, and use of Avamar Downloader Service.

Note: 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 Avamar Support landing page: https://support.emc.com/products/Avamar.

Once the packages are updated in GSAN they are visible in Avamar Client Manager's Select Package window, and upgrades can be performed as described in "Upgrading Avamar client software" on page 484.

If packages do not appear in the Select Package window, follow the procedure in "Checking the EMC repository" on page 412.

NOTICE

Do not rename client installation packages. The Avamar push upgrade mechanisms are incompatible with renamed packages.

Upgrading Avamar client software

To upgrade Avamar clients:

1. On the Avamar Client Manager button bar, click **Upgrade**.

   The Upgrade page appears with the Select Package window open. To open the Select Package window manually, on the Upgrade page, click **Select Package**.

2. In the **Select Package** window, select an Avamar client version or hotfix to install:

   a. (Optional) Filter the list of packages by selecting one of the following options in **Show**:

      – **All** — Both upgrade and hotfix packages
      – **Upgrade** — Only upgrade packages
      – **Hotfix** — Only hotfix packages

   b. Select a package by clicking **Select** next to the package listing.

   The Select Package window closes, and the Select Servers window appears with the selected package as its focus.

3. Begin defining the pool of Avamar client computers that require the upgrade by selecting their associated Avamar servers.

   Only servers with the same version of Avamar server software as the Avamar Client Manager host are shown.

   Selected servers must display `ready` in the status column of the Select Servers window. To change a server's status to `ready`, download the package to the server cache using the methods described in "Downloading a client package to all servers" on page 486 and "Downloading a client package to selected servers" on page 487.

4. Click **OK**.

   The Client Filters window appears.

5. Filter the available Avamar clients for an upgrade or hotfix:

   - In **Server**, select the servers with clients to include in the upgrade or hotfix.
   - In **OS**, select the type of operating system for clients to include in the upgrade or hotfix.
   - In **Version**, select the current Avamar client versions on clients to include in the upgrade or hotfix.
   - In **Plug-in**, select the Avamar plug-in types used by clients to include in the upgrade or hotfix.
   - In **Client by Name/Username**, type a text string to match with the hostname of Avamar client computers and usernames listed for Avamar client computers, and then click the button next to the text field to apply the text string filter.

     Matches of both types are possible from a single text string. You can use an asterisk (*) wildcard character to match one or more characters.

   If you do not make a selection for a filter, then all values in the category are included. For example, if you make no selections in Server, then clients from all servers are included.

   NOTICE

   Only computers with an upgrade-compliant version of Avamar client version 6.0 or later appear in the Clients pane.

6. Select the computers to upgrade.

   - To select all computers on the current page of the Clients pane, select the box at the top of the selection column.
   - To select all computers on all pages, click **Select All**.

   Client selections are retained during page navigation.

7. Click **OK**.

   The Client Upgrade window appears with all selected clients listed.

8. (Optional) Click ⊗ in the **Remove** column to remove a client.

9. Click **Start Upgrade**.

   The upgrade or hotfix processes run in the background.

10. (Optional) Check the status of an upgrade or hotfix by clicking **View Status** on the Client Upgrade window.

    The Client Upgrade Status report opens and displays the status of each upgrade and hotfix task.

    You can also cancel an upgrade or hotfix task by clicking **Cancel** in the Action column of the Client Upgrade Status report. When an upgrade or hotfix task is canceled the client reverts back to the version in use at the time the task was scheduled.

Requirements for successful package downloads

To ensure successful package downloads, complete each of the following:

- Confirm that the Avamar Downloader Service (ADS) can communicate with the FTP server.
- Confirm that ADS can communicate with the Avamar server that is hosting the Enterprise Manager service.
- Confirm that the computer running ADS has access to sufficient mounted disk space to accomodate the package downloads.

Downloading a client package to all servers

To transfer a client package from the Avamar package repository to the local cache on all Avamar servers:

1. On the Avamar Client Manager button bar, click **Upgrade**.

   The Upgrade page appears with the Select Package window open. To open the Select Package window manually, on the Upgrade page, click **Select Package**.

2. In the **Select Package** window, select an Avamar client version or hotfix to install:

   a. (Optional) Filter the list of packages by selecting one of the following options in **Show**:

      – **All** — Both upgrade and hotfix packages
      – **Upgrade** — Only upgrade packages
      – **Hotfix** — Only hotfix packages

   b. Select a package by clicking **Select** next to the package listing.

   The Select Package window closes, and the Select Servers window appears with the selected package as its focus.

3. Click **Download To All**.

   The client package is downloaded to the local cache on all Avamar servers. A progress bar appears for each download.

   To cancel an active download for a particular server, on that server's row, click **Cancel**.

4. After all downloads have finished, click **Refresh** to display the additional Avamar servers with the package.

When a package download fails, the message "Download Failed" appears in the Status column and an informational message is sent to the log file. In a short time, "Available" appears in the Status column. At that point, the download can be retried.

Downloading a client package to selected servers

To transfer a client package from the Avamar package repository to the local cache on selected Avamar servers:

1. On the Avamar Client Manager button bar, click **Upgrade**.

   The Upgrade page appears with the Select Package window open. To open the Select Package window manually, on the Upgrade page, click **Select Package**.

2. In the **Select Package** window, select an Avamar client version or hotfix to install:

   a. (Optional) Filter the list of packages by selecting one of the following options in **Show**:

      - **All** — Both upgrade and hotfix packages
      - **Upgrade** — Only upgrade packages
      - **Hotfix** — Only hotfix packages

   b. Select a package by clicking **Select** next to the package listing.

   The Select Package window closes, and the Select Servers window appears with the selected package as its focus.

3. On each server row, click **Download**.

   The client package is downloaded to the local cache on the selected Avamar servers. A progress bar appears for each download.

   To cancel an active download for a particular server, click **Cancel** on that server row.

   Servers that already have the package in their local cache have `ready` in the Status column. The Download button does not appear on the row of those servers.

4. After all downloads have finished, click **Refresh** to display the additional Avamar servers with the package.

When a package download fails, the message "Download Failed" appears in the Status column and an informational message is sent to the log file. In a short time, "Available" appears in the Status column. At that point, the download can be retried.

Removing a client package

To remove a client package from the local cache on Avamar servers:

1. On the Avamar Client Manager button bar, click **Upgrade**.

   The Upgrade page appears with the Select Package window open. To open the Select Package window manually, on the Upgrade page, click Select Package.

2. In the **Select Package** window, select an Avamar client version or hotfix to remove:

   a. (Optional) Filter the list of packages by selecting one of the following options in **Show**:

      – **All** — Both upgrade and hotfix packages
      – **Upgrade** — Only upgrade packages
      – **Hotfix** — Only hotfix packages

   b. Select a package by clicking **Select** next to the package listing.

   The Select Package window closes, and the Select Servers window appears with the selected package as its focus.

3. Click **Delete** next to a server to remove the package from that server.

   To delete the package from all Avamar servers, click **Delete From All**.

4. Click **Yes** on the confirmation message.

Client Upgrade Status report

The Client Upgrade Status Report provides information about each upgrade and hotfix launched from the Avamar Client Manager Upgrade process.

Viewing the Client Upgrade Status report

To view the Client Upgrade Status report:

1. On the Avamar Client Manager button bar, click **Upgrade**.

2. Complete an upgrade or hotfix task, as described in "Upgrading Avamar client software" on page 484.

   Alternatively, to use the report without first completing an upgrade or hotfix, close any windows above the Client Upgrade window.

3. On the Client Upgrade window, click **View Status**.

   The Client Upgrade Status Report appears with a set of filters on the left and the information pane on the right.

4. (Optional) Filter the report based on the servers and status:

   - In the **Server** section of the filters, select the Avamar servers associated with the clients to include in the report.

   - In the **Status** section of the filters, select each status type to include in the report.

5. (Optional) Perform one or more of the following tasks:

   - To export the Client Upgrade Status Report as a CSV file, click 💾.

     The formatted file, clientUpgradeReport.csv, is sent to the browser.

   - To view a task log for a completed task, click **View Log** in the **Action** column for the task. Then click **OK** to close the log.

   - To cancel an upgrade or hotfix after it starts, click **Cancel** in the **Action** column for the task.

Client Upgrade Status report details

The Client Upgrade Status report contains the information listed in the following table.

Table 101 Client Upgrade Status report columns

Column	Description
Name	Hostname of the Avamar client.
Server	Hostname of the Avamar server.
Version	Version of the Avamar client or hotfix that existed before the upgrade.
Start Time	Start time of the upgrade or hotfix.
End Time	End time of the upgrade or hotfix.
Status	Current status of the upgrade or hotfix.
Action	Option to cancel an active process and view the log of a finished process.

The status types in the following table may appear in the Status column of the Client Upgrade Status report.

Table 102 Client Upgrade Status report status types

Status type	Description
Active	The task is in progress.
Waiting-client	The client is busy. The task starts when the client is available.
Waiting-queued	The Avamar server cannot contact the client. The task starts when the client can be contacted.
Timed out	The client has taken too long to respond. The task must be restarted.
Dropped session	The task started on the client, but then communication was lost. The task must be restarted.
Canceled	The task was canceled. You can cancel a task by clicking Cancel in the Action column of the Client Upgrade Status Report or through Avamar Administrator.
Complete	The task finished successfully.
Completed w/ Exception(s)	The task completed but there was at least one exception.
Failed	The task finished unsuccessfully.

Activating clients

Avamar Client Manager enables you to activate a large number of clients at the same time.

To activate clients with Avamar Client Manager:

1. Load the list of clients for activation in Avamar Client Manager, as discussed in "Loading the list of clients for activation" on page 490.

   This step provides Avamar Client Manager with information about the computers in the organization and the relationships between those computers. The information is used during the registration and activation of the computers as Avamar clients.

2. On the **Server Information** title bar of the **Activate** page, use the server list to select the Avamar server to which to add the clients.

3. Select the clients to activate. You can either browse for the clients or, if there is a large list of clients, search for specific client computers by all or part of a local hostname, as discussed in "Searching for computers to activate" on page 493.

4. Initiate the activation using one of the following methods:

   - "Activating selected computers" on page 494
   - "Activating computers by organizational unit" on page 495

Loading the list of clients for activation

You can load the list of clients for activation in Avamar Client Manager using one of the following methods:

- Query an LDAP v.3 compliant directory service, such as Microsoft Active Directory, to obtain information about clients and, if available, directory service organizational units, such as directory domains and directory groups.

- Import a comma-separated values (CSV) file that you either create manually or output from a Systems management tool such as Microsoft System Center Configuration Manager or Systems Management Server.

Loading clients from a directory service

To query an LDAP v.3 compliant directory service, such as Microsoft Active Directory, for a list of clients to activate with Avamar Client Manager:

1. Ensure that you have completed LDAP server configuration for Avamar Client Manager as described in "Configuring directory service information" on page 378.

2. On the Avamar Client Manager button bar, click **Activate**.

   The Activate page appears.

3. On the **Client Information** title bar, click ▼ and select **Directory Service** from the menu.

   The Directory Service dialog box appears.

4. In **User Domain**, select a directory service domain to use for directory service authentication.

5. In **User Name**, type a username for directory service authentication.

6. In **Password**, type the password for the username.
7. In **Directory Domain**, select a directory domain to query for client information.
8. Click **OK**.

   Retrieving the directory service data can take some time. To stop the data retrieval, click **Cancel**.

   The directory service authentication information is verified, client and organizational unit information is obtained from the specified directory domain, and Client Information is populated with this information.

Loading clients from a CSV file

You can load the list of clients for activation in Avamar Client Manager by importing a comma-separated values (CSV) file that you either create manually or output from a Systems management tool such as Microsoft System Center Configuration Manager or Systems Management Server.

CSV file format

The CSV file that you use to load a list of clients for activation in Avamar Client Manager should use the following format:

```
Hostname,Group
CLIENT-HOSTNAME1,GROUP1/GROUP2/GROUP3
CLIENT-HOSTNAME2,GROUP1/GROUP2
CLIENT-HOSTNAME3,
```

where:

- The first line (Hostname,Group) is an optional header value separated by a comma. You can leave this line blank, but it may make the file more accessible to others if you use the headers as shown.

  NOTICE

  Line 1 must contain the header names as shown, or a blank line. Otherwise, import fails with the following message: "Invalid file or invalid format".

- CLIENT-HOSTNAME1, CLIENT-HOSTNAME2, and CLIENT-HOSTNAME3 are the hostnames of the clients to add.
- GROUP1/GROUP2/GROUP3 and GROUP1/GROUP2 are the optional directory service logical group names to which to add the clients. A forward slash (/) is used to separate the hierarchical levels of the directory service logical group name. If you do not specify a directory service logical group name, then the client is added at the root level of the hierarchical display.
- A comma immediately follows the client hostname and precedes the directory service logical group name. The comma is required, even when a group is not listed.
- Each client is listed on a separate line.

Consider 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,
```

When you import this example file, the clients are added to the groups listed in the following table.

Table 103 Groups to which clients are added

Client	Group to which the client is added
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	Root level of the hierarchical display
ser4-desktop.Acme.corp.com	Root level of the hierarchical display

NOTICE

If you use spreadsheet software such as Microsoft Excel to create or edit the client list, do not add a comma to the end of the first cell or the beginning of the second cell in an attempt to create comma-separated values. This is not necessary because when you save the client list in the editor using the CSV file type, the editor adds the comma separators as part of the file conversion process. To verify that the client list is correctly formatted, open it in a text editor.

Loading the CSV file

After you create the CSV file with clients for activation, you can import the client list in Avamar Client Manager.

To load the CSV file:

1. On the Avamar Client Manager button bar, click **Activate**.

   The Activate page appears.

2. On the Client Information title bar, click ▼ and select **CSV File**.

   The CSV File dialog box appears.

3. Click **Browse** and select the CSV file formatted as described in "CSV file format" on page 491.

4. Click **Upload**.

   Client and organizational unit information is obtained from the imported CSV file, and Client Information is populated with this information. Avamar Client Manager displays only those clients with the Avamar software successfully installed.

Searching for computers to activate

If there is a large list of clients to activate in Client Information, then you can search for specific client computers by all or part of a local hostname.

When you perform a search, the search string is compared to the local hostname of each computer, and not the fully qualified domain name. For example, the search string "*abc*" would match the computer "abc123.dfg.example.com" but not the computer "dfg456.abc.example.com."

To find computers in Client Information:

1. On the **Client Information** title bar, click .
2. On **Find Computers**, click **Show** to include computers that are already activated, or **Hide** to hide them.
3. Choose whether to produce standard or highlighted results.
   - Clear **Highlight Search** to produce standard results.

     The standard view displays all top-level computers that match the search criteria, and all top-level folder hierarchies that contain at least one matching computer at any level. To see matching computers contained in top-level folder hierarchies, expand the displayed folder and any subfolders until the computers appear.
   - Select **Highlight Search** to produce highlighted results.

     The highlighted view displays the results of a focused search of computers that are currently visible either on the top level or in open folders on an expanded branch. Computers that are not currently visible but are on a branch that was expanded and then collapsed during the current session are also included in the search.

     The search does not include computers that are on a branch that has not been expanded during the current session.

     The highlighted view displays and selects the computers that match the search criteria. The results may require scrolling to see every matching computer.
4. Type a search string to match all or part of a local hostname.

   The search string must comply with the following rules:

   - Be no more than 24 characters.
   - Cannot start with a period character.
   - May contain an asterisk (*) to represent zero or more characters.
   - Cannot contain any of the following characters: `/:?"<>\,~!@#$%^|&’(){}_`
5. Click the button next to the search string text box to initiate the search.

   The search process can take some time. To stop a search, click Cancel.

   When the search is complete, Find Computers closes and the results are displayed in Client Information.
6. (Optional) To clear the search results and return to the full list, click on the **Client Information** title bar, and then click the **X** to the right of the text field on **Find Computers**.

Activating selected computers

After you load the list of clients, select the Avamar server to which to add them, and select the clients for activation, you can initiate the activation of the selected computers.

To activate one or more selected computers with the Avamar client software installed:

1. Select the domain for the selected computers by dragging and dropping the selected computers in **Client Information** onto one of the domains shown in **Server Information**:

   - To drag and drop matching computers in the standard results view, select the top-level computers and all top-level folder hierarchies, and drag that selection set. Selecting a folder in this view selects the matching computers that it contains. It does not select any non-matching computers that the folder contains.

   - To drag and drop matching computers in the highlighted results view, drag any one of the selected computers. All selected computers at all levels are included. To drag a single computer, click the computer name to maintain its selection, and clear all other computers.

   The Select Groups dialog box appears and lists the groups available in the domain.

2. Select the groups to which to assign the selected computers, or create a group for the computers.

   To create a group:

   a. In the **Group Name** box on the **Create Group** dialog box, type a name for the new group.

      The following characters are not allowed in a group name:
      ~!@$^%(){}[]|,`;#\/:*?‹›'"&.

   b. Choose whether to enable scheduled backups of computers in the group as soon as they are activated by selecting or clearing the **Enable** checkbox.

   c. Select a dataset, schedule, and retention policy for the group.

   d. Click **Create Group**.

3. After you select the groups in the **Select Groups** dialog box, click **Add Clients**.

   The Select Groups dialog box closes.

4. Click **Activate**.

   Show Clients for Registration appears and lists all clients available for activation.

   The Selected for Registration status indicates that the client was scheduled for activation during the current session but activation has not yet been attempted.

   The Activation Failure status indicates that a previous activation task for the client has failed, both in the initial attempt and through the queue. Clients with Activation Failure status are selected for activation by default.

5. (Optional) Remove clients from the activation:

   - To remove clients with either the **Selected for Registration** or **Activation Failure** status type, clear the appropriate checkbox.

   - To remove a specific client, Clear the checkbox next to each client that should not be included in the activation, clear the checkbox next to its name and click **Remove.**

6. Click **Commit**.

   Tasks to register and activate the selected computers are initiated as background processes. To check the status of the processes, use the "Analyzing client activity" on page 471. To check the status of the tasks, use the Activation Log, as described in "Activation log and Management log" on page 455.

   Computers that are not activated during the first attempt are added to the "Retrying activations" on page 497.

Activating computers by organizational unit

After you load the list of clients, select the Avamar server to which to add them, and select the clients for activation, you can use a directory service organizational unit to activate one or more computers with the Avamar client software installed.

To activate computers by organizational unit:

1. In **Client Information**, select the folder icon that represents the organizational unit with the computers to activate.

   When Client Information is displaying the results of a search, only those computers in the organizational unit that are also in the search results are included in the selection.

2. Select the domain for the computers in the organizational unit by dragging and dropping the organizational unit onto an Avamar server or domain in **Server Information.**

   You are prompted whether to create a domain.

3. Click **Yes** to create a domain, or click **No** to assign the computers in the organizational unit to the existing domain.

   To create a domain:

   a. In the **New Domain Name** box on the **Create Domain** dialog box, type a name for the domain.

   b. (Optional) Provide information in the **Contact**, **Phone**, **Email**, and **Location** fields.

   c. Click **OK.**

   The Select Groups dialog box appears.

4. Select the groups to which to assign the computers in the organizational unit, or create a group for the computers.

   To create a group:

   a. In the **Group Name** box on the **Create Group** dialog box, type a name for the new group.

      The following characters are not allowed in a group name:
      ~!@$^%(){}[]|,`;#\/:*?‹›'"&+

   b. Choose whether to enable scheduled backups of computers in the group as soon as they are activated by selecting or clearing the **Enable** checkbox.

   c. Select a dataset, schedule, and retention policy for the group.

   d. Click **Create Group**.

5. After you select the groups in the **Select Groups** dialog box, click **Add Clients**.

   The Select Groups dialog box closes.

6. Click **Activate**.

   Show Clients for Registration appears and lists all clients available for activation.

   If a client has the Selected for Registration status, then the client was scheduled for activation during the current session but activation has not yet been attempted.

   If a client has the Activation Failure status, then a previous activation attempt for the client has failed, both in the initial attempt and through the queue. Clients with Activation Failure status are selected for activation by default.

7. (Optional) Remove clients from the activation:

   - To remove clients with either the **Selected for Registration** or **Activation Failure** status type, clear the appropriate checkbox.

   - To remove a specific client, Clear the checkbox next to each client that should not be included in the activation, clear the checkbox next to its name and click **Remove**.

8. Click **Commit**.

   Tasks to register and activate the selected computers are initiated as background processes. To check the status of the processes, use the "Analyzing client activity" on page 471. To check the status of the tasks, use the Activation Log, as described in "Activation log and Management log" on page 455.

   Computers that are not activated during the first attempt are added to the "Retrying activations" on page 497.

Retrying activations

An activation invitation that does not immediately succeed is added to the queue. The invitation is tried again every 2 hours until it succeeds or until the limit of 24 attempts is reached. The queue can be monitored through the Activation Log.

The following table lists the status code and description of the errors that cause an invitation to be added to the queue. This information appears in the Activation Log.

Table 104 Status codes and errors that put activation invitations in the queue

Status code	Description
22271	Invitation failed — Client software could not be contacted
22237	Activation failed — Client previously activated or cannot communicate with Avamar
22280	Client reconnect error — Hostname mismatch
22282	Client reconnect error — Unknown ID
22295	Client registration error — Server not available

Removing a queued invitation

An invitation is removed from the queue if a second invitation command issued through Avamar Client Manager succeeds or if the client is removed from the pending activation state through Avamar Client Manager.

Log descriptions for queued invitations

The queue reports the progress of each invitation in the Activation Log. The possible entries for queued invitations are described in the following table.

Table 105 Entry formats for queued invitations

Entry format	Description
Activation at commit failed. Client scheduled for 24 retries. *description*	First entry displayed after an activation invitation fails when you click Commit. The *description* value is a message that describes the cause of the failure.
(*n*/24) - Activation failed - *description*	Entry displayed after n attempts fail, where *n* is an integer starting with 1 and increased by 1 after each attempt. The *description* value is a message that describes the cause of the failure.
Invitation failed. - *description*	Entry displayed after all 24 attempts fail. The *description* value is a message that describes the cause of the failure.

Creating a domain

To create a domain or subdomain on an Avamar server:

1. In the **Server Information** pane on the **Activate** window in Avamar Client Manager, select the root domain or a subdomain in which to create the domain.
2. Click **Create Domain**.

   The Create Domain dialog appears.
3. In **New Domain Name**, type a name for the domain.

   The following characters are not allowed in a domain name:
   ~!@$^%(){}[]|,`;#\/:*?‹›'"&+
4. (Optional) Provide information in the **Contact**, **Phone**, **Email**, and **Location** fields.
5. Click **OK**.

Creating a group

To create a group:

1. In the **Server Information** pane on the **Activate** window in Avamar Client Manager, select the root domain or a subdomain in which to create the group.
2. Click **Create Group**.

   The Create Group dialog box appears.
3. In **Group Name**, type a name for the new group.

   The following characters are not allowed in a group name:
   ~!@$^%(){}[]|,`;#\/:*?‹›'"&+
4. Choose whether to enable scheduled backups of computers in the group as soon as they are activated by selecting or clearing the **Enable** checkbox.
5. Select a dataset, schedule, and retention policy for the group.
6. Click **OK**.

Viewing group information for a domain

To determine the appropriate group for the clients that you are activating, it may be helpful to view a list of groups for a domain, as well as group details, such as the dataset, schedule, retention policy, and status (enabled or disabled) for the group.

To view group information for a domain:

1. Select a domain in the **Server Information** pane on the **Activation** window, and click **Show Groups**.

   Show Groups appears and lists all groups in the selected domain and any domains above it.
2. (Optional) Click **Create Group** to create a group, as discussed in "Creating a group" on page 498.
3. Click **Close**.

Viewing clients for a domain

To view a list of clients for a domain, as well as the groups to which those clients are assigned:

1. Select a domain in the **Server Information** pane on the **Activation** window, and click **Show Clients**.
2. (Optional) Filter the list of clients:
   - To view the clients for certain Avamar server, select the checkbox next to the server names in the **Server** pane.
   - To view only clients with a certain status, select the checkbox next to the status in the **Client Status** pane. The following table describes each status.

Table 106 Client status descriptions

Client Status	Description
Selected for Registration	Client has been dragged from Client Information and dropped in Server Information but has not yet been submitted for activation.
Pending Client Response	Client has been submitted for activation but has not yet responded. Client is in the queue.
Activation Failure	All client activation attempts through the queue were unsuccessful.
Activated Client	Client activation succeeded.

3. (Optional) Sort the client list in ascending or descending order by clicking a column header:
   - **Client** (local hostname)
   - **Domain**
   - **Group**
4. Click **Close**.

Searching for clients

To search for clients:

1. Click 🔍 to open the search dialog box:
   - To search all clients of all servers available to Avamar Client Manager, click the search icon on the **Server Information** title bar.
   - To search all clients in the selected Avamar domain, as well as all subdomains of the domain, click the search icon on the **Show Clients** dialog box.
   - To search all clients available for activation, click the search icon on the **Show Clients for Activation** dialog box.
2. In the text box, type a search string to match all or part of a local hostname.

   Use an asterisk (*) to represent zero or more characters.

The search string must comply with the following rules:

- No more than 24 characters
- Cannot start with a period character
- Cannot contain any of the following characters: /:?"<>\,~!@#$%^|&’(){}_

3. Limit the search to only those clients with a certain status by selecting the checkbox next to the status:

   - Selected for Registration
   - Pending Client Response
   - Activation Failure
   - Activated Client

   The Pending Client Response and Activated Client status types are not included when you search for all clients available for activation.

4. Click the button next to the text field to initiate the search.

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 describe the Avamar Desktop/Laptop features:

- Features 502
- Environment requirements 503
- User authentication 506
- Apache web server authentication 518
- Changing the default web UI port 518
- Alternate file browsing method for clients 519
- Rebranding the web UI 520
- Checking the status of Avamar Desktop/Laptop server 521
- Stopping and starting Avamar Desktop/Laptop server 521
- User selectable backup start times 521
- On-demand backups 522
- Source data additions 525
- Selectable backup sets 526
- Restore of replicated backups 527
- Restore from an alternate computer 527
- Server-class clients 529
- Restore data size limit 532
- Restore queue limit 533
- Downloads link 533
- Installing the Avamar client software 534
- Uninstalling the Avamar client software 538
- Windows and Mac client log locations 539
- Macintosh clients with Entourage 540

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 503
- "Network requirements" on page 504
- "LDAP authentication requirements" on page 504
- "Avamar system requirements" on page 505

Computer requirements

Avamar client computers using Avamar Desktop/Laptop must meet the minimum requirements in the following table.

Table 107 Minimum requirements for client computers using Avamar Desktop/Laptop

Category	Requirement
Operating system	Windows, Mac, or Linux operating systems 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 529.
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 versions 6.x.x, 7.x.x, 8.x.x, and 9.x.x • Mozilla Firefox 3.x.x On Macintosh: • Apple Safari 3.x.x, 4.x.x, and 5.x.x On Linux: • Mozilla Firefox 3.x.x 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 108 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, as described in "LDAP authentication" on page 510 and "Mixed authentication" on page 515, the environment must meet the minimum requirements in the following table.

Table 109 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 listed in ldap.properties. "dpnctl start dtlt" on page 510 provides more information about these requirements.
User accounts	Users must log in to the client computer using a domain account authenticated through the directory service. The account cannot be a generic local or domain administrator account, but can be an account with those privileges. For example, the "Administrator" account does not work, but an account named "smithb" with domain administrator rights does work.

Avamar authentication requirements

To use Avamar authentication, as described in "Avamar authentication" on page 513, the environment must meet the minimum requirements in the following table.

Table 110 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 provide NIS support, as described in "User authentication" on page 506, the environment must meet the minimum requirements in the following table.

Table 111 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.

NOTICE

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. However, certain basic requirements are common for all desktop and laptop deployments.

The requirements listed in the following table are common to all Avamar systems supporting Avamar Desktop/Laptop.

Table 112 Avamar system requirements for supporting Avamar Desktop/Laptop

Category	Requirement
Number of clients per Avamar server	Maximum of 5,000 desktops and laptops
Avamar server software version	Version 6.0 or later
Avamar client version	Version 6.0 or later
Avamar Desktop/Laptop version	Version 6.0 or later

User authentication

Avamar Desktop/Laptop enhanced features use a separate server process running on the Avamar system. The Avamar Desktop/Laptop server is installed as part of every Avamar server installation.

By default the Avamar Desktop/Laptop server provides pass-through authentication of users who are logged in to Windows and Mac computers using domain credentials. This feature does not require additional configuration. It is described in "Pass-through authentication" on page 507.

The following table provides a quick view of pass-through authentication and the other authentication methods available with Avamar Desktop/Laptop. Additional information about a method, and how to configure Avamar Desktop/Laptop to use the method, is available in the sections that follow.

Table 113 Avamar Desktop/Laptop user authentication methods (page 1 of 2)

Method	Description	Compatible options
Pass-through	Permits domain users on Windows and Mac computers to restore files without additional login. Obtains their domain credentials from the computer's OS. This method is enabled by default. It uses Avamar Desktop/Laptop's LDAP Kerberos module but does not require the configuration of that module. See "Pass-through authentication" on page 507.	• LDAP Kerberos only • Mixed Only for qualified users in domains that are not specified for Avamar authentication • NIS NIS users must log in • Local user access
LDAP	Uses an existing LDAP v.3 compatible directory service to authenticate users. The LDAP method requires configuration of directory service information and specific options. Can be used with Kerberos encryption (default) or plain text. See "LDAP authentication" on page 510.	• Pass-through Kerberos mode only • NIS NIS users must log in • Local user access Kerberos mode only

Table 113 Avamar Desktop/Laptop user authentication methods (page 2 of 2)

Method	Description	Compatible options
Avamar	Authenticates users by comparing log in credentials with user records stored on the Avamar server. The Avamar method must be enabled. User credentials must be provided. See "Avamar authentication" on page 513.	• NIS
Mixed	Authenticates users in specified Avamar domains using Avamar authentication. All other users are authenticated using LDAP in Kerberos mode, or NIS. The mixed method requires the configuration specified for both LDAP and Avamar methods. See "Mixed authentication" on page 515.	• Pass-through Only for qualified users in domains that are not specified for Avamar authentication • NIS
NIS	Authenticates users of Linux computers using an existing NIS domain. This method is compatible with all other methods. When it is enabled, every user of a Linux computer is authenticated through the NIS server by using credentials provided at the Avamar Desktop/Laptop login screen. The NIS method requires configuration to enable it. The steps to do this are included in the tasks for each of the other authentication methods.	• Pass-through Only for users who are not authenticated by NIS • LDAP • Avamar • Mixed

Pass-through authentication

Pass-through authentication uses encrypted channels to obtain user credentials from the client computer's OS and associate the credentials with file ownership properties. With this default setting, users can restore files that they own without seeing the Avamar Desktop/Laptop login screen.

On Windows, users with local administrator privileges are able to restore files owned by anyone on the computer without additional login.

Pass-through authentication is the default authentication method used by Avamar Desktop/Laptop. However, it is limited to Windows and Mac operating systems. Users logged in to computers with other operating systems are authenticated through the Avamar Desktop/Laptop login screen. To require the login screen for all users, see "Disable pass-through authentication" on page 509.

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.

Windows or Mac user authentication using common access card (CAC) technology is supported to the same extent as user authentication that uses the OS-default login mechanism.

Table 114 summarizes the configuration factors that determine whether pass-through authentication is enabled for a user.

Table 114 Authentication configuration factors that impact pass-through authentication

Configuration	Pass-through?
• OS is Windows or Mac • Pass-through authentication is enabled	Yes Users see only their data that is in backups that were created by a 6.x or newer version of Avamar client
• OS is Windows or Mac • Pass-through authentication is enabled • User logs in with a local (non-domain) account	No
• OS is not Windows or Mac • Pass-through authentication is enabled	No
• Pass-through authentication is disabled	No

Enable local users

Avamar Desktop/Laptop provides the option to enable local user access when pass-through authentication is enabled. A local user is one who is authenticated through a local computer account instead of a domain account. When local user access is enabled, local users can access the Avamar client web UI to restore their data that was backed up from the authenticating computer.

Local user access is available on supported Windows or Mac computers, and only when pass-through authentication is also enabled. 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 507.

2. Log in to the Avamar utility node as root.

   The following change applies to all clients and backups associated with the server.

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 the local user key and set its value to true.

   Change:

   ```
   #allowLocalUsers=false
   ```

   To:

   ```
   allowLocalUsers=true
   ```

6. Save and close the file.
7. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

Disable pass-through authentication

You can disable pass-through authentication and require that all users log in through the Avamar Desktop/Laptop login screen.

NOTICE

When pass-through authentication is disabled one of the following methods of authentication must be configured as the mechanism for authenticating user logins: LDAP, Avamar, or Mixed.

To disable pass-through authentication:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Create or edit the value of the userLoginRequired key:

   Change:

   ```
   userLoginRequired=false
   ```

   to:

   ```
   userLoginRequired=true
   ```

5. Save and close the file.

6. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

LDAP authentication

Avamar Desktop/Laptop can use a company's LDAP v.3-compliant directory service to authenticate users with their directory service username and password. The authentication process can use Kerberos in a Simple Authentication and Security Layer (SASL) Bind, the default, or it can use plaintext in a Simple Bind.

For a Windows or Mac user who does not qualify for pass-through authentication, the username for the domain account that is currently logged in to the computer is automatically entered in a read-only field on the Avamar Desktop/Laptop login screen. This enhances data protection on those platforms.

Configuring LDAP authentication

To configure Avamar Desktop/Laptop to authenticate users through an LDAP v.3-compliant directory service, and optionally NIS:

1. Configure Avamar with information about the directory service, as described in "Configuring directory service information" on page 378.

2. (Optional) Configure Avamar with information about your organization's NIS, as described in "Providing NIS information" on page 380.

3. Log in to the Avamar utility node as root.

4. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

5. Run **avldap** with the LDAP authentication configuration option:

   ```
   /usr/local/avamar/bin/avldap --configauth
   ```

   Depending on the current setting for the login screen, one of the following prompts appears.

   When the login screen is enabled by the current setting:

   ```
   The DT/LT login screen is currently enabled. Do you wish to disable
   DT/LT login screen (Y/N)?
   ```

   When the login screen is disabled by the current setting:

   ```
   The DT/LT login screen is currently disabled. Do you wish to enable
   DT/LT login screen (Y/N)?
   ```

   To use pass-through authentication, the login screen should be disabled.

6. To change the current setting, type **Y**.

   To retain the current setting, type **N**.

   When you type **Y**, the following messages appear:

   ```
   Modifying the DT/LT login screen property in LDAP configuration file
   (ldap.properties).
   ```

Depending on the current setting for NIS authentication, one of the following prompts appears.

When NIS authentication is enabled:

```
INFO: The NIS Authentication mechanism for Unix clients is currently
enabled.
Do you wish to disable NIS Authentication (Y/N)?
```

When NIS authentication is disabled:

```
INFO: The NIS Authentication mechanism for Unix clients is currently
disabled.
Do you wish to enable NIS Authentication (Y/N)?
```

Enabling NIS is optional. To use NIS it must be enabled here.

7. To change the current setting, type **Y**.

   To retain the current setting, type **N**.

   When you type **Y**, the following messages appear:

   ```
   Modifying the DT/LT login screen property in LDAP configuration file
   (ldap.properties).
   ```

   A message appears that indicates the authentication method that is currently set. The message relates to the following possible authentication methods:

   - LDAP with Kerberos encryption

     ```
     INFO: The existing authentication mechanism is KERBEROS
     Authentication.
     ```

   - LDAP with plain-text

     ```
     INFO: The existing authentication mechanism is Non-KERBEROS
     Authentication.
     ```

   - Avamar

     ```
     INFO: The existing authentication mechanism is AVAMAR
     Authentication.
     ```

   - Mixed

     ```
     INFO: The existing authentication mechanism is a mix of AVAMAR AND
     KERBEROS Authentication.
     ```

   The following selection prompt appears:

   ```
   CONFIGURABLE OPTIONS:
   [1] Kerberos
   [2] Non-Kerberos
   [3] Avamar
   [4] Mix
   [5] No change
   Provide the option for authentication:
   ```

8. Type **1** or **2**.

   To retain the current setting, type **5**.

   When you type **1 or 2**, the following messages appear:

   ```
   Configuring authentication mechanism in LDAP configuration file
   (ldap.properties).
   The DTLT and EMS services must be restarted to apply your changes.
   Do you wish to restart dtlt and ems services (Y/N)?
   ```

9. To restart the services and apply the change, type **Y**.

   The services restart and the following success message appears:

   ```
   Changes to the LDAP configuration file are successfully applied.
   ```

Configuration of the LDAP authentication method, and optionally NIS, is complete.

Changing the default Kerberos encryption type

The encryption type used with 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 change the default Kerberos encryption type:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open krb5.conf in a text editor.

   The file contains the following specification of encryption type:

   ```
   [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 specification, as shown in the following example section:

   ```
   #[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
   ```

Avamar authentication

The Avamar authentication implementation compares username/password combinations with user records that have been entered into Avamar server. When this form of authentication is used, the Avamar Desktop/Laptop login screen allows you to type both a username and a password. "Adding a user to a client or domain" on page 81 describes how to add user credentials for this method of authentication.

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)

NOTICE

The Avamar client web UI does not authenticate users from client-level access lists. For web UI authentication, users must be on a domain-level access list. This means that an account that is assigned one of the four client-level User roles cannot be used to access the web UI. User roles are described in "User roles" on page 74.

Configuring Avamar authentication

To configure Avamar Desktop/Laptop to use the Avamar authentication method:

1. (Optional) Configure Avamar with information about your organization's NIS, as described in "Providing NIS information" on page 380.
2. Log in to the Avamar utility node as root.
3. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

4. Run **avldap** with the LDAP authentication configuration option:

   ```
   /usr/local/avamar/bin/avldap --configauth
   ```

   Depending on the current setting for the login screen, one of the following prompts appears.

   When the login screen is enabled by the current setting:

   ```
   The DT/LT login screen is currently enabled. Do you wish to disable
   DT/LT login screen (Y/N)?
   ```

   When the login screen is disabled by the current setting:

   ```
   The DT/LT login screen is currently disabled. Do you wish to enable
   DT/LT login screen (Y/N)?
   ```

NOTICE

The login screen setting does not apply when the Avamar authentication method is used. A login screen is always displayed with this method.

5. Type **N**.

   Depending on the current setting for NIS authentication, one of the following prompts appears.

   When NIS authentication is enabled:

   ```
   INFO: The NIS Authentication mechanism for Unix clients is currently
   enabled.
   Do you wish to disable NIS Authentication (Y/N)?
   ```

   When NIS authentication is disabled:

   ```
   INFO: The NIS Authentication mechanism for Unix clients is currently
   disabled.
   Do you wish to enable NIS Authentication (Y/N)?
   ```

   Enabling NIS is optional. To use NIS it must be enabled here.

6. To change the current setting, type **Y**.

   To retain the current setting, type **N**.

   When you type **Y**, the following messages appear:

   ```
   Modifying the DT/LT login screen property in LDAP configuration file
   (ldap.properties).
   ```

   A message appears that indicates the authentication method that is currently set. The message relates to the following possible authentication methods:

   - LDAP with Kerberos encryption

     ```
     INFO: The existing authentication mechanism is KERBEROS
     Authentication.
     ```

   - LDAP with plain-text

     ```
     INFO: The existing authentication mechanism is Non-KERBEROS
     Authentication.
     ```

   - Avamar

     ```
     INFO: The existing authentication mechanism is AVAMAR
     Authentication.
     ```

   - Mixed

     ```
     INFO: The existing authentication mechanism is a mix of AVAMAR AND
     KERBEROS Authentication.
     ```

The following selection prompt appears:

```
CONFIGURABLE OPTIONS:
[1] Kerberos
[2] Non-Kerberos
[3] Avamar
[4] Mix
[5] No change
Provide the option for authentication:
```

7. Type **3**.

   To retain the current setting, type **5**.

   When you type **3**, the following messages appear:

   ```
   Configuring authentication mechanism in LDAP configuration file
   (ldap.properties).
   The DTLT and EMS services must be restarted to apply your changes.
   Do you wish to restart dtlt and ems services (Y/N)?
   ```

8. To restart the services and apply the change, type **Y**.

   The services restart and the following success message appears:

   ```
   Changes to the LDAP configuration file are successfully applied.
   ```

Configuration of the Avamar authentication method is complete.

Mixed authentication

Mixed authentication provides the ability to use LDAP with Kerberos authentication (with or without pass-through authentication) together with Avamar authentication. The domains that use Avamar authentication are specified in a value in ldap.properties. Domains that are not specified in that value use LDAP with Kerberos authentication.

All users in the domains specified for Avamar authentication always see a login screen and must use their Avamar account information to log in.

Pass-through authentication is enabled by default in all domains that are not specified for Avamar authentication.

To select and configure the mixed authentication method:

1. Configure Avamar with information about the directory service, as described in "Configuring directory service information" on page 378.

2. (Optional) Configure Avamar with information about your organization's NIS, as described in "Providing NIS information" on page 380.

3. Log in to the Avamar utility node as root.

4. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

5. Run **avldap** with the LDAP authentication configuration option:

   ```
   /usr/local/avamar/bin/avldap --configauth
   ```

Depending on the current setting for the login screen, one of the following prompts appears.

When the login screen is enabled by the current setting:

```
The DT/LT login screen is currently enabled. Do you wish to disable
DT/LT login screen (Y/N)?
```

When the login screen is disabled by the current setting:

```
The DT/LT login screen is currently disabled. Do you wish to enable
DT/LT login screen (Y/N)?
```

To use pass-through authentication, the login screen should be disabled, as described in "Pass-through authentication" on page 507.

6. To change the current setting, type **Y**.

   To retain the current setting, type **N**.

   When you type **Y**, the following messages appear:

   ```
   Modifying the DT/LT login screen property in LDAP configuration file
   (ldap.properties).
   ```

   Depending on the current setting for NIS authentication, one of the following prompts appears.

   When NIS authentication is enabled:

   ```
   INFO: The NIS Authentication mechanism for Unix clients is currently
   enabled.
   Do you wish to disable NIS Authentication (Y/N)?
   ```

   When NIS authentication is disabled:

   ```
   INFO: The NIS Authentication mechanism for Unix clients is currently
   disabled.
   Do you wish to enable NIS Authentication (Y/N)?
   ```

   Enabling NIS is optional. To use NIS it must be enabled here.

7. To change the current setting, type **Y**.

   To retain the current setting, type **N**.

   When you type **Y**, the following messages appear:

   ```
   Modifying the DT/LT login screen property in LDAP configuration file
   (ldap.properties).
   ```

A message appears that indicates the authentication method that is currently set. The message relates to the following possible authentication methods:

- LDAP with Kerberos encryption

  ```
  INFO: The existing authentication mechanism is KERBEROS
  Authentication.
  ```

- LDAP with plain-text

  ```
  INFO: The existing authentication mechanism is Non-KERBEROS
  Authentication.
  ```

- Avamar

  ```
  INFO: The existing authentication mechanism is AVAMAR
  Authentication.
  ```

- Mixed

  ```
  INFO: The existing authentication mechanism is a mix of AVAMAR AND
  KERBEROS Authentication.
  ```

The following selection prompt appears:

```
CONFIGURABLE OPTIONS:
[1] Kerberos
[2] Non-Kerberos
[3] Avamar
[4] Mix
[5] No change
Provide the option for authentication:
```

8. Type **4**.

   To retain the current setting, type **5**.

   When you type **4**, the following prompt appears:

   ```
   Enter the path of Avamar Domains to be configured for Avamar
   Authentication as a comma separated list.
   ```

9. Type the names of the Avamar domains that will use Avamar authentication as a comma-separated list.

   For example, if the Avamar domains to use Avamar authentication are called Louisville, Irvine, and Bangalore, type:

   `Louisville, Irvine, Bangalore`

   The following messages appear:

   ```
   Configuring authentication mechanism in LDAP configuration file
   (ldap.properties).
   The DTLT and EMS services must be restarted to apply your changes.
   Do you wish to restart dtlt and ems services (Y/N)?
   ```

10. To restart the services and apply the change, type **Y**.

    The services restart and the following success message appears:

    ```
    Changes to the LDAP configuration file are successfully applied.
    ```

Configuration to use the mixed authentication method is complete.

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.

Changing the default web UI port

Access to the web UI involves HTTPS communication between the Avamar server and the client's web browser. When a "Back Up..." or "Restore..." request is made from 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.

Client change

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 115 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

Server changes

To change the HTTPS listening port on Avamar server:

1. Log in to the Avamar utility node as root.
2. Open the Apache SSL configuration file in a plain text editor.

Table 116 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

3. Find and change the HTTPS port listening directive.

   Change:

   ```
   Listen 443
   ```

   to

   ```
   Listen n
   ```

   where *n* is the new initial contact port.

4. Save and close the file.
5. Restart the Apache server daemon, httpd, using apachectl:

   ```
   apachectl restart
   ```

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:

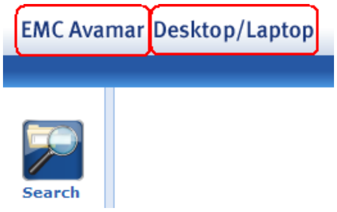
- Port 28002 on the client is blocked by a firewall rule
- The client is behind a NAT

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. Log in to the Avamar utility node as root.
3. Change the working directory by typing:

```
cd /usr/local/avamar-dtlt-tomcat/webapps/dtlt/images/banner
```

4. Make backup copies of the original graphics by typing:

```
cp ProductNameAvamar.png ProductNameAvamar.png_orig
cp ProductNameDTLT.png ProductNameDTLT.png_orig
```

5. Move the 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.

6. To view the new graphic on those browsers, delete cached copies of previously viewed files.

Table 117 Steps for deleting cached files by browser (page 1 of 2)

Browser	Steps to Delete Cached Copies of Files
IE6	1. Select **Tools** › **Internet Options** › **General** (tab) › **Delete Files**. 2. Click **OK** and click **OK** again.
IE 7	1. Select **Tools** › **Delete Browsing History** › **Temporary Internet Files** › **Delete Files**. 2. Click **Close** and click **OK**.
IE 8	Select **Tools** › **Delete Browsing History** › **Temporary Internet Files** › **Delete**.

Table 117 Steps for deleting cached files by browser (page 2 of 2)

Browser	Steps to Delete Cached Copies of Files
Firefox 3.x	Select **Tools** › **Clear Private Data** › **Cache** (checkbox) › **Clear Private Data Now.**
Firefox 3.5.x and 3.6.x	Select **Tools** › **Clear Recent History** › **Time range to clear** (list box; select: **Everything**) › **Details** (list box; select: **Cache**) › **Clear Now.**
Safari 3, 4, and 5 for Macintosh	Select **Safari** (menu)› **Empty Cache** › **Empty.**

Checking the status of Avamar Desktop/Laptop server

To check the status of Avamar Desktop/Laptop server:

1. Log in to the Avamar utility node as root.
2. 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. Log in to the Avamar utility node as root.
2. To stop Avamar Desktop/Laptop, type:

   ```
   dpnctl stop dtlt
   ```

3. To start Avamar Desktop/Laptop, type:

   ```
   dpnctl start dtlt
   ```

User selectable backup start times

With the Avamar Desktop/Laptop enhancements you can allow users to select a different backup start time 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

A user can select from the available start time list if all of the following is true:

- Client's group uses a Daily schedule.
- Client has the Override group schedules setting enabled, as described in "Allowing users to select an alternative backup start time" on page 173.
- Time entries have been added to the Override Daily Schedule, as described in "Editing the override schedule" on page 141.

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 schedule" on page 141.

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 on an alternative start time is also removed.

Time zone

The server's time zone is used when editing the Override Daily Schedule, as described in "Editing the override schedule" on page 141.

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 118 Operating systems and associated datasets used by on-demand backups

Operating system	Data backed up
Non-server-class Windows and all Macintosh	Dataset for each assigned group
Server-class Windows, as discussed in "Server-class clients" on page 529	Default dataset, as discussed in "Datasets" on page 120

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 526.

On-demand backups that start during daily server system maintenance are rejected with the following message:

```
Back Up Now is unavailable because daily system maintenance is running.
   Try your backup again later. Daily maintenance is configured to
   occur during a period of low system usage. For information about
   daily maintenance start and stop times contact your backup
   administrator.
```

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
- Backups cannot be run during the maintenance window

When these practical limitations are not enough to ensure that the number of on-demand backups from clients 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 119 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 2^{63} and a day is defined as midnight to midnight using the Avamar server’s time zone. Unsuccessful backups do not count towards the total.

To set an on-demand backup limit:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Edit the value of the restrictBackupsPerDay key:

   Change:

   ```
   restrictBackupsPerDay=false
   ```

   To:

   ```
   restrictBackupsPerDay=n
   ```

   where *n* is any positive integer less than 2^{63} or *n* is **0**.

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server by typing:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

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 146. 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.

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 174 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
- On demand, back up 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 the Avamar Desktop/Laptop enhancements 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 179.
- Changing a value in dtlt.properties, as described in “Enable selectable backup sets for Avamar Desktop/Laptop clients” on page 526.

Enable selectable backup sets for Avamar Desktop/Laptop clients

To enable selectable backup sets for Avamar Desktop/Laptop clients:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Edit the value of the allowUserInititedBackupsFileSelection key:

   Change:

   ```
   allowUserInititedBackupsFileSelection=false
   ```

   To:

   ```
   allowUserInititedBackupsFileSelection=true
   ```

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server by typing:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

Restore of replicated backups

An Avamar client can be moved to a new server, either by using Avamar Client Manager as described in "Moving clients to a new server" on page 460, or by using Enterprise Manager's replication commands. When a client is moved, its backups are replicated on the new server.

Replicated backups must be indexed before they can be available to browse or search in the web UI. Indexing is initiated by a user, after logging in to the web UI.

When a computer has replicated backups that have not yet been indexed, users accessing the web UI are presented with the login screen. The login screen appears for all users with replicated backups that have not yet been indexed, including those that normally qualify for transparent login. After indexing, the login screen does not appear for users who qualify for transparent login.

After the 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 this 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, the user's web browser is sent a refresh command and the data from the replicated backups is fully available 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 120 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 120 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. Also, users who are local administrators on a Windows source computer at the time of a backup, can restore any file from that source computer, regardless of ownership, to a target computer.

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. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Create or edit the value of the disableRestoreFromAlternateComputer key:

   Change:

   ```
   disableRestoreFromAlternateComputer=false
   ```

   to:

   ```
   disableRestoreFromAlternateComputer=true
   ```

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

Server-class clients

In addition to support for traditional desktop and laptop computers, the Avamar Desktop/Laptop enhancements also support some server-class computers. Supported are computers that are running the server versions of the Windows and Macintosh operating systems.

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:

- (Windows servers only) "Back up now dataset" on page 530
- "Backup of large number of files" on page 530
- "Backup on battery power" on page 530
- "Disable restores" on page 531

Back up now dataset

On Windows server-class computers only, clicking Back Up Now on the Client menu or on the Backup reminder launches a backup of the client's dataset.

By default the dataset assigned to server-class computers is the Default Dataset. This is the dataset assigned to the Default Group.

The initial settings of the Default Dataset are designed to be as inclusive as possible. They are:

- Use all available source data plug-ins
- Limited inherent exclusions and no explicit exclusions

These default settings are described in "Datasets, Schedules, and Retention Policies" on page 119.

On Macintosh server-class computers and on Windows and Macintosh desktop and laptop computers, clicking Back Up Now on the client menu or on the backup reminder launches a backup of each dataset, for each of the groups for the computer.

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 532, 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 85.

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 527 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.

Disable restores for server-class computers

To disable restores on server-class computers:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Edit the value of the allowServerRestores key:

   Change:

   ```
   allowServerRestores=true
   ```

   To:

   ```
   allowServerRestores=false
   ```

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server by typing:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

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. If 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 529.

To set a restore data size limit:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Uncomment and edit the value of the limitRestoreSize key:

   Change:

   ```
   #limitRestoreSize=500
   ```

   To:

   ```
   limitRestoreSize=n
   ```

   where *n* is the data size limit in megabytes.

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

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.

To allow multiple restore tasks:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.
4. Create or edit the value of the disallowMultipleRestores key:

   Change:

   ```
   disallowMultipleRestores=true
   ```

   to:

   ```
   disallowMultipleRestores=false
   ```

5. Save and close the file.
6. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

Downloads link

The Downloads link is a hyperlink that appears on the Avamar Desktop/Laptop login window. This link provides access to a web page with client and plug-in installer package downloads. For computers that have Avamar Desktop/Laptop installed, this link can be hidden or visible. By default the link is hidden.

Users who log in from a Windows or Mac computer do not see the login screen if they meet the requirements of pass-through authentication described in "Pass-through authentication" on page 507. To ensure those users have access to the Downloads link when it is visible, a login screen must be displayed for all users.

To display the downloads link:

1. Log in to the Avamar utility node as root.
2. Change the current working directory by typing:

   ```
   cd /usr/local/avamar/etc
   ```

3. Open the Avamar Desktop/Laptop properties file, dtlt.properties, in a text editor such as vi or Emacs.

4. Create or edit the value of the show.downloads.link key:

   Change:

   ```
   show.downloads.link=false
   ```

   to:

   ```
   show.downloads.link=true
   ```

5. Create or edit the value of the userLoginRequired key:

   Change:

   ```
   userLoginRequired=false
   ```

   to:

   ```
   userLoginRequired=true
   ```

6. Save and close the file.

7. Restart the Avamar Desktop/Laptop server:

   ```
   dpnctl stop dtlt
   dpnctl start dtlt
   ```

Installing the Avamar client software

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 assign computers to groups as described in "Activating clients" on page 490.

Avamar client for Windows can be installed using several silent install options. These are described in "Windows install options" on page 535.

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 install 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 filesystem and the bracketed arguments are optional, as described in "Windows install options" on page 535.

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 121 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 sucessfully installed but is not activated.
Set the Avamar domain path used 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".

Table 121 Arguments to apply Windows install options (page 2 of 2)

Description	Argument
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.
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 install 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 filesystem and *install_location* is the location in which to install the software.

   Normally, *install_location* is the root (/), but any local volume is allowed.

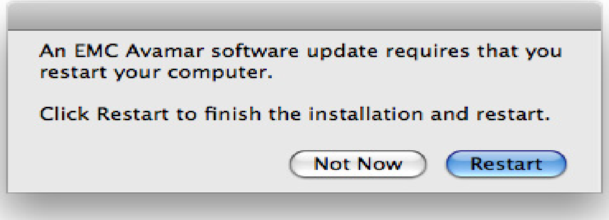
5. Launch the Systems management tool installation process.

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.



An EMC Avamar software update requires that you restart your computer.

Click Restart to finish the installation and restart.

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 "Downloads link" on page 533. 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*.

Uninstalling the Avamar client software

The following topics explain how to uninstall the Avamar client and the Avamar Desktop/Laptop software.

Uninstalling on Windows

To uninstall the Avamar client and the Avamar Desktop/Laptop 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**.

Uninstalling on Macintosh

To uninstall the Avamar client and the Avamar Desktop/Laptop 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 command "sudo" 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
   ```

Windows and Mac client log locations

Local logs on Windows and Mac 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 122 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 Mac computers the logs are available through the paths in the following table.

Table 123 Paths to logs on Macintosh computers

Log	Path
Workorder	/var/avamar/clientlogs/
Agent	/var/avamar/
Console	$HOME/.avamardata/

Macintosh clients with Entourage

Microsoft Entourage is a Macintosh email client that uses the Microsoft Database Daemon to manage its database. To protect the Entourage data, both Entourage and the Microsoft Database Daemon must be shut down during backups. The Avamar client software provides scripts to:

- Shut down Entourage and the Microsoft Database Daemon before running a backup.
- Restart the Microsoft Database Daemon when the backup is complete.

  You must manually restart the Entourage program.

Dataset policies are used to run the scripts. Macintosh clients running Entourage should be assigned to groups using a dataset with these policies. Other clients should be assigned to groups using a dataset without these policies.

NOTICE

Assigning Macintosh clients running Entourage to groups without these policies causes the Entourage database to be skipped during backups, and errors to appear in the client logs.

Creating the dataset

All groups for Macintosh clients running Entourage should use a dataset that provides the necessary policies.

To create a dataset with the required policies:

1. Create a dataset as described in "Creating a dataset" on page 124.

   The plug-in type must be Macintosh Desktop/Laptop.

2. Select the dataset **Options** tab.

3. Select **Show Advanced Options.**

4. In the **Pre-Script** section of that tab, in **Run user-defined script at beginning of backup**, type:

   ```
   shutdown.sh
   ```

5. In the **Pre-Script** section of that tab, select **Abort backup if script fails.**

6. In the **Post-Script** section of that tab, in **Run user-defined script at end of backup**, type:

   ```
   startup.sh
   ```

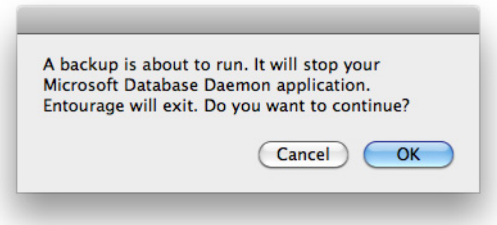
7. In the Post-Script section of that tab, select **Exit process with script failure exitcode.**

8. When all other configuration for the dataset is complete, click **OK.**

Assign this dataset, or one with the same changes on the Options tab, to each group for Macintosh clients with Entourage.

Client backup message

Macintosh clients that are assigned to a group that uses a dataset configured for Macintosh clients with Entourage see a message whenever a scheduled or on-demand backup task is initiated.



A backup is about to run. It will stop your Microsoft Database Daemon application. Entourage will exit. Do you want to continue?

The options with this message are in the following table.

Table 124 Client backup message options

Option	Result
Cancel	The Microsoft Database Daemon is not shut down, and the backup task is canceled.
OK	The Microsoft Database Daemon is immediately terminated, Entourage is shut down, and the backup task is started. At the conclusion of the backup, the Microsoft Database Daemon is restarted. Manual startup of Entourage is required.
No Action	The message is displayed for 30 seconds, after which the Microsoft Database Daemon is terminated, Entourage is shut down, and the backup task is started. At the conclusion of the backup, the Microsoft Database Daemon is restarted. Manual startup of Entourage is required.

CHAPTER 21
Using Avamar with Data Domain

The following topics provide details on how to use Avamar with Data Domain:

- How Avamar and Data Domain work together 544
- Managing Data Domain systems 549
- Backup to a Data Domain system 554
- Restore from a Data Domain system 556
- System maintenance with Data Domain 556
- Replication with Data Domain 558
- Monitoring and reporting with Data Domain 565
- Troubleshooting Data Domain 567

How Avamar and Data Domain work together

You can store Avamar backups on one or more Data Domain systems, and then seamlessly restore data from the backups.

Avamar clients that support backup and restore to and from Data Domain include:

- IBM DB2
- Microsoft Exchange VSS
- Microsoft Hyper-V VSS
- Microsoft SQL Server
- Microsoft SharePoint VSS
- Oracle
- SAP
- Sybase
- VMware® image backup and restore

The storage and retrieval of backups for these clients on a Data Domain system may be faster than on an Avamar server, especially if there is a large, active database in the environment.

A Data Domain system manages large datasets of greater than 5 TB more effectively than an Avamar server. A Data Domain system also manages large datasets with a high daily change rate of more than 5 percent more effectively than an Avamar server.

Architecture of Avamar with Data Domain

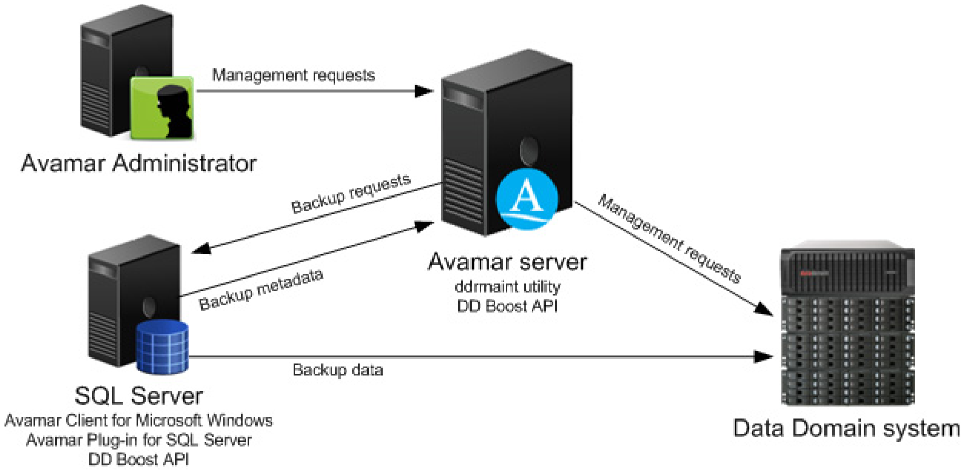
Avamar clients use the DD Boost API to access a Data Domain system. The DD Boost API is installed automatically on the client computer when you install the Avamar client.

The **ddrmaint** utility implements all required operations on the Data Domain system for the Avamar server. The **ddrmaint** utility is installed on the utility node of a multi-node server, or the single node of a single-node server, during Avamar server installation. It is not installed on the data nodes of the Avamar server.

The **ddrmaint** utility uses the DD Boost API to connect to a Data Domain system. The DD Boost API is installed with the **ddrmaint** utility automatically when you install Avamar.

Basic architecture

The following figure illustrates a basic Avamar environment with a Data Domain system. In this example, the client is a SQL server that sends Avamar backup data to a Data Domain system.

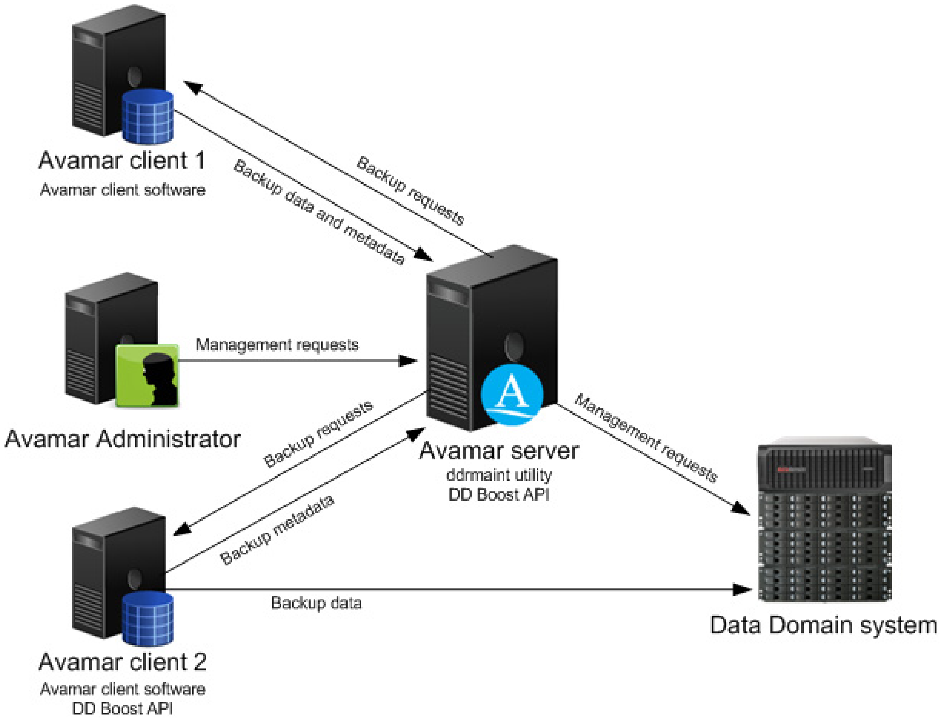


NOTICE

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.

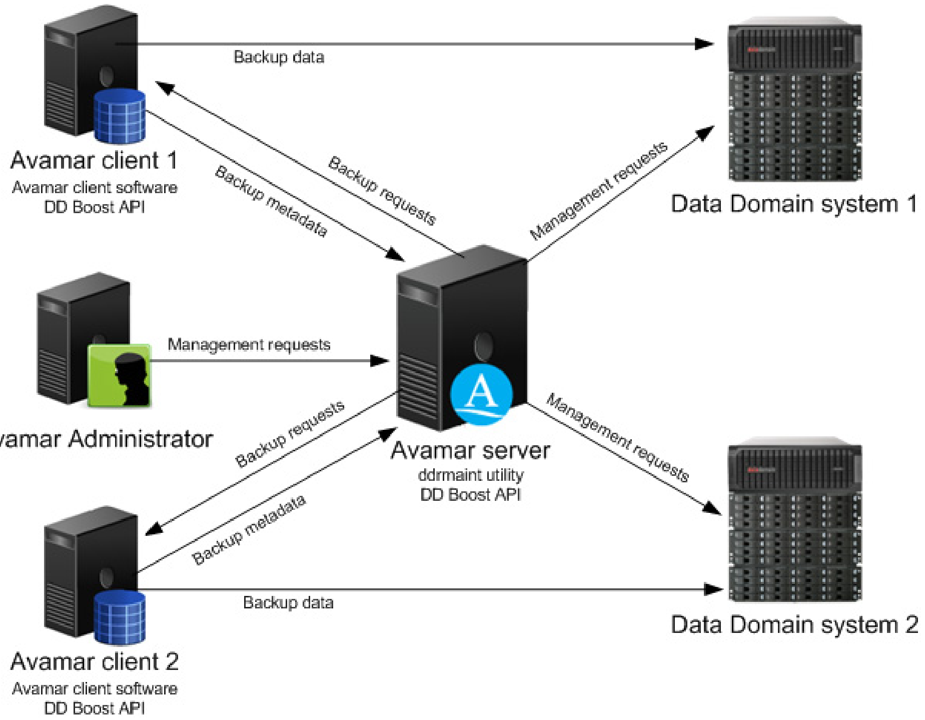
Mixed client environment

In an environment with multiple Avamar clients, some Avamar clients can send backups to the Data Domain system, while other clients send backups to the Avamar server. In the following figure, Avamar client 1 sends backups to the Avamar server, and Avamar client 2 sends backups to the Data Domain system.



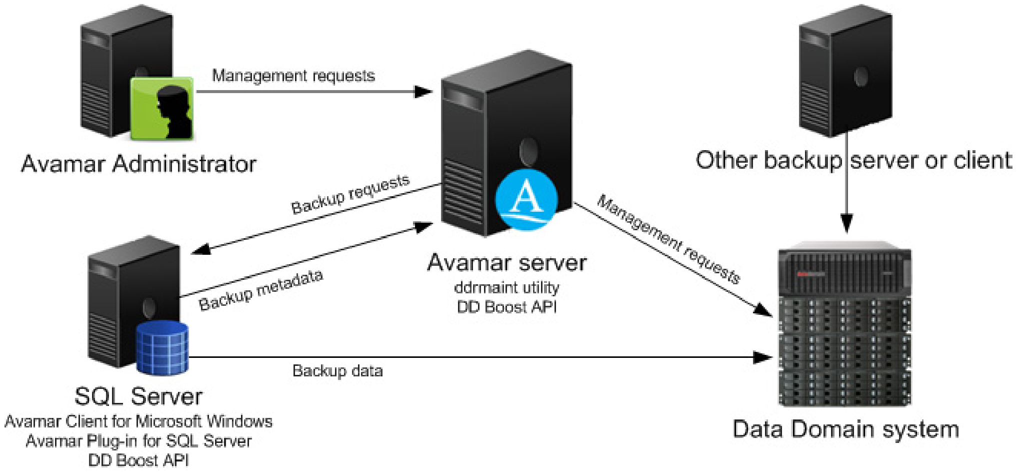
Multiple Data Domain systems

To segregate data, use multiple Data Domain systems with a single Avamar server. In the following figure, Avamar client 1 sends backups to Data Domain system 1, and Avamar client 2 sends backups to Data Domain system 2.



Shared Data Domain system

Avamar can share a Data Domain system with other backup solutions, as shown in the following figure.



The other backup solution can be any other backup product that uses a Data Domain system, or it can be another Avamar server.

The architecture of an Avamar environment with Data Domain is flexible and can combine several different strategies. For example, multiple Avamar clients can send backups to a single Data Domain system that is shared with another backup server, while other Avamar clients send backups to the Avamar server.

Supported backup types

You can perform full backups, incremental backups, and differential backups when a Data Domain system is the backup target. You can also perform VMware backups with change-block tracking enabled.

Store the full backup for a client and all subsequent incremental and differential backups on either the Avamar server or a single Data Domain system. Avamar does not support:

- Full backup on a Data Domain system and incremental or differential backups on the Avamar server
- Full backup on the Avamar server and incremental or differential backups on a Data Domain system
- Full backup on one Data Domain system and incremental or differential backups on another Data Domain system

If you change the device on which backups for a client are stored, then you must perform a full backup before any further incremental or differential backups.

There are two exceptions to the requirement for storing all backup types on a single server:

- If you use the Avamar Plug-in for SQL Server and you perform a tail-log backup during a restore, then the tail-log backup is always stored on the Avamar server.
- If you use the Avamar Plug-in for Exchange VSS, then the Microsoft Exchange log files are always backed up to the Avamar server. In addition, files in Exchange VSS backups that are less than 10 MB are always stored on the Avamar server, regardless of the selected backup target.

System requirements

The *EMC Avamar and Data Domain Integration Guide* provides details on system requirements to use Avamar with Data Domain, including:

- Supported Data Domain device types
- Supported Data Domain Operating System (DD OS) version
- DD Boost configuration requirements
- Licensing requirements

Managing Data Domain systems

The following topics provide details on how to manage Data Domain systems in the Avamar configuration:

- "Preparing the Data Domain system" on page 549
- "Adding a Data Domain system" on page 550
- "Editing a Data Domain system" on page 552
- "Deleting a Data Domain system" on page 553

Preparing the Data Domain system

Before you can add a Data Domain system to the Avamar configuration, you must prepare the Data Domain system by enabling DD Boost and creating a DD Boost user account for Avamar to use to access the Data Domain system for backups, restores, and replication, if applicable.

NOTICE

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.

To prepare the Data Domain system:

1. Enable DD Boost on the Data Domain system by logging in to the Data Domain CLI as an administrative user and typing:

   ```
   ddboost enable
   ```

2. Create a DD Boost account and password:

   a. Log in to the Data Domain CLI as an administrative user.

   b. Create the user account with admin privileges by typing:

      ```
      user add USER priv admin
      ```

      where USER is the username for the new account.

   c. Set the new account as the DD Boost user by typing:

      ```
      ddboost set user-name USER
      ```

      where USER is the username for the account.

   d. Disable and then reenable DD Boost to allow the changes to take effect by typing the following commands:

      ```
      ddboost disable
      ddboost enable
      ```

Adding a Data Domain system

When you add a Data Domain system to the Avamar configuration, Avamar creates an MTree on the Data Domain system for the Avamar server. The MTree refers to the directory created within the DD Boost path.

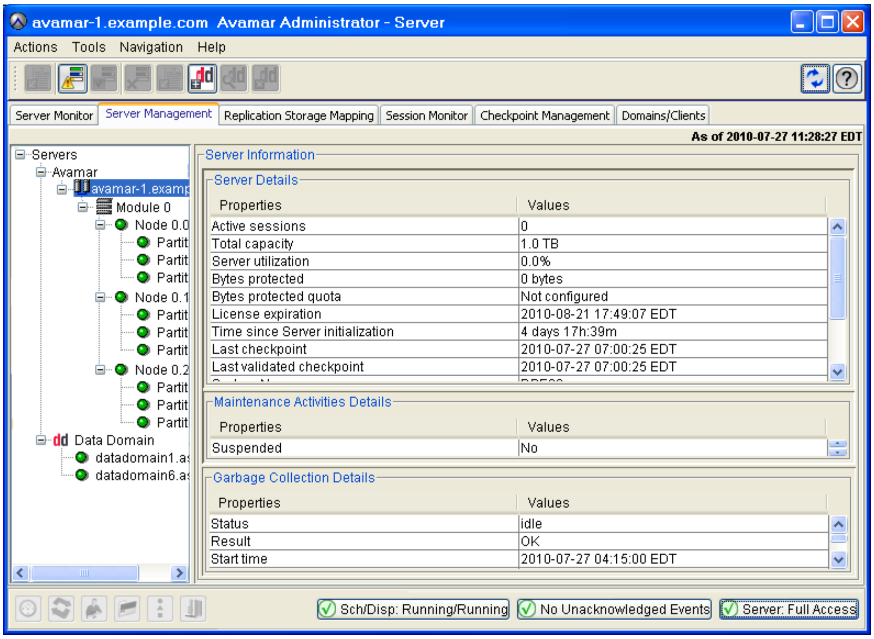
Data Domain systems support a maximum of 100 MTrees. If you reach the limit, then you cannot add the Data Domain system to the Avamar configuration.

To add a Data Domain system to the Avamar configuration:

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

   The Server window appears.

2. Click the **Server Management** tab.



As of 2010-07-27 11:28:27 EDT

Server Information

Server Details

Properties	Values
Active sessions	0
Total capacity	1.0 TB
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	2010-08-21 17:49:07 EDT
Time since Server initialization	4 days 17h:39m
Last checkpoint	2010-07-27 07:00:25 EDT
Last validated checkpoint	2010-07-27 07:00:25 EDT

Maintenance Activities Details

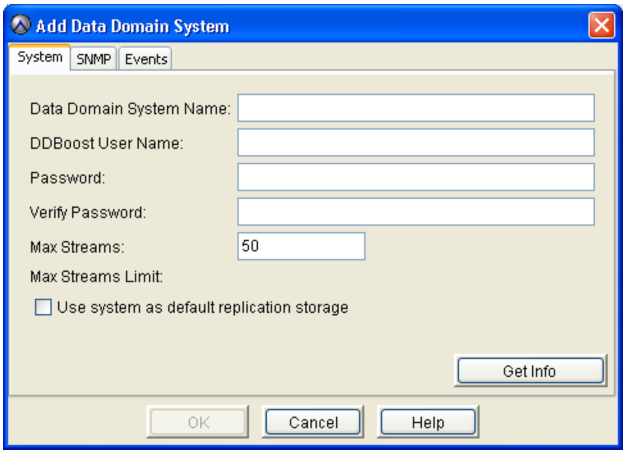
Properties	Values
Suspended	No

Garbage Collection Details

Properties	Values
Status	idle
Result	OK
Start time	2010-07-27 04:15:00 EDT

3. Select **Actions › Add Data Domain System**.

   The Add Data Domain System dialog box appears.



Data Domain System Name:

DDBoost User Name:

Password:

Verify Password:

Max Streams: 50

Max Streams Limit:

☐ Use system as default replication storage

4. In the **Data Domain System Name** box, type the fully qualified domain name of the Data Domain system to add.

NOTICE

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.

5. 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.
6. 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.
7. In the **Verify Password** box, type the password again to verify it.
8. Click the **Get Info** button in the bottom right corner of the dialog box.

   The maximum number of streams that the Data Domain system supports is listed next to Max Streams Limit.
9. In the **Max Streams** box, type the maximum number of Data Domain system streams that Avamar can use at any one time to perform backups and restores.

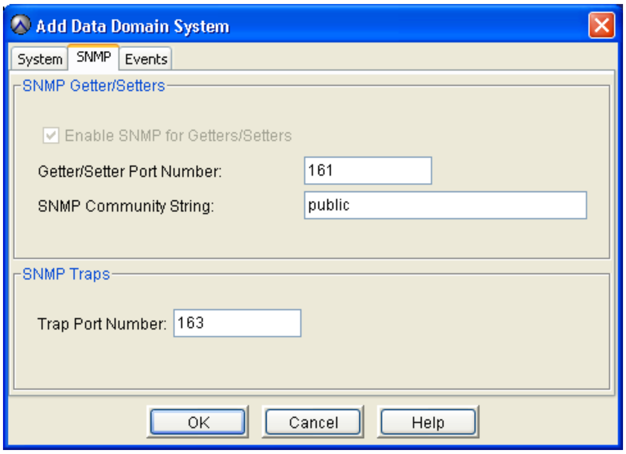
   Consider both the maximum number of streams that the Data Domain system supports (listed next to Max Streams Limit), as well as whether other applications are using streams to send data to and receive data from the Data Domain system.

   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.

   NOTICE

   Avamar uses multiple streams for backups to and restores from Data Domain for Microsoft Exchange VSS, Microsoft Hyper-V VSS, Microsoft SharePoint VSS, Microsoft SQL Server, Oracle, SAP, and Sybase. Multiple streams to and from a Data Domain system are *not* supported for IBM DB2 and VMware image backups.
10. To use the Data Domain system as the default replication destination when a destination Data Domain system is not identified, select the **Use system as default replication storage** option. "Replication with Data Domain" on page 558 provides details.

11. Click the **SNMP** tab.



Add Data Domain System

SNMP Getter/Setters

☑ Enable SNMP for Getters/Setters

Getter/Setter Port Number: 161

SNMP Community String: public

SNMP Traps

Trap Port Number: 163

12. On the **SNMP** tab, verify the SNMP configuration:

    - The **Getter/Setter Port Number** 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** box lists the community string for Avamar to have read/write access to the Data Domain system.
    - The **Trap Port Number** box lists the trap port on the Avamar server. The default value is 163.

    SNMP configuration enables Avamar to collect and display data for health monitoring, system alerts, and capacity reporting.

13. Click **OK**.

Editing a Data Domain system

To edit the configuration for a Data Domain system in Avamar:

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

   The Server window appears.

2. Click the **Server Management** tab.

3. Select the Data Domain system to edit.

4. Select **Actions › Edit Data Domain System**.

   The Edit Data Domain System dialog box appears.

5. Edit the settings for the Data Domain system as necessary. "Adding a Data Domain system" on page 550 provides details on each setting.

   NOTICE

   If the **Re-add SSH Key** and **Re-add Trap Host** buttons are enabled, then click the buttons to restore the SSH key and trap host values on the Data Domain system. When these buttons are enabled, then the configuration on the Avamar server is not synchronized with the configuration on the Data Domain system. Clicking the buttons restores the values to the Data Domain system to ensure synchronization.

6. Click **OK**.
7. If you edited the Data Domain system name, the DD Boost username, or the DD Boost password, then create and validate a new checkpoint.

   If you perform a rollback to a checkpoint with the outdated Data Domain system name or DD Boost information, then the rollback fails.

Deleting a Data Domain system

You can delete a Data Domain system from the Avamar configuration if the Data Domain system is online and if there are multiple Data Domain systems configured on the Avamar server.

If you are deleting the only Data Domain system configured on the Avamar server, or if the Data Domain system is offline, then the Avamar server requires advanced service. Contact your EMC sales representative to purchase this service.

To delete a Data Domain system from the Avamar configuration:

1. Ensure that no backups are stored on the Data Domain system:
   - Delete each backup for all clients that use the Data Domain system as a backup target.
   - Ensure that all backups on the Data Domain system are expired and deleted through the Avamar GC process.
   - Ensure that there are no checkpoints for the Avamar server with backups on the Data Domain system. There are two ways to do this:
     - Wait for all checkpoints that contain backups for the Data Domain system to expire.
     - Perform and validate a new checkpoint after all backups to the Data Domain system are deleted, and then delete all other checkpoints.
2. Ensure that the Data Domain system is not the default replication storage system.

   "Setting the default Data Domain destination" on page 563 provides details on designating a default replication storage system.
3. In Avamar Administrator, click the **Server** launcher button.

   The Avamar Server window appears.
4. Select the **Server Management** tab.
5. Select the Data Domain system to delete.
6. Select **Actions** › **Delete Data Domain System**.

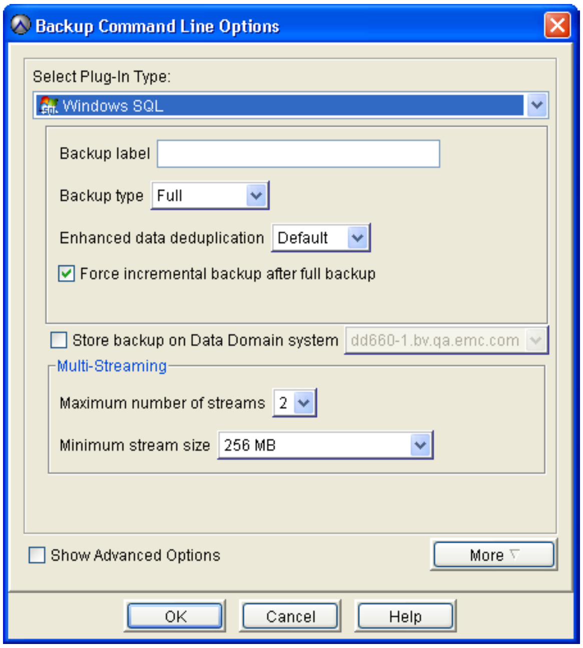
   A confirmation message appears.
7. Click **OK**.
8. Create and validate a new checkpoint.

   If you perform a rollback to a checkpoint with the deleted Data Domain system, then the Data Domain system is restored to the configuration.

Backup to a Data Domain system

To configure backups from an Avamar client to a Data Domain system:

1. Add the Data Domain system to the Avamar configuration, as discussed in "Adding a Data Domain system" on page 550.
2. Select the Data Domain system as the target for the backup:
   - For an on-demand backup, open the **Backup Command Line Options** dialog box, select **Store backup on Data Domain system**, and then select the Data Domain system to use from the list, as shown in the following example for a SQL Server plug-in.



Backup Command Line Options

Select Plug-In Type: Windows SQL

Backup label

Backup type Full

Enhanced data deduplication Default

☑ Force incremental backup after full backup

□ Store backup on Data Domain system dd660-1.bv.qa.emc.com

Multi-Streaming

Maximum number of streams 2

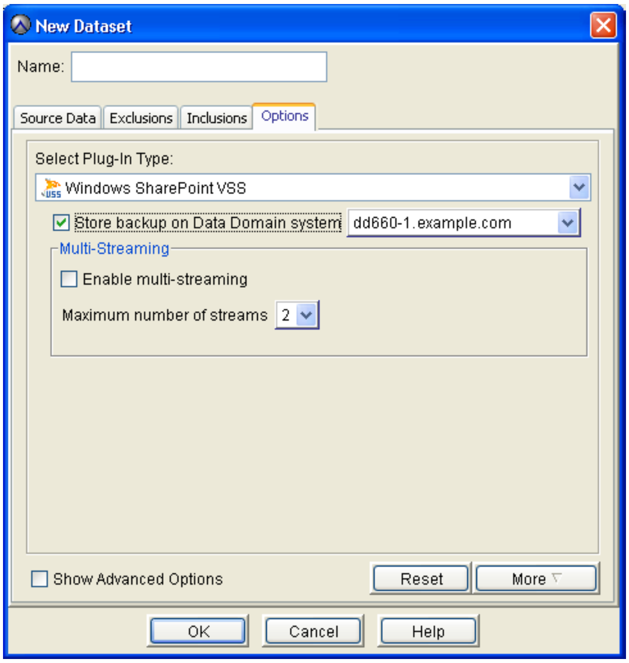
Minimum stream size 256 MB

□ Show Advanced Options

A Data Domain system in the list is dimmed when a plug-in does not support the DD OS version on the Data Domain system. You cannot store backups for the plug-in on the Data Domain system.

"Performing an on-demand backup" on page 86 provides details on on-demand backups.

- For a scheduled backup, select the Data Domain system on the **Options** tab for the dataset, as shown in the following example for a SharePoint VSS plug-in.



Select Plug-In Type: Windows SharePoint VSS

☑ Store backup on Data Domain system dd660-1.example.com

Multi-Streaming

□ Enable multi-streaming

Maximum number of streams 2

□ Show Advanced Options

If a Data Domain system in the list is dimmed, then the plug-in listed in the **Select Plug-In Type** list does not support the DD OS version on the Data Domain system. You cannot store backups for the plug-in on the Data Domain system.

"Creating a dataset" on page 124 provides details on dataset settings.

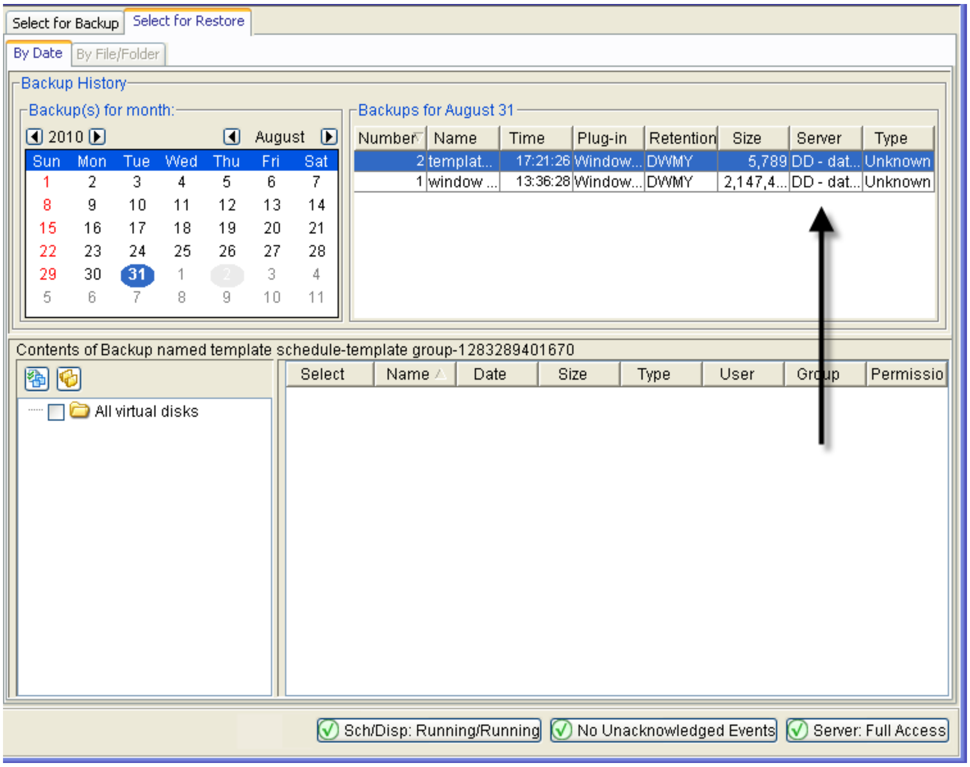
NOTICE

If you cancel a backup while it is in progress, then Avamar deletes the backup data that was written to the Data Domain system during the next cycle of the Garbage Collection (GC) process.

Restore from a Data Domain system

When you restore an Avamar backup from a Data Domain system, the data streams directly from the Data Domain system to the Avamar client.

When you select a backup to restore, you can identify whether a backup is on the Avamar server or on a Data Domain system by viewing the Server column on the Select for Restore tab of the Backup and Restore window, as shown in the following example.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Backups for August 31

Number	Name	Time	Plug-in	Retention	Size	Server	Type
2	templat...	17:21:26	Window...	DWMY	5,789	DD - dat...	Unknown
1	window ...	13:36:28	Window...	DWMY	2,147,4...	DD - dat...	Unknown

Contents of Backup named template schedule-template group-1283289401670

Select	Name	Date	Size	Type	User	Group	Permissio

If replication is enabled, you can restore from a replicated Data Domain system.

System maintenance with Data Domain

Avamar system maintenance operations include backup data that is stored on configured Data Domain systems.

Avamar system maintenance processes operate on backup data that is stored on both the Avamar server and any configured Data Domain systems.

Avamar performs the system maintenance operations for backup data on the Data Domain system. Data Domain maintenance operations may also run on the Data Domain system. However, these operations do not replace Avamar maintenance operations.

If an Avamar system maintenance operation succeeds on the Avamar server and fails on the Data Domain system, then Avamar reports the operation as completed or completed with exceptions in the log files. In addition, Avamar generates a MSG_ERR_DDR_ERROR status for the operation. The details for the failure are available in the log file for the **ddrmaint** utility.

The deletion or expiration of a backup succeeds on the Avamar server even if the deletion of a backup fails on the Data Domain system. The Garbage Collection process must remove the backup that Avamar did not successfully delete on the Data Domain system.

The following topics provide details on Avamar system maintenance processes that operate on Avamar backup data on a Data Domain system:

- "HFS check" on page 557
- "Checkpoints" on page 557
- "Rollbacks" on page 557
- "Garbage Collection" on page 557
- "Secure deletion" on page 558

HFS check

When HFS check runs on the Avamar server, it verifies backup data on both the Avamar server and the Data Domain system. However, the HFS check verifies only file existence, file size, and file modification time for data on the Data Domain system.

The Data Invulnerability Architecture (DIA) on the Data Domain system performs a more comprehensive integrity check on the Avamar data that is stored on the Data Domain system.

Checkpoints

When you perform a checkpoint on the Avamar server, then the checkpoint includes Avamar data on the Data Domain system. If a checkpoint succeeds on the Avamar server but fails for Avamar data on a Data Domain system, then the checkpoint fails. All checkpoint names on a Data Domain system match the checkpoint names on the Avamar server.

Rollbacks

When you perform a rollback on the Avamar server, then a rollback is performed on Avamar data on the Data Domain system. If a rollback succeeds on the Avamar server but fails for Avamar data on a configured Data Domain system, then the rollback fails.

Garbage Collection

When Garbage Collection runs on the Avamar server, it deletes expired Avamar backup data on both the Avamar server and the Data Domain system. Garbage Collection may perform other cleanup operations on the Data Domain system as required, such as removing deleted checkpoints and backups, and removing incomplete, aborted, and failed backups.

The Data Domain file system cleaning operation reclaims space on the Data Domain system from data that the Avamar Garbage Collection process deletes. The Avamar Garbage Collection process does not initiate the Data Domain file system cleaning operation. The file system cleaning operation typically runs automatically each Tuesday. However, you also can manually initiate file system cleaning using the Data Domain Enterprise Manager.

The following processes may need to run before the Data Domain file system cleaning operation can completely free allocated space from a deleted backup or a checkpoint:

- Two Avamar Garbage Collection operations
- Checkpoint creation
- HFS check
- Checkpoint deletion

Secure deletion

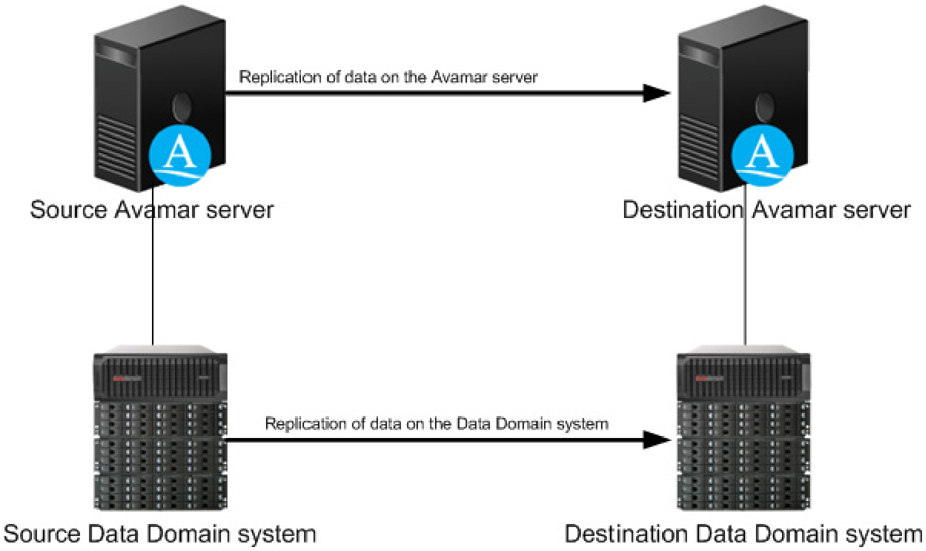
Manual secure deletion is possible on both the Avamar and Data Domain servers. There is also a data shredding feature on Data Domain systems, but data shredding is not currently supported for Avamar data on a Data Domain system. The *EMC Avamar Product Security Guide* provides details on how to securely delete backups from the Avamar server.

Replication with Data Domain

The following topics provide details on replication of Avamar data on a Data Domain system.

How replication works with Avamar and Data Domain

The Avamar replication feature transfers data from a source Avamar server to a destination Avamar server. When you use a Data Domain system with Avamar, then the replication process transfers Avamar data from the source Data Domain system to a destination Data Domain system, as shown in the following figure.


Replication of data on the Avamar server
Source Avamar server
Destination Avamar server
Replication of data on the Data Domain system
Source Data Domain system
Destination Data Domain system

If a Data Domain system is configured with a source Avamar server, then there must be a corresponding Data Domain system configured with a destination server. If there is no destination Data Domain system configured with the destination Avamar server, then replication fails for backups on the source Data Domain system.

Replication control

Avamar replicates Avamar data from the source Data Domain system to the destination Data Domain system. The Data Domain replication feature is not used. You must have a Data Domain replication license to copy data from one system to another.

You configure and monitor replication on the Avamar server. There is no way to track replication using Data Domain administration tools.

Even though Avamar does not use Data Domain replication, other products in the environment may use this feature. If you replicate an entire Data Domain system, then Data Domain replicates the Avamar data that is stored on the Data Domain system.

Do not use Data Domain replication to replicate data to another Data Domain system that is configured for use with Avamar. When you use Data Domain replication, the replicated data does not refer to the associated Avamar server.

Replication data flow

Avamar replicates the data directly from one Data Domain system to another. In other words, Avamar does not stage the data on the Avamar server before replicating the data to the destination Data Domain system.

Replication schedule

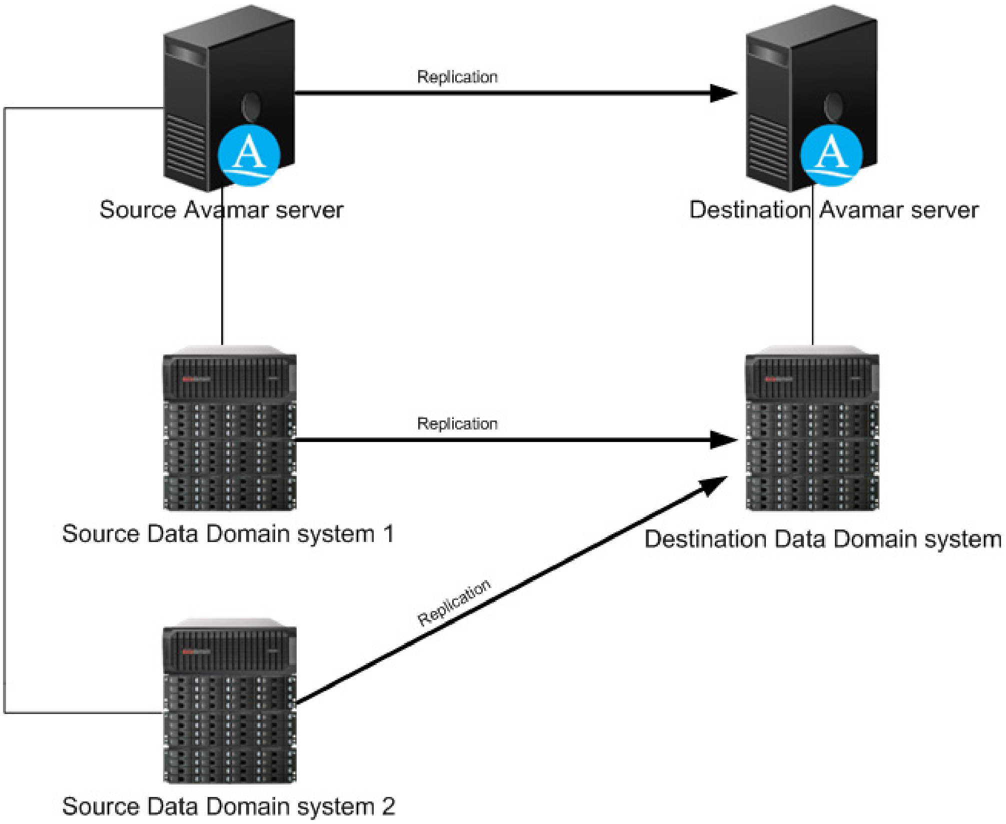
The replication of Avamar data on a Data Domain system occurs on the Avamar replication schedule. You cannot schedule replication of data on the Data Domain system separately from the replication of data on the Avamar server.

Replication environments

If the source Avamar server uses more than one Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems. Also, if the source Avamar server uses a single Data Domain system, then you can use either a single destination Data Domain system or multiple destination systems.

You can replicate from a standard Data Domain system to a Data Domain Archiver, or from a Data Domain Archiver to a standard Data Domain system. If the replication source is a Data Domain Archiver, then the replicated data can be on the active tier, an target archive tier, or a sealed archive tier.

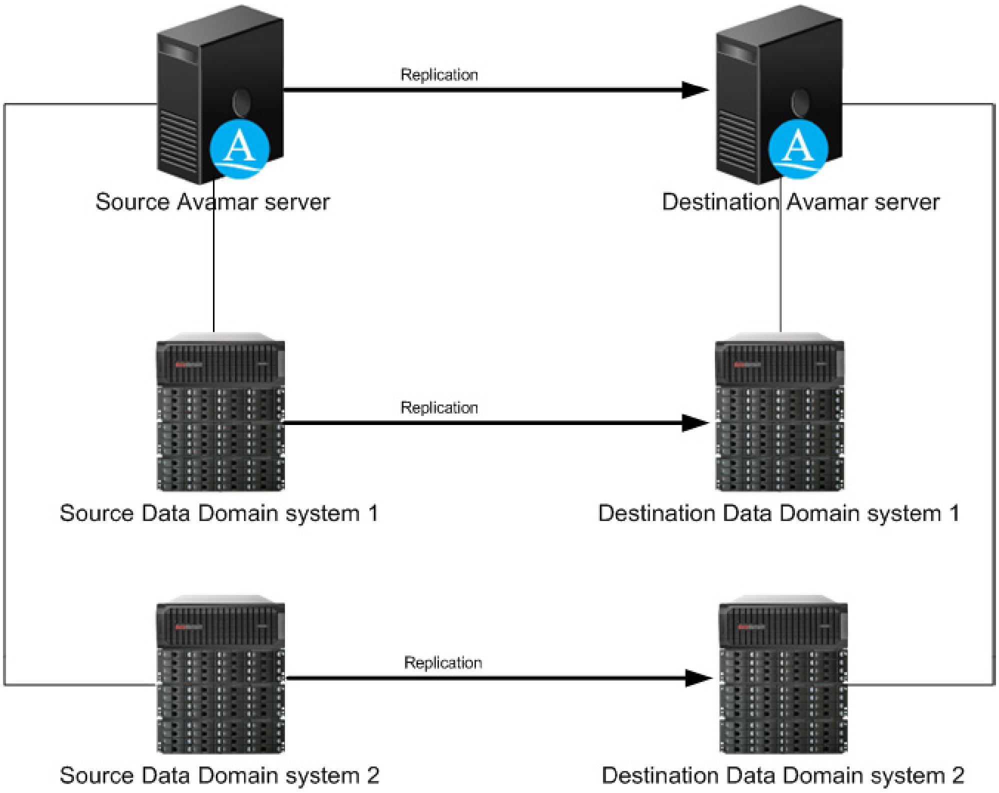
The following figure illustrates a source Avamar system that uses two Data Domain systems. Avamar replicates the backup data on the two source Data Domain systems to a single destination Data Domain system.


Replication
Source Avamar server
Destination Avamar server
Replication
Source Data Domain system 1
Destination Data Domain system
Replication
Source Data Domain system 2

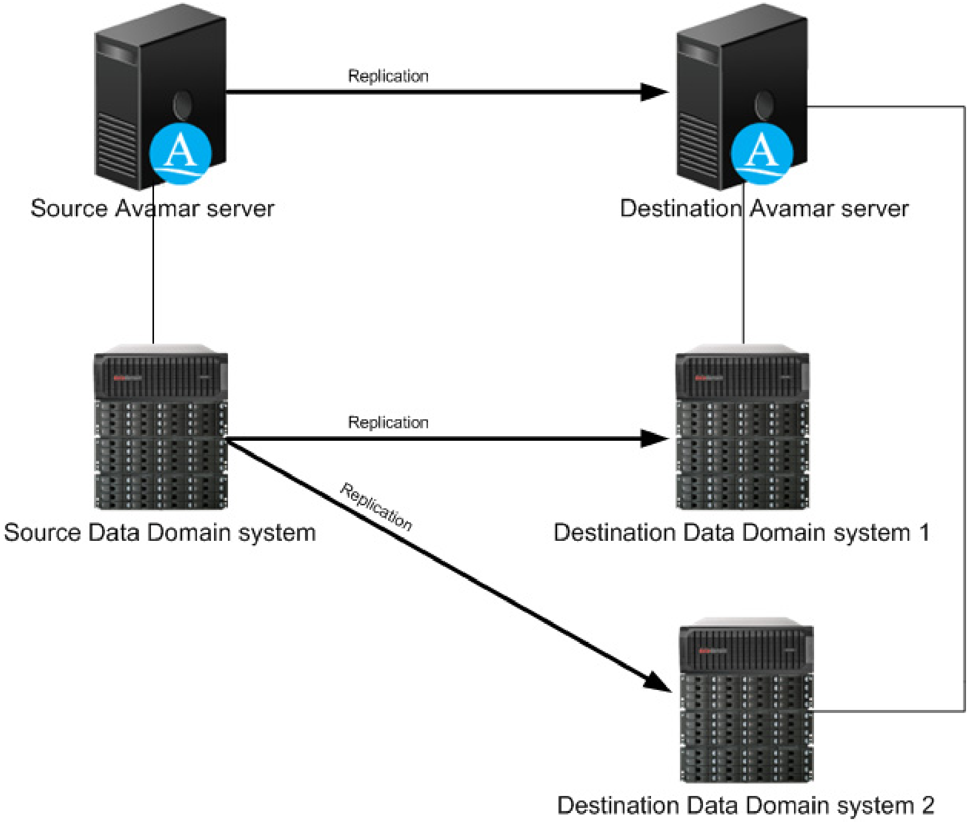
NOTICE

Ensure that the destination Data Domain system can accommodate the replicated data from both source Data Domain systems.

The following figure illustrates an environment with multiple destination Data Domain systems.


Replication
Source Avamar server
Destination Avamar server
Replication
Source Data Domain system 1
Destination Data Domain system 1
Replication
Source Data Domain system 2
Destination Data Domain system 2

The following figure illustrates an environment where Avamar replicates backup data from a single source Data Domain system to multiple destination Data Domain systems.


Replication
Source Avamar server
Destination Avamar server
Replication
Replication
Source Data Domain system
Destination Data Domain system 1
Destination Data Domain system 2

In a configuration with multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system by mapping a domain on the source Avamar server to a destination Data Domain system. "Mapping a domain to a Data Domain system" on page 563 provides details.

Configuring replication

To configure replication when you use a Data Domain system as a backup target for Avamar:

1. Configure replication from the source Avamar server to the destination Avamar server by using either Avamar Administrator or Avamar Enterprise Manager:

   - On the **Services Administration** tab in the **Administration** window of Avamar Administrator, update the properties for the **Replication cron job** entry to include information about the destination server, backups to replicate, schedule, and other replication settings.

   - On the **Replicator Setup** page in Avamar Enterprise Manager, click the link for the source Avamar server, and then specify information about the destination server, backups to replicate, schedule, and other replication settings.

   Chapter 15, "Replication," provides detailed steps to configure replication in either Avamar Administrator or Avamar Enterprise Manager.

2. If there is more than one destination Data Domain system, specify which Data Domain system is the default destination. "Setting the default Data Domain destination" on page 563 provides detailed steps.

3. If there is more than one destination Data Domain system, map the domains on the source Avamar server to a destination Data Domain system. "Mapping a domain to a Data Domain system" on page 563 provides detailed steps.

Setting the default Data Domain destination

In a replication environment with more than one destination Data Domain system, specify which Data Domain system is the default destination. The default destination is the Data Domain system to which Avamar replicates data when a destination Data Domain system is not identified on the Replication Storage Mapping tab. "Mapping a domain to a Data Domain system" on page 563 provides details on mapping a domain on a source Avamar server to a destination Data Domain system for replication.

To specify the default destination Data Domain system:

1. Open Avamar Administrator on the destination Avamar server.

2. Click the **Server** launcher button.

   The Avamar Server window appears.

3. Click the **Server Management** tab.

4. Select the destination Data Domain system.

5. Select **Actions** › **Edit Data Domain System**.

   The Edit Data Domain System dialog box appears.

6. On the **System** tab, select the **Use system as default replication storage** checkbox.

7. Click **OK**.

Mapping a domain to a Data Domain system

If there are multiple destination Data Domain systems, you can control which system receives the data that replicates from the source Data Domain system. To specify the destination Data Domain system, map a domain on the source Avamar server to a destination Data Domain system. If you do not provide a mapping, then Avamar replicates the data from the source Data Domain system to the default destination that you identified in "Setting the default Data Domain destination" on page 563.

NOTICE

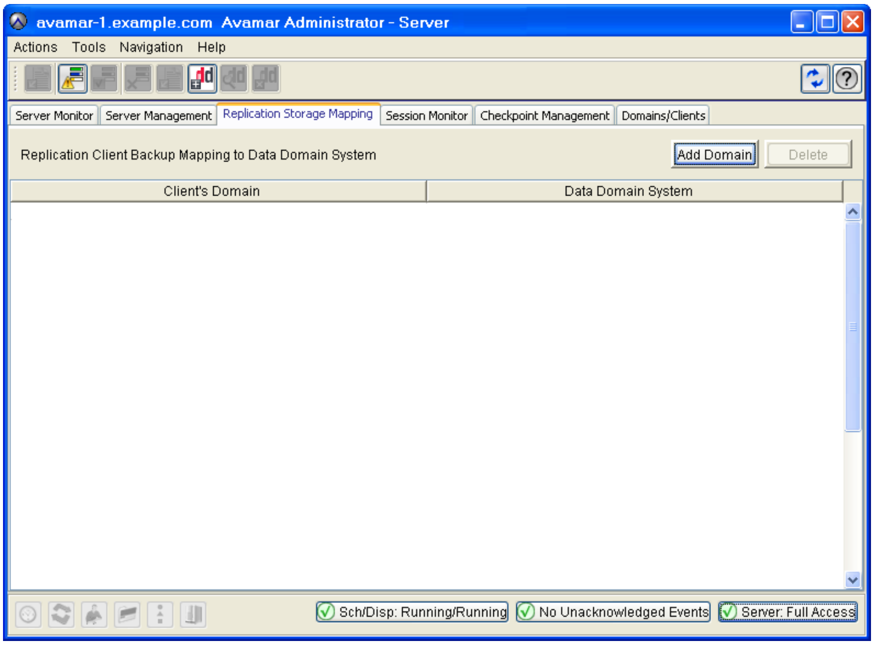
You cannot map the domains on the source Avamar server to a destination Data Domain system until after the first replication. During the first replication, the data replicates to the default destination.

To map a domain on a source Avamar server to a destination Data Domain system:

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

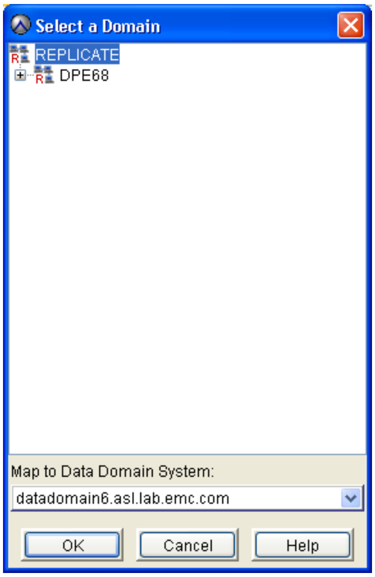
   The Avamar Server window appears.

2. Select the **Replication Storage Mapping** tab.



3. Click **Add Domain**.

   The Select a Domain dialog box appears.



Map to Data Domain System: datadomain6.asl.lab.emc.com

4. Browse to and select a domain from the tree.

5. From the **Map to Data Domain System** list, select the Data Domain system to use as the replication target.

6. Click **OK**.

Deleting a domain mapping

When you delete a domain mapping, any data that has already replicated to the destination Data Domain system remains there. However, any new data replicates to the default destination system unless you create a new mapping to a different Data Domain system.

To delete a mapping between a domain on a source Avamar server and a destination Data Domain system:

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

   The Avamar Server window appears.

2. Select the **Replication Storage Mapping** tab.
3. Select the mapping and click **Delete**.
4. Click **Yes** on the confirmation message.

Monitoring and reporting with Data Domain

The following topics provide details on how to monitor Data Domain system activity and to retrieve reports on a Data Domain system that is configured as a backup target for Avamar.

Monitoring Data Domain with SNMP

Avamar can collect and display data for health monitoring, system alerts, and capacity reporting on a Data Domain system using SNMP. To enable Avamar to collect the data, specify the port number on which to receive traps when you add the Data Domain system to the Avamar configuration, as discussed in "Adding a Data Domain system" on page 550.

Activity monitoring

You can monitor recent backup, restore, and validation activities for a Data Domain system by using the Activity Monitor in Avamar Administrator. The Server column in the Activity Monitor lists the server—either the Avamar server or the Data Domain system—on which the activity occurred. The Activity Monitor displays the most recent 5,000 client activities during the past 72 hours. You can filter the Activity Monitor to view only activities for data on a Data Domain system. "Monitoring backup, restore, or validation activities" on page 113 provides details on activity monitoring.

Server monitoring

The Server Monitor in Avamar Administrator provides CPU, disk activity, and network activity for each node on the Data Domain system. "Monitoring the server" on page 260 provides details.

Event monitoring

When you configure SNMP communication for Avamar and Data Domain, the Avamar Event Monitor displays relevant events for the Data Domain system. You can filter the events to display only those events for a Data Domain system. "Viewing system events" on page 276 provides details.

Capacity monitoring

Avamar checks the capacity of each Data Domain system every 24 hours. Avamar then logs an event in the Event Monitor if the capacity reaches 95% full, or if the forecast number of days until the capacity is full is less than or equal to 90 days.

You can also monitor the capacity of a Data Domain system using either Avamar Administrator or Enterprise Manager. In Avamar Administrator, Data Domain system capacity summary statistics are available on the Server Management tab in the Server window. The Capacity column on the Dashboard page in Avamar Enterprise Manager provides used and forecast capacity information for the Data Domain system.

You can also view the percentage of used and forecast capacity for Data Domain systems during a specific time period by selecting the Data Domain Capacity Usage Report and Data Domain Capacity Forecast Report, respectively, in the Reports list on the Avamar Enterprise Manager Reports page.

The System Status page in Avamar Enterprise Manager provides details on forecast capacity and capacity usage. "Viewing system events" on page 276 and "Capabilities and limitations" on page 312 provide details.

Replication monitoring

There are several ways to monitor replication activity in Avamar, including replication activities associated with a Data Domain system:

- The Avamar Activity Monitor in Avamar Administrator provides a list of recent replication activities. If you select a Replication Source or Replication Destination activity and select Actions › View Statistics, then you can view additional statistics about the replication, including:
  - A list of backups that were replicated
  - The clients associated with the replicated backups
  - The scheduled start and end times for the replication
  - The actual start and end times for the replication
  - A list of errors that occurred, if any
- The Replication Report in Avamar Administrator provides details on recent replication activities. You can filter the report to view only replication activities associated with a Data Domain system.
- The Replicator Status page in Avamar Enterprise Manager provides a consolidated daily replication status summary for each Avamar system that you monitor.

Reports

The Avamar Activity Report and Replication Report list the server—either the Avamar server or the Data Domain system—on which the activity occurred. This information appears in the server and ddr_hostname columns of each report.

If there are a significant number of activities in a report, you can filter the report to view only information related to a Data Domain system. When you create a custom report, you can filter the report to view information related to a Data Domain system.

"Reporting" on page 223 provides details on Avamar reports.

Troubleshooting Data Domain

The following topics provide details on how to view detailed status for and troubleshoot problems when you use a Data Domain system with Avamar:

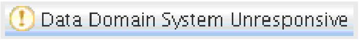
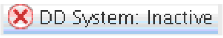
- "Viewing detailed status information for troubleshooting" on page 567
- "Data Domain status and resolutions" on page 568
- "Monitoring status details" on page 572

Additional troubleshooting details are available in the *EMC Avamar and Data Domain Integration Guide*.

Viewing detailed status information for troubleshooting

The status bar in Avamar Administrator indicates whether there is a problem either with the Avamar connection to a Data Domain system or with a Data Domain system itself, as shown in the following table.

Table 125 Status bar icons for troubleshooting Data Domain

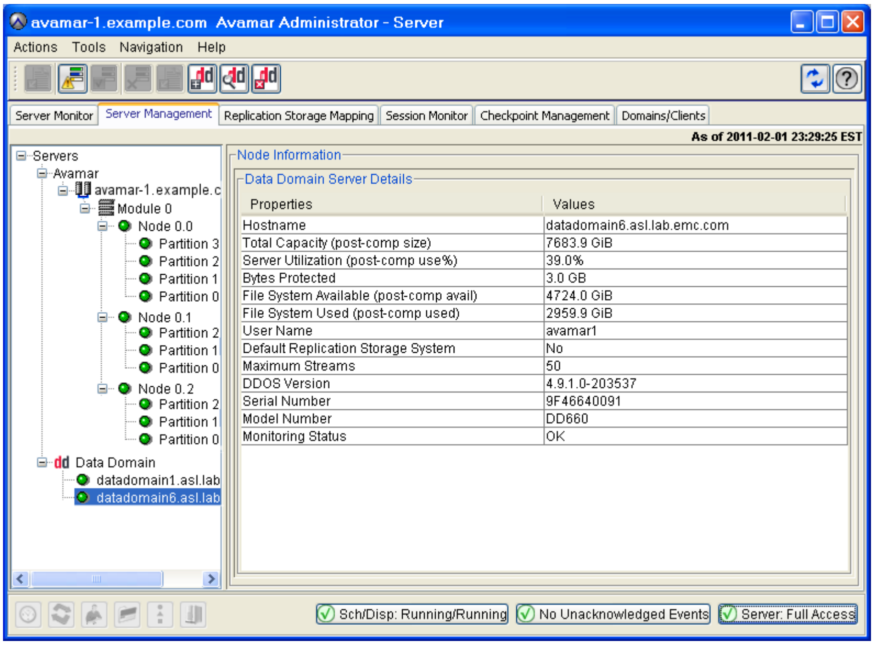
Status bar icon	Description
 ! Data Domain System Unresponsive	Avamar cannot retrieve information from a Data Domain system. However, backups and restores can continue during this condition.
 ☒ DD System: Inactive	Avamar cannot connect to a Data Domain system, or a Data Domain system is disabled in some way. Backups and restores do not occur during this condition.

You can view more detailed status information about the problem on the Server Management tab in the Server window.

To view detailed Data Domain status information:

1. In **Avamar Administrator**, select **Navigation** › **Server**.
2. Select the **Server Management** tab, and then select the Data Domain system in the tree.

   The Monitoring Status row in the right pane provides detailed status of the Data Domain system, as shown in the following figure.



Properties	Values
Hostname	datadomain6.asl.lab.emc.com
Total Capacity (post-comp size)	7683.9 GiB
Server Utilization (post-comp use%)	39.0%
Bytes Protected	3.0 GB
File System Available (post-comp avail)	4724.0 GiB
File System Used (post-comp used)	2959.9 GiB
User Name	avamar1
Default Replication Storage System	No
Maximum Streams	50
DDOS Version	4.9.1.0-203537
Serial Number	9F46640091
Model Number	DD660
Monitoring Status	OK

Data Domain status and resolutions

The following table lists the available values for the Monitoring Status row on the Server Management tab in the Server window in Avamar Administrator. If the status indicates a problem, a proposed resolution is provided.

Table 126 Monitoring Status on the Server Management tab (page 1 of 4)

Monitoring status	Resolution
OK	No resolution is required.
SNMP Getter/Setter disabled	Use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**
Unable to get CPU, disk, and network statistics data	Use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**
Unable to get CPU and disk statistics data	Use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**
Unable to get network statistics data	Use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**
Unable to get file system statistics data	Use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**

Table 126 Monitoring Status on the Server Management tab (page 2 of 4)

Monitoring status	Resolution
Error invoking ssh cli command	Review the system log files to determine the cause of the problem. You should also review the *Data Domain Command Reference Guide*, which is available through https://my.datadomain.com.
File system disabled	Use the Data Domain SSH CLI to enable Data Domain file system operations by typing: **`filesys enable`** When the Data Domain file system is disabled, Avamar cannot perform backups to and restores from the device. After you enable file system operations, it may take as many as 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is a Data Domain Archiver. 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.
Unable to get SNMP file system status	Verify that the SNMP getter/setter port is valid. This is the port that you specified when you added the Data Domain system to the Avamar configuration.
Failed to authenticate ssh cli connection with ssh key	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system. The *EMC Avamar and Data Domain Integration Guide* provides details on configuring the SSH public/private key pair.
Failed to authenticate SSH CLI connection with credentials	Verify that the DD Boost user credentials are correct. The credentials are the username and password that you specified when you added the Data Domain system to the Avamar configuration.
Unable to retrieve ssh key file pair	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system, and that the public key was copied to the correct location on the Data Domain system. The *EMC Avamar and Data Domain Integration Guide* provides details on configuring the SSH public/private key pair.
Unable to retrieve ssh public key file	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system, and that the public key was copied to the correct location on the Data Domain system. The *EMC Avamar and Data Domain Integration Guide* provides details on configuring the SSH public/private key pair.
Unable to retrieve ssh private key file	Verify that the SSH public/private key pair was set up correctly on both the Avamar server and the Data Domain system. The *EMC Avamar and Data Domain Integration Guide* provides details on configuring the SSH public/private key pair.
DDBoost disabled	EEnable DD Boost using either the Data Domain SSH CLI or the web-based Data Domain Enterprise Manager. To enable DD Boost by using the SSH CLI, type: **`ddboost enable`** When DD Boost is disabled, Avamar cannot perform backups to and restores from the device.

Table 126 Monitoring Status on the Server Management tab (page 3 of 4)

Monitoring status	Resolution
DDBoost user disabled	Use the Data Domain SSH CLI to enable the DD Boost user by typing: `user enable USERNAME` where USERNAME is the username of the DD Boost user. When the DD Boost user is disabled, Avamar cannot perform backups and restores to and from the device.
DDBoost user changed on Data Domain system	If you edited the DD Boost user account information on the Data Domain system, then you must edit the DD Boost user account information in the Data Domain configuration on the Avamar server using the instructions in "Editing a Data Domain system" on page 552. When you edit the DD Boost user account information in Avamar Administrator, the SSH key may fail. To resolve this issue, re-add the SSH key using the instructions in the *EMC Avamar and Data Domain Integration Guide*.
DDBoost option disabled	Use the Data Domain SSH CLI to enable DD Boost by typing the following command: `ddboost option set distributed-segment-processing enabled` Backups continue when DD Boost is disabled. However, performance decreases.
DDBoost option not available	No resolution is required. The Data Domain system is in a cluster, and DD Boost is not available in a cluster.
DDBoost not licensed	Use the Data Domain SSH CLI to add the license for DD Boost by typing: `license add LICENSE` where LICENSE is the license code.
Invalid SNMP port	Verify that you specified the correct getter/setter port when you added the Data Domain system to the Avamar configuration, and ensure that the getter/setter port is open on the Data Domain system by typing: `snmp show trap-hosts`

Invalid SNMP trap host or trap port	Use the Data Domain SSH CLI to verify that the Avamar server is configured as a trap host on the Data Domain system by typing:
	`snmp show trap-hosts`
	If necessary, use the Data Domain SSH CLI to add the Avamar server as a trap host on the Data Domain system by typing:
	`snmp add trap-host HOSTNAME`
	where HOSTNAME is the hostname of the Avamar server. By default, port 163 is used.
	Verify that you specified the correct trap port when you added the Data Domain system to the Avamar configuration.

Invalid SNMP community string	Use the Data Domain SSH CLI to verify the SNMP community string by typing: `snmp show ro-communities` Verify that you specified the correct SNMP community string when you added the Data Domain system to the Avamar configuration.

Table 126 Monitoring Status on the Server Management tab (page 4 of 4)

Monitoring status	Resolution
Error getting SNMP objects	Review the system log files to determine the cause of the problem. Search the Data Domain knowledgebase at https://my.datadomain.com for the error message.
Non-ost user state is Unknown	Use the **user show** commands in the Data Domain SSH CLI to verify the status of the user. The *DD OS Command Reference Guide* provides details.
Non-ost user Invalid	Use the Data Domain SSH CLI to create the user by typing: `user add USERNAME priv admin` where USERNAME is the name of the user account.
Non-ost user disabled	Use the Data Domain SSH CLI to enable the user by typing: `user enable USERNAME` where USERNAME is the name of the user account.
Non-ost user is not an admin user	Use the Data Domain SSH CLI to change the user privilege level for the user from user to admin by typing: `user change priv USERNAME admin` where USERNAME is the name of the user account.
SNMP trap manager is not running	Start the Data Domain SNMP Manager service: 1. In Avamar Administrator, click the **Administration** launcher button. The Administration window appears. 2. Click the **Services Administration** tab. 3. Right-click the **Data Domain SNMP Manager** row in the right pane and select **Start Data Domain SNMP Manager**.
Unknown Host	The DNS server cannot resolve the hostname of the Data Domain system. Ensure that the hostname and IP address for the Data Domain system are configured correctly in DNS.
Host is not reachable	Avamar cannot connect to the hostname or IP address of the Data Domain system. This may be because the device is powered off, there is a network connection issue, the connection is blocked by the firewall, and so on.
Invalid host, user name, or password	Ensure that you specified the hostname or IP address of the Data Domain system, the DD Boost username, and password. Attempt to log in to the Data Domain system with the specified username and password. Verify that the Avamar server can ping the Data Domain system.
Synchronization of maintenance operations is off	Avamar cannot synchronize maintenance operations such as checkpoints, HFS checks, and Garbage Collection with the Data Domain system. EMC Customer Service must enable synchronization of these operations by using the **avmaint config** command to set the **useddr** value to TRUE.
Unknown	Contact Data Domain Support at https://my.datadomain.com.

Monitoring status details

When the monitoring status on the Server Management tab in the Server window in Avamar Administrator is a value other than OK, then additional information appears in a list below the Monitoring Status. The following table provides details on the available values and a resolution to the issue if the status indicates a problem.

Table 127 Additional information below the Monitoring Status (page 1 of 3)

Monitoring status details	Description
• DDBoost Licensed, or • DDBoost not Licensed	DD Boost licensing status. If the value is DDBoost not licensed, then use the Data Domain SSH CLI to add the license for DD Boost by typing: `license add LICENSE` where LICENSE is the license code.
• DDBoost Enabled, or • DDBoost Disabled	DD Boost status. If the value is DDBoost Disabled, then enable DD Boost using either the Data Domain SSH CLI or the web-based Data Domain Enterprise Manager. To enable DD Boost using the SSH CLI, type: `ddboost enable` When DD Boost is disabled, Avamar cannot perform backups to and restores from the device.
• DDBoost User Enabled, or • DDBoost User Disabled	DD Boost user status. If the value is DDBoost User Disabled, then use the Data Domain SSH CLI to enable the DD Boost user by typing: `user enable USERNAME` where USERNAME is the username of the DD Boost user. When the DD Boost user is disabled, Avamar cannot perform backups to and restores from the device.
• DDBoost User Valid, or • DDBoost User Changed	DD Boost user status. If the value is DDBoost User Changed and you edited the DD Boost user account information on the Data Domain system, then you must edit the DD Boost user account information in the Data Domain configuration on the Avamar server using the instructions in "Editing a Data Domain system" on page 552. When you edit the DD Boost user account information in Avamar Administrator, the SSH key may fail. To resolve this issue, re-add the SSH key using the instructions in the *EMC Avamar and Data Domain Integration Guide*.

Table 127 Additional information below the Monitoring Status (page 2 of 3)

Monitoring status details	Description
• DDBoost Option Enabled, or • DDBoost Option Disabled, or • DDBoost Option not Available	DD Boost option status. If the value is DDBoost Option Disabled, then use the Data Domain SSH CLI to enable DD Boost by typing the following command on a single command line: **`ddboost option set distributed-segment-processing enabled`** Backups continue when DD Boost is disabled. However, performance decreases. If the value is DDBoost Option not Available, then the Data Domain system is in a cluster, and DD Boost is not available in a cluster.
• Non-ost user state is Unknown, or • Non-ost user Invalid, or • Non-ost user disabled, or • Non-ost user is not an admin user	Status of the non-OST user: • If the value is Non-ost user state is Unknown, then Use the user show commands in the Data Domain SSH CLI to verify the status of the user. The *DD OS Command Reference Guide* provides details. • If the value is Non-ost user Invalid, then use the Data Domain SSH CLI to create the user with the admin privilege level by typing: **`user add`** `USERNAME` **`priv admin`** where USERNAME is the name of the user account. • If the value is Non-ost user disabled, then use the Data Domain SSH CLI to enable the user by typing: **`user enable`** `USERNAME` where USERNAME is the name of the user account. • If the value is Non-ost user is not an admin user, then use the Data Domain SSH CLI to change the user privilege level from user to admin by typing: **`user change priv`** `USERNAME` **`admin`** where USERNAME is the name of the user account. **Note:** This row does not appear if the non-OST user has not been configured.

Table 127 Additional information below the Monitoring Status (page 3 of 3)

Monitoring status details	Description
• SNMP Enabled, or • SNMP Disabled	SNMP status. If the value is SNMP Disabled, then use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`**
• File System Running, or • File System Enabled, or • File System Disabled, or • File System Unknown, or • File system status unknown since SNMP is disabled	Status of the Data Domain file system. When the Data Domain file system is disabled, Avamar cannot perform backups to and restores from the device. If the value is File System Disabled, then use the Data Domain SSH CLI to enable Data Domain file system operations by typing: **`filesys enable`** If the value is File system status unknown since SNMP is disabled, then use the Data Domain SSH CLI to enable SNMP by typing: **`snmp enable`** If the value is File System Unknown, then verify that the SNMP getter/setter port is valid. This is the port that you specified when you added the Data Domain system to the Avamar configuration. If you enable file system operations, it may take as many as 10 minutes before Avamar Administrator correctly reflects the status of the Data Domain system, especially if the Data Domain system is a Data Domain Archiver. 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.
• Synchronization of maintenance operations is off. or • Synchronization of maintenance operations is on.	Synchronization status of maintenance operations, such as checkpoints, HFS checks, and Garbage Collection, between the Avamar server and the Data Domain system. If the value is Synchronization of maintenance operations is off, then EMC Customer Service must enable synchronization of these operations by using the **avmaint config** command to set the **useddr** value to TRUE.

CHAPTER 22
Avamar File System (AvFS)

The Avamar File System (AvFS) provides a browsable virtual filesystem view of the normally inaccessible Avamar server filesystem. It also provides read-only access at the individual file level to all backups stored on an Avamar server. The following topics provide details on the Avamar File System:

- Capabilities and limitations 576
- Security recommendations.. 576
- Installing and enabling AvFS 576
- Shutting down AvFS 577
- Configuring Samba for use with AvFS 578
- Strengthening Samba security 581

Capabilities and limitations

This topic discusses various capabilities and limitations of Avamar File System (AvFS).

Samba is supported with limitations

Samba exports of AvFS are supported. However, be advised that certain characters that are not allowed in Windows filenames are not translated properly. "Configuring Samba for use with AvFS" on page 578 provides information.

NFS mounts not supported

NFS mounting AvFS is not supported. This is primarily due to in order caching on clients and the difficulties converting a 20-byte hash into a 6-byte in order value.

Windows volume names

When you view Windows volumes, all root-level colons (:) appear as dollar signs ($). For example, volume C: becomes C$.

Data Domain Samba mounts not supported

AvFS cannot be used to implement Samba mounts of Data Domain filesystems. There is no user readable data and doing so might cause unexpected application behavior.

Security recommendations

You cannot limit file access in AvFS for a user. Any user with access to AvFS can view all files in all backups on that server. As a result, it is vitally important that you limit access to AvFS to authorized users only.

Furthermore, if you are configuring AvFS for use with Samba, you should strengthen the default Samba security by implementing one or all of the suggested security measures described in "Strengthening Samba security" on page 581.

Installing and enabling AvFS

To install and enable AvFS:

1. Use the Avamar Enterprise Manager System Maintenance page to install the Avamar File System software.

   "Server Updates and Hotfixes" on page 403 provides details.

2. Open a command shell and log in to the utility node as root.

3. Start AvFS by typing:

   ```
   service axionfs start
   ```

The following information appears in the command shell:

```
axionfs Info: Loading fuse module.
axionfs Info: Avamarfs started on /mnt/axion.[ OK ]
```

AvFS appears as /mnt/axion. It is read-only.

4. Verify that the **axionfs** service is running by typing:

   ```
   ps -ef | grep axionfs
   ```

   The following information appears in the command shell:

   ```
   root 29454 1 0 15:16 ? 00:00:00 /usr/local/avamar/bin/axionfs
   --vardir=/usr/local/avamar/var --bindir=/usr/local/avamar/bin
   --sysdir=/usr/local/avamar/etc --mountpoint=/mnt/axion
   ```

5. Verify that AvFS is being exported by typing:

   ```
   cd /mnt/axion
   ls
   ```

   A listing of the /mnt/axion directory should appear in the command shell.

6. (Optional) Enable AvFS to start automatically on reboot by typing:

   ```
   /sbin/chkconfig --add axionfs
   /sbin/chkconfig --level 345 axionfs on
   ```

Shutting down AvFS

To shut down AvFS:

1. Open a command shell and log in to the utility node as root.
2. Type:

   ```
   service axionfs stop
   ```

Configuring Samba for use with AvFS

To configure Samba for use with AvFS:

1. For Avamar utility nodes with SUSE Linux Enterprise Server (SLES), install Samba as described in "Installing Samba on utility nodes with SLES" on page 578.

   Samba is installed by default on utility nodes with Red Hat Enterprise Linux (RHEL).

2. Configure and start Samba as described in "Configuring and starting Samba" on page 579

Installing Samba on utility nodes with SLES

To configure Samba for use with AvFS on Avamar utility nodes with SLES:

1. Open a command shell and log in to the utility node as root.

2. Install the following packages in order by typing:

   ```
   cd /usr/local/avamar/src/SLES11_64
   rpm -ivh fam-2.7.0-130.21.x86_64.rpm
   rpm -ivh libiniparser0-2.17-87.17.x86_64.rpm
   rpm -ivh libnscd-32bit-2.0.2-73.18.x86_64.rpm
   rpm -ivh libtalloc1-32bit-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh libtdb1-32bit-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh libwbclient0-32bit-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh samba-32bit-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh samba-client-32bit-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh samba-client-3.4.3-1.17.2.x86_64.rpm
   rpm -ivh samba-3.4.3-1.17.2.x86_64.rpm
   ```

3. If the avfirewall hardening package is installed on the server, perform the following steps:

   a. Open /etc/firewall.base in a UNIX text editor such as vi or emacs.

   b. Locate the following entries:

   ```
   # 7. Allow DNS and NTP access from any servers
   # NOTE: add a "-s <ip address>" before the "-j" to specify which
   # DNS and NTP servers may be allowed
   $IPT -A INPUT -p udp --dport 53 -j ACCEPT
   $IPT -A INPUT -p tcp --dport 53 -j ACCEPT
   $IPT -A INPUT -p udp --dport 123 -j ACCEPT
   $IPT -A INPUT -p tcp --dport 123 -j ACCEPT
   ```

   c. Add the following line:

   ```
   $IPT -A INPUT -p tcp -m multiport --dport 139,445 -j ACCEPT
   ```

   d. Save the changes.

   e. Restart the avfirewall service by typing:

   ```
   service avfirewall restart
   ```

   The *EMC Avamar Product Security Guide* provides additional information about the avfirewall hardening package.

Configuring and starting Samba

To configure and start Samba:

1. Log in to the utility node as root.
2. Save a backup copy of the /etc/samba/smb.conf file by typing:

   ```
   cd /etc/samba/
   cp -p ./smb.conf ./smb.conf.orig
   ```

3. Grant access to the Samba mount:

   a. Open /etc/samba/smb.conf in a text editor such as vi or Emacs.

   b. Add the following entry to the [global] section of /etc/samba/smb.conf:

   ```
   hosts allow = IP-ADDRESS
   ```

   where IP-ADDRESS is the Windows machine IP address. List multiple IP addresses on the same line separated by spaces:

   ```
   hosts allow = IP-ADDRESS1 IP-ADDRESS2 IP-ADDRESS3
   ```

   c. Add following entries to the end of /etc/samba/smb.conf:

   ```
   [axionfs]
   path = /mnt/axion
   read only = yes
   browseable = no
   public = no
   ```

   d. Save the changes.

4. Create a user account that is used to access the AvFS Samba mount (/etc/passwd):

   a. Add the user account by typing:

   ```
   useradd USERNAME
   ```

   where USERNAME is the name of the account to add.

   b. Assign a Samba password for the new user account by typing:

   ```
   smbpasswd -a USERNAME
   ```

   where USERNAME is the name of the account you created

   The following information appears in the command shell:

   ```
   New SMB password:
   ```

   c. Type a password for the account and press **Enter**.

   The following information appears in the command shell:

   ```
   Retype new SMB password:
   ```

d. Retype the password and press **Enter**.

The following information appears in the command shell:

```
startsmbfilepwent_internal: file /etc/samba/smbpasswd did not
exist. File successfully created.

Added user preview.
```

5. Start AvFS by typing:

```
service axionfs start
```

The following information appears in the command shell:

```
axionfs Info: Loading fuse module.
axionfs Info: Avamarfs started on /mnt/axion.[ OK ]
```

6. Start the samba service by typing:

```
service smb start
```

The following information appears in the command shell:

```
Starting SMB services:                                   [ OK ]
Starting NMB services:                                   [ OK ]
```

7. (Optional) To enable AvFS and the Samba mount to start automatically on reboot, type:

```
/sbin/chkconfig --add axionfs
/sbin/chkconfig --level 345 axionfs on
/sbin/chkconfig --add smb
/sbin/chkconfig --level 345 smb on
```

8. Verify that the AvFS Samba mount is functioning properly by connecting to the Avamar server from Windows Explorer:

a. On a Microsoft Windows computer, open the Windows **Start** menu and select **Run**.

A command prompt appears.

b. Type:

```
\\AVAMARSERVER
```

where AVAMARSERVER is the Avamar server name as defined in corporate DNS. If there is a DNS resolution issue, type the Avamar server IP address instead.

A Connect to dialog box appears.

c. Type the username and password and click **OK**.

In Windows Explorer, a top-level axion folder shows the contents of /mnt/axion. Various subdirectories list all backups stored on the server indexed according to various attributes. For example:

- The by-date directory lists backups stored on the server indexed according to creation date.
- The by-label directory lists all backups stored on the server indexed according to label.
- The by-number directory lists backups stored on the server indexed according to numerical ID.

Strengthening Samba security

If you are configuring AvFS for use with Samba, you should strengthen the default Samba security by implementing one or all of the suggested security measures described in this topic.

All suggested security measures involve logging in to the utility node as root, opening the Samba configuration file (/etc/samba/smb.conf) in a text editor, and either adding new entries or editing entries.

"Example Samba configuration file" on page 583 provides an example listing of a fully strengthened Samba configuration file.

Require a Samba username and password

If you have not already done so, configure Samba to require that a valid Samba username and password must be provided for access.

The default smb.conf file currently installed by AvFS requires valid Samba credentials to connect to the share. Adding the null passwords setting further strengthens security.

To configure Samba to require that a valid Samba username and password are provided for access:

1. Edit the **security** global setting:

   ```
   security = user
   ```

2. Add the **null passwords** global setting:

   ```
   null passwords = no
   ```

3. Add the **encrypt passwords** global setting:

   ```
   encrypt passwords = yes
   ```

Limit access to listed hosts and networks

The hosts allow and hosts deny settings allow or deny access to only the listed networks or IP addresses, respectively.

The hosts allow setting is the method used by the default smb.conf file currently installed by AvFS.

To limit access to listed hosts and networks:

1. Add the **hosts deny** global setting:

   ```
   Hosts deny 0.0.0.0/0
   ```

2. Edit the **hosts allow** global setting:

   ```
   Hosts allow 127.0.0.1 IP-ADDRESS
   ```

   Specifying a client IP address is more secure than specifying the network that the client is a member of. The loopback or localhost IP address is required for local utilities to work. Hostnames can be used instead of IP addresses, but verify that name lookups work first.

Limit access to specific interfaces

If more than one network interface card is installed on the Avamar server, then you can configure Samba to answer requests on specific interfaces.

For example, if you have an interface connected to a private network and a client is also connected to the private network, then you can configure Samba to only answer requests from the interface connected to the private network.

To configure Samba to answer requests on specific interfaces, add the bind interfaces only and interfaces global settings:

```
bind interfaces only = yes
interfaces = lo PRIVATE-NETWORK-NAME-OR-IP-ADDRESS
```

You can use interface device names such as lo, eth0, eth1, or the IP address of an interface, for example, 127.0.0.1 for lo, or 192.168.100.33 for eth1. The loopback lo interface or IP address 127.0.0.1 is required for local utilities to work.

Limit share visibility

Another method to make the exported share more secure is to prevent uninformed users from knowing of its existence. The share does not have to be public, which enables guest access. Instead, Samba can be configured to require a specific set of user credentials to access the share.

Furthermore, you can also configure the share to not be browsable, which further hides the share name.

To limit share visibility:

1. Add the **browseable** share setting:

   ```
   browseable = no
   ```

2. Edit the **public share** setting:

   ```
   public = no
   ```

Example Samba configuration file

The following example shows a fully strengthened Samba configuration file (/etc/samba/smb.conf). Important settings discussed in previous topics are shown in bold.

```
# This is the main Samba configuration file.

   # Read the smb.conf(5) manual page for additional information
   # on the options used.
   # For a guide on installing and configuring AvFS and Samba on an
   # Avamar Server see Tech Note Avamar File System (AvFS) P/N
   # 300-009-660.
   # Any line which starts with a ; (semi-colon) or a # (hash)
   # is a comment.
   # After modifying this file run the command "testparm" to check for
   # basic syntax errors.
   # Run as root 'service smb restart' to apply the changes.

   #======================= Global Settings ====================================
   [global]
   # Workgroup = NT-Domain-Name or Workgroup-Name.
    workgroup = AXIONFS
   # Server string is the equivalent of the NT Description field.
    server string = Samba Server
   # Define in which mode Samba will operate. Select user level security.
    security = user
   # Use a separate log file for each machine that connects.
    log file = /var/log/samba/%m.log
   # Put a limit on the size of the log files (in Kb).
    max log size = 50
   # Default. Do not allow null passwords.
    null passwords = no
    encrypt passwords = yes
   # 'hosts allow' and 'hosts deny' allows restrictions on connections.
   # 'allow hosts' and 'deny hosts' are synonyms. Note that access still
   # requires suitable user-level credentials. The localhost address
   # 127.0.0.1 will always be allowed access unless specifically denied
   # by a 'hosts deny' option. Specify host names, ip, network/netmask
   # pairs, and netgroup. Use of host names is not recommended. Fully
   # test name resolution before using host names. The EXCEPT keyword
   # can be used to limit an allow list.
   # Default: hosts allow = # none (i.e., all hosts permitted access)
   # Example: allow all IPs in 192.168.*.* except one
   # hosts allow = 192.168. EXCEPT 192.168.100.66
   # Example: allow hosts that match the given network/netmask
   # hosts allow = 192.168.100.0/255.255.255.0
   # Example: allow a couple of hosts
   # hosts allow = hostname1, hostname2
   # Example: allow IPs in 192.168.100.* plus one specific host
   # hosts allow = 192.168.100. myhost.mynet.edu
   # Example: allow only hosts in NIS netgroup "somenet", but deny
   # access from one particular host
   # hosts allow = @somenet
   # hosts deny = hostname3
   # Deny everything first including loopback
    hosts deny = 0.0.0.0/0
   # Specify exactly what to allow
    hosts allow = 127.0.0.1 IP-ADDRESS
   # Only listen on the interfaces specified by 'interfaces'. By default
   # Samba queries the kernel for all active interfaces and uses
   # interfaces that are broadcast capable except 127.0.0.1 (lo).
    bind interfaces only = yes
   # Configure Samba to use specific interfaces. Each network interface
   # to be used must be listed here.
   # · A network interface name such as eth0. This may include wildcards
   # so eth* will match any interface starting with "eth".
   # · An interface IP/mask pair.
   # · An interface IP address. The netmask is determined from the list
   # of interfaces obtained from the kernel.
   # · A broadcast/mask pair.
   # The "mask" parameter can be a bit length or a full netmask in dotted
   # decimal form.
   # The "IP" parameter can be a full dotted decimal IP address or a
   # hostname. Hostnames are not recommended. Fully test name resolution
   # before using hostnames.
   # Default: interfaces =
   # Example: interfaces = eth0 192.168.100.10/24
   # Example: interfaces = 192.168.100.10/255.255.255.0 eth1
   # Specify loopback so local access continues to work. Specify
   # device name or IP of the interfaces to use.
    interfaces = lo PRIVATE-NETWORK-NAME-OR-IP-ADDRESS
   # Set local master to no so that Samba won't become a master
   # browser on a network. Otherwise the normal election rules apply.
    local master = no
   # Tell Samba whether or not to try to resolve NetBIOS names via DNS
   # nslookups.
    dns proxy = no

   #============================ Share Definitions =============================

   # This is the share defined for the default AvFS mountpoint.
   # Edit the 'hosts allow' and 'interfaces' entries above to enable and control
   access.
   [axionfs]
    path = /mnt/axion
   # Default. Inverted synonym is writeable = no or writable = no.
    read only = yes
   # Do not list shares. Share names must be known for access. (browsable is a
   synonym)
    browseable = no
   # Default. Password is required to connect (guest ok is a synonym for public)
    public = no
```

APPENDIX A
Command Shell Server Logins

The following topics describe the command shell server logins:

- User accounts 586
- Starting command shell sessions.. 586
- Switching user IDs.. 586
- Using sudo... 587

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 590
- Backup options 590
- Restore options 592

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 128 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.
Logging	

Table 128 Backup plug-in options (page 2 of 3)

Option	Description
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 filesystem 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 filesystem 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 filesystem 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.
Client Cache Options	

Table 128 Backup plug-in options (page 3 of 3)

Option	Description
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 = 0.772.
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 129 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.
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.

Table 129 Restore plug-in options (page 2 of 2)

Option	Description
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 596
- MCS database views 596
- EMS database views 638

Data types

Each column in a database view stores one of the data types listed in the following table.

Table 130 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 599. Official support for this database view is likely to be discontinued in a future release.

Table 131 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 131 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 131 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 131 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 629.

Table 132 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 132 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 132 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 132 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 133 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 134 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 134 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 134 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 135 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 136 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 608. All official support for this database view is likely to be discontinued in a future release.

Table 137 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 607.
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 137 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 138 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 609.
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 138 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 139 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 140 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 141 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 142 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 143 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 144 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 145 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 146 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 147 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 148 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 149 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 150 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 150 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 150 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 151 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 152 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 153 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 154 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 155 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 156 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 157 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 158 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 159 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 160 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 161 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 162 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 163 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 164 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 165 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 165 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 166 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 167 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 168 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 169 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 170 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 171 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 171 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 for each plug-in.

Table 172 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	
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	
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
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 173 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 174 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 175 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 176 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 176 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.
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.
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

Table 176 MCS database v_repl_activities view (page 3 of 3)

Column	Type	Description
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 177 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.
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.

Table 177 MCS database v_repl_backups view (page 2 of 2)

Column	Type	Description
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 178 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 179 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 180 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 180 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 181 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 181 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 636. Official support for this database view is likely to be discontinued in a future release.

Table 182 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 182 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 183 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 183 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 184 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 185 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 185 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 186 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 187 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 642).

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 as opposed to merely being 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 a new feature. This feature is called System Maintenance.

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 filesystems. Although more efficient than a conventional incremental backup, a backup is always a full, just 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 filesystem.

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 filesystems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

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 MCSs.

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 Filesystem. The content addressed storage area inside the Avamar server used to store client backups.

HFS check An Avamar Hash Filesystem 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 Filesystem.

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. When the EMC Subscribenet team adds packages to the EMC repository, it then adds an entry to the manifest file that describes the package. When EMC Subscribenet team removes the package from the repository, it then removes the entry for the package from the manifest file.

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 Filesystem.

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 642).

replication Replication is an optional feature that enables one Avamar server to store a read-only copy of its data on another Avamar server to support future disaster recovery of that server.

restore File or object restore. An operation that retrieves one or more filesystems, directories, files, or data objects from a backup and writes the data to a designated location.

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.