Service Assurance Suite

Version 9.5

SolutionPack Articles

302-003-624

REV 02

EMC²

Copyright © 2015-2017 Dell Inc. or its subsidiaries All rights reserved.

Published December 2017

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

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

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

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

CONTENTS

Figures 19

Tables 21

Part 1 SolutionPacks for Use with Smarts Domain Managers 23

Chapter 1 How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts 25

Overview 26
- Resource allocation for SAM and EMC M&R 26
- Port configuration between SAM and the SolutionPack for EMC Smarts 26

Workflow for setting up SAM 27
- Command syntax for registering the SAM Notification Cache service 28
- Server tool limitations in the EMC M&R User Interface 29
- Change the Smarts EDAA Tomcat port when it conflicts with the Web Console Tomcat port 30

Workflow for setting up EMC M&R 31
- User management for SolutionPack for EMC Smarts 32
- Set default navigation style 34
- Hide unused entries in the navigation tree 34
- Viewing notifications from the EMC M&R User Interface 34
- Troubleshooting an empty notification list 35
- Troubleshooting notification list errors 35
- Troubleshooting Notification view popouts 35
- Customizing the tools that are available in the Notification view 35
- Creating client tools 36
- Invoking Perl scripts with client tools in Notification views 37
- Editing client tools in SmartsTools.json 38
- Enrich device location data in Smarts geographical maps 39

SSL setup for SAM and EMC M&R 41
- Linux SSL Setup 42
- Enable SSL port and protocol settings in SolutionPack for EMC Smarts 42
- Linux: Generate the keystore file for EMC M&R 43
- Linux: Editing the EMC M&R server.xml file 44
- Configuring SAM environment variables to support SSL 44
- Linux: Generating the SAM Tomcat server keystore file and certificate 45
- Linux: Editing the SAM server.xml file 46
- Linux: Creating the trust relationship between SAM and EMC M&R 46
- Windows SSL Setup 48
- Enable SSL port and protocol settings in SolutionPack for EMC Smarts 48
- Windows: Generate the keystore file for EMC M&R 49
- Windows: Editing the EMC M&R server.xml file 50

Configuring SAM environment variables to support SSL..... 50
Windows: Generating the SAM Tomcat server keystore file and certificate..... 51
Windows: Editing the SAM server.xml file..... 52
Windows: Creating the trust relationship between SAM and EMC M&R.....52
Configuring Smarts SolutionPack in HTTP mode.....54

Chapter 2 SolutionPack for EMC Smarts 3.0 Summary Sheet 57
Overview..... 58
Technical specifications..... 58
Where to find the latest SolutionPack software..... 59
Configuring Elastic Search..... 59
Installation steps..... 61
Installing the SolutionPack for EMC Smarts.....61
Post-installation steps..... 67
Database types for storing event data..... 67
Enabling event reporting for MySQL database in Smarts SolutionPack.....67
Enabling event reporting for Elastic Search database in Smarts SolutionPack..... 68
Configure icStats helper for EMC Smarts health collection.....69
Set role restrictions for non-administrator users of SolutionPack for Smarts.....69
Confirming report creation..... 69
Set default navigation style..... 70
Hide unused entries in the navigation tree..... 70
Migrating Smarts SolutionPack from Datastore to Elastic Search.....71
Scheduling the Event-Processing Tasks..... 72
Troubleshooting 72
What to do if data does not appear in any reports..... 73
What to do if data does not appear in some reports.....73
Generating and downloading diagnostic files..... 74
Viewing collector errors in the Collector-Manager log files.....74
Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation... 75

Chapter 3 Troubleshooting the Deployment of SAM, EMC M&R and the SolutionPack for EMC Smarts 77
Overview..... 78
Log files.....78
Status checks on services..... 79
Checking elasticsearch..... 79
Checking the notifications exchange.....80
Checking the RabbitMQ configuration.....80
Checking Tomcat..... 81
Checking Alerts EDAA.....81
Checking Smarts EDAA.....81
Unable to access Smarts EDAA..... 82
Notification cache is empty..... 82
Stale alerts and messages appear in Notification cache.....84
Stopping the SAM publisher to clear the Notification cache.....84
Stopping SAM to clear the Notification cache.....84
Troubleshooting notification list errors.....85

Troubleshooting an empty notification list....85
Troubleshooting Notification view popouts.... 85
RabbitMQ does not start....85
Tomcat does not start.... 86
Tomcat starts but then stops.... 86
Changing the password of the EDAA account.... 86
How do I change the RabbitMQ passwords.... 87
Changing the RabbitMQ admin password.... 87
Changing the RabbitMQ publisher password.... 88
Changing the RabbitMQ ingestion password.... 89
UI cannot display alerts or Smarts topology when CAS is enabled....90
Wrong CAS host name in runcmd_env.sh.... 90
Services remain registered and running after an uninstall.... 91
Stopping services on Linux....91
Stopping services on Windows.... 92
Retrieving the current elasticsearch PID 93
Multi-sort option not working after clicking on Notification column title.... 93
Ports that must be open between SAM and EMC M&R.... 93

Chapter 4 How to Maintain IP Manager Settings 95
Overview....96
Requirements.... 97
Workflow for maintaining IP Manager settings....98
Adding an IP Manager to Configuration Manager....100
Disabling an IP Manager from Configuration Manager control.... 100
Modifying IP settings while Configuration Manager transfer is delayed....101
Removing an IP Manager from Configuration Manager control.... 101
Configuring settings for a selected group.... 102
Configuring matching criteria for a selected group.... 102
Configuring target domains for a selected group.... 103
Adding a description for a selected group.... 104
Configuring device access for a selected group.... 104
Configuring unique identifier tags for a selected group....105
Configuring discovery settings....105
Configuring discovery filters.... 106
Adding a new group.... 106
Deleting a group....107
Changing the priority of the groups....107
Copying the configuration of a group....108
Displaying IP Manager groups....108
Displaying IP Manager attributes.... 108
Configuring EDAA mode for 9.2 and 9.1 IP Managers....109
Automatically loading settings from a running IP Manager into the Configuration Manager....110
Other modifications to sm_settings.pl output....111
sm_service install commands for Linux....112
sm_service install commands for Windows....113

Chapter 5 How to Set Up the EMC Smarts Server Manager for Citrix XenServer 117
How to Set Up the EMC Smarts Server Manager for Citrix XenServer....118
Specify XenServer information....118
Verify that XenServer credentials are accepted in the log file....119

How to Update the XenServer Credentials for the Server Manager Configuration 120

Chapter 6 How to Set Up the EMC Smarts Server Manager for Software-Defined Networks Feature 121
How to Set Up the EMC Smarts Server Manager for Software-Defined Networks (SDN) Feature..... 122
Specify NSX Manager information..... 122
Verify that NSX credentials are accepted in the log file..... 123
How to Update the NSX Manager Administrator Credentials for the Server Manager Configuration 124

Chapter 7 SolutionPack for EMC Network Configuration Manager 3.0 Summary Sheet 125
Overview.....126
Technical specifications..... 126
Where to find the latest SolutionPack software..... 127
Configuring NCM SP with Elastic Search.....127
Installing the SolutionPack for EMC Network Configuration Manager 129
Post-installation steps.....132
Setting the IP address of the EMC M&R server.....132
Setting the collector heap memory size in the EMC M&R UI..... 133
Vstatus Configuration 134
Configuring Certificate Monitoring reports with NCM server running 9.5.....136
Configuring Certificate Monitoring reports with NCM server running 9.5 - Third-party certificate installed.....137
Configuring access to Change Detail Reports..... 138
Confirming report creation.....139
Upgrading NCM SolutionPack from 6.7u1 to 6.8u2 139
Installing the event block 140
Troubleshooting 140
Troubleshooting Change Detail Report certificate errors in Chrome.. 140
Troubleshooting Change Detail Report certificate errors in Firefox... 141
Troubleshooting Change Detail Report certificate errors in Internet Explorer..... 141
What to do if data does not appear in any reports.....142
What to do if data does not appear in some reports..... 142
Viewing collector errors in the Collector-Manager log files..... 143
Troubleshooting a broken connection between NCM and EMC M&R 143

Chapter 8 SolutionPack for Optical Wavelength Services Summary Sheet 145
Overview.....146
Technical specifications..... 146
Where to find the latest SolutionPack software.....146
Installing a SolutionPack.....147

Chapter 9 Excluding Planned Maintenance Periods from Reports 149

Planned maintenance periods....150
Creating a maintenance period....150
Associating a maintenance period with a report....151
Installing Maintenance Manager.... 151

Part 2 SolutionPacks for Mobile Devices 155

Chapter 10 SolutionPack for Ericsson eNodeB Summary Sheet 157
Overview....158
Technical specifications.... 158
Where to find the latest SolutionPack software....158
Performing prerequisite installation tasks.... 158
Installing a SolutionPack.... 159
Performing post installation tasks....160
Confirming report creation....160

Chapter 11 SolutionPack for Ericsson IMS CSCF Summary Sheet 161
Overview....162
Technical specifications.... 162
Where to find the latest SolutionPack software....163
Collecting performance parameters.... 163
Node, performance category, default file name pattern and 3GPP format.... 164
Configuring the user process limits for a Linux installation....164
Installing a SolutionPack.... 165
Confirming report creation....166
Troubleshooting.... 166
What to do if data does not appear in any reports....166
What to do if data does not appear in some reports.... 167
Viewing collector errors in the Collector-Manager log files.... 167

Chapter 12 SolutionPack for Ericsson IMS HSS SLF Summary Sheet 169
Overview....170
Technical specifications.... 170
Where to find the latest SolutionPack software....171
Collecting performance parameters....171
Node, performance category, default file name pattern and 3GPP format.... 172
Configuring the user process limits for a Linux installation.... 172
Installing a SolutionPack....173
Confirming report creation....174
Troubleshooting 174
What to do if data does not appear in any reports.... 174
What to do if data does not appear in some reports.... 175
Viewing collector errors in the Collector-Manager log files.... 175

Chapter 13 SolutionPack for Ericsson IMS IPWorks Summary Sheet 177
Overview....178
Technical Specifications....178
Where to find the latest SolutionPack software.... 179
Collecting performance parameters.... 179

Node, performance category, default file name pattern and 3GPP format 179
Configuring the user process limits for a Linux installation.....180
Installing a SolutionPack..... 181
Confirming report creation..... 181
Troubleshooting..... 182
What to do if data does not appear in any reports.....182
What to do if data does not appear in some reports..... 182
Viewing collector errors in the Collector-Manager log files..... 183

Chapter 14 SolutionPack for Ericsson IMS MRFP Summary Sheet 185
Overview.....186
Technical specifications..... 186
Where to find the latest SolutionPack software..... 187
Collecting performance parameters..... 187
Node, performance category, default file name pattern and 3GPP format 187
Configuring the user process limits for a Linux installation.....188
Installing a SolutionPack..... 188
Confirming report creation.....189
Troubleshooting..... 189
What to do if data does not appear in any reports.....190
What to do if data does not appear in some reports.....190
Viewing collector errors in the Collector-Manager log files.....191

Chapter 15 SolutionPack for Ericsson IMS MTAS Summary Sheet 193
Overview.....194
Technical specifications..... 194
Where to find the latest SolutionPack software.....195
Collecting performance parameters..... 195
Node, performance category, default file name pattern and 3GPP format.... 196
Configuring the user process limits for a Linux installation..... 197
Installing a SolutionPack..... 198
Confirming report creation.....198
Troubleshooting 199
What to do if data does not appear in any reports.....199
What to do if data does not appear in some reports..... 199
Viewing collector errors in the Collector-Manager log files.....200

Chapter 16 SolutionPack for Ericsson IMS SOI Summary Sheet 201
Overview..... 202
Technical specifications..... 202
Where to find the latest SolutionPack software..... 202
Collecting performance parameters..... 203
Node, performance category, default file name pattern and 3GPP format.... 203
Configuring the user process limits for a Linux installation..... 204
Installing a SolutionPack.....204
Confirming report creation.....205
Troubleshooting..... 205
What to do if data does not appear in any reports..... 206
What to do if data does not appear in some reports..... 206
Viewing collector errors in the Collector-Manager log files.....207

Chapter 17 SolutionPack for Ericsson IMS TSP Summary Sheet 209
Overview....210
Technical specifications....210
Where to find the latest SolutionPack software....210
Collecting performance parameters....210
Node, performance category, default tile name pattern and 3GPP format 211
Configuring the user process limits for a Linux installation....212
Installing a SolutionPack....213
Confirming report creation....214
Troubleshooting....214
What to do if data does not appear in any reports....214
What to do if data does not appear in some reports....215
Viewing collector errors in the Collector-Manager log files....215

Chapter 18 SolutionPack for Ericsson MGW Summary Sheet 217
Overview....218
Technical specifications....218
Where to find the latest SolutionPack software....218
Performing prerequisite installation tasks....219
Installing a SolutionPack....219
Performing post installation tasks....220
Confirming report creation....220
Troubleshooting....220
What to do if data does not appear in any reports....221
What to do if data does not appear in some reports....221
Viewing collector errors in the Collector-Manager log files....222

Chapter 19 SolutionPack for Ericsson RNC Summary Sheet 223
Overview....224
Technical specifications....224
Where to find the latest SolutionPack software....225
Performing prerequisite installation tasks....226
Installing a SolutionPack....226
Performing post installation tasks....227
Confirming report creation....227
Troubleshooting....228
What to do if data does not appear in any reports....228
What to do if data does not appear in some reports....228
Viewing collector errors in the Collector-Manager log files....229

Chapter 20 SolutionPack for Ericsson SGSN Summary Sheet 231
Overview....232
Technical specifications....232
Where to find the latest SolutionPack software....233
Performing prerequisite installation tasks....233
Installing a SolutionPack....234
Performing post installation tasks....234
Confirming report creation....235
Troubleshooting....235
What to do if data does not appear in any reports....235
What to do if data does not appear in some reports....236
Viewing collector errors in the Collector-Manager log files....236

Chapter 21 SolutionPack for Huawei iManager M2000 Summary Sheet 239
Overview....240
Technical specifications....240
Where to find the latest SolutionPack software....241
Performing prerequisite installation tasks....241
Determining the format of the performance data....241
Installing a SolutionPack....242
Performing post installation tasks....243
Setting up sectorized cell views on geo maps....243
Confirming report creation....244
Alerts....245
Adding new metrics in the collector....248
Troubleshooting....251
What to do if data does not appear in any topology reports....251
What to do if data does not appear in some topology reports....252
Viewing collector errors in the Collector-Manager log files....252

Chapter 22 SolutionPack for ip.access nano3G Small Cell Summary Sheet 253
Overview....254
Technical specifications....254
Where to find the latest SolutionPack software....254
Performing prerequisite installation tasks....255
Installing a SolutionPack....255
Performing post installation tasks....256
Confirming report creation....256
Enriching data in access point cells....256
Troubleshooting....257
What to do if data does not appear in any reports....258
What to do if data does not appear in some reports....258
Viewing collector errors in the Collector-Manager log files....259

Part 3 SolutionPacks for Infrastructure 261

Chapter 23 SolutionPack for Acme Packet SBC Summary Sheet 263
Overview....264
Support....264
License management....264
Installation....264
Logging in to Centralized Management....265
Installing the SolutionPack....265
Adding devices for monitoring....266
Log files....266
Configuring the user process limits for the Linux installation....266
Uninstalling a SolutionPack....267
Viewing SolutionPack reports....267
SolutionPack for Acme Packet SBC Reports....268
Report metrics....269
SSL certificates....271
SSL certificate error examples....271
Troubleshooting an SSL certificate error: Accepting the exception... 272

Installing a self-signed SSL certificate from an Internet Explorer browser....272
Importing an SSL certificate into your truststore....273
Exporting an SSL certificate from an Internet Explorer browser..274

Chapter 24 SolutionPack for Alcatel-Lucent 5620 SAM Summary Sheet 275
Overview....276
Technical specifications....276
Where to find the latest SolutionPack software....277
Performing prerequisite installation tasks....277
Installing the SolutionPack for Alcatel-Lucent 5620 SAM....277
Performing post installation tasks....278
Add the Alcatel SAM5620 configuration details....278
Confirming report creation....279
Troubleshooting....279
What to do if data does not appear in any reports....279
What to do if data does not appear in some reports....280
What to do if the Collector-Manager does not start....280

Chapter 25 SolutionPack for Aruba Wi-Fi Summary Sheet 283
Overview....284
Technical specifications....284
Where to find the latest SolutionPack software....285
Installing a SolutionPack....285
Confirming report creation....286
Troubleshooting....286
What to do if data does not appear in any reports....286
What to do if data does not appear in some reports....287
Viewing collector errors in the Collector-Manager log files....288

Chapter 26 SolutionPack for Avaya Aura Summary Sheet 289
Overview....290
Support....290
Set up Avaya CDR and RTCP....291
Enabling Call Detail Records (CDR)....291
Adding node names for CDR monitoring....291
Adding IP CDR Service for CDR Monitoring....292
Setting CDR System Parameters for CDR Monitoring....293
Enabling Intra-switch CDRs....294
Enabling trunk groups for CDR monitoring....295
CDR monitoring for 10 Digit Plus dial plans....295
Configuring RTCP Monitoring....298
License management....300
Installation....300
Logging in to Centralized Management....300
Installing the SolutionPack....301
Starting the CDR and RTCP Listeners....302
Log files....304
Configuring the user process limits for the Linux installation....304
Uninstalling a SolutionPack....305
Viewing SolutionPack reports....305
Avaya Reports....305
Metrics for Avaya VoIP....306
SSL certificates....311

SSL certificate error examples..... 312
Troubleshooting an SSL certificate error: Accepting the exception... 312
Installing a self-signed SSL certificate from an Internet Explorer browser..... 312
Importing an SSL certificate into your truststore..... 313
Exporting an SSL certificate from an Internet Explorer browser.. 314

Chapter 27 SolutionPack for Blue Coat PacketShaper Summary Sheet 317
Overview.....318
Technical specifications..... 318
Where to find the latest SolutionPack software.....318
Installing a SolutionPack..... 319
Configuring SNMP device discovery.....319
Confirming report creation..... 320
Troubleshooting 321
What to do if data does not appear in any reports.....321
What to do if data does not appear in some reports..... 321
Viewing collector errors in the Collector-Manager log files.....322

Chapter 28 SolutionPack for BGP Summary Sheet 323
Overview..... 324
Technical specifications.....324
Where to find the latest SolutionPack software..... 325
Installing a SolutionPack.....325
Configuring SNMP device discovery..... 326
Confirming report creation..... 327

Chapter 29 SolutionPack for Check Point Firewall Summary Sheet 329
Overview..... 330
Technical specifications..... 330
Where to find the latest SolutionPack software.....331
Installing a SolutionPack..... 331
Configuring SNMP device discovery..... 332
Confirming report creation..... 333
Troubleshooting 333
What to do if data does not appear in any reports..... 333
What to do if data does not appear in some reports.....334
Viewing collector errors in the Collector-Manager log files.....335

Chapter 30 SolutionPack for Cisco Firewall Summary Sheet 337
Overview..... 338
Technical specifications.....338
Where to find the latest SolutionPack software..... 339
Installing a SolutionPack.....339
Configuring SNMP device discovery..... 340
Confirming report creation.....341
Troubleshooting 341
What to do if data does not appear in any reports.....341
What to do if data does not appear in some reports.....342
Viewing collector errors in the Collector-Manager log files.....343

Chapter 31 SolutionPack for Cisco IP-SLA Summary Sheet 345
Overview.... 346
Technical specifications....346
Where to find the latest SolutionPack software.... 347
Prerequisite.... 347
Installing the SolutionPack.... 348
Polling groups definitions....349
Configuring probes on Cisco devices....350
Guidelines to setting up probes polled via statistics tables.... 351
Guidelines to setting up probes polled via history operation table.... 352
About probe creation and management.... 352
Confirming report creation.... 352
Troubleshooting.... 353
What to do if some probes are missing from the inventory reports in the Cisco IPSLA: High Frequency Polling section.... 353
What to do if no data is collected.... 353
What to do if no data appears for Jitter probes; Inventory data is displayed correctly and is up to date....353
What do when the information is not always up to date in the Probes Inventory.... 353
Probes performance data is erratic....354
Collector does not start after configuration files were edited....354
SSL certificates....354
SSL certificate error examples.... 355
Troubleshooting an SSL certificate error: Accepting the exception... 355
Installing a self-signed SSL certificate from an Internet Explorer browser.... 355
Importing an SSL certificate into your truststore.... 356
Exporting an SSL certificate from an Internet Explorer browser..357

Chapter 32 SolutionPack for Cisco Unified Communications Manager 3.0 Summary Sheet 359
Overview....360
Technical specifications.... 360
Where to find the latest SolutionPack software.... 362
Performing prerequisite configurations 362
Install Cygwin (Windows servers)....362
Create CDR directory on the EMC M&R collector 362
Configure CUCM access to CDR directory....363
Perform additional prerequisite configurations.... 364
Configuring CUCM SP with Elastic Search....364
Installing a SolutionPack....366
Performing post-installation configuration tasks.... 366
Configure the user process limits for a Linux installation.... 367
Add the gateway and call manager details.... 367
Upgrading SolutionPack for CUCM components....368
Migrating CUCM SolutionPack from Datastore to Elastic Search.... 371
Configuring SNMP device discovery....373
Import devices from Smarts.... 374
Confirming report creation.... 375
Troubleshooting 375
What to do if data does not appear in any reports.... 375

What to do if data does not appear in some reports.....376
Viewing collector errors in the Collector-Manager log files.....376
Accessing event-processing log files..... 377
Enable the Event Spy for debugging log file errors..... 377
SSL certificates..... 377
SSL certificate error examples.....378
Troubleshooting an SSL certificate error: Accepting the exception... 378
Installing a self-signed SSL certificate from an Internet Explorer browser..... 379
Importing an SSL certificate into your truststore.....379
Exporting an SSL certificate from an Internet Explorer browser..380

Chapter 33 SolutionPack for Cisco UCS 4.0 Summary Sheet 383
Overview..... 384
Technical specifications.....384
Configuring the UCS Manager.....384
Installing the SolutionPack..... 385
Importing the new database schema..... 386

Chapter 34 SolutionPack for Cisco Wi-Fi Summary Sheet 389
Overview.....390
Technical specifications..... 390
Where to find the latest SolutionPack software.....391
Installing the SolutionPack.....391
Confirming report creation..... 392
Troubleshooting 392
What to do if data does not appear in any reports..... 392
What to do if data does not appear in some reports..... 393
Viewing collector errors in the Collector-Manager log files.....394

Chapter 35 SolutionPack for Juniper Firewall Summary Sheet 395
Overview.....396
Technical specifications..... 396
Where to find the latest SolutionPack software..... 397
Installing a SolutionPack.....397
Configuring SNMP device discovery..... 398
Confirming report creation..... 399
Troubleshooting 399
What to do if data does not appear in any reports..... 400
What to do if data does not appear in some reports..... 400
Viewing collector errors in the Collector-Manager log files..... 401

Chapter 36 SolutionPack for Juniper QoS Summary Sheet 403
Overview..... 404
Technical specifications..... 404
Where to find the latest SolutionPack software..... 405
Installing a SolutionPack.....405
Configuring SNMP device discovery..... 406
Confirming report creation..... 407
Troubleshooting 407
What to do if data does not appear in any reports..... 407
What to do if data does not appear in some reports..... 408

Viewing collector errors in the Collector-Manager log files.....408

Chapter 37 SolutionPack for Juniper RPM Summary Sheet 411
Overview.....412
Technical specifications.....412
Where to find the latest SolutionPack software.....412
Installing a SolutionPack.....413
Configuring SNMP device discovery.....413
Confirming report creation.....414
Troubleshooting.....415
What to do if data does not appear in any reports.....415
What to do if data does not appear in some reports.....415
Viewing collector errors in the Collector-Manager log files.....416

Chapter 38 SolutionPack for Microsoft Hyper-V 1.3.5 Summary Sheet 417
Overview.....418
Technical specifications.....418
Configuring credentials for SolutionPack for Microsoft Hyper-V.....419
Requirements for data collection.....419
Installing the SolutionPack.....419
Using a test script to query WMI objects.....420
Configuring the UCS Manager.....421

Chapter 39 SolutionPack for Microsoft SCOM Summary Sheet 423
Overview.....424
Technical specifications.....424
Where to find the latest SolutionPack software.....425
Installing the SolutionPack.....425
Confirming report creation.....426
Troubleshooting.....426
What to do if data does not appear in any reports.....427
What to do if data does not appear in some reports.....427
What to do when raw data continues to appear on reports.....428
Viewing collector errors in the Collector-Manager log files.....428

Chapter 40 SolutionPack for Microsoft SQL Server 4.0 Summary Sheet 429
Overview.....430
Technical Specifications.....430
Where to find the latest SolutionPack software.....431
User privilege requirements for SolutionPack for Microsoft SQL.....431
Configuring the SolutionPack with an unprivileged account.....432
Installing the SolutionPack for Microsoft SQL.....433
Limitations for Microsoft SQL Server.....434
Troubleshooting.....434
What to do if data does not appear in reports.....435
Running a scheduled task to import data into reports.....435
Viewing collector errors in the Collector-Manager log files.....436

Chapter 41 SolutionPack for MPLS Summary Sheet 437
Overview.....438
Technical specifications.....438
Where to find the latest SolutionPack software.....439

Installing a SolutionPack....439
Configuring SNMP device discovery.... 440
Confirming report creation....441

Chapter 42 SolutionPack for OpenStack Summary Sheet 443
Overview.... 444
Technical Specification....444
Where to find the latest SolutionPack software.... 445
Installing a SolutionPack....445
Performing post-installation configuration tasks.... 446
Add the OpenStack server details....446
SSL certificates....446
SSL certificate error examples....447
Troubleshooting an SSL certificate error: Accepting the exception... 447
Installing a self-signed SSL certificate from an Internet Explorer browser.... 448
Importing an SSL certificate into your truststore....448
Exporting an SSL certificate from an Internet Explorer browser..449

Chapter 43 SolutionPack for Oracle Database 4.0 Summary Sheet 451
Overview.... 452
Technical specifications.... 452
Installing the SolutionPack.... 453
Configuring the SolutionPack with an unprivileged account.... 455
Limitations....456
Confirming report creation.... 456

Chapter 44 SolutionPack for Oracle MySQL Database 4.0 Summary Sheet 457
Overview.... 458
Technical Specifications....458
Where to find the latest SolutionPack software.... 458
Preparing MySQL database for discovery and data collection 459
Installing the SolutionPack 459
Limitations....460
Confirming report creation.... 460
Troubleshooting 460
What to do if data does not appear in any reports....461
What to do if data does not appear in some reports.... 462
Viewing collector errors in the Collector-Manager log files....462

Chapter 45 SolutionPack for Riverbed SteelHead Summary Sheet 463
Overview.... 464
Technical specifications....464
Where to find the latest SolutionPack software.... 465
Installing a SolutionPack....465
Configuring SNMP device discovery.... 466
Confirming report creation.... 467

Chapter 46 SolutionPack for Traffic Flows 4.0 Summary Sheet 469
Overview.... 470

Technical specifications....470
Where to find the latest SolutionPack software.... 470
Configuring Elastic Search.... 470
Installing the SolutionPack for Traffic Flows....472
Combined collector and database setup when installing SolutionPack for Traffic Flows - Single server deployment 474
Central database setup when installing SolutionPack for Traffic Flows - Distributed deployment.... 474
Distributed collector setup when installing SolutionPack for Traffic Flows - Distributed deployment.... 475
Report setup when installing SolutionPack for Traffic Flows.... 476
Post installation tasks....476
Starting the Event Processing Manager.... 476
Enabling event reporting and reconfiguring the Tomcat Frontend server (Linux).... 477
Enabling event reporting in SolutionPack for Traffic Flows (Windows)....478
Starting the Tomcat service.... 478
Confirming report creation.... 479
Upgrading Traffic Flows SolutionPack from 6.5u4 and 6.6u1 to 6.8u2....479
Upgrading Traffic Flows SolutionPack from 6.7u1 to 6.8u2.... 480
Migrating Traffic Flows SolutionPack from Datastore to Elastic Search... 481
Scheduling the Event-Processing Tasks.... 482
Troubleshooting 482
What to do if data does not appear in any reports.... 483
What to do if data does not appear in some reports.... 483
Viewing errors in the Event-Processing-Manager log files....484
What to do if parsing errors related to resource link updating occur....484

Chapter 47 SolutionPack for Transaction Summary Sheet 487
Overview.... 488
Technical specifications....488
Where to find the latest SolutionPack software.... 488
Installing the SolutionPack.... 489
Configuring the SolutionPack....490
Confirming report creation.... 490

Chapter 48 SolutionPack for UPS Summary Sheet 493
Overview.... 494
Technical specifications....494
Where to find the latest SolutionPack software.... 494
Installing the SolutionPack.... 495
Configuring SNMP device discovery.... 495
Confirming report creation.... 496
Troubleshooting 497
What to do if data does not appear in any reports.... 497
What to do if data does not appear in some reports....497
Viewing collector errors in the Collector-Manager log files....498

Chapter 49 SolutionPack for VMware vCenter 4.0 Summary Sheet 499
Overview....500
Technical specifications.... 500
Configuring the SolutionPack to collect Powerpath data.... 500
Installing this SolutionPack.... 501

Post-install requirements..... 503
Adding devices to discovery groups..... 504
Limitations..... 505

Part 4 Troubleshooting SolutionPack Configurations 507

Chapter 50 SolutionPack for EMC M&R Health 2.1 Summary Sheet 509
Overview.....510
Technical specifications.....510
Installing the SolutionPack.....510

Chapter 51 Troubleshooting techniques 513
Troubleshooting 514
What to do if data does not appear in any reports.....514
What to do if data does not appear in some reports..... 514
Viewing collector errors in the Collector-Manager log files..... 515

FIGURES

1 Data Collection example.... 64
2 Events setup example.... 65
3 Report setup example.... 67
4 Scheduled Event-Processing example.... 72
5 Example of polling settings.... 96
6 Example of discovery settings.... 97
7 Text from comment field.... 150
8 Outages type and Outages property.... 151
9 Scheduled Event-Processing example.... 373
10 SolutionPack for Oracle Database.... 452
11 Scheduled Event-Processing example.... 482

TABLES

1 Sample data enrichment import file column layout..... 40
2 Security settings for the SAM runcmd_env.sh file..... 62
3 SAM services when Notification Cache Publishing is enabled.....62
4 Software components required when collecting data from optical networks.....147
5 Node, Performance Category, Default file name pattern and 3GPP Format 164
6 Node, Performance Category, Default file name pattern and 3GPP Format 172
7 Node, Performance Category, Default file name pattern and 3GPP Format 180
8 Node, Performance Category, Default file name pattern and 3GPP Format 188
9 Node, Performance Category, Default file name pattern and 3GPP Format 196
10 Node, Performance Category, Default file name pattern and 3GPP Format 203
11 Node, Performance Category, Default file name pattern and 3GPP Format 211
12 Example of performance properties 242
13 Accessibility alerts.....245
14 Retainability alerts.....246
15 Mobility alerts.....247
16 Utilization alerts.....247
17 Object name examples.....249
18 Prerequisites for the SolutionPack for Acme Packet SBC..... 264
19 Top-level reports..... 268
20 Metrics..... 269
21 Prerequisites for the SolutionPack for Avaya Aura Communication Manager.....290
22 Avaya CM Native console commands..... 299
23 Report metrics..... 306
24 Support for Cisco UCS..... 384
25 Support for Microsoft Hyper-V 418
26 End-to-end capacity use cases..... 431
27 Support for Oracle Database..... 452
28 Support for VMware vCenter..... 500

PART 1

SolutionPacks for Use with Smarts Domain Managers

This section describes these SolutionPacks.

Chapter 1, "How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts"

Chapter 2, "SolutionPack for EMC Smarts 3.0 Summary Sheet"

Chapter 3, "Troubleshooting the Deployment of SAM, EMC M&R and the SolutionPack for EMC Smarts"

Chapter 4, "How to Maintain IP Manager Settings"

Chapter 5, "How to Set Up the EMC Smarts Server Manager for Citrix XenServer"

Chapter 6, "How to Set Up the EMC Smarts Server Manager for Software-Defined Networks Feature"

Chapter 7, "SolutionPack for EMC Network Configuration Manager 3.0 Summary Sheet"

Chapter 8, "SolutionPack for Optical Wavelength Services Summary Sheet"

Chapter 9, "Excluding Planned Maintenance Periods from Reports"

CHAPTER 1

How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts

- Overview 26
- Workflow for setting up SAM 27
- Workflow for setting up EMC M&R 31
- SSL setup for SAM and EMC M&R 41
- Configuring Smarts SolutionPack in HTTP mode 54

Overview

Service Assurance Suite combines some of the best features of Service Assurance Manager and EMC M&R to provide a common interface for viewing Notifications and reports on historical events. You must install and configure EMC Service Assurance Manager (SAM), EMC M&R, and the SolutionPack for EMC Smarts before you can view notifications or reports from the EMC M&R Report Library.

When EMC M&R platform and the SolutionPack for EMC Smarts are deployed with Service Assurance Manager, these features may be accessed from the EMC M&R interface:

- Notifications
- Reports showing geographical representation of Smarts network devices, physical inventory of device groups, and a physical inventory of the IP network
- IP Configuration Manager settings such as polling and thresholds
- Discovery and topology settings for underlying domain managers

In addition, the EMC Smarts Failover System now supports failover of the services used to communicate between Service Assurance Manager and EMC M&R platform. The *EMC Smarts Failover System User Guide* provides more information.

When upgrading to a newer version of the SolutionPack for EMC Smarts, ensure you upgrade and configure the Presentation Service Assurance Manager before upgrading the EMC M&R core software. Services must be installed and running before you install or upgrade the SolutionPack for EMC Smarts.

Additional information is described in these documents:

- *Service Assurance Suite Installation and Configuration Guide for EMC M&R*
- *SolutionPack for EMC Smarts Summary Sheet*
- *How to Maintain IP Manager Settings*
- *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts*

Resource allocation for SAM and EMC M&R

Ensure you dedicate resources (4CPU, 16GB) to SAM and also to the EMC M&R servers.

Typically, EMC M&R deployment is divided among different virtual machines (Backend, Frontend, Collector, and so forth). Ensure that sufficient memory and CPU are available in the virtual machine. Otherwise the system will fail.

Port configuration between SAM and the SolutionPack for EMC Smarts

When you install the SolutionPack for EMC Smarts, you must configure the ports between EMC M&R and the server hosting the Smarts EDAA (EMC Data Access API) to ensure communication across the firewalls.

The default port for the Smarts EDAA is 8080 (8443 in SSL mode). However, this port can be configured manually. If EMC M&R (with SolutionPack for EMC Smarts) and SAM are installed on different hosts, you must open the access to the EDAA port. Additionally, the Smarts Collector used by the SolutionPack connects to the Smarts Domain Manager servers via the ports they are started on. You must open a range of

ports, including the Broker, in order for data to pass between the Smarts domains and EMC M&R.

Workflow for setting up SAM

Configure the Presentation Service Assurance Manager (SAM-PRES) server to communicate with the SolutionPack for EMC Smarts installed on the EMC M&R platform.

During SAM installation you have a choice between two SAM services:

- EMC Smarts Service Assurance Manager Server (Notification Cache Publishing)
  - Start the Presentation SAM server with the EMC Smarts Service Assurance Manager Server (Notification Cache Publishing) service if you plan to integrate EMC M&R with this installation. When the SAM server is started with this service, SAM communicates with both EMC M&R and Smarts analysis domains.
- EMC Smarts Service Assurance Manager Server
  - Start Aggregation-level SAM servers with the EMC Smarts Service Assurance Manager Server service in environments with hierarchical SAM configurations.

One Presentation SAM server may be configured to work with one SolutionPack for EMC Smarts. By default, the SolutionPack for EMC Smarts connects to the Smarts Broker. When installing or updating the SAM software, you must enable Notification Cache Publishing so that notifications will flow into EMC M&R. Notification Cache Publishing enables SAM to publish its notifications to the Notification Cache. The Notification Cache is a separate collection of components, including RabbitMQ, ElasticSearch, and two webapps running under Tomcat (Ingestion and the Alert EDAA). Services for all of these components must be installed and running before notifications display in the EMC M&R User Interface.

Note

Both Smarts Web Console and the SAM Tomcat Server use the same default port (8080). If installing both on the same machine, change the port for one of them.
Change the Smarts EDAA Tomcat port when it conflicts with the Web Console Tomcat port on page 30

---

1. Ensure the Presentation SAM server has been upgraded to the latest version of the Service Assurance Suite. Select these options:
   - Under **Core Services**, select **EMC Smarts Broker** if you plan to run the Broker from the Presentation SAM server. If you run the Broker from another server, make note of the Fully Qualified Domain Name (FQDN) of the server.
   - Under **Service Assurance Manager Services**, select **EMC Smarts Service Assurance Manager Server (notification cache publishing)**
   - Under **EMC Data Access API**, select all of the entries:
     - **EMC Smarts Data Web Applications (Tomcat)**
     - **EMC Smarts Data Web Applications (Tomcat)**
     - **EMC Smarts Notification Exchange (Rabbit MQ)**
     - **EMC Smarts Notification Cache (ElasticSearch)**
   - Enter the port for the Broker service.
2. Configure your SAM license using smarts.lic or the license server.

3. Do one of the following:
   a. For configuring port and protocol settings when enabling SSL encryption in SAM and EMC M&R, see, SSL setup for SAM and EMC M&R on page 41.

      Or,

   b. For configuring Smarts SP in HTTP mode, see Configuring Smarts SolutionPack in HTTP mode on page 54.
4. Start the services. (Start the Broker service before starting the Tomcat service in your Presentation SAM installation.)
5. Issue the `sm_service show` command to ensure these services associated with the Presentation SAM installation are running:

Service name	Description of feature
`ic-broker`	Broker connected to Presentation SAM server
`ic-sam-server-pres`	SAM server with Notification Cache
`smarts-tomcat`	Smarts EDAA (controlled by Tomcat server)
`smarts-rabbitmq`	Rabbit MQ
`smarts-elasticsearch`	Elastic Search

6. When connecting to domain managers running pre-9.4 versions of Service Assurance Suite software, add two parameters that control security settings to the `runcmd_env.sh` file in the Presentation SAM server:
   - `SM_TLS_PROTOCOLS=+TLSv1.1`
   - `SM_ALLOW_LEGACY_CRYPTO=TRUE`

Note

When upgrading from older versions of SAM to version 9.3 or higher, you must manually register and start the SAM Notification Cache service (INCHARGE-SA-PRES). Command syntax for registering the SAM Notification Cache service on page 28

Command syntax for registering the SAM Notification Cache service

After an upgrade of older SAM software to version 9.3 or higher, you must register the SAM Notification Cache service and start it manually if you intend to use the SolutionPack for EMC Smarts to view notifications from the EMC M&R User Interface.

Register the SAM Notification Cache service

```
sm_service install --force  --unmanaged  --startmode=runonce '--
name=ic-sam-server-pres' '--description=EMC Smarts Service
Assurance Manager Server (notification cache publishing)' '/opt/
InCharge/SAM/smarts/bin/sm_server' '-n' 'INCHARGE-SA-PRES' '--
config=ics' '--port=0' '--edaa=sam-presentation/2.0' '--
bootstrap=bootstrap-amqp.conf' '--ignore-restore-errors' '--output'

sm_service show --cmdline ic-sam-server-pres
```

Start the SAM Notification Cache service

From the `SAM/smarts/bin` folder, issue the command, `sm_service start ic-sam-server-pres`

Check on status of running services

```
sm_service show
RUNNING ic-broker
RUNNING ic-sam-server-pres
NOT RUNNING ic-mbim-server
RUNNING smarts-tomcat
RUNNING smarts-rabbitmq
RUNNING smarts-elasticsearch
NOT RUNNING ic-sam-server
```

Smarts ElasticSearch service syntax for manual startup

```
smarts-elasticsearch
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged --startmode=runonce
--name=smarts-elasticsearch
--description=”EMC Smarts Notification Cache (ElasticSearch)”
/opt/InCharge/SAM/smarts/bin/sm_elasticsearch
--ignoreme
```

EMC Smarts Notification Exchange (Rabbit MQ) service syntax for manual startup

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force
--unmanaged --startmode=runonce
--name=smarts-rabbitmq
--description=”EMC Smarts Notification Exchange (Rabbit MQ)”
/opt/InCharge/SAM/smarts/bin/sm_rabbitmq
--ignoreme
```

EMC Smarts Data Web Applications (Tomcat) service syntax for manual startup

```
/opt/InCharge/SAM/smarts/bin/sm_service install --force --unmanaged
--startmode=runonce
--name=smarts-tomcat'
--description=”EMC Smarts Data Web Applications (Tomcat)”
/opt/InCharge/SAM/smarts/bin/sm_tomcat
--ignoreme
```

Server tool limitations in the EMC M&R User Interface

Only server tools available from the Presentation SAM server may be invoked from the EMC M&R User Interface.

In a hierarchical SAM deployment, server tools that need to be executed at the Aggregate Sam (SAM-AGG) layer will fail if they rely on communication with an underlying Smarts domain manager. When the server tool executes a script, it will still work at the Aggregate SAM level (for example, the LSP Ping server tool in MPLS or the Remedy Adapter).

If your server tool is not working as expected, you may need to edit the ASL scripts to invoke the SAM-AGG layer to work around this problem.

Change the Smarts EDAA Tomcat port when it conflicts with the Web Console Tomcat port

Change the ports for Smarts EDAA when the ports are already being used by the EMC Smarts Web Console which is installed on the same server. You also have to change the port setting for the SM_TOMCAT_SERVER environment variable.

The default ports when configuring Tomcat are 8080, 8005 and 8009.
If the Web Console is running Tomcat on these ports as described for a default installation, setting up a service like EDAA on same server causes a port conflict because the default ports for this Tomcat version are also 8080, 8005 and 8009.

When the Web Console and EDAA are running on same server, they require two versions of Tomcat to run: One is installed with the Console for the Dashboard service and the other for the SAM server services that require it such as EDAA.

To change the ports for Smarts EDAA, follow this procedure.

Procedure

1. Determine which ports are not being used on the server. For a list, run the command:
   - For Linux: **`netstat -anpt`**
   - For Windows: **`netstat -anb -p TCP`**
2. On the server where EDAA is installed, go to the Tomcat directory of the SAM installation (for example: **`./SAM/smarts/tomcat/conf`**).
3. Save a copy of the `server.xml` file as `server.xml.orig`.
4. Edit the `server.xml` file. Change the ports 8080, 8005 and 8009 to ports that are not being used (in this example, 8015, 8181 and 8019):

```
<Server port="8015" shutdown="SHUTDOWN">
  <!-- Security listener. Documentation at /docs/config/
listeners.html
 <Listener
className="org.apache.catalina.security.SecurityListener" />
 -->
 <!--APR library loader. Documentation at /docs/apr.html -->
 <Listener
className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
       .
       .
       .
<Service name="Catalina">
 <!--The connectors can use a shared executor, you can define
one or more named thread pools-->
 <!--
 <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
    maxThreads="150" minSpareThreads="4"/>
 -->

 <Connector port="8181" protocol="HTTP/1.1"
      connectionTimeout="20000"
      redirectPort="8443" />

 <!-- Define an AJP 1.3 Connector on port 8009 -->
 <Connector port="8019" protocol="AJP/1.3"
redirectPort="8443" />
```

5. Set the SM_TOMCAT_SERVER environment variable to the replacement port for 8080 (line with: `protocol="HTTP/1.1"`) in the `runcmd_env.sh` file:
   a. Use `sm_edit` from the `<BASEDIR>/smarts/bin` directory to open the file. For example: **`sm_edit conf/runcmd_env.sh`**
   b. Change the SM_TOMCAT_SERVER environment variable from `SM_TOMCAT_SERVER=http://<public_hostname>:<public_port>` to 8181 for this example:

```
SM_TOMCAT_SERVER=http://<public_hostname>:8181
```

   c. Save the file.
6. Restart the Tomcat service.

   For Linux: Type these commands from the `<BASEDIR>/smarts/bin` directory:

```
sm_service stop smarts-tomcat
sm_service show
sm_service start smarts-tomcat
```

   For Windows:

   a. Use the Service control panel to stop the service named "EMC Smarts Data Web Applications (Tomcat)".
   b. Use the Service control panel to start the service named "EMC Smarts Data Web Applications (Tomcat)" .

Workflow for setting up EMC M&R

1. Install or upgrade to the latest version of EMC M&R. The *Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides more information.
2. Start the services. For example, `/opt/APG/bin/manage-modules.sh service start all`
3. New installations of EMC M&R provide a 30-day trial license for all SolutionPacks. Ensure you obtain and install permanent licenses for SolutionPacks you plan to use longer than 30 days.
4. Install the SolutionPack for EMC Smarts.
   The article, *SolutionPack for EMC Smarts Summary Sheet* on page 55 of this document , provides more information.
   - On the Reports page of the SolutionPack installation wizard, you must enter the Fully Qualified Domain Name (FQDN) of the EMC M&R Tomcat server. This address must match the entry in the `SM_CAS_SERVER` parameter setting in the `runcmd_env.sh` file in the Presentation SAM server.

   Note

   Use the FQDN, not an IP address, when configuring the SolutionPack for EMC Smarts.

- Enter the FQDN for the server hosting the Smarts EDAA.
- Accept the default values for the other fields unless your deployment has a non-default SAM setup. For example,
  - SAM Presentation server is not named `INCHARGE-SA-PRES`
  - SAM server is using SSL
  - The admin-profile in SAM has changed
- On the Reports page of the SolutionPack installation wizard, enter the Smarts Configuration Manager domain name if you plan to manage settings for your IP domains from the EMC M&R interface.

Note

Ensure you restart the Presentation SAM services after you configure the SolutionPack for EMC Smarts. This forces the CAS webapp to run with the latest configuration.

After installation of the SolutionPack for EMC Smarts, configure IP settings in the Configuration Manager and push them to the remote IP domain managers. Access the IP settings from **Administration** > **Modules** > **Smarts**. Additional information is provided in this article:

- *How to Maintain IP Manager Settings*

5. Create user accounts for operators in EMC M&R. The Administrator must also create new Roles for these users and map them to existing profiles in Service Assurance Manager (SAM).
6. Set the default navigation style to **Use tree navigation**. This setting is recommended for the SolutionPacks for the 9.5 release.
7. You can customize the tools available in the Notification views depending on the value of the **User Status**.
8. You can customize the client tools available from the Notification reports if you want to add scripts to show notification name or severity.
9. Run manual Topology import from **Administration** > **Centralized Management** > **Scheduled Tasks** > **Topology**. Click **sm-collector/import-smarts-topology** and click **Run**.
   By default the task runs every day at midnight.

User management for SolutionPack for EMC Smarts

In order to manage notifications from the SolutionPack for EMC Smarts, the Administrator must set up users and roles in EMC M&R that correspond to the profiles set up in Service Assurance Manager (SAM).

In the SAM Global Manager Administration Console, the Administrator configures profiles that define which Notifications, Actions, and Tools are available to each group of users (for example, OPER profile and so forth).

The Administrator providing access to SolutionPack for EMC Smarts views has to create users and roles in EMC M&R that reflect the characteristics of the SAM profiles that are in use.

If Administrators need to restrict Notifications, Actions, or Tools available to a user in EMC M&R, they need to define the restrictions first in the corresponding SAM profile.

Note

The Administrator should not duplicate EMC M&R users in SAM unless a user needs access to both the SolutionPack for EMC Smarts views and classic SAM Consoles. Users working only in EMC M&R need only the user login and role definition created in EMC M&R.

Set role restrictions for non-administrator users of SolutionPack for Smarts

If you want additional user roles, such as oper (operator), or profiles configured in your Presentation SAM server, you must set role restrictions after installing the SolutionPack for Smarts.

The default role is assigned to administrator. Add additional roles as needed.

Procedure

1. From **Administration** > **Roles**, click **New Role**.
2. Click **Modules & Restrictions Access** and expand the **Smarts** module.
3. Add an existing smarts profile (such as `oper-profile` or `default-profile`) and click **Save**.
4. From **Administration** > **Users**, create a new user and assign a role to the new user.

   You can assign one or more roles to a new user.

   Note

   Notification actions (like Acknowledge/Unacknowledge, Take/Release Ownership, and so on) in the Notifications view are available for a user who is assigned multiple roles that have the same sam-profiles. Notification actions are not available for a user who is assigned multiple roles that have different sam-profiles.

SAM user profile mapping and EMC M&R role-based access

After you set up the user profiles and assign them to roles in EMC M&R, the administrator must associate those profiles and roles with users who need to access both Service Assurance Manager (SAM) Consoles and the EMC M&R User Interface.

Administrator profile behavior

The EMC M&R administrator role is mapped to the EMC Smarts Admin profile when the SolutionPack for EMC Smarts is installed.

Note

If you try to assign a SAM profile to the EMC M&R Admin user, that SAM profile will be overwritten with the EMC M&R profile.

User profile behavior

The administrator can assign a SAM profile to an EMC M&R non-administrator user from **Administration** > **Modules & Restrictions Access** > **Smarts**.

- Ensure you assign an existing SAM Profile to the user, (for example, oper-profile, default-profile, and so forth).

- You can assign more than one Role with a SAM Profile to a user.

Set default navigation style

The navigation style controls the look and feel of the left navigation column in the reporting interface.

This procedure sets the global default navigation style. Users can override the global default style for their user account on **Profile** > **View Profile** > **Preferences**.

Procedure

1. Click **Administration** > **Portal**.
2. Click the **Default Display** tab.
3. In **Navigation Style**, make a selection.

Option	Description
Use icon navigation	The navigation column contains icons that expand into reporting categories
Use tree navigation	The navigation column is a hierarchical tree of report names

4. Click **Save**.

Hide unused entries in the navigation tree

You can hide default entries in the navigation tree if you have not installed the products that populate them with data.

Before you begin

The default EMC M&R platform displays nodes such as **Operations**, **Explore**, **Dashboards**, and **Planning** in the navigation tree. Other product suites that also use EMC M&R as their platform display entries under these nodes by default. However, no data populates these entries unless you are using those products. The SolutionPack for EMC Smarts populates data in the **Network** block under **Operations**, **Explore**, and **Dashboards**.

Procedure

1. To hide entries in the navigation tree, click **Edit Mode** from the EMC M&R User Interface.
2. Find the storage-related blocks in the list and select, **Always Hide**.

   Do not hide the **Network** block under the **Operations**, **Explore**, or **Dashboards** nodes. The **Network** block contains all of the SolutionPack for EMC Smarts views and reports. The **Planning** node is not used by the SolutionPack for EMC Smarts.

Viewing notifications from the EMC M&R User Interface

Launch Object Details from the Notifications view.

Before you begin

You can view notifications coming from the Presentation SAM server in the EMC M&R User Interface.

Procedure

1. To view Notifications where an element name is collected, launch the Object Details report with map, details, containment, and so forth.
2. To view Notifications with an element name that is not collected by the SolutionPack for EMC Smarts, launch only the Details view.

   The SolutionPack for EMC Smarts does not collect every class and instance that exists in the Smarts domains. It selects "top level" classes like Routers, Switch and some of their underlying components.

Troubleshooting an empty notification list

After creating a new Notification List in Service Assurance Manager, the notifications are not visible in the EMC M&R User Interface.

When you create a new Notification List in Service Assurance Manager, you must issue this command to have notifications populate the correct reports in EMC M&R. This command ensures notifications are re-cached so they display in the correct Notification List.

Issue this command from the Presentation Service Assurance Manager *<install_directory>*\SAM\smarts\bin folder: `dmctl> invoke ICS_NLManager::ICS-NLManager renotifyAllEvents`

Troubleshooting notification list errors

Notifications are not visible in the EMC M&R user interface. "MSAException" and "Map is showing HTTP Error" messages display.

Check the `/etc/hosts` file in the Presentation SAM server. If the `/etc/hosts` file does not list the Fully Qualified Domain Name of the EMC M&R host, these errors will display.

Add the entry in the `/etc/hosts` file and restart all SAM services.

Troubleshooting Notification view popouts

The popout option that was formerly available under the gear tool for the Notification report is not available.

Select **View in Full Page** under the Display option in the EMC M&R user interface. This opens the Notification report in a new window.

Customizing the tools that are available in the Notification view

Depending on your business needs, you can customize which tools are available for the user in the Notification view. When you create the EMC M&R user, the value that you select for the User Status field determines which tools will appear for the view.

By default, for a non-administrator user (Normal user), all tools except Associate User and Clear Customizations are enabled. All tools are enabled for the admin user (Global Administrator).

Procedure

1. Go to the `<installdirectory>/APG/Web-Servers/Tomcat/Default/webapps/dojoviews/WEB-INF/classes/resources/view/AlertView` directory.
2. Edit the userStatus section in the `SmartsAlertTools.xml` file.

Change the values to **`true`** or **`false`**. Do not edit other sections of the file.

```
<userStatus>
<status name ="Global Administrator" isAdministrator="true"
   <filter>true</filter>
   <clearFilter>true</clearFilter>
   <associateUser>true</associateUser>
   <clearCustomization>true</clearCustomization>
   <multiSort>true</multiSort>
   <manageColumns>true</manageColumns>
   <manageColor>true</manageColor>
</status>
<status name ="Normal User" isAdministrator="false"
   <filter>true</filter>
   <clearFilter>true</clearFilter>
   <associateUser>false</associateUser>
   <clearCustomization>false</clearCustomization>
   <multiSort>true</multiSort>
   <manageColumns>true</manageColumns>
   <manageColor>true</manageColor>
</status>
</userStatus>
```

The Audible Alert tool is not listed because it cannot be enabled or disabled.

3. Save the file.
4. Restart the Tomcat services.
5. Verify by logging in as the user, select **Operations** > **Network** > **Notifications**, and select the **gear** icon near the Notification view.

Creating client tools

Client tools are programs the operator invokes by right-clicking on a notification.

The default client tool, **Launch EMC M&R**, launches the EMC M&R home page. You can create others by editing the `SmartsTools.json` file.

Procedure

1. To create client tools, log in to **Centralized Management** and expand **Logical Overview** > **Miscellaneous** > **Custom**.
2. Click **Webapps-Resources::Default** and expand the list of Configuration files.
3. Select the checkbox for `/conf/SmartsTools.json` and click the pencil icon to edit the file.

   Use this file to add or modify options that appear in the Notifications **Client Tools** right-click menu. You can edit the tool to launch any URI and pass in any notification property as a parameter by surrounding it with brackets.

   You must encode `&` characters as `%26`.

   Column headers which are available in Notifications can be passed as arguments to the URI. The various notification properties that can be used are Acknowledged, Active, Category, Certainty, ClassName, ClassDisplayName, ClearOnAcknowledge, ElementClassName, ElementName, EventText, EventName, EventState,EventType, EventDisplayName, FirstNotifiedAt, Impact, InstanceName, IsProblem, IsRoot, InMaintenance, LastClearedAt, LastNotifiedAt, LastChangedAt, Name, NotificationID, OccurrenceCount, Owner, Severity, SourceDomainName, SourceEventType, TroubleTicketID, UserDefined 1 to 20.

Example client tool:

```
{
         "name": "Example 1",
         "url": " http://www.emc.com/?class={ClassName}
%26source={SourceDomainName}"
        },
```

In this example, `"name":"Example 1"` is the name which appears on the sub-menu for the right click action on the notification. This causes the text, "Example 1" to display. When you right-click on a Notification, you will see **Client Tools** > **Example 1**.

In this example, `"url": " http: //www.emc.com/?class={ClassName}%26source={SourceDomainName}"` provides the URL to which a notification attribute can be appended as a parameter. In this example, ClassName and SourceDomainName are used. When invoked, this tool would launch, `http://www.emc.com/?class=Host&source=INCHARGE-AM-PM`.

Additional files that may be used when creating client tools include `conf/common.properties` and `mib-browser/mib-browser.xml`.

Invoking Perl scripts with client tools in Notification views

Configure client tools to execute Perl scripts when you right-click a notification. This is not part of the default installation and must be configured manually.

Before you begin

This feature is available when the Presentation SAM is upgraded to version 9.4.2 onwards and EMC M&R is upgraded to 6.7u1 onwards. The SolutionPack for EMC Smarts must also be upgraded to get support for this feature.

Procedure

1. Create a folder, `clientTools`, in `<installdirectory>/APG/Web-Servers/Tomcat/Default/webapps/dojoviews/WEB-INF`.
2. Copy a valid Perl script file, `<file_name>.pl`, to this location.
3. Edit `dojoviews.xml` and add **`privileged="true"`** as an attribute for the Context tag. For example, `<Context reloadable="false" privileged="true">`

   `dojoviews.xml` is in `<install directory>/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost`
4. Save the file.
5. Modify `web.xml` to uncomment the servlet, `cgi`, and its servlet mapping.

   `web.xml` is in `<install directory>/APG/Web-Servers/Tomcat/Default/webapps/dojoviews/WEB-INF`
6. Restart the tomcat services
7. Test the script by invoking the URL. For example, from this location, `<install directory>/APG/Web-Servers/Tomcat/Default/webapps/dojoviews/WEB-INF`, enter this URL: `http://<M&R_Host>:<Port>/dojoviews/client-tool/<file_name>.pl`

8. Modify `SmartsTools.json` to add the new tool as a Notification attribute.

   `SmartsTools.json` is in EMC M&R Centralized Management at **Logical Overview** > **Miscellaneous** > **Custom** > **WebApps-Resources**.

Perl script example for use with client tool in Notification view

This example script prints the notification name and severity and displays it in a web browser.

Example 1 alertExample.pl

```
#!/usr/bin/perl -w
use CGI qw(:standard);
use strict;
my $query = new CGI;
my $notification = $query->param('notification');
my $severity = $query->param('severity');
print $query->header("text/html");
print "Notification $notification has severity value $severity\n";
```

Editing client tools in SmartsTools.json

You must edit `SmartsTools.json` to add the Perl script as an attribute on the Notification table. This allows you to right-click the notification and select the client tool that invokes a Perl script.

To add the script to the client tool available from the Notification view, copy the script to a file with a `.pl` extension, for example, `alertExample.pl`.

You must add the script to the Notification Client tool by modifying `SmartsTools.json` in this Centralized Management path: **Logical Overview** > **Miscellaneous** > **Custom**.

Procedure

1. Click **Webapps-Resources::Default** and expand the list of Configuration files.
2. Select the checkbox for `/conf/SmartsTools.json` and click the pencil icon to edit the file.
3. Add these lines to the .json file and save the changes.

```
{
"name": "Alert Attribute",
"url": "/dojoviews/client-tool/alertExample.pl?notification=
{Name}
&severity=
{Severity}
"
}
```

4. Test the client tool changes by invoking the alertExample.pl script from a Notification.

   Select a notification in the **Operation** > **Network** > **Notification**report. Right-click the notification and select **`Alert Attribute`** to invoke the example Perl script.

Results

This will display the notification name and severity value.

Enrich device location data in Smarts geographical maps

The Smarts geographical map (geomap) shows the location of Smarts-enabled devices in the network. Before viewing Smarts geomaps, perform data enrichment of the device locations to provide more details in the map.

Before you begin

Ensure device discovery has finished and devices display in the user interface before enriching the location data. Look in the **Explore** > **Network** tree to view the discovered devices. The **Location** attribute of the device object in Smarts IP Manager populates the **Device Location** dropdown after discovery.

The *APG-Centralized-Management-Guide*, found in the `/APG/Doc` folder in your EMC M&R installation, provides additional information.

Procedure

1. Register the Collector Manager module with the hostname of the EMC M&R installation.
   a. From **Centralized Management** > **Data Enrichment**, click **Register** for New Module.
   b. Click **<hostname>** in the first column.
   c. Click **Collecting** in the second column.
   d. Click **Collector Manager :: emc-smarts :: DataEnrichment** in the third column.

      Do not select any other modules from the list. They are not required for geomaps.
2. Select **Collector Manager :: emc-smarts :: DataEnrichment** and click **geo-map-enrichment**.

   The DataEnrichment property is used to enrich the values in **Device Location** to match meaningful values in the **smlocale** column.

   a. Find the columns for **Device Location** and **smlocale**.

      By default the first row displays `@MATCHALL` for **Device Location** and `@NULL` for **smlocale**.
   b. Replace the default values with meaningful names, for example, **`*white`**, in **Device Location** can map to **`White Plains, New York`** for the **smlocale** value.

      Enter a valid **smlocale** name which will be identifiable on the geomap.

      The **Device Location** dropdown menu displays accurate data only after device discovery has finished. For example, typing **`'W'`** displays all locations having names with **`'W'`**. Typing **`*`** displays all locations.
   c. Save the changes.
   d. Click **Update** in the **Save Data Enrichment** window.

   All values in the dropdown windows must be enriched to get all locations in the geomap.

To add a new row for enrichment, right-click the icon appearing in front of the row. This gives options to **Insert Before**, **Insert After**, or **Delete** a row.

3. Restart the Database and Backend.
   a. Go to **Centralized Management** > **Scheduled Tasks**.
   b. Click **Select All**.
   c. Uncheck the **Update Online** option.
   d. Click **Run now** to restart the Database and Backend.
4. Restart the EMC M&R services.

   This restarts the Collector Manager.

   After some time, the Smarts Geography geomap will be uploaded to **Dashboard** > **Network** > **EMC Smarts Geography**. Click the icons on the map to view devices present at that location.

Alternate method of data enrichment using file import

Use the Import/Export function in the UI to import CSV or XLS files with Device Location and smlocale mapping as an alternative method of enriching Smarts geomap data.

The XLS or CSV files must have two columns of values in the same order as the columns mentioned in data enrichment. Here is an example:

Table 1 Sample data enrichment import file column layout

Device Location column data	smlocale column data
white*	White Plains, NY
10;PUGET SOUND;United States;REDMOND, WA;11	Redmond, Washington
Westchester Ave	White Plains, NY
LOCATION	Bangalore, India
EMC E-Labs Building 119	Bangalore, India
Hopkinton	Hopkinton, MA
DevLab, row 2-rack 2, 44 S Broadway, 7th floor	Bangalore, India
10.3.2	Delhi, India
Chicago, IL	Chicago, IL

Although the value, *<city>*, is enough for **smlocale** to render points in the map, enter *<city, state>* or *<city,country>* to avoid duplicates or conflicts. Ensure the location name is valid because it will display in the maps report.

Map reports

A map report is basically a standard table report where each child node displays as a point in a geographical map. You can edit the location and the name of the location as well as the size, color, and shape of marker displayed on the map.

In **Report Type** on the **Report Configuration** tab, you select the map report from the miscellaneous section.

You can edit the following attributes on a map report:

- **Location** locates an element on the map.
- **Name** provides a name to a location, such as device name, region, and sitename.
- **Size** sets the size of the marker. The size of the marker is based on a given metric value, such as the number of devices at the site.
- **Color** sets the color of the marker. The color relies on the threshold definition where green represents no thresholds, yellow represents a major threshold, and red represents a critical threshold.
- **Marker** sets the shape of the marker, such as circle, square, triangle, inverted triangle, pentagon, and sector.

Switch between OpenStreetMap and Google Maps

OpenStreetMap is used as the default platform mapping software. Use this procedure to configure EMC M&R to use other mapping software, such as Google Maps.

Procedure

1. To switch from OpenStreetMaps (osm) to Google Maps (google), navigate to `APG/Web-Applications/APGFrontend/APG/conf/common.properties`.
   a. Add these lines to `common.properties`:

   ```
   #==========================================================
   Setting for Google Maps (client-side)
   #==========================================================
   apg.maps.geocode=false
   apg.maps.provider=google
   apg.maps.geocoder=google
   ```

   b. Restart all managed module services including tomcat.
2. To switch back to OpenStreetMaps from Google Maps
   a. Comment the lines of code you added to `common.properties` file to disable them.
   b. Restart all managed module services including tomcat.

SSL setup for SAM and EMC M&R

Adjust the port and protocol settings when enabling SSL encryption in SAM and EMC M&R.

The procedures for SSL setup assume use of the Java Keytool. You may, optionally, use a different encryption tool.

This keytool generates keystore files in the location where the commands are issued. For these SSL procedures, the following assumptions are made:

1. When configuring EMC M&R (Watch4net) with CLI commands, issue the commands from the `bin` folder of the installation path. For example, `/opt/APG/bin` or from `c:\Program Files\APG\bin`.
2. When configuring Service Assurance Manager (SAM) with CLI commands, issue the commands from the base directory path. For example, `/opt/`

`InCharge/SAM/smarts` or from `c:\Program Files\InCharge\SAM\smarts`.

3. Both EMC M&R and SAM installations include versions of Java. Check to ensure the correct versions of Java are in use in both the EMC M&R server and in the SAM server. Java is usually installed into the `...usr/bin` path. (The versions may differ between EMC M&R and SAM.)

Workflow

1. Edit the Reports configuration settings in the SolutionPack for EMC Smarts to adjust port and protocol settings.
2. Generate the SSL certificate for the EMC M&R (Watch4net) server where the Tomcat server is running. The Java documentation provides details.
3. Generate the SSL certificate for the Service Assurance Manager (SAM) server where the Tomcat server is running. The Java documentation provides details.
4. Ensure the configuration settings have been adjusted for SSL. For example, check the **SM_CAS_SERVER** and **SM_TOMCAT_SERVER** settings in the `runcmd_env.sh` file in SAM and edit the settings to add the secure port numbers and change the protocol from `http` to `https`. (When you change runcmd_env.sh, you must stop and restart the SAM service. For example, `sm_service stop|start ic-sam-server-pres`)

   Note

   Where **SM_CAS_SERVER** is the URL that identifies the EMC M&R Tomcat server host, and it has to specify the protocol and port used to log into EMC M&R. And, **SM_TOMCAT_SERVER** specifies the Fully Qualified Domain Name (FQDN) of the SAM Tomcat server.

5. Enable the `https` protocol in the `server.xml` files in both the SAM and EMC M&R deployments. Add the `Http11Protocol` and `Http11NioProtocol` sections if missing from the `server.xml` file.
6. Export the EMC M&R certificate and import to the SAM server.
7. Export the SAM certificate and import to the EMC M&R server.
8. Stop and start the SAM Tomcat server.
9. Restart the EMC M&R Tomcat server.

Linux SSL Setup

Enable SSL port and protocol settings in SolutionPack for EMC Smarts

When enabling SSL, you must edit the Reports configuration of the SolutionPack for EMC Smarts and ensure use of secure port and protocol settings.

Before you begin

This procedure assumes the SolutionPack for EMC Smarts is already installed and running. If not, the *SolutionPack for EMC Smarts Summary Sheet* article provides installation instructions.

Edit the Reports configuration page to enable SSL for the SolutionPack for EMC Smarts. Access this page from **Centralized Management.** Expand **SolutionPacks** > **Infrastructure** and click **EMC Smarts**.

Procedure

1. Click the **Pencil** icon by the Reports SolutionPackBlock.

   The Reports reconfiguration page appears.
2. Expand Tomcat Configuration and choose **Add a new Tomcat configuration** in the dropdown box.
3. Click the checkbox for **HTTPS Enabled for EMC M&R and Smarts**.
4. Enter the Fully Qualified Domain Name or IP address of the EMC M&R Tomcat server.

   This name must match the host name portion of the entry in **SM_CAS_SERVER** in the Presentation SAM `runcmd_env.sh` file. Ensure consistent use of either IP address or FQDN in all of the field entries. Do not mix the entry formats.
5. Enter the secure port for the EMC M&R Tomcat server. (Default SSL port is 58443).
6. Expand the Smarts and Alerts EDAA Configuration and choose **Add a new Smarts and Alerts EDAA Configuration** in the dropdown box.

   Check the entry in the **Smarts EDAA hostname or IP address** field. This entry must match the host name portion of the entry in **SM_TOMCAT_SERVER** in the Presentation SAM `runcmd_env.sh` file.
7. Enter the secure port for the Smarts EDAA server. (Default SSL port is 8443).
8. Adjust other entries if needed and then click **Reconfigure**.

After you finish

Continue with the SSL certificate generation, import, and export steps. The changes will not take effect until the Tomcat servers are restarted in both SAM and EMC M&R.

Linux: Generate the keystore file for EMC M&R

Create the keystore file for the EMC M&R host. This file stores the Tomcat server's private key and self-signed certificate.

Before you begin

Stop the EMC M&R Tomcat service. For example, **`opt/APG/bin/manage-modules.sh service stop tomcat`**

Procedure

1. Generate the keystore. For example, run this command for the EMC M&R host if it has a Fully Qualified Domain Name (FQDN):

   ```
   /opt/APG/Java/Sun-JRE/8.0.141/bin/keytool -genkey -alias
   tomcat
   -keyalg RSA -ext san=dns:localhost,dns:<M&R frontend FQDN>,ip:
   127.0.0.1 -keystore /opt/APG/.keystore
   ```

   a. Enter **`changeit`** for the keystore password.

   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, **`itops-dev-204.lss.emc.com`**.

c. Answer the other questions and type **yes** when asked for confirmation.

If you are using an IP address naming convention for the configuration, run this command and specify the IP address of the EMC M&R host for <*ip:x.x.x.x*>.

```
/opt/APG/Java/Sun-JRE/8.0.141/bin/keytool -genkey -alias
tomcat
-keyalg RSA -ext SAN=dns:localhost,ip:x.x.x.x,ip:127.0.0.1 -
keystore /opt/APG/Web-Servers/Tomcat/Default/conf/.keystore
```

Results

This creates a keystore file inside `/opt/APG` folder with name `.keystore`. This is a hidden file in Linux.

Linux: Editing the EMC M&R server.xml file

Edit the server.xml file to tell Tomcat server which secure port to use.

Update the `https` connector configuration in `server.xml` in this path, `/opt/APG/Web-Servers/Tomcat/Default/conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.

   For new installation, `https` connector configuration in server.xml is enabled by default.

2. Add the path to the keystore file. For example,

```
 <Connector port="58443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
               maxThreads="150" SSLEnabled="true"
scheme="https" secure="true"
               compression="2048"
               clientAuth="false" sslProtocol="TLSv1.2"
URIEncoding="UTF-8"
               sslEnabledProtocols="TLSv1.2"
keystoreFile="/opt/APG/.keystore"
keystorePass="changeit"

ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" />
```

Configuring SAM environment variables to support SSL

Edit the environment variables in the SAM runcmd_env.sh file to support SSL.

Before you begin

Both SM_CAS_SERVER and SM_TOMCAT_SERVER must be configured to support SSL. The SM_CAS_SERVER environment variable is set to the URL for EMC M&R. The SM_TOMCAT_SERVER environment variable is set to the URL for the SAM Tomcat server.

Procedure

1. Enter the secure port and protocol used to log into EMC M&R in the SM_CAS_SERVER variable. For example, `SM_CAS_SERVER=https://<cas-serverhost>:58443`
2. Enter the secure port and protocol used to log into SAM Tomcat server in the SM_TOMCAT_SERVER variable. For example, `SM_TOMCAT_SERVER=https://<smarts-tomcat-server-host>:8443`

After you finish

Stop and restart the SAM service to make the changes take effect. For example:

```
sm_service stop ic-sam-server-pres
```

```
sm_service start ic-sam-server-pres
```

Linux: Generating the SAM Tomcat server keystore file and certificate

Create the Tomcat server keystore file and certificate.

Before you begin

Generate the keystore file in the home directory where you issue the command.

Procedure

1. Issue the command to generate the keystore file. For example, run this command for the SAM host if it has a Fully Qualified Domain Name (FQDN):

   ```
   /opt/InCharge/SAM/smarts/jre/bin/keytool -genkey -alias
   tomcat -keyalg RSA
   ```

   To specify a different location or filename, add the `-keystore` parameter followed by the complete pathname to the keystore file. For example,

   ```
   /opt/InCharge/SAM/smarts/jre/bin/keytool -genkey -alias
   tomcat -keyalg RSA
   -keystore /opt/InCharge/SAM/smarts/.keystore
   ```

   a. Enter **`changeit`** for the keystore password.

   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, **`itops-dev-204.lss`**.emc.com.

   c. Answer the other questions and type **`yes`** when asked for confirmation.

   If you are using an IP address naming convention for the configuration, run this command and specify the IP address of the SAM host for <*ip:y.y.y.y*>.

   ```
   /opt/InCharge/SAM/smarts/jre/bin/keytool -genkey -alias
   tomcat -keyalg RSA -ext SAN=<ip:y.y.y.y> -keystore /opt/
   InCharge/SAM/smarts/.keystore
   ```

Results

This creates a keystore file inside `/opt/InCharge/SAM/smarts` folder with name `.keystore`.

Linux: Editing the SAM server.xml file

Edit the server.xml file to tell the SAM Tomcat server which secure port and protocol to use.

Update the `https` connector configuration in `server.xml` in this path, `/opt/InCharge/SAM/smarts/tomcat/conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file and the password. For example,

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https"
secure="true" keystoreFile="/opt/InCharge/SAM/
smarts/.keystore" keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2" />
```

Note

Update the `sslEnabledProtocols`, if you are using different version s of TLS.

Linux: Creating the trust relationship between SAM and EMC M&R

You must export and import certificates to get the SAM Tomcat server and EMC M&R Tomcat server to trust each other.

Before you begin

First, export a certificate on the SAM server. Then import it into the EMC M&R Tomcat server. Then export a certificate from the EMC M&R server and import it into the SAM Tomcat server.

Procedure

1. Export a certificate from the SAM Tomcat server. For example,

```
/opt/InCharge/SAM/smarts/jre/bin/keytool -export -
keystore /opt/InCharge/SAM/smarts/.keystore -alias tomcat -
rfc > SAMtomcat.cert
```

   a. Copy SAMtomcat.cert to the host where EMC M&R Tomcat server is installed.

   b. On the EMC M&R host, import the SAMtomcat.cert. For example,

```
/opt/APG/Java/Sun-JRE/8.0.141/bin/keytool -import -file
SAMtomcat.cert -alias SAMtomcat -keystore /opt/APG/.keystore
```

Note

If you see the following warning, type yes and continue :

```
Certificate already exists in keystore under alias <tomcat>
Do you still want to add it? [no]: yes
Certificate was added to keystore
```

c. Back up the original EMC M&R `cacerts` file.

```
cp /opt/APG/Java/Sun-JRE/8.0.141/lib/security/
cacerts /opt/APG/Java/Sun-JRE/8.0u51/lib/security/cacerts-
SAVE    # Backup old cacerts file
```

d. Copy `.keystore` and rename it to `cacerts`.

```
cp /opt/APG/.keystore /opt/APG/Java/Sun-JRE/8.0.141/lib/
security/cacerts
```

2. Restart Tomcat server on the EMC M&R host.

```
/opt/APG/bin/manage-modules.sh service restart tomcat
```

3. Export a certificate from the EMC M&R host. For example,

```
/opt/APG/Java/Sun-JRE/8.0.141/bin/keytool -export -
keystore /opt/APG/.keystore -alias tomcat -rfc >
W4Ntomcat.cert
```

4. Copy W4ntomcat.cert to the SAM server host.
5. On the SAM server host, run this command to import a certificate copied from the EMC M&R server host.

```
/opt/InCharge/SAM/smarts/jre/bin/keytool -import -file
W4Ntomcat.cert -alias W4Ntomcat -keystore /opt/InCharge/SAM/
smarts/.keystore
```

Note

If you see the following warning, type yes and continue :

```
Certificate already exists in keystore under alias <tomcat>
Do you still want to add it? [no]: yes
Certificate was added to keystore
```

6. Copy the keystore file.

```
cp /opt/InCharge/SAM/smarts/jre/lib/security/cacerts /opt/
InCharge/SAM/smarts/jre/lib/security/cacerts-SAVE    # Backup
old cacerts file
```

```
cp /opt/InCharge/SAM/smarts/.keystore /opt/InCharge/SAM/
smarts/jre/lib/security/cacerts
```

7. Confirm the certificates copied properly (review entries).

   For SAM

```
/opt/InCharge/SAM/smarts/jre/bin/keytool -list -keystore /opt/
InCharge/SAM/smarts/.keystore
```

   For EMC M&R

```
/opt/APG/Java/Sun-JRE/8.0.141/bin/keytool -list -
keystore /opt/APG/.keystore
```

8. Stop and start the Tomcat service on the SAM server:
   a. `/opt/InCharge/SAM/smarts/bin/sm_service stop smarts-tomcat`
   b. `/opt/InCharge/SAM/smarts/bin/sm_service start smarts-tomcat`
9. Restart the EMC M&R services.

```
/opt/APG/bin/manage-modules.sh service restart all
```

10. Check the `<SAM_BASEDIR>/smarts/local/logs/tomcat/smarts-edaa.log` file for certificate exchange errors (SSLHandshake exception).

    If you see any such certificate exchange errors, it is recommended to remove `<SAM_BASEDIR>/smarts /.keystore and /opt/APG/.keystore` files and regenerate the certificates and perform certificate exchange again.

Windows SSL Setup

Enable SSL port and protocol settings in SolutionPack for EMC Smarts

When enabling SSL, you must edit the Reports configuration of the SolutionPack for EMC Smarts and ensure use of secure port and protocol settings.

Before you begin

This procedure assumes the SolutionPack for EMC Smarts is already installed and running. If not, the *SolutionPack for EMC Smarts Summary Sheet* article provides installation instructions.

Edit the Reports configuration page to enable SSL for the SolutionPack for EMC Smarts. Access this page from **Centralized Management.** Expand **SolutionPacks** > **Infrastructure** and click **EMC Smarts**.

Procedure

1. Click the **Pencil** icon by the Reports SolutionPackBlock.

   The Reports reconfiguration page appears.
2. Expand Tomcat Configuration and choose **Add a new Tomcat configuration** in the dropdown box.
3. Click the checkbox for **HTTPS Enabled for EMC M&R and Smarts**.
4. Enter the Fully Qualified Domain Name or IP address of the EMC M&R Tomcat server.

   This name must match the host name portion of the entry in **SM_CAS_SERVER** in the Presentation SAM `runcmd_env.sh` file. Ensure consistent use of either IP address or FQDN in all of the field entries. Do not mix the entry formats.
5. Enter the secure port for the EMC M&R Tomcat server. (Default SSL port is 58443).
6. Expand the Smarts and Alerts EDAA Configuration and choose **Add a new Smarts and Alerts EDAA Configuration** in the dropdown box.

   Check the entry in the **Smarts EDAA hostname or IP address** field. This entry must match the host name portion of the entry in **SM_TOMCAT_SERVER** in the Presentation SAM `runcmd_env.sh` file.
7. Enter the secure port for the Smarts EDAA server. (Default SSL port is 8443).
8. Adjust other entries if needed and then click **Reconfigure**.

After you finish

Continue with the SSL certificate generation, import, and export steps. The changes will not take effect until the Tomcat servers are restarted in both SAM and EMC M&R.

Windows: Generate the keystore file for EMC M&R

Create the keystore file for the EMC M&R host. This file stores the tomcat server's private key and self-signed certificate.

Before you begin

Stop the EMC M&R Tomcat service. For example, **`c:\Program Files\APG\bin\manage-modules.cmd service stop tomcat`**

Procedure

1. Generate the keystore. For example, run this command for the EMC M&R host if it has a Fully Qualified Domain Name (FQDN):

```
C:\Program Files\Java\Sun-JRE\8.0.141\bin\keytool.exe -genkey
-alias tomcat
-keyalg RSA -ext san=dns:localhost,dns:<M&R frontend FQDN>,ip:
127.0.0.1  -keystore C:\Program Files\APG\.keystore
```

   a. Enter **`changeit`** for the keystore password.

b. When asked for your first and last name, enter the fully qualified name of the machine, for example, **`itops-dev-204.lss.emc.com`**.

c. Answer the other questions and type **`yes`** when asked for confirmation.

If you are using an IP address naming convention for the configuration, run this command and specify the IP address of the EMC M&R host for <*ip:x.x.x.x*>.

```
C:\Program Files\Java\Sun-JRE\8.0.141\bin\keytool.exe -genkey
-alias tomcat -keyalg RSA -ext
SAN=dns:localhost,dns:127.0.0.1,dns:<ip:x.x.x.x> -keystore C:
\Program Files\APG\Web-Servers\Tomcat\Default\conf\.keystore
```

Results

This creates a keystore file inside `C:\Program Files\APG` folder with name `.keystore`.

Windows: Editing the EMC M&R server.xml file

Edit the server.xml file to tell Tomcat server which secure port to use.

Update the `https` connector configuration in `server.xml` in this path, `c:\Program Files\APG\Web-Servers\tomcat\Default\conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file. For example,

```
 <Connector port="58443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
               maxThreads="150" SSLEnabled="true"
scheme="https" secure="true"
               compression="2048"
               clientAuth="false" sslProtocol="TLSv1.2"
URIEncoding="UTF-8"
               sslEnabledProtocols="TLSv1.2" keystoreFile="C:
\Program Files\APG\.keystore"

keystorePass="changeit"

ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" />
```

Configuring SAM environment variables to support SSL

Edit the environment variables in the SAM runcmd_env.sh file to support SSL.

Before you begin

Both SM_CAS_SERVER and SM_TOMCAT_SERVER must be configured to support SSL. The SM_CAS_SERVER environment variable is set to the URL for EMC M&R. The SM_TOMCAT_SERVER environment variable is set to the URL for the SAM Tomcat server.

Procedure

1. Enter the secure port and protocol used to log into EMC M&R in the SM_CAS_SERVER variable. For example, `SM_CAS_SERVER=https://<cas-serverhost>:58443`
2. Enter the secure port and protocol used to log into SAM Tomcat server in the SM_TOMCAT_SERVER variable. For example, `SM_TOMCAT_SERVER=https://<smarts-tomcat-server-host>:8443`

After you finish

Stop and restart the SAM service to make the changes take effect. For example:

```
sm_service stop ic-sam-server-pres
```

```
sm_service start ic-sam-server-pres
```

Windows: Generating the SAM Tomcat server keystore file and certificate

Create the Tomcat server keystore file and certificate.

Before you begin

Generate the keystore file in the home directory where you issue the command.

Procedure

1. Issue the command to generate the keystore file. For example,

   ```
   C:\InCharge\SAM\smarts\jre\bin\keytool.exe -genkey -alias
   tomcat -keyalg RSA
   ```

   To specify a different location or filename, add the `-keystore` parameter followed by the complete pathname to the keystore file. For example,

   ```
   C:\InCharge\SAM\smarts\jre\bin\keytool.exe -genkey -alias
   tomcat -keyalg RSA -keystore C:\InCharge\SAM\smarts\.keystore
   ```

   a. Enter **`changeit`** for the keystore password.

   b. When asked for your first and last name, enter the fully qualified name of the machine, for example, **`itops-dev-204.lss.emc.com`**.

   c. Answer the other questions and type **`yes`** when asked for confirmation.

   If you are using an IP address naming convention for the configuration, run this command and specify the IP address of the SAM host for <*ip:y.y.y.y*>.

   ```
   C:\InCharge\SAM\smarts\jre\bin\keytool.exe -genkey -alias
   tomcat -keyalg RSA -ext SAN=<ip:y.y.y.y> -keystore C:\InCharge
   \SAM\smarts\.keystore
   ```

Results

This creates a keystore file inside `C:\InCharge\SAM\smarts\keystore` folder with name `.keystore`.

Windows: Editing the SAM server.xml file

Edit the server.xml file to tell the SAM Tomcat server which secure port and protocol to use.

Update the `https` connector configuration in `server.xml` in this path, `c:\InCharge\SAM\smarts\tomcat\conf`.

Procedure

1. Uncomment the `https` connector configuration in server.xml.
2. Add the path to the keystore file and the password. For example,

```
 <Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
               maxThreads="150" SSLEnabled="true"
scheme="https" secure="true" keystoreFile="C:\InCharge\SAM
\smarts\keystore"
keystorePass="changeit"
               clientAuth="false"
sslEnabledProtocols="TLSv1.2" />
```

Note

Update the `sslEnabledProtocols`, if you are using different version s of TLS.

Windows: Creating the trust relationship between SAM and EMC M&R

You must export and import certificates to get the SAM Tomcat server and EMC M&R Tomcat server to trust each other.

Before you begin

First, export a certificate on the SAM server. Then import it into the EMC M&R Tomcat server. Then export a certificate from the EMC M&R server and import it into the SAM Tomcat server.

Procedure

1. Export a certificate from the SAM Tomcat server. For example,

```
 C:\InCharge\SAM\smarts\jre\bin\keytool.exe -export -keystore
C:\InCharge\SAM\smarts\keystore -alias tomcat -rfc >  C:
\InCharge\SAM\smarts\SAMtomcat.cert
```

   a. Copy `SAMtomcat.cert` to the host where EMC M&R Tomcat server is installed.

b. Import the `SAMtomcat.cert` into the EMC M&R host. (Copy the files manually using Windows Explorer and CTRL+C and CTRL+V commands.) For example,

```
c:\Program Files\APG>"C:\Program Files\Java\<JDK_version>
\bin\keytool.exe" -import -file "c:\Program Files\APG\
SAMtomcat.cert" -alias SAMtomcat -keystore "C:\Program Files
\APG\.keystore
```

Note

If you see the following warning, type yes and continue :

```
Certificate already exists in keystore under alias <tomcat>
Do you still want to add it? [no]: yes
Certificate was added to keystore
```

c. Back up the original `cacerts` file before this next step.

```
Rename file C:\Program Files\APG\Java\Sun-JRE\8.0.141\lib
\security\cacerts to C:\Program Files\APG\Java\Sun-JRE
\8.0.141\lib\security\cacerts-SAVE    # Backup old cacerts
file
```

d. Copy `.keystore` located at `c:\Program Files\APG\.keystore` to this location, `C:\Program Files\APG\Java\Sun-JRE\8.0.141\lib\security`, and rename it to `cacerts`

2. Restart Tomcat server on the EMC M&R host.

```
/opt/APG/bin/manage-modules.sh service restart tomcat
```

3. Export a certificate from the EMC M&R host. For example,

```
C:\Program Files\APG\Java\Sun-JRE\8.0.141\bin\keytool.exe -
export  -keystore "C:\Program Files\APG\.keystore" -alias
tomcat -rfc > "C:\Program Files\APG\W4Ntomcat.cert"
```

a. Copy `W4ntomcat.cert` to the SAM server host.

b. On the SAM server host, run these commands to import a certificate copied from the EMC M&R server host. (Copy the files manually using Windows Explorere and CTRL+C and CTRL+V commands.)

```
C:\InCharge\SAM\smarts\jre\bin\keywtool.exe -import -file C:
\InCharge\SAM\smarts\ W4Ntomcat.cert -alias W4Ntomcat -
keystore C:\InCharge\SAM\smarts\keystore
```

Note

If you see the following warning, type yes and continue :

```
Certificate already exists in keystore under alias <tomcat>
Do you still want to add it? [no]: yes
Certificate was added to keystore
```

c. Back up the original `cacerts` file before this next step. Rename the `cacerts` file located at `C:\InCharge\SAM\smarts\jre\lib\security\cacerts` to `C:\InCharge\SAM\smarts\jre\lib\security\cacerts-SAVE # Backup old cacerts file`

d. Copy the keystore file from `C:\InCharge\SAM\smarts\keystore` and rename it to `cacerts` at this location `C:\InCharge\SAM\smarts\jre\lib\security\cacerts`

4. Stop and start the Tomcat service on the SAM server:

   a. `c:\InCharge\SAM\smarts\bin\sm_service stop smarts-tomcat`

   b. `c:\InCharge\SAM\smarts\bin\sm_service start smarts-tomcat`

5. Restart the EMC M&R services.

```
c:\Program Files\APG\bin\manage-modules.sh service restart all
```

Configuring Smarts SolutionPack in HTTP mode

If you want to access Smarts SolutionPack in the HTTP mode, perform the following steps:

1. Add the parameter, `SM_CAS_SERVER`, to the `runcmd_env.sh` file in the Presentation SAM server. `SM_CAS_SERVER` is the URL that identifies the EMC M&R Tomcat server host, and it has to specify the protocol and port used to log into EMC M&R. Example: `SM_CAS_SERVER=http://M&R IP:58080`. You must use the `SM_CAS_SERVER` entry to connect to the EMC M&R server. IF M&R was upgraded and was not changed to run on HTTPS, then `SM_CAS_SERVER=http://M&R IP:58080.`

Note

The entries in the Reports configuration screen of the SolutionPack for EMC Smarts must match the values in `SM_CAS_SERVER`. In the example above:

- Set `EMC M&R tomcat hostname or IP address` to `mnrhost.domain.com`
- Ensure `EMC M&R tomcat port number` matches the port specified in `SM_CAS_SERVER` (58080 in the example)
- Ensure the Frontend server in the Physical Overview uses the same naming convention (You must use the FQDN across all field entries.)
- Use the FQDN, not the IP address, for hostnames; otherwise CAS (Central Authentication Service) will not work properly.

2. Set the `SM_TOMCAT_SERVER` parameter in the `runcmd_env.sh` file of the Presentation SAM server to specify the Fully Qualified Domain Name (FQDN) of the SAM Tomcat server. Example: the value for HTTP mode is `SM_TOMCAT_SERVER=http://<hostname.com>:8080`. This `SM_TOMCAT_SERVER` entry must match the name and port values in the **Smarts EDAA host name or IP address** and **Smarts EDAA port number** fields of the Reports configuration block in the SolutionPack for EMC Smarts.
3. In the `/opt/APG/Web-Servers/Tomcat/Default/conf/server.xml` file:
   a. Locate and remove the entry `redirectPort="58443"`
   Before removing the entry `redirectPort="58443"`, it appear as follows:

```
<Connector port="58080" protocol="HTTP/1.1"
connectionTimeout="20000"
compression="2048"/>
redirectPort="58443" URIEncoding="UTF-8" />
```

   After removing the entry `redirectPort="58443"`, it must appear as follows:

```
<Connector port="58080" protocol="HTTP/1.1"
connectionTimeout="20000"
compression="2048"
URIEncoding="UTF-8" />
```

   b. Comment out the following line:

```
<Valve className="com.watch4net.apg.v2.gui.tomcat.ForceSSL" />
```

4. Restart the Tomcat service.
5. Clear the browser cache, and then log in using HTTP.

CHAPTER 2

SolutionPack for EMC Smarts 3.0 Summary Sheet

- Overview 58
- Technical specifications 58
- Where to find the latest SolutionPack software 59
- Configuring Elastic Search 59
- Installation steps 61
- Post-installation steps 67
- Migrating Smarts SolutionPack from Datastore to Elastic Search 71
- Troubleshooting 72

Overview

Learn how to install and configure the SolutionPack for EMC Smarts. This SolutionPack, available with the EMC M&R 6.8u2 platform and later 6.8uX platforms, notifies your operators of real-time network events and displays the root-cause and impact of the event. Historical event data is available as well.

The SolutionPack for EMC Smarts collects performance and availability metrics from your Smarts domain managers and displays them in Dashboard reports.

When the SolutionPack for EMC Smarts is configured to work with Service Assurance Manager, the network operator can view and manage notifications from the EMC M&R Operations interface.

When the SolutionPack for EMC Smarts is configured to work with the IP Configuration Manager, the administrator can maintain IP polling and threshold settings from the EMC M&R Administration interface. The article, *How to Maintain IP Manager Settings*, provides more information.

Technical specifications

SolutionPack version
3.0

Compatible EMC M&R version
6.8u2 and later

Data collection method
Smarts collector

Main reports
Reports display in **Report Library** > **EMC Smarts**.

Events
Lists events from networks monitored by EMC Smarts domain managers.

Domain Manager Health
Provides health-related metrics for networks monitored by EMC Smarts domain managers.

ESM Performance
Provides performance metrics for the EMC Smarts Server Manager.

IP (AM-PM)
Provides availability and performance metrics for IP networks monitored by EMC Smarts domain managers.

ACM Performance
Provides performance metrics for the EMC Smarts Application Connectivity Manager.

Additional reports display in these tabs:

- **Dashboards** > **Network**
- **Explore** > **Network**
- **Operations** > **Network**

By default, the SolutionPack for EMC Smarts uses the Smarts discovery associated with a Presentation Service Assurance Manager (SAM). When you configure the SolutionPack to link to the Presentation SAM server and to its Broker, the SolutionPack connects to the domain managers through the `host:port/DM_name` settings. Notifications from SAM display in the Notification List in the EMC M&R User Interface. Device details from underlying Smarts domain managers connected to that Broker display in other EMC M&R reports.

Alternatively, you may connect the SolutionPack for EMC Smarts directly to the underlying Smarts domain managers.

Here are examples of the statistics collected by the SolutionPack for EMC Smarts:

- IP Availability Manager (AM)/Performance Manager (PM) (statistics on network devices and links)
- Server Performance Manager (SPM)/EMC Server Manager (ESM) (statistics on UNIX and Windows servers, physical and virtual servers and applications)
- Application Connectivity Monitor (ACM) (statistics on transaction response time and availability
- Service Assurance Manager (SAM) (historical view of SAM notifications)
- SAM (real-time view of SAM notifications)

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Configuring Elastic Search

Complete this procedure to configure the Elastic Search.

Before you begin

- Perform M&R 6.8u2 installation successfully.

Procedure

1. Navigate to `/opt/APG/bin/` directory.
2. Open the /etc/sysctl.conf file.
3. Add the following line:

```
vm.max_map_count=262144
```

4. Open the /etc/security/limits.conf file.
5. Add the following line for the user:

In this example, the user is apg.

```
apg hard nofile 65536
apg soft nofile 65536
apg hard nproc 65536
apg soft nproc 65536
```

6. Save the file.
7. To install the Elastic Search cluster package, invoke the following command:

```
./manage-modules.sh install elasticsearch-cluster
```

When you are prompted for the IP address, provide the M&R host IP address. In the **more entries** option, select **no** unless Elastic Search needs to be configured in the cluster mode.

8. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

Following is the output:

```
open files                      (-n) 65536
max user processes              (-u) 65536
```

9. In `/opt/APG/Databases/Elasticsearch/Default/conf/elasticsearch.yml` file, add the following entry:

```
bootstrap.seccomp: false
script.max_compilations_per_minute: 120
```

In `elasticsearch.yml` file, add the above line at the end.

10. Restart Elastic Search server.

    Ensure that, Elastic Search server is running.
11. Create a resource for each newly added elastic search database. Perform this operation every time a new Elastic Search node is added to the environment to scale-out backends.

    For example, to create a database resource:

    In Linux:

```
./manage-resources.sh create dba/ES-RPE2-ARCH '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://<Elastic
Search Server IP>:9200"],"prefix": "/smarts*"},"settings":
{"mapping": "ES-RPE2.xml"},"disabled": false }'
```

In Windows:

```
manage-resources.cmd create dba/ES-RPE3-ARCH
{"type":'elasticsearch',"datasource":"{"hosts":['http://
```

```
<Elastic Search Server IP>:9200'],"prefix":'/
smarts*'}","settings":"{"mapping":'ES-
RPE2.xml'}","disabled":false}
```

Note

You need to specify the IP address for <Elastic Search Server>.

Installation steps

Installing the SolutionPack for EMC Smarts

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Ensure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Service Assurance Suite Installation and Configuration Guide for EMC M&R* for more information.
- If you are upgrading older software components to the latest release, review these recommendations. When upgrading from EMC M&R pre-6.4u1 and Smarts domain managers pre-9.3, follow this upgrade order:
  1. Upgrade Smarts Service Assurance Manager (SAM) to 9.5 or higher and configure SAM with Notification Cache Publishing enabled. This starts the services for Smarts EDAA, Elastic Search and Rabbit MQ. Ensure you also upgrade SAM Console and Smarts domains such as Adapter Platform (OI), MBIM, Trap Receiver/Exploder, and so forth to the latest build. The *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers* provides more information.
  2. Upgrade EMC M&R to 6.8u2 or higher and install the SolutionPack for EMC Smarts 2.2 or higher. The *Service Assurance Suite Installation Guide for EMC M&R* provides information.
  3. Upgrade Smarts IP domains to 9.5 or higher.
  4. Upgrade the remaining Smarts analysis domains that are configured to communicate with the SolutionPack for EMC Smarts.
  5. If Network Configuration Manager (NCM) is part of the deployment, there is no specific upgrade order for NCM. The NCM 9.5 software is backwards compatible with the SolutionPack for NCM and other Smarts domains.
- When upgrading from EMC M&R 6.4u1 and Smarts domain managers 9.3 and higher, follow this upgrade order. (This assumes you have already installed SAM with Notification Cache Publishing enabled and that Smarts EDAA, Elastic Search and Rabbit MQ services have already been configured.)
  1. Upgrade the Presentation Service Assurance Manager to 9.5 first. Then upgrade EMC M&R to 6.8u2. Both deployments need to be upgraded to their latest versions in order for the latest set of features to work.

2. Upgrade Smarts IP domains to 9.5 or higher.
3. Upgrade the remaining Smarts analysis domains that are configured to communicate with the SolutionPack for EMC Smarts.
4. If Network Configuration Manager (NCM) is part of the deployment, there is no specific upgrade order for NCM. The NCM 9.5 software is backwards compatible with the SolutionPack for NCM and other Smarts domains.

- Ensure you have installed and configured the Presentation Service Assurance Manager (SAM) server with Notification Cache Publishing enabled.
- Ensure you have enabled security settings to allow interoperability with EMC M&R by setting these flags in the `runcmd_env.sh` file:

  Table 2 Security settings for the SAM runcmd_env.sh file

Flag	Value
SM_ALLOW_LEGACY_CRYPTO=	TRUE
SM_TLS_PROTOCOLS=	+TLSv1.1

- Ensure these services associated with the Presentation SAM installation are running:

  Table 3 SAM services when Notification Cache Publishing is enabled

Service name	Description of feature
`ic-broker`	Broker connected to Presentation SAM server
`ic-sam-server-pres`	Presentation SAM with Notification Cache Publishing
`smarts-tomcat`	Smarts EDAA and Notification Cache (hosted by Tomcat server)
`smarts-rabbitmq`	Notification Exchange (Rabbit MQ)
`smarts-elasticsearch`	Storage/Search engine used by the Notification Cache

- Obtain the login credentials and the Fully Qualified Domain Names (FQDN) for the servers where Smarts Broker, Smarts EDAA, and Presentation SAM servers are running.
- Review the article, *How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts*, for additional configuration procedures.

Follow these steps to install the SolutionPack for EMC Smarts.

Procedure

1. Log in to **Administration** > **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.
3. Select **SolutionPack for EMC Smarts** in the **Browse and Install SolutionPacks** window.
4. Read the summary information and click **Install**.
5. Accept the default instance name or type a new name.

   One SolutionPack for EMC Smarts instance may be configured for each Presentation SAM server.

6. Select which server each component will be installed on.

   The recommended servers are:

   - Data Collection--Collector
   - Events--Primary Backend
   - Reports--Front End

7. Click **Next** and complete the field entries for the **Data collection**, **Database**, **Events**, and **Reports** screens.

   Click the question mark icon to access field-level help. (Actual screens and version numbers will vary from the examples shown in this article.)

   - Data collection setup when installing SolutionPack for EMC Smarts on page 64
   - Event database when installing SolutionPack for EMC Smarts on page 64
   - Report setup when installing SolutionPack for EMC Smarts on page 65

8. Click **Install** after you complete the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

11. Restart the Presentation SAM services.

    This step is important because the SAM server may have an existing entry in the `runcmd_env.sh` file that points to a previous CAS configuration. Restarting the Presentation SAM services forces the CAS webapp to run with the latest configuration.

After you finish

Perform these post-installation tasks:

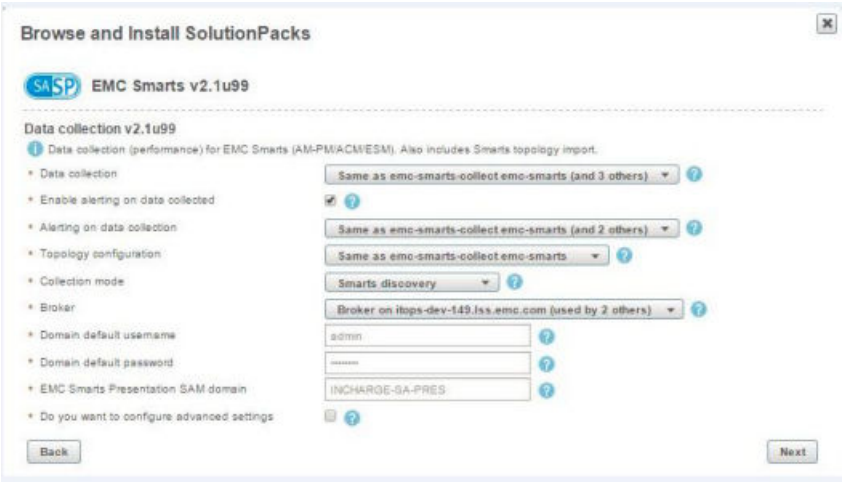
- For Windows environments only, configure the Domain Manager Health collection package. (No additional configuration is required for EMC Smarts domain managers running on Linux platforms.)
- If you chose `MySQL` as the Database Type in the **Events** list box, follow these steps: Enabling event reporting for MySQL database in Smarts SolutionPack on page 67.
- If you chose `Elastic Search` as the Database Type in the **Events** list box, follow these steps, Enabling event reporting for Elastic Search database in Smarts SolutionPack on page 68, and create the Elastic Search database schema.
- Set up non-administrator roles and assign users to these roles.
- Set the default navigation style to **Use tree navigation**. This setting is recommended for the SolutionPacks for the 9.5 release.
- If using the IP Configuration Manager, set the polling and thresholds values. The article, *How to Manage IP Settings*, provides more information.

Data collection setup when installing SolutionPack for EMC Smarts

Accept the default settings or configure custom data collection settings.

- In the **Collection** list box, you can accept the default `Smarts Discovery` option to connect the SolutionPack to the Smarts Broker, Service Assurance Manager, and the underlying Smarts domains. You can filter domains for data collection by selecting, **Do you want to configure advanced settings**.
- If you choose `Smarts collector` instead of `Smarts Discovery`, you can collect topology data from individual Smarts domain managers by configuring their credentials.

Figure 1 Data Collection example



Event database when installing SolutionPack for EMC Smarts

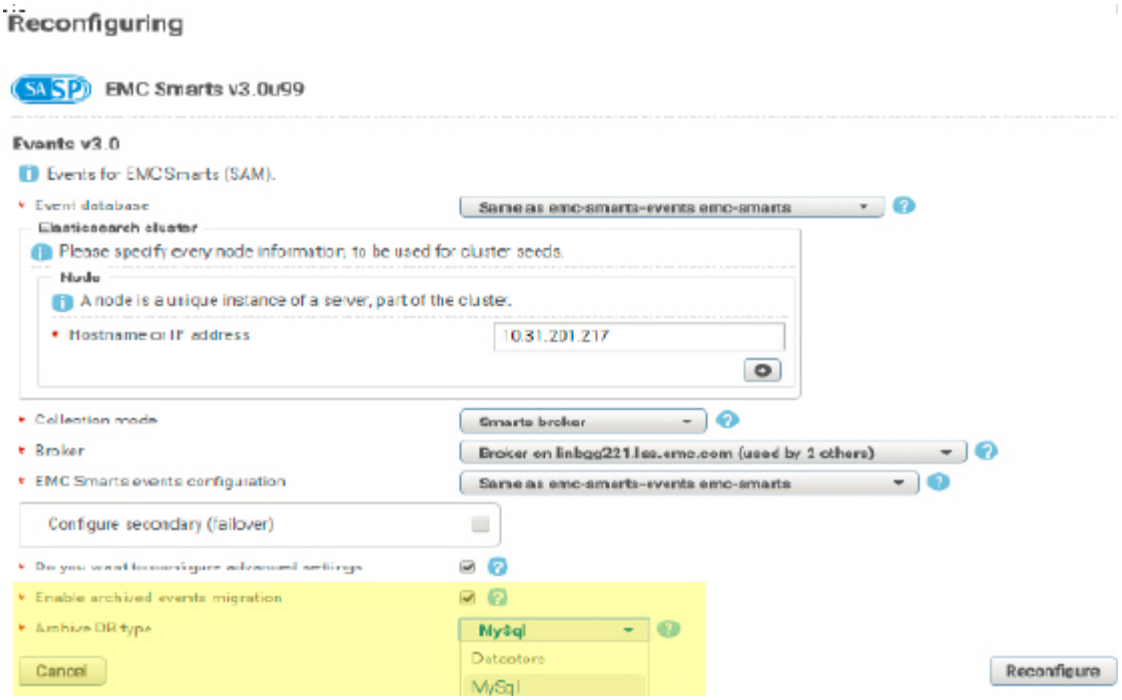
The `MySQL` database can hold both active and inactive (archived) event data. If you choose `Elastic Search` as the Database Type, `MySQL` will still hold active event data, but `Elastic Search` will hold the inactive (archived) event data.

New installations of the SolutionPack for Smarts should choose the `Elastic Search` option as the Database Type. Do not enable the option, **Do you want to configure advanced settings**, because this is used when migrating archived event data and that is not applicable to new installations.

Note

Deployments that used `MySQL` as the Events database in earlier versions of Watch4net may want to use the default `MySQL` entry when updating SolutionPackBlocks. After migration or update processes have successfully completed, you can change the entry to use `Elastic Search` as the database for inactive (archived) events.
If you are updating the SolutionPackBlocks and you choose `Elastic Search` as the Database Type, do not enable the option, **Do you want to configure advanced settings**. First, ensure you have successfully installed the SolutionPack for EMC Smarts and performed the post-installation steps. Then return to the Events setup screen to migrate the event data using the **Do you want to configure advanced settings** option.

Figure 2 Events setup example



Upgrading Smarts SP

To upgrade the Smarts SP to 6.8u2, you must update the Events block.

Procedure

1. Upgrade the M&R platform version from 6.6 or 6.7.
2. From the frontend update the Smarts Solution Pack from Centralized-Management.
3. Update the Events block and select the following options for migration to Elastic Search:
   - Do you want to configure advance settings
   - Enable archived events migration
   - Archive DB type:
     - MySQL
     - DataStore

Report setup when installing SolutionPack for EMC Smarts

In the Report list box, you must specify

- **HTTPS enabled for EMC M&R and Smarts services**—Select the checkbox if you plan to enable the HTTPS mode.
- **EMC M&R Tomcat Hostname**—Enter in the Fully Qualified Domain Name (FQDN) of your EMC M&R Frontend server. For example, if your EMC M&R Frontend server is at `https://example.com:58443/APG`, type, `www.example.com` here.
  - Ensure you added the parameter, `SM_CAS_SERVER`, to the `runcmd_env.sh` file in the Presentation SAM server. The hostname portion of the URL entry for `SM_CAS_SERVER` has to match the hostname in the **EMC M&R Tomcat**

Hostname field. Use only the Fully Qualified Domain Name (FQDN). Do not use the IP address.

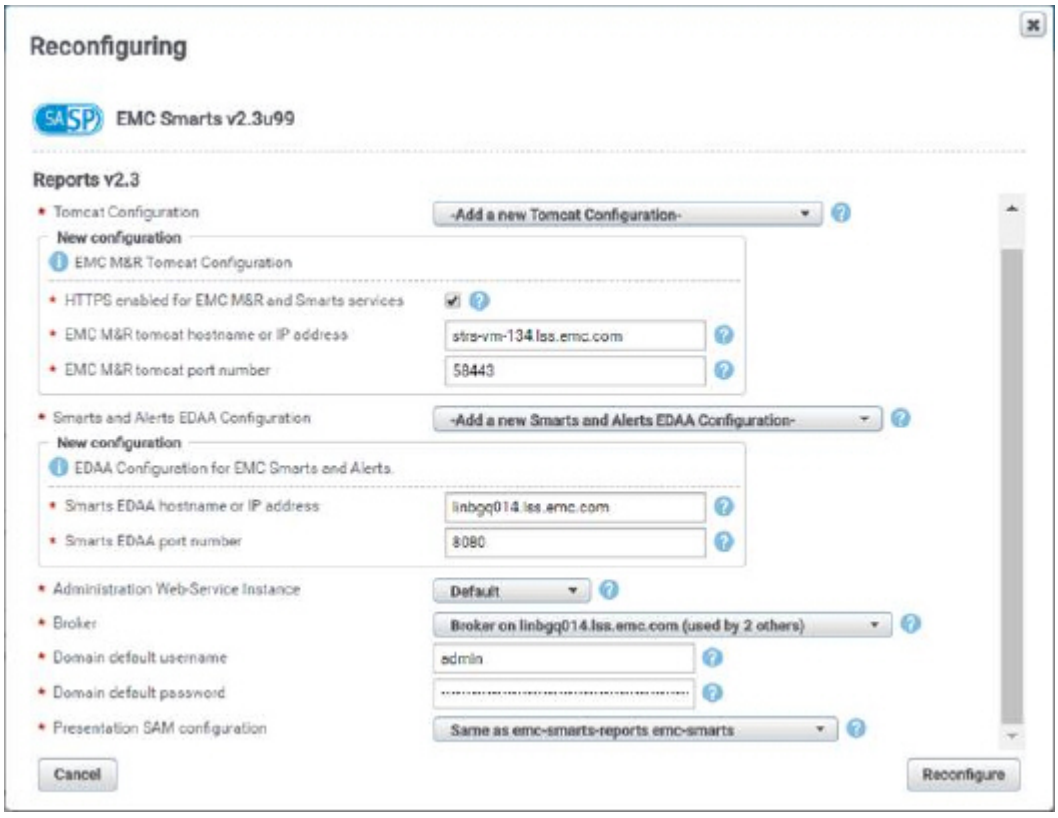
Note

Depending on the server configuration, the EMC M&R tomcat may run in HTTPS port 58443 or in HTTP mode port 58080. If you have upgraded and followed the procedure in the SSL setup for SAM and EMC M&R on page 41 to switch back to HTTPS mode.

- **Smarts EDAA hostname or IP address**—Enter the Fully Qualified Domain Name (FQDN) of your EMC Smarts EDAA Hostname. For example, if your EMC Smarts EDAA Hostname is at `https://www.example.com:8443/`, type `www.example.com` here.
- **Presentation SAM configuration**—Type the name of the Presentation SAM Server that was started with the Notification Cache Publishing option. (This is the domain name, such as `INCHARGE-SA-PRES`. Do not enter the service name, such as `ic-sam-server-pres`.)
- **Use Smarts Configuration Manager**—Select this checkbox if you plan to use EMC M&R and the SolutionPack for EMC Smarts to manage IP Settings such as polling and thresholds. Specify the name of the Configuration Manager in the Configuration Manager field if it does not use the default name. If you are enabling this feature after you have already installed the SolutionPack for EMC Smarts, click **Reconfigure** to apply the new settings.

If you enabled the security configuration checkbox (`HTTPS enabled for Watch4net and Smarts`), you must adjust the port settings to reflect your security configuration.

Figure 3 Report setup example



Post-installation steps

Database types for storing event data

Complete the post-installation configuration steps for the type of database (MySQL or Elastic Search) that holds the archived event data.

Depending upon which Database Type you choose, you must enable event reporting in order for your reports to point to the correct database. If you switch from one database to another after you install the SolutionPack, you must adjust the configuration so the reports will continue to display archived event data properly.

- If you choose MySQL as the Database type, follow instructions in this topic: Enabling event reporting for MySQL database in Smarts SolutionPack on page 67
- If you choose Elastic Search as the Database type, follow instructions in these topics: Enabling event reporting for Elastic Search database in Smarts SolutionPack on page 68.

Enabling event reporting for MySQL database in Smarts SolutionPack

If you chose the MySQL database to store archived events in, you must enable event reporting.

Run these commands once after a new installation. Do not run these commands after an upgrade or reconfiguration.

Procedure

1. For Linux, execute these commands from the `APG/bin` directory:

```
#./manage-resources.sh update dba/FLOW-RPE2-ARCH
'{"disabled":true}'
#./manage-resources.sh update dba/FLOW-RPE2-LIVE
'{"disabled":false}'
```

2. For Windows, execute these commands from the APG\bin folder:

```
manage-resources.cmd update dba/FLOW-RPE2-ARCH
{"disabled":true}
manage-resources.cmd update dba/FLOW-RPE2-LIVE
{"disabled":false}
```

3. Restart the Tomcat service in order to make the changes effective

Enabling event reporting for Elastic Search database in Smarts SolutionPack

If you chose the Elastic Search database to store archived events in, you must enable event reporting.

Run these commands once after a new installation. Do not run these commands after an upgrade or reconfiguration.

Procedure

1. For Linux, execute these commands from the `APG/bin` directory:

```
#./bin/manage-resources.sh update dba/FLOW-RPE2-ARCH
'{"disabled":false,"datasource":
{"driverClassName":"com.watch4net.x100.jdbc.Driver","validatio
nQueryTimeout":null,"username":"admin","password":"
{65901E8A34371DBC8627A4FC9B5DCD30FB83529BB380BB6670FB3D0F1E33B
9CD114922FC7713361287955791DD0C6EBA}","url":"jdbc:x100://
localhost:48443/Databases/APG-Datastore/Default"}}'
./bin/manage-resources.sh update dba/FLOW-RPE2-LIVE
'{"disabled":false}'
```

2. For Windows, execute these commands from the `APG\bin` folder:

```
manage-resources.cmd update dba/FLOW-RPE2-ARCH
{"disabled":false,"datasource":
{"driverClassName":'com.watch4net.x100.jdbc.Driver','validatio
nQueryTimeout":null,"username":'admin','password':'
{65901E8A34371DBC8627A4FC9B5DCD30FB83529BB380BB6670FB3D0F1E33B
9CD114922FC7713361287955791DD0C6EBA}
','url':'jdbc:x100://localhost:48443/Databases/APG-Datastore/
Default'}}
manage-resources.cmd update dba/FLOW-RPE2-LIVE
{"disabled":false}
```

3. Restart the Tomcat service in order to make the changes effective

Configure icStats helper for EMC Smarts health collection

Additional configuration is required to enable Smarts Health data collection for EMC Smarts domains running on Windows. Metrics for the processor, memory, and other domain information cannot be collected until icStats helper is set up.

EMC Smarts health collection is now part of the emc-smarts-collect package, installed as part of the SolutionPack for EMC Smarts.
Configure the icStats helper for EMC Smarts domains running on Windows platforms. (No additional configuration is required for EMC Smarts domains running on Linux platforms.)

Procedure

1. Obtain `plist.exe` from http://technet.microsoft.com/en-us/sysinternals/bb896682.aspx
2. Install `plist.exe` in the PATH statement for each Windows host.

Set role restrictions for non-administrator users of SolutionPack for Smarts

If you want additional user roles, such as oper (operator), or profiles configured in your Presentation SAM server, you must set role restrictions after installing the SolutionPack for Smarts.

The default role is assigned to administrator. Add additional roles as needed.

Procedure

1. From **Administration** > **Roles**, click **New Role**.
2. Click **Modules & Restrictions Access** and expand the **Smarts** module.
3. Add an existing smarts profile (such as `oper-profile` or `default-profile`) and click **Save**.
4. From **Administration** > **Users**, create a new user and assign a role to the new user.

   You can assign one or more roles to a new user.

   Note

   Notification actions (like Acknowledge/Unacknowledge, Take/Release Ownership, and so on) in the Notifications view are available for a user who is assigned multiple roles that have the same sam-profiles. Notification actions are not available for a user who is assigned multiple roles that have different sam-profiles.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Set default navigation style

The navigation style controls the look and feel of the left navigation column in the reporting interface.

This procedure sets the global default navigation style. Users can override the global default style for their user account on **Profile** > **View Profile** > **Preferences**.

Procedure

1. Click **Administration** > **Portal**.
2. Click the **Default Display** tab.
3. In **Navigation Style**, make a selection.

Option	Description
Use icon navigation	The navigation column contains icons that expand into reporting categories
Use tree navigation	The navigation column is a hierarchical tree of report names

4. Click **Save**.

Hide unused entries in the navigation tree

You can hide default entries in the navigation tree if you have not installed the products that populate them with data.

Before you begin

The default EMC M&R platform displays nodes such as **Operations**, **Explore**, **Dashboards**, and **Planning** in the navigation tree. Other product suites that also use EMC M&R as their platform display entries under these nodes by default. However, no data populates these entries unless you are using those products. The SolutionPack for EMC Smarts populates data in the **Network** block under **Operations**, **Explore**, and **Dashboards**.

Procedure

1. To hide entries in the navigation tree, click **Edit Mode** from the EMC M&R User Interface.
2. Find the storage-related blocks in the list and select, **Always Hide**.

   Do not hide the **Network** block under the **Operations**, **Explore**, or **Dashboards** nodes. The **Network** block contains all of the SolutionPack for EMC Smarts views and reports. The **Planning** node is not used by the SolutionPack for EMC Smarts.

Migrating Smarts SolutionPack from Datastore to Elastic Search

To migrate from previous database to the new database, you must perform the following steps:

Before you begin

- Install and configure previous M&R version. For example, install and configure 6.7u1.
- Configure 6.7u1 for Smarts SP CDR/CMR configurations. Verify CallOverview reports are present.
- Download the latest M&R build. The *Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides more information.
- Install the M&R, by invoking the following command:

```
sh setup-linux-x86_64-v95.sh
```

- To upgrade the platform, install the new packages in:

```
/opt/APG/Tools/Module-Repository [Y/n]? Y
/opt/APG/bin/manage-modules.sh update module-manager
/opt/APG/bin/manage-modules.sh service update all
/opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
```

- Configure the Elastic Search, see Configuring Elastic Search on page 59 for more information.
- Restart Elastic Search server. Ensure Elastic Search server is running.

Procedure

1. Update the Smarts package.
2. Update the Smarts versions from SolutionPacks.
3. Update the post install procedure.
4. Manually create the schema for the CDR database, you have to create the following **FLOW-RPE2** resource for the tomcat server to enable the connection to the CDR database.

   On Linux:

```
./bin/manage-resources.sh create dba/ES-RPE2-ARCH '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://<Elastic
Search Server IP>:9200"],"prefix": "/cdr*"},"settings":
{"mapping": "ES-RPE2.xml"},"disabled": false }'
```

   On Windows:

```
APG PATH\bin\manage-resources.cmd create dba/ES-RPE3-ARCH
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
<Elastic Search Server IP>:9200"],"prefix": "/
cdr*"},"settings": {"mapping": "ES-RPE2.xml"},"disabled":
false }'
```

5. Delete "dba/FLOW-RPE2" table from manage-resources list.
6. Restart the Tomcat service.
7. Restart the Elastic Search server.
8. Stop the event processing manager service for emc-smarts.
9. Run the data-migration task which is enabled for run, see the Scheduling the Event-Processing Tasks on page 72 for more information.
10. Verify the Event Processing for `smarts*`, CDR records are read and processed.
11. Ensure from Elastic Search, that data is flowing.
12. Add new CDR records and verify new CallOverview reports are also fetched.

Scheduling the Event-Processing Tasks

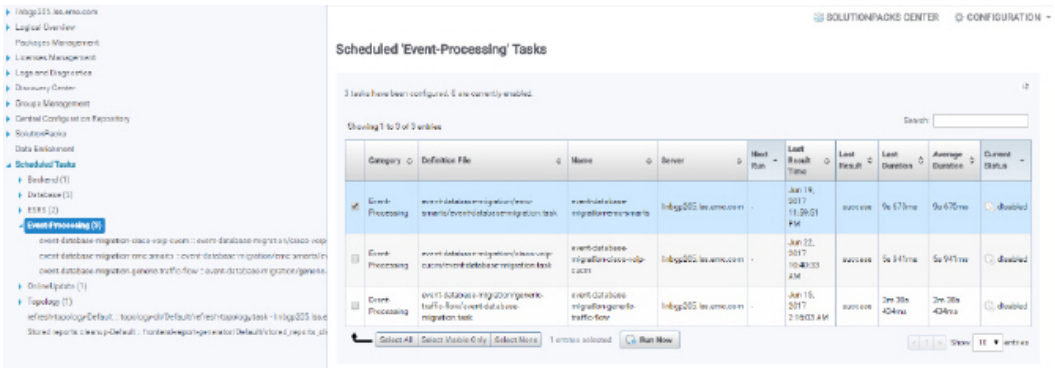
You need to configure the event processing task, in order to run the data-migration task which is enabled for run.

Procedure

1. On the EMC M&R Console, navigate to **Centralized Management** > **Scheduled Tasks** .
2. Click **Event-Processing**.

   The scheduled event-processing tasks appears in the right pane.
3. Select the event processing task.

   Figure 4 Scheduled Event-Processing example



4. Click **Run Now**, to run the data-migration task which is enabled for run.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Generating and downloading diagnostic files

Diagnostic files are a collection of system configuration files and log files that can help in researching problems.

Procedure

1. Go to **Administration** > **Centralized Management** > **Logs and Diagnostics** > **Diagnostic Files**.
2. Click **Generate diagnostic files**.

   This action generates a zip file of XML, CSV, properties, script, and java files that define your current configuration and implementations. Some log files are also included.

   When generation is completed, a **Download** button appears.
3. Click **Download** to access the `.zip` file.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation

If you want to access M&R 6.8u2 in the HTTP mode, complete the following steps:

Note

When you install M&R 6.8u2, by default it is installed in the HTTPS mode.

Procedure

1. In the `/opt/APG/Web-Servers/Tomcat/Default/conf/server.xml` file:
   a. Locate and remove the entry `redirectPort="58443"`.
   Before removing the entry `redirectPort="58443"`, it appear as follows:

   ```
   <Connector port="58080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   compression="2048"/>
   redirectPort="58443" URIEncoding="UTF-8" />
   ```

   After removing the entry `redirectPort="58443"`, it must appear as follows:

   ```
   <Connector port="58080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   compression="2048"
   URIEncoding="UTF-8" />
   ```

   b. Comment out the following line:

   ```
   <Valve
   className="com.watch4net.apg.v2.gui.tomcat.ForceSSL" />
   ```

2. Restart the Tomcat service.
3. Clear the browser cache, and then log in using HTTP.

CHAPTER 3

Troubleshooting the Deployment of SAM, EMC M&R and the SolutionPack for EMC Smarts

- Overview 78
- Log files 78
- Status checks on services 79
- Unable to access Smarts EDAA 82
- Notification cache is empty 82
- Stale alerts and messages appear in Notification cache 84
- Troubleshooting notification list errors 85
- Troubleshooting an empty notification list 85
- Troubleshooting Notification view popouts 85
- RabbitMQ does not start 85
- Tomcat does not start 86
- Tomcat starts but then stops 86
- Changing the password of the EDAA account 86
- How do I change the RabbitMQ passwords 87
- UI cannot display alerts or Smarts topology when CAS is enabled 90
- Wrong CAS host name in runcmd_env.sh 90
- Services remain registered and running after an uninstall 91
- Retrieving the current elasticsearch PID 93
- Multi-sort option not working after clicking on Notification column title 93
- Ports that must be open between SAM and EMC M&R 93

Overview

Use this article to help you find solutions to issues you may have with SAM, the EMC M&R platform, and the SolutionPack for Smarts.

Log files

Log files help you diagnose issues that you may have with SAM, the EMC M&R platform, and the SolutionPack for EMC Smarts.

SAM log files

The SAM log file names may differ depending on the domain name. You can find these log files in `SAM/smarts/local/logs`.

brstart_en_US_UTF-8.log

Created by the Smarts broker.

emc-alerts-es.log

Created by the elasticsearch service. The Notifications cache uses elasticsearch to store and index its notifications to be served by the Alerts EDAA.

INCHARGE-SA-PRES.audit

The SAM audit log.

INCHARGE-SA-PRES_en_US_UTF-8.log

The SAM server log. In this case, the log's name represents the INCHARGE-SA-PRES domain.

rabbit@<*HOSTNAME*>.log

Created by the RabbitMQ service. The Notification cache uses the RabbitMQ service to transfer notifications from SAM to the Notification cache. This log file name depends on the host name of the SAM installation.

setup_elasticsearch.log

Created the first time you run the elasticsearch service. This service must be primed the first time it is run, and this log records the setup results.

setup_rabbitmq.log

Created the first time that you run the RabbitMQ service. This service must be primed the first time it is run, and this log records the setup results.

sm_serviced_en_US_UTF-8.log

Created by the sm_serviced daemon process that is responsible for running the registered Smarts services.

Tomcat log files

These log files are generated by Tomcat and any web applications running within Tomcat. You can find these log files in `SAM/smarts/local/logs/tomcat`.

alerts-edaa.log

Created by the Alerts EDAA web application. This web application exposes notifications in the Notification cache.

alerts-ingestion.log

Created by the alerts-ingestion web application. This web application populates notifications in to the Notification cache that come from SAM via RabbitMQ.

catalina.<*date*>.log

The Tomcat engine writes log messages pertaining to Tomcat.

catalina.out

Logs the code output running under Tomcat. This output is also written to System.out or System.err.

localhost.<*date*>.log

Logs information about the virtual host within Tomcat. Always check this log if you cannot find an error in catalina.out or if something is seriously wrong.

localhost_access_log.<*date*>.txt

Logs the calls being made to the Tomcat server.

smarts-edaa.log

Created by the smarts-edaa web application. This web application exposes the topology from one or more domain managers in a RESTful feed.

Status checks on services

You can verify that the services are running and performing their required tasks.

Perform status checks on services by following these procedures:

- Checking elasticsearch on page 79
- Checking the notifications exchange on page 80
- Checking the RabbitMQ configuration on page 80
- Checking Alerts EDAA on page 81
- Checking Smarts EDAA on page 81

Checking elasticsearch

The elasticsearch service, a component of the Notifications cache, is only accessible from the local machine. Verify this service is running and serving requests.

Procedure

1. Verify elasticsearch is running by typing `$ smarts/bin/sm_service show`.

   The expected result is: RUNNING smarts-elasticsearch

2. Verify elasticsearch is serving requests from a browser on the same machine on Windows or using a tool like curl on Linux.

   Browser example:

   ```
   http://localhost:9200/_status
   ```

   A page specific to the browser appears.

   Linux examples:

   ```
   curl -XGET http://localhost:9200/_status
   curl http://localhost:9200/smarts/alert/_count
   ```

A JSON page appears indicating success and showing Smarts as one of the indices. For example:

```
"_shards":{"total":10,"successful":5,"failed":0}
.
.
.
"indices":{"smarts":...
```

3. If the Smarts index does not exist, the setup script has failed. Check the `setup_elasticsearch.log` file. Note that after you first start elasticsearch, it may take a few minutes before the setup script begins running.

Checking the notifications exchange

The RabbitMQ service exchanges notifications from SAM to the Notification cache. This service is running by default and is a password-protected web-based management interface running on port 15672.

Procedure

1. Verify RabbitMQ is running: **`http://<HOSTNAME>:15672/`**
2. Type the credentials for the RabbitMQ interface. The default values are **`admin`** for the user and **`changeme`** for the password.

   The main page shows various statistics and status information for RabbitMQ.

Checking the RabbitMQ configuration

Follow these steps to check if the RabbitMQ service was properly configured.

When you start the `sm_rabbitmq` script, it verifies the RabbitMQ configuration and creates the required exchanges, queues, users, and priming message in `qnameq` if they do not exist. If this script fails, check the `local/logs/setup_rabbitmq.log` file.

Procedure

1. Log in to the RabbitMQ interface: **`http://<HOSTNAME>:15672/`**
2. Type the credentials for the RabbitMQ interface. The default values are **`admin`** for the user and **`changeme`** for the password.
3. Verify these exchanges are under the **Exchanges** tab:
   - `emc.smarts.notifications` (of type topic)
   - `emc.smarts.notifications.ingestion` (of type x-consistent-hash)
4. Verify these queues are under the **Queues** tab:
   - `emc.smarts.notifications.q1`, the main queue for holding notifications for ingestion
   - `emc.smarts.notifications.qnameq`

   If a high number of messages appear under `emc.smarts.notifications.q1`, ingestion is either backlogged or has stopped.

   One message should appear under `emc.smarts.notifications.qnameq`.

5. Verify these users are defined under the **Admin** tab, and have access to the emc.smarts.notifications vhost:
   - admin (with the administrator tag)
   - ingestion
   - publisher

Checking Tomcat

Verify Tomcat is running and serving requests.

Procedure

1. Verify Tomcat is running by typing `$ bin/sm_service show`.

   The expected result is: RUNNING smarts-tomcat
2. Verify Tomcat is serving requests from a browser: `http://<HOSTNAME>:8080/`

   A welcome page for Tomcat Version 8.x appears.

Checking Alerts EDAA

Verify the Alerts EDAA, a component of the Notification cache, is running and connected to elasticsearch.

Procedure

1. Verify Tomcat is running, as described in Checking Tomcat on page 81.
2. Verify `alerts_edaa` is running.

   For example:

   ```
   http://itops-qa-192.lss.emc.com:8080/alerts-edaa/msa?
   alt=json&pretty=true
   ```
3. Make sure there is an entry for alerts on the page.
4. Check that the cache is connected to the elasticsearch service and has the expected notifications.

   For example:

   ```
   http://itops-qa-192.lss.emc.com:8080/alerts-edaa/msa/
   alerts/instances?alt=json&pretty=true
   ```

Checking Smarts EDAA

Verify the Smarts EDAA is running, connected to the broker and is able to retrieve information from your presentation SAM.

Procedure

1. Verify Tomcat is running, as described in Checking Tomcat on page 81.
2. Verify `smarts-edaa` is running.

   For example:

   ```
   http://itops-qa-192.lss.emc.com:8080/smarts-edaa/msa?
   alt=json&pretty=true
   ```
3. Make sure there are entries for the dmbroker and the presentation SAM.
4. Verify `smarts-edaa` is connected to the broker.

For example:

```
http://itops-qa-192.lss.emc.com:8080/smarts-edaa/msa/
dmbroker/types/DomainManager/instances?
alt=json&pretty=true
```

5. Make sure there are entries for the various domains registered with the broker.
6. Verify `smarts-edaa` can retrieve information from your presentation SAM.

   For example:

   ```
   http://itops-qa-192.lss.emc.com:8080/smarts-edaa/msa/
   INCHARGE-SA-PRES/instances/SM_System::SM-System?
   alt=json&pretty=true
   ```

7. Make sure you can see the properties of `SM_System::SM-System`.

Unable to access Smarts EDAA

If your system cannot access Smarts EDAA, follow these steps.

Procedure

1. Verify the SAM server is not using a broker from a pre-9.4 Smarts installation.
2. Verify the SAM broker is configured for Smarts EDAA access:
   <*SAM_base_directory*>/SAM/smarts/bin> dmctl -s localhost:426/dmbroker getI EDAAService

   The expected result is: `SMARTS-EDAA`
3. If you made configuration changes to the broker or SAM using the `runcmd_env.sh` file, do the following in this order:
   a. Shutdown SAM.
   b. Shutdown Tomcat.
   c. Shutdown the broker.
   d. Restart the broker.
   e. Restart Tomcat.
   f. Restart SAM.

Notification cache is empty

Follow these steps when notifications are not appearing in the Notification cache.

Before you begin

Review this before you start the troubleshooting steps.

- If alerts show up in the Alerts EDAA but not in EMC M&R, the issue is in EMC M&R.
- If you see a backup of messages in RabbitMQ, the SAM publisher is working but the ingestion service or elasticsearch service may be failing.
- If no messages are passing through into RabbitMQ, the problem is on the SAM publisher side.

Procedure

1. Verify all services are running, as described in Status checks on services on page 79.
2. Check that SAM has started to publish to RabbitMQ and started with `--bootstrap=bootstrap-amqp.conf`.
3. Verify SAM is exposed via the EDAA and started with `--edaa=sam-presentation/2.0`.
4. Under the **Connections** tab in the RabbitMQ web-based management interface, do the following:
   a. Verify that there are two connections: one from RabbitMQ / Java and the other from rabbitmq-c.
   b. If RabbitMQ / Java is not present, check if Tomcat is running and view the `<SAM_base_directory>/SAM/smarts/local/logs/tomcat/alert-ingestion`.
   c. If rabbitmq-c is not present and if SAM is running, check the presentation SAM log to see if it is publishing to RabbitMQ.
5. From the host running the presentation SAM server, check if you can access the elasticsearch database and verify the count from a browser on Windows or using a tool like curl on Linux.

   Browser example:

   `http://localhost:9200/smarts/alert/_count`

   Linux example:

   `curl http://localhost:9200/smarts/alert/_count`

   A result similar to this appears:

   `{"count":50002,"_shards":{"total":5,"successful":5,"failed":0}}`
6. If the count is zero, check if there are any notifications in SAM.
7. From a browser, check if you can access Tomcat in the SAM server host.

   For example:

   `http://hostname:8080`
8. Verify elasticsearch is running by checking `<SAM_base_directory>/SAM/smarts/local/logs/tomcat/alert-ingestion.log`

   If the service was running and is now shut down or unable to process notifications, a message similar to this may appear in the `alerts-ingestion.log` file:

```
{date} {time},{pid} INFO  'ALERTS-IN' EventConsumerService
EventConsumerPool-1 watchdog attemps to reconnect
 {date} {time},{pid} INFO  'ALERTS-IN' plugins
EventConsumerPool-1 [La Lunatica] loaded [], sites [] {date}
{time}
 {date} {time},{pid} ERROR 'ALERTS-IN'
ElasticsearchNodeConfigurationService EventConsumerPool-1
 ElasticSearchNodeConfigurationService::verifyIndexing:
ElasticSearch :

SERVICE_UNAVAILABLE :org.elasticsearch.client.transport.NoNode
```

```
AvailableException: No node available
 {date} {time},{pid} INFO  'ALERTS-IN' transport
elasticsearch[Ent][generic][T#8] [Ent] failed to get node
info for [#transport#-1][inet
 [localhost/127.0.0.1:9300]], disconnecting...
 org.elasticsearch.transport.NodeDisconnectedException: []
[inet[localhost/127.0.0.1:9300]][cluster/nodes/info]
disconnected
```

Stale alerts and messages appear in Notification cache

If the Notification cache contains stale alerts and messages, you can synchronize SAM and the Notifications cache. This happens when you restart SAM with a different RPS file.

You have two options to synchronize SAM and the Notification cache:

- Stopping the SAM publisher to clear the Notification cache on page 84. This is the recommended option because it has low impact on the system.
- Stopping SAM to clear the Notification cache on page 84.

Stopping the SAM publisher to clear the Notification cache

This method of clearing the Notification cache has less impact on the system because you are only stopping the SAM publisher.

Procedure

1. Stop the publisher: **`$ bin/dmctl -s INCHARGE-SA-PRES invoke SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher stop`**
2. Clear the Notifications cache by typing these commands:
   a. **`$ bin/sm_service stop smarts-elasticsearch`**
   b. **`$ rm -rf local/repos/emc-alerts-es`**
   c. **`$ bin/sm_service start smarts-elasticsearch`**
3. Restart the publisher: **`$ bin/dmctl -s INCHARGE-SA-PRES invoke SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher start`**

Stopping SAM to clear the Notification cache

This method of clearing the Notification cache has a substantial impact on the system.

Procedure

1. Stop SAM: **`$ bin/sm_service stop ic-sam-pres`**
2. Clear the Notifications cache by typing these commands:
   a. **`$ bin/sm_service stop smarts-elasticsearch`**
   b. **`$ rm -rf local/repos/emc-alerts-es`**
   c. **`$ bin/sm_service start smarts-elasticsearch`**
3. Restart SAM: **`$ bin/sm_service start ic-sam-pres`**

Troubleshooting notification list errors

Notifications are not visible in the EMC M&R user interface. "MSAException" and "Map is showing HTTP Error" messages display.

Check the `/etc/hosts` file in the Presentation SAM server. If the `/etc/hosts` file does not list the Fully Qualified Domain Name of the EMC M&R host, these errors will display.

Add the entry in the `/etc/hosts` file and restart all SAM services.

Troubleshooting an empty notification list

After creating a new Notification List in Service Assurance Manager, the notifications are not visible in the EMC M&R User Interface.

When you create a new Notification List in Service Assurance Manager, you must issue this command to have notifications populate the correct reports in EMC M&R. This command ensures notifications are re-cached so they display in the correct Notification List.

Issue this command from the Presentation Service Assurance Manager <*install_directory*>\SAM\smarts\bin folder: `dmctl> invoke ICS_NLManager::ICS-NLManager renotifyAllEvents`

Troubleshooting Notification view popouts

The popout option that was formerly available under the gear tool for the Notification report is not available.

Select **View in Full Page** under the Display option in the EMC M&R user interface. This opens the Notification report in a new window.

RabbitMQ does not start

Follow these steps to determine why the RabbitMQ service does not start.

Procedure

1. Verify RabbitMQ is NOT already running by typing **`sm_service show`**.
2. Verify the `Erlang` process is NOT running by typing **`ps -ef | grep erl`**.
3. If the Erlang process is running, kill it before restarting RabbitMQ.

   The Erlang process may be running from a prior installation, or was started outside the `sm_service` mechanism.
4. Verify the `qpidd` process is NOT running by typing **`ps -ef | grep qpidd`**.
5. If the `qpidd` process is running, kill it before restarting the RabbitMQ service.

   The `qpidd` process runs on some Linux distributions and can conflict with RabbitMQ by using the same port.
6. Check that no other RabbitMQ installation exists by typing **`ps -ef | grep rabbit`**.

Tomcat does not start

Follow these steps to determine why Tomcat does not start.

Procedure

1. Verify that Tomcat is NOT already running by typing **`sm_service show`**.

   Tomcat may be running from a prior install, or was started outside of the `sm_service` mechanism. Also, another instance of Tomcat or another web server may be running on the system that prevents this Tomcat instance from binding to port 8080, causing it to shut down.

2. Verify the underlying application is not already running Tomcat by typing **`ps -ef | grep java`**.

   If you see that the `/opt/InCharge/SAM/smarts/tomcat/bin/bootstrap.jar` process is running, then Tomcat is likely running as well.

3. Review the messages in `SAM/smarts/local/logs/tomcat/catalina.out` and `SAM/smarts/local/logs/tomcat/catalina.<date>.log`.

Tomcat starts but then stops

Procedure

1. Follow the steps in Tomcat does not start on page 86
2. Check if another process is running on port 8080.

   This can cause Tomcat to start for a few minutes and then return to a NOT RUNNING state.

Changing the password of the EDAA account

The Smarts EDAA logs into domains using the EDAA account `_edaa`. This account has the same access privileges as the admin account as well as the ability to perform actions on behalf of other users. To secure this account, change its default password, which is changeme.

Procedure

1. In the install directory of each domain server accessed by Smarts EDAA, type `sm_edit conf/serverConnect.conf`

   By default, only presentation SAM is exposed.

2. In the `serverConnect.conf` file, change the encrypted default password for the `_edaa` account.

   For example, you can change this password:

```
*:_edaa:<E-1.0>94C355DA7E0EB7AADE32F80F201F70C5CCA88288443EE23
CB5249ACD10C773E1:Impersonate
```

to the new password:

```
*:_edaa:<new_password>:Impersonate
```

When you save the `serverConnect.conf` file, `sm_edit` encrypts the new password.

3. In the install directory of the SAM server hosting the Smarts EDAA, type `sm_edit conf/edaaClientConnect.conf`
4. In the `edaaClientConnect` file, change the encrypted default password for the `_edaa` account.

   For example, you can change this password:

```
*:*:_edaa:<E-1.0>94C355DA7E0EB7AADE32F80F201F70C5CCA88288443EE
23CB5249ACD10C773E1
```

   to the new password:

```
*:*:_edaa:<new_password>
```

   When you save the `edaaClientConnect` file, `sm_edit` encrypts the new password.

5. Stop the Smarts Tomcat hosting the Smarts EDAA by typing `bin/sm_service stop smarts-tomcat`.
6. Restart the Smarts Tomcat hosting the Smarts EDAA by typing `bin/sm_service start smarts-tomcat`.
7. Verify that the Smarts EDAA can access each domain.

How do I change the RabbitMQ passwords

There are three default accounts in the RabbitMQ installation: an admin account, an account used by the SAM publisher to deliver messages into RabbitMQ, and an account used by the ingestion process to pull messages from RabbitMQ. You can change the password for each one of these accounts.

Follow these procedures to change the passwords of the RabbitMQ accounts:

- Changing the RabbitMQ admin password on page 87
- Changing the RabbitMQ publisher password on page 88
- Changing the RabbitMQ ingestion password on page 89

Changing the RabbitMQ admin password

The RabbitMQ admin account is used for configuring RabbitMQ and accessing RabbitMQ's web-based management interface. It is not used by any other component of the system except for the initial RabbitMQ setup process.

Procedure

1. Make sure the smarts-rabbitmq service was started.

2. To access the RabbitMQ web-based management interface, connect with a browser to port 15672 on the host where RabbitMQ is installed.

   For example:

   `http://my-pres-sam-host.example.com:15672/`
3. Log in as **`admin`** using the default password of **`changeme`**.
4. If this is the first time RabbitMQ was started, make sure the first-time setup has completed before continuing, as explained Checking the RabbitMQ configuration on page 80. The setup process uses the default `admin/changeme` login credentials to make changes to RabbitMQ.
5. Click the **Admin** tab and select **admin** from the list of RabbitMQ login users.
6. Click **Update this user**.
7. Type the new password in both password fields. Do not change the **Tags** field.
8. Click **Update User**.

   A message appears indicating the login failed. This is because you changed the password for the user that is currently logged on, making the password invalid.
9. Click **Log Out**.

   A new login form appears.
10. Type **`admin`** and the new password to confirm the password was successfully changed.

Changing the RabbitMQ publisher password

The publisher is a component in the presentation SAM domain that sends notifications into RabbitMQ. The RabbitMQ login for this process is `publisher` with the default password of `changeme`. To change this password, you must update both RabbitMQ and the SAM configuration with a new matching password.

Procedure

1. Log in to the RabbitMQ web-based management interface as **`admin`**.
2. Click the **Admin** tab and select **publisher** from the list of RabbitMQ login users.
3. Click **Update this user**.
4. Enter the new password in both password fields.
5. Click **Update User**.
6. To change the password in the SAM configuration:
   a. Log in to the host where the presentation SAM is installed.
   b. Type **`sm_edit conf/clientConnect.conf`**.
   c. In the `clientConnect.conf` file, look for a line beginning with `AMQP/*`

      It is similar to this:

      ```
      *:AMQP/
      *:publisher:<E-1.0>94FF41842043EDA1DE6E67FB08015B3D456752865
      F8B5D7DC63F259270B36092
      ```

   d. In the `AMQP/*"` line, replace the password field with the same password that you entered for the RabbitMQ publisher account.

In this example, the password was set to `california`:

```
*:AMQP/*:publisher:california
```

e. Save `clientConnect.conf` and exit `sm_edit`.

7. Restart the publisher by connecting to your presentation SAM using `dmctl`.

   For example:

   a. **`$ dmctl -s INCHARGE-SA-PRES`**

   b. **`dmctl> invoke SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher stop`**

   Note

   If the `stop` command hangs, verify that you entered the same password for the RabbitMQ publisher and SAM.

   c. **`dmctl> invoke SM_AMQPNotificationPublisher::SM-AMQPNotificationPublisher start`**

8. In the RabbitMQ interface, click the **Connections** tab and verify the publisher is connected.

Changing the RabbitMQ ingestion password

Alert-ingestion is a component running in Tomcat that pulls notifications from RabbitMQ and inserts them in to the Notification cache. The RabbitMQ login for this service is `ingestion` with the default password of `changeme`. To change this password, you must update both RabbitMQ and the alerts-ingestion configuration with a new matching password.

Procedure

1. Log in to the RabbitMQ web-based management interface as **`admin`**.
2. Click the **Admin** tab and select **ingestion** from the list of RabbitMQ login users.
3. Click **Update this user**.
4. Enter the new password in both password fields.
5. Click **Update User**.
6. To change the password in alerts-ingestion:

   a. Stop the Smarts Tomcat service by typing **`sm_service stop smarts-tomcat`**.

   b. Using a text editor, open the file `smarts/tomcat/webapps/alerts-ingestion/WEB-INF/classes/rabbitmq-config.xml`.

   c. Find the password line that looks like this:

   ```
   <property name="password" value="changeme" />
   ```

   d. Replace **`changeme`** with the new password.

   In this example, the password was changed to `california`:

   ```
   <property name="password" value="california" />
   ```

e. Restart the Smarts Tomcat service by typing **`sm_service start smarts-tomcat`**.

7. In the RabbitMQ interface, click the **Connections** tab and verify alerts-ingestion is connected. It may take a few minutes for Tomcat to start and for alerts-ingestion to connect.

UI cannot display alerts or Smarts topology when CAS is enabled

Follow these steps when the Central Authentication Service is enabled and the UI is unable to display information about alerts and objects in the Smarts topology.

Procedure

1. Verify the status of the Alerts EDAA, as described in Checking Alerts EDAA on page 81.
2. Verify the status of the Smarts EDAA, as described in Checking Smarts EDAA on page 81.
3. If Tomcat is running but queries to the EDAA result in the browser hanging, type this command on the SAM server:

   ```
   cd /opt/InCharge/SAM/smarts/bin
   ./runcmd_env.sh
   ```

4. In the `runcmd_env.sh` output:

   a. If `SM_CAS_SERVER` exists, verify this entry includes the protocol, fully-qualified domain name of the EMC M&R host, and the port number. Make sure there is nothing after the port number (not even a "/").

   b. If the https protocol is used, make sure the port is correct for https.

   c. Verify `SM_TOMCAT_SERVER` has an URL for Tomcat that is part of the SAM installation.

   d. Make sure localhost and 127.0.0.1 are NOT in `SM_CAS_SERVER` or `SM_TOMCAT_SERVER` entries. These environment variables must contain URLs that reach services from outside the host machine.

Wrong CAS host name in runcmd_env.sh

The UI informs you when you entered an incorrect Central Authentication Service host name in the runcmd_env.sh script.

This error message appears throughout the UI when you specify an incorrect host name for CAS in `runcmd_env.sh`:

```
java.util.concurrent.ExecutionException:com.emc.asd.mashupengine.uti
ls.JSONException:A JSONObject text must begin with '{' at 1
[character 2 line 1]
```

Procedure

- Specify the correct CAS host name in the `runcmd_env.sh` script.

Services remain registered and running after an uninstall

If you did not stop all services before performing an uninstall, the services are still running and using ports. If you do not want to reboot your system, you must manually stop these services to allow other services to use these ports.

An uninstall only removes those services that were configured during the installation of the software being uninstalled. If there are services configured by a second installation on the same host or by manually invoking `sm_service install`, those services are not removed.

Follow these procedures to stop services:

- Stopping services on Linux on page 91
- Stopping services on Windows on page 92

Stopping services on Linux

Follow this procedure if you did not stop all services before performing an uninstall. This procedure shows you examples of how to find the process IDs of the services that you need to stop on Linux systems.

Procedure

1. Find the process ID for elasticsearch, a Java process running `org.elasticsearch.bootstrap.ElasticSearch`

   For example:

   ```
   root      7223 10165  0 Jun05 ?        00:11:36 /opt/
   InCharge/SAM/smarts/jre/bin/java -cp /opt/InCharge/SAM/smarts/
   toolbox/elasticsearch/lib/elasticsearch-0.90.7.jar:/opt/
   InCharge/SAM/smarts/toolbox/elasticsearch/lib/*:/opt/
   InCharge/SAM/smarts/toolbox/elasticsearch/lib/sigar/* -Xms1g -
   Xmx1g -Xss256k -Djava.awt.headless=true -XX:+UseParNewGC -XX:
   +UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:
   +UseCMSInitiatingOccupancyOnly -XX:
   +HeapDumpOnOutOfMemoryError -Delasticsearch -Des.pidfile=/opt/
   InCharge/SAM/smarts/local/logs/elasticsearch.pid -
   Des.foreground=yes -Des.path.home=/opt/InCharge/SAM/smarts/
   toolbox/elasticsearch -Des.path.data=/opt/InCharge/SAM/smarts/
   local/repos -Des.path.logs=/opt/InCharge/SAM/smarts/local/
   logs -Des.path.conf=/opt/InCharge/SAM/smarts/conf/
   elasticsearch org.elasticsearch.bootstrap.ElasticSearch
   ```

2. Find the process ID for Tomcat, a Java process running `org.apache.catalina.startup.Bootstrap`

   For example:

   ```
   root     12495 10165  0 Jun05 ?        00:31:17 /opt/
   InCharge/SAM/smarts/jre/bin/java -Xrs -Xms1g -Xmx3g -
   XX:PermSize=512m -XX:+HeapDumpOnOutOfMemoryError -
   classpath /opt/InCharge/SAM/smarts/tomcat/bin/
   bootstrap.jar:/opt/InCharge/SAM/smarts/tomcat/bin/tomcat-
   juli.jar:/opt/InCharge/SAM/smarts/local/l10n/spool:/opt/
   InCharge/SAM/smarts/local/l10n:/opt/InCharge/SAM/smarts/l10n -
   Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManag
   er -Djava.util.logging.config.file=/opt/InCharge/SAM/smarts/
   tomcat/conf/logging.properties -Djava.endorsed.dirs=/opt/
   InCharge/SAM/smarts/tomcat/endorsed -
   ```

```
Dsmarts.remote.broker=localhost:426 -Dcatalina.logdir=/opt/
InCharge/SAM/smarts/local/logs/tomcat -Dcatalina.base=/opt/
InCharge/SAM/smarts/tomcat -Dcatalina.home=/opt/InCharge/SAM/
smarts/tomcat -Djava.io.tmpdir=/opt/InCharge/SAM/smarts/
tomcat/temp -Djava.awt.headless=true -
Dcom.smarts.disable_ci_jni=true -Djava.security.egd=file:/
dev/./urandom -Dcom.emc.msa.dmt.clientconnect=/opt/
InCharge/SAM/smarts/conf/edaaClientConnect.conf -
Dsmarts.cas.server=https://itops-dev-121.lss.emc.com:58443 -
Dcom.smarts.incoming_protocol=1,0 -
Dcom.smarts.outgoing_protocol=1,0 -
Dcom.smarts.fips_mode=FALSE -Dsmarts.tomcat.server=https://
itops-dev-120.lss.emc.com:8443
org.apache.catalina.startup.Bootstrap --ignoreme start
```

3. Find the process ID for RabbitMQ, an Erlang beam process running with `-s rabbit`

   For example:

```
root      7221 10165  0 Jun05 ?        00:24:03 /opt/
InCharge/SAM/smarts/toolbox/OTP/erts-5.9.3.1/bin/beam.smp -W
w -K true -A30 -P 1048576 -- -root /opt/InCharge/SAM/smarts/
toolbox/OTP -progname erl -- -home /root -- -pa /opt/
InCharge/SAM/smarts/toolbox/rabbitmq/ebin -noshell -noinput -
s rabbit boot -sname rabbit@itops-dev-120 -boot start_sasl -
config /opt/InCharge/SAM/smarts/conf/rmq/rabbitmq.config -
kernel inet_default_connect_options [{nodelay,true}] -sasl
errlog_type error -sasl sasl_error_logger false -rabbit
error_logger {file,"/opt/InCharge/SAM/smarts/local/logs/
rabbit@itops-dev-120.log"} -rabbit sasl_error_logger
{file,"/opt/InCharge/SAM/smarts/local/logs/rabbit@itops-
dev-120-sasl.log"} -rabbit enabled_plugins_file "/opt/
InCharge/SAM/smarts/conf/rmq/enabled_plugins" -rabbit
plugins_dir "/opt/InCharge/SAM/smarts/toolbox/rabbitmq/
plugins" -rabbit plugins_expand_dir "/opt/InCharge/SAM/smarts/
local/repos/rmq/rabbit@itops-dev-120-plugins-expand" -os_mon
start_cpu_sup false -os_mon start_disksup false -os_mon
start_memsup false -mnesia dir "/opt/InCharge/SAM/smarts/
local/repos/rmq/rabbit@itops-dev-120" --ignoreme
```

4. Use the process IDs to kill these three processes: **`$ kill -9 7223 12495 7221`**

Stopping services on Windows

Follow this procedure if you did not stop all services before performing an uninstall.

Procedure

1. Access the **Services Management Console** to see which services are still registered and running.
2. Stop the services from the **Services Management Console**.
3. Delete the SAM directory from `\InCharge\SAM`.
4. Manually remove the services using the command prompt tool name `sc`. For example:
   a. **`sc delete ic-broker`**
   b. **`sc delete smarts-tomcat`**
   c. **`sc delete ic-sam-server-pres`**

Retrieving the current elasticsearch PID

You can monitor the resource consumption of elasticsearch using the Linux `top -p <pid>` command. This procedure explains where to retrieve the current process ID of elasticsearch.

Procedure

- To determine the current process ID of elasticsearch, view `<SMARTSHOME>/local/logs/elasticsearch.pid`.

Multi-sort option not working after clicking on Notification column title

When you click the column title in Notification view and then try to set the multi-sort option for the same column, multi-sort does not work.

From **Operations** > **Network** > **Notifications**, select a notification and click a column title. This sorts the data in the column (also called "UI sort.") If you try to enable multi-sort for the same column, it will not work. The sort order remains the same as when you clicked on the column heading.

In addition, you cannot restore the default sort order.

Procedure

1. To clear the UI sort, refresh the Notification view.
   - Multi-sort is based on Backend sorting
   - UI sorting (when you click on the column title) overrides the multi-sort feature. You must clear this before multi-sort will work again.

Ports that must be open between SAM and EMC M&R

Ensure that the firewall between the server hosting SAM and the servers hosting EMC M&R (Watch4net) are open. EMC M&R collects data from the Smarts domain managers. Configure the firewall settings to allow access across ports.

Ports in use with HTTP (no SSL encryption)

- Tomcat server in Service Assurance Manager (SAM): 8080
- Tomcat server in EMC M&R (Watch4net): 58080
- Smarts Broker: 426 (also used for SSL encryption)
- Smarts License Server: 1744 (also used for SSL encryption)
- Elasticsearch: 9200
- RabbitMQ: 15672

Ports in use with HTTPS enabled (SSL encryption)

- Tomcat server in SAM: 8443
- Tomcat server in EMC M&R (Watch4net): 58443

- Smarts Broker: 426
- Smarts License Server: 1744

CHAPTER 4

How to Maintain IP Manager Settings

- Overview 96
- Requirements 97
- Workflow for maintaining IP Manager settings 98
- Adding an IP Manager to Configuration Manager 100
- Disabling an IP Manager from Configuration Manager control 100
- Modifying IP settings while Configuration Manager transfer is delayed 101
- Removing an IP Manager from Configuration Manager control 101
- Configuring settings for a selected group 102
- Configuring matching criteria for a selected group 102
- Configuring target domains for a selected group 103
- Adding a description for a selected group 104
- Configuring device access for a selected group 104
- Configuring unique identifier tags for a selected group 105
- Configuring discovery settings 105
- Configuring discovery filters 106
- Adding a new group 106
- Deleting a group 107
- Changing the priority of the groups 107
- Copying the configuration of a group 108
- Displaying IP Manager groups 108
- Displaying IP Manager attributes 108
- Configuring EDAA mode for 9.2 and 9.1 IP Managers 109
- Automatically loading settings from a running IP Manager into the Configuration Manager 110
- sm_service install commands for Linux 112
- sm_service install commands for Windows 113

Overview

Use the Configuration Manager in the EMC M&R UI to apply a centralized copy of configuration settings to all IP Managers in your deployment. Configuration settings can include: polling intervals, thresholds, device access credentials, unique tagging identifiers for discovered topology, and discovery configuration parameters.

For deployments with multiple IP Managers, Service Assurance Suite provides the Configuration Manager, so you can consistently maintain configuration settings. The Configuration Manager is an optional component.

- Polling settings define the polling intervals. Polling occurs when an IP Manager communicates with a managed device to determine the device's operational status.
- Thresholds are values that define acceptable or unacceptable levels of connectivity or performance. The polled data is compared to the threshold values for monitoring purposes.
- Device access settings define the credentials needed to access the managed devices.
- IP tagging defines a tag that the IP Manager uses to uniquely identify discovered topological objects that have identical names.
- Discovery configuration settings define the discovery process that the IP Manager performs.

The Configuration Manager feature supports the following IP Managers: IP Availability Manager, IP Performance Manager, and the combined IP Availability and Performance Manager.

Figure 5 Example of polling settings

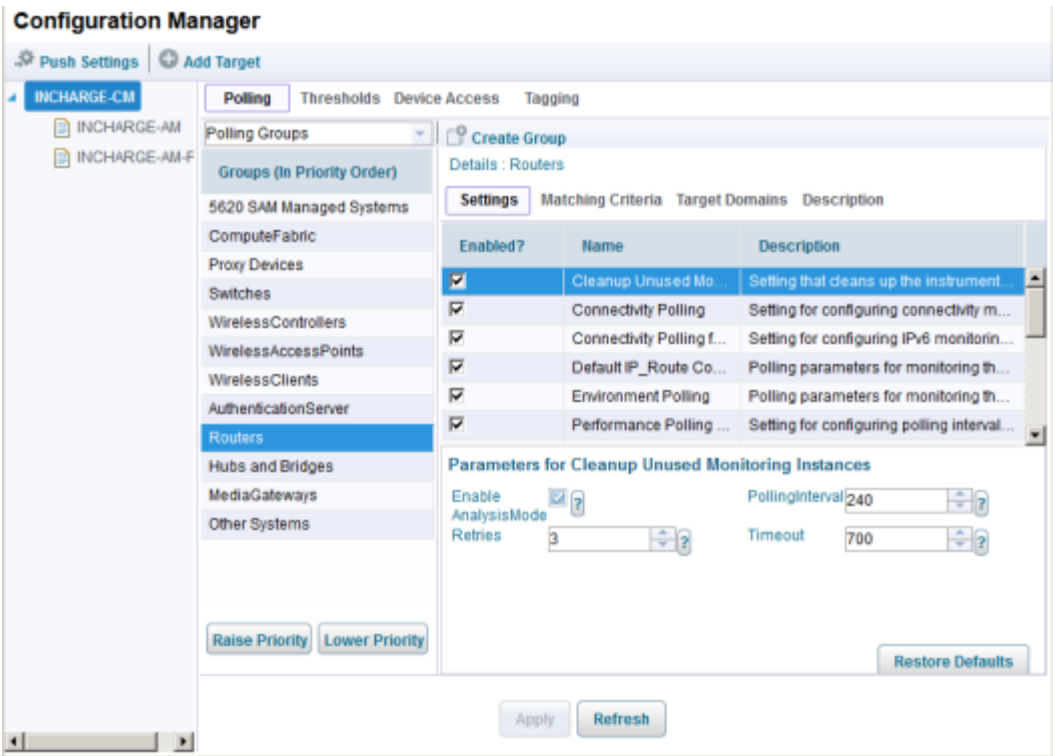
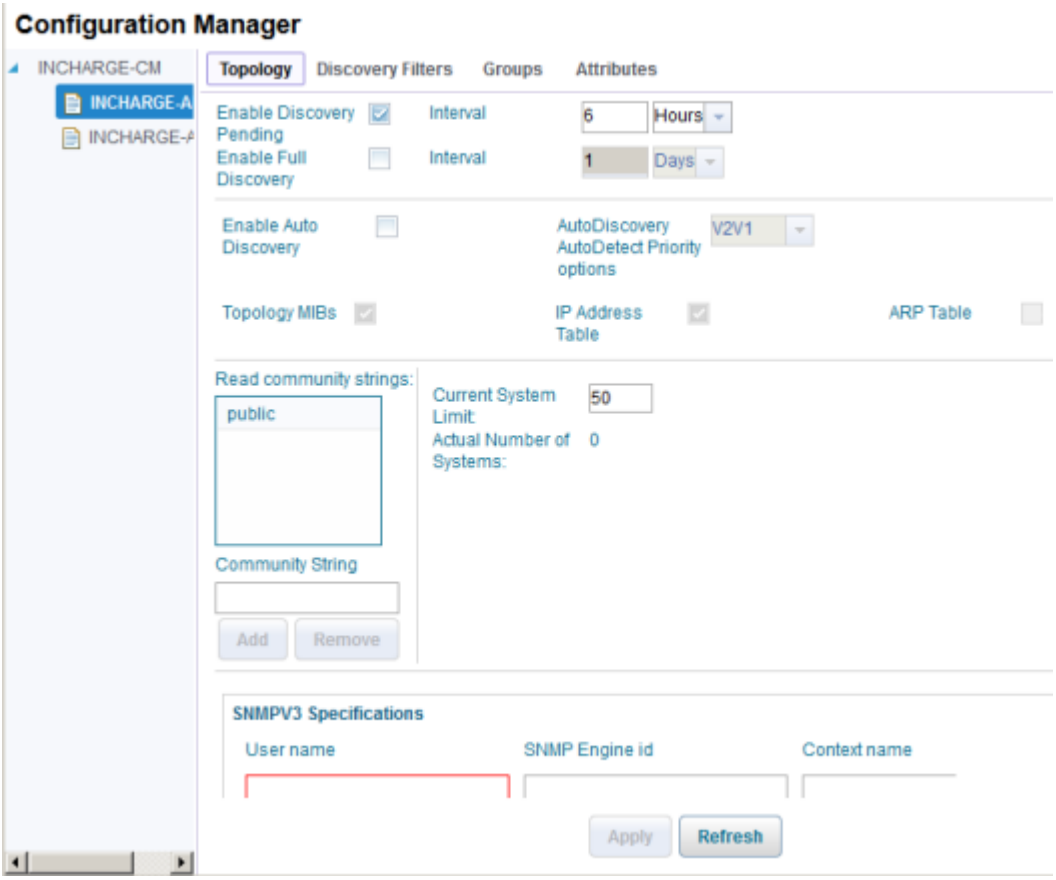


Figure 6 Example of discovery settings



Additional information is described in these documents:

- *EMC M&R Installation and Configuration Guide*
- *SolutionPack for EMC Smarts Summary Sheet*
- *How to Set Up SAM, EMC M&R, and the SolutionPack for EMC Smarts*
- *Troubleshooting the Deployment of SAM, EMC M&R, and the SolutionPack for EMC Smarts*

Requirements

When using the Configuration Manager in the EMC M&R UI to control your configuration settings, ensure that you have the following components set up in your deployment:

- A valid EMC Smarts license, that includes the Configuration Manager, is installed.
- The Configuration Manager is installed and is started with the EMC Data Access API service option (`--edaa=ip/2.0`).
- The SolutionPack for EMC Smarts is installed and configured with the Configuration Manager instance name. In the Report block, under Presentation SAM Configuration Section, select the **Use Smarts Configuration Manager** checkbox and specify the name of the Configuration Manager in the Configuration Manager field if it does not use the default name.
- You planned your configuration carefully:

- Identified the IP Managers to assign to the Configuration Manager. IP Managers 9.1 and higher are supported but there is limited backward compatibility for 9.1 IP Managers.
- Modified the `sm_service install` command for the identified 9.4 and 9.3 IP Managers to include the `--edaa=ip/2.0` option (for example: sm_service install commands for Linux on page 112 and sm_service install commands for Windows on page 113).
  9.2 and 9.1 IP Managers do not support the service command `--edaa=ip/2.0` option. For 9.1 IP Managers, the Configuration Manager does not support discovery configuration settings, but other configuration settings are supported. Use: Configuring EDAA mode for 9.2 and 9.1 IP Managers on page 109
- Be aware that when the Configuration Manager is connected to running IP Managers, it by default transfers the settings and may overwrite unique settings in the IP Managers.
  If you do not want Configuration Manager to transfer the settings to the IP Managers on the initial connection, uncheck the **Config Enabled** checkbox when you add the IP Manager as a target as described in Adding an IP Manager to Configuration Manager on page 100.
- Once you use the Configuration Manager to control configuration settings in the IP Managers, you are no longer able to modify polling and thresholds group settings locally in the IP Managers.
  - The Configuration Manager overwrites all configuration settings in the IP Managers.
  - You can only view the polling and thresholds settings and not modify them in the Domain Manager Administration Console.

  The Topology and Discovery Filters settings remain locally defined for each IP Manager. You can continue to modify the Topology and Discovery Filters settings from the Domain Manager Administration Console and the EMC M&R UI.

- EMC M&R is installed and you have valid administrator credentials.

Workflow for maintaining IP Manager settings

Use the Configuration Manager to apply a centralized copy of configuration settings to all IP Managers in your deployment.

1. Log in to the EMC M&R platform with your administrator username and password.
2. Select **Administration** > **Modules** > **Smarts**.
3. Select the Configuration Manager (Default: INCHARGE-CM).
   - Ensure that the IP Managers are assigned.
   - If not, add the IP Managers: Adding an IP Manager to Configuration Manager on page 100
   - To keep IP Managers assigned but disabled: Disabling an IP Manager from Configuration Manager control on page 100
   - To remove IP Managers: Removing an IP Manager from Configuration Manager control on page 101
4. Click one of the following: **Polling**, **Thresholds**, **Device Access**, **Tagging**, or an IP Manager for discovery configuration and make your configurations accordingly:

- To configure settings for a selected group: Configuring settings for a selected group on page 102
- To configuring matching criteria: Configuring matching criteria for a selected group on page 102
- To configure target domains: Configuring target domains for a selected group on page 103
- To add a description: Adding a description for a selected group on page 104
- To configure device access: Configuring device access for a selected group on page 104
- To configure tagging: Configuring unique identifier tags for a selected group on page 105
- To configure the discovery process: Configuring discovery settings on page 105
- To configure discovery filters: Configuring discovery filters on page 106
- To create more groups: Adding a new group on page 106
- To delete groups: Deleting a group on page 107
- To change the priority order of the groups: Changing the priority of the groups on page 107
- To copy the configuration of a group to make a new group: Copying the configuration of a group on page 108

5. Start the services for one or more IP Managers.
   Linux: Issue the command:

```
/opt/InCharge/IP/smarts/bin/sm_service start <service_name>
```

   Windows: From the application server's desktop, select **Start** > **Administrative Tools** > **Services** and start the service.

IP Manager	Service name
IP Availability Manager	ic-am-server
IP Performance Manager	ic-pm-server
IP Availability and Performance Manager	ic-am-pm-server

   Before you start the service, if you have not already done so, you need to issue the `sm_service install` command to register the product: sm_service install commands for Linux on page 112 and sm_service install commands for Windows on page 113

6. Click **Push Settings**:
   - If you changed configuration settings for one of the target IP Managers.
   - After you enabled the Config Enabled attribute for a target IP Manager.

   The Configuration Manager transfers the settings whenever the IP Managers connect or are reconnected, or when you click Push Settings.

Adding an IP Manager to Configuration Manager

Add one or more IP Managers to the Configuration Manager list if they are not included.

Procedure

1. For the selected Configuration Manager, click **Add Target**.
2. Type the IP Manager instance name in the **Element Name** field (for example, INCHARGE-AM).
3. Decide if you want to keep the following checkboxes selected:

Checkbox	Description
Config enable	By default, this checkbox is selected so that the Configuration Manager automatically transfers the configuration settings to the IP Manager if the IP Manager is started. If you clear the checkbox, the IP Manager is added to the Configuration Manager list but the Configuration Manager does not transfer the settings. Use this option if you want to control when the Configuration Manager transfers the settings. Modifying IP settings while Configuration Manager transfer is delayed on page 101
Reconfigure after push	By default, this checkbox is selected so that the Configuration Manager initiates a reconfigure action on the modified or newly-added configuration settings in the IP Manager. If you clear the checkbox, then you have to manually reconfigure the IP Manager.

4. Click **OK**.

Disabling an IP Manager from Configuration Manager control

You can temporarily stop the Configuration Manager from sending the centralized settings to an IP Manager without removing it from the Configuration Manager list. For example, you can disable the transfer of settings for a specific IP Manager while you create new groups or change settings.

Procedure

1. In the Configuration Manager list, right-click the IP Manager and select **Modify Attributes**.
2. Select the **Config enable** checkbox to remove the checkmark.
3. Select the **Reconfigure after push** checkbox to remove the checkmark.
4. Click **OK**.

Modifying IP settings while Configuration Manager transfer is delayed

Use this alternate approach if you want to configure groups and settings while delaying the transfer of the settings.

Before you begin

The IP Manager is added to the Configuration Manager list but you temporarily disabled it from the Configuration Manager.

Procedure

1. Review which groups are assigned to the IP Manager and their settings.
2. Modify the groups and their settings if necessary.
3. Right-click the IP Manager and select **Modify Attributes**.
4. Select the **Config enable** checkbox.
5. Select the **Reconfigure after push** checkbox.
6. Click **Push Settings** to transfer the settings.

Removing an IP Manager from Configuration Manager control

One method to stop the Configuration Manager from sending the centralized settings to an IP Manager is to permanently remove it from the Configuration Manager list. Or, if you accidently added the incorrect IP Manager to the Configuration Manager list, you can remove it.

Procedure

1. Clear the value for the Service Name attribute.
   a. Attach the Domain Manager Administration Console to the IP Manager.
   b. Press **Ctrl + ALT + M**.
   c. Go to **ICIM_Manager->ICIM-Manager.**
   d. Clear the value in the Service Name attribute.
   e. Click **Apply**.
2. In the EMC M&R UI, in the Configuration Manager list, right-click the IP Manager and select **Delete**.
3. Reinstall the service for the IP Manager without the `--edaa` option.
   a. Stop the IP Manager service.

      Linux: Issue the command:

      ```
      /opt/InCharge/IP/smarts/bin/sm_service stop <service_name>
      ```

      Windows: From the application server's desktop, select **Start** > **Administrative Tools** > **Services** and stop the service.

b. Issue the `sm_service install` command for the IP Manager minus the `--edaa` option.

c. Start the IP Manager service.

Configuring settings for a selected group

You can accept the default settings or change the settings and their parameters for a selected group.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Settings**.

   The default settings are already enabled.
5. To add more settings to the group,

   a. Scroll and click the **Enabled** checkbox for each setting that you want to apply.

   b. Click **Apply** and **Refresh**.

   The Configuration Manager transfers only the enabled settings.
6. To examine the parameters of each setting, click the setting.
7. To modify the setting parameters, click the setting, and modify the values as necessary.

   To restore the parameters to their default values, click **Restore Defaults**.
8. Click **Apply** to save your changes.

Configuring matching criteria for a selected group

You can configure matching criteria for a selected group. The matching criteria determines group membership. A managed object becomes a member of the group, when the managed object matches a group's target class and matches all of the attributes defined for the target class.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.

- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Matching criteria** to create matching criteria which determines the members of the group.

   a. Select a class attribute from the dropdown box.

   b. Specify a value for the class attribute.

   Value can be: Boolean, text, integers, and wildcard characters. The Value field is not case-sensitive.
5. Click **Add** to add more pairs of class attributes and values.

   To remove a class attribute and its value, click the **Delete icon**.
6. Click **Apply** to save your changes.

Configuring target domains for a selected group

You can specify IP Managers for a selected group and assign the setting to specific IP Managers. For example, you have a group of routers with a specific threshold setting and three IP Managers monitor the routers.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Target Domains** to assign the setting to specific IP Managers.
5. Specify a filter in the group that you want to assign to the target IP Managers.

a. Type wildcard characters, integers, regular expressions, or an IP Manager name in the `Search By` field and click **Search** to search for particular IP Managers or a group of IP Managers.

b. Select one or more IP Managers from the list.

The IP Managers that you select can be a subset of the IP Managers listed under the IP Configuration Manager. Previously enabled or disabled IP Managers (other than the search criteria) will not be modified.

6. Click **Apply** to save your changes.

Adding a description for a selected group

You can create a description to identify a group.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following choices:
   - Polling
   - Thresholds
   - Device Access
   - Tagging
2. Select a group category from the dropdown box.
3. Select a group from the list that appears for the group category.
4. Click **Description** and type information about the group.
5. Click **Apply** to save your changes.

Configuring device access for a selected group

You can configure the device access setting for a selected group. Device credentials, for example login credentials, are used for command line interface (CLI) discovery, CLI polling, and XML discovery.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click **Device Access**.
2. Select the group category **Device Access Configurations** from the dropdown box.
3. Select a group (for example, **CLI Access Group** or **XML Access Group**) from the list that appears for the group category.

4. Click **Settings**.

   The default settings are already enabled.

   The Configuration Manager transfers only the enabled settings.
5. To examine the parameters of each setting, click the setting.
6. To modify the credentials, click the setting, and modify the values as necessary.
7. Click **Apply** to save your changes.

Configuring unique identifier tags for a selected group

You can configure an IP tag naming convention that the IP Manager uses to uniquely identify discovered topological objects that have identical names.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click **Tagging**.
2. Select the group category **System IP Tag Groups** from the dropdown box.
3. Select a group (for example, **IP Tag**) from the list that appears for the group category.
4. Click **Settings**.

   The default settings are already enabled.

   The Configuration Manager transfers only the enabled settings.
5. To create the tagging convention, click the setting, and modify the values as necessary.
6. Click **Apply** to save your changes.

Configuring discovery settings

You can configure the discovery process for the IP Manager. You can specify whether the IP Manager performs a full discovery or autodiscovery, the time intervals for discovery, whether pending discovery is performed for candidate systems, user-defined community strings, and SNMPV3 specifications.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Topology**.

3. Click the checkboxes and modify the values as necessary.
4. Click **Apply** to save your changes.

Configuring discovery filters

You can configure discovery filters for candidate systems that the IP Manager uses during the discovery process. The filters can include IP address ranges, System OIDs, and so on.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Discovery Filters**.
3. Click the checkboxes and modify the values as necessary.

   Use the **View Extended Filter** checkbox for SNMP fields and SNMPV3 specifications.
4. Click **Apply** to save your changes.

Adding a new group

When you are using the Configuration Manager to maintain settings for IP Managers, you can add a new group to the group category for Polling, Thresholds, Device Access, or Tagging.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. Click **Create Group**.
4. Type the name of the new group and a description. Click **OK**.

   The new group appears in the group list.

Deleting a group

When you are using the Configuration Manager to maintain settings for IP Managers, you can delete a user-defined group or a default group from the group category for Polling, Thresholds, Device Access, or Tagging.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, right-click the group and select **Delete**.

Changing the priority of the groups

In any group category, you can arrange the groups in a high-to-low priority. During the matching criteria process which determines the members of a group, a candidate member object is compared against the highest priority group first. The candidate becomes a member of the first group for which there is a criteria match.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, select the group and click either **Raise Priority** or **Lower Priority** to move the group to the appropriate position in the list.
4. Click **Apply** to save your changes.

Copying the configuration of a group

When you are using the Configuration Manager to maintain settings for IP Managers, you can create a new group by copying an existing group with its configurations, making minimal changes, and reassigning IP Managers to it.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the following: **Polling**, **Thresholds**, **Device Access**, or **Tagging**.
2. Select a group category from the dropdown box.

   The choices vary accordingly for Polling, Thresholds, Device Access, or Tagging.
3. In the group list, right-click the group to copy and select **Copy Configuration**.
4. Type the new group name, the description, the IP Managers to assign to it, select the **Copy Matching Criteria** checkbox, and click **OK**.

   Helper lists the configuration-enabled IP Managers.

   The new group appears above the source group from which it was copied. This ensures that the custom group settings are applied first to the IP Managers assigned to this group and not overwritten by the default group settings.

Displaying IP Manager groups

You can view all of the groups for a specific IP Manager.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).
- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Groups**.

Displaying IP Manager attributes

You can view all of the attributes for a specific IP Manager.

Before you begin

- Log in to the EMC M&R platform with your administrator username and password.
- Navigate to the Configuration Manager (Select **Administration** > **Modules** > **Smarts**.).

- Assign IP Managers.

Procedure

1. Click one of the IP Managers in the Configuration Manager list.
2. Click **Attributes**.

Configuring EDAA mode for 9.2 and 9.1 IP Managers

Configure EDAA mode for the services of the older IP Managers so the IP Managers can interact with the Configuration Manager. Older IP Managers do not support the service command `--edaa=ip/2.0` option.

Procedure

1. Edit the `msa-sources.xml` file located in the SAM installation in `<SAM-BASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes` to add entries for your IP Managers.

   a. For example, add the entry key information:

   ```
   <entry key="INCHARGE-AM-92"
   value-ref="MsaDMTDataSource__INCHARGE-AM-92" />
   ```

   b. Add the corresponding bean id information.

   ```
   <bean id="MsaDMTDataSource__INCHARGE-AM-92"
    class="com.emc.msa.dmt.dmpool.MSADMTContext">
    <property name="brokerContext"
   ref="MsaDMTDataSource__Broker" />
    <property name="dmtName" value="INCHARGE-AM-92" />
    <property name="dataSourceName" value="INCHARGE-AM-92" />
    <property name="modelName" value="ip" />
    <property name="modelVersion" value="2.0" />
    <property name="useTLS" value="true" />
    <property name="disableKeepalives" value="true" />
    <property name="lockBoxSupport" value="false" />
    <property name="excludeClasses" ref="IP-
   ExcludeClassesDefault"/>
    <property name="excludeAttributes" ref="IP-
   ExcludeAttrsDefault"/>
    </bean>
   ```

   Use the full domain name as it is registered with the Broker (for example, INCHARGE-AM-92 and not AM-92). The entry key parameter value should match the datasource name (the domain name with which the IP Manager is started).

   The value of the bean id parameter must match the value-ref parameter value.

   The dmtName property value and the dataSourceName property value must match the entry key value.

2. Open the `msa-model-defaults.xml` file in the `<SAM-BASEDIR>/smarts/tomcat/webapps/smarts-edaa/WEB-INF/classes/` directory. If not commented, comment the MR_MetaObject value in the xml node with `id="IP-ExcludeClassesDefault"`. For example:

   ```
   <!-- Start of Default Values for Provider Entries -->
    <util:list id="IP-ExcludeClassesDefault">
   ```

```
<value>GA.*</value>
<!--<value>MR_MetaObject</value> -->
<value>ICIM_Test</value>
<value>NasManager</value>
<value>Topo.*</value>
<value>Hierarchical.*</value>
<value>VOIP.*</value>
</util:list>
```

3. Use sm_edit to open the `<SAM-BASEDIR>/smarts/conf/edaaClientConnect.conf` file.
   a. Add an entry for the IP Manager using the format `*:<DOMAIN-NAME>:admin:changeme`.

      ```
      *:INCHARGE-AM-92:admin:changeme
       ::_edaa:changeme
      ```

      The account `_edaa` is used to log in to IP Managers 9.3 and higher.

   b. Save the file.
4. Stop and start the smarts-tomcat, smarts-rabbit-mq, and smarts-elasticsearch services.

Automatically loading settings from a running IP Manager into the Configuration Manager

Manually transferring settings from a running IP Manager into the Configuration Manager can be time-consuming. You can use an automated alternative, the sm_settings.pl script, to export the settings from the IP Manager and import them into the Configuration Manager.

Procedure

1. To export the settings from a running IP domain manager, run the script from `<BASEDIR>/IP/smarts/bin`:

   ```
   ./sm_perl sm_settings.pl --server=<server_name> --
   export=<filename>
   ```

   For example: `./sm_perl sm_settings.pl -s INCHARGE-AM --export=pt_goups`

   The export output is written as a file to the `<BASEDIR>/IP/smarts/local/logs` directory.
2. Optional, you can modify the script output to include new polling groups: Other modifications to sm_settings.pl output on page 111
3. To import the content into the Configuration Manager, run the script from `<BASEDIR>/IP/smarts/bin`:

   ```
    ./sm_perl sm_settings.pl --server=<CM_server> --
   import=<filename>
   ```

For example: `./sm_perl sm_settings.pl -s INCHARGE-CM --import=pt_goups`

Other modifications to sm_settings.pl output

When you use the sm_settings.pl script, you can also modify the script output to include new polling groups, for example, before importing the content into the Configuration Manager.

If you want add another polling group, use sm_edit from the BASEDIR/smarts/bin directory to open the exported output file (for example, type: `sm_edit <BASEDIR>/IP/smarts/local/logs/pt_groups`). Add the new group definition under the polling category ICIM_UnitaryComputerSystem Polling Groups line. Below this line, you see definitions for all polling groups applicable to Unitary Computer systems (routers, switches, etc). Add the new definition immediately after the category line or between other definitions, as long as it is above the next category line.

- To create a new group definition, you can copy an existing group in the file and modify it.
- Alternatively, you can run the sm_settings.pl script against an IP Manager that is not under Configuration Manager control and that contains the desired group definition. Then, copy and paste the group definition into the file.

In addition, after you add the group definition, type the IP Manager or multiple IP Managers for the group. The general syntax is: `config <Group Name>: DM1|DM2`

Then, save the file and import it into the Configuration Manager.

If a domain name specified in a group definition is not configured as a target IP Manager for the Configuration Manager, the IP Manager will be added as part of the import.

The settings for the newly-added Domain Managers need to be verified and then pushed manually.

Note

Export can be run on any of the installations of IP Manager. However, to import the settings, the file needs to be placed at SM_HOME/local/logs or SM_WRITEABLE/logs of the server's installation folder and then import needs to be invoked from the bin folder of the same install.

Note

Even though the Device Access groups can be imported into the IP Configuration Manager, passwords still need to be added manually because passwords are not exported due to security reasons. However, once the Configuration Manager pushes the settings to the target domains, it is done through secure connection, so it can push the credentials.

The output file contains configuration of all polling and threshold groups and settings. Each group definition starts with `config <group name>` line. Group definitions are separated from each other by blank lines. They are also organized by category. When you add a new group, make sure that the new group definition is added under the correct category.

```
Polling Group Categories
polling category CIM_FileSystem Managed FileSystems
```

```
polling category RedundancyGroup Unmanaged RedundancyGroups
polling category Interface Unmanaged Interfaces
polling category RedundancyGroup Managed RedundancyGroups
polling category Interface Managed Interfaces
polling category CIM_FileSystem Unmanaged FileSystems
polling category ICIM_ServiceAccessPoint Managed STPNodes
polling category ICIM_UnitaryComputerSystem Polling Groups
polling category CIM_LogicalDevice Unmanaged Logical Devices
polling category Port Managed Port
polling category CIM_LogicalDevice Managed Logical Devices
polling category ICIM_ServiceAccessPoint Unmanaged STPNodes
polling category Port Unmanaged Ports

Threshold Group Categories
threshold category Port Port Groups - Trunk Ports
threshold category FileSystem File Systems
threshold category ICIM_UnitaryComputerSystem System Resource Groups
threshold category WirelessControllerRedundancyGroup
WirelessControllerRedundancyGroups
threshold category ICIM_UnitaryComputerSystem System VLAN Tag Groups
threshold category Port Port Groups - Access Ports
threshold category TemperatureSensor TemperatureSensor
threshold category Interface Interface Groups
threshold category WirelessRadioInterface
WirelessRadioInterfaceGroup
threshold category AggregatePort AggregatePortsGroup
threshold category VoltageSensor VoltageSensor

Tagging
tagging category ICIM_UnitaryComputerSystem System IP Tag Groups

CLI groups
security category ICIM_UnitaryComputerSystem Device Access
Configurations
```

sm_service install commands for Linux

The `sm_service install` command for products that interoperate with the EMC M&R User Interface includes additional options. Before you start the service, if you have not already done so, you need to issue the `sm_service install` command from the `/opt/InCharge/IP/smarts/bin` directory to register the product with the EMC Smarts Broker.

sm_service install command for Configuration Manager

As a prerequisite, the Configuration Manager is already running.

```
/opt/InCharge/IP/smarts/bin/sm_service install --force
--unmanaged
--startmode=runonce
--name=ic-ip-configuration-edaa
"--description=EMC Smarts IP Configuration Manager for EDAA"
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-CM
--config=icf-c
--bootstrap=bootstrap.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--nodx
--output
```

sm_service install command for IP Availability Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-server
"--description= EMC Smarts IP Availability Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM
--config=icf
--bootstrap=bootstrap-am.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install command for IP Performance Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-pm-server
"--description= EMC Smarts IP Performance Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-PM
--config=icf
--bootstrap=bootstrap-pm.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install command for IP Availability-Performance Manager

```
/opt/InCharge/IP/smarts/bin/sm_service install
--force
--name=ic-am-pm-server
"--description= EMC Smarts IP Availability Manager and Performance
Manager Server"
--startmode=runonce
/opt/InCharge/IP/smarts/bin/sm_server
--name=INCHARGE-AM-PM
--config=icf
--bootstrap=bootstrap-am-pm.conf
--port=0
--edaa=ip/2.0
--ignore-restore-errors
--output
```

sm_service install commands for Windows

The `sm_service install` command for products that interoperate with the EMC M&R User Interface includes additional options. Before you start the service, if you have not already done so, you need to issue the `sm_service install` command

from the `/opt/InCharge/IP/smarts/bin` directory to register the product with the EMC Smarts Broker.

sm_service install command for Configuration Manager

As a prerequisite, the Configuration Manager is already running.

```
C:\InCharge\IP\smarts\bin\sm_service install --force
--unmanaged
--startmode=runonce
--name=ic-ip-configuration-edaa
"--description=EMC Smarts IP Configuration Manager for EDAA"
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-CM"
"--config=icf-c"
"--bootstrap=bootstrap.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors "
"--nodx "
"--output"
```

sm_service install command for IP Availability Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-am-server
"--description= EMC Smarts IP Availability Manager Server"
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-AM"
"--config=icf"
"--bootstrap=bootstrap-am.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

sm_service install command for IP Performance Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-pm-server
"--description= EMC Smarts IP Performance Manager Server"
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-PM"
"--config=icf"
"--bootstrap=bootstrap-pm.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

sm_service install command for IP Availability-Performance Manager

```
C:\InCharge\IP\smarts\bin\sm_service install
--force
--name=ic-am-pm-server
"--description= EMC Smarts IP Availability Manager and Performance
Manager Server"
```

```
--startmode=runonce
C:\InCharge\IP\smarts\bin\sm_server.exe
"--name=INCHARGE-AM-PM"
"--config=icf"
"--bootstrap=bootstrap-am-pm.conf"
"--port=0"
"--edaa=ip\2.0"
"--ignore-restore-errors"
"--output"
```

CHAPTER 5

How to Set Up the EMC Smarts Server Manager for Citrix XenServer

- How to Set Up the EMC Smarts Server Manager for Citrix XenServer 118
- Specify XenServer information 118
- How to Update the XenServer Credentials for the Server Manager Configuration 120

How to Set Up the EMC Smarts Server Manager for Citrix XenServer

The EMC Smarts Server Manager probes the Citrix® XenServer® hypervisor and XenCenter to discover and monitor the XenServer Hypervisor and Xen Virtual Machines in your virtual network.

This article is for IT networking administrators.

The procedure in this article assumes that your Service Assurance Suite deployment includes:

- EMC Smarts Server Manager (ESM) installed and operational. For example,
  - The Server Manager is configured to communicate with the IP Manager.
  - The Server Manager is configured with Citrix read-only credentials for your XenServer hypervisor. You should also have access to XenAPI.
  - The IP Manager can discover the XenServer servers configured in the XenCenter.
- A valid EMC Smarts license for XenServer installed.
- Global Console installed.
- Valid read-only credentials for your XenServer hypervisor and the IP address of the host where the hypervisor resides.

For information about these prerequisites, consult the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*, the *EMC Smarts Server Manager User and Configuration Guide*, and the *EMC Smarts Release Notes for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*.

Specify XenServer information

To configure the EMC Smarts Server Manager for XenServer, specify the XenServer hypervisor credentials and the IP address of the host where the hypervisor resides.

Before you begin

EMC Smarts administrator credentials are required to access the **Configure** menu.

Procedure

1. Open the **Service Assurance Manager Global Console** attached to the Server Manager (INCHARGE-ESM, by default).
2. In the **Topology Browser Console**, select **Configure** > **Domain Manager Administration Console**.
3. Right-click the **ESM server** in the left pane and select **Configure ESM credentials**.
4. In the **Configure ESM credentials** dialog box, select **XenServer** for the host type.
5. Type values in the following fields:

Field	Value
Host	IP address for the master and slave XenServer or standalone XenServer where the individual XenServer hypervisor resides
User ID	XenServer read-only user name
Password	XenServer read-only password

6. Click **Apply credential with testing**.
7. Verify that your XenServer credentials are accepted for the XenServer hypervisor by checking the status indicator in the **Configure ESM credentials** dialog box.

   A green `Passed test` status indicates that the credentials are accepted for the XenServer hypervisor.

   If the XenServer credentials are not accepted, confirm that the credentials are correct and enter them again in the **Configure ESM credentials** dialog box.

   You can also check the log file: Verify that XenServer credentials are accepted in the log file on page 119
8. Click **Close**.
9. In the **Domain Manager Administration Console**, select your IP Manager and select **Topology** > **Discover All** to discover the XenServer servers. At the end of the IP Manager discovery process, the Server Manager discovery process is automatically started.

After you finish

After the topology for your virtual network has been discovered, to continue to monitor and analyze your network, use the EMC M&R UI or the Service Assurance Global Console.

For information about how to use the EMC M&R UI, consult the online help.

For information about the XenServer topology, consult the *EMC Smarts Server Manager User and Configuration Guide*.

Verify that XenServer credentials are accepted in the log file

Verify that your XenServer credentials are accepted for the XenServer hypervisor by checking your log file.

Procedure

1. Open the Server Manager log file in the `opt/InCharge/ESM/smarts/local/logs` directory.
2. Locate the credential messages.

   For example, the following messages indicate that the XenServer credentials are accepted:

```
[December 3, 2014 7:27:40 AM EST +990ms] t@1262713152
SM_ProtocolEngine-1 19488 IC Console - V9.4.0.0
DISC-*-CAL_FR-Credential_Util::addCredential : was called for
credential: XEN-<IP_Address>

[December 3, 2014 7:27:41 AM EST +663ms] t@1262713152
```

```
SM_ProtocolEngine-1 19488 IC Console - V9.4.0.0
DISC-*-CRT_CRED-Credential_Util::addCredential: Creating
credential: XEN-<IP_Address>
```

How to Update the XenServer Credentials for the Server Manager Configuration

If the Citrix XenServer administrator changed the credentials for the XenServer hypervisor, update the XenServer credentials for the Service Manager configuration.

Procedure

- Follow the instructions in Specify XenServer information on page 118, and then perform a discovery (**Topology** > **Discover All**) from the Server Manager.

CHAPTER 6

How to Set Up the EMC Smarts Server Manager for Software-Defined Networks Feature

- How to Set Up the EMC Smarts Server Manager for Software-Defined Networks (SDN) Feature 122
- Specify NSX Manager information 122
- How to Update the NSX Manager Administrator Credentials for the Server Manager Configuration 124

How to Set Up the EMC Smarts Server Manager for Software-Defined Networks (SDN) Feature

The EMC Smarts Server Manager for Software-Defined Networks (SDN) feature probes the VMware® NSX Manager and vCenter to discover and monitor the virtual elements in your virtual network. This feature provides end-to-end visibility into SDN-based data center infrastructure. This article describes how to set up the EMC® Smarts® Server Manager for Software-Defined Networks feature.

This article is for IT networking administrators.

The procedure in this article assumes that your Service Assurance Suite deployment includes:

- EMC Smarts Server Manager (ESM) installed and operational. For example,
  - The Server Manager is configured to communicate with the IP Manager.
  - The Server Manager is configured with VMware read-only credentials for the Virtual Center associated with your NSX Manager.
  - The IP Manager can discover the ESX servers configured in the VMware vCenter.
- A valid EMC Smarts license with the EMC Smarts Server Manager for Software-Defined Networks feature installed.
- Global Console installed.
- Valid VMware administrator credentials for your NSX Manager and the IP address of the host where the NSX Manager resides.

For information about these prerequisites, consult the *EMC Smarts Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*, the *EMC Smarts Server Manager User and Configuration Guide*, and the *EMC Smarts Release Notes for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers*.

Specify NSX Manager information

To configure EMC Smarts Server Manager for Software-Defined Networks, specify the NSX Manager administrator credentials and the IP address of the host where the NSX Manager resides.

Before you begin

EMC Smarts administrator credentials are required to access the **Configure** menu.

Procedure

1. Open the **Service Assurance Manager Global Console** attached to the Server Manager (INCHARGE-ESM, by default).
2. In the **Topology Browser Console**, select **Configure** > **Domain Manager Administration Console**.
3. Right-click the ESM server in the left pane and select **Configure ESM credentials**.
4. In the **Configure ESM credentials** dialog box, select **NSX** for the host type.
5. Type values in the following fields:

Field	Value
Host	IP address for the NSX Manager host
User ID	NSX Manager administrator user name
Password	NSX Manager administrator password

6. Click **Apply credential with testing**.
7. Verify that your NSX credentials are accepted for the NSX Manager by checking the status indicator in the **Configure ESM credentials** dialog box.

   A green `Passed test` status indicates that the credentials are accepted for the NSX Manager.

   If the NSX credentials are not accepted, confirm that the credentials are correct and enter them again in the **Configure ESM credentials** dialog box.

   You can also check the log file: Verify that NSX credentials are accepted in the log file on page 123
8. Click **Close**.
9. In the **Domain Manager Administration Console**, select your IP Manager and select **Topology** > **Discover All** to discover vCenter and the NSX Manager. At the end of the IP Manager discovery process, the Server Manager discovery process is automatically started.

After you finish

After the topology for your virtual network has been discovered, to continue to monitor and analyze your network, use the EMC M&R UI or the Service Assurance Global Console.
For information about how to use the EMC M&R UI, consult the online help.

For information about the SDN topology, consult the *EMC Smarts Server Manager User and Configuration Guide*.

Verify that NSX credentials are accepted in the log file

Verify that your NSX credentials are accepted for the NSX Manager by checking your log file.

Procedure

1. Open the Server Manager log file in the `opt/InCharge/ESM/smarts/local/logs` directory.
2. Locate the credential messages.

   For example, the following messages indicate that the NSX credentials are accepted:

```
[March 10, 2014 3:35:58 PM EDT +084ms] t@1302337856
SM_ProtocolEngine-125 7924 IC Console - V9.3.0.0
DISC-*-CAL_FR-Credential_Util::addCredential : was called for
credential: NSX-<IP_address>

[March 10, 2014 3:35:58 PM EDT +387ms] t@1302337856
SM_ProtocolEngine-125 7924 IC Console - V9.3.0.0
```

```
DISC-*-CRT_CRED-Credential_Util::addCredential: Creating
credential: NSX-<IP_address>
```

How to Update the NSX Manager Administrator Credentials for the Server Manager Configuration

If the VMware administrator changed the administrator credentials for the NSX Manager, update the NSX Manager credentials for the Service Manager configuration.

Procedure

- Follow the instructions in Specify NSX Manager information on page 122, and then perform a discovery (**Topology** > **Discover All**) from the Server Manager.

CHAPTER 7

SolutionPack for EMC Network Configuration Manager 3.0 Summary Sheet

- Overview 126
- Technical specifications 126
- Where to find the latest SolutionPack software 127
- Configuring NCM SP with Elastic Search 127
- Installing the SolutionPack for EMC Network Configuration Manager 129
- Post-installation steps 132
- Upgrading NCM SolutionPack from 6.7u1 to 6.8u2 139
- Troubleshooting 140

Overview

Learn to install and configure the SolutionPack for EMC Network Configuration Manager (NCM). This SolutionPack, available with the EMC M&R version 6.8u2 platform and later 6.8uX platforms, provides a wide spectrum of reports for NCM Application Servers and Device Servers.

It enables you to quickly determine the inventory and assets, compliance, jobs and all changes being made to any NCM Application, Device, or Combo Server.

Technical specifications

SolutionPack version
3.0

Compatible EMC M&R versions
6.8u2 and later

Compatible NCM version
NCM 9.5

Data collection methods
SQL collector

XML collector

Remote Shell collector

Main reports
Action Error Code

Certificate Monitoring: Provides detailed information about certificates, the hosts where they reside, and certificate expiration dates (end dates). These certificates govern the communication between the Application Server and Device Server and between the User Interface and Application Server. You must renew certificates before they expire or NCM will stop functioning.

Change and Change Detail reports: The `msa-user` login credentials to NCM EDAA (EMC Data Access API) are required to retrieve and view configuration differences from devices managed by NCM.

Deployment Topology

Device Compliance

Job Reporting

NCM Status

NCM Server Health

Number of Devices in this NCM

Number of Historical Jobs

Number of Interfaces in this NCM

Sites

Standard Compliance Reports: Provides information about PCI DSS 1.1, PCI DSS 1.2, PCI DSS 2.0, DISA STIG 1.1 Compliance Standards available in NCM. In the reports, you can drill down on Policies, Standards, and Tests to view detailed information.

Users

User Change Ratio Report & Config Change Distribution by Type

Views

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Configuring NCM SP with Elastic Search

Before you begin

- Perform M&R 6.8u2 installation successfully.

Procedure

1. Navigate to `/opt/APG/bin/` directory.
2. Open the /etc/sysctl.conf file.
3. Add the following line:

```
vm.max_map_count=262144
```

4. Open the /etc/security/limits.conf file.
5. Add the following line for the user:

   In this example, the user is apg.

```
apg hard nofile 65536
apg soft nofile 65536
apg hard nproc 65536
apg soft nproc 65536
```

6. Save the file.
7. To install the Elastic Search cluster package, invoke the following command:

```
./manage-modules.sh install elasticsearch-cluster
```

   When you are prompted for the IP address, provide the M&R host IP address. In the **more entries** option, select **no** unless Elastic Search needs to be configured in the cluster mode.

8. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

Following is the output:

```
open files                      (-n) 65536
max user processes              (-u) 65536
```

9. In `/opt/APG/Databases/Elasticsearch/Default/conf/elasticsearch.yml` file, add the following entry:

```
bootstrap.seccomp: false
script.max_compilations_per_minute: 120
```

In `elasticsearch.yml` file, add the above line at the end.

10. Restart Elastic Search server.

Ensure that, Elastic Search server is running.

11. Create a resource for each newly added elastic search database. Perform this operation every time a new Elastic Search node is added to the environment to scale-out backends.

For example, to create a database resource:

In Linux:

```
./bin/manage-resources.sh create dba/ES-NCM-JOBS '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://<Elastic
Search Server IP Address>:9200"],"prefix": "/
ncm*"},"settings": {"mapping": "ES-NCM-JOBS.xml"},"disabled":
false }'
```

In Windows:

```
APG PATH\bin\manage-resources.cmd create dba/ES-NCM-JOBS
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
<Elastic Search Server IP Address>"],"prefix": "/
ncm*"},"settings": {"mapping": "ES-NCM-JOBS.xml"},"disabled":
false }'
```

Note

You need to specify the IP address for <Elastic Search Server>.

12. Restart the Tomcat service.

Installing the SolutionPack for EMC Network Configuration Manager

To view data from Network Configuration Manager, install the SolutionPack for EMC Network Configuration Manager in the EMC M&R platform.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Service Assurance Suite Installation and Configuration Guide for EMC M&R* for more information.
- The Network Configuration Manager is installed and running.
- You have root login credentials for the Network Configuration Manager.
- The SolutionPack for EMC Network Configuration Manager license is uploaded to the EMC M&R platform.
- The EMC M&R platform is updated to 6.8u2 and later.

Procedure

1. Log in to the EMC M&R server with root privileges.

   For example, `https://Frontend-hostname:58443/APG`
2. Select **Administration**.
3. Select **Centralized Management** in the **Administration** tree.
4. Select **SOLUTIONPACK CENTER**.
5. Select the **EMC Network Configuration Manager** in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Accept the default name, `emc-ncm`, in the **Instance name** field.
   b. Select the EMC M&R server that will host the data collector in the **Data collection** list box.
   c. Select the EMC M&R server to host the reports in the **Reports** list box.
   d. Click **Next**.
8. Accept the default values for the **Data Collection** and **Alerting on Data Collection** panes.
9. Select the NCM server version in the **NCM Version** drop-down field in the **Server Configuration** pane.
10. Select **Device server**, **Distributed Server**, or **Combo Server** in the **NCM Server Type** drop-down field and complete the fields depending on your deployment:

Deployment	Provide information for the following fields
Device Server	Select **Device server** in the **NCM Server Type** drop-down field. • Fully qualified System IP address or host name • System root user account and password
Distributed deployment	Select **Distributed Server** for a distributed NCM server in the **NCM Server Type** drop-down field. For the Application Server, • Fully qualified System IP address or host name • System root user account and password • NCM System administrator user name (for example, `sysadmin`) and password. The NCM System credentials are required for certificate monitoring reports. To collect Database Server information, you also need: • NCM database IP address or host name • NCM database port number or accept the default port 5435 • NCM database name in EMC M&R in the **NCM instance name** field or accept the default name • NCM database password Use the **+** icon to add one or more Device, Distributed, or Combo Servers.
Combo Server	Select **Combo Server** in the **NCM Server Type** drop-down field. • Fully qualified System IP address or host name • System root user account and password • NCM System administrator user name (for example, `sysadmin`) and password. The NCM System credentials are required for certificate monitoring reports. To collect Database Server information, you also need: • NCM database port number or accept the default port 5435 • NCM database name in EMC M&R in the **NCM instance name** field or accept the default name • NCM database password

11. Optional, select the **Configure collector advanced settings** checkbox to configure the polling interval for data collection and also to configure the collection of different types of data, or accept the defaults.

    a. For Compliance, Jobs, and Inventory data, set the polling interval from 300 to 86400 seconds in the **Polling period for DB and System data collection** field or accept the default 900.

The M&R polling interval determines the frequency of data collection. For example, the default 900 means that once in every 15 minutes, polling occurs and new raw values are collected.

b. For Historical data, set the polling interval from 604800 to 2678400 seconds in the **Polling period for DB and System data collection** field or accept the default 604800.

c. If you do not want the data to be collected, clear the selected checkbox for **Compliance data**, **Jobs data**, or **Inventory data**. The latest data collection will not occur for or be updated in:

- Compliance reports like Standard Compliance Reports, Device Compliance Reports
- Jobs reports like Active Job Report and Historical Job Reports
- All inventory-related reports like database, interface reports

d. If you have selected Jobs Data to be collected in the above step, you have an option to use the new Elastic Search DB . Clear the **Enable ElasticSearch DB** checkbox, If you want to continue using the MySql DB for Jobs data.

e. Select **Reconcile Device Names**, if you want to discover the common devices across Smarts SP and NCM SP.

f. Optional, select **Advanced Search Feature** if you want to allow the EMC M&R search engine to search all metrics collected by the SQL Collector.

12. Click **Next** on the **Data Collection** pane.

Note

In the **Data Collection** pane when you select the **Enable ElasticSearch DB** check box, you must select **Use ElasticSearch DB** in the **Events** and **Reports** pane also. If you clear the **Enable ElasticSearch DB** check box in the **Data Collection** pane, you must deselect **Use ElasticSearch DB** check box in the **Events** and **Reports** pane also.

---

13. In the **Events** pane, select **Use ElasticSearch DB**, if you have used Elastic Search DB for jobs data collection.
14. Enter the Hostname or IP address details of the Elastic Search DB.
15. In the **Reports** section, select the gateway and the administration web-service instance or accept the default values.
16. Select the **Use ElasticSearch DB** checkbox, if you have used Elastic Search DB for jobs data collection.
17. Select **Install** to install the SolutionPack.

After you finish

Allow four to five polling cycles to pass before viewing reports.

Post-installation steps

Setting the IP address of the EMC M&R server

After you install the SolutionPack for EMC Network Configuration Manager, you must configure the IP address of the EMC M&R server in the NCM Application Server. If the EMC M&R IP address was already set during the NCM installation, skip this task.

Procedure

- Follow these steps to set the IP address of the EMC M&R server in the NCM Application Server:

Operating system	Steps
Linux	1. Open the `<Product directory>/db/controldb/data/pg_hba.conf` file for editing. 2. Add this line at the end of the `pg_hba.conf` file: `host all all <EMC M&R IP address>/32 md5` 3. Save and exit the `pg_hba.conf` file. 4. Open the `<Product directory>/db/controldb/data/postgresql.conf` file for editing. 5. Find the line `#listen_addresses = 'localhost'`. 6. Add the EMC M&R entry. For example: `listen_addresses = 'localhost,10.31.149.68,10.31.151.223'` 7. Save and exit the `postgresql.conf` file. 8. Type `service controldb restart` to restart the controldb service.
Windows	1. Open the `<Product directory>\db\controldb\data\pg_hba.conf` file for editing. 2. Add this line at the end of the `pg_hba.conf` file: `host all all <EMC M&R IP address>/32 md5` 3. Save and exit the `pg_hba.conf` file. 4. Open the `<Product directory>\db\controldb\data\postgresql.conf` file for editing. 5. Find the line `#listen_addresses = 'localhost'`. 6. Add the EMC M&R entry. For example: `listen_addresses = 'localhost,10.31.149.68,10.31.151.223'` 7. Save and exit the `postgresql.conf` file. 8. Navigate to **Start** > **Administrative Tools** > **Services** > **NCM_Controldb** to restart the `controldb` service.

- If you have selected ElastiSearch DB for Jobs data, you need to manually create the schema. You have to create the following ES-NCM-JOBS resource for the tomcat server, This enables the connection to NCM Jobs database. For example, to create a schema:

In Linux:

```
Elastic Search:
        ./bin/manage-resources.sh create dba/ES-NCM-JOBS
'{ "type": "elasticsearch", "datasource":
        { "hosts": ["http://<Elastic Search Server IP Address>:
9200"],"prefix": "/ncm*"},"settings": {"mapping": "ES-NCM-
JOBS.xml"},
        "disabled": false }'
```

In Windows:

```
Elastic Search:
         APG PATH\bin\manage-resources.cmd create dba/ES-NCM-
JOBS '{ "type": "elasticsearch",
         "datasource": { "hosts": ["http://<Elastic Search
Server IP Address>:9200"],"prefix": "/ncm*"},"settings":
{"mapping":
         "ES-NCM-JOBS.xml"},"disabled": false }'
```

- Restart Tomcat service.

Setting the collector heap memory size in the EMC M&R UI

Use the EMC M&R UI to set the collector heap memory size to run the SolutionPack reports. Since the SolutionPack for EMC Network Configuration Manager collects data from a large number of devices, you may need to increase the collector heap memory to a suitable level.

Before you begin

1. For additional details about determining configuration size, refer to or *EMC Service Assurance Suite SolutionPack Performance and Scalability Guidelines* available on the EMC Online Support website.

Procedure

1. Log in to EMC M&R with root privileges.

   For example, `https://Frontend-hostname:58443/APG`

2. Go to **Administration** > **Centralized Management** > **Logical Overview** > **Collecting** > **Collector-Manager::*emc-ncm-<host-id>***
3. Expand **Configuration Files**.
4. Scroll to the `conf/unix-services.properties` file or the `conf/win-services.properties` file.
5. Edit the `conf/unix-services.properties` or `conf/win-services.properties` file by setting the collector heap memory value in the memory.max parameter.

   Set the value based on the Planner tool sizing information.

6. Click **Save**.
7. SSH to the EMC M&R Collector host.
8. Log in with root privileges to the EMC M&R Collector host and navigate to the `bin` directory of the EMC M&R installation.

9. Update the collector service. In this case, the service is **`collector-manager emc-ncm`**. Type the command for your operating system from the `bin` directory of the EMC M&R installation.

   For UNIX, type:

   ```
   ./manage-modules.sh service update collector-manager emc-ncm
   ```

   For Windows, type:

   ```
   manage-modules.cmd service update collector-manager emc-ncm
   ```

10. Restart the collector service (**`collector-manager emc-ncm`**) that stopped as a result of the `update` command. Type the command for your operating system from the `bin` directory of the EMC M&R installation.

    For UNIX, type:

    ```
    ./manage-modules.sh service start collector-manager emc-ncm
    ```

    For Windows, type:

    ```
    manage-modules.cmd service start collector-manager emc-ncm
    ```

Vstatus Configuration

After you install the SolutionPack for EMC Network Configuration Manager, you must configure the variable status task for the SQL Collector. Use the EMC M&R UI to change the value from 14 days to 1 day to avoid stale data in NCM reports. To configure the vstatus filter for the Activity table report, the configuration of variable status is modified to take care of the inactive metrics. To configure variable status, perform the following procedure:

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Scheduled Tasks**.
3. In the **Scheduled Tasks** pane, click the **Backend** category.
4. In the **Task backend/Default/import_variable_status.task** pane, expand **Configuration Files**.
5. Click the pencil icon for **data/task_repository/backend/Default/import_variable_status.task**.

   The `import_variable_status.task` file opens.
6. For the `inactive` parameter, change **`14d`** to **`1d`**.

   Before editing:

   ```
   <param>{"inactive":"14d","vgroups":[{"condition":
   [{"source":"VMWareCollector"}], "group":
   ```

```
["vcenter","devtype","parttype"],"max-inactive":"24h"},
{"condition": [{"source":"VMWareCollector"}], "group":
["vcenter","devtype"],"max-inactive":"24h"},{"condition":
[{"devtype":"FabricSwitch"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"condition": [{"devtype":"PassiveHost"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"group":
["devtype","device","source","parttype","collcfg"],"max-
inactive":"24h"},{"group":
["devtype","device","source","parttype","datagrp"],"max-
inactive":"24h"},{"group":
["devtype","device","source","datagrp"],"max-inactive":"24h"},
{"group":["devtype","device"],"max-inactive":"24h"}]}</param>
```

For **MySQL**, for DB activity and job use the following configuration:

After editing:

```
<param>{"inactive":"1d","vgroups":[{"condition":
[{"source":"EMC-NCM"},{"parttype":"DBACTIVITY"}], "group":
["appsrv"],"max-inactive":"5m"},{"condition": [{"source":"EMC-
NCM"},{"parttype":"JOBS"}], "group":["appsrv"],"max-
inactive":"5m"},{"condition": [{"source":"VMWareCollector"}],
"group":["vcenter","devtype","parttype"],"max-
inactive":"24h"},{"condition":
[{"source":"VMWareCollector"}], "group":
["vcenter","devtype"],"max-inactive":"24h"},{"condition":
[{"devtype":"FabricSwitch"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"condition": [{"devtype":"PassiveHost"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"group":
["devtype","device","source","parttype","collcfg"],"max-
inactive":"24h"},{"group":
["devtype","device","source","parttype","datagrp"],"max-
inactive":"24h"},{"group":
["devtype","device","source","datagrp"],"max-inactive":"24h"},
{"group":["devtype","device"],"max-inactive":"24h"}]}</param>
```

For **Elastic Search**, for DB activities only use the following configuration:

After editing:

```
<param>{"inactive":"1d","vgroups":[{"condition":
[{"source":"EMC-NCM"},{"parttype":"DBACTIVITY"}], "group":
["appsrv"],"max-inactive":"5m"},{"condition":
[{"source":"VMWareCollector"}], "group":
["vcenter","devtype","parttype"],"max-inactive":"24h"},
{"condition": [{"source":"VMWareCollector"}], "group":
["vcenter","devtype"],"max-inactive":"24h"},{"condition":
[{"devtype":"FabricSwitch"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"condition": [{"devtype":"PassiveHost"}], "group":
["device","parttype","datagrp"],"max-inactive":"24h"},
{"group":
["devtype","device","source","parttype","collcfg"],"max-
inactive":"24h"},{"group":
["devtype","device","source","parttype","datagrp"],"max-
inactive":"24h"},{"group":
["devtype","device","source","datagrp"],"max-inactive":"24h"},
{"group":["devtype","device"],"max-inactive":"24h"}]}</param>
```

7. Click **Save**.
8. Click **Restart** in the **Service Status** pane to restart the collector-manager service.

Configuring Certificate Monitoring reports with NCM server running 9.5

Additional steps are required for the Certificate Monitoring reports to work on the NCM server running version 9.5 software. These steps are required for accessing the WS API in NCM used by the Certificate Monitoring reports. Otherwise, the logs show certificate and communication errors and the Certificate Monitoring reports are empty.

Before you begin

Install version 9.5 software on the NCM server. If you are using a third-party certificate, follow the procedures in Configuring Certificate Monitoring reports with NCM server running 9.5 - Third-party certificate installed on page 137.

Procedure

1. Log in to the NCM host and copy `"$VOYENCE_HOME/conf/bundle.p12"` to the EMC M&R destination machine where the WS API client is configured (for example, `/opt`).
2. On the destination machine, type the following command as one line and press **Enter**:

```
$APG_HOME/Java/Sun-JRE/8.0.92/bin>keytool -changealias -
keystore "/opt/bundle.p12" -alias 1 -destalias newalias -
storetype pkcs12
```

3. Enter the keystore password.

   Type the PassPhrase entered during the NCM server installation.
4. On the destination machine, type the following command as one line and press **Enter**.

```
$JAVA_HOME/bin>keytool -importkeystore -srckeystore "/opt/
bundle.p12" -destkeystore "$APG_HOME/Java/Sun-JRE/8.0.92/lib/
security/cacerts" -srcstoretype pkcs12
```

5. Enter the destination keystore password: **`changeit`**
6. Enter the source keystore password.

   Type the PassPhrase entered during the NCM server installation.

   These results should display:

   ```
   Entry for alias 1 successfully imported. Import command
   completed: 1 entries successfully imported, 0 entries
   failed or cancelled.
   ```
7. Go to the `<EMC_M&R_install>/bin` directory and run the following command to restart all of the services:

```
./manage-modules service restart all
```

The following exception message should no longer display in the collector logs (`APG/Collecting/Collector-Manager/emc-ncm/logs`):

```
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building
failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested
target at
sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
```

Configuring Certificate Monitoring reports with NCM server running 9.5 - Third-party certificate installed

Additional steps are required for the Certificate Monitoring reports to work on the NCM server running version 9.5 software. These steps are required for accessing the WS API in NCM used by the Certificate Monitoring reports. Otherwise, the logs show certificate and communication errors and the Certificate Monitoring reports are empty.

Before you begin

Install version 9.5 software on the NCM server. If you are not using a third-party certificate, follow the procedures in Configuring Certificate Monitoring reports with NCM server running 9.5 on page 136.

Procedure

1. Log in to the NCM host and copy "`$VOYENCE_HOME/conf/server.p12`" to the EMC M&R destination machine where the WS API client is configured (for example, `/opt`).

   `server.p12` will be generated when installing the third-party certificate using the SSL utility for NCM.

2. On the destination machine, type the following command as one line and press **Enter**:

   ```
   $APG_HOME/Java/Sun-JRE/8.0.92/bin>keytool -changealias -
   keystore "/opt/server.p12" -alias 1 -destalias newalias -
   storetype pkcs12
   ```

3. Enter the keystore password.

   Use the same password given during certificate installation.

4. On the destination machine, type the following command as one line and press **Enter**.

   ```
   $JAVA_HOME/bin>keytool -importkeystore -srckeystore "/opt/
   server.p12" -destkeystore "$APG_HOME/Java/Sun-JRE/8.0.92/lib/
   security/cacerts" -srcstoretype pkcs12
   ```

5. Enter the EMC M&R destination keystore password: **`changeit`**
6. Enter the source keystore password.

   Use the source keystore password given during certificate installation.

   These results should display:

```
Entry for alias 1 successfully imported. Import command
completed: 1 entries successfully imported, 0 entries
failed or cancelled.
```

7. Go to the `<EMC_M&R_install>/bin` directory and run the following command to restart all of the services:

```
./manage-modules service restart all
```

The following exception message should no longer display in the collector logs (`APG/Collecting/Collector-Manager/emc-ncm/logs`):

```
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building
failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested
target at
sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
```

Configuring access to Change Detail Reports

The first time you attempt to view a Change Detail Report, you will see a certificate warning message. To resolve the message and view the report, you need to accept the certificate and authenticate the msa-user account credentials to the NCM EDAA server. Depending on your browser, perform the steps in these troubleshooting topics to configure access to all Change Detail Reports:

- Troubleshooting Change Detail Report certificate errors in Chrome on page 140
- Troubleshooting Change Detail Report certificate errors in Firefox on page 141
- Troubleshooting Change Detail Report certificate errors in Internet Explorer on page 141

The Change Detail Reports contain the configuration differences and audit trails for devices managed by NCM. These reports require access to an external URL. The external web application is hosted on the NCM EDAA (also called MSA) Tomcat server in your NCM deployment. The default user name is **`msa-user`** and the default password is **`sysadmin`**. To allow authentication to this application, a CAS authentication server is deployed along with ncm-msa service. When you try to access the Change Detail Reports, the UI prompts you for the username and password.

If needed, use this procedure to change the NCM EDAA password: Changing the NCM EDAA password to access Change Detail Reports on page 138

Changing the NCM EDAA password to access Change Detail Reports

To change the NCM EDAA password, you must do so from the NCM server where the NCM EDAA Tomcat server resides. For a distributed NCM server deployment, you need to change the password in the Application Server host.

Procedure

1. Run `[Product_directory]/tools/password-change.pl`.
2. Select the option **[C]hange Single Password**.
3. Select **msa-user** from the list of users and enter the new password.

4. Restart the vcmaster service by typing:

```
service vcmaster restart
```

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Upgrading NCM SolutionPack from 6.7u1 to 6.8u2

Before you begin

Download the EMC M&R 6.8u2 build from EMC Online Support website at http://support.emc.com.

Procedure

1. Upgrade the EMC M&R core to 6.8u2, by invoking the following command:

   ```
   sh setup-linux-x86_64-v95.sh
   ```

   For more details, refer the *EMC M&R 6.8u2 Installation and Configuration guide* for M&R Core upgrade procedures.

2. To upgrade the platform:

   ```
   /opt/APG/bin/manage-modules.sh update module-manager
   /opt/APG/bin/manage-modules.sh service update all
   /opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
   ```

3. Install the Elastic Search cluster package, see Configuring NCM SP with Elastic Search on page 127 for more information.
4. Update the NCM SolutionPack.
5. Install events block after upgrading , if Elastic Search DB is needed for Jobs data.
6. If Elastic Search needs to be used for jobs data , select the option **Enable ElasticSearch DB** in **Browse and Install SolutionPacks** screen. See Installing the SolutionPack for EMC Network Configuration Manager on page 129 for more information.

   Data collection and Reports Blocks are updated.

7. Install the Event block manually for upgrading the NCM SolutionPack from 6.7u1 to 6.8u2. Installing the event block on page 140.
8. Start the Event Processing manager.
9. Restart tomcat services.

Installing the event block

You must install the Event blocks manually, when you are upgrading the NCM SolutionPack from 6.7u1 to 6.8u2.

Procedure

1. Log in to the EMC M&R server with root privileges.
2. Select **Administration**.
3. Select **Centralized Management** in the **Administration** tree.
4. Select **SOLUTIONPACK CENTER**.
5. Select the **EMC Network Configuration Manager** in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select instance only from the **Events** drop-down list.

   *Do not select the instance for **Data collection** and **Reports**.*
8. Create the resources as displayed in the post install message, see Configuring NCM SP with Elastic Search on page 127 for more information.

Troubleshooting

Report display problems

- Review the `Collecting.log` file located in **Centralized Management** > **Logical Overview** > **Collecting** > **Collector-Manager::*emc-ncm-<host-id>***.
- Troubleshooting Change Detail Report certificate errors in Chrome on page 140
- Troubleshooting Change Detail Report certificate errors in Firefox on page 141
- Troubleshooting Change Detail Report certificate errors in Internet Explorer on page 141
- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Troubleshooting a broken connection between NCM and EMC M&R on page 143

Troubleshooting Change Detail Report certificate errors in Chrome

A certificate error displays when connecting to the Change Detail Report from EMC M&R in the SolutionPack for EMC Network Configuration Manager.

Note

Firefox is the recommended browser for viewing reports in the EMC M&R SolutionPack. If the problems with Chrome persist, try using a different browser.

The steps may vary slightly depending on your browser version.

Procedure

1. On the report that generates the SSL error message, right-click and select **View frame source**.
2. In the **View Frame Source** tab, click **Advanced**.
3. Click **Proceed to <*Server name/IP address*>**.
4. Wait for the content to load.
5. Go back to the report, right-click and select **Reload frame**.
6. In the **EMC Smarts Network Configuration Manager authentication** pane, log in to the NCM EMC Data Access API (EDAA) with the msa-user account credentials (defaults: `msa-user/sysadmin`).

   The report displays in the frame.

Troubleshooting Change Detail Report certificate errors in Firefox

A certificate error displays when connecting to the Change Detail Report from EMC M&R in the SolutionPack for EMC Network Configuration Manager.

The steps may vary slightly depending on your browser version.

Procedure

1. On the report that generates the `This Connection is Untrusted` error message, right-click and select **This Frame** > **Open Frame in New Tab**.
2. Click **I understand the Risks**.
3. Click **Add Exception**.
4. Click **Confirm Security Exception**.
5. Go back to the report, right-click and select **This Frame** > **Reload Frame**.
6. In the **EMC Smarts Network Configuration Manager authentication** pane, log in to the NCM EMC Data Access API (EDAA) with the msa-user account credentials (defaults: `msa-user/sysadmin`).

   The report displays in the frame.

Troubleshooting Change Detail Report certificate errors in Internet Explorer

A certificate error displays when connecting to the Change Detail Report from EMC M&R in the SolutionPack for EMC Network Configuration Manager.

Note

Firefox is the recommended browser for viewing reports in the EMC M&R SolutionPack. If the problems with Internet Explorer persist, try using a different browser.

The steps may vary slightly depending on your browser version.

Procedure

1. On the report that generates the `Content was blocked` error message, click **Show Content**.
2. Click **Proceed to the Page**.
3. Click the certificate error and select **View Certificate**.

4. Follow the prompts to save the certificate under Trusted Root Certificates.
5. Log in to the EMC M&R server (defaults: `admin/changeme`).
6. Go back to the report.
7. In the **EMC Smarts Network Configuration Manager authentication** pane, log in to the NCM EMC Data Access API (EDAA) with the msa-user account credentials (defaults: `msa-user/sysadmin`).

   The report displays in the frame.

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

Troubleshooting a broken connection between NCM and EMC M&R

You can analyze the SolutionPack for EMC Network Configuration Manager logs in EMC M&R to troubleshoot a broken connection.

Procedure

1. Log in to the EMC M&R server.
2. Go to the `/opt/APG/Collecting/Collector-Manager/<ncm_instance_name>/logs` directory to view the log files.

   For Linux, navigate to your emc-ncm instance and check the log files, `/opt/APG/Collecting/Collector-Manager/<emc-ncm-instance-name>/logs/collecting-0-0.log`
   For Windows, navigate to `C:\Program Files\APG\Collecting\Collector-Manager\<emc-ncm-instance-name>\logs\collecting-0-0.log`

CHAPTER 8

SolutionPack for Optical Wavelength Services Summary Sheet

- Overview 146
- Technical specifications 146
- Where to find the latest SolutionPack software 146
- Installing a SolutionPack 147

Overview

Learn how to install and configure the SolutionPack for Optical Wavelength Services. This SolutionPack discovers and monitors TMF864-compliant Element Management Systems.

Use this SolutionPack as one component of your Optical Transport Manager (OTM) deployment. Other components include

- EMC Smarts 9.4 Optical Transport WDM-NG domain manager
- EMC Smarts 9.4 Service Assurance Manager
- EMC M&R 6.5u1 with SolutionPack for EMC Smarts installed

Data flow among the OTM components
The SolutionPack for Optical Wavelength Services uses a Stream Collector (SC) to poll TMF 864-compliant Element Management Systems (EMS) at a configurable polling interval. The information that is collected is persisted in the EMC M&R database so that the EMC Smarts WDM-NG domain manager can retrieve the data and build topology based on the property information. The SC makes SOAP WebService requests to the EMS to retrieve the topology and extract information. First the authentication / login request is sent and then the security ID is extracted. This security ID (session ID) is sent as part of the SOAP envelope in all the subsequent calls.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Supported Element Management Systems (EMS)
TMF864-compliant Element Management Systems such as Coriant Intelligent Node Manager SR 6.0 SP2

Data collection method

- Stream collector (for data parsing)
- Stream listener (for event processing)

Main reports
There are no reports associated with this SolutionPack. You must install the SolutionPack for EMC Smarts to view reports and topology associated with data collected from TMF 864-compliant Element Management Systems. View Topology maps under **Explore** > **Network** and Notifications under **Operations** > **Notifications**.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC support website http://support.emc.com.
- Ensure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.
- Obtain the login credentials and protocol information for the TMF864-compliant Element Management System(s)
- Ensure all software for your EMC Smarts Optical Transport Manager deployment is installed with services running.

Table 4 Software components required when collecting data from optical networks

Software component	Purpose
EMC Smarts Optical Transport Manager installed with WDM-NG domain manager service	Analyzes the events collected by the SolutionPack for Optical Wavelength Services and determines the root cause of problems occurring in the optical network.
EMC Smarts Service Assurance Manager installed with Notification Cache Publishing	Converts events to notifications and sends the root cause and impact to the SolutionPack for EMC Smarts.
SolutionPack for EMC Smarts	Provides reports showing notifications and topology collected from the optical network.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Review the default instance name and edit if needed.

You may install more than one instance of the SolutionPack. Each instance name must be unique and connected to different Element Management Systems.

b. Select the EMC M&R servers in one or more list boxes. For example, select the collector host in the **Data collection** and the backend host in the **Events** list boxes.

c. Click **Next**.

8. For each list box you select, a screen appears.

   a. Click **Next** after you complete each screen.

      Default RabbitMQ credentials are `admin` and `changeme` when using SAM with Notification Cache Publishing enabled.

   b. Click **Install** after you complete the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

CHAPTER 9

Excluding Planned Maintenance Periods from Reports

- Planned maintenance periods 150
- Creating a maintenance period 150
- Associating a maintenance period with a report 151
- Installing Maintenance Manager 151

Planned maintenance periods

Learn how to exclude maintenance period data from the totals in a graph or table report by creating a maintenance period, assigning devices to it using names or a filter, and associating it with a report. As a result, data for devices in planned maintenance periods does not affect the report totals.

This feature is implemented by the EMC M&R Maintenance Manager module. The Maintenance Manager replaces the Outage Manager and Outage Detector that existed in previous M&R releases. In an upgrade situation, outages that were defined by the older Outage Manager are honored by Maintenance Manager.

Note

The previous Outage Detector feature that permitted a user to view and edit a list of maintenance periods is not supported by Maintenance Manager.

Creating a maintenance period

Procedure

1. Click **Administration**.
2. **Select Modules** > **Maintenance Editor**.
3. Type a title for the maintenance period
4. Select a start date and end date.
5. Optionally, enter a comment.

   The comment will appear on the maintenance period when the maintenance period appears in a report. The following graphic illustrates a report with an associated maintenance period, which is indicated by yellow. Text from the **Comment** field is indicated by the small red box.

   Figure 7 Text from comment field

6. To keep the maintenance period out of report totals, leave the **Use in report computation** field blank
7. Select the devices to which the maintenance period applies.

Option	Description
Add with Filter	Select from a list of devices that match the values specified in the Edit Mode settings **Outages type** and **Outages property**.
Add by Name	Enter the name of a device.

The devices are displayed in the Objects list.

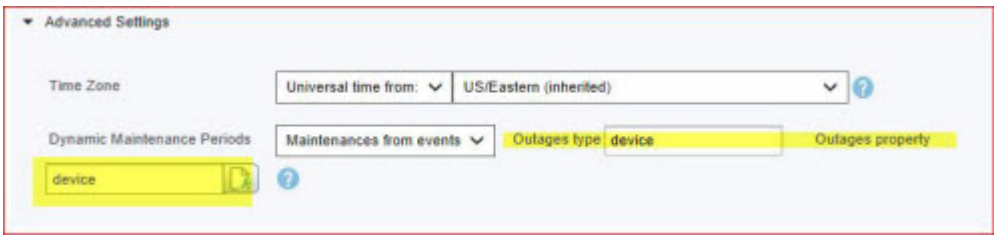
8. Click **Save**.

Associating a maintenance period with a report

Procedure

1. With a report displayed, click **Edit Mode**.
2. Click the **Report Configuration** tab.
3. Click **Advanced Settings**.
4. In **Dynamic Maintenance Period**, select **Maintenance from Events**.
5. Set the **Outages type** to the category set in the Maintenance Editor.

   Figure 8 Outages type and Outages property



6. Set the **Outages property** to the property you will use for matching.

Assume you have created a maintenance period with a category value of "device" and the objects "localhost" and "lglad118". You have a report in your tree, and on that node, you have the property "part" whose value is "localhost". If you were to set outage type to "device" and outage property to "part", then the "localhost" object from the maintenance period would be matched with the "part" property from the node, and the maintenance period would apply. The maintenance periods that match the values for outages type and the outages property will appear in this report.

Installing Maintenance Manager

Use this procedure to install Maintenance Manager.

Typically, the Maintenance Manager is installed automatically with other modules during normal installations. In certain upgrade situations, the Maintenance Manager is not installed. For example, if your existing installation did not include the Maintenance Manager, then an upgrade also would not include it.

Your site needs a license to use the Maintenance Manager. If you need a license, contact EMC Technical Support.

If you receive an error message after navigating to **Administration** > **Modules** > **Maintenance Editor**:

- Make sure you have a license to use Maintenance Manager.
- Install Maintenance Manager, if needed.

Note

If you do not have a license for Maintenance-Manager, contact EMC Technical Support.

Procedure

1. Navigate to **Administration** > **Centralized Management** > **Physical Overview** > ***server_name***.
2. In the right pane, click the green **Install** button.
3. On the **Packages Installation** screen:
   a. In the **Categories** list, select **Block**.
   b. In the **Packages** list, select **generic-maintenance-manager-*vx.x.x***, where *vx.x.x* matches the EMC M&R installed version on the server.
   c. Click **Launch** at the bottom of the page.
4. Provide an instance name for the component and click **Install**.
5. Install each component as the UI presents them on the screen, clicking **Install** for each one.
6. For the **generic-maintenance-manager** component, provide the following information on the installer command line when the prompts appear:

Database Type	1
Database hostname or IP address	IP address of the Events Database server
Database port [53306]	typically use the default
Database name [events]	typically use the default
Database username [apg]	typically use the default
Database password	password for the apg user on the database
Listener port [22666]	typically use the default

7. Type **yes** to start the installed services.
8. When the installation completes, add the new resource to the Tomcat service, as follows:
   a. Navigate to **Centralized Management** > **Miscellaneous** > **WebServers** > **Tomcat** > **Default-<*servername*>**.
   b. Under **Configuration Files**, locate the `APG.xml` file.
   c. Make sure that the following line is present in the file. If not, then add it.

```
<Resource name="outage/OUTAGE-MANAGER"
factory="org.apache.naming.factory.BeanFactory"
type="com.watch4net.apg.v2.gui.action.outage.OutageConnectio
nFactory"
/>
```

d. Save the file.

e. If you changed the file, restart the Tomcat service.

9. Navigate to **Administration** > **Modules** > **Maintenance Editor** to use Maintenance Manager features.

PART 2

SolutionPacks for Mobile Devices

This section describes these SolutionPacks.

Chapter 10, "SolutionPack for Ericsson eNodeB Summary Sheet"

Chapter 11, "SolutionPack for Ericsson IMS CSCF Summary Sheet"

Chapter 12, "SolutionPack for Ericsson IMS HSS SLF Summary Sheet"

Chapter 13, "SolutionPack for Ericsson IMS IPWorks Summary Sheet"

Chapter 14, "SolutionPack for Ericsson IMS MRFP Summary Sheet"

Chapter 15, "SolutionPack for Ericsson IMS MTAS Summary Sheet"

Chapter 16, "SolutionPack for Ericsson IMS SOI Summary Sheet"

Chapter 17, "SolutionPack for Ericsson IMS TSP Summary Sheet"

Chapter 18, "SolutionPack for Ericsson MGW Summary Sheet"

Chapter 19, "SolutionPack for Ericsson RNC Summary Sheet"

Chapter 20, "SolutionPack for Ericsson SGSN Summary Sheet"

Chapter 21, "SolutionPack for Huawei iManager M2000 Summary Sheet"

Chapter 22, "SolutionPack for ip.access nano3G Small Cell Summary Sheet"

CHAPTER 10

SolutionPack for Ericsson eNodeB Summary Sheet

- Overview 158
- Technical specifications 158
- Where to find the latest SolutionPack software 158
- Performing prerequisite installation tasks 158
- Installing a SolutionPack 159
- Performing post installation tasks 160
- Confirming report creation 160

Overview

Learn how to install and configure the SolutionPack for Ericsson eNodeB. This SolutionPack is a mobile network management solution designed to generate reports that show key metrics and key performance indicators (KPIs) for Ericsson eNodeB nodes. It provides real-time and historical performance reports.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
Stream collector

Main reports

Dashboard

Shows snapshots of key performance indicator (KPI) reports. You can drill down into these individual KPI reports per eNodeB and per cell:

- Inventory of network elements monitored by this SolutionPack
- Session Setup Success Rate (KPI)
- eNodeB Availability (KPI)
- Throughput (DL/UL KPIs)
- Intra-Freq Handover Success Rate (KPI)
- Drop Rate (KPI)

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from eNodeB nodes be locally available on the EMC M&R server hosting the Stream

collector. You must ensure the Operations Support System-Radio and Core (OSS-RC) can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from the OSS-RC to the EMC M&R server. Contact the OSS-RC administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and the OSS-RC server.
3. Configure OSS-RC to push the raw PM data files on a regular time interval to this default directory on the EMC M&R server: `<install directory>/Collecting/Stream-Collector/<SP-name>/IncomingData/`

   Here is an example of the name of a PM file: `A20140710.0545+0300-0600+0300_SubNetworkONRM_RootMo,SubNetworkLTERAN,MeContextABC123_statsfile.xml`.

   You can override the default directory during the SolutionPack installation.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.

8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. If you selected `Move` as the **Post processing action** during the installation, which keeps all processed performance management XML files, make sure you have a maintenance task running on the server that periodically deletes these files. You can do this manually or by scheduling Cron jobs.
2. If using the default directory to store the performance management XML files, verify that the `apg` user has read/write permissions on it.
3. If not using the default directory, make sure the directory that you are using to store the performance management XML files is on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 11

SolutionPack for Ericsson IMS CSCF Summary Sheet

- Overview 162
- Technical specifications 162
- Where to find the latest SolutionPack software 163
- Collecting performance parameters 163
- Node, performance category, default file name pattern and 3GPP format 164
- Configuring the user process limits for a Linux installation 164
- Installing a SolutionPack 165
- Confirming report creation 166
- Troubleshooting 166

Overview

Learn how to install and configure the ReportPack for Ericsson IMS CSCF (Call Session Control Function). This SolutionPack monitors all signaling from end-users to services and other networks in the IP Multimedia Subsystem and provides comprehensive performance information about CSCF.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Performance measurement data
The SolutionPack for Ericsson IMS TSP monitors and collects performance measurement data for this SolutionPack. If you want to generate the reports that show this data, make sure you install the SolutionPack for Ericsson IMS TSP.

Main reports
Summary Active Users / Registrations

Summary Failed Registrations

Summary Active Sessions

Summary CSCF Session Establishment in Busy Hour

Summary Dropped Sessions

Summary IMS-AKA Successful Authentications

Summary IMS-AKA Failed Authentications

Summary Accounting Requests

TSP – CSCF

CSCF:

- CSCF Registrations
- CSCF Sessions
- Emergency Sessions
- IMS AKA Authentication
- Session Initiator Protocol (SIP) traffic
- Diameter (Cx - Rf)

Equipment-Related Measurements:

- Summary of Equipment Related Measurement
- CPU Load (Maximum and Average %) of each Processor and System

- Disk Usage per IO Processor
- IPv4 Statistic per Interface
- Memory Usage (Used, Free, and Maximum %) of each Processor and System
- Cluster and Processor Uptime

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/cscf`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/cscf`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.
5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for each file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 5 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
CSCF	Cscf	`A20.*_Cscf`	`nPMF 32.401v5.0`
CSCF	Cscf2	`A20.*_Cscf2`	`nPMF 32.401v5.0`
CSCF	CscfSipServer	`A20.*_CscfSipServer`	`nPMF 32.401v5.0`
CSCF	CscfSipClient	`A20.*_CscfSipClient`	`nPMF 32.401v5.0`
TSP	IPv4_MeassurementJob	`A20.*cscf.*_IPv4.*`	`nPMF 32.401v5.0`
TSP	Diameter	`A20.*cscf.*_Diameter.*`	`nPMF 32.401v5.0`
TSP	PlatformMeassures	`A20.*cscf.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP	IPv6_MeassurementJob	`A.*cscf.*_IPv6.*`	`nPMF 32.401v5.0`
TSP	OamProvision-Meassurement	`A20.*cscf.*_OamProvisioning.*`	`nPMF 32.401v5.0`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

In this example, the user is `apg`.

```
apg   hard  nofile  65534
apg   soft  nofile  65534
apg   hard  nproc   65534
apg   soft  nproc   65534
```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ```

   ```
   ./manage-modules.sh service start all
   ```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .

2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*

5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 12

SolutionPack for Ericsson IMS HSS SLF Summary Sheet

- Overview 170
- Technical specifications 170
- Where to find the latest SolutionPack software 171
- Collecting performance parameters 171
- Node, performance category, default file name pattern and 3GPP format 172
- Configuring the user process limits for a Linux installation 172
- Installing a SolutionPack 173
- Confirming report creation 174
- Troubleshooting 174

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS HSS SLF (Subscriber Locator Function). The Home Subscriber Server (HSS) is the central IMS user database that stores all IMS subscription information. The SolutionPack for Ericsson IMS HSS SLF reports on the information in the HSS, including user registration and user subscription.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Performance measurement data
The SolutionPack for Ericsson IMS TSP monitors and collects performance measurement data for this SolutionPack. If you want to generate the reports that show this data, make sure you install the SolutionPack for Ericsson IMS TSP.

Main reports
Diameter (Cx):

- IMS Number of Protocol Errors and Permanent Failures per HSS, SLF
- IMS Number of Sent / Received Requests
- IMS Number of Sent / Received Answers
- IMS Number of Sent / Received Unsuccessful Answers
- IMS Number of Incoming / Outgoing Discarded Messages

HSS

SLF:

- SLF Overall Summary
- IMS SLF Number of Users
- Redirected Correct Answers Per Destination Server (per Node)
- Number of Dx Answers with the DIAMETER_ERROR_USER_UNKNOWN (per CSCF)
- Number of Dx Answers with the DIAMETER_REALM_NOT_SERVED
- IMS SLF Dx-Query Attempts (per second) per CSCF
- IMS SLF Dx-Query Answer Success (per second) per CSCF

Equipment-Related Information:

- CPU Load (Max, Avg) % each processor and system
- DiskUsage per IO processor

- IPv4 Statistic per Interface
- Memory (Used, Free, Max) % each processor and system
- ProcessorUptime per processor
- TSPClusterUptime

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/hss_slf`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/hss_slf`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.
5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for each file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 6 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
HSS-SLF	ISM	`A20.*_HSS-ISM`	`nPMF 32.401v5.0`
HSS-SLF	SLF	`A20.*_HSS-SLF`	`nPMF 32.401v5.0`
HSS-SLF	SDA	`A20.*_HSS-SDA`	`nPMF 32.401v5.0`
TSP	IPv4_MeassurementJob	`A20.*hss.*_IPv4.*`	`nPMF 32.401v5.0`
TSP	Diameter	`A20.*hss.*_Diameter.*`	`nPMF 32.401v5.0`
TSP	PlatformMeassures	`A20.*hss.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP	IPv6_MeassurementJob	`A.*hss.*_IPv6.*`	`oPMF 32.401v5.0`
TSP	OamProvision-Meassurement	`A20.*hss.*_OamProvisioning.*`	`nPMF 32.401v5.0`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

```
apg   hard  nofile  65534
apg   soft  nofile  65534
```

```
apg   hard  nproc   65534
apg   soft  nproc   65534
```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.

5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 13

SolutionPack for Ericsson IMS IPWorks Summary Sheet

- Overview 178
- Technical Specifications 178
- Where to find the latest SolutionPack software 179
- Collecting performance parameters 179
- Node, performance category, default file name pattern and 3GPP format 179
- Configuring the user process limits for a Linux installation 180
- Installing a SolutionPack 181
- Confirming report creation 181
- Troubleshooting 182

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS IPWorks. Ericsson IPWorks delivers centrally managed Domain Name System (DNS), Telephone Number Mapping (ENUM), and Dynamic Host Configuration Protocol (DHCP) services for mobile and wireline IP networks.

This SolutionPack collects and reports on data related to the ENUM & DNS functions in an IMS network as well as equipment related measurements such as CPU and memory utilization, disk capacity, system load, and interface statistics.

Technical Specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Main reports
IPWorks (ENUM / iDNS):

- Summary Total Number of DNS queries
- Summary Number DNS Query Requests [per second]
- Summary Number ENUM Requests [per second]
- Summary Number of ENUM Requests
- Summary Number of MAP Queries
- Summary Statistic per Location

IPWorks (ENUM / iDNS):

- DNS
- ENUM
- ERH

Equipment-Related Measurement per Storage Server (dnsst):

- CPU
- Memory
- Disk
- System Load
- Interface

Equipment-Related Measurement per Protocol Server (idns):

- CPU
- Memory

- Disk
- System Load
- Interface

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/ipworks`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/ipworks`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.
5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for each file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 7 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
IPWorks	Platform	`.*_PLATFORM.*`	`oPMF 32.401v5.0`
IPWorks	ENUM	`.*_ENUM.*`	`oPMF 32.401v5.0`
IPWorks	DNS	`.*_DNS.*`	`oPMF 32.401v5.0`
IPWorks	DHCP	`.*_DHCPv4.*`	`oPMF 32.401v5.1`
IPWorks	AAA	`.*_AAA.*`	`oPMF 32.401v5.2`
IPWorks	CLF	`.*_CLF.*`	`oPMF 32.401v5.3`
IPWorks	PMAL	`.*_PMAL.*`	`oPMF 32.401v5.4`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ```

```
./manage-modules.sh service start all
```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 14

SolutionPack for Ericsson IMS MRFP Summary Sheet

- Overview 186
- Technical specifications 186
- Where to find the latest SolutionPack software 187
- Collecting performance parameters 187
- Node, performance category, default file name pattern and 3GPP format 187
- Configuring the user process limits for a Linux installation 188
- Installing a SolutionPack 188
- Confirming report creation 189
- Troubleshooting 189

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS Media Resource Function Processor (MRFP). The Media Resource Function Processor is a subsystem of the Media Resource System (MRS) in the IP Media Subsystem (IMS). The SolutionPack for Ericsson IMS MRFP reports on the MRFP functionality of MRS.

This SolutionPack reports on the following:

- Performance of the various MRS resources such as MRFP services, VMRFP (Visited Media Resource Function Processor), MRFP Association, Interactive Messaging, and the IP system.
- Performance of overall MRFP functions such as MRFP audio and multimedia sessions.
- Performance of the related equipments such as plug-in units, IP interfaces, Gigabit Ethernet, Ethernet Switch module ports, and Et Resource.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Main reports
Resources:

- MRFP Services
- MrfpFunctions
- Vmrfp
- MrfpH248Association
- MS Processing
- Interactive Messaging
- IP Oam
- IP System

Equipment-Related Measurements:

- PluginUnit
- EtResource
- IPinterface
- GigabitEthernet
- EthernetSwicthModulePort

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/mrfp`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/mrfp`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.

5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for the file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 8 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default File name pattern	3GPP format
MRS	MRFP	`A20.*\.xml`	`oPMF 32.401v5.0`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ```

   ```
   ./manage-modules.sh service start all
   ```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 15

SolutionPack for Ericsson IMS MTAS Summary Sheet

- Overview 194
- Technical specifications 194
- Where to find the latest SolutionPack software 195
- Collecting performance parameters 195
- Node, performance category, default file name pattern and 3GPP format 196
- Configuring the user process limits for a Linux installation 197
- Installing a SolutionPack 198
- Confirming report creation 198
- Troubleshooting 199

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS Multimedia Telephony Application Server (MTAS). The SolutionPack for Ericsson IMS MTAS monitors the Multimedia Telephony Application Server (MMTel AS), the Scheduled Conference Application Server (Conf AS), and the Service Centralization and Continuity Application Server (SCC AS).

The following describes the severs monitored by this SolutionPack:

- MMTel AS provides multimedia telephony service and supplementary services according to 3GPP standards and service creation interfaces.
- Conf AS offers scheduled conference services according to 3GPP standards.
- SCC AS provides centralized services (ICS) and single radio voice all continuity (SR-VCC) according to 3GPP standards.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Performance measurement data
The SolutionPack for Ericsson IMS TSP monitors and collects performance measurement data for this SolutionPack. If you want to generate the reports that show this data, make sure you install the SolutionPack for Ericsson IMS TSP.

Main reports
Summary MMTEL AS Number of Simultaneous Sessions

Summary MMTel AS Simultaneous Sessions in Busy Hour

Summary SCC AS Number of Mobile Service Simultaneous Sessions

Summary SCC AS Mobile Service Simultaneous Sessions in Busy Hour

Summary MTAS Initial Registrations (per second)

Summary MTAS Initial De-registration (per second)

Summary ASR per CSCF

Summary CPS

Summary SCC AS (SRVCC) Invocation Attempts (per second)

Summary MTAS Number of SIP Requests (per second)

Summary MTAS Number of Charging Requests (per second)

TSP – MTAS:

- MMTel-AS

- SCC-AS
- MRFC
- XDMS (Ut) - Interface
- IMS ADA Authentications (USIM)
- Diameter (Rf - Sh)
- Equipment-Related Measurements

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/mtas`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/mtas`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.

5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for each file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 9 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
MTAS	MtasCDiv	.*_MtasCDiv.*	nPMF 32.401v5.0
MTAS	MtasCharging	.*_MtasCharging.*	nPMF 32.401v5.0
MTAS	MtasComBarring	.*_MtasComBarring.*	nPMF 32.401v5.0
MTAS	MtasConf	.*_MtasConf.*	nPMF 32.401v5.0
MTAS	MtasFcd	.*_MtasFcd.*	nPMF 32.401v5.0
MTAS	MtasFunction	.*_MtasFunction.*	nPMF 32.401v5.0
MTAS	MtasH248	.*_MtasH248.*	nPMF 32.401v5.0
MTAS	MtasHold	.*_MtasHold.*	nPMF 32.401v5.0
MTAS	MtasIdPres	.*_MtasIdPres.*	nPMF 32.401v5.0
MTAS	MtasMmt	.*_MtasMmt.*	nPMF 32.401v5.0
MTAS	MtasMrfc	.*_MtasMrfc.*	nPMF 32.401v5.0
MTAS	MtasXdms	.*_MtasXdms.*	nPMF 32.401v5.0
MTAS	MtasQos	.*_MtasQos.*	nPMF 32.401v5.0
MTAS	MtasScc	.*_MtasScc.*	nPMF 32.401v5.0
MTAS	MtasShInterface	.*_MtasShInterface.*	nPMF 32.401v5.0
MTAS	MtasSip	.*_MtasSip.*	nPMF 32.401v5.0
MTAS	MtasSrvcc	.*_MtasSrvcc.*	nPMF 32.401v5.0
MTAS	MtasSubsData	.*_MtasSubsData.*	nPMF 32.401v5.0
MTAS	MtasTraf	.*_MtasTraf.*	nPMF 32.401v5.0
MTAS	MtasLicenses	.*_MtasLicenses.*	nPMF 32.401v5.0
TSP	IPv4_MeassurementJob	A.*_IPv4.*	nPMF 32.401v5.0

Table 9 Node, Performance Category, Default file name pattern and 3GPP Format (continued)

Node	Performance category	Default file name pattern	3GPP format
TSP	Diameter	`.A.*_Diameter.*`	`nPMF 32.401v5.0`
TSP	PlatformMeassures	`.A.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP	IPv6_MeassurementJob	`A.*_IPv6.*`	`oPMF 32.401v5.0`
TSP	OamProvision-Measurement	`A.*_OamProvisioning.*`	`nPMF 32.401v5.0`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 16

SolutionPack for Ericsson IMS SOI Summary Sheet

- Overview 202
- Technical specifications 202
- Where to find the latest SolutionPack software 202
- Collecting performance parameters 203
- Node, performance category, default file name pattern and 3GPP format 203
- Configuring the user process limits for a Linux installation 204
- Installing a SolutionPack 204
- Confirming report creation 205
- Troubleshooting 205

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS ServiceOn Integrator (SOI). The SolutionPack for Ericsson IMS SOI reports on SOI performance information in the IP Multimedia subsystem (IMS). It measures request counts and response time and transactions per second from the SOI to other interfaces.

This SolutionPack reports on the following:

- Application data
- Service provider data
- Service SIP Business data
- Service Over Service Provider data
- SOM data
- Lictor data

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Main reports
Overall Summary

Application/System

Lictor

Service (overall-system)

Service over Service Provider

Service SIP-Business

SOM

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/soi`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/soi`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.

5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default file name pattern and 3GPP format

You can change the default file name pattern.

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for the file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 10 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
SOI	ims-ems-activation	`C20.*ims-emsactivation.xml`	`PM 3GPPXML TS 32.435`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. To verify the changes, type the following command:

   ```
   su apg -c 'ulimit -n -u'
   ```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 17

SolutionPack for Ericsson IMS TSP Summary Sheet

- Overview 210
- Technical specifications 210
- Where to find the latest SolutionPack software 210
- Collecting performance parameters 210
- Node, performance category, default tile name pattern and 3GPP format 211
- Configuring the user process limits for a Linux installation 212
- Installing a SolutionPack 213
- Confirming report creation 214
- Troubleshooting 214

Overview

Learn how to install and configure the SolutionPack for Ericsson IMS Telecom Server Platform (TSP). The SolutionPack for Ericsson IMS TSP monitors and collects performance measurement data, such as disk usage, IPv4 statistics, CPU load, cluster and system uptime, and diameter related measurements. The SolutionPack for Ericsson IMS CSCF, the SolutionPack for Ericsson IMS MTAS, and the SolutionPack for Ericsson IMS HSS SLF use this data to for their reports.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u2 and later

Data collection method
XML collector

All metrics are parsed through 3GPP standard xml files.

Main reports
The SolutionPack for Ericsson IMS TSP does not produce its own reports. It collects the following information for the SolutionPack for Ericsson IMS CSCF, the SolutionPack for Ericsson IMS MTAS, and the SolutionPack for Ericsson IMS HSS SLF:

- CPU load
- Disk usage
- IPv4 statistic
- Memory usage
- Processor and cluster uptime
- Diameter related measurements

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Collecting performance parameters

Before installing a SolutionPack, you must perform certain steps to ensure the SolutionPack is able to collect performance parameters from various IMS

components. These parameters are transferred in 3GPP-compliant XML files from IMS to the EMC M&R host using SFTP.

Before you begin

Review the configuration options for the XML collector in the *APG-Text-Parsing-Library.pdf* file located in the `<Install_Dir>/APG/Doc` directory of the EMC M&R host.

Procedure

1. Create a directory in the EMC M&R host for collecting performance data.

   For example: `/opt/IMS/incoming/tsp`

2. On the directory that you just created, change the permissions to `apg`.

   For example: `# chown -R apg:apg /opt/IMS/incoming/tsp`

3. Configure the OSS-RC, EMS (Element Management System), mediation node, or other to push the 3GPP-compliant XML files (i.e., Ericsson Report Output Files (ROP)) to the directory created in step 2.

   These 3GPP-compliant XML files are listed in the section called *Node, Performance category, Default filename pattern and 3GPP format.*

4. Verify the periodic transfer of the 3GPP-compliant XML files is set accordingly. If your SolutionPack is set to look for updates every five minutes (the default), make sure SFTP is invoked every five minutes as well.
5. SFTP the 3GPP-compliant XML files into the directory that you just created.

Node, performance category, default tile name pattern and 3GPP format

The *Ericsson IMS Metrics File* provides a complete listing of the expected counters for each file pattern type. This spreadsheet is available on the EMC support website http://support.emc.com.

Table 11 Node, Performance Category, Default file name pattern and 3GPP Format

Node	Performance category	Default file name pattern	3GPP format
TSP-CSCF	IPv4_MeassurementJob	`A20.*cscf.*_IPv4.*`	`nPMF 32.401v5.0`
TSP-CSCF	Diameter	`A20.*cscf.*_Diameter.*`	`nPMF 32.401v5.0`
TSP-CSCF	PlatformMeassures	`A20.*cscf.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP-CSCF	IPv6_MeassurementJob	`A.*cscf.*_IPv6.*`	`nPMF 32.401v5.0`
TSP-CSCF	OamProvision-Meassurement	`A20.*cscf.*_OamProvisioning.*`	`nPMF 32.401v5.0`
TSP-HSS	IPv4_MeassurementJob	`A20.*hss.*_IPv4.*`	`nPMF 32.401v5.0`

Table 11 Node, Performance Category, Default file name pattern and 3GPP Format (continued)

Node	Performance category	Default file name pattern	3GPP format
TSP-HSS	Diameter	`A20.*hss.*_Diameter.*`	`nPMF 32.401v5.0`
TSP-HSS	PlatformMeassures	`A20.*hss.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP-HSS	IPv6_MeassurementJob	`A.*hss.*_IPv6.*`	`nPMF 32.401v5.0`
TSP-HSS	OamProvision-Meassurement	`A20.*hss.*_OamProvisioning.*`	`nPMF 32.401v5.0`
TSP-MTAS	IPv4_MeassurementJob	`A.*_IPv4.*`	`nPMF 32.401v5.0`
TSP-MTAS	Diameter	`A.*_Diameter.*`	`nPMF 32.401v5.0`
TSP-MTAS	PlatformMeassures	`.A.*_PlatformMeasures.*`	`oPMF 32.401v5.0`
TSP-MTAS	IPv6_MeassurementJob	`A.*_IPv4.*`	`nPMF 32.401v5.0`
TSP-MTAS	OamProvision-Meassurement	`A.*_OamProvisioning.*`	`nPMF 32.401v5.0`

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

```
apg   hard  nofile  65534
apg   soft  nofile  65534
apg   hard  nproc   65534
apg   soft  nproc   65534
```

3. Save the file.
4. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

5. In the `apg.properties` file, edit the hostname to a FQDN host name.
6. To restart the services, type the following commands from the `bin` directory of the installation:

```
./manage-modules.sh service stop all
./manage-modules.sh service start all
```

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.

7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 18

SolutionPack for Ericsson MGW Summary Sheet

- Overview 218
- Technical specifications 218
- Where to find the latest SolutionPack software 218
- Performing prerequisite installation tasks 219
- Installing a SolutionPack 219
- Performing post installation tasks 220
- Confirming report creation 220
- Troubleshooting 220

Overview

Learn how to install and configure the SolutionPack for Ericsson MGW (Media Gateway). This SolutionPack is a mobile network management solution designed to generate reports that show key metrics and key performance indicators (KPIs) for Ericsson MGW. It presents real-time and historical performance reports.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
Stream collector

Supported version
Ericsson MGW R12

Main reports

MGW Summary
: Displays all managed objects, the average processor load %, the media stream utilization rate %, and the KPI dashboard.

MGW Availability
: Displays detailed information about the accessibility of the MGW nodes (aggregated and per node).

MGW Processor Load
: Displays detailed information about the processor load of the MGW nodes (aggregated and per node).

MGW Traffic Load (Erlang)
: Displays detailed information about the current traffic load in Erlang of the MGW nodes (aggregated and per node).

GCP Availability
: Displays detailed information about the GCP (Gateway Control Protocol) link availability (aggregated and per node).

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new

SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from the MGW nodes be locally available on the EMC M&R server hosting the Stream collector. You must ensure the Operations Support System-Radio and Core (OSS-RC) can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from OSS-RC to the EMC M&R server. Contact the OSS-RC administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and the OSS-RC server.
3. Configure OSS-RC to push the raw PM files to this default directory on the EMC M&R server: `<install directory>/Collecting/Stream-Collector/<SP-name>/Incomingdata/`

   Here is an example of the name of a raw PM file: `A*.*-2100_SVMGW267:1.xml`.

   You can override the default directory during the SolutionPack installation.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.

7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. If you selected `Move` as the **Post processing action** during the installation, which keeps all processed performance management XML files, make sure you have a maintenance task running on the server that periodically deletes these files. You can do this manually or by scheduling Cron jobs.
2. If using the default directory to store the performance management XML files, verify that the `apg` user has read/write permissions on it.
3. If not using the default directory, make sure the directory that you are using to store the performance management XML files is on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73

- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 19

SolutionPack for Ericsson RNC Summary Sheet

- Overview 224
- Technical specifications 224
- Where to find the latest SolutionPack software 225
- Performing prerequisite installation tasks 226
- Installing a SolutionPack 226
- Performing post installation tasks 227
- Confirming report creation 227
- Troubleshooting 228

Overview

Learn how to install and configure the SolutionPack for Ericsson RNC (Radio Network Controller). This SolutionPack is a mobile network management solution designed to generate reports that show key metrics and key performance indicators (KPIs) for Ericsson RNC. It presents real-time and historical performance information.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
Stream collector

Supported version
Ericsson RNC CXP9014711/7_R11UA05

Main reports

Accessibility:

- Call Setup Success Rate (RNC)
- Call Setup Success Rate (CELL)
- CS Setup Success Rate (CELL)
- PS Setup Success Rate (CELL)
- Iu Setup Success Rate
- CN paging to UE in URA State
- RNC Sending Paging Failure Rate
- UTRAN Paging to UE in URA State
- RNC Type 1 Paging Attempt Success Rate
- RNC Type 2 Paging Attempts (CELL)
- RRC Setup Success Rate (CELL)
- RRC Terminating Success Rate (CELL)
- HSDPA Access Failure Rate

Availability:

- Cell Availability Summary
- R99 RNC Availability

Capacity:

- RNC Main Processor Load
- Average Users HS

Average Users Ps Data

Average Users Speech

Power Limit Failure

Mobility

Cell Update Success Rate

HSDPA Cell Change SR

Successful RL Addition Source Best Cell Speech

URA Update Success Rate

Retainability:

HSDPA Drop Rate

RAB Drop Rate

RRC Drop Ragte Speech

Traffic:

Traffic Speech

Traffic AMR

Traffic AMR-WB

Traffic CS57

Traffic CS64

Traffic PS Interactive

Traffic PS Interactive DCH/FACH

Traffic PS EUL

Traffic PS HS

Traffic PSSTR HS

RNC PS Stream

RNC PS Stream 128

PS Data Average Total Throughput UL

PS Data Average Total Throughput DL

PS Data Average Throughput Net

HS Data Average Throughput Net

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new

SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from RNC be locally available on the EMC M&R server hosting the Stream collector. You must ensure the Operations Support System-Radio and Core (OSS-RC) can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from OSS-RC to the EMC M&R server. Contact the OSS-RC administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and the OSS-RC server.
3. Configure OSS-RC to push the raw PM data files on a regular time interval to this default directory on the EMC M&R server: `<install directory>/Collecting/Stream-Collector/<SP-name>/Incomingdata/`

   Here is an example of the name of a raw PM file: `A20140915.2115+0100-2130+0100_SubNetwork=XXXX_RootMo,SubNetwork=XXXXXX,MeContext=XXXXXX_statsfile.xml`.

   You can override the default directory during the SolutionPack installation.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.

6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. If you selected `Move` as the **Post processing action** during the installation, which keeps all processed performance management XML files, make sure you have a maintenance task running on the server that periodically deletes these files. You can do this manually or by scheduling Cron jobs.
2. If using the default directory to store the performance management XML files, verify that the `apg` user has read/write permissions on it.
3. If not using the default directory, make sure the directory that you are using to store the performance management XML files is on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 20

SolutionPack for Ericsson SGSN Summary Sheet

- Overview 232
- Technical specifications 232
- Where to find the latest SolutionPack software 233
- Performing prerequisite installation tasks 233
- Installing a SolutionPack 234
- Performing post installation tasks 234
- Confirming report creation 235
- Troubleshooting 235

Overview

Learn how to install and configure the SolutionPack for Ericsson SGSN (Serving GPRS Support Node). This SolutionPack is a mobile network management solution designed to generate reports that show key metrics and key performance indicators (KPIs) for Ericsson SGSN nodes. This enables you to understand the functioning of the SGSN nodes and their packet core network.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
Stream collector

Supported versions
Ericsson SGSN R13A

Ericsson SGSN R10A

Main reports

KPI Dashboard

Provides detailed information on the key performance indicators affecting the overall functionality of the SGSN node. These KPIs are categorized into Accessibility, Retainability, Traffic, and Subscriber information. Several reports display valuable information on the SGSN and packet core network functionality.

Components Overview

Reports on the SGSN node and its components. Each SGSN node has various components that produce metrics, and both are shown in this report. It also provides detailed information on the performance of the SGSN node.

Inter SGSN RAU Failure Ratio

Displays the Routing Area Update (RAU) failure rate across SGSNs. RAU is performed whenever the mobile device is in motion.

Attach Failure Ratio

Shows the GPRS GSM failure of attaches. When a 2G or 3G user cannot access the packet data service, it displays in this key performance indicator.

Number of SAU

Provides the number of Simultaneously Attached Users (SAU), and indicates the probable load on the SGSN. The higher the number of SAU, the more the load.

Top-N Reports

Shows the Top-5 SGSN and Top-5 Routing areas in terms of various key performance indicators, such as the Top-5 SGSN with Number of SAUs, Top-5 Routing Areas with most Attach Failures, and Top-5 Busiest SGSNs.

Metrics and Measurement Inventory

Lists all the metrics and KPIs generated by an SGSN. This report is similar to the Components Overview report.

SGSN Mobility Management

Lists all the Mobility management KPIs, such as RAU failures and Paging Failures.

SGSN Traffic Management

Lists all the Traffic management KPIs, such as instance Total Uplink, Total Downlink, and Number of PDP.

SGSN Accessibility Management

Lists all the Accessibility management KPIs, such as instance Attach failure, RAB establishment failure, and PDP Context Activation Failure.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from the SGSN nodes be locally available on the EMC M&R server hosting the Stream collector. You must ensure the Operations Support System-Radio and Core (OSS-RC) can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from the OSS-RC server to the EMC M&R server. Contact the OSS-RC administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and the OSS-RC server.
3. Configure OSS-RC to push the raw PM data files on a regular time interval to this default directory on the EMC M&R server: `<install directory>/Collecting/Stream-Collector/<SP-name>/Incomingdata/`

   Here is an example of the name of a raw PM file: `A20140914.1145+0100-20140914.1200+0100_Meas_SS7_all_13A_LGSGSN03.145.xml`.

   You can override the default directory during the SolutionPack installation.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. If you selected `Move` as the **Post processing action** during the installation, which keeps all processed performance management XML files, make sure you have a maintenance task running on the server that periodically deletes these files. You can do this manually or by scheduling Cron jobs.
2. If using the default directory to store the performance management XML files, verify that the `apg` user has read/write permissions on it.

3. If not using the default directory, make sure the directory that you are using to store the performance management XML files is on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.

3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*

5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 21

SolutionPack for Huawei iManager M2000 Summary Sheet

- Overview 240
- Technical specifications 240
- Where to find the latest SolutionPack software 241
- Performing prerequisite installation tasks 241
- Determining the format of the performance data 241
- Installing a SolutionPack 242
- Performing post installation tasks 243
- Setting up sectorized cell views on geo maps 243
- Confirming report creation 244
- Alerts 245
- Adding new metrics in the collector 248
- Troubleshooting 251

Overview

Learn how to install and configure the SolutionPack for Huawei iManager M2000. This SolutionPack monitors the performance of the mobile network managed by Huawei iManager M2000.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
Stream collector

Main reports

Topology Map:

Topology Map for 3G By Cell

Topology Map for 3G By Station

Accessibility:

Accessibility Success Rate

SDCCH Congestion by Cell

Retainability:

Call Drop Rate by Cell

Mobility:

Handover Success Rate

Traffic Integrity:

2G Data Avg Throughput Downlink

2G Data Avg Throughput Uplink

3G Data Avg Throughput Downlink

3G Data Avg Throughput Uplink

Availiability:

2G Cell Downtime

3G Cell Downtime

Utilization:

2G Site Utilization

3G Site Utilization

CE Utilization

Simultaneous Data Users

Situations to Watch:

Call Drop Rate

Cell Down Time

Handover Success Rate

SDDCH Congestion

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from Huawei iManager M2000 be locally available on the EMC M&R server hosting the Stream collector. You must ensure Huawei iManager M2000 can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from Huawei iManager M2000 to the EMC M&R server. Contact the Huawei iManager M2000 administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and Huawei iManager M2000.
3. Configure Huawei iManager M2000 to push the raw PM data files on a regular time interval to this default directory on the EMC M&R server: `<install directory>/Collecting/Stream-Collector/<collector instance name>/data/`

   Here is an example of a raw PM file name: `pmresult_67109379_*.csv`.

   You can override the default directory during the SolutionPack installation.
4. Verify that the required counters are enabled on Huawei iManager M2000 EMS (Element Management System). These counters are listed in the *SolutionPack for Huawei iManager M2000 Counter Prerequisites*.

Determining the format of the performance data

The Huawei iManager M2000 formats the data in the performance management files based on the counter ID (numerical representation), the counter name or the counter

description. For the Stream collector to correctly parse the metrics in these files, you must indicate the format of these PM files during the SolutionPack installation.

The Huawei iManager M2000 creates one performance management CSV file for each counter group ID. This table shows the performance properties for Counter Group ID:-67109381.

Table 12 Example of performance properties

Counter ID	Counter name	Counter description
67189749	IRATHO.AttRelocPrepOutCS	Number of Preparation Attempts for CS Outgoing Inter-RAT Handover for Cell
67189755	IRATHO.SuccOutCS	Number of Successful CS Outgoing Inter-RAT Handovers for Cell

Procedure

1. Using a text editor, open one of the performance management CSV files.
2. In the column header after **Reliability**, check for these formats. The italicized text shows the actual format example.

Format	Example
Counter ID	`Result Time,Granularity Period,Object Name,Reliability,"67202488"`
Counter name	Result Time,Granularity Period,Object Name,Reliability,*"VS.HSUPA.16QAM.UtilizeTimePermillage"*
Counter description	`Result Time,Granularity Period,Object Name,Reliability,"AR3010A:Mean Number of Dynamically Configured Channels(SDCCH) (900/850/810 band)"`

You are asked for this format when you install the SolutionPack.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.

2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. If you selected `Move` as the **Post processing action** during the installation, which keeps all processed performance management XML files, make sure you have a maintenance task running on the server that periodically deletes these files. You can do this manually or by scheduling Cron jobs.
2. If using the default directory to store the performance management XML files, verify that the `apg` user has read/write permissions on it.
3. If not using the default directory, make sure the directory that you are using to store the performance management XML files is on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.

Setting up sectorized cell views on geo maps

You can provide views of the individual cells, which are the sectors of a cellsite, on the geo maps in this SolutionPack. To do this, you customize a default property tagging filter and edit an existing sample CSV file according to your specifications. The information you enter into this filter processes the properties that you specify in the CSV file to enrich the views on the geo maps.

Procedure

1. Navigate to **Centralized Management**.
2. Under **Logical Overview**, click **Collecting**.
3. Select the **Property-Tagging-Filter** for the Huawei iManager M2000 instance. For example: Property-Tagging-Filter::huawei-m2000 <*server*>

You can also modify the property tagging filter using the Data Enrichment functionality in Centralized Management. For more information, see the online help in the EMC M&R platform.

4. Click **Configuration Files** in the blue bar.
5. Select `conf/property-tagging-filter_m2000.xml`.
6. Click **Edit** to add these required key properties and provide processing instructions for the CSV file:
   - device
   - siteid
   - sitename
   - sitetype: indoor or outdoor
   - celltype: 2G, 3G, or 4G
   - location: latitude and longitude of the site location
   - azimuth: orientation of the cell/sector
   - radius: approximate radius of coverage
   - beamwidt: beam width view of the cell/sector

   For instructions on customizing this property tagging filter, click `doc/APG-Property-Tagging-Filter.pdf` under **Documentation**.
7. Under **Configuration Files**, do one of the following:
   - To add locations based on the cell ID, edit the sample file `M2000-cellid-map.csv` to meet your requirements, and then click **Save**.
   - To add locations based on the device, edit the sample file `M2000-device-map.csv` to meet your requirements, and then click **Save**.

   The following shows sample entries for this type of CSV file:

```
device,siteid,sitename,sitetype,celltype,location,azimuth,radi
us,be
amwidt
31071,EN107,Enma Mall,Indoor,3G,24.1298 56.5743,90,25000,120
31074,EN107,Enma Mall,Indoor,3G,33.1298 40.5743,210,25500,120
31072,EN107,Enma Mall,Indoor,3G,26.1298 50.5743,330,25500,120
```

After the next polling cycle, you will see sectorized cell views on the geo maps.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Alerts

This SolutionPack generates alerts when specific thresholds are reached in the mobile network. These alerts cover the areas of accessibility, retainability, mobility, and utilization.

Table 13 Accessibility alerts

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
Access Failure by Chanel Element Congestion Rate	("VSRABFailEstabCSULCECong' + 'VSRABFailEstabCSDLCECong') / ('VSRABAttEstabAMR')	Rate is greater than 2%	Access failure by channel element congestion rate is more than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is greater than 1%	Access failure by channel element congestion rate is more than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
Access Failure by Code Congestion Rate per Cell	('VSRABFailEstabCSCodeCong') / ('VSRABAttEstabAMR')	Rate is greater than 2%	Access failure by code congestion rate per cell is more than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is greater than 1%	Access failure by code congestion rate per cell is more than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
Access Failure by Power Congestion Rate per Cell	(name=='VSRABAbnormRelAMR') / (name=='VSRABNormRelAMR' + name=='VSRABAbnormRelAMR') * 100	Rate is greater than 2%	Access failure by power congestion rate per cell is more than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is greater than 1%	Access failure by power congestion rate per cell is more than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
SDCCH Congestion by Cell	('K3001:Failed SDCCH Seizures	Rate is greater than 2%	SDCCH congestion	Rate is greater than 1%	SDCCH congestion

Table 13 Accessibility alerts (continued)

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
	due to Busy SDCCH')/ ('K3000:SDCCH Seizure Requests')		rate is greater than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*		rate is greater than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
TCH Congestion by Cell	('K3021:Failed TCH Seizures due to Busy TCH (Signaling Channel)' + 'K3011A:Failed TCH Seizures due to Busy TCH (Traffic Channel)') / ('K3020:TCH Seizure Requests (Signaling Channel)' + 'K3010A:TCH Seizure Requests (Traffic Channel)')	Rate is greater than 2%	TCH congestion rate is greater than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is greater than 1%	TCH congestion rate is greater than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*

Table 14 Retainability alerts

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
Call Drop - SDCCH for tracking calls	(name=='VSRABAbnormRelAMR') / (name=='VSRABNormRelAMR' + name=='VSRABAbnormRelAMR') * 100	Rate is greater than 2%	Call drop rate more than 2% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is greater than 1%	Call drop rate more than 1% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
Call Drop - TCH for tracking call drop rates in the network	('K3023:Successful TCH Seizures (Signaling Channel)' + 'K3013A:Successful TCH Seizures (Traffic Channel)'	Rate is greater than 2%	Call drop rate more than 2% for PROP.*devtype* and PROP.*cellid* and	Rate is greater than 1%	Call drop rate more than 1% for PROP.*devtype* and PROP.*cellid* and

Table 14 Retainability alerts (continued)

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
	+ 'K3013B:Successful TCH Seizures in TCH handovers (Traffic Channel)')		PROP.*network* at PROP.*siteid* PROP.*location*		PROP.*network* at PROP.*siteid* PROP.*location*

Table 15 Mobility alerts

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
Handover Success Rate - GSM to UTRAN Cell Selection Lost Rate	('RRCAttConnEstabIRATCelRes' - 'RRCSuccConnEstabIRATCelRes') / ('RRCAttConnEstabIRATCelRes')	Rate is less than 85%	Hand over success rate is less than 85% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is less than 90%	Hand over success rate is less than 90% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*
Handover Success Rate - GSM to UTRAN Cell Selection Success Rate	('RRCSuccConnEstabIRATCelRes')/ ('RRCAttConnEstabIRATCelRes')	Rate is less than 50%	Hand over success rate is less than 50% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*	Rate is less than 60%	Hand over success rate is less than 60% for PROP.*devtype* and PROP.*cellid* and PROP.*network* at PROP.*siteid* PROP.*location*

Table 16 Utilization alerts

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
3G Site Utilization - HS User Utilization	(VSHSDPAUEMeanCell / 64.0) * 100	Utilization is greater than 95	3G Site utilization has crossed 95% for PROP.*devtype* and PROP.*cellid* and PROP.*network*	Utilization is greater than 90	3G Site utilization has crossed 90% for PROP.*devtype* and PROP.*cellid* and PROP.*network*

Table 16 Utilization alerts

Alert	KPI used in computation	Major threshold	Message of major threshold	Minor threshold	Message of minor threshold
			`at PROP.`*`siteid`* `PROP.`*`location`		`at PROP.`*`siteid`* `PROP.`*`location`

Adding new metrics in the collector

The SolutionPack supports some metrics that are not part of the installation. This sample procedure shows you the steps to follow when adding these new metrics to the Stream collector.

This sample procedure adds new metrics to the counter names VS.AttCellUpdt.RLFail, VS.FailCellUpdt.RLFail.NoReply and VS.SuccCellUpdt.RLFail, which are in counter group ID 67109382 . These metrics are listed in the *SolutionPack for Huawei iManager M2000 Counter Prerequisites* spreadsheet.

Procedure

1. Back up the original collector and parser files. For example: `huawei-collecting-name.xml` to `huawei-collecting-name.xml.bak` and `huawei-parsing.xml` to `huawei-parsing.xml.bak`.
2. Search for the counter name VSAttCellUpdtRLFail (without '.') in `huawei-collecting-name.xml`.
3. If found in `huawei-collecting-name.xml`, uncomment the following lines:

```
<values required="false"context-key=VS.AttCellUpdt.RLFail;">
<name>VSAttCellUpdtRLFail</name>
<unit>Nb</unit>
</values>
```

4. If not found in `huawei-collecting-name.xml`, do the following:
   a. Check the contents of the counter group ID 67109382. For example: `cat pmresult_67109382_30_201302201600_201302201630.csv`

```
Result Time,Granularity Period,Object
Name,Reliability,"VS.AttCellUpdt.RLFail","VS.FailCellUpdt.RL
Fail.NoReply","VS.SuccCellUpdt.RLFail"
,Minutes,,,none,none,none
2013-02-20 16:00,30,"RNC/BSC6900UCell:Label=PO230A1,
CellID=32301",Reliable,0,0,0
2013-02-20 16:00,30,"RNC/BSC6900UCell:Label=PO430B2,
CellID=32305",Reliable,0,0,0
2013-02-20 16:00,30,"RNC/BSC6900UCell:Label=PO430B1,
CellID=32302",Reliable,0,0,0
2013-02-20 16:00,30,"RNC/BSC6900UCell:Label=PO230A2,
CellID=32304",Reliable,0,0,0
```

   b. Match one of the above object name patterns with an object name in this table. The Stream collector extracts required performance management data from the object name. The object type is the logical grouping of the counter group IDs.

Table 17 Object name examples

PM file name example	Object name example	Object type
pmresult_67109379_*.csv	RNC/ BSC6900UCell:Label=PO 230A1	obj1
pmresult_67109377_*.csv		
pmresult_67109381_*.csv		
pmresult_67109471_*.csv		
pmresult_67109391_*.csv		
pmresult_67109365_*.csv		
pmresult_67109367_*.csv		
pmresult_67109368_*.csv		
pmresult_67109369_*.csv		
pmresult_67109372_*.csv		
pmresult_67109373_*.csv		
pmresult_67109376_*.csv		
pmresult_67109385_*.csv		
pmresult_67109390_*.csv		
pmresult_67109420_*.csv	RNC/ BSC6900UMTSFunction: RNC	obj2
pmresult_67109421_*.csv		
pmresult_67109446_*.csv		
pmresult_67109473_*.csv		
pmresult_67109519_*.csv	RNC/ CNOPERATOR:CNNAME =0, CNINDEX=0	obj3
pmresult_67109516_*.csv	"RNC/DPU:SRN=0, SN=9, BT=DPUB" AND "BSC/DPU:Slot No.=11, Subrack No=0, Subsystem No.=0"	obj4
pmresult_50331652_*.csv	RM190/NodeB:RM190/ MocID:2/Operator:-1	obj5
pmresult_1275069419_*.csv	BSC/ GCELL:LABEL=RML190A, CellIndex=0, CGI=42601006F076D	obj6
pmresult_1275072526_*.csv		

Table 17 Object name examples (continued)

PM file name example	Object name example	Object type
pmresult_1275072528_*.csv pmresult_1275072525_*.csv pmresult_1275072527_*.csv pmresult_1275071435_*.csv pmresult_1275072618_*.csv mresult_1275071427_*.csv pmresult_1275071429_*.csv		
pmresult_1275072018_*.csv	BSC/BSCRPT:BSC	

c. Since the object name pattern `RNC/BSC6900UCell:Label=PO230A1` matches one that is of obj1 type, search for `<hardcoded-properties key="hwobjid">obj1</hardcoded-properties>`

d. Add these values to the metrics:

```
<values required="false" context-key=VS.AttCellUpdt.RLFail >
<name> VSAttCellUpdtRLFail </name>
<unit>Nb</unit>
</values>
<values required="false" context-
key=VS.FailCellUpdt.RLFail.NoReply >
<name>VSFailCellUpdtRLFailNoReply</name>
<unit>Nb</unit>
</values>
<values required="false" context-key=VS.SuccCellUpdt.RLFail
>
<name>VSSuccCellUpdtRLFail</name>
<unit>Nb</unit>
</values>
```

e. Save `huawei-collecting-name.xml`.

In this example, the performance data is formatted by the counter name. If data is formatted by the counter ID or the counter description, you must add the metric information to `huawei-collecting-id.xml` or `huawei-collecting-desc.xml`, respectively, instead of `huawei-collecting-name.xml`.

5. Append this directory file-pattern to the `huawei-parsing.xml` file:

```
<directory file-pattern="pmresult_67109379_*.csv|
pmresult_67109377_*.csv|pmresult_ 67109382 *.csv"
recursive="true">data/</directory>
```

6. Save `huawei-parsing.xml`.
7. Restart the Stream collector.

Troubleshooting

Report display problems

- What to do if data does not appear in any topology reports on page 251
- What to do if data does not appear in any topology reports on page 251
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any topology reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. Check these feeds to the topology reports:
   - `http://<EMC M&R-Instance>:58083/topology/repository/`
   - `http://<EMC M&R-Instance>:58083/topology/report/map?device=<STATION_NAME>&devtype=Station&mapType=STATION_MAP`
   - `http://<EMC M&R-Instance>:58083/topology/resources/mobilepaths/topo:MobileStation:<STATION_NAME>`
4. To view the log files for errors, go to **Centralized Management** and click **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some topology reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. In the database, search for these metrics that are used to stretch the topology from controller to station to cell:
   - RRCAttConnEstabReg for cell-specific metric (device ->siteid) inverse connection to station
   - VSIUBDLCongTime for station-specific metric (device ->cntlr) inverse connection to controller
   - VSRRCAttConnEstabRNC for controller-specific metric
3. To view the log files for errors, go to **Centralized Management** and click **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 22

SolutionPack for ip.access nano3G Small Cell Summary Sheet

- Overview 254
- Technical specifications 254
- Where to find the latest SolutionPack software 254
- Performing prerequisite installation tasks 255
- Installing a SolutionPack 255
- Performing post installation tasks 256
- Confirming report creation 256
- Enriching data in access point cells 256
- Troubleshooting 257

Overview

Learn how to install and configure the SolutionPack for ip.access nano3G Small Cell. This SolutionPack is a mobile network management solution designed to generate reports that show key metrics and key performance indicators (KPIs) for the ip.access nano3G access points (cells) and the ip.access controllers. It presents real-time and historical performance reports.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R version
6.5u1 and later

Compatible operating system
Linux

Data collection method
Stream collector

Main reports
PS Calls

CS Calls

CS Traffic Erlang

PS Drop Rate (%)

CS Drop Rate (%)

Download PS Traffic

Upload PS Traffic

RAB Establishment Success

RRC Success

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that the performance management (PM) data from the ip.access Network Orchestration System (NOS) be locally available on the EMC M&R server hosting the Stream collector. You must ensure ip.access NOS can push the PM data files to the EMC M&R server.

This procedure includes a task for sending the PM files from ip.access NOS to the EMC M&R server. Contact the ip.access NOS administrator about where the PM files are stored and how they are processed.

Procedure

1. Verify the SFTP or FTP server is running on the EMC M&R server where the Stream collector resides.
2. Verify that connectivity exists between the EMC M&R server and ip.access NOS.
3. Configure ip.access NOS to push the access controller (AC) and access point (AP) PM data files to separate directories on the EMC M&R server on a regular time interval. You are asked for these directories during the SolutionPack installation.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.

c. Click **Next**.

8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After installing the SolutionPack, you must perform certain tasks.

Procedure

1. Make sure the directories that you are using to store the AC and AP performance management XML files are on a valid partition and that the `apg` user has read/write permissions on it. If using another user, make sure that user is in the same UNIX permissions group as the `apg` user.
2. Verify that the Linux `unzip` command is available on the EMC M&R server where the Stream collector resides. The Stream collector uses this command to unzip the AC and AP PM files in order to read them.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Enriching data in access point cells

By using the Data Enrichment functionality, you can quickly tag data coming from the SolutionPack's Collector-Manager to display in the access point cells of the reports' tables and graphs. By default, only the device name displays in these cells but you can define additional properties to appear in these cells, such as the customer name, the cell ID, and the device model.

Procedure

1. Navigate to **Centralized Management**.
2. Click **Data Enrichment** > **Register a new module**.
3. On the **Register a new module** window, do the following:

   a. Select the Collector-Manager server on which the SolutionPack's collection block resides, which was set during installation.

b. Select the **Collecting** category.

c. Select the PTF-femto-AP module. For a default installation, the module is Collector-Manager::ipaccess-nano3g::PTF-femto-AP.

d. Click **Register**.

e. Select the PTF-femto-AP module, such as Collector-Manager::ipaccess-nano3g::PTF-femto-AP.

The **New tagging** window appears. To enrich the data in the access point cells, you can manually tag new properties or you can create and import a CSV file that contains new properties and their values.

4. If tagging new properties:

a. Click **Add new property**.

b. Fill out the fields on the **Create a new key** window.

c. Click **Save**.

5. If creating a CSV file:

a. Use a format similar to this one:

```
device,siteid,sitename,sitetype,celltype
31071,EN107,Enma Mall,Indoor,3G
31074,EN107,Enma Mall,Indoor,3G
```

For more information on how property tagging works with the CSV file, see the *Property Tagging Filter Administration Guide* in the `/APG/Doc` folder of your installation path.

b. When you are finished creating the CSV file, click **Import CSV**.

c. Click **Choose File** to navigate to your CSV file.

d. Click **Ok**.

Results

After the next polling cycle, you will see the access point cells displaying the additional data.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

PART 3

SolutionPacks for Infrastructure

This section describes these SolutionPacks.

Chapter 23, "SolutionPack for Acme Packet SBC Summary Sheet"

Chapter 24, "SolutionPack for Alcatel-Lucent 5620 SAM Summary Sheet"

Chapter 25, "SolutionPack for Aruba Wi-Fi Summary Sheet"

Chapter 26, "SolutionPack for Avaya Aura Summary Sheet"

Chapter 27, "SolutionPack for Blue Coat PacketShaper Summary Sheet"

Chapter 28, "SolutionPack for BGP Summary Sheet"

Chapter 29, "SolutionPack for Check Point Firewall Summary Sheet"

Chapter 30, "SolutionPack for Cisco Firewall Summary Sheet"

Chapter 31, "SolutionPack for Cisco IP-SLA Summary Sheet"

Chapter 32, "SolutionPack for Cisco Unified Communications Manager 3.0 Summary Sheet"

Chapter 33, "SolutionPack for Cisco UCS 4.0 Summary Sheet"

Chapter 34, "SolutionPack for Cisco Wi-Fi Summary Sheet"

Chapter 35, "SolutionPack for Juniper Firewall Summary Sheet"

Chapter 36, "SolutionPack for Juniper QoS Summary Sheet"

Chapter 37, "SolutionPack for Juniper RPM Summary Sheet"

Chapter 38, "SolutionPack for Microsoft Hyper-V 1.3.5 Summary Sheet"

Chapter 39, "SolutionPack for Microsoft SCOM Summary Sheet"

Chapter 40, "SolutionPack for Microsoft SQL Server 4.0 Summary Sheet"

Chapter 41, "SolutionPack for MPLS Summary Sheet"

Chapter 42, "SolutionPack for OpenStack Summary Sheet"

Chapter 43, "SolutionPack for Oracle Database 4.0 Summary Sheet"

Chapter 44, "SolutionPack for Oracle MySQL Database 4.0 Summary Sheet"

Chapter 45, "SolutionPack for Riverbed SteelHead Summary Sheet"

Chapter 46, "SolutionPack for Traffic Flows 4.0 Summary Sheet"

Chapter 47, "SolutionPack for Transaction Summary Sheet"

Chapter 48, "SolutionPack for UPS Summary Sheet"

Chapter 49, "SolutionPack for VMware vCenter 4.0 Summary Sheet"

CHAPTER 23

SolutionPack for Acme Packet SBC Summary Sheet

- Overview 264
- Support 264
- License management 264
- Installation 264
- Logging in to Centralized Management 265
- Installing the SolutionPack 265
- Adding devices for monitoring 266
- Log files 266
- Configuring the user process limits for the Linux installation 266
- Uninstalling a SolutionPack 267
- Viewing SolutionPack reports 267
- SolutionPack for Acme Packet SBC Reports 268
- Report metrics 269
- SSL certificates 271

Overview

Learn how to install and configure the SolutionPack for Acme Packet SBC. You can monitor and report on Acme Packet devices for performance and utilization information as well as view the inventory of all devices and session metrics.

Use these guidelines in the following sections to prepare your environment for installation of the SolutionPack for Acme Packet SBC.

- Use support information to verify that prerequisite software is installed in your environment.
- Check that your EMC M&R network configuration has the minimum requirements to run reports.
- Manage licenses for the SolutionPack

Support

This table lists the prerequisite support for this SolutionPack.

Table 18 Prerequisites for the SolutionPack for Acme Packet SBC

Device	Version
EMC Watch4net	6.3
Acme Packet Net-Net	9200 X
Acme Packet Net-Net	4500 X
Acme Packet Net-Net	4000 Series SBC X
Acme Packet Net-Net	3820 X
Acme Packet Net-Net	3800 X

License management

You can evaluate features in the SolutionPack Center using 30-day temporary licenses included with EMC M&R software. If you install or plan to use the SolutionPack for longer than 30 days, contact EMC Online Support for permanent license files.

If you have an existing permanent license or a temporary license that requires updating, use the license upload feature in EMC M&R Centralized Management. Both permanent and temporary licenses are distributed in .zip files.

The EMC M&R license name is either EMC M&R for Acme Packet SBC or ReportPack for Acme Packet SBC. If either license is present, the system will use it.

Installation

Review this information before beginning the installation.

- Make sure you review and perform the prerequisites outlined in the first chapter.

- Perform the installation with administrative privileges on the EMC M&R User Interface.

Logging in to Centralized Management

Log in to Centralized Management to perform operations that affect all servers.

Procedure

1. Point your browser to the URL.

   For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

   a. Type the login credentials.

      The default username is **`admin`** and the default password is **`changeme`**.

   b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Installing the SolutionPack

After you log in as an administrator, you can install this SolutionPack from Centralized Management.

Before you begin

Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases**, **Backends**, **Frontends**, **Miscellaneous** (except Blocks). The recommended module update order varies. Refer to the *EMC M&R Installation and Configuration Guide* for information on module update order for multiple hosts or single host deployments.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the Acme VoIP SolutionPack on the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.

   a. Type the instance name.

   b. Select the server in one or more list boxes. For example, select the server in the **Collector**, and **Reports** list boxes.

   c. Click **Next**.

8. For each list box you select, a screen appears.

   a. Click **Next** after you complete each screen.

   b. Click **Install** after you complete the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. After installation is complete, verify the SolutionPack version number along with SolutionPackBlock information. Select **Centralized Management** > **SolutionPacks** > **Acme VoIP**.

Adding devices for monitoring

After installation, you must manually add devices for monitoring.

Before you begin

Procedure

1. Create the collector. In the EMC M&R console, navigate to **Device discovery** > **Collectors** > **Add New Collector**.
2. Add a device for collection. Navigate to **Device discovery** > **Devices** > **Add New Device**.

   a. In Main Parameters, enter the name of the device and IP address.

   b. Configure SNMP Credentials by adding a collector that was previously created.

   c. Select appropriate Acme Capabilities.

   Repeat this procedure until all desired devices are added.

3. Distribute device(s). Navigate to **Device discovery** > **Dashboard**, and then click on **Distribute all approved devices with Capabilities on all enabled collectors**.

Log files

Information on the log files for this SolutionPack follows.

This SolutionPack does not have Acme Packet SBC-specific log files. Logging for the SolutionPack is part of the Generic SNMP collector:`<APG_install>/Collecting/Collector-Manager/Generic-SNMP/logs`.

Configuring the user process limits for the Linux installation

Increase the user process limits for the user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed.

Before you begin

- Make sure you have a login with root privileges.

- The EMC M&R platform installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6.
- The name specified for the user account during the installation.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. Type the following commands from the `bin` directory of the installation to restart the services:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

   After restarting, check the status of services, enter: **`./manage-modules.sh service status all`**
5. Type the following command to verify the changes:

   ```
   su apg -c 'ulimit -n -u'
   ```

Uninstalling a SolutionPack

If you no longer want to view the reports of a certain SolutionPack, you can uninstall that SolutionPack from the server.

Procedure

1. Log in with administrator credentials for EMC M&R platform and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select the SolutionPack that you want to uninstall in the **Installed SolutionPacks** screen.
5. In the **Properties** area, click **Trashcan** icon for each instance of the SolutionPackBlock and click **Remove**.

Viewing SolutionPack reports

You can view your reports from the EMC M&R console.

Before you begin

After installing the SolutionPack, access the EMC M&R User Interface.

Procedure

1. Point your web browser to `http://[serverIP:port]/APG`.

   An example default URL is `http://localhost:58080/APG`.
2. On the login screen, enter your EMC M&R username and password, and click **Sign In**.
3. View SolutionPack reports by expanding **Report Library** > ***Your SolutionPack Name***.

SolutionPack for Acme Packet SBC Reports

A list of "out-of -the box" reports available with this SolutionPack appears in the table that follows.

You can drill-down on some top-level reports to view sub-level reports with specific metrics related to objects in the top-level report.

Table 19 Top-level reports

Reports	Description
CPU Usage %	Lists the CPU Utilization (%) for each polled device.
Memory Usage %	Lists the Physical Memory Utilization (%) for each polled device.
Global active Sessions NB	Displays the total instant number of Global Concurrent Sessions as of report generation time.
Inventory	Displays the inventory for all devices that are Acme Packet Net-Net capable including: • Routers: number of routers • Interfaces: number of couple routers / interfaces • KPIs: number of Key Performance Indicators (KPI) polled by APG for each object
Router Summary	This report lists all Acme devices with their global performance information. Click a device to get a full summary of the performance of that device
Realms Performance	Includes: • Realm Sessions Active: The active sessions report includes the sum of the number of active inbound realm sessions and the number of active outbound realm sessions. • Realm Sessions Rejected: The Realm Sessions Rejected Ratio is calculated as a percentage of the sum of realm rejected

Table 19 Top-level reports (continued)

Reports	Description
	(outbound and inbound) indicator that identify the total number of sessions rejected (outbound and inbound) due to insufficient bandwidth divided by the sum of total realm number of sessions. • Realm Sessions ASR%: This report displays the Answered to Seizures Ratio (ASR). This ratio is calculated as a percentage of total number of answered realm sessions by total number of seizured realm sessions
Sessions Performance	Includes: • Sessions Active: This report displays the total active sessions by device. The total active sessions by device is the sum of active sessions for all sessions. The active sessions is the sum of the number of active inbound sessions and the number of active outbound sessions. • Sessions Rejected: This report displays the total active sessions by device which equals the sum of active sessions for all sessions. Active sessions equals the sum of the number of active inbound sessions and the number of active outbound sessions. • Sessions ASR %: The report displays the Answered to Seizures Ratio (ASR) The ratio is calculated as a percentage of total number of answered sessions by total number of seizures sessions • Registration Statistics

Report metrics

The SolutionPack software uses report metrics to gather information from your ACME Packet SBC devices for monitoring and report creation.

This table lists metrics for the SolutionPack.

Table 20 Metrics

Metric type	Table	Metric name	W4n Collection Mode
ACME Session	InboundActionNSEPSession		SNMP

Table 20 Metrics (continued)

Metric type	Table	Metric name	W4n Collection Mode
	apCombinedSessionAgentStatsTable	InboundActive	SNMP
		OutboundActive	
		TotalInbound	
		InboundRejected	
		TotalOutbound	
		OutboundRejected	
		Seizures	
		Answered	
	apSigRealmStatsTable	InboundActive	SNMP
		OutboundActive	
		TotalInbound	
		InboundRejected	
		TotalOutbound	
		OutboundRejected	
		Seizures	
		Answered	
		Rfactor	
ACME-RESOURCES	apSysTable	ArpUtilization	SNMP
		ContactCount	
		CurrentLoad	
		GatewayCount	
		H323Count	
		MessagesRejected	
		NatUtilization	
		CurrentUtilization	CPU
		CurrentUtilization	Memory
		Health	
		SessionCount	
		CallCount	
	apEnvMonFanStatusTable		SNMP

Table 20 Metrics (continued)

Metric type	Table	Metric name	W4n Collection Mode
	apEnvMonPhyCardStatusTable		SNMP
	apEnvMonPowerSupplyStatusTable		SNMP
	apEnvMonTemperatureStatusTable		SNMP

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 271 provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 272.

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 272
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 274 2. Importing an SSL certificate into your truststore on page 273
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 273

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 274.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are

attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

  This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
   a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.
6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 273
  - Importing an SSL certificate in Firefox on page 273
  - Importing an SSL certificate in Internet Explorer on page 273

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** > **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** > **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** > **Options** > **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
8. Share the resulting exported SSL certificate with other users to use.

CHAPTER 24

SolutionPack for Alcatel-Lucent 5620 SAM Summary Sheet

- Overview 276
- Technical specifications 276
- Where to find the latest SolutionPack software 277
- Performing prerequisite installation tasks 277
- Installing the SolutionPack for Alcatel-Lucent 5620 SAM 277
- Performing post installation tasks 278
- Add the Alcatel SAM5620 configuration details 278
- Confirming report creation 279
- Troubleshooting 279

Overview

Learn how to install and configure the SolutionPack for Alcatel-Lucent 5620 SAM (Service Aware Manager). This SolutionPack collects data from the Alcatel-Lucent 5620 Service Aware Manager platform. This platform offers element, network, and service management for advanced Layer 2 and Layer 3 network solutions and services based on the Alcatel-Lucent's Carrier Ethernet and the IP/MPLS Service Routing portfolio.

SolutionPack for Alcatel-Lucent 5620 SAM offers the following:

- Highly scalable solutions supporting active and standby Alcatel-Lucent SAM architectures
- Powerful dashboards
- Topology data and device statistics collected from Alcatel-Lucent equipment
- Accurate real-time service-oriented views for operations, engineering, and customers
- Provisioning and statistics within the MPLS infrastructure integrated with other managed networks and equipment
- Report data based on the following:
  - Customers and Services
  - MPLS, Tunnels, and VRE
  - Performance, Health, and OAM probes

Technical specifications

SolutionPack version
3.0

Compatible EMC M&R versions
6.8u2 and later

Data collection method
Alcatel-Lucent 5620 SAM-O collector

The collector for Alcatel-Lucent 5620 SAM communicates with the Alcatel-Lucent SAM-O module via the Statistic Log Subscription using the Java Messaging Service (JMS). The Alcatel-Lucent 5620 SAM-O collector does the following:

- Sends XML requests to the Alcatel-Lucent SAM-O module.
- Subscribes to the JMS event for request completion.
- Fetches the response file to process it.

Supported devices
Alcatel-Lucent 5620 SAM release 11

Alcatel-Lucent 5620 release 11 (SAM-O module)

Main reports
Generic Device Performance (such as CPU and memory)

Physical and Logical Interface Performance

Multiprotocol Label Switch (MPLS) and Label-Switched Paths (LSPs) & Virtual Routing and Forwarding (VRF) Measurements

Service Access Points (SAPs)

Service Tunnel Traffic (SDPs)

Class of Forwarding Measurements

Ingress and Egress Traffic Details

Service Level Agreement (SLA)

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite installation tasks

This SolutionPack requires that you verify that the Alcatel-Lucent 5620 SAM environment is ready for the installation.

Procedure

1. Verify the Alcatel-Lucent 5620 SAM-O Module is configured and running.
2. Verify the FTP or SFTP server is running on the Alcatel-Lucent 5620 SAM server with valid permissions to the `server` folder, which stores the log files. These permissions enable the Alcatel-Lucent 5620 SAM-O collector to retrieve log files from the Alcatel-Lucent 5620 SAM server.
3. During the installation, you are asked for details about the Alcatel-Lucent 5620 SAM server, such as user name, password, and SAM-O Module port number. Contact the Alcatel-Lucent 5620 SAM administrator for these details.

Installing the SolutionPack for Alcatel-Lucent 5620 SAM

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Fill out the form with details for the **Alcatel-Lucent 5620 SAM Collector** and **Alcatel SAM 5620 specific configuration** and click **Next**.
7. Select the **Administration Web-Service Instance** as the default and click **Next**.
8. Wait until the installation is complete and then click **OK.**
9. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post installation tasks

After you install the SolutionPack for Alcatel-Lucent 5620 SAM, you must perform certain tasks.

Procedure

1. Copy the `samOss.jar` file from your Alcatel-Lucent 5620 SAM installation to your EMC M&R Stream collector `lib` folder.

   For example, copy `/opt/5620sam/client/nms/lib/SAM_11_0_R1/samOss.jar` to `/opt/APG/Collecting/Stream-Collector/alcatel-sam5620/lib/samOss.jar`
2. Change the ownership on the jar file in the Stream collector path.

   For example, `chown apg:apg /opt/APG/Collecting/Stream-Collector/alcatel-sam5620/lib/samOss.jar`
3. Start the collector by going to **Centralized Management** > **Collecting** > **Collector-Manager::alcatel-sam5620** > **Start**.
4. Check the logs at `/opt/APG/Collecting/Collector-Manager/alcatel-sam5620/logs`

Add the Alcatel SAM5620 configuration details

Ensure the Alcatel SAM5620 configuration details are added so discovery can occur.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Navigate to **Discovery Center** under **Centralized Management**.
3. Click **Inventory Management**.
4. Click **Alcatel Sam5620 Configuration**.

   The Alcatel SAM5629 configuration appears in the right pane
5. Click **Add** and provide the necessary details for Alcatel SAM 5620 SAM server.
6. Click **Validate and Add** to validate the details.

7. Click **OK**.
8. Click **Save**.

   The configurations are saved and the ASAM collector manager restarts.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Searching for metrics in the database on page 74
- Running a scheduled task to import data into reports on page 73
- What to do if the Collector-Manager does not start on page 280

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .

2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

What to do if the Collector-Manager does not start

Error message shown in log file

If you see this type of error message in the log files, verify the `samOss.jar` file from the Alcatel-Lucent 5620 SAM installation is correctly installed in the EMC M&R server. See Performing post installation tasks on page 278.

```
SEVERE   -- [2014-12-01 02:19:22 EST] -- StreamCollector::start():
Error while starting
```

```
com.watch4net.apg.ubertext.parsing.retriever.StreamRetrieverException:
Error while creating JMS context for source jnp://hostname:1099
at com.watch4net.apg.ubertext.parsing.retriever.JMSListenerRetriever
$JMSConnection.<init>(JMSListenerRetriever.java:404)
at com.watch4net.apg.ubertext.parsing.retriever.JMSListenerRetriever
$JMSConnection.<init>(JMSListenerRetriever.java:329)
at
com.watch4net.apg.ubertext.parsing.retriever.JMSListenerRetriever.startAutomaticRetrieving(
JMSListenerRetriever.java:127)
at
com.watch4net.apg.ubertext.parsing.DataRetriever.startAutomaticRetrieving(DataRetriever.jav
a:227)
at com.watch4net.apg.ubertext.collector.Collecting.scheduleCollecting(Collecting.java:148)
at com.watch4net.apg.ubertext.collector.StreamCollector.start(StreamCollector.java:129)
at
com.watch4net.apg.v2.collector.CollectorManagerImpl.startComponents(CollectorManagerImpl.ja
va:601)
at com.watch4net.apg.v2.collector.CollectorManagerImpl.start(CollectorManagerImpl.java:665)
at com.watch4net.apg.v2.collector.Bootstrap.serviceStart(Bootstrap.java:91)
at com.watch4net.apg.v2.collector.Bootstrap.main(Bootstrap.java:140)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:483)
at com.watch4net.apg.module.plugin.service.Bootstrap.main(Bootstrap.java:59)
```

CHAPTER 25

SolutionPack for Aruba Wi-Fi Summary Sheet

- Overview 284
- Technical specifications 284
- Where to find the latest SolutionPack software 285
- Installing a SolutionPack 285
- Confirming report creation 286
- Troubleshooting 286

Overview

Learn how to install and configure the SolutionPack for Aruba Wi-Fi. This SolutionPack provides the performance reports for the Aruba Wi-Fi controller, station, and Access Points. It collects and interprets data across multiple Aruba devices and performs resource grouping and mathematical calculations to help you evaluate performance.

This SolutionPack helps you:

- Check the number of stations connected to your controller in real-time.
- View all controllers, access points, ESSIDs, and radio through its inventory.
- Verify the access point efficiency by monitoring the transmitted packets, bandwidth, and signal-to-noise ratio, which demonstrates gains and lets you fine tune the device configuration for better results.
- Monitor the Aruba routers in real-time and pro-actively optimize the availability of your services.
- Understand the access point activity to see which AP device is being used the most, such as the peaks and busy hours of the device.

Technical specifications

SolutionPack version
2.0

Compatible EMC M&R versions
6.8u2 and later

Data collection method
SNMP collector

Supported devices
Aruba 3000 Series

Aruba 6000 Series

Supported MIBs
WLSX-SWITCH-MIB.mib

RFC1213-MIB.mib

Main reports
CPU Utilization for each device

Association (average/minimum)

Controller Summary of all devices managed in terms of number of access points, Availability %, CPU Utilization %, and access points bandwidth

Inventory of controllers, Extended Service Set Identifications (ESSID), access points, access point groups, and users

Performance Scorecard of association, ESSIDs, station, access point, access point groups, and radio summary

Situations to Watch, including the Top-5 Users Currently Connected (by Access Points), the Top-5 Currently High Bandwidth (by Stations), and the Top-5 Moving Users reports

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Follow these steps to install the SolutionPack for Aruba Wi-Fi and perform Aruba device discovery.

Procedure

1. Log in to **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.
3. Select the **SolutionPack for Aruba Wi-Fi** in the **Browse and Install SolutionPacks** screen.
4. Read the summary information and click **Install**.
5. Select the **Administration Web-Service Instance** as the default and click **Next**.
6. In the **SNMP Masks** wizard, click **Install**.
7. Wait until the installation is complete for both SNMP Masks and Report and then click **OK.**
8. Under **Collecting**, click **Administration** > **Device Discovery**.
9. On the **Device Discovery** page, click **Collectors**.
10. Create a new collector by accepting all the default options.
11. Click **Device** and add the Aruba device to be discovered.
    a. Type the IP address, the SNMP community string, and assign the collector that you previously created.

b. Select all Aruba capabilities to be discovered and any other capabilities.

12. Select the Aruba device that you just added and click **Approve.**
13. From the Dashboard:
    a. Click **Import devices from all enabled device sources**.
    b. Click **Discover capabilities from all approved devices**.
    c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
    d. Click **Send the generated configurations on all available collectors**.

    Green indicators appear on the Dashboard after successful executions of the above functions.
14. Select **Centralized Management** > **SolutionPack** to verify the installedSolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 26

SolutionPack for Avaya Aura Summary Sheet

- Overview 290
- Support 290
- Set up Avaya CDR and RTCP 291
- License management 300
- Installation 300
- Logging in to Centralized Management 300
- Installing the SolutionPack 301
- Starting the CDR and RTCP Listeners 302
- Log files 304
- Configuring the user process limits for the Linux installation 304
- Uninstalling a SolutionPack 305
- Viewing SolutionPack reports 305
- Avaya Reports 305
- Metrics for Avaya VoIP 306
- SSL certificates 311

Overview

Learn how to install and configure the SolutionPack for Avaya Aura. This SolutionPack reports on health statistics for the Avaya Aura Communication Manager call servers. The metrics are collected using SNMP for host statistics and call services.

In addition this SolutionPack:

- Reports on health statistics for the Avaya Aura Communication Manager call servers. Metrics are Collected via SNMP for host statistics, and call services.
- Provides inventory views for Network Regions, and phone end points, as well as registration status. This information is collected via SSH/SAT connections to the ACM <Perl>.
- Provides reports for MOS per phone call. This is collected via CDR (Call Detail Records). You must configure ACM CDR destination to W4N Text Collector, and RTCP (Real Time Communication Protocol) (Perl- based listener, IIRC).

Use these guidelines to prepare your environment for installation of the SolutionPack for Avaya VoIP.

- Verify that prerequisite software is installed in your environment. Support information
- Check that your EMC M&R network configuration has the minimum requirements to run reports.
- Set up your Avaya Aura environment.
  - Enable Call Detail Records (CDR)
  - Configure RTCP monitoring

After setting up your environment:

- Manage SolutionPack licenses.
- Install the SolutionPack for Avaya VoIP (first-time installations)

Support

Before installing this SolutionPack, review version support information.

Verify that prerequisite software is installed in your environment.

Table 21 Prerequisites for the SolutionPack for Avaya Aura Communication Manager

Software	Version
Watch4net	6.3 or higher installed on Red Hat LINUX or Windows
Perl (Linux)	5.8.8 or higher
Strawberry Perl (Windows)	5.18.2
Net-SSH (Linux only)	Net-SSH2-0.48

Set up Avaya CDR and RTCP

Before installing your SolutionPack you must configure your Avaya Aura environment to work with EMC M&R.

Avaya Aura CDR and RTCP monitoring must be configured so that Watch4net can communicate with your environment and generate Avaya Aura SolutionPackreports.

Enabling Call Detail Records (CDR)

In order for the SolutionPack for Avaya Aura to provide a full range of call metrics, you must configure the Avaya PBX so that Call Detail Records (CDRs) are sent to the IP address of the Watch4net Server.

Follow the steps in the following sections to configure CDR for Avaya Aura.

Procedure

1. Add node names.
2. Add an IP CDR service.
3. Set CDR system parameters.
4. Enable intra-switch CDRs.
5. Enable trunk groups.
6. Configure 10-Digit Plus dial plans..

After you finish

For additional details on performing any of these procedures, refer to *Configure CDR Monitoring*, Avaya document 100059519, available on the Avaya website: http://www.avaya.com.

Adding node names for CDR monitoring

With this procedure, you can configure the AVAYA device to send data to the EMC M&R instance where the SolutionPack is installed.

Follow these steps to add a new node for CDR monitoring. Make sure you have login credentials with proper administrative rights to make this configuration.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
   a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
   b. Enter password.
   c. Enter terminal type: `vt100`.
   d. At the prompt, enter `sat`.
   e. Enter terminal type: `W2KTT`.
2. Execute this command: `change node-names ip`.

```
change node-names ip
Page 1 of 2
                                IP NODE NAMES
```

```
    Name                IP Address            Name
IP Address
clan1                 10.1.10.21
clan2                 10.1.10.22
default               0.0.0.0
medpro1               10.1.10.31
medpro2               10.1.10.32
procr                 10.1.10.9
vall                  10.1.10.41
prognosis             10.1.10.105
```

3. Complete the following fields: `Name:` Add a name, then `IP Address:` Add the IP address of the host where Watch4net is running.
4. Press **`Esc + e`** to save and exit.

NAT Environment: In the case of a NAT environment the IP Address should be set to the Public IP address assigned to the IP Telephony Manager Monitoring server.

Note

If the PBX has an S85xx or S87xx series Media Server, then ensure that a valid node name for the CLAN board exists as well. If it has an S8300 series Media Server, then ensure that a valid node name for the PROCR also exists.

Adding IP CDR Service for CDR Monitoring

Use this procedure to define the CDR link.

Procedure

1. Execute the command: **`change ip-services`**.

```
 change ip-
services                                                Page 1 of
4
                                IP SERVICES
 Service      Enabled       Local      Local
Remote       Remote
Type                      Node       Port        Node
Port
CDR1                       clan1       0
prognosis      50000
```

2. To define a primary CDR link, enter the following details:
   - `Service Type: CDR1` - If CDR1 already exists, add a new destination by defining the Service Type to CDR2 (or as appropriate).
   - `Local Node: clan1` - Add the node name for the CLAN (S85xx or S87xx series) or PROCR (S8300 series).

     Note

     Execute list node-names `ip all` command to view the node name that refers to the ACM IP Address.

   - `Local Port: 0` - The Local Port is fixed to 0 as Avaya Communication Manager initiates the CDR link.
   - `Remote Node:` - This is the name you specified in `change node-names ip` step 3 in the previous section (Adding node names for CDR monitoring).

- `Remote Port:` - Set port to 5001. This is the port where the SolutionPack listens for the CDR data. With multiple Avaya hosts, all send data to the same port on the SP host.

3. Disable the Reliable Session Protocol (RSP) from the CDR link by setting the `Reliable Protocol` field to *n*.
4. Use `Esc n` to get to the `SESSION LAYER TIMERS` page. Set the value for the CDR you used in the previous screen for the Reliable Protocol to `n`. For example:

```
                            SESSION LAYER TIMERS
 Service   Reliable    Packet Resp    Session Connect
SPDU   Connectivity Type     Protocol      Timer
Message Cntr     Cntr      Timer
CDR1          n          30            3
3         60
```

5. Press **`Esc + e`** to save and exit.

Setting CDR System Parameters for CDR Monitoring

The CDR SYSTEM PARAMETERS form of the Avaya SAT program should be set up with the required parameters for the type of calls to track and format the CDR data.

Procedure

1. Execute the command: `change system-parameters cdr`

```
 change system-parameters
cdr                                      Page 1 of 1
                          CDR SYSTEM PARAMETERS
Node Number: (Local PBX ID)                       CDR Date
Format: month/day
  Primary Output Format: unformatted      Primary Output
Endpoint: CDR1
Secondary Output Format:                Secondary Output
Endpoint:
           Use ISDN Layouts? n                 Enable CDR
Storage on Disk? n
       Use Enhanced Formats? n    Condition Code 'T' For
Redirected Calls: n
     Use Legacy CDR Formats? y                Remove # From
Called Number? n
Modified Circuit ID Display? n
Intra-switch CDR? y
                Record Outgoing Calls Only? n     Outg Trk
Call Splitting? y
Suppress CDR for ineffective Call Attempts? y       Outg Attd
Call Record? y
    Disconnect Information in Place of FRL? n
Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis
Form? n
                                   Calls to Hunt Group -
Record: member-ext
Record Called Vector Directory Number Instead of Group or
Member? n
Record Agent ID on Incoming? n       Record Agent ID on
Outgoing? y
     Inc Trk Call Splitting? n
  Record Non-Call Assoc TSC? n          Call Record Handling
Option: warning
      Record Call-Assoc TSC? n  Digits to Record for Outgoing
```

```
Calls: dialed
   Privacy - Digits to Hide: 0              CDR Account Code
Length: 15
```

2. Edit the information. The following settings are recommended:
   - CDR Date Format: month/day
   - Primary Output Format: unformatted
   - Primary Output Endpoint: CDR1

   The following parameters define the type of calls that will be recorded and what data will be included in the record.

   - **Use Legacy CDR Formats? y** Specifies the use of the Avaya Communication Manager 3.x (legacy) formats in the CDR records produced by the system.
   - **Intra-switch CDR: y** If CDRs are required for intra-PBX calls, then the **Intra-switch CDR?** option must be set to `y`. This setting allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form.
   - **Record Outgoing Calls Only? n** Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
   - **Outg Trk Call Splitting? y** Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.
   - **Inc Trk Call Splitting? n** Disallows a separate call record for any portion of an incoming call that is transferred or conferenced.

   This is the recommended PBX setting, although setting `n` to all options is also possible. By using these recommended settings CDRs will be sent for most types of calls (conference calls, transfers, attendant) and intra-switch. Unless there is a requirement for any other particular option, the default should be `n`.

Enabling Intra-switch CDRs

CDRs are usually only sent when calls are made through a trunk. In the case of an Intra-switch call (for example, a call that goes to another phone directly connected to the PBX), a CDR will not be sent unless Intra-switch CDR has been enabled. Intra-switch CDRs are only available if enabled for specific extensions.

Before you begin

If the Intra-switch CDR field is set to *y* on Page 1 of the CDR SYSTEM PARAMETERS form, then the INTRA-SWITCH CDR form also needs to be updated to define the extensions that will be subjected to call detail recording.

Procedure

1. Execute the command: `change intra-switch-cdr`.

```
 change intra-switch-
cdr                                          Page 1 of 3
                               INTRA-SWITCH CDR


                                Assigned Members: 6    of
4000 administered
  Extension         Extension           Extension
```

```
Extension
  3001
  3002
  3003
  3004
  3005
  3006
```

2. In In the `Assigned Members` field, enter the individual extensions for usage tracking with the CDR records.

Enabling trunk groups for CDR monitoring

Enabling trunk groups is not required for configuring the SolutionPack, however if you do not configure them you will not get trunk group-related traffic statistics.

For each trunk group where CDR records are required, verify that CDR reporting is enabled.

Procedure

1. Execute the command: `change trunk-group`*<n>* (where *<n>* is the trunk group number.

```
change trunk-group
1                                          Page 1 of 21
                                   TRUNK GROUP
Group Number: 1                    Group Type: isdn
CDR Reports: y
  Group Name: Bondi H.323              COR: 1     TN:
1           TAC: 501
   Direction: two-way     Outgoing Display? y       Carrier
Medium: H.323
 Dial Access? n             Busy Threshold: 255     Night
Service:
Queue Length: 0
Service Type: tie                Auth Code? n       TestCall
ITC: rest
                       Far End Test Line No:
TestCall BCC: 4
```

2. Make sure that the CDR Reports field is set to *y*.
3. Repeat for all trunk groups to be reported.

CDR monitoring for 10 Digit Plus dial plans

You can optionally configure 10 Digit Plus dial plans for CDR.

Options include:

- Configure the Avaya PBX Custom Fields. Use this procedure when no other customized CDR system parameters have been specified for any other purposes on the Avaya PBX
- Including with other customized formats. Use this procedure if existing customized CDR system parameters are already configured on the Avaya PBX for the Billing Server or other CDR applications.

Configuring Avaya PBX custom fields

There are two options when configuring 10 Digit Plus dial plans for CDR.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
   a. Type: **ssh <username>@<ACM FQDN>** and then press **Enter**.
   b. At the prompt, type: **sat** and then press **Enter**.
   c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: **change system-parameters cdr**
3. Set the Output Format to **customized**. For example:

```
change system-parameters
cdr                                          Page 1 of 1
                           CDR SYSTEM PARAMETERS
Node Number: (Local PBX ID)                        CDR Date
Format: month/day
  Primary Output Format: customized       Primary Output
Endpoint: CDR1
Secondary Output Format:                Secondary Output
Endpoint:
           Use ISDN Layouts? n                 Enable CDR
Storage on Disk? n
       Use Enhanced Formats? n    Condition Code 'T' For
Redirected Calls: n
...
```

4. Go to page 2 of the CDR System Parameters form (Esc - n) and specify the customized CDR parameters as shown in the following code.

```
                           CDR SYSTEM PARAMETERS
   Data Item - Length         Data Item - Length         Data
Item - Length
 1: time             - 4   17: ins              - 3
33:                 -
 2: duration         - 4   18: ixc-code         - 4
34:                 -
 3: cond-code        - 1   19: bcc              - 1
35:                 -
 4: code-dial        - 4   20: ma-uui           - 1
36:                 -
 5: code-used        - 4   21: res_flag         - 1
37:                 -
 6: dialed-num       - 15  22: tsc_flag         - 1
38:                 -
 7: calling-num      - 15  23: null             - 1
39:                 -
 8: acct-code        - 15  24:                  -
40:                 -
 9: auth-code        - 13  25:                  -
41:                 -
10: frl              - 1   26:                  -
42:                 -
11: in-crt-id        - 3   27:                  -
43:                 -
12: out-crt-id       - 3   28:                  -
44:                 -
13: feat-flag        - 1   29:                  -
45:                 -
14: attd-console     - 2   30:                  -
```

```
46:                 -
15: in-trk-code       - 4   31:                  -
47:                 -
16: node-num          - 2   32:                  -
48:                 -
                              Record length = 103
```

Configuring other customized formats

Follow the procedure to configure the Avaya PBX and for other customized formats .

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
   a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
   b. At the prompt, type: `sat` and then press **Enter**.
   c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: **change system-parameters cdr**
3. Set the Output Format related to IP Telephony Manager to `customized`. For example:

```
change system-parameters
cdr                                       Page 1 of 1
                            CDR SYSTEM PARAMETERS
Node Number: (Local PBX ID)                        CDR Date
Format: month/day
  Primary Output Format: customized       Primary Output
Endpoint: CDR1
Secondary Output Format:                Secondary Output
Endpoint:
           Use ISDN Layouts? n                 Enable CDR
Storage on Disk? n
       Use Enhanced Formats? n    Condition Code 'T' For
Redirected Calls: n
...
```

   Go to page 2 of the form (Esc - n) and specify at least the following parameters:

   - time (4)
   - duration (4) or sec-dur (4)
   - cond-code (1)
   - code-used (4)
   - dialed-num (15)
   - calling-num (15), plus in-trk-code (4), or calling-num (15), plus in-trk-code (4), plus in-crt-id (3)

   These minimum parameters are required and must be added to the custom settings page along with the minimum field lengths as specified. You can also include additional parameters as shown in Standard Custom Format.

Configuring RTCP Monitoring

In order for the SolutionPack for Avaya Aura to receive RTCP data necessary to create SolutionPack reports, the Avaya PBX needs to be configured to send the reporting data to the IP address of the VoIP Monitor server

Procedure to set up RTCP.

Procedure

1. Set up the PBX
2. Set up network regions
3. Set up Avaya voice stream Monitoring
4. After configuring RTCP

Setting up the PBX

Perform these tasks to setup your PBX to work with the SolutionPack software.

Before you begin

Make sure you have login credentials with proper administrative rights to make this configuration.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
   a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
   b. At the prompt, type: `sat` and then press **Enter**.
   c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: `change system-parameters ip-options`
3. In the RTCP MONITOR SERVER section of the code, input the following values:
   - Set the **Default Server IP Address** to the IP address of the VoIP Monitor server.
   - Set the **Default Server Port** to 5005.
   - Set the **Default RTCP Report Period** (secs) to 5.
4. When finished press `Esc+e` to submit the changes.

Setting up network regions

After you set up the VoIP Monitor IP address on the Avaya PBX, configure the associated network regions IP addresses. You can configure either a default setting or add individual IP addresses for each region.

Procedure

1. Execute the command: `change ip-network-region <n>`, where `<n>` is the IP network region number to be monitored.
2. Set the **RTCP Reporting Enabled?** field to `y (yes)` and the **Use Default Server Parameters?** field to `y (yes)`.

   Only one RTCP MONITOR SERVER can be configured per IP network region.
3. Repeat Step 2 for all IP network regions that are required to be monitored, and then press `Esc+e` to submit the changes.

Results

The RTCP changes are implemented immediately for all calls, including those already in progress.

Setting up Avaya voice stream monitoring

Voice stream data settings direct voice stream RTCP information to VoIP Monitor.

To monitor voice stream data for Avaya SIP Phones, edit these settings in the Avaya `46xxsettings.txt` file.

Procedure

1. Edit `SET RTCPMON <ip_address>` and insert the `<ip_address>` of the VoIP Monitor server.
2. Edit `SET RTCPMONPORT <port_number>` and set the port number of the port used to send RTCP information to the IP address of the VoIP Monitor server, as specified in the `RTCPMON` statement. When possible use the default setting `5005`.
3. Edit `SET RTCPMONPERIOD <n>` where <n> specifies the time interval in seconds when the system sends RTCP monitoring reports (5-30 seconds, with the default of 5). Use the default.

After configuring RTCP Monitoring

After you set the default RTCP monitoring, make sure that you set all phone network regions to use the default RTCP server.

Procedure

1. To set all phone network regions to use the default RTCP server use the `change ip-network-region <n>` command (n = network region) from the Avaya CM command console, and make sure that all phone network regions use the default RTCP server.
2. Use these Avaya CM Native console commands to display and configure additional phones, IP addresses and network regions as needed.

Table 22 Avaya CM Native console commands

Command	Result
`list ip-interface all`	Lists IP interfaces/network regions
`display ip-network-region <n>`	Displays ip network region configuration.
`change ip-network-region <n>`	Change configuration for network region <n>
`list registered-ip-stations`	List of registered ip stations
`list station`	Avaya stations list

License management

You can evaluate features in the SolutionPack Center using 30-day temporary licenses included with EMC M&R software. If you install or plan to use the SolutionPack for longer than 30 days, contact EMC Online Support for permanent license files.

If you have an existing permanent license or a temporary license that requires updating, use the license upload feature in EMC M&R Centralized Management. Both permanent and temporary licenses are distributed in .zip files.

- Permanent licenses do not have expiration dates and may be associated with a host ID.
- Temporary licenses have expiration dates and are not associated with a host ID. When temporary licenses expire, the module license checks fail and the modules stop working. For example, the collector modules stop collecting new information and, if the front-end module fails, you cannot access the User Interface.

The SolutionPack license name is either SolutionPack for Avaya or ReportPack for Avaya. The system will use either license.

Installation

Review this information before beginning the installation.

- Make sure you review and perform the prerequisites outlined in the first chapter.
- Perform the installation with administrative privileges on the EMC M&R User Interface.

Logging in to Centralized Management

Log in to Centralized Management to perform operations that affect all servers.

Procedure

1. Point your browser to the URL.

   For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

   a. Type the login credentials.

      The default username is **`admin`** and the default password is **`changeme`**.

   b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Installing the SolutionPack

Using the EMC M&R console, install the SolutionPack.

Before you begin

Make sure you review requirements and complete relevant procedures described in Overview on page 290, and have your credentials for Avaya Aura Communication Manager and EMC M&R on hand.

Procedure

1. Log in to EMC M&R with root privileges.

   For example, `http://Frontend-hostname:58080/APG`

2. Select **Administration**.
3. Select **Centralized Management** in the **Administration** tree.
4. Select **SolutionPack Center**.
5. Select **Avaya Aura Communication Manager** in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Accept the default name, `avaya-voip-acm`, in the **Instance name** field.
   b. Select the EMC M&Rserver that will host the data collector in the **Data collection** list box.
   c. Select the EMC M&R server to host the reports in the **Reports** list box.
   d. Click **Next**.
8. Accept the default values for the **Data Collection** and **Alerting on Data Collection** panes.
9. Enter the server addresses, root credentials, and path to the Perl executable directory for the Avaya VoIP-specific configuration. The default Perl path for Windows: `C:\strawberry\perl\bin` and for Linux : `/usr/bin`

   After installing the SolutionPack, you can click the Device Discovery link in the post install message window, and follow this link to configure SNMP monitoring for the Avaya Call Managers you provided during SolutionPack installation. Alternatively you can add the devices later by accessing the Device Discovery module from Administration window. Follow these steps:

   a. Create a collector (if you have not already created one). Navigate to **Device Discovery** > **Collectors** > **Add New Collector**.
   b. Add a device to Watch4net: Navigate to **Administration** > **Modules** > **Device Discovery** > **Devices** > **Add New Device**, and then configure the name of the device and IP address as part of Main parameters.

   Note

   Make the **Device Type** `CallManager`, otherwise data for Avaya Health reports will not be displayed in the console.

c. Configure SNMP Credentials.

d. Add the previously created collector.

e. Select appropriate Avaya capabilities for `AVAYA-SERVER, GENERIC-INTERFACES, GENERIC-SYSUPTIME`.

f. Distribute: navigate to **Device Discovery** > **Dashboard** and then click `distribute all approved devices with Capabilities on all enabled collectors`.

After you finish

Allow four to five polling cycles to pass before viewing reports.

Note

If data for CDR reports does not appear, verify whether the CDR Link established successfully by executing the `status cdr-link` command from SAT terminal. Link state should be up.

```
sample output :
                                  CDR LINK STATUS
                    Primary                       Secondary

       Link State: up                             down
Number of Retries:                                ÿÿÿÿ
      Date & Time: 2014/02/06 03:46:08            2014/01/16 10:08:20
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK                             Maintenance busy

2. If Link state is down, then execute "test cdr-link primary long"
command from SAT terminal to test primary cdr link. Test 215 should
PASS.
   Sample Output :
                                            TEST RESULTS

Port        Mtce Name   Alt. Name        Test No.  Result
Error Code

            PRI-CDR                      213       PASS
            PRI-CDR                      215       PASS
```

If the Test 215 = fail, verify:

- Watch4Net server is reachable from ACM
- CDR Listener is running on Watch4Net Server on port 5001(default)

Starting the CDR and RTCP Listeners

After installing the SolutionPack, start the CDR and RTCP listeners.

Procedure

1. For Linux, go to `<APG_HOME>/Collecting/Text-Collector/avaya-voip-acm/conf/scripts`.
   - ./avayaListeners.sh start – This option starts both RTCP and CDR listener
   - ./avayaListeners.sh status - This option shows the status of the listeners in the system.

- ./avayaListeners.sh stop - This option stops the listeners.
- ./avayaListeners.sh install – This option runs the listeners as a start option mentioned above addition to install the listeners into System startup so that it starts automatically when the system gets restarted / rebooted.

Note

As you run the above script with parameter start and install, two additional script files are generated. They are `runAvayaCDRListener.sh` and `runAvayaRTCPListener.sh`. These are actual files to start the listeners created by this script.

2. For Windows, go to `<APG_HOME>/Collecting/Text-Collector/avaya-voip-acm/conf/scripts`, and run `avayaListeners.bat` to start the listeners using the command: **`Cmd> avayaListeners.bat`**

Note

As you run the batch file, two additional batch files are generated. They are `runAvayaCDRListener.bat` and `runAvayaRTCPListener.bat`. Use these files to start the listeners created by this batch file.

To start the listeners automatically on the system restart, add these scripts separately as two tasks in Task Scheduler. This step is carried out after running the avayaListeners.bat. The procedure follows:

a. Go to **Start** > **All Programs** > **Accessories** > **System Tools** > **Task Scheduler**
b. Select **Action** > **Create Task**
c. Add the name of the task to be created under **General Tab**.
d. Select **Run** whether or not the user is logged on.
e. Select **Run** with highest privileges.
f. Go to the **Triggers** tab.
g. Add **New Trigger**.
h. Select **Begin the Task** as **At Startup**.
i. In **Advanced settings**, select **Enabled**.
j. Go to the **Actions** tab.
k. Select **New** action.
l. Select **Action** as **Start a Program**.
m. In **Settings** section below in the same tab, select **Program Script**– select the `runAvayaRTCPListener.bat` from `conf/scripts` folder.
n. Go to last tab Settings and deselect **Stop the task if it runs longer than** option.
o. Click **OK**.

Repeat these steps to create a task with different name for the `runAvayaCDRListener.bat` script. With Step M, you need to select the `runAvayaCDRListener.bat` file.

Log files

Information on the log files for this SolutionPack follow.

Log files for the SolutionPack for Avaya Aura are located in: `<APG_installdir>/Collecting/Collector-Manager/avaya-voip-acm/logs`.

Since this SolutionPack also uses Generic SNMP collector, the log files for this collector appear in `<APG_install>/Collecting/Collector-Manager/Generic-SNMP/logs`.

Configuring the user process limits for the Linux installation

Increase the user process limits for the user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed.

Before you begin

- Make sure you have a login with root privileges.
- The EMC M&R platform installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6.
- The name specified for the user account during the installation.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

   In this example, the user is `apg`.

   ```
   apg   hard  nofile  65534
   apg   soft  nofile  65534
   apg   hard  nproc   65534
   apg   soft  nproc   65534
   ```

3. Save the file.
4. Type the following commands from the `bin` directory of the installation to restart the services:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

   After restarting, check the status of services, enter: **`./manage-modules.sh service status all`**

5. Type the following command to verify the changes:

   ```
   su apg -c 'ulimit -n -u'
   ```

Uninstalling a SolutionPack

If you no longer want to view the reports of a certain SolutionPack, you can uninstall that SolutionPack from the server.

Procedure

1. Log in with administrator credentials for EMC M&R platform and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select the SolutionPack that you want to uninstall in the **Installed SolutionPacks** screen.
5. In the **Properties** area, click **Trashcan** icon for each instance of the SolutionPackBlock and click **Remove**.

Viewing SolutionPack reports

You can view your reports from the EMC M&R console.

Before you begin

After installing the SolutionPack, access the EMC M&R User Interface.

Procedure

1. Point your web browser to `http://[serverIP:port]/APG`.

   An example default URL is `http://localhost:58080/APG`.
2. On the login screen, enter your EMC M&R username and password, and click **Sign In**.
3. View SolutionPack reports by expanding **Report Library** > ***Your SolutionPack Name***.

Avaya Reports

This list includes the "out-of -the box" reports available with this SolutionPack.

Some top-level reports include additional sub-level reports with specific metrics related to the top-level report.

- CPU Utilization for System %
- CPU Utilization for Calls %
- CPU Utilization %
- Avaya Health
- Busy Calls
  - Data
  - Media
  - Service
  - Total

    - Voice
- Calls completed
    - Data
    - Media
    - Service
    - Total
    - Voice
- Other Reports
    - Alarm Occurrences
    - Number of Connections to Switch
    - More Reports
        - Registered Phone Summary
        - Port Network Summary
            - Avaya CDR Reports - Call Data Records (Call Detail and Duration)
            - Avaya RTCP Reports - RTCP Summary Report (all network with Source of the call)
        - Media Gateways
        - Network Region Report
        - Occupancy Summary Report
            - Occupancy - Reports time 000 till 2300 - for last 24 hours
            - Calls Summary Report
            - Connections Summary Report
            - Idle Occupancy Report
        - Trunk Group Report
            - Trunk Group Inventory Report
            - Trunk Group Member Report

Metrics for Avaya VoIP

Report metrics are used to create various reports within the SolutionPack. Metrics gather information on values such as switch name, product ID, RTCP Monitoring IPV4 address, Trunk Group number, and many more listed in this table.

Table 23 Report metrics

Group Metrics	Details of the Metric	Mode of Collection in APG
IP Phones		
extension	Extension	Text-Collector
set_type	Model /Type	Text-Collector
product_id	Product ID	Text-Collector

Table 23 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
station_ip	IP Address	Text-Collector
product_release	Software Release Version of the Phone	Text-Collector
gatekeeper_ip	Gatekeeper's IP Address	Text-Collector
ACM Processor Occupancy Summary		
meas_hour	Measurement Hour (0000, 0100, 0200,0300...2300)	Text-Collector
switch_name	Switch Name	Text-Collector
date	Date of the collected information	Text-Collector
static_occ	Static Occurrence	Text-Collector
cm_occ	CM Occurrence	Text-Collector
sm_occ	SM Occurrence	Text-Collector
idle_occ	Idle Occurrence	Text-Collector
total_calls	Total no of calls	Text-Collector
tandem_calls	Total no of tandem calls	Text-Collector
total_conn	Total Connections	Text-Collector
intcom_atmpts	Internal Communication attempts	Text-Collector
inc_atmpts	Incoming attempts	Text-Collector
out_atmpts	Outgoing attempts	Text-Collector
pnet_atmpts	Port Networking attempts	Text-Collector
Network Region Information		
Region	Network Region number	Text-Collector
Name	Name of the NR	Text-Collector
ipv4PortNum	IPV4 Port Number	Text-Collector
rtcpMonIPv4	RTCP Monitoring IPV4 address	Text-Collector
rptPeriod	Report Period	Text-Collector
udpMinPort	UDP port allocated Minimum	Text-Collector
udpMaxPort	UDP port allocated Maximum	Text-Collector
codecStatus	CODEC Status	Text-Collector
Port Network Data		
portnetwork	Port Network Number	Text-Collector

Table 23 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
major	No of Major alarms	Text-Collector
minor	No of Minor alarms	Text-Collector
Warning	No of Warning alarms	Text-Collector
CarrierlocA	Carrier Location A	Text-Collector
CarrierlocB	Carrier Location B	Text-Collector
pnctrlActive	Port Network Controller Active	Text-Collector
pncontrolStdby	Port Network Controller Standby Status	Text-Collector
Trunk Group Status and Monitoring		
TrunkGroupNo	Trunk Group Number	Text-Collector
Size	Size of the TG	Text-Collector
Active	Status of the TG	Text-Collector
QueueSize	Queue Size	Text-Collector
Waiting	No of waiting calls in that TG	Text-Collector
tac	Trunk Access Code	Text-Collector
tgtype	TG Type	Text-Collector
group_name	TG Name	Text-Collector
mem_numbers	Number of members in that TG	Text-Collector
cor	COR (Class of Restriction)	Text-Collector
cdr	CDR (Call Data Record)	Text-Collector
CDRData		
Date	Date of the call monitored	Text-Collector
Time	Time of the call monitored	Text-Collector
To	Extension To	Text-Collector
From	Extension From	Text-Collector
Duration	Duration of the call	Text-Collector
MediaGatewayInfo		
number	Media Gateway Number	Text-Collector
gwname	Gateway Name	Text-Collector
gwserial	GW Serial Number	Text-Collector
gwtype	GW Type	Text-Collector

Table 23 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
gwip	GW IP address	Text-Collector
gwnrnet_region	Network Region to which the Gateway belongs	Text-Collector
gwregd	GW Registration Status	Text-Collector
firmware_ver	Firmware Version of the GW	Text-Collector
hardware_vintage	Hardware Vintage Version	Text-Collector
clan_ipaddress	CLAN IP Address	Text-Collector
RTCPData		
station-ip	IP Address	Text-Collector
packet-type	Packet Type (SR, RR, SDES etc.)	Text-Collector
ssrc	SSRC - Source of the call	Text-Collector
lastseq	Last Sequence Number	Text-Collector
lsr	Last SR Received	Text-Collector
dlsr	Delay value from the Last SR received	Text-Collector
time	Time of the monitoring data	Text-Collector
jitter	Jitter	Text-Collector
frlost	Fraction Lost	Text-Collector
packlost	Packet Lost	Text-Collector
MoS	Computed based on Latency, PacketLost,Jitter	Formula
R-Factor	Computed based on Latency, PacketLost,Jitter	Formula
OtherACMDatacollectedatACMlevel		
sysUpTime	Uptime	SNMP-Collector
g3connectState	Availability	SNMP-Collector
g3connectTimeUp	Uptime	SNMP-Collector
g3connectAttempts	Attempts	SNMP-Collector
g3connectSuccess	Success	SNMP-Collector
g3connectRequests	DataRequests	SNMP-Collector
g3connectResponses	DataResponses	SNMP-Collector
g3connectErrors	DataErrors	SNMP-Collector
g3connectQueued	DataQueued	SNMP-Collector

Table 23 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
g3healthMajor	AlarmsMajor	SNMP-Collector
g3healthMinor	AlarmsMinor	SNMP-Collector
g3healthWarning	AlarmsWarning	SNMP-Collector
g3healthTrkBusy	TrunksBusy	SNMP-Collector
g3healthStnBusy	StationsBusy	SNMP-Collector
g3healthOthBusy	OthersBusy	SNMP-Collector
g3healthLogins	ActiveLogins	SNMP-Collector
g3healthStaticOcc	CurrentUtilization	SNMP-Collector
g3healthCallpOcc	CurrentUtilization	SNMP-Collector
g3healthSysMgmtOcc	CurrentUtilization	SNMP-Collector
g3healthIdleOcc	CpuIdle	SNMP-Collector
g3pnchealthPncAMajor	AlarmsMajor Port Network Controller A	SNMP-Collector
g3pnchealthPncAMinor	AlarmsMinor Port Network Controller A	SNMP-Collector
g3pnchealthPncAWarning	AlarmsWarning Port Network Controller A	SNMP-Collector
g3pnchealthPncBMajor	AlarmsMajor Port Network Controller B	SNMP-Collector
g3pnchealthPncBMinor	AlarmsMinor Port Network Controller B	SNMP-Collector
g3pnchealthPncBWarning	AlarmsWarning Port Network Controller B	SNMP-Collector
g3stamediaAlarmMajor	AlarmsMajor	SNMP-Collector
g3stamediaAlarmMinor	AlarmsMinor	SNMP-Collector
g3stamediaAlarmWarning	AlarmsWarning	SNMP-Collector
g3stamediaBusyOutTrunks	TrunksBusy	SNMP-Collector
g3stamediaBusyOutStations	StationsBusy	SNMP-Collector
g3stamediaH248LinksDown	H248LinksDown	SNMP-Collector
g3stamediaH248LinksUp	H248LinksUp	SNMP-Collector
g3stamediaNbrLogins	ActiveLogins	SNMP-Collector
g3callratedataNumCalls	CallCompleted	SNMP-Collector
g3callratedataBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratevoiceNumCalls	CallCompleted	SNMP-Collector
g3callratevoiceBsyCalCmpl	BusyCallCompleted	SNMP-Collector

Table 23 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
g3callratesrvNumCalls	CallCompleted	SNMP-Collector
g3callratesrvBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratemediaNumCalls	CallCompleted	SNMP-Collector
g3callratemediaBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratetotalNumCalls	CallCompleted	SNMP-Collector
g3callratetotalBsyCalCmpl	BusyCallCompleted	SNMP-Collector

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 271 provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 272.

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 272
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 274 2. Importing an SSL certificate into your truststore on page 273
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 273

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 274.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

  This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
   a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.

6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 273
  - Importing an SSL certificate in Firefox on page 273
  - Importing an SSL certificate in Internet Explorer on page 273

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** > **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** > **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** > **Options** > **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.

8. Share the resulting exported SSL certificate with other users to use.

CHAPTER 27

SolutionPack for Blue Coat PacketShaper Summary Sheet

- Overview 318
- Technical specifications 318
- Where to find the latest SolutionPack software 318
- Installing a SolutionPack 319
- Configuring SNMP device discovery 319
- Confirming report creation 320
- Troubleshooting 321

Overview

Learn how to install and configure the SolutionPack for Blue Coat PacketShaper. This SolutionPack monitors most Blue Coat PacketShaper devices to provide real-time views of your wide area network traffic, including the top ten busiest WAN traffic classes. It reports on inbound and outbound traffic classifications and shows historical data for periods ranging from an hour, day, week, month, or a customized time slot.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIB
BLUECOAT-PACKETSHAPER-MIB

Supported devices
This SolutionPack can collect data from any Blue Coat PacketShaper device that supports the BLUECOAT-PACKETSHAPER-MIB.

Main reports
Top 10 Traffic Classes Chart, inbound and outbound traffic (bit/s)

View Global Statistics

View Traffic Per Classes

CPU Utilization

Memory Available

Availability of Devices

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.

3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.

   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.

      On the **Main parameters** tab, make sure you specify `Probe` for **Device Type**.

   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

      Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 28

SolutionPack for BGP Summary Sheet

- Overview 324
- Technical specifications 324
- Where to find the latest SolutionPack software 325
- Installing a SolutionPack 325
- Configuring SNMP device discovery 326
- Confirming report creation 327

Overview

Learn how to install and configure the SolutionPack for BGP (Border Gateway Protocol). This SolutionPack provides analytics on BGP routers and neighbors, traffic on links, and exception reports on down or flapping links. BGP is the core routing protocol of the Internet. It maintains the table of IP networks that designates network reachability among autonomous systems (AS).

BGP neighbors, or peers, are established by manual configuration between routers to create a TCP session on port 179. The BGP speaker periodically sends 19-byte keep-alive messages to maintain the connection, which is every 60 seconds by default.

The SolutionPack for BGP tracks the following information:

- Overall BGP traffic (peaks may indicates abnormal activity such as high route changes.
- All disconnect BGP sessions or flapping sessions (session duration that averages less than one hour).
- All properties and statistics per BGP neighbor.
- All properties and statistics per BGP router.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIB
BGP4-MIB

Supported devices
This SolutionPack can collect data from any BGP-enabled device that supports BGP4-MIB.

Main reports

BGP Traffic
: Shows the overall BGP traffic.

Exception: Flapping (or disconnected) BGP Neighbors
: Lists all disconnect BGP sessions or flapping sessions (session duration averaging less than one hour).

View per BGP Neighbors
: Displays all properties and statistics per BGP neighbor.

View per BGP Routers
: Shows all properties and statistics per BGP router.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.

d. Click **Send the generated configurations on all available collectors**.

Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 29

SolutionPack for Check Point Firewall Summary Sheet

- Overview 330
- Technical specifications 330
- Where to find the latest SolutionPack software 331
- Installing a SolutionPack 331
- Configuring SNMP device discovery 332
- Confirming report creation 333
- Troubleshooting 333

Overview

Learn how to install and configure the SolutionPack for Check Point Firewall. This SolutionPack provides unified monitoring of all the Check Point devices distributed in a network with firewall capabilities. It collects and interprets data across multiple Check Point devices, and performs resource grouping and mathematical calculations to generate performance information.

The SolutionPack for Check Point Firewall helps you do the following:

- Verify the traffic accept by the firewall and check how many packets are dropped by the firewall.
- See the number of connections over time.
- Monitor the Check Point routers in real-time and pro-actively, so you optimize your services availability.
- Understand your devices activity, to know which Check Point device has the most traffic by application, for example when devices reach peak loads.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R version
6.5u1 and later

Data collection method
SNMP collector

Supported MIBs
CHECKPOINT-MIB.mib

RFC1213-MIB.mib

Supported devices
Check Point 2200 appliances

Check Point 4000 appliances

Check Point Firewall-1

Main reports

Session Failure %
Shows a Session Failure graph over a period of time for each polled firewall.

Firewall CPU Usage %
Shows a CPU Usage graph over a period of time for each polled firewall.

Firewall with Most Connections
Provides a TopN Firewall graph showing a firewall with the highest number of connections over a selected time period.

Firewall Summary
Provides summaries of the Availability %, CPU Usage %, Session Load %, and Number of Connections of firewall devices.

Inventory

Displays the inventory (count only) of the Cisco Firewall network.

Performance Scorecard

Reports on firewall hardware availability for memory, CPU, interface, units, disk, and power.

Situations to Watch

Displays critical and major interface errors, such as half open connections and session bottlenecks, for each polled firewall.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.
- Make sure you know the name, IP address, SNMP port, and the community string of the firewall device.
- Verify the firewall is configured to allow network access to the SNMP port.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.

7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. For each list box you select, a screen appears.
   a. Click **Next** after you complete each screen.
   b. Click **Install** after you complete the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.

      On the **Main parameters** tab, make sure you specify `Firewall` for **Device Type**.

b. Click **Save** on each tab.

6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

   Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 30

SolutionPack for Cisco Firewall Summary Sheet

- Overview 338
- Technical specifications 338
- Where to find the latest SolutionPack software 339
- Installing a SolutionPack 339
- Configuring SNMP device discovery 340
- Confirming report creation 341
- Troubleshooting 341

Overview

Learn how to install and configure the SolutionPack for Cisco Firewall. This SolutionPack provides unified monitoring of all the Cisco ASA/PIX devices distributed in the network.

The SolutionPack for Cisco Firewall enables you to do the following:

- Verify the load session both for IKE Phase 1 and IPSec Phase 2 VPN tunnels.
- Verify the firewall efficiency by monitoring the packet rate and connections, so you can demonstrate gains and fine-tune your device configuration.
- Monitor the Cisco ASA/PIX devices in real-time to pro-actively optimize your services availability.
- Understand your device activity, for example, listing which Cisco ASA opens the most firewall connections, as well as activity peak times and more.
- Collect and interpret data across multiple Cisco ASA devices to perform resource grouping and mathematical calculations making performance information readily available.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIBs
CISCO-CRYPTO-ACCELERATOR-MIB.mib

CISCO-IPSEC-FLOW-MONITOR-MIB.mib

OLD-CISCO-INTERFACES-MIB.mib

CISCO-FIREWALL-MIB.mib

CISCO-REMOTE-ACCESS-MONITOR-MIB.mib

Supported devices
Cisco ASA 5500 Series

Cisco PIX 500 Series

Main reports

Session Failure %
Shows a Session Failure graph over a period of time for each polled firewall.

Firewall CPU Usage %
Shows a CPU Usage graph over a period of time for each polled firewall.

Firewall with Most Connections
Provides a TopN Firewall graph showing a firewall with the highest number of connections over a selected time period.

Firewall Summary

Provides summaries of the Availability %, CPU Usage %, Session Load %, and Number of Connections of firewall devices.

Inventory

Displays the inventory (count only) of the Cisco Firewall network.

Performance Scorecard

Reports on firewall hardware availability for memory, CPU, interface, units, disk, and power.

Situations to Watch

Displays critical and major interface errors, such as half open connections and session bottlenecks, for each polled firewall.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.
- Make sure you know the name, IP address, SNMP port, and the community string of the firewall device.
- Verify the firewall is configured to allow network access to the SNMP port.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.

4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. For each list box you select, a screen appears.
   a. Click **Next** after you complete each screen.
   b. Click **Install** after you complete the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.

a. On the **New Device** window, click each tab and type the required information for the device.

   On the **Main parameters** tab, make sure you specify `Firewall` for **Device Type**.

b. Click **Save** on each tab.

6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:

   a. Click **Import devices from all enabled device sources**.

   b. Click **Discover capabilities from all approved devices**.

   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.

   d. Click **Send the generated configurations on all available collectors**.

   Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.

4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 31

SolutionPack for Cisco IP-SLA Summary Sheet

- Overview 346
- Technical specifications 346
- Where to find the latest SolutionPack software 347
- Prerequisite 347
- Installing the SolutionPack 348
- Polling groups definitions 349
- Configuring probes on Cisco devices 350
- Confirming report creation 352
- Troubleshooting 353
- SSL certificates 354

Overview

Learn how to install and configure the SolutionPack for Cisco IP-SLA.

The SolutionPack for Cisco IP-SLA is specifically designed to monitor most common IP-SLA probes running on Cisco IP-SLA enabled devices. Supported probe types include: Jitter, HTTP, IcmpEcho and several others. This SolutionPack provides two ways of polling the Cisco IP-SLA enabled devices, which allow long term trend analysis or punctual troubleshooting when required.

Technical specifications

SolutionPack version
2.0

Compatible EMC M&R version
6.8u2 and later

Data collection methods
SNMP collector

Supported devices
WLSX-SWITCH-MIB.mib

RFC1213-MIB.mib

Main Reports

IP-SLA Probe Inventory View (By Device and Probe type)

Includes both running probes and device capabilities. The IP-SLA Probe Performance View (By Device and Probe type) includes detailed reports on the following probe types:

- TCP Connect operation
- DHCP Operation
- DNS Operation
- ICMP Echo Operation
- Jitter Operation
- HTTP Operation
- FTP Operation

IP-SLA Probe Performance View (By device)

Lists all the probes by device.

IP-SLA Probe Performance View (By probe type)

Lists all the probes by probe type.

Situations to Watch

Displays unsuccessful operations, latency, and reachability problems.

History and Last Operation table based reports

Displays history and last operation reports.

Note

The “History and Last Operation table based reports” are disabled by default. This node must be enabled by editing it. Data collection for those reports is also disabled by default as it requires more bandwidth and resources.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Prerequisite

Before installing the SolutionPack for Cisco IP-SLA, perform these prerequisite tasks:

1. M&R's Backend and Frontend must be installed. Versions higher than 6.5u4 are supported.
2. Cisco Routers are supported by this SolutionPack. IOS version 11.2 and later are supported. IOS 12.0(5)T and higher is recommended.
3. Currently, supported probes are IP/ICMP Echo, SNA Echo, TCP Connection, UDP Echo, Jitter/UDP Plus. VoIP UDP Jitter (MOS / ICPIF) also supported (last operation table polling only), HTTP, FTP, DHCP, and DNS.
   Probe support also depends upon the Cisco IOS version installed on the polled devices.

   Note

   Certain metrics, such as MOS and ICPIF, may be obtained only from devices which support them (IOS 12.3(14)T or later provides these metrics).

   IP-SLA was introduced on IOS 12.3(14)T. It supercedes SAA (Service assurance agent). This SolutionPack is compatible with both IPSLA and SAA, since both technologies are similar and use the same basic MIB.

   SAA operation types were introduced gradually, starting from IOS 11.2:

   - dhcp: 12.0(5)T
   - dlsw: 12.0(5)T
   - dns: 12.0(5)T
   - echo (ipIcmpEcho, snaRUEcho, snaLUEchoAppl, snaLU2EchoAppl): 11.2
   - ftp: 12.1(1)T
   - http: 12.0(5)T

- jitter: 12.0(5)T
- tcpConnect: 12.0(3)T
- udpEcho: 12.0(3)T

4. Supported probes must be configured for the CISCO devices. As a general guideline, leave the buckets-of-history-kept, distributions-of-statistics-kept, filter-forhistory, hops-of-statistics-kept, hours-of-statistics-kept, lives-of-history-kept, paths-of-statistics-kept, samples-of-history-kept, statistics-distribution-interval and other parameters related to probe history/statistics to their DEFAULT VALUE when creating the probe on the Cisco device.

Note

The Cisco IP-SLA SolutionPack does not focus on configuring the probes currently, as user interface to configure IP-SLA probes is not part of the EMC M&R Platform .

Installing the SolutionPack

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Watch4net Installation and Configuration Guide* provides for more information.

Follow these steps to install the SolutionPack for Cisco IP-SLA and perform Cisco device discovery.

Procedure

1. Log in to **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.
3. Select the **SolutionPack for Cisco IP-SLA** in the **Browse and Install SolutionPacks** screen.
4. Read the summary information and click **Install**.
5. Select the **Administration Web-Service Instance** as the default and click **Next**.
6. In the **SNMP Masks** wizard, click **Install**.
7. Wait until the installation is complete for both SNMP Masks and Report and then click **OK.**
8. Under **Collecting**, click **Administration** > **Device Discovery**.
9. On the **Device Discovery** page, click **Collectors**.
10. Create a new collector by accepting all the default options.
11. Click **Device** and add the Cisco device to be discovered.
    a. Type the IP address, the SNMP community string, and assign the collector that you previously created.

b. Select all Cisco capabilities to be discovered and any other capabilities.

12. Select the Cisco device that you just added and click **Approve.**
13. From the Dashboard:
    a. Click **Import devices from all enabled device sources**.
    b. Click **Discover capabilities from all approved devices**.
    c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
    d. Click **Send the generated configurations on all available collectors**.

    Green indicators appear on the Dashboard after successful executions of the above functions.

After you finish

After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Polling groups definitions

The following table provides information on various types of polling groups.

Polling Group Name	Polling Period	Agents Group	Snmp masks	Notes
G_CISCO_IPSLA_INV ENTORY	900 seconds. A 15 minute polling period allows quick probe discovery when they are set up.	IPSLA	CISCO-IPSLAINVENTORY	This polling group is used to poll inventory data on the probes.
PG_CISCO_IPSLA_HIS TORY	300 seconds.	IPSLA_HISTORY	CISCO-IPSLAHISTORY	This polling group is used to poll the IPSLA History table (rttMonHistoryCollectionTable). This table contains dat about the latest “n” operations for a probe. “n” being the number of statistics buckets configured for the probe. This group must be enabled manually to be used.
PG_CISCO_IPSLA	300 seconds.	IPSLA	CISCO-IPSLASTATSTABLE	Poll all probes, except Jitter, HTTP and IcmpPathEcho, using the statistics table.

Polling Group Name	Polling Period	Agents Group	Snmp masks	Notes
PG_CISCO_IPSLA_JITTER	300 seconds.	IPSLA	CISCO-IPSLAJITTERSTATSTABLE	Polls the Jitter probes, using the statistics table.
PG_CISCO_IPSLA_HTTP	300 seconds.	IPSLA	CISCO-IPSLAHTTPSTATSTABLE	Polls the HTTP probes, using the statistics table.
PG_CISCO_IPSLA_LATEST_OPERATION	60 seconds. The polling period should be set to the shortest probe frequency in order to gather all data. Data point will be missing if polling occurs more slowly.	PG_CISCO_IPSLA_LATEST_OPERATION	CISCO-IPSLAHTTP-LATEST, CISCO-IPSLAJITTER-LATEST	Use this polling group to poll the latest operation tables for HTTP and Jitter probes. This group is OPTIONAL as it generates a lot of network traffic and cpu load on the device and collector.

NOTE about the POLLING PERIOD on the polling groups using the STATISTICS TABLES:
The polling period must be set to a value equal or higher than the slowest probe being queried. Otherwise, spurious values (with a zero value) may appear in the reports. This applies to the polling groups using the CISCO-IPSLA-XXX-STATSTABLE.

NOTE about the POLLING PERIOD on the polling groups using the LATEST-OPERATION tables:
The polling period must be set to a value smaller than the probe with the smallest frequency. This shall be done to ensure that no data points are lost.

NOTE about the POLLING PERIOD on the polling groups using the HISTORY tables:
The polling group periods for those tables depend upon the probe configurations:

- The period may be set to 300 seconds when multiple history lives and buckets are used. For a typical application (a IcmpEcho probe, setup with a 60 seconds frequency, 15 buckets: 15 minutes retention time), a 300 seconds (10 minute) period could be used. However, it would also be possible to use 600 seconds (10 minutes) as it still falls within the probe's data retention time.
- The period must be set to a value smaller than the most frequently occurring probe if the probe buckets and lives are set to 1.

Configuring probes on Cisco devices

Probes may be set on the polled Cisco routers though the command line interface. However, certain guidelines apply to their creation in order to ensure polling result correctness.

There are two different ways to poll the IP-SLA probes on the Cisco devices. One can either choose to poll the statistics tables, located in the rttMonStats branch of the Cisco- RttMon-Mib mib or poll the last operation result tables, located in the

rttMonHistory and rttMonLatestOper mib branches. Both ways offer pros and cons which are as follows:

	Statistics Tables	Latest Operation Tables (HTTP / Jitter)	History Operation Table (other probes)
Polling period	Long: 5 minutes or more is OK.	Short: Must be as short as the most frequently occurring probe on the polled devices, otherwise there will be missing data points.	Long: 5 minutes or more is OK if multiple history lives and buckets are setup for the probe. This increases memory usage on the polled device. Short: Must be as short as the most frequently occurring probe on the polled devices, otherwise there will be missing data points. This is the case when history buckets and lives are set to 1 to reduce memory usage on the polled device.
Data volume	Low, since the polling period is longer.	High, since the polling period is shorter.	High or Low, depending upon the case.
Collecting host CPU utilization	Low	High	High or Low, depending upon the case.
Polled device CPU utilization	Low, might have a slightly noticeable effect on the device CPU utilization statistics.	High, will have a visible effect on the device CPU utilization statistics.	High or Low, depending upon the case.
Data granularity	Low: Averages are calculated on the polling period. Suitable for performance trending.	High. Suitable for troubleshooting specific problems, occurring at a precise time.	High. Suitable for troubleshooting specific problems, occurring at a precise time.

Guidelines to setting up probes polled via statistics tables

1. The owner must be set to a value. Any value is acceptable, as long as there is one. (i.e. John Smith, Sysadmin).
2. The tag must be set to a meaningful value. (IcmpEcho to www.google.com).
3. Leave the buckets-of-history-kept, distributions-of-statistics-kept, filter-for-history, hops-of-statisticskept, hours-of-statistics-kept, lives-of-history-kept, paths-of-statistics-kept, samples-of-history-kept, statistics-distribution-interval

and other parameters related to probe history/statistics to their **DEFAULT VALUE** when creating the probe on the Cisco device.

4. The probe frequency can be set to any number. However, keep in mind that this should be a reasonable value, such as 30, 60, 120, 240 or 300 seconds. Reports might seem a bit erratic if the probe frequency does not match the polling frequency: a “sawtooth” pattern may appear in the probe number of completed operations graph and packet metrics. This is normal but may be a bit alarming to a new user.
5. The probe's life must be set to “forever”, as they will be used for performance and trending purposes.

Guidelines to setting up probes polled via history operation table

1. These probes must have lives-of-history set to 1 or more (usually, 1 is enough).
2. These probes must have buckets-of-history-kept set to 1 or more (for a probe running every 30 second, on a device being polled every 5 minutes, this value should be greater than 10 to avoid losing any data).
3. These probes must have filter-for-history set to all (otherwise, no data will appear in the History table).

About probe creation and management

Since APG keeps historical data about every metric it receives, creating a new probe to replace a new one can be tricky as **probes are identified by their index number**. So, when a new probe is created in place of an old one, this new probe should be the same type as the one it replaces. To ensure this, probe management could be organized as follows:

Probe index range	Probe type
1 - 30	Jitter
30 - 60	HTTP
60 - 90	Other types, EXCEPT IpIcmpEcho, PathEcho, PathJitter
90 - 120	IpIcmpEcho
120 - 150	PathEcho (Not handed by this report pack).
150 - 180	PathJitter (Not handled by this report pack)

Note

Make sure the PathEcho and PathJitter (if used) probes are created at indexes higher than the last IpIcmpEcho probe. Doing otherwise will likely affect the polling of other probe types.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

- What to do if no data is collected on page 353
- What to do if some probes are missing from the inventory reports in the Cisco IPSLA: High Frequency Polling section on page 353
- What to do if no data appears for Jitter probes; Inventory data is displayed correctly and is up to date. on page 353
- What do when the information is not always up to date in the Probes Inventory on page 353
- Probes performance data is erratic on page 354
- Collector does not start after configuration files were edited on page 354

What to do if some probes are missing from the inventory reports in the Cisco IPSLA: High Frequency Polling section

Probes that are not setup to be polled via their latest operation table will not appear in this report. (their owner is not M&R).

What to do if no data is collected

Procedure

1. Make sure the snmp-agent is configured correctly (snmp version and community string).
2. Make sure the name attribute in snmp-polling-distribution.xml, <snmp-slave-poller> element, is the same as the one defined in slavesnmp- poller.xml file.
3. Make sure the polled agent supports CISCO SAA and that it's probes are running.

What to do if no data appears for Jitter probes; Inventory data is displayed correctly and is up to date.

The “ipsla monitor responder” or “rtr responder” may not be correctly set on the probe target device. This will cause the probe to fail. The rttMonJitterStatsError metric will increase in this case. No other data will be provided in the performance metrics, aside from error metrics.

The probe configuration may be incorrect: check for discrepancies when setting the source interface, port, target address and port.

What do when the information is not always up to date in the Probes Inventory

This may be due to the fact that some data is too old to be displayed in the table. Increasing the "**Time Threshold**" value in **Table** > **Value** > **Time Management** might solve this problem.

Probes performance data is erratic

This may be due to a buggy IOS implementation.

Known bugs include:

rttMonJitterStatsCompletions: counter increases while the operation was not successful (rttMonJitterStatsNumOfRTT does not increase). This affects the Success % calculated metric.

Collector does not start after configuration files were edited

Multiple causes are possible in this case. Check the logfiles, located in /APG-Backend/logs/collecting-*.log for details.

The most common errors are made when manually editing the config files. Make sure they are formed properly, with end tags, and that elements are in the right place in the structure.

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 271 provides a list of sample errors.

Temporary resolution
Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 272.

Permanent resolution
Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 272
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 274 2. Importing an SSL certificate into your truststore on page 273
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 273

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 274.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

  This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.

a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.

6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 273
  - Importing an SSL certificate in Firefox on page 273
  - Importing an SSL certificate in Internet Explorer on page 273

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** > **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** > **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** > **Options** > **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.

8. Share the resulting exported SSL certificate with other users to use.

CHAPTER 32

SolutionPack for Cisco Unified Communications Manager 3.0 Summary Sheet

- Overview 360
- Technical specifications 360
- Where to find the latest SolutionPack software 362
- Performing prerequisite configurations 362
- Configuring CUCM SP with Elastic Search 364
- Installing a SolutionPack 366
- Performing post-installation configuration tasks 366
- Configuring SNMP device discovery 373
- Import devices from Smarts 374
- Confirming report creation 375
- Troubleshooting 375
- Accessing event-processing log files 377
- Enable the Event Spy for debugging log file errors 377
- SSL certificates 377

Overview

Learn how to install and configure the SolutionPack for Cisco Unified Communication Manager.

This SolutionPack monitors communications for Cisco Unified Communications Manager (CUCM) as well as all of the gateways connected to the CUCM. The SolutionPack reports on voice quality, availability, and VoIP performance. It also provides status and metrics for service level measurement.

The reports in this SolutionPack cover the following objects:

- Gateway and CUCM health
- Gateway and CUCM inventory
- Calls overview, including number of calls, QoS, and MoS
- Phones, Route Patterns, IP trunks, and services
- Gateway statistics, such as utilization and availability
- Situations to watch, including reports for Call Manager availability, Gateway and IP trunk outage details, and calls with bad jitter, MOS, and high latency.

The SolutionPack provides the following features for administrators:

- Helps avoid the risk of VoIP service degradation or outages—Identifies and helps resolve issues.
- Measures voice quality—Establishes voice quality trends over time and helps troubleshoot VoIP calls for failures and quality deterioration.
- Helps optimize resources—Identifies usage and shows reductions or increases in capacity.
- Delivers real-time insight—Provides views into performance, both at a glance and in-depth.

Technical specifications

SolutionPack version
3.0

Compatible EMC M&R version
6.8u2 and later

Data collection methods
SNMP collector

XML collector

In addition, the billing server accesses call detail records (CDRs) and processes them using the Event Processor.

Supported devices
Cisco Unified Communications Manager (CUCM) 9.0 through 11.0. (CUCM 8.x is not supported.)

Note

The latest version of AXL API 11.0 does not support CUCM 8.x. Therefore, the VoIP domain manager and the SolutionPack for CUCM do not support CUCM 8.x. This Cisco website provides details: https://developer.cisco.com/site/axl/overview/versioning.

Cisco Universal Gateways AS5xxx Series

Main reports

Devices Health - All Devices

Includes health information for all gateway and call manager devices per cluster - drill down on a device for metrics such as CPU usage, average used memory, availability, interface usage and statistics.

Call Managers Inventory

Lists all call managers per cluster as well as their availability.

Calls Overview

Displays important information per cluster, including:

- Call duration
- Cause for disconnected calls
- Call quality (Qos and MoS)
- Call statistics

CUCM Reports

Call Manager reports include reports per cluster on services, cluster health, phones, route pattern, trunks, and media resources. Drill down on any device for more metrics and reports.

Note

A license report is supported for CUCM 6.0 to 9.0. this report is not supported for CUCM 10.0 to 11.0.

Gateway Reports

Gateway reports per cluster show gateway trunk utilization, trunk statistics, trunk availability, and so on.

Polled Metrics

Devices

Memory, CPU usage, Interface usage, Availability

IP Trunks

Calls Active, Video Calls Active, Calls Attempted, Calls Completed, In Port Number, Out Port Number

Call Managers

Registered Phones, Unregistered Phones, Rejected Phones, Availability, Heartbeat, Calls Rejected due to ICT and Generic Throttling, Registration Status, Signalling Status, Installed Services and their Status

Gateways

Signalling Status, Calls Completed, Calls Failures, Channel Status, ActiveConnections, Availability, Channels Count, Active Calls, Registration Status, Active Channels, Total Channels

Route Patterns

Orders, Endpoint, Port, RouteGroupList Enabled

Calls Overview

Duration, Type, QoS, MoS, Jitter, Latency, CalledParty, CallingParty, Pkid, DateTimeConnect

Phones

Type, Model, Registration Status

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Performing prerequisite configurations

Before installing the SolutionPack for Cisco Unified Communication Manager, perform these prerequisite tasks.

Install Cygwin (Windows servers)

This SolutionPack requires the Cynwin interface on Windows servers.

If the EMC M&R configuration uses a Windows server as the Collector host, that host must have Cygwin installed on it.

Procedure

1. Download Cygwin and install the software following instructions provided by the vendor.

Create CDR directory on the EMC M&R collector

Create the directory on the EMC M&R collector that will receive the information from the CUCM.

Procedure

1. Log onto the command line of the EMC M&R collector..
2. Create a folder to receive the FTP information from CUCM.

3. Change the ownership of the folder to **apg**.

   For example, `chown -R apg:apg <directory name>`

4. Provide read, write, and execute permissions to access that directory to a user or group that you will configure for FTP in the following procedure.

   For example, on a UNIX server, the result might be:

```
drwxr-xr-x  4 apg apg 77824 Nov  7 05:14 CDR
```

Configure CUCM access to CDR directory

Complete this procedure to configure the Cisco Call Manager device to FTP CDR and CMR data so that the SolutionPack for Cisco Unified Communication Manager can generate reports.

Before you begin

You need administrator access to Cisco Unified Communications Manager and Cisco Unified Serviceability.

Procedure

1. Log on to your Cisco Unified Communications Manager Administration page with Administrative privileges.
2. From the drop-down menu on the top of the window, select **Cisco Unified Serviceability**, and then click **Go**.
3. On the Service Parameter page, click **Tools** > **CDR Management**.
4. Click **Add new** and configure FTP communication between CUCM and the EMC M&R collector.

Field	Example
FTP Host/Destination This is the EMC M&R collector host.	`10.9.13.175`
User	Enter the ssh username of the EMC M&R collector host.
Password	Enter the ssh password for the EMC M&R collector host.
Protocol:	**SFTP**
Directory This is the specific directory on the EMC M&R collector host that holds the call data records.	Enter the EMC M&R collector `cdr` directory path . Make sure you set **apg** ownership for the `cdr` directory. UNIX path example: `/opt/APG/cdr/` Windows path example: `/cygdrive/c/APG/cdr/`
Resend on Failure	**TRUE**

5. Activate the service for Cisco CDR located at **Tools** > **Control Center Network Services**.

Perform additional prerequisite configurations

Perform these steps on all of the Cisco call managers and gateways that require polling.

Procedure

1. Enable SNMP on all Call Managers and Gateways that require polling.
2. Enable AXL for the Call Managers that require polling.

   Refer to the following Cisco website for information on this step and the next step:
   http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/devguide/9_1_1/axl.html#wp1054628

3. Obtain the CUCM DB schema version to be used with AXL requests.

   See the link cited in the previous step for information about the CUCM schema version.

4. Obtain the Username and Password to include in the AXL/SOAP requests

   This information will be used during SolutionPack installation. (Refer to the CUCM Administration Guide for credentials.)

Configuring CUCM SP with Elastic Search

Complete this procedure to configure CUCM Solution Pack with Elastic Search.

Before you begin

- Perform M&R 6.8u2 installation successfully.

Procedure

1. Navigate to `/opt/APG/bin/` directory.
2. Open the /etc/sysctl.conf file.
3. Add the following line:

   ```
   vm.max_map_count=262144
   ```

4. Open the /etc/security/limits.conf file.
5. Add the following line for the user:

   In this example, the user is apg.

   ```
   apg hard nofile 65536
   apg soft nofile 65536
   apg hard nproc 65536
   apg soft nproc 65536
   ```

6. Save the file.
7. To install the Elastic Search cluster package, invoke the following command:

   ```
   ./manage-modules.sh install elasticsearch-cluster
   ```

When you are prompted for the IP address, provide the M&R host IP address. In the **more entries** option, select **no** unless Elastic Search needs to be configured in the cluster mode.

8. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

Following is the output:

```
open files                      (-n) 65536
max user processes              (-u) 65536
```

9. In `/opt/APG/Databases/Elasticsearch/Default/conf/elasticsearch.yml` file, add the following entry:

```
bootstrap.seccomp: false
script.max_compilations_per_minute: 120
```

In `elasticsearch.yml` file, add the above line at the end.

10. Restart Elastic Search server.

Ensure that, Elastic Search server is running.

11. Create a resource for each newly added elastic search database. Perform this operation every time a new Elastic Search node is added to the environment to scale-out backends.

For example, to create a database resource:

In Linux:

```
./bin/manage-resources.sh create dba/ES-TF-VOIP '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://<Elastic
Search Server IP>:9200"],"prefix": "/cdr*"},"settings":
{"mapping": "ES-CISCO-CDR.xml"},"disabled": false }'
```

In Windows:

```
    APG PATH\bin\manage-resources.cmd create dba/ES-TF-VOIP
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
<Elastic Search Server IP>:9200"],"prefix": "/
cdr*"},"settings": {"mapping": "ES-CISCO-
CDR.xml"},"disabled": false }
```

Note

You need to specify the IP address for <Elastic Search Server>.

12. Restart the Tomcat service.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post-installation configuration tasks

After installing or upgrading the SolutionPack, you must configure call manager settings in order for discovery to work properly.

If upgrading from an earlier release, review post-upgrade configuration tasks described in this topic: Upgrading SolutionPack for CUCM components on page 368.

For new SolutionPack for CUCM installations, perform these post-installation configuration tasks:

- Configure the user process limits for a Linux installation on page 367

- Add the gateway and call manager details on page 367
- Migrating CUCM SolutionPack from Datastore to Elastic Search on page 371

When configuration is complete, continue with device discovery using either the SNMP discovery or the Import devices from Smarts procedures. Configuring SNMP device discovery on page 373 or Import devices from Smarts on page 374.

Configure the user process limits for a Linux installation

Increase the user process limits for the user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed.

Before you begin

Make sure you have:

- A login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, or SUSE Linux Enterprise Server (SLES) 11.
- The name specified for the user account during the installation.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add lines similar to the following for the user.

   In this example, the user is `apg`.

   ```
   apg hard nofile 65534
   apg soft nofile 65534
   apg hard nproc 65534
   apg soft nproc 65534
   ```

3. Save the file.
4. Type the following commands from the `bin` directory of the installation to restart the services:

   ```
   ./manage-modules.sh service stop all
   ./manage-modules.sh service start all
   ```

5. Type the following command to verify the changes:

   ```
   su apg -c 'ulimit -n -u'
   ```

Add the gateway and call manager details

Ensure the VoIP Gateway and Call Manager details are added so discovery can occur.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Navigate to **Discovery Center** under **Centralized Management**.
3. Click **Devices Management** and edit the **Device Types**.

4. Click **Call Manager Information** and enter the Call Manager details in the **Add a new device** fields.
5. Click **VoIP Gateway Information** and enter the VoIP Gateway details in the **Add a new device** fields.

Upgrading SolutionPack for CUCM components

After upgrading from EMC M&R 6.5u4, 6.6u1, or 6.7u1 to 6.8u2, you must perform these updates before discovery will work properly.

Procedure

1. Install the SNMP block for the SolutionPack for CUCM.

   Navigate to **Centralized Management** > **SolutionPack Center** to update the SNMP block. The *EMC Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides information on updating SolutionPack components.

   Note

   Once the CUCM SolutionPack is upgraded, warning message appears that can be ignored.

2. Before upgrading the SolutionPack for CUCM to the 2.1 version, ensure you export all CUCM AXL and SNMP configurations to a file with .csv format. Exporting Call Manager data before upgrading the SolutionPack for CUCM on page 368

   Call Managers are removed from Discovery Center in EMC M&R during the SolutionPack upgrade. If you export the Call Manager data before upgrading, you can add it back after the upgrade.

3. Add a new SNMP Collector (CiscoCUCMCollector). Adding the CiscoCUCMCollector on page 369.
4. Update the datastore that holds Call Manager data. Create the Elastic Search resource on page 370
5. If you exported Call Manager data before upgrading the SolutionPack for CUCM, import the modified .csv file. Importing Call Manager data after upgrading the SolutionPack for CUCM on page 370
6. If needed, you can manually update the Call Manager information for the devices. Adding Call Manager information for devices after an upgrade on page 371

Exporting Call Manager data before upgrading the SolutionPack for CUCM

Call Managers that were configured in EMC M&R prior to a SolutionPack upgrade are removed after the SolutionPack is updated in EMC M&R 6.7u1.

The Call Manager data in **Discovery Center** > **Devices Management**in EMC M&R is removed during the SolutionPack upgrade. You can export this data prior to performing the upgrade with this procedure.

Procedure

1. Navigate to **Discovery Center** > **Devices Management** > **Call Manager Information.**

2. Click the **Export** button to export all CUCM AXL and SNMP configurations to a file in .csv format.
3. Edit the .csv file to make it compatible with the new version of the SolutionPack for CUCM.
   a. Delete the columns named **snmpversion** and **communitystring**.
   b. Add a column named **publisher** to the right of the other columns in the .csv file. Populate this column with values (`true` or `false`) for each call manager depending upon whether the call manager is a publisher or not.

      If the Call Manager is a publisher, enter `true`; otherwise, enter `false`.

   Example of a modified .csv file

```
Server    Instance    name    host    cluster    username    password    version
publisher
itops-qa-198.lss.emc.com'    'cisco-voip-cucm'    'cucm11-01'    '10.9.11.71'
'StandAloneCluster'    'admin'
'{EC5CAACFC6E5A467BD1C933A61C8E0F1724FE6DE415202BD4BC00AC9E4A6940C7495C046EE9AC644A191
B327D176FA34}'    '11'    'true'
itops-qa-198.lss.emc.com'    'cisco-voip-cucm'    'nvla-cucm-303'    '10.9.18.190'
'nvla-cucm-303'    'admin'
'{882C7AD590E3F05B06A1954A2ED430FF163F36C417545681F07D0CB9ABBA4402790D78C775EB7BA6A964
8D7FBA065FA2}'    '10.5'    'false'
itops-qa-198.lss.emc.com'    'cisco-voip-cucm'    'cucm11-02'    '10.9.11.72'
'StandAloneCluster'    'admin'
'{E5D67C13A6511355E51C49DF731AD9357BC5300221E6B58F13C0D02CF674ADC81278F3C01440266D0BBA
F009826CFE24}'    '11'    'false'
```

4. Upgrade the SolutionPack for CUCM.
5. Import the revised .csv file back into the new SolutionPack for CUCM after the upgrade and post-upgrade configuration tasks are completed.

Adding the CiscoCUCMCollector

After an upgrade, you must add a new SNMP collector (CiscoCUCMCollector) in order to collect the CUCM data.

Procedure

1. Navigate to **Centralized Management** > **SolutionPack Center**.
2. Click **Collectors** > **New Collector**.
3. Add `CiscoCUCMCollector`.

   Do not use the Generic SNMP collector.
4. Navigate to `https://<MnR_Host>:58443/device-discovery/#/collectors`.
5. Click the new Collector and enter the CUCM port as `52006`.
6. Save the collector by selecting the other options.
7. Continue with device discovery using either the SNMP discovery or the Import devices from Smarts procedures. Configuring SNMP device discovery on page 373 or Import devices from Smarts on page 374.
8. In the SNMP device discovery section, for all Call Managers and Gateways, change the collector from `Watch4NetSnmpCollector-1` to `CiscoCUCMCollector`.

9. After changing the collector to `CiscoCUCMCollector`, trigger **Device Capability Discovery** and **Device Distribution**.

Note

If there are any issues with SNMP collection, restart `Collector-Manager::cisco-voip-cucm` and repeat step 9.

Create the Elastic Search resource

After an upgrade, you must create the ES-TF-VOIP resource.

Procedure

1. Issue the `manage-resources.sh` or `manage-resources.cmd` command from the installation `bin` folder to update the ES-TF-VOIP resource.

   For example, to create a database resource:

   In Linux:

```
 ./bin/manage-resources.sh create dba/ES-TF-VOIP '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://<Elastic
Search Server IP>:9200"],"prefix": "/cdr*"},"settings":
{"mapping": "ES-CISCO-CDR.xml"},"disabled": false }'
```

   In Windows:

```
APG PATH\bin\manage-resources.cmd create dba/ES-TF-VOIP
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
<Elastic Search Server IP>:9200"],"prefix": "/
cdr*"},"settings": {"mapping": "ES-CISCOCDR.
xml"},"disabled": false }
```

2. Restart the Tomcat service.

Importing Call Manager data after upgrading the SolutionPack for CUCM

Call Managers that were configured in EMC M&R prior to a SolutionPack upgrade are removed after the SolutionPack is updated in EMC M&R 6.7u1. If you exported the data prior to upgrading the SolutionPack, you can import it back into the SolutionPack for CUCM.

Procedure

1. Navigate to **Discovery Center** > **Devices Management** > **Call Manager Information.**
2. Click the **Import** button and browse to the .csv file which was modified to match the new SolutionPack for CUCM format.
3. Verify the import happens properly and save the configurations.

Adding Call Manager information for devices after an upgrade

After the upgrade, previously added call manager devices are removed. If you exported the information prior to the upgrade, you can import it back. But, if you need to manually edit the Call Manager details, use this procedure.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Navigate to **Discovery Center** under **Centralized Management**.
3. Click **Devices Management** and edit the **Device Types**.
4. Click **Call Manager Information** and enter the Call Manager details in the **Add a new device** fields.

Migrating CUCM SolutionPack from Datastore to Elastic Search

To migrate from previous database to the new database, you must perform the following steps:

Before you begin

- Install and configure previous M&R version. For example, install and configure 6.7u1.
- Configure 6.7u1 for Smarts SP CDR/CMR configurations. Verify CallOverview reports are present.
- Download the latest M&R build. The *Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides more information.
- Install the M&R, by invoking the following command:

```
setup-linux-x86_64-v95.sh
```

- To upgrade the platform, install the new packages in:

```
/opt/APG/Tools/Module-Repository [Y/n]? Y
/opt/APG/bin/manage-modules.sh update module-manager
/opt/APG/bin/manage-modules.sh service update all
/opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
```

- Configure the Elastic Search, see Configuring Elastic Search on page 59 for more information.
- Restart Elastic Search server. Ensure Elastic Search server is running.

Procedure

1. Update the CUCM package.
2. Update the CUCM versions from SolutionPacks.
3. Ensure that CDR Processing block in the CUCM SP is updated with the Elastic Search host IP address instead of the localhost.
4. Update the post install procedure.
5. Manually create the schema for the CDR database, you have to create the following **ES-TF-VOIP** resource for the tomcat server to enable the connection to the CDR database.

On Linux:

```
./bin/manage-resources.sh create dba/ES-TF-VOIP '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"],"prefix": "/cdr*"},"settings": {"mapping": "ES-CISCO-
CDR.xml"},"disabled": false }'
```

On Windows:

```
APG PATH\bin\manage-resources.cmd create dba/ES-TF-VOIP
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
localhost:9200"],"prefix": "/cdr*"},"settings": {"mapping":
"ES-CISCO-CDR.xml"},"disabled": false }'
```

6. Perform one of the following:
   - For migration from 6.6u1 or 6.7u1, delete the "dba/FLOW-TF-VOIP" table from manage-resources list.
   - For migration from 6.5u4, delete the resource link for FLOW-TF-VOIP from APG.xml and Server.xml.
7. Restart the Tomcat service.
8. Restart the Elastic Search server.
9. Stop the event processing manager service for cisco-voip-cucm.
10. Run the data-migration task which is enabled for run, see the Scheduling the Event-Processing Tasks on page 372 for more information.
11. Verify the Event Processing for cisco-cucm, CDR records are read and processed.
12. Ensure from Elastic Search, that data is flowing.

    URL to check the data in Elastic Search are:

    ```
    http://<Host IP of Elastic Search>:9200/_cat/indices
    http://<Host IP of Elastic Search>:9200/_template?pretty
    http://<Host IP of Elastic Search>:9200/cdr*/_search?pretty
    ---to get the total hits rows/records
    ```

13. Add new CDR records and verify new CallOverview reports are also fetched.

Scheduling the Event-Processing Tasks

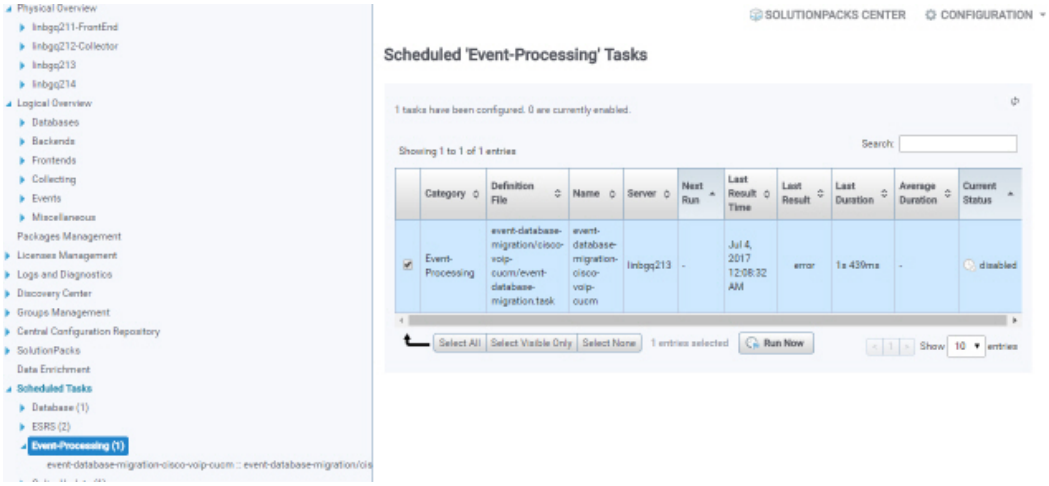
You need to configure the event processing task, in order to run the data-migration task which is enabled for run.

Procedure

1. On the EMC M&R Console, navigate to **Centralized Management** > **Scheduled Tasks** .
2. Click **Event-Processing**.

   The scheduled event-processing tasks appears in the right pane.
3. Select the event processing task.

Figure 9 Scheduled Event-Processing example



4. Click **Run Now**, to run the data-migration task which is enabled for run.

   Ensure from Elastic Search, that data is flowing.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

Ensure the CiscoCUCMCollector has been added. Use this collector instead of the Generic SNMP Collector.
Ensure the SNMP SolutionPack block available with SolutionPack for CUCM 2.1 has been installed.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.

   a. Type the main parameters and click **Save**.

   b. Under the **Seed File** tab, click **Upload new definition seed file**.

   c. Navigate to the seed file and click **Ok**.

   d. Click **Save.**
4. To manually add devices, click **Devices** > **New Device**.

   a. On the **New Device** window, click each tab and type the required information for the device.

   b. Click **Save** on each tab.

5. Select the device that you just added and click the **Approve** action, which is the checkmark.
6. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

   Green indicators appear on the **Dashboard** after successful executions of the above functions.

Import devices from Smarts

Use this procedure to import all devices from the INCHARGE-AM-PM or INCHARGE-AM servers or from all other domains running on a specified Smarts Broker.

Use either SNMP device discovery or the Import devices from Smarts procedure to import the devices.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.
3. To add Smarts source files, click **Device Source** > **New Smarts source**.
4. Specify the require information for Smarts device collection. For example:
   a. Enter the Source, Import Priority, and Action policies on the **Main Parameters** tab.
   b. Enter the Smarts configuration and Broker details on the **Smarts:Domain** tab.
   c. Select **Smarts:Capability** exclusions.
   d. Select **CiscoCUCMCollector** on the SNMP:Collectors tab.
5. Click `Save`.

   This saves the choices you just entered.
6. From the Dashboard, do the following steps:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

   Green indicators appear on the Dashboard after successful execution of these functions.
7. Verify that all Devices that were part of the Imported IP domain are respectively discovered as Call Managers, Gateways, Hosts, and so forth.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.

6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

Accessing event-processing log files

You can access the log file to view event processing of CDR/CMR files. By looking at this log you can check the number of records processed for CDR/CMR.

Procedure

1. On the EMC M&R collector host, log in with administrator privileges.
2. Navigate to the following path to view the log files:

```
/opt/APG/Event-Processing/Event-Processing-Manager/cisco-voip-
cucm/logs
```

Enable the Event Spy for debugging log file errors

Use the Event Spy to debug errors.

Procedure

1. Install the module, Event-Processing-Utils, with the SolutionPack for CUCM instance installed from the Centralized-Management page.
2. Edit the `processing.xml` file under `Event-Processing/Event-Processing-Manager/<CUCM_instance>/conf` to enable the Event Spy. Here is a sample `processing.xml` file that includes the EVENT-SPY entries:

```
  <!-- Debugging -->
<!-- Event spy for debugging purposes:
outputs events to log files. Install the event-processing-
utils
modules to use this. --> <processing-element name=" EVENT-SPY
" type="EventSpy"
config="Event-Processing-Utils/cisco-voip-cucm /conf"
/><processing-element enabled="true"
name="VOIP-ENRICHMENT"
config="Event-Property-Tagger/cisco-voip-cucm/conf/flow-
enrichment.xml"
data="DATASTORE-VOIP" /><processing-element enabled="true"
name="VOIP-ENRICHMENT"
config="Event-Property-Tagger/cisco-voip-cucm/conf/flow-
enrichment.xml"
data="DATASTORE-VOIP" /> <processing-element enabled="true"
name="CISCO-VOIP-COLLECTOR"
config="Cisco-VoIP-Collector/cisco-voip-cucm/conf/cisco-voip-
collector.xml"
data=" EVENT-SPY VOIP-ENRICHMENT" />
```

3. Restart the Event-Processing Manager.

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 271 provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 272.

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 272
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 274 2. Importing an SSL certificate into your truststore on page 273
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 273

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 274.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

  This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
   a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.
6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 273
  - Importing an SSL certificate in Firefox on page 273
  - Importing an SSL certificate in Internet Explorer on page 273

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** > **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** > **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.

4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** > **Options** > **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`

2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
8. Share the resulting exported SSL certificate with other users to use.

CHAPTER 33

SolutionPack for Cisco UCS 4.0 Summary Sheet

- Overview 384
- Technical specifications 384
- Configuring the UCS Manager 384
- Installing the SolutionPack 385

Overview

The SolutionPack for Cisco UCS generates reports that encompass compute, network, and storage access components of the unified fabric.

The SolutionPack generates uptime reports for the UCS Managers and enables you to see into the solution as managed by the unified management domain. In addition, the SolutionPack for Cisco UCS obtains real-time and historical data through various reports that indicate events and faults in the system.

Data collection methods
UCS XML API

Technical specifications

SolutionPack version
4.0

Compatible EMC M&R versions
6.7u1

Supported Cisco UCS versions

Table 24 Support for Cisco UCS

Supported Collection Interfaces	Prerequisites	Ports
Cisco UCS Manager 2.0 and higher Cisco UCS C-Series (CIMC) 1.4 and higher		80 443

Configuring the UCS Manager

Enable XML API for the Cisco UCS Manager.

Before you begin

Procedure

1. Log in to the Cisco UCS Manager web console.
2. Navigate to **Admin** > **Communication Management** > **Communication Services**.
3. Verify that the HTTP & CIM XML services are enabled.

   If the **Redirect HTTP to HTTPS** option is enabled, you will need to use secure communication when configuring your SolutionPack block.
4. If you want to use secure communications between the collector and the UCS Manager:
   - Choose the secure communication option when adding the UCS Manager.
   - Configure HTTPS on the **Communication Services** page of UCS Manager.

After you finish

EMC recommends that you create a new dedicated service account for SolutionPack integration. Role-read-only role is sufficient for the SolutionPack to work properly.

Installing the SolutionPack

Before you begin

Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. Type the instance name.
7. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
8. Click **Next**.

   The window displays pre-configured alert details.
9. From the **Alerting on data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, type information about the alerting configuration. In **Alerting Backend hostname or IP address**, specify the Primary Backend host.
10. Click **Next**.

    The window displays data collection details.
11. From the **Data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
12. From the **Frontend Web service** drop-down menu, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
13. Select the **Enable events collection** checkbox.
14. In the **Event server hostname or IP address** field, select the Backend host where the events server runs. The default port is 52007.

15. In the **Even server port number** field, enter a port number for events collection.
16. Select **Configure advanced settings** to configure polling settings.
17. Click **Next**.

    The window displays event settings.
18. Select an **Event database**. If you select **Add a new Events** database, type information for the new events database. Type the database information for the events database that runs on the Primary Backend host. The default **Database port** is 53306. The default **Event server port number** is 52007.
19. Click **Next**.

    The window displays reports settings.
20. In **Administration Web-Service Instance**, select an existing instance or create a custom instance.
21. Click **Install.**
22. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
23. Click **Discovery Center** > **Devices Management**.
24. Click **Cisco UCS**.
25. Click **Add new device**.
26. Specify the details of the Cisco UCS configuration.
    a. In the Device location section, select the server and instance where you want to store the configuration details for this device.
    b. In the **UCS type** field, select UCS Manager (Blade Chassis) or UCS C-Series (Server).
    c. In **Hostname or IP address** type the UCS management host.
    d. In the **Username** and **Password** fields, type the credentials for the management server.
    e. Select **Enable secure connection**, if desired.
    f. In the **Communication port** field, type the port number for the management server.
27. Click **Validate and Add** to validate the credentials.
28. Click **OK**.
29. Click **Save**.

After you finish

If you want to discover the Cisco UCS Fabric Interconnects in your environment via SNMP, you must install the Cisco MDS /Nexus SolutionPack in your environment to provide full SNMP masks and capabilities for the SNMP discovery.

Cisco UCS events are commented out by default in frontend configuration files. To enable Cisco UCS events, uncomment Cisco UCS events in the following configuration files: APG.xml, APG-WS.xml, and report-generation-config.xml.

Importing the new database schema

Before you begin

Starting with Watch4net 6.2u4, schema are preloaded. If you installed from an earlier version, import the new database schema.

Procedure

1. Load the events block file `Event-Processing/Generic-Live-Writer/cisco-ucs/ddl/my-ucs_live.sql`.
2. Run `mysql-client.sh` (`mysql-client.cmd` on Windows).
3. Type username, database name, and password.
4. Copy the contents of the `/my-ucs_live.sql` file and paste it into the mysql client at the `mysql>` prompt.

   This creates the `ucs_live` table.
5. Start the event processing manager service.
6. To enable events reporting from the frontend:
   a. Edit the Web-Application configuration file `Web-Servers/Tomcat/Default/conf/Catalina/localhost/APG.xml`.
   b. If the `cisco-ucs-events` section is present, uncomment it.
   c. If the `cisco-ucs-events` section is missing, add the following lines:

```
<!-- cisco-ucs-events -->
<ResourceLink name="jdbc/FLOW-UCS-LIVE:{ mapping=FLOW-
UCS.xml, table=ucs_live
 }" global="jdbc/FLOW-EVENTS" type="javax.sql.DataSource" />
```

7. Restart the tomcat service.

CHAPTER 34

SolutionPack for Cisco Wi-Fi Summary Sheet

- Overview 390
- Technical specifications 390
- Where to find the latest SolutionPack software 391
- Installing the SolutionPack 391
- Confirming report creation 392
- Troubleshooting 392

Overview

Learn how to install and configure the SolutionPack for Cisco Wi-Fi. This SolutionPack monitors and creates reports for the most common Cisco Wi-Fi Access Points. It reports on Controllers and Access Points that include inventory views, real-time performance views, and historical performance.

Technical specifications

SolutionPack version
2.0

Compatible EMC M&R versions
6.8u2 and later

Data collection method
SNMP collector

Supported MIBs
All CISCO Aironet Wi-Fi Access Points support these MIBs:

- CISCO-DOT11-IF-MIB.my
- CISCO-DOT11-QOS-MIB.my
- IEEE802dot11-MIB.my
- CISCO-AAA-SERVER-MIB.my
- CISCO-IETF-DOT11-QOS-MIB.my

Main reports
Total Number of Clients

Controller Summary:

- Number of Clients By Controller (over time)
- Cisco Wireless Association Statistics

Total Number of Clients

Controller Summary

Inventory:

- Access Point Distribution among Controllers
- Access Point Inventory by Controller
- Cisco Wireless Inventory

Performance Scorecard:

- Access Point Availability among Wi-Fi Controllers
- Cisco AAA (Authentication Authorization Accounting)
- Cisco Lightweight Wireless Access Point Performance
- Cisco Lightweight Wireless Access Point Controller performance (LWWAP)
- Cisco Wireless Access Point MAC Statistics
- Cisco Wireless Access Point QoS

- Users Currently Connected

Situations to Watch:

- Possible Misallocated Access Points (SNR vs. Number of Clients)
- Rogue Access Point

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing the SolutionPack

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Watch4net Installation and Configuration Guide* provides for more information.

Follow these steps to install the SolutionPack for Cisco Wi-Fi and perform Cisco device discovery.

Procedure

1. Log in to **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.
3. Select the **SolutionPack for Cisco Wi-Fi** in the **Browse and Install SolutionPacks** screen.
4. Read the summary information and click **Install**.
5. Select the **Administration Web-Service Instance** as the default and click **Next**.
6. In the **SNMP Masks** wizard, click **Install**.
7. Wait until the installation is complete for both SNMP Masks and Report and then click **OK.**
8. Under **Collecting**, click **Administration** > **Device Discovery**.
9. On the **Device Discovery** page, click **Collectors**.
10. Create a new collector by accepting all the default options.

11. Click **Device** and add the Cisco device to be discovered.
    a. Type the IP address, the SNMP community string, and assign the collector that you previously created.
    b. Select all Cisco capabilities to be discovered and any other capabilities.
12. Select the Cisco device that you just added and click **Approve.**
13. From the Dashboard:
    a. Click **Import devices from all enabled device sources**.
    b. Click **Discover capabilities from all approved devices**.
    c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
    d. Click **Send the generated configurations on all available collectors**.

    Green indicators appear on the Dashboard after successful executions of the above functions.

After you finish

After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration**.
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.

4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 35

SolutionPack for Juniper Firewall Summary Sheet

- Overview 396
- Technical specifications 396
- Where to find the latest SolutionPack software 397
- Installing a SolutionPack 397
- Configuring SNMP device discovery 398
- Confirming report creation 399
- Troubleshooting 399

Overview

Learn how to install and configure the SolutionPack for Juniper Firewall. This SolutionPack collects and interprets data across multiple Juniper ASA devices, and performs resource grouping and mathematical calculations to make performance information available.

The SolutionPack for Juniper Firewall provides unified monitoring of all Juniper firewall devices distributed in the network. In particular, it helps you to do the following:

- Verify session load and firewall failures.
- Verify firewall efficiency by monitoring packet rate and connections to demonstrate gains and fine-tune your device configuration for better results.
- Monitor Juniper Firewalls in real-time, pro-actively, to optimize service availability.
- Understand device activity, for example, which Juniper device opens the most firewall connections. You can also determine peak times for traffic and other metrics.

Technical specifications

SolutionPack version
2.0

Compatible EMC M&R versions
6.8u2 and later

Data collection method
SNMP collector

Supported MIBs
JUNIPER-SRX5000-SPU-MONITORING-MIB.mib

mib-jnx-chassis-alarm.txt

mib-jnx-chassis.txt

mib-jnx-js-idp.txt

SYSAPPL-MIB.mib

mib-jnx-chassis-fwdd.txt

mib-jnx-ipv6.txt

Supported devices
Juniper NetScreen Series (NS):

- NS-208
- NS-5xx Series
- NS-5200
- NS-5400

Juniper SSG Series:

- SSG5
- SSG140
- SSG320M

- SSG350M
- SSG520M
- SSG550M

Main reports

Session Failure %

Shows a Session Failure graph over a period of time for each polled firewall.

Firewall CPU Usage %

Reports on the CPU utilization for each polled firewall.

Firewall with Most Connections

Shows a Session Failure graph over a period of time for each polled firewall.

Firewall Summary

Provides summaries of the Availability %, CPU Usage %, Session Load %, and Number of Connections of firewall devices.

Inventory

Displays the inventory (count only) of the Juniper Firewall network.

Performance Scorecard

Reports on firewall hardware availability for memory, CPU, interface, units, disk, and power.

Situations to Watch

Displays critical and major interface errors, such as half open connections and session bottlenecks for each polled firewall.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.
- Make sure you know the name, IP address, SNMP port, and the community string of the firewall device.
- Verify the firewall is configured to allow network access to the SNMP port.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. For each list box you select, a screen appears.
   a. Click **Next** after you complete each screen.
   b. Click **Install** after you complete the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.

c. Click **Save**.

4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.

   a. Type the main parameters and click **Save**.

   b. Under the **Seed File** tab, click **Upload new definition seed file**.

   c. Navigate to the seed file and click **Ok**.

   d. Click **Save.**

5. To manually add devices, click **Devices** > **New Device**.

   a. On the **New Device** window, click each tab and type the required information for the device.

      On the **Main parameters** tab, make sure you specify `Firewall` for **Device Type**.

   b. Click **Save** on each tab.

6. Select the device that you just added and click the **Approve** action, which is the checkmark.

7. On the **Dashboard**, do the following:

   a. Click **Import devices from all enabled device sources**.

   b. Click **Discover capabilities from all approved devices**.

   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.

   d. Click **Send the generated configurations on all available collectors**.

      Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73

- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 36

SolutionPack for Juniper QoS Summary Sheet

- Overview 404
- Technical specifications 404
- Where to find the latest SolutionPack software 405
- Installing a SolutionPack 405
- Configuring SNMP device discovery 406
- Confirming report creation 407
- Troubleshooting 407

Overview

Learn how to install and configure the SolutionPack for Juniper QoS (Quality of Service). This SolutionPack monitors QoS-enabled Juniper devices to help you evaluate and improve the network performance of critical applications. You can analyze the network class of services by monitoring how the QoS configuration affects the pattern of network traffic through a Juniper router.

The SolutionPack for Juniper QoS helps you do the following:

- Verify whether dropped packets are due to random early detection dropping or to tail dropping.
- Verify QoS efficiency by monitoring transmitted packets.
- Monitor the Juniper routers in real time to better optimize the availability of services.
- Analyze the activities of each device to determine the busiest time intervals and to see which devices are dropping the most packets and at what time intervals.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIBs
JUNIPER-CHASIS-MIB.mib

JUNIPER-COS-MIB.mib

Supported devices
Any Juniper QoS-enabled router

Juniper J Series

Juniper EX Series

Juniper M Series

Juniper MX Series

Juniper T Series

Main reports
Generic Policy Traffic Reports

Situations to Watch

Traffic Shaping Reports

Match Statements Statistics

Police Action Statistics

Precedence WRED (Weighted Random Early Detection) Statistics

QoS Statistics

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.

d. Click **Send the generated configurations on all available collectors**.

Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.

3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*

5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 37

SolutionPack for Juniper RPM Summary Sheet

- Overview 412
- Technical specifications 412
- Where to find the latest SolutionPack software 412
- Installing a SolutionPack 413
- Configuring SNMP device discovery 413
- Confirming report creation 414
- Troubleshooting 415

Overview

Learn how to install and configure the SolutionPack for Juniper RPM (real-time performance monitoring). This SolutionPack provides unified monitoring of all probes running on routers and switches distributed across a network.

Technical specifications

SolutionPack version
2.0

Compatible EMC M&R versions
6.8u2 and later

Data collection method
SNMP collector

Supported MIBs
JUNIPER-PING-MIB.mib

JUNIPER-RPM-MIB.mib

JUNIPER-SMI.mib

Supported devices
Juniper EX3200 ethernet switches

Juniper EX4200 ethernet switches

Juniper J series services routers

Juniper M series multiservice edge routers

Juniper MX series 3D universal edge routers

Juniper T series core routers

Juniper SRX series services gateways

Main reports
RPM Probe Performance View by Device

RPM Probe Performance View by Probe Type

Situations to Watch

Latency (ICMP or UDP Echo)

High Latency Application Connect Time (TCP connect)

Reachability (ICMP ping)

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new

SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask

components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

      Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.

2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.

2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 38

SolutionPack for Microsoft Hyper-V 1.3.5 Summary Sheet

- Overview 418
- Technical specifications 418
- Configuring credentials for SolutionPack for Microsoft Hyper-V 419
- Requirements for data collection 419
- Installing the SolutionPack 419
- Using a test script to query WMI objects 420
- Configuring the UCS Manager 421

Overview

The SolutionPack for Microsoft Hyper-V generates real-time and historical reports so you understand Hyper-V performance through global and detailed status of Hyper-V hosts and underlying virtual machines.

Main reports

Inventory

Displays the inventory of devices, parts and metrics from Hypervisors and Virtual Machines

Virtual Disk Use Analysis

Tool to analyze the utilization profile of Virtual Hard Disk images

All Hosts | All Virtual Machines

Displays all available performance graphs for Hypervisors and Virtual Machines

Global Status

Shows the global status of all hosts and running virtual machines in the environment, detailed by component type

SLA Detailled View

Shows the current and forecasted SLA values for Hypervisors and Virtual Machines

Virtual Machines Running On Snapshot Disks

Shows all virtual machines running on snapshot disks. They impact disk performance and impact storage performance when it is time to commit changes on the original virtual disk.

Technical specifications

SolutionPack version
1.3.5

Compatible EMC M&R versions
6.7u1

Supported Microsoft Hyper-V versions

Table 25 Support for Microsoft Hyper-V

Supported Family/Models	Prerequisites	Ports
Hyper-V on Windows Server 2008 R2 Service Pack 1 or later Hyper-V Server 2008 Hyper-V Server 2008 or later Hyper-V on Windows 2012 R2	Requires PowerShell	

Note

This SolutionPack can only be installed on a Windows collector host.

Configuring credentials for SolutionPack for Microsoft Hyper-V

- Hyper-V Collector Manager must have the right to query WMI objects from Hyper-V hosts
- PowerShell must allow the execution of unassigned PowerShell scripts

Requirements for data collection

In order to collect data from Microsoft Hyper-V hosts, the environment needs to meet the following requirements:

- The Collect SolutionPack Block must be installed in a server using Windows Server 2008 R2 Service Pack 1 or later.
- The Collect SolutionPack Block must be able to query WMI objects in remote Microsoft Hyper-V hosts.
- The Collect SolutionPack Block machine must allow the execution of unsigned PowerShell scripts. To provide this capability, run the following command as an administrative user: `PowerShell -C Set-ExecutionPolicy Unrestricted`.

Installing the SolutionPack

Before you begin

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. Type the instance name.
7. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
8. Click **Next**.

   The window displays data collection details.
9. From the **Data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port

2020, which is the Collector host where the Load Balancer Connector is installed.

10. Click **Next**.

    The window displays reports settings.

11. In **Administration Web-Service Instance**, select an existing instance or create a custom instance.
12. Click **Install.**
13. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
14. Click **Discovery Center** > **Devices Management**.
15. Click Microsoft Hyper-V.
16. Click **Add new device**.
17. Select the server and collector instance where you want to store the configuration details for this device, and then enter the hostname or IP address of the host, supply the login credentials, and specify the appropriate configuration settings.

    Clicking the **Test** button results in a warning message that can be ignored.

18. Click **OK**.
19. Click **Save**.

Using a test script to query WMI objects

The Test feature located in the **Discovery Center** under the **Centralized Management** UI is not supported for the SolutionPack for Microsoft Hyper-V. Instead, use the test method presented in this topic.
The SolutionPack for Microsoft Hyper-V provides a script that can be used to check if is possible to query all required WMI objects using the provided user. The script is in the folder `<APG_FOLDER>/Collecting/XML-Collector/<SolutionPack_instance_name>/conf/`. You must execute the script from the Collect SolutionPack Block machine. Use the following syntax to run the script:

```
TestWMI.ps1 -Computer <ip-or-hostname>
          -Username <domain-or-machine\username>
          -Password <password> [-NoPing]
```

`-Computer`

Remote Hyper-V host IP address or hostname

`-Username`

Username used to perform remote WMI queries, in the format *DOMAIN\username* for domain users or *MACHINE\username* for local users

`-Password`

Password of the user specified with the `-Username` parameter

`-NoPing`

(optional) If the remote Hyper-V host is blocking ping requests, you must use this parameter to skip connectivity tests

Configuring the UCS Manager

Enable XML API for the Cisco UCS Manager.

Before you begin

Procedure

1. Log in to the Cisco UCS Manager web console.
2. Navigate to **Admin** > **Communication Management** > **Communication Services**.
3. Verify that the HTTP & CIM XML services are enabled.

   If the **Redirect HTTP to HTTPS** option is enabled, you will need to use secure communication when configuring your SolutionPack block.
4. If you want to use secure communications between the collector and the UCS Manager:
   - Choose the secure communication option when adding the UCS Manager.
   - Configure HTTPS on the **Communication Services** page of UCS Manager.

After you finish

EMC recommends that you create a new dedicated service account for SolutionPack integration. Role-read-only role is sufficient for the SolutionPack to work properly.

CHAPTER 39

SolutionPack for Microsoft SCOM Summary Sheet

- Overview 424
- Technical specifications 424
- Where to find the latest SolutionPack software 425
- Installing the SolutionPack 425
- Confirming report creation 426
- Troubleshooting 426

Overview

Learn how to install and configure the SolutionPack for Microsoft System Center Operation Manager (SCOM). This SolutionPack provides an integrated experience for the management of Microsoft Windows systems and the discovery of their workloads across platforms in the data center.

The SolutionPack for Microsoft SCOM helps you:

- Manage Windows servers and their performance
- Manage key performance indicators (KPIs)
- Manage application-related metrics
- Report on Microsoft applications and services, including Microsoft Operations Manager (MOM), server and agents, Active Directory, DNS, SQL, and Internet Information Services (IIS)
- Report on the main management packs of MOM
- Easily expand on new report sets per management pack

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u1 and later

Data collection method
SQL collector

Supported versions
System Center 2012 Operations Manager

System Center 2012 R2 Operations Manager

Supported Microsoft applications and services
Operations Manager

Server and agents

Active Directory

DNS

SQL 2012

IIS

User privilege requirements
An SQL or Windows user must have SELECT and CONNECT privileges on the SCOM Operations Manager Data Warehouse Database called OperationsManagerDW.

Main reports

Microsoft Products/Microsoft System Center

Displays the health (%) of the agents with an alert meter, data access and NT service statistics, and general information about the agents per management server

Microsoft Products/Microsoft Windows Operating System

Provides the OS distribution, top 10 processor consuming servers, and a complete list of servers.

Microsoft Products/Microsoft Active Directory

Provides the established TCP connections and the LDAP client sessions per server.

Microsoft Products/Microsoft SQL

Shows user connections per database and the databases with the lowest amount of free space.

Microsoft Products

Displays the product names, number of product instances, and the DNS and IIS data.

Managed Windows Server

Provides CPU usage %, free memory, and free page memory.

Per Operating System

Displays the server types and the number of servers.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing the SolutionPack

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC support website http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Watch4net Installation and Configuration Guide* provides for more information.

Procedure

1. Log in to **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.

3. Select the **SolutionPack for SCOM** in the **Browse and Install SolutionPacks** screen.
4. Read the summary information and click **Install**.

   You can select either Simple or Advanced as the configuration mode. Simple mode lets you select Windows authentication for database access. Advanced mode is typically for the user who is configuring the SQL server connection using the JDBC driver.
5. When you select `Simple` as the configuration mode for the OperationsManagerDW (SCOM Operations Manager Data Warehouse) database, set these values:
   - **Hostname or IP address of the database server**
   - **Database port**
   - **Instance name**
   - **Choose if you want to use Windows authentication**
   - **Username**
   - **Password**
6. When you select `Advanced` as the configuration mode for the OperationsManagerDW database, set these values:
   - **Connection string**
   - **Username**
   - **Password**

After you finish

After the installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- What to do when raw data continues to appear on reports on page 428
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

What to do when raw data continues to appear on reports

If the SQL collector continues to collect unprocessed data, which appears as zeros on reports, after three polling cycles, follow these instructions.

Procedure

1. Log in into the SQL server.
2. Execute the `SELECT MAX(vPR.DateTime) AS LatestDateTime FROM Perf.vPerfRaw AS vPR` query to display the last date and time in which data was written to the database.
3. If this is not a realtime value, check the Microsoft System Center Operation Manager for issues.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 40

SolutionPack for Microsoft SQL Server 4.0 Summary Sheet

- Overview 430
- Technical Specifications 430
- Where to find the latest SolutionPack software 431
- User privilege requirements for SolutionPack for Microsoft SQL 431
- Configuring the SolutionPack with an unprivileged account 432
- Installing the SolutionPack for Microsoft SQL 433
- Limitations for Microsoft SQL Server 434
- Troubleshooting 434

Overview

Learn how to install and configure the SolutionPack for Microsoft SQL Server. This SolutionPack provides the unified monitoring of Microsoft SQL databases using SQL queries targeted at servers.

The reports in the SolutionPack for Microsoft SQL Server give key information about status including:

- performance and availability of constituent databases
- datafile and logfile capacities
- performance metrics such IO, Wait, Memory pressure, and Host performance details
- End-to-End capacity reports (MS-SQL Server Application to LUN Detail)

Technical Specifications

SolutionPack version
4.0

Compatible EMC M&R versions
6.7u1

Supported Microsoft SQL versions
SQL Server 2008R2

SQL Server 2012

SQL Server 2014

Port
1433 (This is the default port on which the MS-SQL instance is running on the MS-SQL Server. It is configurable.)

Data collection method
SQL collector

SQL commands
This SolutionPack uses these commands:

- SELECT
- CONNECT
- INSERT
- CREATE TABLE
  - This creates temporary tables used when gathering the capacity-related information of databases. The temporary tables are created in the `tempdb` table. These tables are later dropped.
- EXEC
  - Executes a stored procedure that lists disks and their available free space.
- DROP
  - Removes temporary tables created earlier in the `tempdb` table.

Main reports

- Instance Sizes
- SQL Server Instances Overview
  - This includes reports for database sizes, database overview, and performance KPIs such as configuration parameters, IO, access methods, buffer manager, general statistics, and memory manager.
- Inventory of servers, instances, databases, and data/log files
- Situations to Watch
  - This includes index fragmentation, data/log files out of space, inactive devices and components, and actual and forecasted SLA values.
- SQL Server to SAN Inventory
  - Lists capacity reports per SQL Server instance

Table 26 End-to-end capacity use cases

Supported	Not supported
MS-SQL Server > FS > LUN	MS-SQL Server > VMDK
MS-SQL Server > RDM	MS-SQL > FS using VPLEX

Support for Host Details report

- Host Details report supports virtual machines.
- Host Details report does not support physical hosts.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

User privilege requirements for SolutionPack for Microsoft SQL

The Microsoft SQL Server can be discovered with SQL Authentication or Windows Authentication.

Microsoft SQL authentication

SQL authentication works for users having either SYSADMIN privileges or an unprivileged account.

Note

An unprivileged account can be created and used to discover the Microsoft SQL Server. Configuring the SolutionPack with an unprivileged account on page 432

Windows authentication

A Windows user account must be imported into the Microsoft SQL Server with settings similar to these:

- Server role of **Public**
- Securable grants for **Connect SQL**, **View any definitions**, and **View server state**

Configuring the SolutionPack with an unprivileged account

Create a `watch4net` account with specific grants required by the Microsoft SQL SolutionPack collector.

The collector must connect to each instance of MS-SQL Server and perform SQL queries. You can use either an administrator equivalent system account or create a dedicated system account for the collector. If you want a dedicated system account, please ask the DBA administrator to create a `watch4net` account with specific grants for the collector.

Procedure

1. Follow this example to create a `watch4net` account.

   The default database must be used as the *[master]* database in this procedure.

```
USE [master]
GO

CREATE LOGIN [watch4net]
WITH PASSWORD=N'<securepassword> ',
DEFAULT_DATABASE=[master],
DEFAULT_LANGUAGE=[us_english],
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF
GO

EXECUTE master.sys.sp_MSforeachdb
'USE [?];
CREATE USER watch4net FOR LOGIN watch4net
GO

GRANT VIEW SERVER STATE TO watch4net
GO

GRANT VIEW ANY DEFINITION TO watch4net
GO
;
```

Results

Your dedicated account is configured.

Installing the SolutionPack for Microsoft SQL

Before you begin

- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. The installation guide for your product provides more information.
- Ensure you create a `watch4net` user prior to installing the SolutionPack. You may need this to ensure correct credentials are added to Microsoft SQL Server Devices Management during the installation process.

Procedure

1. Log in to your product and click **Administration** > **Centralized Management**.
2. Click **SolutionPacks** and select **SOLUTIONPACK CENTER**.
3. Select the **SolutionPack for Microsoft SQL Server** in the **Browse and Install SolutionPacks** window.
4. Read the summary information and click **Install**.
5. Type the instance name.
6. Assign a server for each of the components.
7. Click **Next**.

   The window displays pre-configured alerts details.
8. From the **Pre-Configured Alerts** drop-down menu, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
9. Click **Next**.

   The window displays the data collection details.
10. Make a selection in the **Data Collection** drop-down menu.

    Select existing settings that have been specified for other components or select **Add a new data collection**.
11. If you select **Add a new Data collection**, type information about the data collection. In the **Hostname or IP address to send data** field, use `localhost` on default port 2020.

    This is the Collector host where the Load Balancer Connector is installed.
12. Select the **Frontend Web Service** option.

    Select existing settings that have been specified or choose **Add a new Frontend Web Service**.
13. If you select **Configure Collector advanced settings**, you have the option to select different polling periods.

    The default polling period is 15 minutes. Consult with your database administrator to set the polling period based on the number of SQL Server instances that are being polled by this collector manager instance. For example, you have the option to select 5 minutes, 15 minutes, 30 minutes, or one hour.
14. Click **Next**.
15. If you select **Add a new Web-Service Gateway**, type information about the web-service gateway.

16. In the **Administration Web-Service instance**, select an existing instance or create a custom instance.
17. Click **Install**.
18. Click **OK**.

    Monitor the installation logs to ensure that the installation completes successfully.

19. Click **Discovery Center** > **Device Management**.
20. Click **Microsoft SQL Server**.
21. Click **Add new device**.

    Note

    Threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **MS-SQL Alert definition**.

22. Select the server and collector instance where you want to store the configuration details for this device.
23. Set these values:
    - Enter the Hostname or IP address of the SQL server.
    - Specify the **Database Port** and **Database Instance** name. For example, type `Default` for the SQL Server Instance name or type the named instance.
    - Specify the mode of authentication used for the SQL Server: **SQL Authentication** or **Windows Authentication**
    - If using SQL Server authentication, type the username and password for the SQL Server.
    - If using Windows authentication, provide the Windows domain, username, and password. Use either the local or domain username.
24. Click **Validate and Add** to check connectivity with the SQL Server.
25. Click **OK**.
26. Click **Save**.

Limitations for Microsoft SQL Server

If there are connection problems, find out whether SSL (Secure Socket Layer) is enabled.

Microsoft SQL Server is unable to connect to a Microsoft SQL Server that has SSL enabled. This is due to the inherent limitation of the OpenSource JTDS driver used to connect to the SQL Server.

Troubleshooting

Report display problems

- What to do if data does not appear in reports on page 435
- Running a scheduled task to import data into reports on page 73

- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in reports

Procedure

1. Do the following to check the Collector Manager logs:
   a. View `/opt/APG/Collecting/Collector-Manager/microsoft-sqlserver/logs/collecting-0-0.log`.
   b. Verify that the last message in the log states that a certain number of raw values were collected using nine SQL queries. This message indicates the collector is working.

      For example: `<instance_master> collect done: 2,735 new raw values collected in 0 seconds 527 ms using 9 SQL queries`
   c. Check for any Java exceptions and warning messages.
2. If collector errors exist, do the following:
   a. Ping the Microsoft SQL Server using the fully qualified domain name (FQDN).
   b. Replace the current user, which is the username and password set during SolutionPack installation to retrieve data from the Microsoft SQL sever, with a user with SYSADMIN rights.
   c. Use telnet to check if the Microsoft SQL port is accessible from the SQL collector server.
   d. Reconfigure the SolutionPack by navigating to **Centralized Management** > **SolutionPacks** > **Microsoft SQL Server**.
   e. Under **SolutionPackBlock**, click the pencil next to **Collector** to reconfigure the settings.
   f. To edit advanced connection settings, you may need to manually edit the SQL collector configuration file.
3. If no errors exist and the last message in the log indicates that nine queries were executed, do the following:
   a. Wait a minimum of three polling cycles. By default, one polling cycle is fifteen minutes.
   b. Navigate to **Centralized Management** > **Scheduled Tasks**.
   c. Under the **Backend** category, run `backend/Default/import_variable_status.task`.
   d. Refresh the reports after fifteen minutes.
4. Make sure the **Frontend** is attached to the database used by the SQL collector.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 41

SolutionPack for MPLS Summary Sheet

- Overview 438
- Technical specifications 438
- Where to find the latest SolutionPack software 439
- Installing a SolutionPack 439
- Configuring SNMP device discovery 440
- Confirming report creation 441

Overview

Learn how to install and configure the SolutionPack for SolutionPack for MPLS (Multiprotocol Label Switching). This SolutionPack provides visibility into MPLS virtual private networks (VPNs). It analyzes how MPLS VPNs are configured and utilized, from both a real-time and historical perspective.

EMC M&R polls MPLS devices and interfaces and VRF (virtual routing and forwarding) data to show device and tunnel performance, hot-spot problems, top ten volumes, and MPLS inventory.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIBs
MPLS-LSR-MIB

MPLS-VPN-MIB

Supported devices
This SolutionPack can collect data from any device that supports these MIBs:

MPLS-LSR-MIB

MPLS-VPN-MIB

Main reports

MPLS Performance by VRF and Interface

Provides insight into major MPLS interface metrics, including volume, labels, discards, fragments, and VRF metrics, such as VRF availability and number of routes.

MPLS Inventory by VRF and Interface

Provides an inventory of the MPLS interfaces and VRFs with their corresponding metrics and their values.

Total Routes Added and Used

Provides an overview of the added routes per VRF and labels used per MPLS interface, in the form of a stacked chart.

TopN reports on Labels, Fragments and Discards

Provides values for Labels, Fragments and Discards of each MPLS interface.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.
8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.

d. Click **Send the generated configurations on all available collectors**.

Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 42

SolutionPack for OpenStack Summary Sheet

- Overview 444
- Technical Specification 444
- Where to find the latest SolutionPack software 445
- Installing a SolutionPack 445
- Performing post-installation configuration tasks 446
- SSL certificates 446

Overview

Learn how to install and configure the SolutionPack for OpenStack.

The SolutionPack for OpenStack provides comprehensive reporting of OpenStack inventory, performance and capacity. It provides historical trending as well as projections based on simulated data.

The reports in this SolutionPack cover the following objects:

- Inventory of all compute nodes and instances
- Performance analysis
- Capacity trending and projections
- Operational alerts

The SolutionPack provides the following features for administrators:

- Helps optimize resources- Identifies usage and shows reductions or increases in capacity.
- Delivers real-time insight- Provides views into performance, both at a glance and in-depth.

Technical Specification

SolutionPack version
2.0

Compatible EMC M&R version
6.8u2 and later

Data collection methods
Stream collector

Supported devices
OpenStack Kilo and Mitaka.

Main reports

Inventory
: Includes the lists of all compute nodes, instances and storage volume.

Alerts
: Active and Historical alerts reporting.

Capacity Dashboard
: Capacity trending and projections.

Health Dashboard
: Includes health reports of resources.

Overview
: An overview of resource utilization and stress.

Project Dashboard
: Project level information.

Polled Metrics

Devices

Memory, CPU usage, Disk usage, Interface usage, Availability

Storage

Volume capacity.

Network

IP subnets, Routers, interfaces.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack for EMC Smarts license before the trial period ends. There is no separate license for SolutionPack for OpenStack.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try SolutionPack for OpenStack , you must request a license for SolutionPack for EMC Smarts by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.

b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.

c. Click **Next**.

8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Performing post-installation configuration tasks

For new SolutionPack for OpenStack installations, perform the following post-installation configuration task:

- Add the OpenStack server details on page 446

Add the OpenStack server details

Ensure the OpenStack server details are added so discovery can occur.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Navigate to **Discovery Center** under **Centralized Management**.
3. Click **Inventory Management** > **Open Stack**.
4. Click **Add...** and enter the OpenStack server details in the **Add new OpenStack** fields.
5. Click **Validate** and **Add** once done.
6. Click **Save**, to save new device configuration.

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

SSL certificate error examples on page 271 provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: Troubleshooting an SSL certificate error: Accepting the exception on page 272.

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 272
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 274 2. Importing an SSL certificate into your truststore on page 273
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 273

If you need to prepare an SSL certificate to share with other users, use: Exporting an SSL certificate from an Internet Explorer browser on page 274.

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

```
This site's security certificate is not trusted!
```

Or, a blank pane.

Firefox error example

```
This Connection is Untrusted
```

Internet Explorer error examples

```
There is a problem with this website's security certificate.
```

```
Content was blocked because it was not signed by a valid security
certificate.
```

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- Accept the exception.

  Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
   a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.
6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- Import the certificate using one of the following procedures:
  - Importing an SSL certificate in Chrome on page 273
  - Importing an SSL certificate in Firefox on page 273
  - Importing an SSL certificate in Internet Explorer on page 273

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings** > **Show advanced settings**.
2. Scroll down and select **HTTP/SSL** > **Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox** > **Options** > **Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.
4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.

   For example: `https://<myHostname>.emc.com`

2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.

4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
   a. Click **Next** in the **Welcome** screen.
   b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
   c. Browse to the location where you want to save the certificate.
   d. Specify the certificate file name and click **Save**.
   e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.
   f. Click **Finish**.
   g. Click **OK** when `The export was successful` appears.
7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
8. Share the resulting exported SSL certificate with other users to use.

CHAPTER 43

SolutionPack for Oracle Database 4.0 Summary Sheet

- Overview 452
- Technical specifications 452
- Installing the SolutionPack 453
- Configuring the SolutionPack with an unprivileged account 455
- Limitations 456
- Confirming report creation 456

Overview

Learn how to install and configure the SolutionPack for Oracle Database. The SolutionPack for Oracle Database monitors the status and performance of an Oracle database. The SolutionPack gives visibility into listeners, tablespaces, versions, connections, commits and rollbacks. You can survey the Oracle core process, such as the SGA, and verify the hit ratio about cache, dictionary cache, latch cache, library cache, sort and sessions.

Figure 10 SolutionPack for Oracle Database

Technical specifications

Table 27 Support for Oracle Database

Supported Family/ Models	Collectors	Prerequisites	Ports
Oracle 10 and later	SQL-Collector	The appropriate JDBC driver jar file needs to be in the …/`APG/Databases/JDBC-Drivers/Default/lib` folder. ORACLE database user credentials are required.	1521 TCP

Notes

- Work with your DBA to determine the appropriate JDBC driver based on the installed version of Oracle. Download the JDBC driver from: `www.oracle.com/technetwork/database/features/jdbc`.
- The SolutionPack for Oracle Database was tested with ojdbc5.jar and ojdbc7.jar on Oracle 12g versions.

Main reports

- Entire Oracle database infrastructure summary
- Detailed database size
- Oracle RAC view
- Instances availability
- Cross-server KPIs

Installing the SolutionPack

Before you begin

- The core modules must be up-to-date on all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The appropriate JDBC driver jar file must be in the `.../APG/Databases/JDBC-Drivers/Default/lib` folder. Refer to the support matrix for additional details.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. Type the instance name.
7. Assign a server for each of the components. For Oracle ASM deployments, specify the server where the system will install ASM Data Collection. For additional details about the ASM script and configuring ASM, refer to the SolutionPack for Oracle Database section of the support matrix.
8. Click **Next**.

   The window displays pre-configured alerts details.
9. From the **Pre-Configured Alerts** drop-down menu, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
10. Click **Next**.

    The window displays data collection details.
11. From the **Data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

12. Leave **Activate the FailOver-Filter** checked.
13. From the **Web-Service Gateway** drop-down menu, select existing settings that have been specified for other components, or select **Add a new Web-Service Gateway**.

    If you select **Add a new Web-Service Gateway**, type information about the web-service gateway.
14. The Topology Service automatically includes the standard settings. You should only add a new Topology Service if your Topology Mapping service is installed in a non-default location.
15. If you select **Configure collector advance settings**, you have the option of selecting from polling periods of 5 minutes, 15 minutes, 30 minutes, and 1 hour. The default polling period is set to 15 minutes. Consult with your database administrator to set the polling period based on the number of Oracle Database instances that are being polled by this particular instance of the collector manager.
16. Click **Next**.

    The window displays reports settings.
17. In **Administration Web-Service Instance**, select an existing instance or create a custom instance.
18. Click **Next**.

    The windows displays ASM Data Collection settings.
19. Specify the default collection level for ASM Data Collection. In this case, the default option is Standard.
20. Click **Install.**
21. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
22. Click **Discovery Center** > **Devices Management**.
23. Click **Add new device**.

    Note

    Threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **Oracle Alert Definitions**.
24. Click **Oracle Database**.
25. Select the server and collector instance where you want to store the configuration details for this device, and then enter the hostname or IP address of the host, supply the login credentials, and specify the appropriate configuration settings.

    EMC recommends adding a watch4net user beforehand so that the correct credentials are added to Oracle Database Devices Management. For details about the required grants, refer to Configuring the SolutionPack with an unprivileged account.

    For each Oracle Database instance being polled, it is useful to have the following information on hand before it is added to the Collection devices list:

    - Oracle service name

- Oracle instance name (in case of a RAC setup)
- Username (watch4net user)
- Password
- Port
- Server details (Windows, Linux, or Solaris)
- Server details (Physical or VM)
- Oracle setup (ASM or non ASM)
- Oracle setup (RAC or non RAC)
- Oracle version
- RAC version (if installed)

26. Click **Validate and Add** to validate the credentials.
27. Click **OK**.
28. Click **Save**.

Configuring the SolutionPack with an unprivileged account

The collector must connect to each instance of Oracle databases and perform SQL queries. You can use either an administrator equivalent system account or create a dedicated system account for the collector. If you want to create a dedicated system account, ask the DBA administrator to run the following query against every instances/RAC cluster. This will create a `watch4net` account with specific grants for the collector.

Procedure

1. Create the watch4net user:

```
create user watch4net identified by <securepassword> default
tablespace users temporary tablespace temp;
```

2. Grant the necessary privileges to the watch4net user by running the following grants:

```
grant create session to watch4net;
grant select on dba_data_files to watch4net;
grant select on dba_free_space to watch4net;
grant select on dba_libraries to watch4net;
grant select on dba_objects to watch4net;
grant select on dba_segments to watch4net;
grant select on dba_tablespaces to watch4net;
grant select on gv_$sysmetric to watch4net;
grant select on v_$asm_disk to watch4net;
grant select on v_$asm_diskgroup to watch4net;
grant select on v_$asm_diskgroup_stat to watch4net;
grant select on v_$asm_disk_stat to watch4net;
grant select on v_$database to watch4net;
grant select on v_$dispatcher to watch4net;
grant select on v_$filestat to watch4net;
grant select on v_$instance to watch4net;
grant select on V_$instance_recovery to watch4net;
grant select on v_$latch to watch4net;
grant select on v_$librarycache to watch4net;
```

```
grant select on V_$LOCK to watch4net;
grant select on v_$locked_object to watch4net;
grant select on v_$lock_type to watch4net;
grant select on v_$log to watch4net;
grant select on v_$logfile to watch4net;
grant select on v_$parameter to watch4net;
grant select on V_$PGASTAT to watch4net;
grant select on v_$rollstat to watch4net;
grant select on v_$rowcache to watch4net;
grant select on v_$session to watch4net;
grant select on v_$sesstat to watch4net;
grant select on v_$sess_io to watch4net;
grant select on v_$sgainfo to watch4net;
grant select on v_$statname to watch4net;
grant select on v_$sysmetric to watch4net;
grant select on V_$SYSSTAT to watch4net;
grant select on V_$SYSTEM_event to watch4net;
grant select on v_$system_wait_class to watch4net;
grant select on V_$version to watch4net;
```

Results

Your dedicated account is configured.

Limitations

- On a Windows server, the `ASMDiskDetection.ps1` script must be run using an account that belongs to the 'Administrators' group. With non-admin discovery on Windows, reports such as ASM Datafile Distribution and ASM Disks (under Database Summary) will not work.
- Discovery Center **Test** button fails with the following error: `Cannot locate driver 'oracle.jdbc.driver.OracleDriver' !`
  1. After installing the SolutionPack, put the Oracle driver (ojdbc jar) in the following directory: `/opt/APG/Databases/JDBC-Drivers/Default/lib`
  2. Restart the script Engine.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 44

SolutionPack for Oracle MySQL Database 4.0 Summary Sheet

- Overview 458
- Technical Specifications 458
- Where to find the latest SolutionPack software 458
- Preparing MySQL database for discovery and data collection 459
- Installing the SolutionPack 459
- Limitations 460
- Confirming report creation 460
- Troubleshooting 460

Overview

Learn how to install and configure the SolutionPack for Oracle MySQL Database. This SolutionPack provides management capabilities typically found in database-centric tools along with management support from other technologies. You can measure client activity by reporting on data from your database tier alongside your business logic and presentation tiers.

Technical Specifications

SolutionPack version
4.0

Compatible EMC M&R versions
6.7u1

Supported Oracle MySQL versions
MySQL 5.1

MySQL 5.5

MySQL 5.6

Ports
Port 3306 using TCP

User privilege requirements
This SolutionPack requires MySQL database user login privileges to collect information from MySQL database servers running remotely.

Data collection method
The Oracle MySQL SolutionPack's sql-collector queries the information_schema.GLOBAL_STATUS table and the information_schema.SESSION_VARIABLES table.

Main reports
Query Cache Volume among all MySQL Databases

Number of SQL queries among all MySQL Databases

Total Current Connection

Database Health and Performance

Connection Health

Memory Health

Slave's Health

Database Performance

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Preparing MySQL database for discovery and data collection

Before installation you need to prepare the MySQL Databases to be discovered.

The following procedure describes how to create an unprivileged account to be use by the SolutionPack.

Procedure

1. Identify the Collector IP or FQDN.
2. Connect to one of the MySQL databases and get and generate a non-plain text password using the command below:

   ```
   SELECT PASSWORD('mypass');
   ```

3. Take the result string (for example: *6C8989366EAF75BB670AD8EA7A7FC1176A95CEF4) and grant the privileges on each of your databases as shown in the example below:

   ```
   CREATE USER 'watch4net'@'%'IDENTIFIED BY PASSWORD
   *6C8989366EAF75BB670AD8EA7A7FC1176A95CEF4;
   GRANT ALL ON *.* TO 'watch4net'@'%';
   ```

Installing the SolutionPack

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* provides for more information.

Procedure

1. Log in to **Centralized Management**.
2. Select **SOLUTIONPACK CENTER**.
3. Select the **SolutionPack for MySQL Database** in the **Browse and Install SolutionPacks** screen.
4. Read the summary information and click **Install**.
5. Edit the default instance name, `oracle-mysql-database`, and click **Next**.

6. Select **Administration Web-Service Instance** as the default and click **Install**.
7. When a checkmark appears next to the Collector and the Report, click **OK.**

   Monitor the installation logs to ensure that the installation completes successfully.
8. Click **Discovery Center** > **Devices Management**.
9. Click Oracle MySQL Database.
10. Click **Add new device**.
11. Select the server and collector instance where you want to store the configuration details for this device.
12. Set the following values:
    - Enter the Hostname or IP address of the MySQL server.
    - Specify the Database Port.
    - Provide the username and password.
13. Click **Validate and Add** to validate the credentials.
14. Click **OK**.
15. Click **Save**.
16. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Limitations

- During the Collector block installation, the service will not come up and there will be Severe error in the collector log. However, after adding MySQL devices, the collector will be in the running state.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 461
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports.
2. On the **Device Discovery Dashboard**, verify that all icons are green.
3. To view the log files for errors, go to **Centralized Management** and click **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. Log in to your MySQL database and verify data is being written to the MySQL database server. Look specifically at the `data_property`, `data_variable`, and all cache tables:

```
select * from data_property;
select * from data_variable;
select * from <cache-table-name>;
```

5. In the MySQL database, verify the user has the required login permissions to the local and remote MySQL servers being monitored by the SolutionPack. If not, follow these steps to create credentials for the user:
   a. Navigate to `bin/mysql/ -u root -p <rootUserPassword> -P <mysqlServerPort>`
   b. Type the following commands to create the credentials:

```
use mysql;
CREATE USER 'testuser'@'%'IDENTIFIED BY 'watch4net';
GRANT ALL ON *.* TO 'testuser'@'%';
```

   c. Use these user credentials to log in to the local and remote MySQL database servers from the SolutionPack.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.

7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the Oracle MySQL database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Go to the **Administration** page.
2. Under **Modules**, click **Management of Database Modules**.
3. On the **Metric Selection** page, create the filter.

   For example, to list the `key_reads` (the number of physical reads of a key block from disk to the MyISAM cache), type **`source=='MySQL-Collector' &&name=='key_reads'`** in the **Filter** field.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 45

SolutionPack for Riverbed SteelHead Summary Sheet

- Overview 464
- Technical specifications 464
- Where to find the latest SolutionPack software 465
- Installing a SolutionPack 465
- Configuring SNMP device discovery 466
- Confirming report creation 467

Overview

Learn how to install and configure the SolutionPack for Riverbed SteelHead. This SolutionPack provides unified monitoring of all Riverbed SteelHead appliances distributed in a network.

The SolutionPack for Riverbed SteelHead helps you do the following:

- Verify the efficiency of traffic reduction. You can demonstrate gains and fine-tune your device configuration for better results.
- Monitor the Riverbed SteelHead appliances in real-time to optimize the availability of services.
- Understand your WAN traffic. You can see which applications are using the most bandwidth and their peak utilization time period.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.5u1 and later

Data collection method
SNMP collector

Supported MIBs
steelhead_mib_653.mib

rbt_mib_708.mib

Supported devices
Riverbed SteelHead appliances 250

Riverbed SteelHead appliances 550

Riverbed SteelHead appliances 1050

Riverbed SteelHead appliances 2050

Main reports

SteelHead Appliances Summary

Shows the Riverbed SteelHead utilization, such as the processor load, the availability over a selected time period, and the traffic compression rate per device. When you drill down to a specific appliance, you see CPU utilization %, CPU load, bandwidth passthrough, outgoing traffic reduction, incoming traffic decompression, storage and memory utilization, and detailed connection information.

SteelHead With Most Connections

Displays the appliances with the most connections.

SteelHead Saving Most Traffic (KBytes/sec)

Displays the appliances that save the most WAN traffic.

Performance Scorecard

Provides a summary of appliances showing compression rate (KBytes/sec), no compression (overhead traffic), and SteelHead datastore hits %.

SteelHead Traffic Reports

Reports on SteelHead traffic (KBytes/sec), application traffic (KBytes/sec), bandwidth passthrough (KBytes/sec), and SteelHead WAN links usage %.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *EMC M&R (Watch4net) Installation and Configuration Guide* for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Data collection** and **Reports** list boxes.
   c. Click **Next**.

8. Complete the wizards screens and click **Install** on the last screen.

   The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

   When the installation successfully completes, green checkmarks appear.

10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.

3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.

   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.

7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

      Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 46

SolutionPack for Traffic Flows 4.0 Summary Sheet

- Overview 470
- Technical specifications 470
- Where to find the latest SolutionPack software 470
- Configuring Elastic Search 470
- Installing the SolutionPack for Traffic Flows 472
- Post installation tasks 476
- Upgrading Traffic Flows SolutionPack from 6.5u4 and 6.6u1 to 6.8u2 479
- Upgrading Traffic Flows SolutionPack from 6.7u1 to 6.8u2 480
- Migrating Traffic Flows SolutionPack from Datastore to Elastic Search 481
- Troubleshooting 482
- What to do if parsing errors related to resource link updating occur 484

Overview

Learn how to install and configure the SolutionPack for Traffic Flows. This SolutionPack provides reports that give you a clear understanding of your IT network traffic. It generates a wide spectrum of network traffic reports that highlight key performance indicators (such as router CPU and processor memory used and the most active network devices and applications) to help you better understand their impact on the network of your data center.

Technical specifications

SolutionPack version
4.0

Compatible EMC M&R versions
6.8u2 and later

Support list
Netflow v5.0 and v9.0

Cisco ASA NSEL (Network Security Event Logs)

IP Flow Information Export (IPFIX)

Data collection method
Flow Listener

Main reports
Global, Exporter, Interface-level Reporting

Busy Dashboard

Conversations

Protocol and Applications

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Configuring Elastic Search

Complete this procedure to configure the Elastic Search.

Before you begin

- Perform M&R 6.8u2 installation successfully.

Procedure

1. Open the /etc/sysctl.conf file.
2. Add the following line:

```
vm.max_map_count=262144
```

3. Edit the /etc/security/limits.conf file.
4. Add the following line for the user:

   In this example, the user is apg.

```
apg hard nofile 65536
apg soft nofile 65536
apg hard nproc 65536
apg soft nproc 65536
```

5. Save the file.
6. To install the Elastic Search cluster package, invoke the following command:

```
./manage-modules.sh install  elasticsearch-cluster
```

   When you are prompted for the IP address, provide the M&R host IP address. In the **more entries** option, select **no** unless Elastic Search needs to be configured in the cluster mode.

7. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

   Following is the output:

```
open files                      (-n) 65536
max user processes              (-u) 65536
```

8. In the `/opt/kar/APG/Databases/Elasticsearch/Default/conf/elasticsearch.yaml` file, add the following entry:

```
bootstrap.seccomp: false
script.max_compilations_per_minute: 120
```

   In `elasticsearch.yml` file, add the above line at the end.

Note

Update elasticsearch.yaml file with 0.0.0.0. (Change the parameter : network.host: _site_ to network.host: 0.0.0.0) or Hostname /IP address where Elastic Search is installed. This is to resolve the localhost error, where it is not able to resolve the localhost. For multiple VM , you must give the multiple IP.

---

9. Restart Elastic Search server.

   Ensure that, Elastic Search server is running.

10. Restart Tomcat service.

Installing the SolutionPack for Traffic Flows

After you log in as an administrator, you can install the SolutionPack for Traffic Flows from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Service Assurance Suite Installation and Configuration Guide for EMC M&R* for more information.
- The EMC M&R platform is updated to 6.8u2 and later.
- Obtain the Fully Qualified Domain Name (FQDN) or IP address for one or more servers depending on your deployment.
- Obtain available unique network port numbers for one or more Traffic Flow listener configurations. If you are using a privileged port on UNIX systems, make sure to run the service as root.
- Consider the type of deployment: single server or distributed. For a single server deployment, the SolutionPack for Traffic Flows components are installed on the same server. For a distributed deployment, the minimum components on two servers are: Central Database and Reports on one server, and the Distributed Collector on a second server. Or, install each component on different servers. In a typical distributed deployment, Reports is installed on the EMC M&R Frontend server, Distributed Collector is installed on a server which is the target of traps or traffic flows, and Central Database is installed on a server with sufficient space for the database. Distributed Collector and Central Database blocks cannot reside on the same server.

Procedure

1. Log in to the EMC M&R platform with your user name and password.

   For example, `https://Frontend-hostname:58443/APG`

2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the **Traffic Flows** in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Accept the default instance name (`generic-traffic-flow`) or type a new name.
8. Select the server for each component.

Deployment type	Components
Single server	Select or type the fully qualified host name of the same server for both components: • **Combined Collector & Database** • **Reports** Select **Will not be installed** for the **Central Database** and **Distributed Collector** components.
Distributed deployment	Select or type the fully qualified host name of the server for these components: • **Central Database** • **Distributed Collector** • **Reports** Select **Will not be installed** for the **Combined Collector & Database** component. Distributed Collector and Central Database blocks cannot reside on the same server.

Click **Next**.

9. Complete the field entries for the screens, depending on your deployment.

   Click the question mark icon to access field-level help.

   - Combined collector and database setup when installing SolutionPack for Traffic Flows - Single server deployment on page 474
   - Central database setup when installing SolutionPack for Traffic Flows - Distributed deployment on page 474
   - Distributed collector setup when installing SolutionPack for Traffic Flows - Distributed deployment on page 475
   - Report setup when installing SolutionPack for Traffic Flows on page 476

   Click **Next** after you complete each screen.

10. Click **Install** after you complete the last screen.

    The installation process begins.

11. Select the maximize arrow next to each component to view the installation process.

    When the installation successfully completes, green checkmarks appear.

12. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Perform the post-installation tasks.

Combined collector and database setup when installing SolutionPack for Traffic Flows - Single server deployment

Since the combined data collector and database are being installed on the same server, accept the default settings for all of the fields, except for the following fields where you need to select or provide values.

- In the **Listener configuration** section, for the **Flow type** list box, select **NetFlow** or **sFlow**.
- Type the network port number for the listener. The default ports are:
  - NetFlow: 2055, 9555, 9556, or 9996.
  - sFlow: 6343.
- In the **ElasticSearch Configuration** box, update the ElasticSearch IP Address and Port Number if needed. Default port is 9200.
- Use the **+** icon to add more listeners if needed.
- Accept **10** for the top levels of data to collect for report results or adjust the value.
- Choose whether to enable the **Optional sending of Raw Data to the Database** checkbox.
  Choose this option only if needed, because sending raw data to the database will decrease performance. No reports currently rely on raw data and it is completely optional.
- Select the **Configure advanced settings** checkbox and scroll to see the settings.
- Accept **1** for the **Flow listener threading level** or adjust the value.
  Depending on the system's characteristics, a general rule for a dedicated listener is one thread per CPU (Core). Since the database resides on the same server, adjust the number of threads so it has enough cores to fetch the flows.
- In the **Flow Aggregation Period** field, accept **300** seconds (5 minutes) or adjust the value.
- Accept **1** day for the **Raw Data Retention Policy** or adjust the value.
  This field depends on the setting of the **Optional sending of Raw Data to the Database** checkbox.

Central database setup when installing SolutionPack for Traffic Flows - Distributed deployment

Configure the central database for the server in your distributed deployment:

- If the **Web-Service Gateway** list box appears, select **Add a new Web-Service Gateway**.
  For a new installation, the **Web-Service Gateway** list box does not appear. This list box only appears if another SolutionPack for Traffic Flows or other SolutionPacks are already installed.
- For the Web Service fields for a new Web-Service Gateway, replace the `localhost` value with the IP address of the Backend or Database server and provide the port number. Accept the default username and password.
- If the **Traffic Flow SolutionPack** list box appears, select **Add a new Traffic Flow SolutionPack**.

For a new installation, the **Traffic Flow SolutionPack** list box does not appear. This list box only appears if another SolutionPack for Traffic Flows or other SolutionPacks are already installed.

- For the **Installation Path** field, accept the default setting.
- Choose whether to enable the **Optional sending of Raw Data to the Database** checkbox.
  Choose this option only if needed, because sending raw data to the database will decrease performance. No reports currently rely on raw data and it is completely optional.
- Accept **1** day for the **Raw Data Retention Policy** or adjust the value.
  This field depends on the setting of the **Optional sending of Raw Data to the Database** checkbox.

Distributed collector setup when installing SolutionPack for Traffic Flows - Distributed deployment

Configure the distributed data collector for the server in your distributed deployment:

- In the **Data collection** list box, select **Add a new Data collection**.
- Replace the `localhost` value with the IP address of the Data Collection server or load-balancer connector and provide the network port number.
- If the **Property Store configuration** list box appears, select **Add a new Property Store configuration**.
  For a new installation, the **Property Store configuration** list box does not appear. This list box only appears if another SolutionPack for Traffic Flows or other SolutionPacks are already installed.
- Complete the fields for the new EMC M&R Property Store. For the Web Service fields, replace the `localhost` value with the IP address of the EMC M&R Frontend server and provide the port number. Accept the default username and password.
- In the **Listener configuration** section, for the **Flow type** list box, select **NetFlow** or **sFlow**.
- Type the network port number for the listener. The default ports are:
  - NetFlow: 2055, 9555, 9556, or 9996.
  - sFlow: 6343.
- In the **ElasticSearch Configuration** box, update the ElasticSearch IP Address and Port Number if needed. Default port is 9200.
- Use the **+** icon to add more listeners if needed.
- For the **Central DB hostname** field, replace the `localhost` value with the IP address of the Backend or Database server.
- For the **Central DB port** field, accept the default setting.
- Accept **10** for the top levels of data to collect for report results or adjust the value.
- Choose whether to enable the **Optional sending of Raw Data to the Database** checkbox.
  Choose this option only if needed, because sending raw data to the database will decrease performance. No reports currently rely on raw data and it is completely optional.

- Select the **Configure advanced settings** checkbox and scroll to see the settings.
- Accept **1** for the **Flow listener threading level** or adjust the value.
  Depending on the system's characteristics, a general rule for a dedicated listener is one thread per CPU (Core).
- In the **Flow Aggregation Period** field, accept **300** seconds (5 minutes) or adjust the value.

Report setup when installing SolutionPack for Traffic Flows

Configure the Reports component for the server in your single server or distributed deployment:

- Select the **Select to use either NBAR or local mapping for Application Naming** checkbox.
  Recommended, if you select this checkbox, the mapping files are redirected to use NBAR information or the derived application names. If you leave the checkbox clear, the mapping files use only the derived application names.
- For a single server deployment, accept the default settings for the remaining fields.
- For a distributed deployment, replace the `localhost` value with the IP address of the server where the ElasticSearch instance is running. Accept the default settings for the remaining fields.

Post installation tasks

After you install the SolutionPack for Traffic Flows, complete these tasks in the following order.

1. Starting the Event Processing Manager on page 476
2. Enabling event reporting for single server and distributed deployments
   - Enabling event reporting and reconfiguring the Tomcat Frontend server (Linux) on page 477
   - Enabling event reporting in SolutionPack for Traffic Flows (Windows) on page 478
3. Starting the Tomcat service on page 478
4. Confirming report creation on page 69

Starting the Event Processing Manager

By starting the Event Processing Manager (EPM), you begin traffic flow collection.

Before you begin

Before starting EPM, use the Simple Network Management Protocol (SNMP) to discover the flow exporters, which are managed as routers, into the EMC M&R platform.

Procedure

1. To start EPM, type `/opt/APG/bin/manage-modules.sh service start event-processing-manager <instance_name>`
2. To verify EPM has started, check the `processing-00.log` file in `/opt/APG/EventProcessing/Event-Processing-Manager/<instance_name>`.

This message appears at the end of the log:

```
Processing manager started!
```

Enabling event reporting and reconfiguring the Tomcat Frontend server (Linux)

For Linux, for new single server and distributed installations only, enable the event reporting features and reconfigure the Tomcat Frontend server.

Run this script once after a new installation. Do not run this script after a reconfiguration.

Procedure

1. Execute these commands from the `opt\APG\bin` folder:

```
./manage-resources.sh create "dba/ES-TF-CONV" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-conv-topn*" }, "settings":
{"mapping": "ES-TF-CONV.xml"}, "disabled": false }'
    ./manage-resources.sh create "dba/ES-TF-PROTO" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-protocols*" }, "settings":
{"mapping": "ES-TF-PROTO.xml"}, "disabled": false}'
    ./manage-resources.sh create "dba/ES-TF-ALLPORTS"
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
localhost:9200"], "prefix": "/es-dw-flow-allports*" },
"settings": {"mapping": "ES-TF-ALLPORTS.xml"}, "disabled":
false}'
    ./manage-resources.sh create "dba/ES-TF-APP" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-applications-topn*" },
"settings": {"mapping": "ES-TF-APP.xml"}, "disabled": false}'
    ./manage-resources.sh create "dba/ES-TF-DATA" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-data*" }, "settings":
{"mapping": "ES-TF-DATA.xml"}, "disabled": false}'
    ./manage-resources.sh create "dba/ES-TF-DSTADDR"
'{ "type": "elasticsearch", "datasource": { "hosts": ["http://
localhost:9200"], "prefix": "/es-dw-flow-dstaddr-topn*" },
"settings": {"mapping": "ES-TF-DSTADDR.xml"}, "disabled":
false}'
    ./manage-resources.sh create "dba/ES-TF-HOSTS" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-hosts*" }, "settings":
{"mapping": "ES-TF-HOSTS.xml"}, "disabled": false}'
    ./manage-resources.sh create "dba/ES-TF-INT" '{ "type":
"elasticsearch", "datasource": { "hosts": ["http://localhost:
9200"], "prefix": "/es-dw-flow-topint-topn*" }, "settings":
{"mapping": "ES-TF-INT.xml"}, "disabled": false}'
    ./manage-resources.sh create dba/ES-TF-NOSNMP "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-nosnmp*' }, 'settings':
{'mapping': 'ES-TF-NOSNMP.xml'}, 'disabled': false}}"
./manage-resources.sh create dba/ES-TF-SRCADDR "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-srcaddr-topn*' }, 'settings':
{'mapping': 'ES-TF-SRCADDR.xml'}, 'disabled': false}}"
```

2. Restart the Tomcat service in order to make the changes effective.

Enabling event reporting in SolutionPack for Traffic Flows (Windows)

For Windows, for new single server and distributed installations only, enable the event reporting features.

Run these commands once after a new installation. Do not run these commands after a reconfiguration.

Procedure

1. Execute these commands from the `APG\bin` folder:

```
manage-resources.cmd create dba/ES-TF-CONV "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-conv-topn*' }, 'settings':
{'mapping': 'ES-TF-CONV.xml'}, 'disabled': false }}"
    manage-resources.cmd create dba/ES-TF-PROTO "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-protocols*' }, 'settings':
{'mapping': 'ES-TF-PROTO.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-ALLPORTS "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-allports*' }, 'settings':
{'mapping': 'ES-TF-ALLPORTS.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-APP "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-applications-topn*' },
'settings': {'mapping': 'ES-TF-APP.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-DATA "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-data*' }, 'settings':
{'mapping': 'ES-TF-DATA.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-DSTADDR "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-dstaddr-topn*' }, 'settings':
{'mapping': 'ES-TF-DSTADDR.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-HOSTS "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-hosts*' }, 'settings':
{'mapping': 'ES-TF-HOSTS.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-INT "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-topint-topn*' }, 'settings':
{'mapping': 'ES-TF-INT.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-NOSNMP "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-nosnmp*' }, 'settings':
{'mapping': 'ES-TF-NOSNMP.xml'}, 'disabled': false}}"
    manage-resources.cmd create dba/ES-TF-SRCADDR "{ 'type':
'elasticsearch', 'datasource': { 'hosts': ['http://localhost:
9200'], 'prefix': '/es-dw-flow-srcaddr-topn*' }, 'settings':
{'mapping': 'ES-TF-SRCADDR.xml'}, 'disabled': false}}"
```

2. Restart the Tomcat service in order to make the changes effective.

Starting the Tomcat service

Procedure

- To start the Tomcat service, execute the following command.

For Linux, type:

```
<Install_Directory>/opt/APG/bin/manage-modules.sh service
restart tomcat Default
```

For Windows, type:

```
<Install_Directory>\APG\bin\manage-modules.cmd service restart
tomcat Default
```

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Upgrading Traffic Flows SolutionPack from 6.5u4 and 6.6u1 to 6.8u2

To upgrade from EMC M&R 6.5u4 and 6.6u1 to 6.8u2, you must perform the following steps:

Before you begin

Download the EMC M&R 6.8u2 build from EMC Online Support website at http://support.emc.com

Procedure

1. Upgrade the EMC M&R core to 6.8u2, by invoking the following command:

   ```
   setup-linux-x86_64-v95.sh
   ```

   For more details, refer the EMC M&R 6.8u2 Installation and Configuration guide for M&R Core upgrade procedures.

2. To upgrade the platform:

   ```
   /opt/APG/bin/manage-modules.sh update module-manager
   /opt/APG/bin/manage-modules.sh service update all
   /opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
   ```

3. Install the Elastic Search cluster package, see Configuring Elastic Search on page 470 for more information.

4. Uninstall old Traffic Flows SolutionPack and delete the blocks.

   In case of upgrade from 6.6u1, you need to delete the resources pointing to datastore for TrafficFlows SP.

5. Install the 6.8u2 Traffic Flows SolutionPack.
6. Migrate the old database V2 to V3 to update the latest schema:

   In Linux:

   - Navigate to `/opt/APG/Event-Processing/Elasticsearch-Writer/ <instance_name>/datastore-ddl`.
   - Run the `setup-datastore.sh` script. This runs the migration script ***" flow-database-migrate-V2toV3.ddl "*** on the backend automatically.

   In Windows:

   - Run the migration script on the backend host (in case of distributed setup).
   - Navigate to `/opt/APG/Event-Processing/Elasticsearch-Writer/<instance_name>/datastore-ddl` . The instance name was set during the installation of the SolutionPack.
   - Open the ***flow-database-migrate-V2toV3.ddl*** file and use CTRL+C, to copy the content.
   - Navigate to `APG\Databases\APG-Datastore\Default\bin` .
   - Run the `datastore-client.cmd` script to connect to the datastore.
   - In the SQL prompt, use CTRL+V to paste the contents from the buffer.

7. Restart the Event Processing Manager process.
8. Reconfigure the Tomcat on the frontend, as mentioned in the post installation wizard.

   It is necessary to reconfigure the Tomcat frontend after installation of this SolutionPack and update/upgrade.

9. Run the migration task, see Migrating Traffic Flows SolutionPack from Datastore to Elastic Search on page 481 for more information.

Upgrading Traffic Flows SolutionPack from 6.7u1 to 6.8u2

To upgrade from EMC M&R 6.7u1 to 6.8u2, you must perform the following steps:

Before you begin

Download the EMC M&R 6.8u2 build from EMC Online Support website at http://support.emc.com.

Procedure

1. Upgrade the EMC M&R core 6.8u2, by invoking the following command:

   ```
   setup-linux-x86_64-v95.sh
   ```

   For more details, refer the *EMC MnR 6.8u2 Installation and Configuration guide* for M&R Core upgrade procedures.

2. To upgrade the platform:

```
/opt/APG/bin/manage-modules.sh update module-manager
/opt/APG/bin/manage-modules.sh service update all
/opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
```

3. Install the Elastic Search cluster package, see Configuring Elastic Search on page 470 for more information.
4. Update the SolutionPack blocks for Traffic Flows and all other components (one click upgrade).
5. Run the post upgrade message to create the resources.
6. Restart the services.
7. Run **event-database-migration task** from scheduled tasks.

Migrating Traffic Flows SolutionPack from Datastore to Elastic Search

To migrate from previous database to the new database, you must perform the following steps:

Before you begin

- Download the latest M&R build. The *Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides more information.
- Install the M&R, by invoking the following command:

```
sh setup-linux-x86_64-v95.sh
```

- To upgrade the platform, install the new packages in:

```
/opt/APG/Tools/Module-Repository [Y/n]? Y
/opt/APG/bin/manage-modules.sh update module-manager
/opt/APG/bin/manage-modules.sh service update all
/opt/APG/Tools/Module-Manager/1.13u1/bin/launch-update.sh
```

Procedure

1. Configure the Elastic Search, see Configuring Elastic Search on page 470 for more information.
2. Restart Elastic Search server.

   Ensure Elastic Search server is running.
3. Restart the APG services.

   Make sure there are no errors in the EPM logs, APG cluster logs and Tomcat catalina logs.
4. Stop the event processing manager service for generic-traffic-flow.
5. Run the data-migration task which is enabled for run, see the Scheduling the Event-Processing Tasks on page 482 for more information.
6. Ensure that the data is migrated to Elastic Search.

URL to check the data in Elastic Search are:

```
http://<Host IP of Elastic Search>:9200/_cat/indices

http://<Host IP of Elastic Search>:9200/_template?pretty

http://<Host IP of Elastic Search>:9200/es-dw-flow-dstaddr-
topn-1482192000000/_search?pretty

http://<Host IP of Elastic Search>:9200/es*/_search?pretty
---to get the total number of rows/records
```

7. Start the EPM. Ensure that the Event-Processing for generic-traffic flow, flows are read and processed.
8. Ensure from Elastic Search, that data is flowing.

Scheduling the Event-Processing Tasks

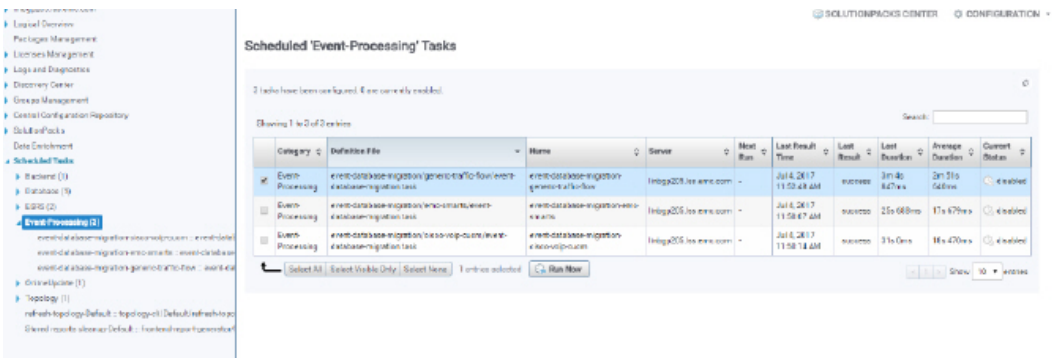
You need to configure the event processing task, in order to run the data-migration task which is enabled for run.

Procedure

1. On the EMC M&R Console, navigate to **Centralized Management** > **Scheduled Tasks** .
2. Click **Event-Processing**.

   The scheduled event-processing tasks appears in the right pane.
3. Select the event processing task.

   Figure 11 Scheduled Event-Processing example



4. Click **Run Now**, to run the data-migration task which is enabled for run.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 483
- Viewing errors in the Event-Processing-Manager log files on page 484

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .

2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing errors in the Event-Processing-Manager log files

Review the Event-Processing-Manager log files to troubleshoot problems.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Events**.
4. Click the Event-Processing-Manager for your instance.

   Event-Processing-Manager::*<Event-Processing-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

What to do if parsing errors related to resource link updating occur

If you observe parsing errors related to resource link updating, follow this procedure.

Procedure

1. On the Frontend server, list the resources. Type the command: `/opt/APG/bin/manage-resources.sh list`

   For example, the output looks like:

```
"dba/ES-TF-ALLPORTS",
  "dba/ES-TF-APP",
  "dba/ES-TF-CONV",
  "dba/ES-TF-DATA",
  "dba/ES-TF-DSTADDR",
  "dba/ES-TF-HOSTS",
  "dba/ES-TF-INT",
  "dba/ES-TF-NOSNMP",
  "dba/ES-TF-PROTO",
  "dba/ES-TF-SRCADDR",
 "dba/APG-DB",
 "mgmt/APG-DB",
```

2. For all of the resources in your list, use the `manage-resources.sh update` command to change the password to **`watch4net`**. Here are two examples. For the dba/APG-DB resource, type:

```
/opt/APG/bin/manage-resources.sh update dba/APG-DB '{
  "type": "jdbc",
  "datasource":   {
    "maxActive": "10",
    "maxIdle": "10",
    "validationQuery": "SELECT 1",
    "testOnBorrow": "false",
    "testWhileIdle": "true",
    "validationQueryTimeout": "5",
    "timeBetweenEvictionRunsMillis": "10000",
    "minEvictableIdleTimeMillis": "60000",
    "maxWait": "10000",
    "removeAbandoned": "true",
    "removeAbandonedTimeout": "60",
    "logAbandoned": "true",
    "driverClassName": "com.mysql.jdbc.Driver",
    "username": "apg",
    "password": "watch4net",
    "url": "jdbc:mysql://wp-dev-098.lss.emc.com:53306/apg?
autoReconnect=true&connectTimeout=20000&maxReconnects=2"
  },
  "settings": {"cachegrp": "DB"}
}'
```

For the mgmt/APG-DB resource, type:

```
/opt/APG/bin/manage-resources.sh update mgmt/APG-DB '{
  "type": "webservice",
  "connection":   {
    "disableSSLValidation": true,
    "url": "https://wp-dev-098.lss.emc.com:48443/Backends/APG-
Backend/Default",
    "user": "admin",
    "password": "watch4net"
  }
}'
```

The *Service Assurance Suite Installation and Configuration Guide for EMC M&R* provides detailed information about resources and the `manage-resources.sh update` command.

3. After you change the password for all of the resources, restart the Tomcat service. Starting the Tomcat service on page 478

CHAPTER 47

SolutionPack for Transaction Summary Sheet

- Overview 488
- Technical specifications 488
- Where to find the latest SolutionPack software 488
- Installing the SolutionPack 489
- Configuring the SolutionPack 490
- Confirming report creation 490

Overview

Learn how to install and configure the SolutionPack for Transaction. This SolutionPack helps you measure the performance of your network by providing transactions that return key performance indicators.

You can execute and report on these transactions using the SolutionPack for Transaction:

- HTTP head - implements an HTTP head request over a specific URL
- HTTP - implements an HTTP request over a specific URL
- SQL-based query - executes a query against an SQL server
- TCP connect - connects to a port on a server and executes a command
- DNS query - executes a query that retrieves DNS records from a specific resolver
- FTP commands - executes the retrieve, store and delete commands
- SFTP - executes the retrieve, store and delete commands over the SSH file transfer protocol
- LDAP - performs a search query against an LDAP server
- RADIUS - performs an authentication request against a RADIUS server
- SCRIPT - executes a custom command on a local machine

Technical specifications

SolutionPack version
1.1

Compatible EMC M&R versions
6.7u1 and later

Data collection method
Transaction Collector

Main reports
Transactions List by Type

Transactions List by Group

Transactions List by Destination (Target)

Transactions List by Source

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a

Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If not listed, obtain a license by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com. This SolutionPack requires a license for the SolutionPack for Transaction and the Transaction Collector.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. The *EMC M&R (Watch4net) Installation and Configuration Guide* provides for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install:
   a. Type the instance name.
   b. Select the server in one or more list boxes. For example, select the server in the **Collector** and **Reports** list boxes.
   c. Click **Next**.

      For each list box you select, a screen appears.
   d. Click **Next** after you complete each screen.
8. When the **Transaction Collector** screen appears, set these values:
   - **Transaction Collector Host or IP**: The IP address of the host where the Transaction Collector is running.
   - **Transaction Collector port**: The port used for communication by the Transaction Collector.
   - **Transaction Collector username**: The EMC M&R login name where you installed the Transaction Collector. (This field displays **admin** by default.)
   - **Transaction Collector password**: The EMC M&R password where you installed the Transaction Collector.
   - **Transaction Collector instance**: The instance name of the Transaction Collector, such as **generic-transaction**.

   If using more than one Transaction Collector instance, click **+** to add more credentials.

9. Click **Install** after you complete the last screen.

   The installation process begins.

10. Select the maximize arrow next to each component to view the installation process.

    When the installation successfully completes, green checkmarks appear.

11. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring the SolutionPack

For the SolutionPack for Transaction to retrieve and process transactions, you must restart the Tomcat service after installation. You can also add new transaction types and edit default transaction types.

The **Administration** > **Modules** > **Transaction Collector** > **Configuration Management** > interface provides an automated way for you to add and edit transaction types. You can also use the `transaction-collector.xml` file to manually add and edit transactions, as explained in the **Configuration** chapter of the *Transaction Collector Administration Guide*. This guide is in the `/APG/Doc` folder of your installation path.

Note

Do not follow the instructions in the **Installation** chapter of the *Transaction Collector Administration Guide* since the Transaction Collector and the `authentication.xml` file are automatically configured during the SolutionPack for Transaction installation.

Procedure

1. To use the Transaction Collector, restart the Tomcat service by executing **`/opt/APG/bin/manage-modules.sh service restart tomcat Default`**
2. To add or edit a transaction, navigate to **Administration** > **Collecting** > **Transaction Collector**.

   The **Configuration Management** screen appears.
3. Click **Retrieve** to edit the running Transaction Collector.
4. You may, optionally, set up default entries that will populate fields in the transaction setup by editing the **Collector Properties** or **Default Attributes** entries in the **Configuration Management** navigation tree.
5. To add a new transaction, expand **Transactions** > **Add a Transaction** and select a transaction type or group.
6. Edit the parameters and attributes. Click **Save**.
7. Click **List** to return to the Configuration Management screen, and click **Push** to restart the collector with the new transaction.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

CHAPTER 48

SolutionPack for UPS Summary Sheet

- Overview 494
- Technical specifications 494
- Where to find the latest SolutionPack software 494
- Installing the SolutionPack 495
- Configuring SNMP device discovery 495
- Confirming report creation 496
- Troubleshooting 497

Overview

Learn how to install and configure the SolutionPack for UPS (Uninterruptible Power Supply). This SolutionPack provides unified monitoring of all the UPS devices distributed in the network. It provides key reports to help you manage the performance and availability of your backup power sources.

The SolutionPack for UPS helps you do the following:

- Maintain an accurate inventory of devices and components.
- Understand device activities.
- Plan for power source requirements.

Technical specifications

SolutionPack version
1.0

Compatible EMC M&R versions
6.3u1 and later

Data collection method
SNMP collector

Supported devices
UPS devices supporting `rfc1628.mib`

APC devices supporting `PowerNet-MIB.mib`

Data collection method
SNMP collector

Main reports

UPS Output Load
: Reports on device-wide distribution of the output load.

Battery Status
: Provides voltage, current, and temperature information.

Input/Output
: Reports on input line metrics, such as voltage and frequency, and output line metrics, including status, load, voltage, current, and frequency.

On Battery Stats
: Shows the current status of a battery and its remaining time and capacity.

Capacity (%)
: Graphs the percentage of battery capacity over a period of time.

Where to find the latest SolutionPack software

Install the latest core software update for your product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use

the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request a license for that SolutionPack by completing a Support Request (SR) form, which is available on the EMC Online Support website at http://support.emc.com.

Installing the SolutionPack

Before you begin

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates listed in **Centralized Management** > **License Management**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the EMC Online Support website at http://support.emc.com.
- Make sure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. See the *Watch4net Installation and Configuration Guide* provides for more information.

Procedure

1. Log in to the EMC M&R platform with your user name and password.
2. Select **Administration**.
3. Select **Centralized Management**.
4. Select **SOLUTIONPACK CENTER**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. In the next window, type the instance name for Reports and SNMP Masks and click **Next**.
8. Select the **Administration Web-Service Instance** as the default and click **Next**.
9. In the SNMP Masks wizard, click **Install**. Green indicators appear next to Reports and SNMP Masks to indicate their installations were successful.
10. Select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

Configuring SNMP device discovery

An SNMP collector discovers the capabilities that you configure for a device. You can use a seed file to import a list of device definitions or manually add and configure devices.

Before you begin

After upgrading from EMC M&R 6.5u4 or 6.6u1 to 6.7u1 or 6.7u2, you must manually install new SolutionPack blocks to ensure the SNMP block and SNMP Mask components are updated. Navigate to **Centralized Management** > **SolutionPack Center**. Select the SolutionPack to be updated and click Install to update the SNMP block.

Procedure

1. Navigate to **Administration** in the EMC M&R platform.
2. Click **Modules** > **SNMP Device Discovery**.

   A **Dashboard** appears where you add new SNMP collectors and devices as well as add devices to existing SNMP collectors.
3. To add an SNMP collector, click **Collectors** > **New Collector**.
   a. Specify the required information for the SNMP collector.
   b. Under **Import Options**, select all options except **Lock collector current capabilities**.
   c. Click **Save**.
4. To upload a seed file, click **Device Sources** > **New Seed File Device Source**.

   For information about defining a seed file, click **Documentation** on **SNMP Device Discovery – EMC M&R**.
   a. Type the main parameters and click **Save**.
   b. Under the **Seed File** tab, click **Upload new definition seed file**.
   c. Navigate to the seed file and click **Ok**.
   d. Click **Save.**
5. To manually add devices, click **Devices** > **New Device**.
   a. On the **New Device** window, click each tab and type the required information for the device.
   b. Click **Save** on each tab.
6. Select the device that you just added and click the **Approve** action, which is the checkmark.
7. On the **Dashboard**, do the following:
   a. Click **Import devices from all enabled device sources**.
   b. Click **Discover capabilities from all approved devices**.
   c. Click **Distribute all approved devices with capabilities on all enabled collectors**.
   d. Click **Send the generated configurations on all available collectors**.

      Green indicators appear on the **Dashboard** after successful executions of the above functions.

Confirming report creation

After you install a SolutionPack, you can view its reports.

To view the reports:

Procedure

1. Go to **User Interface** > **Report Library**.
2. Click the SolutionPack to view its reports.

Results

It may take up to an hour to display all relevant information in these reports.

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.

2. Search for the metric in the database.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration** .
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration** .
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.

CHAPTER 49

SolutionPack for VMware vCenter 4.0 Summary Sheet

- Overview 500
- Technical specifications 500
- Configuring the SolutionPack to collect Powerpath data 500
- Installing this SolutionPack 501
- Post-install requirements 503
- Adding devices to discovery groups 504
- Limitations 505

Overview

The SolutionPack for VMware vCenter generates real-time and historical reports that help you understand VMware performance for VMware Hosts, Virtual Machines, virtual networks and DataStores.

Technical specifications

SolutionPack version
4.0

Compatible EMC M&R versions
6.7u1

Supported VMware vCenter versions

Table 28 Support for VMware vCenter

Supported Family/Models	Prerequisites	Ports
VMware vCenter Server 5.1 VMware vCenter Server 5.5 VMware vCenter Server 6.0	VMware infrastructure. PowerPath/VE 5.8 or later must be installed on the host to fetch PowerPath metrics. Access to VCENTER user credentials, with a minimum privilege level of Browse DataStore and all StorageViews.	443 TCP

Configuring the SolutionPack to collect Powerpath data

This procedure is required to collect PowerPath data from ESX servers.

For monitoring PowerPath performance and path status, an RTools host is required. RTools is the remote CLI software for managing the PowerPath software on ESXi (or other) hosts. The Collector will use the Generic-RSC Collector to issue RTools command scripts to the RTools host to collect PowerPath data directly from the ESXi servers.

Procedure

1. Add the host name and credential of every ESXi host to the RTools default lockbox. Commands will fail if the lockbox is not populated.

   The first use of the command creates the lockbox if necessary.

2. The RTools host has to be discovered by the Generic-RSC Collector. Discover it through the SolutionPack for Physical Hosts using the ESX Linux or the ESX Windows host type. Choose the Linux or Windows type appropriate for the RTools host so that the collector can issue the correct format scripts.
3. Create the default lockbox on RTools Host and add ESXi hostname credentials:

   ```
   rpowermt setup add_host host= username= password=
   ```

4. Turn on performance monitoring on ESXi host from Rtools (if needed):

   ```
   rpowermt set perfmon=on interval= host=
   ```

5. For PASSWORD based discovery Suse Linux hosts from 3.0 RSC, it requires edits to the sshd_config file. Note this file is located under /etc/ssh directory on discovery hosts. You must enable "PasswordAuthentication" and restart sshd service on the host.

   ```
   lglah196:~/.ssh # grep Password /etc/ssh/sshd_config
   #PasswordAuthentication no #PermitEmptyPasswords no
   lglah196:~ # /etc/init.d/sshd restart Shutting down SSH
   daemon done Starting SSH daemon done
   lglah196:~ #
   ```

Installing this SolutionPack

Before you begin

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. Type the instance name.
7. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.

8. Click **Next**.

   The window displays a note about Alert Consolidation.

9. Click **Next**.

   The window displays pre-configured alert details.

10. To receive alerts, select **Enable the Host PowerPath Alerts**.
11. In **Recipient for email alerts**, enter the email addresses in which to send the alerts.
12. Click **Next**.

    The window displays data collection details.

13. From the **Data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

14. From the **Frontend Web service** drop-down menu, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the Frontend Web service.

15. Leave **Enable Topology Backend on data collected** checked.
16. From the **Topology Service** drop-down menu, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down menu, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

17. Optionally, select **Do you want to configure advanced settings** to configure the metric collection level, polling intervals, collection thread settings, and the re-synch interval.

    a. In **Metric Collect Level**, select the level of metrics you want the SolutionPack to collect per VMware collector block. The Metric Collect Level is an internal setting that tells the SolutionPack for VMware vCenter how much data to collect. This setting is not related to vCenter statistics levels.

       Collect-Level 1 collects the minimum required metrics related to capacity, topology, memory, and CPU.

       Collect-Level 2 collects all metrics supported by Collect-Level 1 and additionally all metrics related to disks and memory.

       Collect-Level 3 collects all supported metrics, which includes metrics collected under Collect-Level 1 and Collect-Level 2.

    b. In **Polling interval for VMware vCenter collection**, select a polling interval.

    c. In **Polling interval for VM files only**, select a polling interval.

    d. In **Number of collecting threads**, enter the number of collection threads.

    e. In **Number of collecting threads for VM files**, enter the number of collection threads.

    f. In **Re-Sync interval**, select an interval.

18. Click **Next**.
19. From **Event database**, select a database.

    If you select **Add a new Event Database**, add the Primary Backend host in the **Database hostname or IP address** field.

20. Click **Next**.

    The window displays reports settings.

21. Click **Next**.
22. Select **Collect performance metrics for PowerPath Bus** to collect performance metrics for all the logical Bus managed by PowerPath agent.

23. Select **Collect performance metrics for PowerPath LUNs** to collect performance metrics for all the logical devices managed by PowerPath agent.
24. Select **Collect PowerPath range-bound performance metrics** to collect range-bound performance metrics. Selecting this option increases metric count significantly. Be sure to correctly size your application before enabling this option.
25. Select **Do you want to configure advanced settings** to set the absolute path location of the sudo and pbrun binaries.
26. Click **Install.**
27. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
28. Click **Discovery Center** > **Devices Management**.
29. Click **VMware vCenter (vmware-vcenter-collect <version>)** for data collection and/or **VMware vCenter (vmware-vcenter-events <version>)** for vCenter events collection.

    These steps describe how to add VMware vCenter hosts individually. For information about using discovery groups to use the same credentials to discover multiple VMware vCenter hosts, see Adding devices to discovery groups.
30. Click **Add New Device**.
31. From **Server**, select the server where the device will be dispatched.
32. From **Instance**, select the instance of the vmware-vcenter-collect where the device will be dispatched.
33. In **Hostname or IP address**, type the vCenter service host. Enter the **Username** and **Password** used to poll vCenter.
34. Click **Ok**.
35. Click **Save**.

Post-install requirements

Perform these operations after the installation is complete.

To enable PowerPath LUN or Path performance data collection on Linux, navigate to the `/opt/APG/Collecting/Stream-Collector/<Instance Name>/conf/scripts/` directory.

Procedure

1. In the `LunMappingDetection.pl` script, set `want_powerpath_lun_performance=1`.

   By default, this flag is set to zero.
2. To enable the PowerPath LUN or Path performance data collection on Windows:

   a. Navigate to the `C:\Program Files\APG\Collecting\Stream-Collector\<Instance Name>\conf\scripts\windows` directory.

   b. In the `LunMappingDetection.ps1` script, set `powerPathPerformanceCollection=enabled`.

   By default, this flag is set to disabled.

3. To enable events reporting, open the Web-Application configuration file (`APG.xml`) and uncomment the `vmware-vcenter` section and the `ResourceLink` tag.
4. Restart the Tomcat service to make the changes effective.

Adding devices to discovery groups

Discovery groups simplify the process of working with a large number of devices and their corresponding IP addresses/hostnames and discovery credentials. For example, if you have set of four user/password credentials used among twenty devices, using a discovery group allows you to enter each set of credentials and all of the IP addresses/hostnames, and the discovery group will match the correct credentials to each device.

Procedure

1. From **Centralized Management**, click **Discovery Center** > **Discovery Center Backends**.
2. Select the Backend server.
3. Click **Register**.
4. Select the collector you want to use for discovering your SolutionPack objects.
5. If you are collecting VMware vCenter events, select the primary backend you want to use for discovering the events.
6. Click **Register**.
7. Click **Discovery Center** > **Devices Management**.
8. Click **<Device Name>**.
9. Click the **Discovery Groups** tab.
10. Click **Add new Discovery group**.
11. Provide a name for the group and click **Ok**.
12. Click the newly created group.
13. Under **Credentials**, click **Add new entry**.
14. Type the username.
15. If required, select the authentication type.
16. If you are using password authentication, provide the password and click **Ok**.
17. If you are using key-based authentication, provide the absolute location of the private key and click **Ok**.
18. Repeat the previous five steps to add as many username/password (or key) combinations as you would like.
19. Under **Hostname or IP address**, click **Add new entry**.
20. Provide the Hostname/IP Address of the device. If required, provide the Network Port. Click **Ok**.
21. Repeat the previous two steps to add as many devices as you would like.
22. Click **Save**.
23. Click the **Collected Devices** tab.
24. Click **Discover**.

25. Select the **Discovery group** and **Discovery Mode** and click **Ok**.

    The progress bar is displayed above the Collected Devices tab.
26. When the progress bar is gone, click the**Discovery Results** tab.
27. Click the group name that you added.
28. Under the group name, you can see the status of all the devices that you added.
29. Click **Import to Collected Devices**.
30. Merge the devices if you want to retain older devices that were added previously.
31. Click **Ok**.
32. Select the action and click **Continue**.
33. Click **Save**.

After you finish

Review your devices and credentials to avoid lockout of devices due to multiple attempts of incorrect credentials. EMC recommends that you create groups in such a way that devices have a minimal set of credentials to be tried against. EMC recommends using common public-private key pairs for multiple devices.

Limitations

- The Host Attributes report is missing the IP Address for VMware vCenter.
- Incomplete information for HBA driver, firmware, and HBA model in the discovered value column in Match ESM screen.

PART 4

Troubleshooting SolutionPack Configurations

This section provides troubleshooting tips.

Chapter 50, "SolutionPack for EMC M&R Health 2.1 Summary Sheet"

Chapter 51, "Troubleshooting techniques"

CHAPTER 50

SolutionPack for EMC M&R Health 2.1 Summary Sheet

- Overview 510
- Technical specifications 510
- Installing the SolutionPack 510

Overview

This SolutionPack monitors the health of your EMC M&R infrastructure. Take advantage of this no-charge SolutionPack to keep the EMC M&R services performing optimally, so you have instant access to performance data and reports when you need it.

Supported systems
EMC M&R 6.7u1 and later

Data collection methods
JMX

Main reports
Modules Performance

Collecting Level Performance

Backend & Databases events and utilization

Server summary

Technical specifications

SolutionPack version
2.1

Installing the SolutionPack

Install this SolutionPack on all core software hosts in your environment.

Before you begin

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Click **SolutionPack Center**.
4. Select the SolutionPack in the **Browse and Install SolutionPacks** window.
5. Click **Install**.
6. Type the instance name.
7. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
8. Click **Next**.

   The window displays pre-configured alert details.
9. Click **Next**.

   The window displays data collection details.

10. From the **Data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

11. From the **Alerting on data collection** drop-down menu, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

    If you select **Add a new alerting on data collection**, type information about the alerting configuration. In **Alerting Backend hostname or IP address**, specify the Primary Backend host.

12. Select **Configure advanced settings** to configure polling settings.
13. Click **Next**.

    The window displays reports settings.

14. Click **Install.**
15. Click **Ok** once installation is complete.

    Performance data will displayed in about an hour.
    The following message might appear in the collection log during operation: WARNING -- [2014-04-25 05:26:38 EDT] -- f::a(): JVM IO ERROR 'No such process'. ID: '17032', NAME: 'lib/module-manager.jar exit'. You can ignore this message.

CHAPTER 51

Troubleshooting techniques

- Troubleshooting 514

Troubleshooting

Report display problems

- What to do if data does not appear in any reports on page 73
- What to do if data does not appear in some reports on page 73
- Viewing collector errors in the Collector-Manager log files on page 74
- Reverting HTTPS mode to HTTP mode for M&R 6.8u2 installation on page 75

What to do if data does not appear in any reports

Procedure

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Before you begin

Allow at least three polling cycles to pass before manually running the scheduled task.

Procedure

1. Click **Administration** .
2. Click **Centralized Management**.
3. Expand **Scheduled Tasks**.
4. Click **Database**.
5. Select the **import-properties-Default** task.
6. Click **Run Now**.
7. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Procedure

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.

3. To view the log files for errors, go to **Centralized Management** and click **Logical Overview** > **Collecting** > **Collector-Manager::<*instance name*>** > **Log Files**.
4. To view the log files for errors, go to **Centralized Management** and click **Events** > **Event-Processing_Manager::Instance name** > **Logs**.

   To debug the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Procedure

1. Click **Administration**.
2. Under **Modules**, click **Management of Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.

   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type `name=='Capacity'` in the **Filter** field, `100` in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Procedure

1. Click **Administration**.
2. Click **Centralized Management** > **Logical Overview**.
3. Expand **Collecting**.
4. Click the Collector-Manager for your collector instance.

   Collector-Manager::*<Collector-Manager instance>* - *<host_ID>*
5. Expand **Log Files** and click the **View File** icon to review the error messages.