NetBackup IT Analytics Data Collector Installation and Configuration Guide

Release 11.6

VERITAS
now part of Cohesity

NetBackup IT Analytics Data Collector Installation and Configuration Guide

Last updated: 2026-03-02

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

21 September 2025

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.

- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Cohesity cannot process hardware replacement requests for partner hardware.
2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Section 1 Introduction 23

Chapter 1 Introduction 24

Overview 24
Distributed Data Collector (recommended for NetBackup) 26
Centralized Data Collector 27
Data Collector prerequisites 29

Chapter 2 Install and configure a Data Collector 30

Overview 30
Step-1: Choose operating system and complete prerequisites 31
Factors impacting Data Collector performance and memory requirements 32
Data Collector supported operating systems 32
Data Collector server memory and CPU guidelines 32
Additional prerequisites 33
Linux Data Collector Prerequisites: Changing the Linux Temporary Directory for Collection 34
Step-2: HTTPS requirement 35
Step-3: Add Data Collector on NetBackup IT Analytics Portal 35
Step-4: Install the Data Collector 37
Step-5: Verify the Data Collector is online from the Portal 38
Step-6: Confirm that the Data Collector is updated 38
Step-7: Configure the data collection policy 38
Step-8: Confirm that the data collection policy is collecting data 38

Chapter 3 Installing the Data Collector software 39

Introduction 39
Considerations to install Data Collector on non-English systems 40
Install Data Collector Software on Windows 42
Install Data Collector software on Linux 52
Configure Data Collector manually for Cohesity NetBackup 55
Install Data Collector binaries on Windows (without configuration) 57

Install Data Collector binaries on Linux host (without configuration) 62

Chapter 4 Configure SSL 64

SSL/TLS certificate configuration 64
SSL implementation overview 65
Obtain an SSL certificate 66
Update the web server configuration to enable SSL on the Portal server 67
Enable / Disable SSL for a Data Collector 72
Enable / Disable SSL for emailed reports 72
Test and troubleshoot SSL configurations 73
Keystore file locations on the Data Collector server 74
Import a certificate into the Data Collector Java keystore 74
Keystore on the portal server 76
Add a virtual interface to a Linux server 76
Add a virtual / secondary IP address on Windows 78

Section 2 Data Protection 81

Chapter 5 Configuration for Veritas Backup Exec 82

Introduction 82
Architecture overview (Veritas Backup Exec) 83
Backup Exec terminology 83
Prerequisites for adding data collectors (Veritas Backup Exec) 84
Installation overview (Veritas Backup Exec) 85
Enable TCP/IP for the SQL server 85
Configure a Windows user 85
Add Backup Exec servers 86
Importing Backup Exec Server information 87
Add a Veritas Backup Exec Data Collector policy 88

Chapter 6 Configuration for Cohesity DataProtect 91

Introduction 91
Prerequisites for adding Data Collectors (Cohesity DataProtect) 91
Installation overview (Cohesity DataProtect) 92
Add a Cohesity DataProtect Data Collector policy 92

Chapter 7 Configuration for Commvault Simpana 97

Introduction 97
Architecture overview (Commvault Simpana) 98
Prerequisites for adding Data Collectors (Commvault Simpana) 98
Upgrade troubleshooting: Microsoft SQL Server and Java 11 99
Installation overview (Commvault Simpana) 101
Open TCP/IP access to the Commvault database 101
Additional Static Port Configuration Steps 102
Set up a read-only user in the CommServe server 103
Option 1: Execute SQL commands in the CommServe database 103
Option 2: Use MSSQL Management Studio 104
Load historical data prior to initial data collection 107
Add Commvault Simpana servers 107
Add a Commvault Simpana Data Collector policy 108

Chapter 8 Configuration for EMC Avamar 113

Introduction 113
Architecture overview (EMC Avamar) 114
Prerequisites for adding Data Collectors (EMC Avamar) 114
Installation overview (EMC Avamar) 115
Add EMC Avamar servers 116
Adding an EMC Avamar Data Collector policy 116
Testing the collection 119
Add/Configure an Avamar Server within the Data Collector policy window 120
Import EMC Avamar server information 122
CSV Format Specifications 122
Import Notes 123
Export EMC Avamar server information 123

Chapter 9 Configuration for EMC Data Domain backup ....
1 2 4

Architecture overview (EMC Data Domain Backup) 124
Prerequisites for adding Data Collectors (EMC Data Domain Backup) 126
Installation overview (EMC data domain Backup) 126
Add EMC data domain servers 127
Add an EMC data domain backup Data Collector policy 127
Adding/Configuring an EMC data domain server within the Data Collector policy window 131

Configure a data domain server for file-level compression collection 132

Chapter 10 Configuration for Dell EMC NetWorker backup & recovery 138

Introduction 138
Prerequisites for adding Data Collectors (Dell EMC NetWorker Backup & Recovery) 138
Installation overview (Dell EMC Networker Backup & Recovery) 139
Adding a Dell EMC Networker Backup & Recovery Data Collector policy 140

Chapter 11 Configuration of Dell EMC PowerProtect Data Manager (PPDM) 144

Introduction 144
Prerequisites for adding Data Collectors (Dell PowerProtect Data Manager) 144
Installation overview (Dell PowerProtect Data Manager) 145
Add a Dell PowerProtect Data Manager Data Collector policy 145

Chapter 12 Importing generic backup data 150

About generic backup data collection 150
Considerations 150
Configuring generic backup data collection 151
CSV Format Specification 151
EXAMPLE: genericBackupJobs.csv 153
Manually loading the CSV file 153

Chapter 13 Configuration for generic backup 155

Introduction 155
Generic backup data collection 156
Prerequisites for adding Data Collectors (Generic Backup) 156
Installation overview (generic backup) 157
Add generic backup servers 157
Add a generic backup Data Collector policy 157
Adding/Editing a generic backup server within the Data Collector policy 160
Manually load the CSV file (generic backup) 161
CSV format specification 163
EXAMPLE: genericBackupJobs.csv 165

Chapter 14 Configuration for HP Data Protector 166

Introduction 167
Architecture overview (HP Data Protector) 167
Cell Manager 167
Disk agent (backup agent) 167
Media agent 167
Client systems 167
User interface (UI) 168
Prerequisites for adding Data Collectors (HP Data Protector) 168
Installation overview (HP Data Protector) 168
Identify HP Data Protector collection requirements 169
Cell Manager commands for data collection 170
Preparing for centralized data collection on a remote Cell Manager 171
Configure the Data Collector server in Cell Manager (HP Data Protector) 172
Requirements for the Data Collector (Windows) 172
Steps to Configure the Data Collector Server in Cell Manager 172
Configure an HP Data Protector admin user 173
Validate HP Data Protector setup 174
Add HP Cell Manager servers to NetBackup IT Analytics 174
Add an HP Data Protector Data Collector policy 175
Add/Edit a HP Data Protector server within the Data Collector policy 180
Tune the configuration 181

Chapter 15 Configuration for IBM Spectrum Protect (TSM) 182

Introduction 182
Architecture overview (IBM Spectrum Protect -TSM) 183
IBM Spectrum Protect (TSM) - servers and instances defined 183
Prerequisites for adding data collectors (IBM Spectrum Protect - TSM) 183
Installation overview (IBM Spectrum Protect - TSM) 184
Add IBM Spectrum Protect (TSM) servers 185
Adding an IBM Spectrum Protect (TSM) Data Collector policy 185
Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy 190
Import IBM Spectrum Protect (TSM) information 192
CSV format specifications 192

Export IBM Spectrum Protect (TSM) server information 193

Chapter 16 Configuration for NAKIVO Backup & Replication 194

Introduction 194
Prerequisites for adding data collectors (NAKIVO Backup & Replication) 194
Installation overview (NAKIVO Backup & Replication) 195
Add a NAKIVO Backup & Replication Data Collector policy 195

Chapter 17 Configuration for Oracle Recovery Manager (RMAN) 199

Introduction 199
Prerequisites for adding data collectors (Oracle Recovery Manager - RMAN) 199
Installation overview (Oracle Recovery Manager - RMAN) 201
Add an Oracle Recovery Manager (RMAN) Data Collector policy 201

Chapter 18 Configuration for Rubrik Cloud Data Management 205

Introduction 205
Prerequisites for adding Data Collectors (Rubrik Cloud Data Management) 205
Installation overview (Rubrik Cloud Data Management) 206
Add a Rubrik Cloud Data Management Data Collector policy 206

Chapter 19 Configuration for Veeam Backup & Replication 210

Introduction 210
Prerequisites for adding data collectors (Veeam Backup & Replication) 210
Verifying Data Collector servers can connect to Veeam servers 211
Known issues and limitations (Veeam Backup & Replication) 213
Installation overview (Veeam Backup & Replication) 214
Add a Veeam Backup & Replication Data Collector policy 214

Section 3 Storage (Capacity) 620

Chapter 20 Configuration for Compute Resources 220

Overview 220
Prerequisites for adding Data Collectors - Compute Resources 220
Installation overview 221
Add a Compute Resources policy 221

Chapter 21 Configuration for DELL EMC Elastic Cloud Storage (ECS) 226

Pre-Installation setup for DELL EMC Elastic Cloud Storage (ECS) 226
Prerequisites for adding Data Collectors - DELL EMC Elastic Cloud Storage (ECS) 227
Installation overview - DELL EMC Elastic Cloud Storage (ECS) 227
Add a DELL EMC Elastic Cloud Storage (ECS) Data Collector policy 227

Chapter 22 Configuration for Dell EMC Unity 232

Pre-Installation setup for Dell EMC Unity 232
Prerequisites for adding Data Collectors (Dell EMC Unity) 232
Installation overview (Dell EMC Unity) 233
Add a Dell EMC Unity Data Collector policy 233

Chapter 23 Pre-installation setup for Dell PowerStore 238

Overview 238
Prerequisits for adding Dell PowerStore data collector 239
Add a Dell PowerStore policy 240

Chapter 24 Configuration for EMC data domain storage 243

Architecture overview (EMC data domain storage) 243
Prerequisites for adding data Collectors (EMC data domain storage) 245
Installation overview (EMC data domain storage) 245
Add EMC data domain servers 246
Adding an EMC data domain storage Data Collector policy 248

Chapter 25 Configuration for EMC Isilon 254

Pre-Installation setup for EMC Isilon 254
Prerequisites for adding Data Collectors (EMC Isilon) 254
Configure the Isilon SNMP service 255
Configure Isilon sudo access 258
Modify the Sudo configuration 258
Installation overview (EMC Isilon) 259
Adding an EMC Isilon Data Collector policy 260

Chapter 26 Configuration for EMC Symmetrix 264

Pre-Installation setup EMC Symmetrix 264
Prerequisites for adding Data Collectors (EMC Symmetrix) 264
Installation overview (EMC Symmetrix) 265
Adding an EMC Symmetrix Data Collector policy 266
If the EMC solutions enabler is on a remote server (Recommended) 270

Chapter 27 Configuration for EMC VNX Celerra 273

Pre-Installation setup for EMC VNX Celerra 273
Prerequisites for adding Data Collectors (EMC VNX Celerra) 273
Setup for EMC VNX Celerra arrays 274
Configure a Read-Only user with an Operator role 275
Start the XML API server 276
Installation overview (EMC VNX Celerra) 276
Adding an EMC VNX Celerra Data Collector policy 277

Chapter 28 Configuration for EMC VNX CLARiiON 282

Pre-Installation setup for EMC VNX 282
Prerequisites for adding Data Collectors (EMC VNX) 282
Installation overview (EMC VNX) 283
Adding an EMC VNX Data Collector policy 284

Chapter 29 Configuration for EMC VPLEX 289

Pre-Installation setup for EMC VPLEX 289
Prerequisites for adding Data Collectors (EMC VPLEX) 289
Installation overview (EMC VPLEX) 290
Adding a EMC VPLEX Data Collector policy 290

Chapter 30 Configuration for EMC XtremIO 294

Pre-Installation setup for EMC XtremIO 294
Prerequisites for adding Data Collectors (EMC XtremIO) 294
Installation overview (EMC XtremIO) 295
Add an EMC XtremIO Data Collector policy 295

Chapter 31 Configuration for FUJITSU ETERNUS Data Collector 300

About data collector 300
Pre-installation setup 301
Prerequisites for adding Data Collectors 301
Installation overview 301
Adding a FUJITSU ETERNUS Data Collector policy 302

Chapter 32 Configuration for Hitachi Block 306

Pre-Installation setup for Hitachi Block 306
Prerequisites for adding Data Collectors (Hitachi Block) 306
Installation overview (Hitachi Block Storage) 307
Adding a Hitachi Block Storage Data Collector policy 308
Configuring a Hitachi Device manager user 312
Validate the User ID access 313
Configuring a Collector for Hitachi NAS block storage 315
Adding an HP command view advanced Data Collector policy 315

Chapter 33 Configuration for Hitachi Content Platform (HCP) 316

Pre-Installation setup for Hitachi Content Platform (HCP) 316
Prerequisites for adding Data Collectors (Hitachi Content Platform) 317
Installation overview (Hitachi Content Platform) 317
Add a Hitachi Content Platform (HCP) Data Collector policy 318
Setting up permissions for an HCP local user or active directory user 322
Hitachi content platform system management console 323
Local users 323
Local users and active directory users 323
Hitachi content platform tenant management console 324
Local users 325
Active directory users 326
Local users and active directory users 326

Chapter 34 Configuration for Hitachi NAS 328

Pre-Installation setup Hitachi NAS 328
Prerequisites for adding Data Collectors (Hitachi NAS - HNAS) 328
Installation overview (Hitachi NAS - HNAS) 329
Adding a Hitachi NAS (HNAS) Data Collector policy 330
HNAS configuration requirements 330
Configuring SSC access 330
Adding the collector 331

Chapter 35 Configuration for Hitachi Vantara All-Flash and Hybrid Flash Storage 335

Pre-Installation setup for Hitachi Vantara All-Flash and Hybrid Flash Storage 335
Prerequisites for adding Data Collectors (Hitachi Vantara All-Flash and Hybrid Flash Storage) 336
Installation overview 338
Adding a Hitachi Vantara All-Flash and Hybrid Flash Storage policy 339

Chapter 36 Configuration of Host inventory 343

Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements 344
Access Requirements by OS 345
Host Inventory pre-installation setup 345
Plan host Data Collection 346
WMI Proxy requirements for Windows host Data Collection 346
Host access requirements 347
Verify command paths 348
Host Inventory configuration steps 349
Host Inventory setup overview 350
Host Inventory maintenance overview 351
Before discovering hosts 353
Configure / Search the host Inventory 353
Manage credentials 354
Manage WMI proxy 357
Manage paths 358
Manage access control 360
Host Inventory management 362
Configure host Discovery policies to populate the host Inventory 363
Discovery policy considerations 363
Configure a Discovery policy 364

Collecting from Clustered SQL server and Oracle applications 366
Execute and monitor host Discovery 368
Validate host connectivity 370
Validate hosts 370
Validation history 370
Show errors 371
Filter the host Inventory - hide / un-hide, remove 372
Host Inventory search and host Inventory export 373
Basic search 373
Pre-Defined search 373
Advanced search parameters 374
Export the host Inventory 374
Configure and edit host probes 375
Host Inventory File Analytics probe 377
File Analytics Probe configurations by operating system 377
Both Windows and Linux servers 378
Best practices for Host Inventory File Analytics probes 378
Propagate Probe Settings: Copy Probes, Paste Probes 378
Probe settings 379

Chapter 37 Configuration for HP 3PAR 385

Pre-Installation setup for HP 3PAR 385
Prerequisites for adding Data Collectors (HP 3PAR) 385
Installation Overview (HP 3PAR) 386
Adding an HP 3PAR Data Collector Policy 386
Adding an HP command view advanced Data Collector policy 392

Chapter 38 Configuration for HP EVA 393

Pre-Installation setup for HP EVA 393
Prerequisites for adding Data Collectors (HP EVA) 393
Installation overview (HP EVA) 394
Adding an HP EVA Data Collector policy 394

Chapter 39 Configuration for HPE Nimble Storage 398

Pre-Installation setup for HPE Nimble Storage 398
Prerequisites for adding Data Collectors (HPE Nimble Storage) 398
Installation overview (HPE Nimble Storage) 399
Adding an HPE Nimble Storage Data Collector policy 399

Chapter 40 Configuration for HPE StoreOnce 404

Pre-Installation setup for HPE StoreOnce 404
Prerequisites for adding Data Collectors (HPE StoreOnce) 404
Installation overview 405
Adding a HPE StoreOnce policy 405

Chapter 41 Configuration for IBM Enterprise 410

Pre-Installation setup for IBM Enterprise 410
Prerequisites for adding Data Collectors (IBM Enterprise) 410
Installation overview (IBM Enterprise) 411
Adding an IBM Enterprise Data Collector policy 412

Chapter 42 Configuration for IBM COS 416

Introduction 416
Prerequisites for adding data collectors (IBM COS) 416
Installation overview (IBM COS) 417
Add IBM COS Data Collector policy 417

Chapter 43 Configuration for IBM SVC 421

Pre-Installation setup for IBM SVC 421
Prerequisites for adding Data Collectors (IBM SVC) 421
Installation overview (IBM SVC) 422
Adding an IBM SVC Data Collector policy 422

Chapter 44 Configuration for IBM XIV 427

Pre-Installation Setup for IBM XIV 427
Prerequisites for adding Data Collectors (IBM XIV) 427
Installation overview (IBM XIV) 428
Adding an IBM XIV Data Collector policy 428

Chapter 45 Configuration for Microsoft Windows server 432

Pre-Installation setup for Microsoft Windows server 432
Prerequisites for adding Data Collectors (Microsoft Windows server) 432
Collecting from applications and services logs 433
Installation overview (Microsoft Windows Server) 434
Add a Microsoft Windows server Data Collector policy 435

Chapter 46 Configuration for NetApp-7 439

Pre-Installation setup for NetApp-7 439
Prerequisites for adding Data Collectors (NetApp-7) 439
Data Collector configurations specific to NetApp-7 440
If HTTP access is disabled on the vFiler 440
Installation overview (NetApp-7) 441
Adding a NetApp Data Collector policy 441
Testing the collection 444
Creating a NetApp user with API privileges 445

Chapter 47 Configuration for NetApp StorageGRID 446

NetApp StorageGRID overview 446
Prerequisites for adding Data Collectors (NetApp StorageGRID) 447
Data Collector configuration specific to NetApp StorageGRID 447
Installing NetApp StorageGRID 447
Adding a NetApp StorageGRID Data Collector policy 448
Testing the collection 450

Chapter 48 Configuration for NetApp Cluster 451

Pre-Installation setup for NetApp Cluster 451
Prerequisites for adding Data Collectors (NetApp Cluster) 451
Installation overview (NetApp Cluster-Mode) 452
Adding a NetApp Cluster-Mode Data Collector policy 452
Testing the collection 457
Creating a NetApp Cluster-Mode Read-Only user 457

Chapter 49 Configuration for NetApp E-Series 459

Pre-Installation setup for NetApp E-Series 459
Prerequisites for adding Data Collectors (NetApp E-Series) 459
Installation overview (NetApp E-Series) 460
Adding a NetApp E-Series Data Collector policy 460

Chapter 50 Configuration for NEC HYDRAstor 466

Introduction 466
Architecture overview 466
Supported models and versions 467
Prerequisites for adding a Data Collector 468
Installation overview 468
Adding a policy 469

Chapter 51 Configuration for Pure Storage FlashArray 473

Pre-Installation setup for pure Storage FlashArray 473
Prerequisites for adding Data Collectors (pure Storage FlashArray) 473
Installation overview (Pure storage FlashArray) 474
Add a pure storage FlashArray Data Collector policy 474

Section 4 Compute (Virtualization and Host Collection) 620

Chapter 52 Configuration for VMware 480

Pre-Installation setup for VMware 480
VMware Data Collection 480
Prerequisites for adding data collectors (VMware) 481
Virtualization Manager: Collection of VMware Data 481
Configure VMware Access 481
Installation overview (VMware) 488
Add a VMware Data Collector policy 489
Datastore scan collection 495
Reports impacted by Datastore Collection 496

Chapter 53 Configuration for IBM VIO 498

Pre-Installation setup for IBM VIO 498
Prerequisites for adding data collectors (IBM VIO) 498
Installation overview (IBM VIO) 499
Adding servers for the IBM VIO Data Collector policy 500
VIO servers (IBM Virtual I/O Servers) 500
LPAR clients (IBM Logical Partitioning Clients) managed by VIO servers 501
HMC (IBM Hardware Management Console) 501
Add an IBM VIO Data Collector policy 502

Chapter 54 Configuration for Microsoft Hyper-V 506

Pre-Installation setup for Microsoft Hyper-V 506
Prerequisites for adding data collectors (Microsoft Hyper-V) 506
Installation overview (Microsoft Hyper-V) 507
Add a Microsoft Hyper-V Data Collector policy 508

Section 5 Cloud 620

Chapter 55 Configuration for Amazon Web Services (AWS) 514

Pre-Installation setup for Amazon Web services (AWS) 514
Prerequisites for adding Data Collectors (Amazon Web services) 515
Prerequisite Amazon Web services (AWS) configurations 515
Configure an S3 bucket to receive billing reports 516
Select cost allocation tags 517
Create an AWS IAM user 518
Mandatory probe user privileges 519
For all probes 519
For independent probes 520
Link AWS accounts for Collection of consolidated billing data 523
Create a role for NetBackup IT Analytics Data Collection 523
Add the role to the IAM user 524
Installation overview (Amazon Web Services - AWS) 524
Add an Amazon Web Services (AWS) policy 525

Chapter 56 Configuration for Google Cloud Platform 531

Overview 531
Pre-installation setup for GCP 532
Prerequisites for adding Data Collectors (GCP) 532
Installation GCP 532
Adding policy 533
Testing the collection 534
Creating an IAM role 534
Billing Data Access Role 536
Cloud API 540
Project access 541

Chapter 57 Configuration for OpenStack Ceilometer 542

Pre-Installation setup for OpenStack Ceilometer 542
Prerequisites for adding Data Collectors (OpenStack Ceilometer) 542
Installation Overview (OpenStack Ceilometer) 543
Adding an OpenStack Ceilometer Data Collector policy 543

Chapter 58 Configuration for OpenStack Swift 548

Pre-Installation setup for OpenStack Swift 548
Prerequisites for adding Data Collectors (Dell compellent) 548

Installation overview (OpenStack Swift) 549
Adding an OpenStack Swift Data Collector policy 549

Chapter 59 Configuration for Microsoft Azure 553

Pre-Installation setup for Microsoft Azure 553
Setting up credentials for Microsoft Azure Data Collection 554
Install the Azure PowerShell client on a Windows computer 554
Find your tenant and subscription ID 554
Register a new application for the Data Collector 555
Create a principal and assign role to the application 556
Prerequisites for Adding Data Collectors (Microsoft Azure) 557
Installation overview (Microsoft Azure) 557
Add a Microsoft Azure Data Collector policy 558
Reconfigure an Existing Azure Role for Azure Storage Access 561

Section 6 Fabric 620

Chapter 60 Configuration for Brocade switch 564

Pre-Installation setup for Brocade switch 564
Prerequisites for adding Data Collectors (Brocade switch) 565
Upgrade troubleshooting: Brocade BNA SMI-S (CIM) server and Java 11 571
Supported switches 572
Brocade switches: Default ports and firewall considerations 572
Installation overview (Brocade switch) 573
Brocade switch Data Collector policy 573

Chapter 61 Configuration for Cisco switch 584

Pre-Installation setup for Cisco switch 584
Prerequisites for adding Data Collectors (Cisco switch) 584
Upgrade troubleshooting: Cisco DCNM SMI-S (CIM) server and Java 11 585
Cisco switches: Default ports and firewall considerations 587
Installation overview (Cisco switch) 587
Cisco switch Data Collection policy 587
Before you start Cisco switch Data Collection 591

Chapter 62 Configuration for Brocade Zone alias 592

Pre-Installation setup for Brocade zone alias 592
Prerequisites for adding Data Collectors (Brocade zone alias) 592

Brocade switches: Default ports and firewall considerations 593
Installation overview (Brocade zone alias) 594
Brocade zone alias Data Collector policy 594

Chapter 63 Configuration for Cisco Zone alias 598

Pre-Installation setup Cisco zone alias 598
Prerequisites for adding Data Collectors (Cisco zone alias) 598
Cisco switches: Default ports and firewall considerations 599
Installation overview (Cisco Zone Alias) 599
Cisco zone alias Data Collector policy 600

Section 7 File Analytics 620

Chapter 64 Configuration for File Analytics 605

Pre-Installation setup for File Analytics 605
File Analytics Data Collection overview 606
File Analytics Data Collection architecture 607
File Analytics Data Collector policies 607
Prerequisites for adding Data Collectors (File Analytics) 608
CIFS shares 608
Host Discovery and Collection File Analytics probe 609
File Analytics Probe Configurations by operating system 609
Both Windows and Linux servers 609
Best practices for host Inventory File Analytics probes 610
Adding a File Analytics Data Collector policy 610
Importing the CIFS share configuration 615
Set up FIPS compliant Data Collector for File Analytics 615

Chapter 65 File Analytics Export Folder Size and Folder Depth 617

Extracting File Analytics export folder size 617
Specifying the File Analytics folder depth 618

Section 8 Data Collection Validation and Troubleshooting 620

Chapter 66 Validate data collection 621

Validation methods 621
Data Collectors: Vendor-Specific validation methods 622

Working with on-demand Data Collection 624
View real-time logging during an on-demand collection 626
Generating debug level logs during an on-demand collection 627
Collect historic data on-demand 629
Using the CLI check install utility 631
List Data Collector configurations 633

Chapter 67 Data Collector Troubleshooting 634

Resolving Data Collectors connections issues - Linux specific 635
Resolving Data Collectors connections issues - Windows specific 636
Portal upgrade performance issues 637
Verify the Data Collector configuration 638
Verify Connectivity 638
Configuring web proxy updates 639
Collecting missed events for Veritas Backup Exec 639
Substituting ODBC for JDBC to connect to SQL server for Veritas Backup Exec 639
Useful Data Collection scripts for capacity 643
Host resources troubleshooting 645
Host resources: Check the status of the WMI proxy server 645
Host resources: Post-Installation verification 648
Host resources: Check host connectivity using standard SSH 648
Checking Paths for SSH 649
Environment setting for bash users 650
Host resources: Check host connectivity 650
Host resources: Check host connectivity using Host Resource Configuration file 651
Host resources: Generating host resource configuration files 652
Sample lines in an input file 653
Host resources: Check the execution of a command on a remote server 653
Host resources Data Collection 654
Host resources: Collection in stand-alone mode 654
Configuring parameters for SSH 655
Configure channelWaitTime 656
Configure singleChannelSession 656
Configure sudoWithPassword 656
Identifying Windows file system access errors (File Analytics) 656
Collect from remote shares (File Analytics) 657
Adding a certificate to the Java keystore 657

Chapter 68 Uninstalling the Data Collector 660

Uninstall the Data Collector on Linux 660
Uninstall the Data Collector on Windows 661

Appendix A Firewall Configuration: Default Ports 662

Firewall configuration: Default ports 662

Appendix B Load historic events 667

Introduction 667
Load Commvault Simpana events 668
Load Dell PowerProtect Data Manager jobs 669
Load EMC Avamar events 669
Load EMC NetWorker events 670
Load HP Data Protector events 671
Load IBM Spectrum Protect (TSM) events 672
Load Oracle Recovery Manager (RMAN) events 674
Load Veeam Backup & Replication events 674
Load Veritas NetBackup events 675
Load events for individual NetBackup clients 676
Load events for a group of NetBackup clients 676
Load Veritas Backup Exec events 678
Corrections in duplication of clients 679
Cohesity 680
Dell EMC NetWorker Backup & Recovery 680

Appendix C CRON Expressions for Policy and Report Schedules 687

CRON expressions for policy probe schedules 682
CRON expressions for scheduling reports 684

Appendix D Maintenance Scenarios for Message Relay Server Certificate Generation 687

Regenerate authentication certificate nearing expiry (or already expired) 687
Recover inadvertently deleted `aptare.ks` file 688
Authenticate new database with existing SSL certificates 690
SSL certificate authentication for a new data collector 691

Section 1

Introduction

- Chapter 1. Introduction
- Chapter 2. Install and configure a Data Collector
- Chapter 3. Installing the Data Collector software
- Chapter 4. Configure SSL

Chapter 1

Introduction

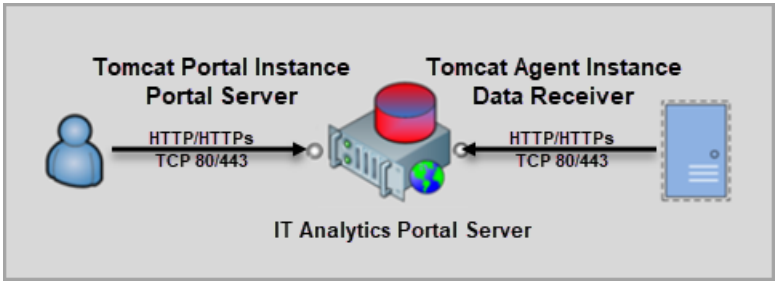
This chapter includes the following topics:

- Overview
- Distributed Data Collector (recommended for NetBackup)
- Centralized Data Collector
- Data Collector prerequisites

Overview

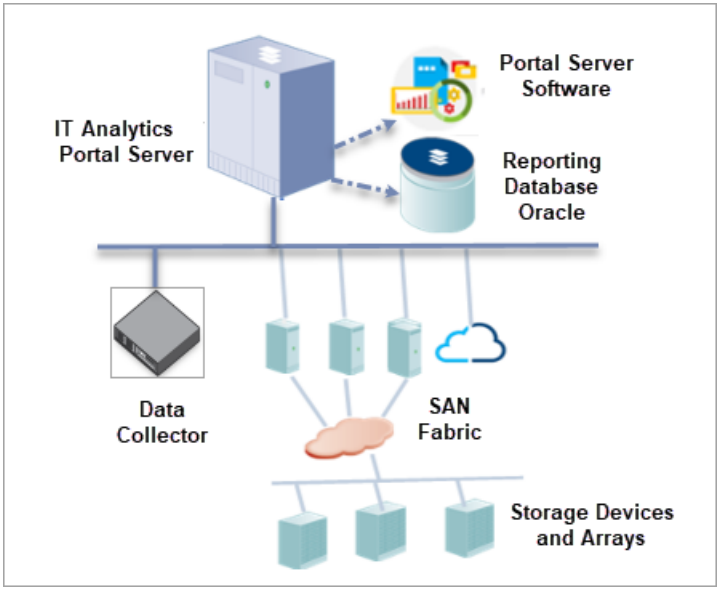
The Data Collector is a Java application responsible for interfacing with enterprise objects and gathering information from backup servers, storage arrays, cloud assets, Compute and SAN Fabric.

The Data Collector continuously collects data and sends this data, using an http or https connection, to another Java application, the Data Receiver. The Data Receiver runs on the NetBackup IT Analytics Portal server and stores the data that it receives in the Reporting Database.



When you use the Portal to generate a report, the Portal requests this information from the Reporting Database, then returns the results in one of the many available

reports. In addition to NetBackup, NetBackup IT Analytics can collect data from Veritas Backup Exec, NetBackup Appliances and Flex, third-party Data Protection vendors, Storage Arrays, SAN Fabric, and Cloud assets.



The Data Collector obtains all its monitoring rules from a Data Collector configuration file. This file resides in the Reporting Database in XML format. When the Data Collector first starts, it downloads this file from the Reporting Database. The Data Collector uses this file to determine the list of enterprise objects that are to be monitored and included in its data collection process. You must align the scope of data collection with your data collection needs.

For example, if just collecting data from NetBackup, you may opt to use the distributed Data Collector, which is installed by default on NetBackup Primary Servers. A distributed Data Collector only collects data from NetBackup.

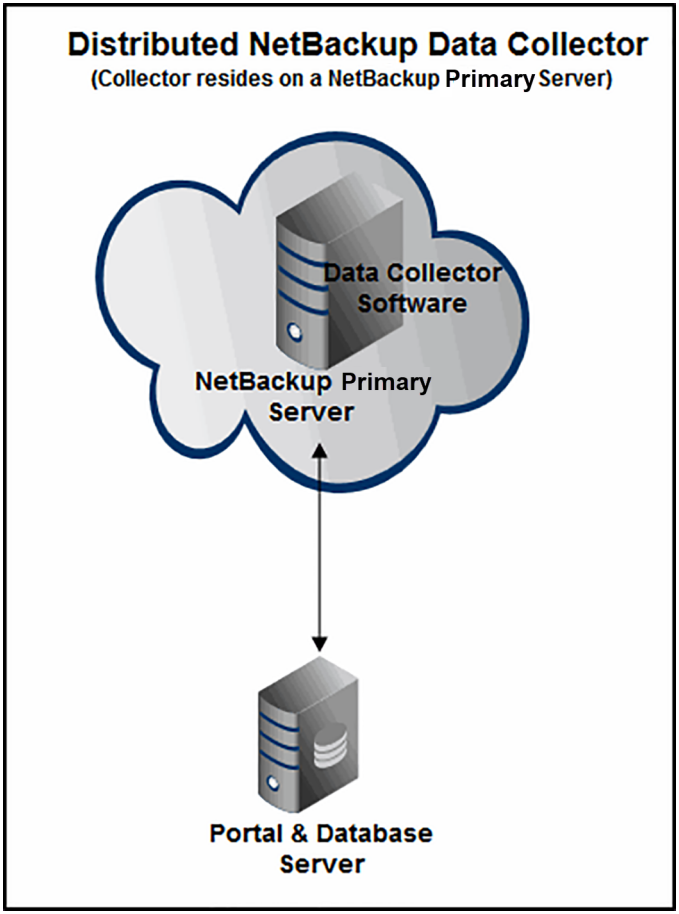
A centralized Data Collector can be used to collect data from all backup products. You can also include other enterprise objects, such as storage arrays, SAN switches, Compute and Cloud assets for a centralized Data Collector.

If you collect data from Veritas Backup Exec, third-party data protection vendors, storage arrays, SAN switches, and cloud assets, then choose a centralized Data Collector that is installed on a remote Linux or Windows Server.

Distributed Data Collector (recommended for NetBackup)

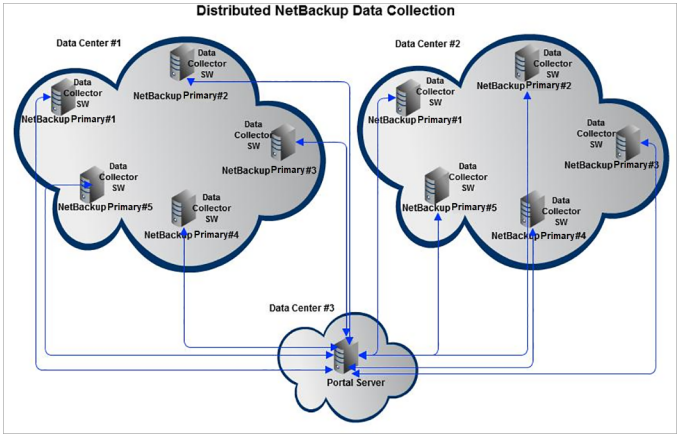
If collecting data from NetBackup, you can use a Distributed Data Collector, which is installed by default on a non-clustered NetBackup Primary Server. A Distributed Data Collector should ONLY be used to collect data from the NetBackup Primary Server and/or the appliance/Flex instance it resides on.

Figure 1-1 Example of a single primary server collection



The below figure shows multiple NetBackup Primaries with a Distributed Data Collector installed on each NetBackup Primary, across two Data Centers. The Data Collectors point back to a NetBackup IT Analytics Portal server, installed in a third Data Center.

Figure 1-2 Example of a multiple primary server collection



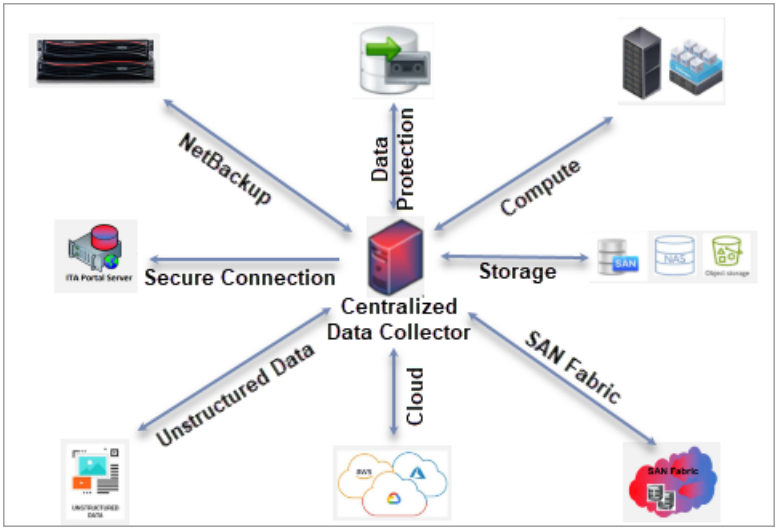
Centralized Data Collector

A centralized Data Collector can collect data from all backup products. You can also include other enterprise objects, such as storage arrays, SAN switches, Compute, and Cloud assets for a Centralized Data Collector. A centralized Data Collector resides on a separate Windows or Linux Server and remotely connects to NetBackup Primaries using Secure Shell Protocol (SSH), Windows Management Instrumentation (WMI), or via REST APIs.

If you are collecting data from Veritas Backup Exec, third-party Data Protection Vendors, Storage Arrays, SAN switches and cloud assets, then you must choose a centralized Data Collector. Note that there can be situations where you can also use a centralized Data Collector to collect from NetBackup, but Cohesity typically recommends using a distributed Data Collector for NetBackup and a centralized Data Collector for all other subsystems you are collecting the data from.

NetBackup security hardening, such as implementing Multifactor Authentication and using a non-privileged service account, adds complexity and additional configuration steps, leveraging the centralized Data Collector for NetBackup collections. There are also additional networking / firewall considerations with a centralized Data Collector for NetBackup.

You can have a mix of distributed and centralized Data Collectors. In the illustration below, a centralized Data Collector is installed in a data center and it collects data from many different subsystems.



A single instance of a centralized Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed to determine how many Data Collectors must be installed and which servers are best suited for the deployment. It is also important to understand that you might want a combination of distributed and centralized Data Collectors, particularly if you are collecting data from other third-party subsystems. A distributed Data Collector embedded by default on a NetBackup Primary Server can only be used to collect data from NetBackup or Veritas Alta Data Protection.

Whether you need to install the Data Collector software depends on the NetBackup version and whether NetBackup is clustered. For NetBackup 10.1.1 or later, the distributed Data Collector binary is already pre-installed provided it is not deployed in a clustered environment. You have the option to configure the data collector to point to NetBackup IT Analytics or Alta View. Note that from NetBackup 10.4 onwards, Data Collector is optional to install. If you are planning to use NetBackup IT Analytics or Alta View, you must opt to install Data Collector while installing/upgrading NetBackup. But if you did not install the Data Collector initially, and later decided to use Alta, then you must install it manually.

For clustered NetBackup Primary Servers or NetBackup Primary Servers on a NetBackup release prior to 10.1.1, a Data Collector is not installed by default and the Data Collector binaries must be manually installed.

Data Collector prerequisites

This list includes the general Data Collector server prerequisites. Specific requirements are listed with each supported subsystem.

- 64-bit OS.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal.
- Install only one Data Collector on a server (or OS instance).
- Verify the rpm fontconfig is installed. Fontconfig is a library designed to provide system-wide font configuration, customization and application access. If the rpm fontconfig is not installed, the installer will not be able to load User Interface Mode. This is a prerequisite for new Data Collector installations.

Chapter 2

Install and configure a Data Collector

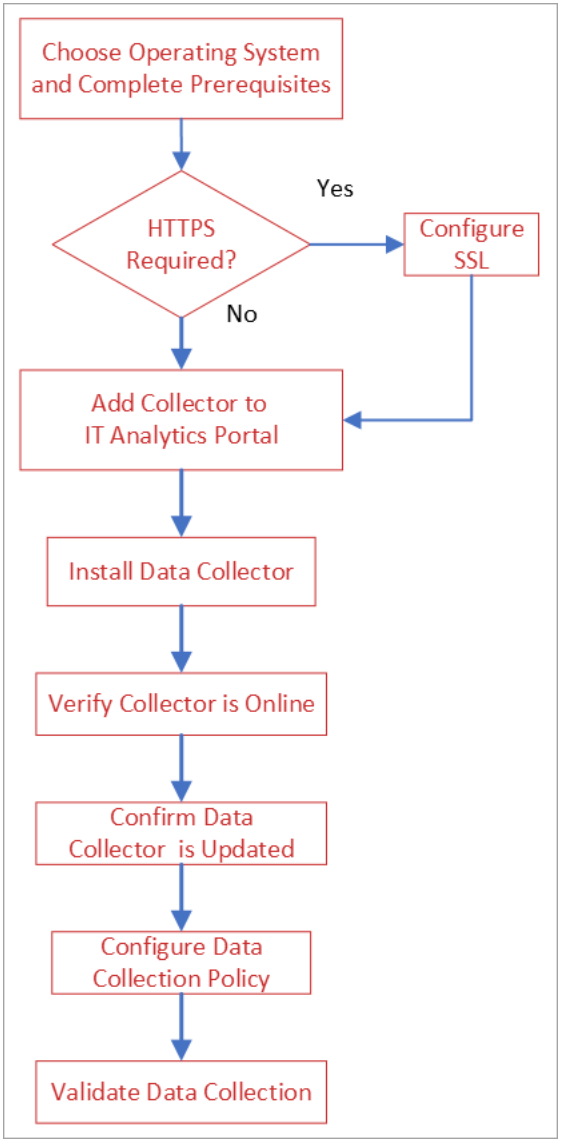
This chapter includes the following topics:

- Overview
- Step-1: Choose operating system and complete prerequisites
- Step-2: HTTPS requirement
- Step-3: Add Data Collector on NetBackup IT Analytics Portal
- Step-4: Install the Data Collector
- Step-5: Verify the Data Collector is online from the Portal
- Step-6: Confirm that the Data Collector is updated
- Step-7: Configure the data collection policy
- Step-8: Confirm that the data collection policy is collecting data

Overview

This section includes preinstallation, installation and configuration instructions for a Data Collector to be used to collect data for supported vendors in the areas of Data Protection, Storage, Cloud, Virtualization, Fabric and File Analytics. The flowchart below details the steps to install and configure a Centralized Data Collector.

Note: Do not use this guide to install and configure a Data Collector to collect data from NetBackup. For NetBackup data collection, please refer to the *NetBackup IT Analytics Data Collector Installation Guide for Cohesity NetBackup*.



Step-1: Choose operating system and complete prerequisites

Prior to deploying a Centralized Data Collector, it is important to determine which operating system to use for the Data Collector. The choices are Windows or Linux.

Things to consider include:

- If you are using the Data Collector to collect from other subsystems and applications, the operating system you select might need to be considered. For example, CommVault and Veeam Backup & Replication require a Data Collector running the Windows Operating System.

Factors impacting Data Collector performance and memory requirements

Because every environment has a unique set of resources, configured and tuned specifically for that environment, there is no one size fits all formula. Several factors can impact performance and memory requirements:

- Number of active Data Collector Policies
- Number of hosts and active probes per host
- Number and types of storage arrays
- Number of LUNs
- Polling frequency and number of devices polled
- Amount of data transmitted
- Performance of array device managers
- Number of NetBackup hosts enabled for File Analytics

Data Collector supported operating systems

Install the Data Collector on a virtual machine (VM). The following 64-bit platforms are supported:

Table 2-1 Data Collector supported operating systems

Operating System	Version
Red Hat Enterprise Linux	8 and 9
SUSE Linux Enterprise	SLES 12 SP5 and SLES 15 SP5
OEL	8 and 9
Windows Server	2016, 2019, and 2022

Data Collector server memory and CPU guidelines

Use the following guidelines for Data Collector Servers.

- Installation on a VM is recommended
- CPU: 2 - 4 CPUs
- Memory: 32 GiB minimum; If collecting from more than 40 backup servers, contact Support for recommendations.
- Installation Directory Disk Space: 200 GiB minimum; If collecting File Analytics data, an additional minimum of 300 GiB of disk space is recommended. Windows default installation directory is: C:\Program Files\Aptare. Linux default installation directory is /opt/aptare.

Additional prerequisites

- Windows Only Requirement - If a Data Collector is required to collect data from Cohesity NetBackup Primary Server running on Windows System to non-English (United States) locale:
  - A Windows user must be created with the Administrators group of Windows system that will run the data Collector with culture set to English-US, and Region and Language set to English -US.
  - The current system locale must be set to the same language as the NetBackup Primary Server.
- For performance reasons, do not install Data Collectors on the same server as the Portal.
- Install only one Data Collector on a server (or OS instance).
- For Cohesity NetBackup collection, the Data Collector server and backup server can be in different time zones.
- Uses ports 443, 1556, and 13724 WMI range of ports, Linux ssh 22
- The NetBackup Event Monitor probe, enabled on the Data Collector policy screen, uses the `nb_monitor_util` executable. This executable is installed by default for all installations. It can be found in the `/usr/openv/netbackup/bin/goodies` directory on Linux and `\Program Files\Veritas\Netbackup\bin\goodies` on Windows. The Event Monitor probe collects events generated by the `nb_monitor_util` and handles create/update/delete events for Backup Policy, Storage Unit, Storage Unit Group and Storage Lifecycle Policy.

Linux Data Collector Prerequisites: Changing the Linux Temporary Directory for Collection

NetBackup IT Analytics uses temporary files on the target server for command output. The location of the temporary files is controlled by the TMPDIR environment variable, defaulting to /tmp.

Option 1: User Profile

NetBackup IT Analytics executes commands on the target NetBackup server using a non-interactive Bourne login shell (/bin/sh -l). On most systems this means that the `/etc/profile` (when a login type of connection like ssh or scp is used) and `${HOME}/.bashrc` (when non-interactive connection like shell exec is used) files will be sourced and can be used to set the TMPDIR environment variable.

1. Log into the collection account on the target server.
2. Modify ${HOME}/.bashrc, set and export TMPDIR:

   ```
   TMPDIR=/path/to/tmp
   export TMPDIR
   ```

   For the NetBackup appliance: all CLI users share the `/home/nbusers` directory. To only change the `TMPDIR` directory for the collection user, you must first check the logged-in user. For example:

   ```
   if [ "${USER}" = "itanalytics" ] ; then
       TMPDIR=/path/to/tmp
       export TMPDIR
   fi
   ```

3. To test, run the following command and verify that it returns the configured TMPDIR:

   ```
   $ ssh <username>@127.0.0.1 '/bin/sh -l -c "echo \${TMPDIR}"'
   /path/to/tmp
   ```

   Note: There may be additional output before the TMPDIR path, for example the NBU appliance displays a banner.

Option 2: Advanced Parameter

The TMPDIR can be set either for all or a select set of target servers in a collector using the advanced parameter: NBU_SSH_TMPDIR. This value will be overridden if TMPDIR is set in the profile on the target server.

```
NBU_SSH_TMPDIR=/path/to/tm
```

Step-2: HTTPS requirement

The default NetBackup IT Analytics configuration is HTTP Port 80 between the Data Collector and the Portal and between the User's Web Browser to the Portal. If HTTP is not acceptable in your environment, you will need to configure HTTPS before proceeding. Once the Data Collection policy configuration is complete, continue to *Step 3*.

If HTTP is acceptable, continue with step 3.

See "*Configure SSL*" on page 64.

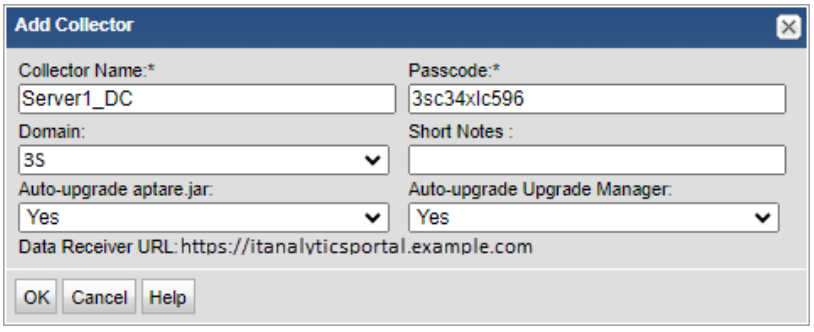
Step-3: Add Data Collector on NetBackup IT Analytics Portal

Once logged in to the Portal:

1. Select **Admin** > **Data Collection** > **Collector Administration**.
2. Click **Add Collector**.

   On the Add Collector screen, you will need to define the Collector Name, Passcode and select the IT Analytics Domain you wish to associate with the Collector and your Auto-upgrade options. Please refer to the table below for additional details regarding each field.

   Although the Data Collector name can be anything, Cohesity recommends that the Data Collector name be the hostname of the server the Data Collector software is installed on. In the example below, we use the Data Collector Server Name followed by "_DC".

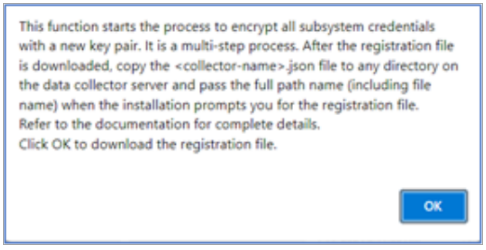


Field	Description
Collector Name*	The collector name cannot include a space and is case sensitive. The names should match exactly as entered in the Data Collector configuration screen and the Data Collector Installer screen. Edit the unique name assigned to this Data Collector. The Data Collector will use this value for authentication purposes. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made.
Passcode*	Edit the passcode assigned to this Data Collector. It can be any character sequence. Unlike other system passwords (which are encrypted and then saved) this Data Collector passcode is not encrypted prior to saving in the database and may appear as clear case in certain files. It simply is intended as a “handshake” identification between the Data Collector and the policy. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made. You can use the following OS-specific special characters in the passcode. Make sure the special characters you include are supported on the OS where the Data Collector is installed. ■ Linux: !@#%^* ■ Windows: !@#$%^&*()
Short Notes	Descriptive notes associated with this Data Collector.
Enable SSL	Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use. This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com

Field	Description
Auto-upgrade aptare.jar	Indicate if you want this configuration file upgraded automatically. This part of the Data Collector is responsible for event and metadata processing threads. The .jar file contains the processing and parsing logic for data collection. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.
Auto-upgrade Upgrade Manager	Indicate if you want this configuration bundle upgraded automatically. This Data Collector component is responsible for managing Data Collector upgrades. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

3 Click **OK**.

You will now be presented with the following message, indicating that a `.json` file has been created. This file is required when you configure and register your Data Collector.



4 Click **OK**.

Step-4: Install the Data Collector

This section assumes that you will install a NetBackup IT Analytics Data Collector 11.4 or greater, which will allow you to register the data collector using a `.json` file. When complete, resume with Step 5.

See "Step-5: Verify the Data Collector is online from the Portal" on page 38.

Step-5: Verify the Data Collector is online from the Portal

1. Login to the NetBackup IT Analytics Portal.
2. Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector is **Online**.

Step-6: Confirm that the Data Collector is updated

On the NetBackup IT Analytics Portal, go to **Admin** > **Data Collection** > **Collector Updates** and select the Data Collector for which the component needs to be upgraded.

Step-7: Configure the data collection policy

Refer to the appropriate configuration chapter of the system you are interested in collecting data from. Once the Data Collection Policy configuration is complete, continue to *Step 8*.

Step-8: Confirm that the data collection policy is collecting data

Select **Collector Administration** and confirm that the **Policy State** column is showing **Collecting**, for the collection policy, or has a green check mark under the **Status** column, indicating a successful collection. Note that you may need to **Refresh** the screen for several minutes.

Chapter 3

Installing the Data Collector software

This chapter includes the following topics:

- Introduction
- Considerations to install Data Collector on non-English systems
- Install Data Collector Software on Windows
- Install Data Collector software on Linux
- Configure Data Collector manually for Cohesity NetBackup
- Install Data Collector binaries on Windows (without configuration)
- Install Data Collector binaries on Linux host (without configuration)

Introduction

This section includes the instructions for installing the Data Collector software on the Data Collector Server. Data Collector software is supported in various flavors of Linux and Windows. On Windows, if you are collecting data from host resources, you may need to install the WMI Proxy Service. The WMI Proxy Service is installed by default, as part of the Data Collector installation on a Windows server.

A GUI based version is available for Windows and a console (command line) based interface is available for Linux.

When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

Note: Log in as a Local Administrator to have the necessary permissions for this installation.

Considerations to install Data Collector on non-English systems

This section describes the prerequisites of NetBackup IT Analytics Data Collector installation on a non-English Windows or a non-English Linux host. Apart from English, Data Collector installation is supported in the following locales, provided the Data Collector host system locale is set to any one of these languages:

- Simplified Chinese
- French
- Korean
- Japanese

After you have set one of the above as system locale, the installation progress and responses appear in the preferred locale. If the system locale is set to any other non-supported locale, the installation progress and responses appear in English.

The OS-specific requirements mentioned below.

Non-English Linux OS

On a non-English Linux host:

- The user locale can be one of the non-English supported locales if the Data Collector will collect only from a Cohesity product.
- The user locale must be English if the Data Collector will be used to collect from any non-Cohesity product.

To install the Data Collector in one of the supported locales, verify whether the host OS has multiple languages and then add the preferred locale for the installation. The procedure below guides you to set one of the supported languages as the system locale.

To set one of the supported languages as the system locale for Data Collector installation, set the preferred language as described below:

1 Check the current language.

```
#locale
```

2 Check whether your system has multiple languages:

```
#locale -a
```

3 To change the System locale into one of the supported languages, run the command `#vi /etc/profile` and add the following at the end of the file based on your preferred language:

- To add Simplified Chinese:

```
export LANG=zh_CN.utf8
export LC_ALL=zh_CN.utf8
```

- To add French:

```
export LANG=fr_FR.utf8
export LC_ALL=fr_FR.utf8
```

- To add Korean

```
export LANG=ko_KR.utf8
export LC_ALL=ko_KR.utf8
```

- To add Japanese

```
export LANG=ja_JP.utf8
export LC_ALL=ja_JP.utf8
```

4 Reboot the host to set the desired system locale for the Data Collector installation.

Having completed setting the system locale, proceed with the Data Collector installation, with the appropriate user locale.

See “Install Data Collector software on Linux” on page 52.

Non-English Windows OS

Cohesity recommends that the user locale to be set to English while installing the Data Collector on a non-English Windows host, be it for a Cohesity or a non-Cohesity product.

To verify the user locale and system locale respectively before the Data Collector installation, run the `get-culture` and `get-winsystemlocale` commands from PowerShell Windows. This way, you can decide which user locale to set for the Data Collector installation.

If you must run the Data Collector installer in one of the supported locales, ensure the Windows OS is installed in either Simplified Chinese, French, Korean, or Japanese. Avoid having Windows OS in English, installed with language pack and changing the locale later. The Data Collector installer detects the locale from the Windows Language Settings and launches the installer in the respective locale. If the Windows Time & Language Setting is set to a language other than Simplified Chinese, French, Korean, or Japanese, the installer is launched in English.

See "Install Data Collector Software on Windows" on page 42.

Install Data Collector Software on Windows

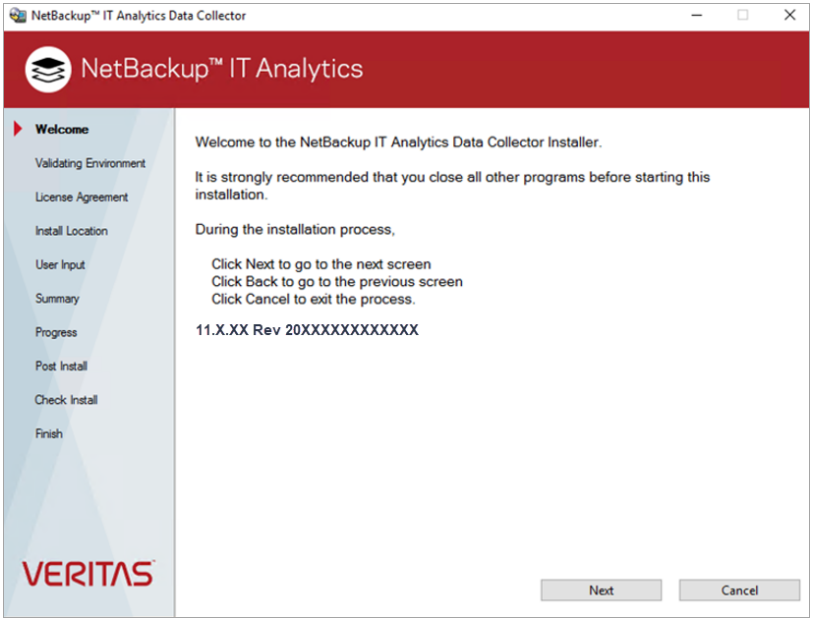
To install your Data Collector software:

1. Login to the Data Collector server as a local administrator.
2. Go to the downloads section under **Support** on *www.veritas.com* and click the relevant download link.

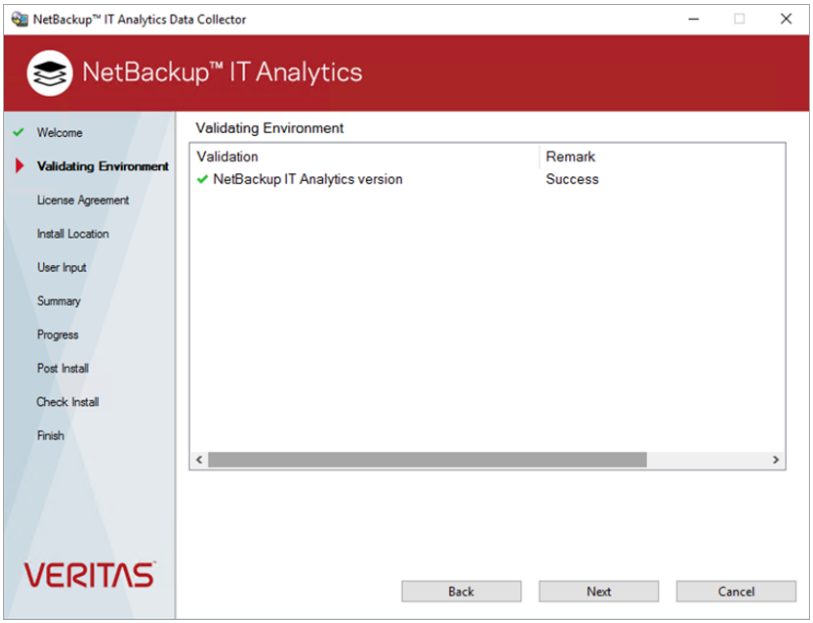
   Once, downloaded, the Data Collector Installation Wizard launches automatically. If it does not, navigate to its directory and double-click the executable file `Setup.exe`.

3 Review the recommendations on the welcome page and click **Next**.

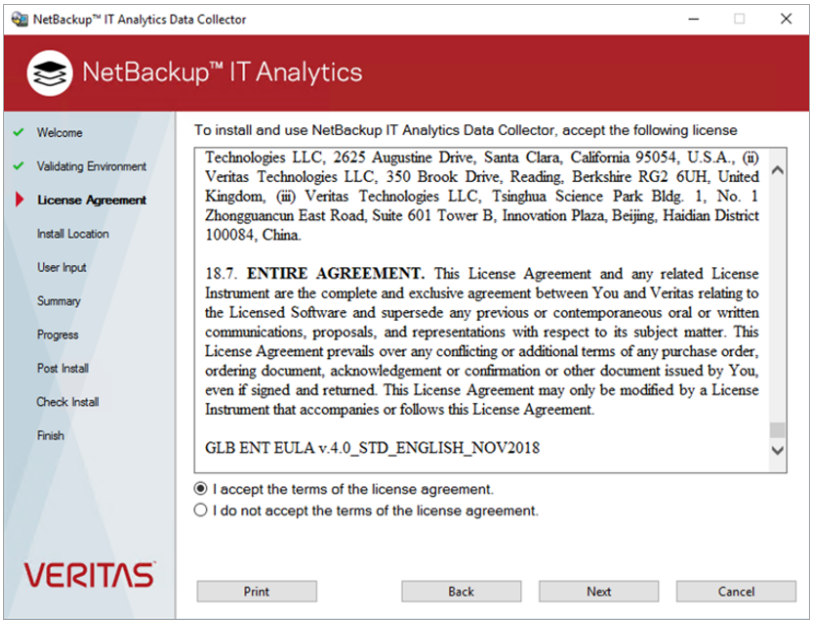
You are advised to close all other programs during this installation.



4 The installation wizard validates the system environment. On successful validation, click **Next**.

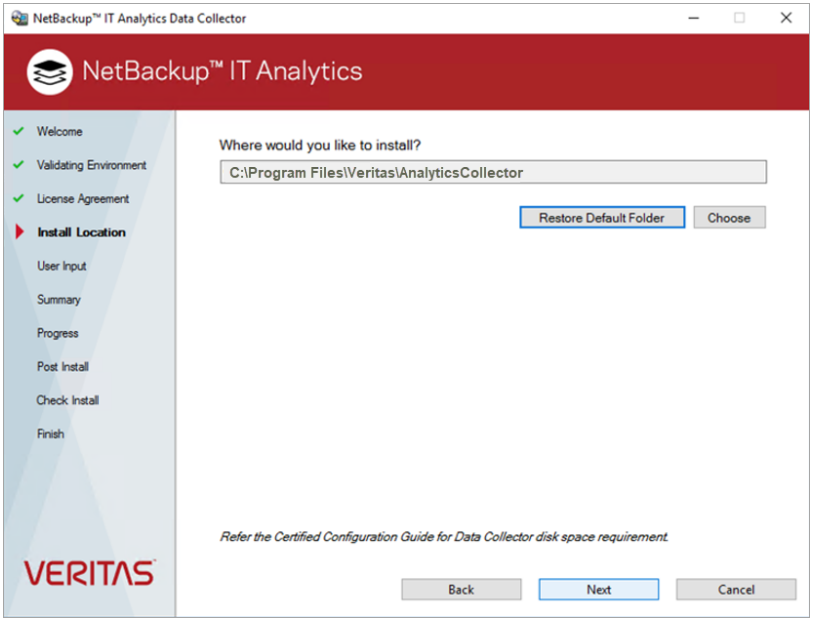


5 Review the End User License Agreement (EULA), select **I accept the terms of the license agreement**, and click **Next**.



6 Specify the directory where you would like to install the Data Collector software and click **Next**. The default Windows path is `C:\Program Files\AptareC:\Program Files\Veritas\AnalyticsCollector`. Accepting the default paths is recommended.

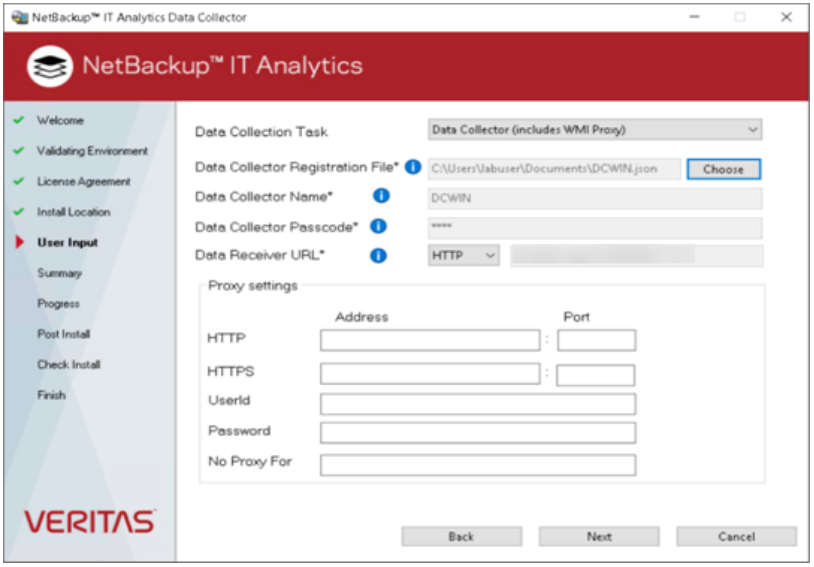
If you specify a custom directory, the install creates the `AnalyticsCollector` folder within the specified directory.



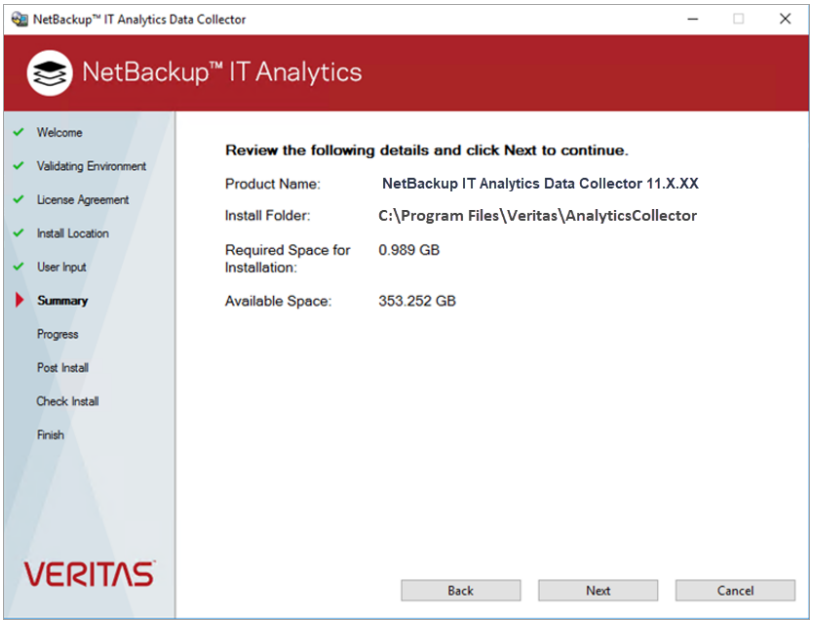
7 Provide accurate details as described below on the next page and then click **Next**.

Data Collection Task	Select **Data Collector (includes WMI Proxy)** or **WMI Proxy Server (only)** from the list. A single Data Collector can be installed for multiple vendor subsystem on a single server.

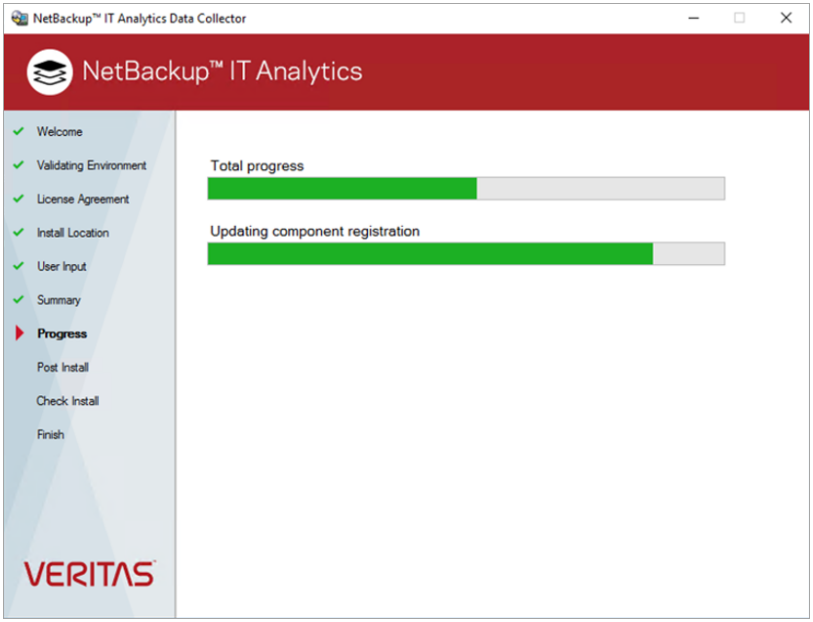
Data Collector Registration File	Enter the absolute path of the registration file downloaded from the NetBackup IT Analytics Portal. If a registration file is not available, generate and download it from the Portal and provide its path. This will auto-populate the next three fields.
Data Collector Name	Read-only and auto-populated.
Data Collector Passcode	Read-only and auto-populated.
Data Receiver URL	Read-only and auto-populated.
Proxy Settings	1 **HTTP/HTTPS**: Enter the hostname or IP address and a port number. 2 **UserId**: User ID of the proxy server. 3 **Password**: Password of the proxy server. 4 **No Proxy For**: Enter the host names or IP addresses separated by commas that will not be routed through the proxy.



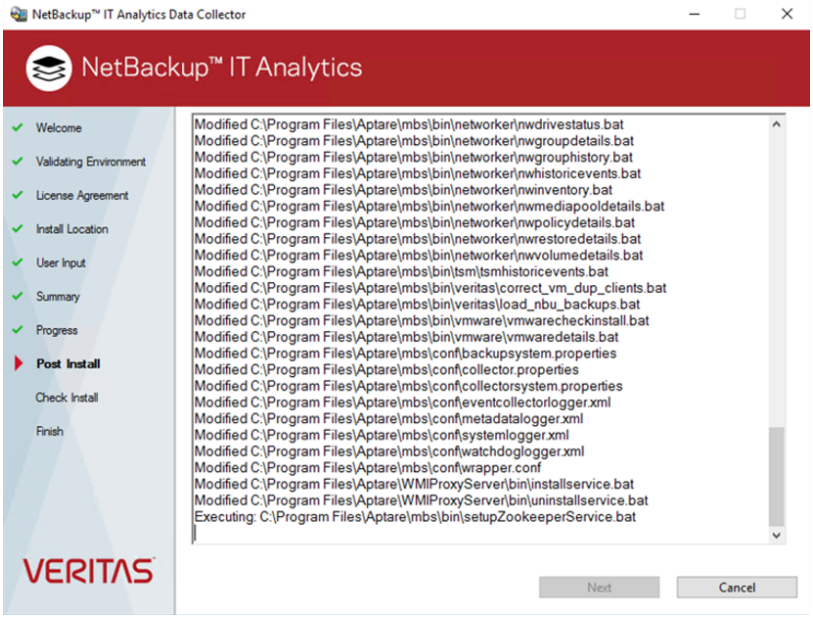
8 Review the installation summary and the available disk space before you proceed with the installation.



9 Click **Next** to initiate the installation.

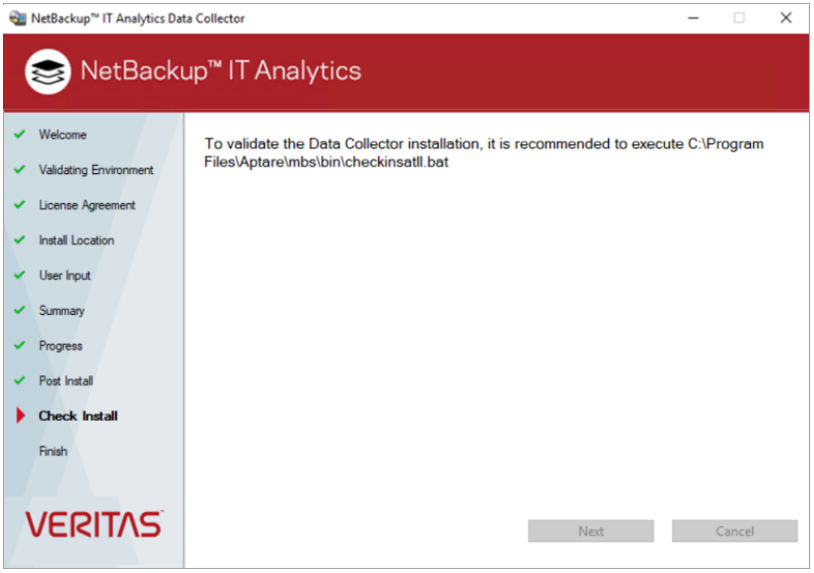


10 Review the post install details and click **Next**.

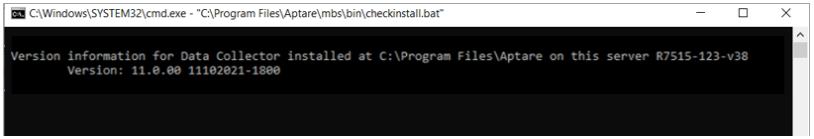


11 To validate the Data Collector installation, run the `C:\Program Files\Veritas\AnalyticsCollector\mbs\bin\checkinstall.bat` batch file.

Close the terminal window once the validation is complete and then click **Next**.

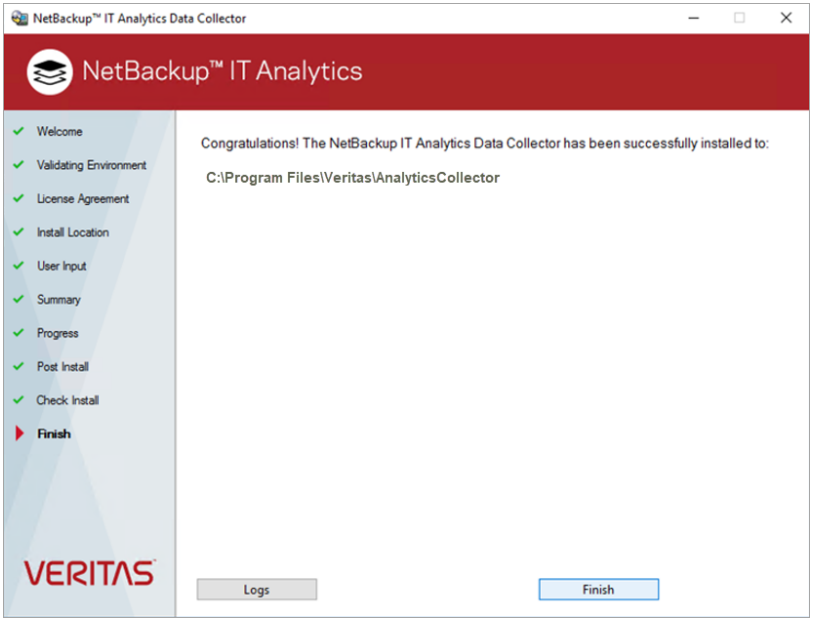


If you wish to run `checkinstall.bat` later, you can run the script from the command prompt.



12 On successful installation of NetBackup IT Analytics Data Collector, click **Finish**.

Your Data Collector installation is complete.



Install Data Collector software on Linux

To install Data Collector software on Linux:

1 Login as root on the server where NetBackup IT Analytics Data Collector has to be installed.

2 If the Data Collector system is having low entropy, it can affect the performance of cryptographic functions and such steps can take considerable amount of time to complete. You can identify the entropy level of the system from the content of the `/proc/sys/kernel/random/entropy_avail` file using command `# cat /proc/sys/kernel/random/entropy_avail`. If this value is not more than 400 consistently, install the rng-tools and start the services as described below on the data collector system.

Install the rng-tools and start the services as described below.

For RHEL or OEL:

- Access the command prompt.

- Install the rng-tools.

  ```
  yum install rng-tools
  ```

- Start the services.

  ```
  systemctl start rngd
  ```

- Enable the services.

  ```
  systemctl start rngd
  ```

For SUSE:

- Access the command prompt.
- Install the rng-tools.

  ```
  zypper install rng-tools
  ```

- Start the services.

  ```
  systemctl start rng-tools
  ```

- Enable the services.

  ```
  systemctl enable rng-tools
  ```

3 Ensure the following rpms are present on the system:

On SUSE: libXrender1 and libXtst6 insserv-compat

On other Linux systems: libXtst and libXrender chkconfig

Since the above rpms are essential for proper functioning of the Data Collector, you can run the below commands on the Data Collector server to check whether the rpms are present.

On SUSE: `rpm -q libXrender1 libXtst6 insserv-compat`

On other Linux systems: `rpm -q libXtst libXrender chkconfig`

The output of the above commands will print the rpms that are present on the system.

4 Go to the downloads section under **Support** on *www.veritas.com* and click the relevant download link.

5 Mount the ISO image that you downloaded.

```
mkdir /mnt/diska
mount -o loop <itanalytics_datacollector_linux_xxxxx.iso>
/mnt/diska
```

Substitute the name of the ISO image downloaded have downloaded.

6 Start the installer:

```
cd /
/mnt/diska/dc_installer.sh
```

7 Review the End User License Agreement (EULA) and enter **accept** to agree.

8 Provide the install location. The default location is `/usr/openv/analyticscollector`. Accepting the default paths is recommended.

If you specify a custom location, `analyticscollector` directory is created at the specified location.

9 The installer requests for the following details.

- **Data Collector Registration File Path**: Enter the absolute file path of the registration file generated and downloaded from the NetBackup IT Analytics Portal.
- Web Proxy (HTTP) settings can be configured. Enter **y** to configure proxy. The installer prompts for:
  - **HTTP Proxy IP Address**: Enter the hostname or IP address and a port number.
  - **HTTP Proxy Port**: Enter the proxy port number for HTTP proxy.
  - **Proxy UserId and password**: Enter the credentials for the proxy server.
  - **No Proxy For**: Enter the host names or IP addresses separated by commas that will not be routed through the proxy.

The Data Collector installation is complete. You can run the `<Data_Collector_Install_Location>/analyticscollector/mbs/bin/checkinstall.sh` file for verification.

Configure Data Collector manually for Cohesity NetBackup

From NetBackup version 10.1.1 onwards, Cohesity NetBackup primary server installation will also deploy NetBackup IT Analytics Data Collector binaries automatically on Windows (`C:\Program Files\Veritas\AnalyticsCollector`) and Linux (`/usr/openv/analyticscollector`) system. Also, if Cohesity NetBackup primary server is managed under Cohesity Alta, the NetBackup IT Analytics Data Collector will be automatically configured with NetBackup IT Analytics Portal.

This procedure provides the manual steps to configure the Data Collector for Cohesity NetBackup when Cohesity NetBackup primary is not managed under Cohesity Alta. Note that NetBackup IT Analytics Portal must be already installed in your data center and a Data Collector entry must be added via the **Collector Administration** screen of the portal for each NetBackup primary server before you perform this configuration.

Keep the registration file path (generated while creating the data collector on the Portal and copied to the NetBackup primary server) handy when you configure the Data Collector.

See *Add/Edit Data Collectors* section in the *NetBackup IT Analytics User Guide* for more information.

To configure the Data Collector manually on Windows:

1. Use the `responsefile.cmd` received through the installer media for this configuration. You can configure it as described in the steps below.
2. Edit the responsefile as a batch script `responsefile.cmd` with the following contents. You can also create one if required with the following content. These are the responses to the user input required to configure the Data Collector:

```
SET DATACOLLECTOR_REGISTRATION_FILE_PATH=<path to the .json file>
SET HTTP_PROXY_CONF=N
SET PROXY_HTTP_URL=
SET PROXY_HTTP_PORT=
SET PROXY_HTTPS_URL=
SET PROXY_HTTPS_PORT=
SET PROXY_USERID=
SET PROXY_PASSWORD=
SET PROXY_NOT_FOR=
```

3. Run the command:

```
"C:\ProgramData\Veritas\NetBackup IT Analytics\DC\configure.cmd"
 /RESPFILE:<response_file_path> /INSTALL_TYPE:CONFIG
```

To configure the Data Collector manually on Linux:

1. Use the sample `responsefile.cmd` available on the install media and also available at the `<Data Collector install location>/installer path` on the system for this configuration. You can configure it as described in the steps below.
2. Update the response file with the following contents. You can also create one if required with the following content.

```
COLLECTOR_REGISTRATION_PATH=<path to the json file>
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

3 Update the value for each field with appropriate data.

A sample responsefile is available on the install media as well as the `<Data collector install location>/installer path` on the system.

4 Run any one of the following command:

```
<Install media>/dc_installer.sh -c <responsefile path>
```

Or

```
<install location>/installer/dc_installer.sh -c <responsefile path>
```

Install Data Collector binaries on Windows (without configuration)

This Data Collector installation allows you to install the collector independent of the portal software installation. The collector remains disconnected from the portal until you configure it using a response file, that contains credentials of the Data Collector created on the NetBackup IT Analytics Portal and the data receiver.

Install the Data Collector

To install a Data Collector:

1 Download and mount the Data Collector installer ISO file.

2 Install the Data Collector using `silentinstall.cmd` and follow the installation prompt.

You can install the Data Collector in the following options:

- Install at default location:

```
<ISO_MOUNT_DRIVE>:\silentinstall.cmd /INSTALL_TYPE:INSTALL
```

- Install at custom location:

```
<ISO_MOUNT_DRIVE>:\silentinstall.cmd /INSTALL_PATH:<custom location for dc installation> /INSTALL_TYPE:INSTALL
```

The independent Data Collector installation is complete.

Configure the Data Collector using responsefile

A sample responsefile is saved when you install the Data Collector. To connect the Data Collector with the NetBackup IT Analytics Portal, you must configure its

responsefile with the credentials of the Data Collector created on the portal and run a configuration command as described in the procedure below.

To configure the Data Collector:

1 Obtain the following details from the NetBackup IT Analytics Portal:

- Registration file downloaded from the Portal.

- Proxy server configuration details

2 Update the `responseFile.cmd` with the above values.

```
@ECHO OFF
REM -----------------------------------------------
SET DATACOLLECTOR_REGISTRATION_FILE_PATH=
REM -----------------------------------------------
REM  Description: Enter the Data Collector's Key File path. The
file path must include name of the file that was downloaded from
 the Portal.
REM  Valid input values: Absolute path of key file
REM  Required: True

REM -----------------------------------------------
SET HTTP_PROXY_CONF=N
REM -----------------------------------------------
REM  Description: It indicate whether proxy should be configured
 or not
REM  Valid input values: Y,N
REM  Default value: N

REM -----------------------------------------------
SET PROXY_HTTP_URL=
REM -----------------------------------------------
REM  Description: IP/hostname for HTTP Proxy
REM  Valid input values: 10.20.30.40, localhost

REM -----------------------------------------------
SET PROXY_HTTP_PORT=
REM -----------------------------------------------
REM  Description: Port for HTTP proxy
REM  Valid input values: Any number between 0 and 65535

REM -----------------------------------------------
SET PROXY_HTTPS_URL=
REM -----------------------------------------------
REM  Description: IP/hostname for HTTPS Proxy
REM  Valid input values: 10.20.30.40, localhost

REM -----------------------------------------------
SET PROXY_HTTPS_PORT=
REM -----------------------------------------------
REM  Description: Port for HTTPS proxy
REM  Valid input values: Any number between 0 and 65535
```

```
REM -------------------------------------------------
SET PROXY_USERID=
REM -------------------------------------------------
REM  Description: Proxy UserId
REM  Default value:

REM -------------------------------------------------
SET PROXY_PASSWORD=
REM -------------------------------------------------
REM  Description: Proxy user password
REM  Default value:

REM -------------------------------------------------
SET PROXY_NOT_FOR=
REM -------------------------------------------------
REM  Description: List of IP/hostname which should be excluded
for proxy
REM  Default value:
```

The Data Collector installation without connecting it with the portal is complete

Configure the Data Collector using responsefile from command prompt

To configure the installation, run the below command from command prompt:

```
<ISO_MOUNT_DRIVE>:\silentinstall.cmd /RESPFILE:<responsefile_path>
/INSTALL_PATH:<Data_Collector_installation_path> /INSTALL_TYPE:CONFIG
```

or

```
<INATALL_PATH>\DC\configure.cmd" /RESPFILE:<response_file_path>
/INSTALL_TYPE:CONFIG
```

Uninstall Data Collector

Remove the Data Collector installation from **Control Panel** > **Add and Remove Programs** menu.

Install Data Collector binaries on Linux host (without configuration)

This installation allows you to install the Data Collector independent of the portal software installation. The collector remains disconnected from the portal until you configure it using a response file, that contains credentials of the Data Collector created on the NetBackup IT Analytics Portal and the data receiver.

To install a Data Collector:

1. Download and mount the Data Collector installer `itanalytics_datacollector_linux_<version>.iso`.

   ```
   #  mount -o loop <ISO file path> <path to mount>
   ```

2. Install the Data Collector at a custom location.

   ```
   # <path to mount>/dc_installer.sh -i <user selected path>
   ```

   Example:

   ```
   # <path to mount>/dc_installer.sh -i /usr/openv -n
   ```

Configure the Data Collector using response file

A sample response file is saved when you install the Data Collector. To connect the Data Collector with the NetBackup IT Analytics Portal, you must configure its responsefile with the credentials of the Data Collector created on the portal and run a configuration command as described in the procedure below.

To configure the Data Collector:

1. Obtain the following details from the NetBackup IT Analytics Portal:
   - Registration file downloaded from the Portal.

- Proxy server configuration details

2 Update the above values in the `responsefile.sample`.

```
COLLECTOR_REGISTRATION_PATH=<path to the .json file>
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

3 Configure the data collector using the above response file.

```
# <path to mount>/dc_installer.sh -c  <responsefile path>
```

or

```
<install location>/installer/ dc_installer.sh -c  <responsefile
path>{}
```

4 Start the data collector service

```
# <install location>/mbs/bin/aptare_agent start
```

Uninstall Data Collector

Run this command to uninstall the Data Collector.

```
<INSTALL_PATH>/UninstallerData/uninstall_dc.sh -r
```

Chapter 4

Configure SSL

This chapter includes the following topics:

- SSL/TLS certificate configuration
- SSL implementation overview
- Obtain an SSL certificate
- Update the web server configuration to enable SSL on the Portal server
- Enable / Disable SSL for a Data Collector
- Enable / Disable SSL for emailed reports
- Test and troubleshoot SSL configurations
- Keystore file locations on the Data Collector server
- Import a certificate into the Data Collector Java keystore
- Keystore on the portal server
- Add a virtual interface to a Linux server
- Add a virtual / secondary IP address on Windows

SSL/TLS certificate configuration

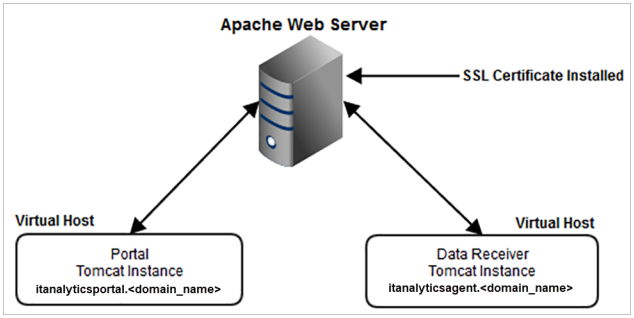
The following sections use the legacy and familiar reference to the Secure Socket Layer (SSL) protocol within NetBackup IT Analytics. In reality, the NetBackup IT Analytics communications are configured to utilize the newer and much more secure TLS (Transport Layer Security) protocols. This document retains the familiar “SSL” terminology. In addition to SSL/TLS configuration details, this section provides (optional) instructions to create a self-signed certificate and to (optionally) add a virtual interface to the portal server.

While these instructions have been validated, there are many variations in the method used to implement SSL. This document is meant only as a guide to one implementation approach and it may not be applicable in all situations.

Note: While directions for generating a self-signed certificate are provided in this documentation, Cohesity recommends the use of a certificate issued by a certificate authority (CA) rather than using a self-signed certificate. When self-signed certificates are used, it requires the additional step of copying and registering the self-signed certificate on every Data Collector.

SSL implementation overview

The Secure Socket Layer (SSL) protocol enables corporations to leverage standards-based security to protect and encrypt traffic between the NetBackup IT Analytics Portal, the Data Collector, and the client browser. The following diagram illustrates how SSL is implemented for NetBackup IT Analytics. The Apache Web Server typically resides on the Portal Server.



Note: The majority of customers that choose to utilize https connection to their portal utilize a single IP address on the Portal server, providing secured connections to both the Portal user interface and data receiver. In these configurations, a single certificate configured for Subject Alternative names protects both the URLs.

Implementing SSL involves these main tasks:

- See “Obtain an SSL certificate” on page 66.
- See “Update the web server configuration to enable SSL on the Portal server” on page 67.
- See “Enable / Disable SSL for a Data Collector” on page 72.

- See "Enable / Disable SSL for emailed reports" on page 72.

Obtain an SSL certificate

Obtain a third-party certificate from a certificate authority (CA) such as VeriSign, Thawte, or GeoTrust. The methods for obtaining a certificate vary. Therefore, refer to the vendor's web site for specific instructions.

You may, for testing purposes or as a permanent solution, use a self-signed certificate. This is not recommended as it makes the implementation slightly more complex and may limit access to NetBackup IT Analytics to some of your users.

The following outlines the process for creating a Subject Alternative Name (the certificate covers more than one hostname under a single certificate) self-signed certificate on a Linux operating system. Steps will be similar on Windows. This certificate secures communication for both the portal and data receiver web instances.

```
cd /tmp


vi san.cnf
```

Sample `san.cnf` file – use this faile as a template and modify this for your environment. The `san.cnf` file will be an input parameter during certificate generation. Note the use of an example domain name of `example.com`; change this to own your environment's domain name.

Under the v3 section, in addition to the portal name, also provision the data receiver under this same certificate.

```
[ req ]
default_bits = 4096
prompt = no
default_md = sha256
distinguished_name = req_distinguished_name
x509_extensions = v3_req

[ req_distinguished_name ]
C = US
ST = New York
L = New York City
O = Veritas
OU = ITA
emailAddress = aReal.emailaddress@yourdomain.com
CN = itanalyticsportal.example.com
```

```
[ v3_req ]
subjectAltName = @alternate_names

[alternate_names]
DNS.1 = itanalyticsportal.example.com
DNS.2 = itanalyticsagent.example.com
```

Generate Certificate using the `san.cnf` file created above

The following command results in the private key name of server.key, and certificate name of server.crt. These names will be used through the remainder of this chapter. You are free to use different names for the certificate and private key files if desired. With this command, we are also creating a self-signed certificate for 3650 days, or 10 years.

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -nodes -keyout
 server.key -out server.crt -config /tmp/san.cnf

Generating a RSA private key
.....................................++++
```



```
writing new private key to 'server.key'
-----
 tmp]# ll
total 276
-rwxrwxrwx 1 root   root      513 Dec 11 01:03 san.cnf
-rw-r--r-- 1 root   root     2187 Dec 11 01:25 server.crt
-rw------ 1 root   root     3272 Dec 11 01:25 server.key
```

Update the web server configuration to enable SSL on the Portal server

These instructions apply to Apache version 2.4.xx and the steps should be taken on the designated Web server (the Portal server). the path mentioned in the sample commands assumes default installation path on Linux and Windows.

1. Create the directory where the certificate and private key files will be located on the portal. Use the `chmod` command to ensure that only the root account

can make changes to this folder as both the key file and certificate will be installed in this folder.

- On Linux: Use the `chmod` command to ensure that only the root account can make changes to this folder as both the key file and certificate will be installed in this folder.
  Example:

  ```
  # cd /opt/apache/conf/
  # mkdir ssl_cert
  # chmod 744 ssl_cert/
  ```

- On Windows: Create folder `ssl_cert` inside `C:\opt\apache\conf\`.

2. Copy the certificate files, typically generated via a certificate authority (CA), to a folder in the Web server's Apache configuration folder.

   Linux:

   ```
   cp -p server.* /opt/apache/conf/ssl_cert/
   ```

   Windows:

   ```
   C:\opt\apache\conf\ssl_cert
   ```

   Note: Configuration files shipped with NetBackup IT Analytics licensed modules may use path names with recommended folder names. To use folders with different names, be sure to update all references to the recommended name in the default configuration files.

3. Stop the Apache and Tomcat services. From a terminal console, enter the following commands.

   Linux

   ```
   /opt/aptare/bin/tomcat-agent stop
   /opt/aptare/bin/tomcat-portal stop
   /opt/aptare/bin/apache stop
   ```

   Windows

   ```
   C:\opt\aptare\utils\stopagent.bat
   C:\opt\aptare\utils\stopportal.bat
   C:\opt\aptare\utils\stopapache.bat
   ```

4. Make a copy of the `httpd.conf` file.

Linux:

```
cp -p /opt/apache/conf/httpd.conf
/opt/apache/conf/original-httpd.conf
```

Windows:

```
Copy C:\opt\apache\conf\httpd.conf as
C:\opt\apache\conf\original-httpd.conf
```

5. Update the Apache configuration file `httpd.conf` to enable SSL.

   Linux: `/opt/apache/conf/httpd.conf`

   Windows: `C:\opt\apache\conf\httpd.conf`

   Un-comment the following lines by removing the highlighted # character.

   ```
   #LoadModule ssl_module modules/mod_ssl.so
   #Include conf/extra/httpd-ssl.conf
   ```

6. When configuring SSL on a Portal server, it is recommended to either disable http or redirect http protocol traffic to https.

   - To disable all http protocol connections, edit `httpd.conf` file and remove the VirtualHost sections.
   - To redirect all connection attempts on the http protocol to the Portal user interface, edit `httpd.conf` file, remove all entries of VirtualHost section of portal configuration and add following lines in same VirtualHost section:

     ```
     ServerName   itanalyticsportal.<domainname>
     Redirect permanent / https://itanalyticsportal.<domainname>/

     IF WILLING TO HAVE INITIAL CONNECTIONS BE ANSWERED using HTTP,
      but redirecting that traffic to HTTPS:
     ServerName   itanalyticsagent.<domainname>
     Redirect permanent / https://itanalyticsagent.<domainname>/
     ```

7. Make a copy of the `http-ssl.conf` file.

   Linux:

   ```
   cp -p /opt/apache/conf/extra/httpd-ssl.conf
   /opt/apache/conf/extra/original-httpd-ssl.conf
   ```

   Windows:

```
Copy C:\opt\apache\conf\extra\httpd-ssl.conf as
C:\opt\apache\conf\extra\original-httpd-ssl.conf
```

8. Update the Apache SSL configuration file.

   Linux: `/opt/apache/conf/extra/httpd-ssl.conf`

   Windows: `C:\opt\apache\conf\extra\httpd-ssl.conf`

9. For each active virtual host section in the Apache SSL configuration file (`httpd-ssl.conf`), ensure that declaration lines beginning with the following are un-commented (they do not have a # at the beginning of the line), and adjust the SSLCertificateFile and SSLCertificateKeyFile sections to point to the respective certificate and private key files referenced in Step 2.

   ```
   SSLCertificateFile <Provide the path of SSL certificate file>
   SSLCertificateKeyFile <Provide the path of SSL key file>
   ```

   Example:

   ```
   SSLCertificateFile /opt/apache/conf/ssl_cert/server.crt
   SSLCertificateKeyFile <Provide the path of SSL key file>
   /opt/apache/conf/ssl_cert/server.key
   ```

   Note: If you have a CA issued certificate, ensure you add the `SSLCertificateChainFile < Provide the path of Certificate chain file >` entry uncommented in `httpd-ssl.conf`.

10. Run the `deployCert` utility as root user on the Portal server to save the SSL certificates configured with Apache in java keystore `itanalytics.jks`.

    Use this as a prerequisite to configure single sign-on and syslog over SSL.

    - Linux portal command location: `/opt/aptare/utils/deployCert.sh update`
    - Windows portal command location: `C:\opt\aptare\utils>deployCert.bat update`

11. Linux only: Verify the Apache configuration is valid.

    ```
    # export LD_LIBRARY_PATH=/opt/apache/ssl/lib:$LD_LIBRARY_PATH
    # /opt/apache/bin/apachectl -t
    ```

    If this message occurs:

```
  httpd: Syntax error on line 23 of /opt/apache/conf/httpd.conf:
 Cannot load modules/mod_ssl.so into server: libssl.so.1.0.0:
cannot open shared object file: No such file or directory.
```

Resolve Syntax Error by linking libraries:

```
cd /usr/lib
# ln -s /opt/apache/ssl/lib/libssl.so.1.0.0 libssl.so.1.0.0
# ln -s /opt/apache/ssl/lib/libcrypto.so.1.0.0 libcrypto.so.1.0.0
```

12. Change the application URL in `portal.properties` to https instead of http. The `portal.properties` file is located here:

    Linux: `/opt/aptare/portalconf/portal.properties`

    Windows: `C:\opt\aptare\portalconf\portal.properties`

13. Start Apache and both Tomcat (Portal and Data Collector) services.

    Linux

    ```
    /opt/aptare/bin/apache start
    /opt/aptare/bin/tomcat-portal start
    /opt/aptare/bin/tomcat-agent start
    ```

    Windows

    ```
    C:\opt\aptare\utils\startapache.bat
    C:\opt\aptare\utils\startagent.bat
    C:\opt\aptare\utils\startportal.bat
    ```

Configure virtual hosts for Portal and / or Data Collector SSL

Refer to the following sections in the *NetBackup IT Analytics Administrator Guide* that are relevant for your environment. The instructions above accomplish SSL Implementation for Both the Portal and Data Collection.

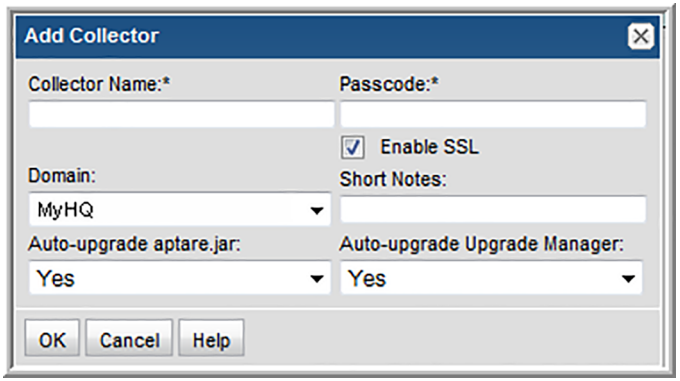
- *SSL Implementation for the Portal only*
- *SSL Implementation for data collection only*
- *SSL Implementation for both portal and data collection*

Enable / Disable SSL for a Data Collector

Once you globally configure SSL, you can change the settings for individual Data Collectors. This provides the capability of supporting a mix of both http and https among your Data Collector servers.

To enable and disable SSL for a specific Data Collector:

1. In the NetBackup IT Analytics Portal, navigate to **Admin** > **Data Collection** > **Collector Administration**.
2. Double-click a Data Collector to view the existing settings or click **Add** to add a Data Collector.



3. Check the **Enable SSL** checkbox.

   Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use.

   This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com
4. Click **OK** to save the setting.

Enable / Disable SSL for emailed reports

When emailing reports, an Add a Live Link option provides the capability of having a hyperlink (View this report in the Portal) in the email to take the user directly to the Portal. In environments where SSL is enabled, a configuration change is required in the portal.properties file to ensure that this link is secure.

Linux: `/opt/aptare/portalconf/portal.properties`

Windows: `C:\opt\aptare\portalconf\portal.properties`

1. In the `portal.properties` file, find the following section and update the value portal.application URL to replace http with https.

   Example:

   ```
   #The Portal environment
   portal.sessionTimeout=3600
   portal.applicationUrl=https://itanalyticsportal.<domainname>
   ```

2. Restart the Portal service.

Test and troubleshoot SSL configurations

The following sections cover common configuration for testing and troubleshooting.

Note: If the URLs for the portal UI and the data receiver are not published in DNS, entries will be required in the hosts file of the server attempting connection.

Test if SSL is set up for the Portal

1. Enter `https://itanalyticsportal.<domainname>/` in a browser.

   The Portal login page should display.

Test if SSL is set up for Data Collection

1. Enter `https://itanalyticsportal.<domainname>/` in a browser. The following should display: Cohesity NetBackup IT Analytics Data Receiver.
2. Enter `https://itanalyticsportal.<domainname>/servlet/util/`in a browser.

   The error message, **GET not SUPPORTED. Illegal Operation!!!**, must be displayed.

If a self-signed certificate is used, configure the Data Collector to trust the certificate. In cases where the certificate authority (CA) is not trusted, as may be the case when using a self-signed or unknown certificate, both the Data Collector and the Upgrade Manager will need to have the certificate imported into the keystore to ensure that the Data Collector can communicate using SSL.

Keystore file locations on the Data Collector server

If you are not running the Data Collector installer from the default collector location for an upgrade (`/opt/aptare` or `C:\Program Files\Aptare`) or for a fresh installation (`/usr/openv/analyticscollector/` or `C:\Program Files\Veritas\AnalyticsCollector`), substitute the appropriate path for <APTARE_HOME> in the command path in the following commands:

- Linux Data Collector: `<APTARE_HOME>/java/lib/security/cacerts`
- Windows Data Collector: `<APTARE_HOME>\java\lib\security\cacerts`
- Linux Upgrade Manager: `<APTARE_HOME>/upgrade/upgradeManager/jre/lib/security/cacerts`
- Windows Upgrade Manager: `<APTARE_HOME>\upgrade\upgradeManager\jre\lib\security\cacerts`

See "Import a certificate into the Data Collector Java keystore" on page 74.

Import a certificate into the Data Collector Java keystore

Use the following steps to add an SSL certificate to the Java keystore for a Data Collector. Some servers, such as vSphere, require a certificate for connection while communicating with SSL.

See "Keystore file locations on the Data Collector server" on page 74.

1. Copy the certificate file (server.crt file) to the Data Collector.
2. If you are not running the Data Collector installer from the default collector location for an upgrade (`/opt/aptare` or `C:\Program Files\Aptare`) or for a fresh installation (`/usr/openv/analyticscollector/` or `C:\Program Files\Veritas\AnalyticsCollector`), substitute the appropriate path for <APTARE_HOME> in the command path in the following commands:

   Linux:

   ```
   <APTARE_HOME>/java/bin/keytool -importcert -alias "somealias"
   -file server.crt -keystore <APTARE_HOME>/java/lib/security/cacerts
   <APTARE_HOME>/java/bin/keytool -import -alias "somealias" -file
   server.crt -keystore
   <APTARE_HOME>/upgrade/upgradeManager/jre/lib/security/cacerts
   ```

Windows:

```
"<APTARE_HOME>\java\bin\keytool" -importcert -alias "somealias"
-file server.crt -keystore
"<APTARE_HOME>\java\lib\security\cacerts"
"<APTARE_HOME>\java\bin\keytool" -import -alias "somealias" -file
 server.crt -keystore
"<APTARE_HOME>\upgrade\upgradeManager\jre\lib\security\cacerts"
```

3. When prompted, enter the default password to the keystore:

   ```
   changeit
   ```

   The results will be similar to the following example:

   ```
   Enter keystore password:
   ......
   Certificate Shown here
   ......
   Trust this certificate? [no]: yes
   ```

4. Once completed, run the following **keytool** command to view a list of certificates from the keystore and confirm that the certificate was successfully added. The certificate fingerprint line displays with the alias name used during the import.

   Linux:

   ```
   <APTARE_HOME>/java/bin/keytool -list -keystore
   <APTARE_HOME>/java/lib/security/cacerts
   ```

   Windows:

   ```
   "<APTARE_HOME>\java\bin\keytool" -list -keystore
   "<APTARE_HOME>\java\lib\security\cacerts"
   ```

   Sample Linux Output

   ```
   Enter keystore password:
   Keystore type: JKS
   Keystore provider: SUN
   Your keystore contains 79 entries
   digicertassuredidrootca, Apr 16, 2008, trustedCertEntry,
   Certificate fingerprint (SHA1):
   05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
   trustcenterclass2caii, Apr 29, 2008, trustedCertEntry,
   Certificate fingerprint (SHA1):
   ```

```
AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
.....
```

Keystore on the portal server

A separate keystore is used on the Portal Server to store and manage certificates when SSL is enabled. Use the Keystore Utility (deployCert) to manage your SSL certificate on the Portal Server. This utility is only needed when the portal is configured for https. Using the utility you can:

- Add the certificate
- Update the certificate
- Download the certificate from the keystore.

The utility is located here:

- linux: /opt/aptare/utils/deployCert.sh
- windows: C:\opt\aptare\utils\deployCert.bat

The keystore is located here:

/opt/aptare/portalconf/itanalytics.jks

After running the Keystore Utility (deployCert), restart Portal Services.

Add a virtual interface to a Linux server

The standard APTARE server configuration uses two virtual hosts on the server. One host, identified by the sub-domain **itanalyticsportal**, handles Portal requests to deliver NetBackup IT Analytics administration and reporting functionality. The second host, identified by the sub-domain **itanalyticsagent**, handles data collection functionality between the data collection agent and the various devices that report to the agent. These virtual hosts are defined in the Apache configuration file; the sub-domain names are used to identify the each host.

When using SSL, unique IP addresses must be assigned to each virtual host. Therefore, if SSL is to be enabled for both the Portal and Data Collection, two IP addresses are required. Two IP addresses can be assigned using two NICs or, on a Linux server, a virtual interface can be created to assign two IP addresses to a single NIC.

1. To verify the number of IP addresses assigned to a Linux server, use the following command:

   ```
   ifconfig -a
   ```

Example result of the **ifconfig -a** command:

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:71:44:C4
          inet addr:10.0.2.15  Bcast:10.0.2.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:310 errors:0 dropped:0 overruns:0 frame:0
          TX packets:372 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:1000
          RX bytes:63235 (61.7 KiB)  TX bytes:28143 (27.4 KiB)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8762 errors:0 dropped:0 overruns:0 frame:0
         TX packets:8762 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:0
          RX bytes:5422509 (5.1 MiB)  TX bytes:5422509 (5.1 MiB)
```

2. You must have two Ethernet connections, identified by the **eth0** label. To add a virtual interface on a Linux server, with a second IP address, to the existing Ethernet interface, use the following command:

   ```
   ifconfig eth0:0 111.222.333.444
   ```

   where

   111.222.333.444 is the new IP address for the virtual interface.

3. You must add a file to the network scripts to recreate the virtual interface when the server is rebooted. If the IP address assigned to the **eth0** interface is static, make a copy of the **ifcfg-eth0** file in **/etc/sysconfig/network-scripts** and name it **ifcfg-eth0:0**.

4. Update the IP address in **ifcfg-eth0:0** to be the new IP address assigned to the virtual interface.

5. If the IP address in the **eth0** interface is dynamically assigned, as indicated by the line **BOOTPROTO=dhcp** in the **ifcfg-eth0** file, create a file named **ifcfg-eth0:0** with the following lines:

   ```
   DEVICE=eth0:0
   IPADDR=111.222.333.444
   ```

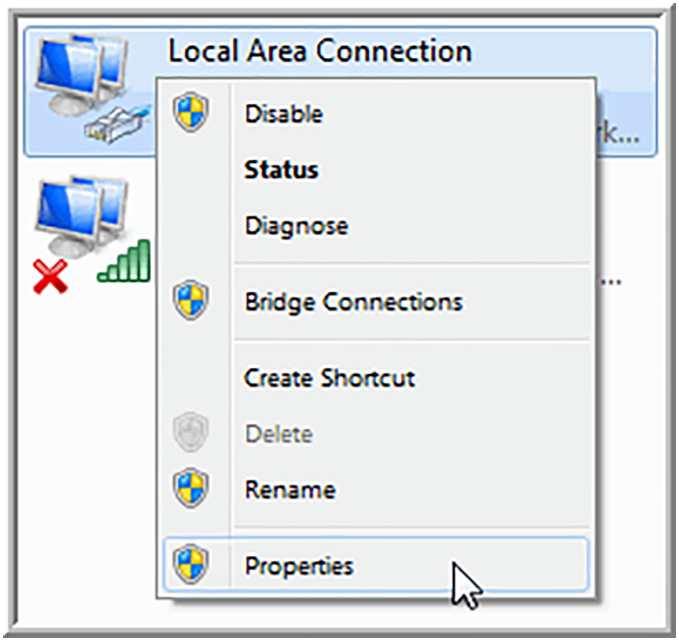
6. Finally, update your DNS server so that the new IP address is mapped to the data collection URL (for example, **itanalyticsportal.<domainname>**).

Add a virtual / secondary IP address on Windows

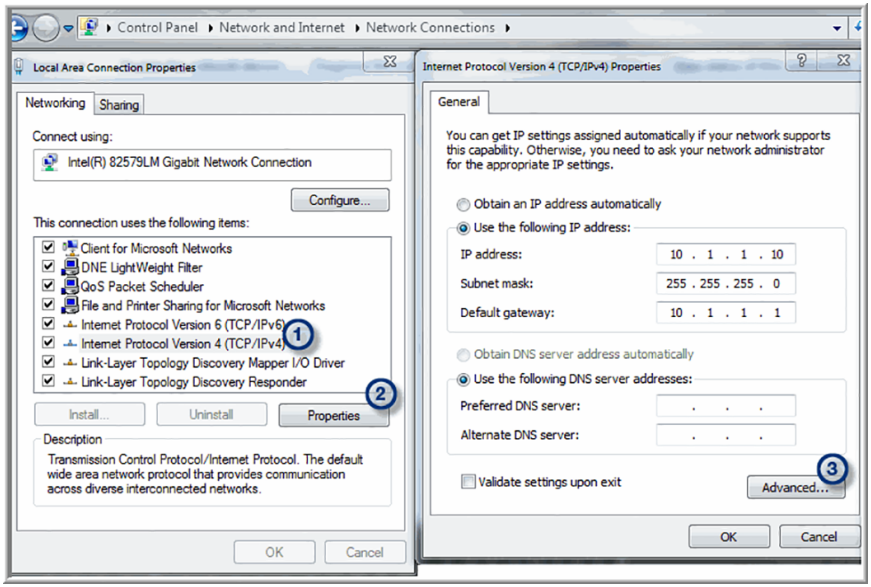
To add a Virtual IP Address on Windows, go to:

Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings

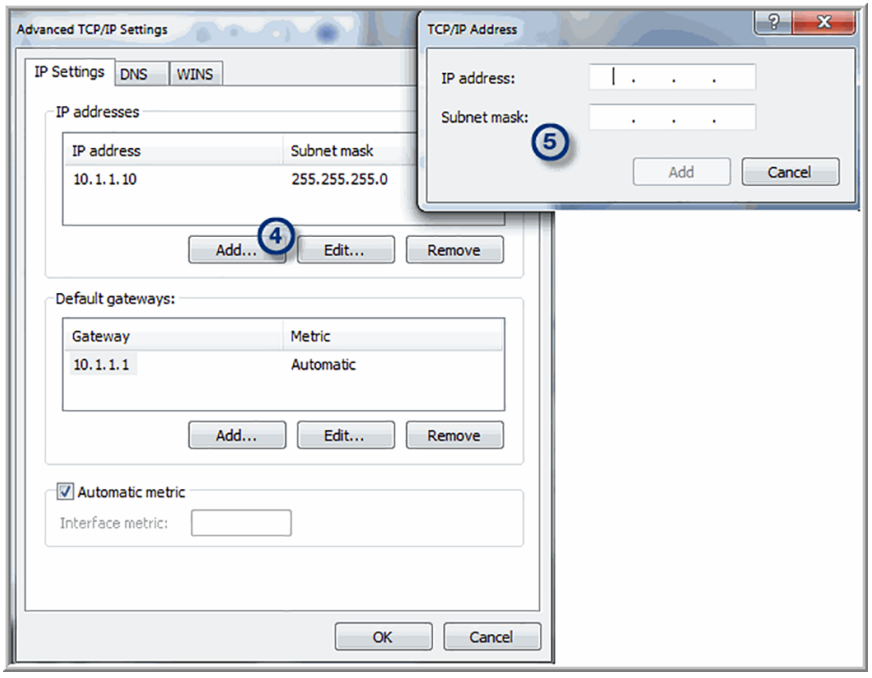
Right-click on a Network connection and select **Properties**.



Take the following steps to configure a secondary IP address.



1. Select the TCP/IP connection.
2. Click **Properties**.
3. For the configured IP address, click **Advanced**.



4. In the Advanced TCP/IP Settings window, click **Add**.
5. Enter the **IP address** and **Subnet mask** and click **Add**.

Section 2

Data Protection

- Chapter 5. Configuration for Veritas Backup Exec
- Chapter 6. Configuration for Cohesity DataProtect
- Chapter 7. Configuration for Commvault Simpana
- Chapter 8. Configuration for EMC Avamar
- Chapter 9. Configuration for EMC Data Domain backup
- Chapter 10. Configuration for Dell EMC NetWorker backup & recovery
- Chapter 11. Configuration of Dell EMC PowerProtect Data Manager (PPDM)
- Chapter 12. Importing generic backup data
- Chapter 13. Configuration for generic backup
- Chapter 14. Configuration for HP Data Protector
- Chapter 15. Configuration for IBM Spectrum Protect (TSM)
- Chapter 16. Configuration for NAKIVO Backup & Replication
- Chapter 17. Configuration for Oracle Recovery Manager (RMAN)
- Chapter 18. Configuration for Rubrik Cloud Data Management
- Chapter 19. Configuration for Veeam Backup & Replication

Chapter 5

Configuration for Veritas Backup Exec

This chapter includes the following topics:

- Introduction
- Architecture overview (Veritas Backup Exec)
- Backup Exec terminology
- Prerequisites for adding data collectors (Veritas Backup Exec)
- Installation overview (Veritas Backup Exec)
- Enable TCP/IP for the SQL server
- Configure a Windows user
- Add Backup Exec servers
- Importing Backup Exec Server information
- Add a Veritas Backup Exec Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Architecture overview (Veritas Backup Exec)

The following diagram provides an example of how the Data Collector could be deployed in your environment.

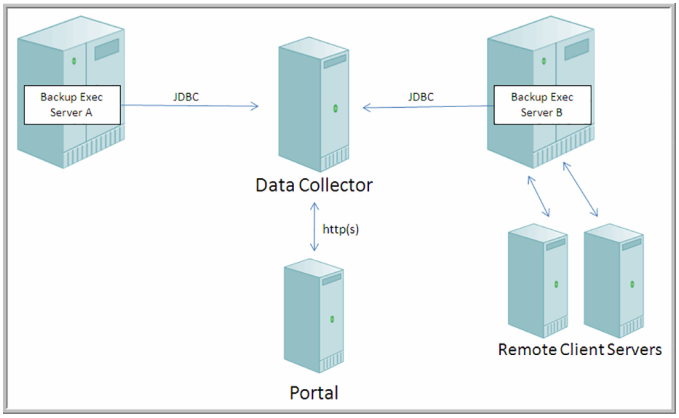


Figure 1 Data Collector in a Veritas Backup Exec Environment

For each Backup Exec server, the Data Collector will establish connections to the Backup Exec database. The connection information for each Backup Exec server is retrieved from the Portal or from a locally stored, encrypted file. This connection information includes parameters such as the Administrator user name, domain name and password, server host name and/or IP address.

The Data Collector will use database commands via TCP/IP to obtain its information from each Backup Exec server. The information is stored in the Portal database, enabling a global view of all of the backup servers and clients.

Backup Exec terminology

Backup Exec Server - The Backup Exec Server is the physical system that is running the Veritas Backup Exec server software. This system will be known by its host name or IP address.

Backup Exec Client Server - The Backup Exec Server backs up data on other servers in a network. In the context of NetBackup IT Analytics, these servers are referred to as the Client Servers.

Prerequisites for adding data collectors (Veritas Backup Exec)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 1433. The BUE collector first connects via UDP on port 1434 to get information about available SQL Server instances, then connects via TCP to the port number that is returned for the specified instance. By default this is 1433.
- If your environment requires NTML v2 authentication (Windows authentication) for the data collection connection, create an Advanced Parameter named USE_NTML_V2 and set the value to Y. Note that the NetBackup IT Analytics default is NTML v1 (database authentication). Windows authentication is used when the Backup Exec server credentials configured in the Data Collector Policy contain a Windows domain name, user name, and password. If Windows credentials are not in the policy, the connection defaults to using database authentication.
- The Backup Exec Administrator account used by the Data Collection policy must have the database role membership of **db_datareader** for the BEDB (Backup Exec Database).
- Note that the version of Backup Exec that is reported by the Backup Exec 15 installation is version 14.2.

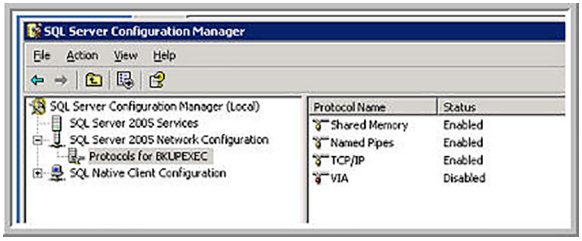
Installation overview (Veritas Backup Exec)

1. Update the local hosts file.
2. In the Portal, add a Data Collector, if one has not already been created.
3. Enable TCP/IP for the SQL Server.
4. Configure a Windows User.
5. Add Veritas Backup Exec Servers.
6. In the Portal, add the Veritas Backup Exec data collector policy.
7. On the Data Collector Server, install the Data Collector software.
8. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal--that is, a HOSTED installation (perhaps for a product evaluation)--skip this section and contact your hosting organization's representative to configure the hosted portal for your Data Collector.

Enable TCP/IP for the SQL server

Ensure that the SQL server has TCP/IP enabled, as shown in the following example:

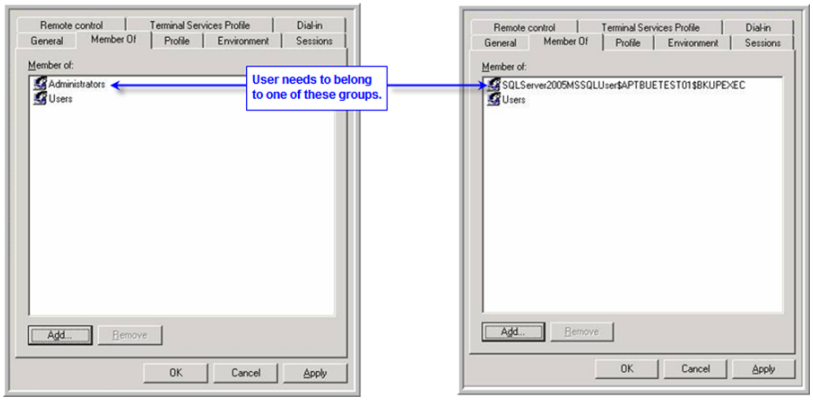


Configure a Windows user

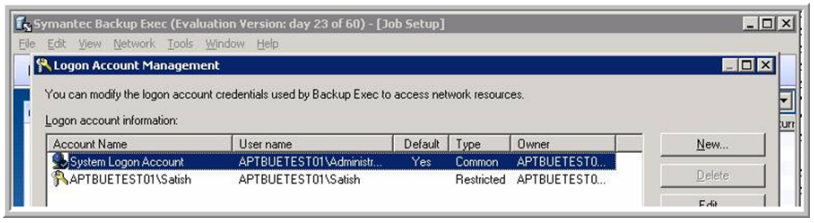
The Data Collector for Backup Exec requires a Windows User with privileges to access the SQL Server that is hosting the Backup Exec database.

1. Complete the worksheet found in the Appendix of this guide, providing configuration details for each backup server that will be polled by a Data Collector.
2. Ensure that you have a **Windows User** that is a member of one of the following groups, either locally or as part of the Windows Domain:

- the local **Administrators** group
- a group named: **SQLServer2005MSSQLUser$ServerName$BKUPEXEC** where ServerName is the name of the server on which the SQL Server and Backup Exec reside, as shown in the following example.



3. The user can be restricted within the context of Backup Exec by configuring the login account, as shown in the following example.



Add Backup Exec servers

For each Backup Exec Server specified in the Data Collector Pre-Installation worksheet, add the Backup Exec Servers to NetBackup IT Analytics.

1. In the Portal, add a host for each Backup Exec server.
   - Host Name - Displayed in the Portal.
   - Internal Host Name - Must match the host name of the Backup Exec server; fully qualified domain name (FQDN).
   - Backup Type - Backup Exec Data Collector.

Importing Backup Exec Server information

For the Data Collector to interrogate the Backup Exec servers and retrieve the necessary information for transmission to the Portal, a list of the Backup Exec servers with corresponding access parameters must be loaded into the Portal database.

1. Create a comma-separated value (CSV) file, and for every Backup Exec Data Collector specified in the Data Collector Pre-Installation worksheet, enter a comma-separated line with: an optional domain name, **mandatory host names** and optional IP addresses, database instance, administrator user names and passwords.

   If the IP Address field is left blank, the Data Collector will detect the null address and perform an IP lookup, using the host name, and then connect to the Backup Exec SQL server.

   Each line in the CSV file should follow this format:

   ```
   WindowsdomainName,hostname,ip_address,dbInstance,adminUserName,adminPassword
   ```

   Example CSV File:

   ```
   ,server1,,,,
   ,server2,,,,
   ,server3,,,,
   ,server4,,,,
   windowsdomainname,myserver,10.0.0.67,scdb,Administrator,password
   ```

   In the previous example file, there are five Backup Exec servers to be loaded into the Portal. The first four servers will use the default credentials. The last server will use the credentials as specified in this file.

   Note: Passwords are stored in the Portal database in a strongly encrypted format and only decrypted in memory once passed to the Data Collector application immediately prior to use.

   WindowsDomainName, adminUserName and adminPassword - [optional] -Supply values for these three parameters if you wish to use a default Windows domain name, domain administrator user name and administrator password to connect to the Backup Exec servers. These default values will apply only to the Backup Exec servers listed in the CSV file that do not already contain values for these fields.

dbInstance- [optional] - Supply the name of a specific database instance, if you want to use a database that is different from the default Backup Exec database.

2. In the **Veritas Backup Exec Data Collector Policy** window, click **Import** to access the **Upload CSV** window where you can enter a default Database Instance and the name of the CSV file in which you placed the server configuration details.

Add a Veritas Backup Exec Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide .
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Adminstration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

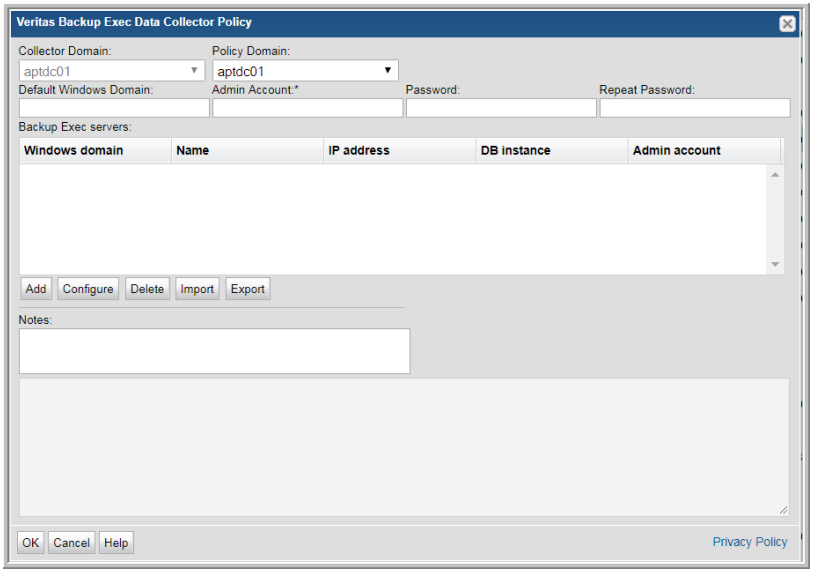
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters.

See See Table 5-1 on page 89.

6 Click **OK** to save the policy.

7 On the Data Collector server, install/update the Data Collector software.

Note: If your environment requires NTML v2 authentication (Windows authentication) for the data collection connection, create an Advanced Parameter named USE_NTML_V2 and set the value to Y. Note that the NetBackup IT Analytics default Windows authentication is NTML v1.

Table 5-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 5-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Default Windows Domain	Windows domain name; If the host is not a member of a domain, or to specify a local user account, use a period (.) to substitute the local host SSID for the domain. Windows authentication is used when the BUE server credentials, added at collector configuration time, contain a Windows domain name, user name and password. If the Windows domain name is missing, the connection defaults to using database authentication.
Admin Account	Veritas Backup Exec Administrator account. This account must have the database role membership of **db_datareader** for the BEDB (Backup Exec Database).
Password	Veritas Backup Exec password associated with the account
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 6

Configuration for Cohesity DataProtect

This chapter includes the following topics:

- Introduction
- Prerequisites for adding Data Collectors (Cohesity DataProtect)
- Installation overview (Cohesity DataProtect)
- Add a Cohesity DataProtect Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Cohesity DataProtect)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- User must be assigned the Cohesity Operator role

Installation overview (Cohesity DataProtect)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Cohesity DataProtect data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Add a Cohesity DataProtect Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

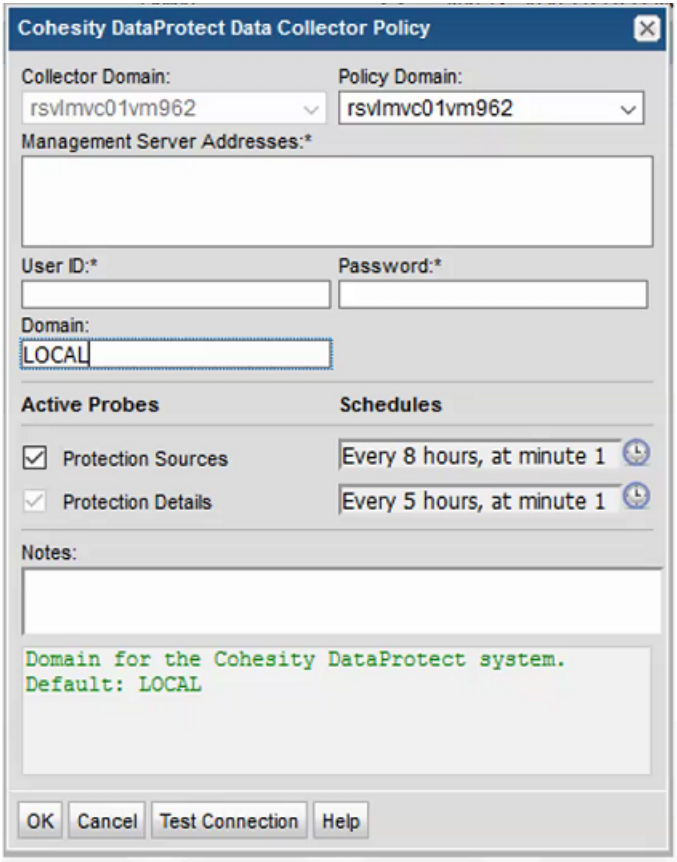
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more DataProtect Management server IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost **Note:** To collect from a Cluster, enter the IP address of only one of the management servers. To collect from multiple nodes, use the primary node IP.
User ID*	This field is required. View-only User ID and password for the Cohesity DataProtect storage system.
Password*	This field is required. Password for the Cohesity DataProtect storage system.
Domain	Domain for the Cohesity DataProtect system. Default is LOCAL.
Active Probes	
Protection Sources	Probe for Cohesity DataProtect Protection Sources.
Protection Details	Probe captures data about Protection Jobs, including their policies, schedules, sessions, and backups.

Field	Description
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin** > **Data Collection** > **Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 7

Configuration for Commvault Simpana

This chapter includes the following topics:

- Introduction
- Architecture overview (Commvault Simpana)
- Prerequisites for adding Data Collectors (Commvault Simpana)
- Upgrade troubleshooting: Microsoft SQL Server and Java 11
- Installation overview (Commvault Simpana)
- Open TCP/IP access to the Commvault database
- Set up a read-only user in the CommServe server
- Load historical data prior to initial data collection
- Add Commvault Simpana servers
- Add a Commvault Simpana Data Collector policy

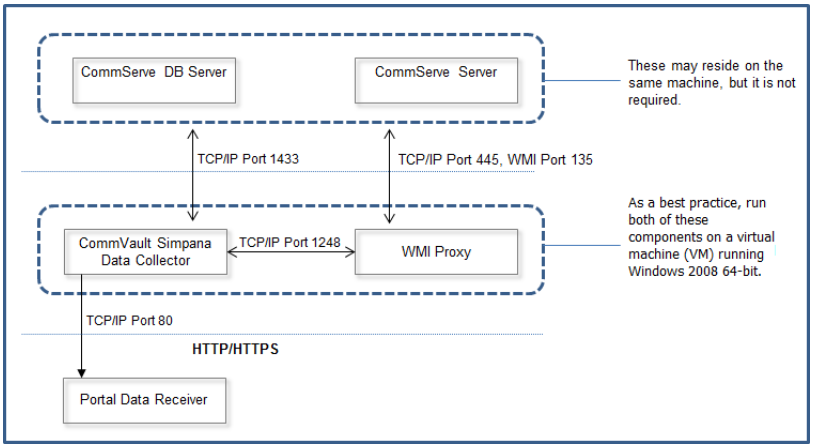
Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Architecture overview (Commvault Simpana)

The Data Collector connects to the Commvault Simpana CommServe database via JDBC to issue SQL queries (including execution of some read-only functions).

To collect more detailed information about individual jobs the Data Collector connects to the CommServe server via WMI and executes the sendLogFiles.exe tool to retrieve the client log files. These are then retrieved from the C$ administrative share. To retrieve this more detailed information a Windows logon with administrative access to the CommServe server must be supplied.



Prerequisites for adding Data Collectors (Commvault Simpana)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect(TSM) collection, the Data Collector server and backup server can be in different time zones.
- Open TCP/IP access to the Commvault database on a static port (1433 recommended).
  See "Open TCP/IP access to the Commvault database" on page 101.
- MS SQL Server needs to be accessible to the collector on a static TCP Port (1433 recommended), requiring a restart of the SQL database service, if not already configured.
- MS SQL Server must be set to Mixed-mode authentication, and the login to be used for collection must be using SQL authentication.
  https://msdn.microsoft.com/en-us/library/ms188670.aspx.
- WMI Proxy access requires the following: Port 135 is required for skipped files collection and 445 for CIFS over TCP. A fixed port can be configured for WMI as specified at:
  http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx
- The Data Collector should be installed on the same server as the WMI proxy server.
- Read-only user configured on the CommServe server.
  See "Set up a read-only user in the CommServe server" on page 103.
- If you want to load historical data from a CommServe database, use the utility described in the following section.
  See "Load historical data prior to initial data collection" on page 107.
- One Data Collector can include all of these backup products: Commvault Simpana, EMC Avamar, EMC NetWorker, EMC Data Domain, Arctera Backup Exec, Cohesity NetBackup, HP Data Protector, IBM Spectrum Protect (TSM) , and Generic Backup products. And, you also can include other enterprise objects, such as storage arrays, in this Data Collector.

Upgrade troubleshooting: Microsoft SQL Server and Java 11

With the introduction of support for Java 11, older versions of MS SQL Server may encounter compatibility issues. The following section covers potential workarounds. Collection occurs from the Microsoft SQL Server database used by the system the data collector is collecting from. The version of Java used by NetBackup IT Analytics disables some insecure TLS algorithms by default. If collection fails with the following

error in the collector logs, the version of MS SQL Server may be incompatible and not allow collection using the TLS algorithms enabled by default with Java 11.

```
Failed to establish JDBC connection to: jdbc:jtds:sqlserver://...
java.sql.SQLException: Network error IOException: null
at net.sourceforge.jtds.jdbc.JtdsConnection.<init>
(JtdsConnection.java:437)
```

Upgrade MS SQL Server to the latest version to enable secure collection. Your MS SQL Server version may not be supported. If upgrade is not possible, a workaround can be attempted to restore compatibility. If the following steps do not resolve the issue, your version of MS SQL Server is not supported.

Use the following steps to modify the enabled algorithms to attempt communication with the data collector. Note that using this workaround will reduce the security of your collection. The default list of disabled algorithms is taken from Java 11.0.6 and may change in later versions.

1. Edit <collector install dir>/java/conf/security/java.security.
2. Search for jdk.tls.disabledAlgorithms.
3. Copy the existing lines and comment (to have a backup for easy restore).

```
#jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
#    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

4. One at a time, remove an algorithm from the jdk.tls.disabledAlgorithms and test the collection, starting at the last algorithm and working backward. Stop once you reach an algorithm containing 'keySize <'.
   - Remove one algorithm - for example NULL

     ```
     jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
     DH keySize < 1024, \
         EC keySize < 224, 3DES_EDE_CBC, anon
     ```

   - Save the file.
   - Run `checkinstall` and verify collection succeeds.
   - If `checkinstall` does not succeed, restore jdk.tls.disabledAlgorithms to its original state.

5. Change to DH keySize<768 - for example.

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 768, \
EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

   - Save the file.
   - Run `checkinstall` and verify collection succeeds.

6. If a working configuration is found, restart the collector service.

Installation overview (Commvault Simpana)

1. See “Open TCP/IP access to the Commvault database” on page 101.
2. See “Set up a read-only user in the CommServe server” on page 103.
3. See “Add Commvault Simpana servers” on page 107.
4. See “Load historical data prior to initial data collection” on page 107.
5. Open TCP/IP access to the Commvault database.
6. Set up a read-only user in the CommServe server.
7. Load historical data (prior to the initial data collection).
8. In the Portal, add a Data Collector, if one has not already been created.
9. In the Portal, add the Commvault Simpana data collector policy.
10. On the Data Collector Server, install the Data Collector software.
11. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal, that is, a HOSTED installation (perhaps for a product evaluation) skip this section and contact your hosting organization’s representative to configure the hosted portal for your Data Collector.

Open TCP/IP access to the Commvault database

The following steps assume that the Commvault database is installed on an MS SQL server instance named COMMVAULT. Substitute the appropriate instance name as required.

Note: MS SQL Server must be set to Mixed-mode authentication and the login to be used for collection must be using SQL authentication.

1. Expand **SQL Server Network Configuration.**
2. Click **Protocols for <COMMVAULT>.**
3. Double-click **TCP/IP.**
4. Verify **Enabled** is set to **Yes** on the **Protocol** tab.
5. Scroll to **IPAll,** and in **TCP Port** enter 1433 on the **IP Addresses** tab. If you do not want to use the default MSSQL server port, you can enter another port number.
6. If you require a static port, clear the **TCP Dynamic Port** value. Note that any value, including 0, enables dynamic ports.

   See "Additional Static Port Configuration Steps" on page 102.
7. Click **OK.**
8. Click **SQL Server Services.**
9. Right-click **SQL Server <COMMVAULT>** and select **Restart.**

Additional Static Port Configuration Steps

If you configured a static port during the port configuration process take the following steps

On the Commvault CommCell Server:

1. Start the **ODBC Data Source Administrator** tool.
2. Select the Commvault database DSN (usually a system DSN) and click **Configure**.
3. Click **Next**.
4. Select **With SQL Server authentication using a login ID and password entered by the user**.
5. Enter the required User ID and password.
6. Click **Client Configuration** and make the following changes.
   - In the Network libraries window, select **TCP/IP**.
   - Enter the server name.
   - De-select **Dynamically determine port**. ODBC uses port 1433 as a default, so it will be grayed out.

- Click **OK**.

7. Click **Next** and change the database, if needed.
8. Click **Next**, then **Finish**.
9. Click **Test Data Source**.
10. Click **OK**.

Set up a read-only user in the CommServe server

The Data Collector uses Java Database Connectivity (JDBC) as a read-only user (including executing some read-only functions) to collect point-in-time data from the Commvault Simpana CommServe database. The Data Collector also uses a Commvault Simpana command-line tool (sendLogFiles.exe - executed using WMI on the CommServe server) to collect log files from client machines managed by the CommServe server.

There are two methods to set up an optional read-only user in the CommServe database. Choose one.

Note: MS SQL Server must be set to Mixed-mode authentication and the login to be used for collection must be using SQL authentication.

---

1. Create a new read-only user with a non-expiring password and assign the **db_datareader** role in the CommServe database. After completing the following steps, verify the connectivity with the read-only user ID.
2. Grant EXECUTE permission for the following stored procedures to the new read-only user:

   dbo.GetDateTime

   dbo.GetUnixTime

   dbo.GetJobFailureReason

   dbo.JMGetLocalizedMessageFunc

There are two methods for assigning EXECUTE permission.

Option 1: Execute SQL commands in the CommServe database

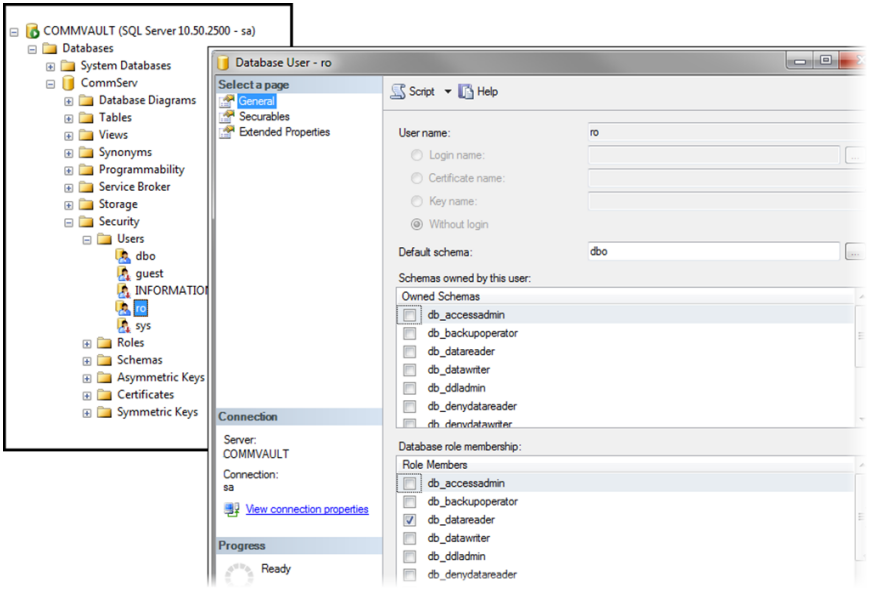
```
GRANT EXECUTE ON CommServ.dbo.GetDateTime TO <ro user>;
GRANT EXECUTE ON CommServ.dbo.GetUnixTime TO <ro user>;
GRANT EXECUTE ON CommServ.dbo.GetJobFailureReason TO <ro user>;
```

```
GRANT EXECUTE ON CommServ.dbo.JMGetLocalizedMessageFunc TO <ro user>;
```

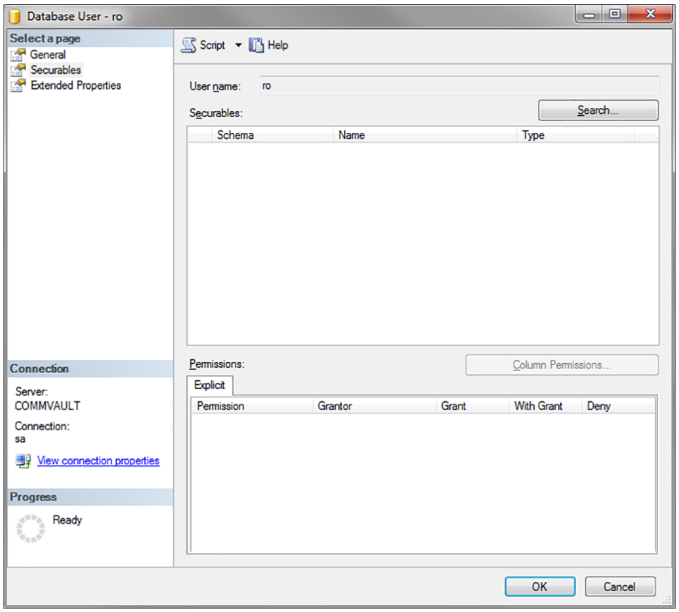
Note: Replace <ro user> with the read-only user.

Option 2: Use MSSQL Management Studio

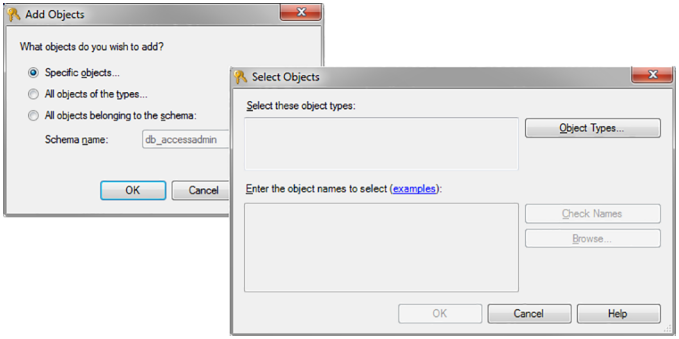
1. Click **Databases > CommServe > Security > Users.**
2. Select **ro** in the **Users** folder and double-click. The Database User screen is displayed.



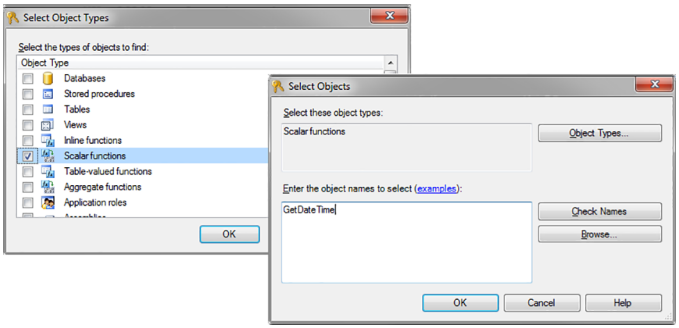
3. Select the **Securables** page.



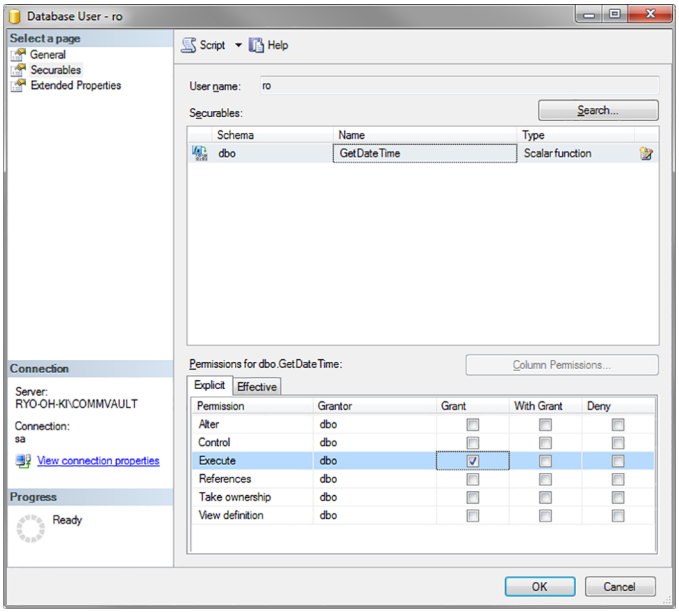
4. Click Search.
5. Add specific objects.



6. Check Object Type **Scalar functions** and click **OK.**



7. Enter the object name **GetDateTime** and click **OK.**



8. Grant execute permissions for GetDateTime by clicking **Execute.** Click **OK.**
9. Repeat steps 4-8 for each function:
   - GetUnixTime
   - GetJobFailureReason
   - JMGetLocalizedMessageFunc
10. Verify connectivity with the read-only user ID.

Load historical data prior to initial data collection

This optional procedure is intended to be used only if you want to load the historical data from a CommServe database. This utility must be run prior to the first data collection. It prompts you for the number of hours to go back in time within the historical data and then configures data collection to capture that data.

To configure data collection to capture historical data, follow these steps.

1. At the command line, go to the database tools directory.

   ```
   cd <HOME>\database\tools
   ```

2. Login to SQL Plus.

   ```
   sqlplus portal/portal@//localhost:1521/scdb
   ```

3. Run the utility that configures the Data Collector to look for historical data. This utility only prompts you to enter hours and then configures data collection accordingly.

   ```
   SQL> @cmv_update_max_lookback_hours.sql
   Enter value for hours: 12
   old   1: UPDATE ptl_system_parameter SET param_value = &hours
   WHERE
   param_name='
   CMV_MAX_LOOK_BACK_HRS'
   new   1: UPDATE ptl_system_parameter SET param_value = 12 WHERE
   param_name='CMV_
   MAX_LOOK_BACK_HRS'
   Commit;
   1 row updated.
   Commit complete.
   ```

4. Exit SQL Plus.

   SQL> exit

Add Commvault Simpana servers

For each Commvault Simpana server specified in the Data Collector Pre-Installation worksheet add the Commvault Simpana servers to NetBackup IT Analytics.

1. In the Inventory, add a host for each CommServe server.
   - Host Name - Displayed in the Portal.

- Internal Host Name - Must match the host name of the CommServe Server.
- IP Address - IP address of the Commserve Server.
- Type - Commvault Server.

Add a Commvault Simpana Data Collector policy

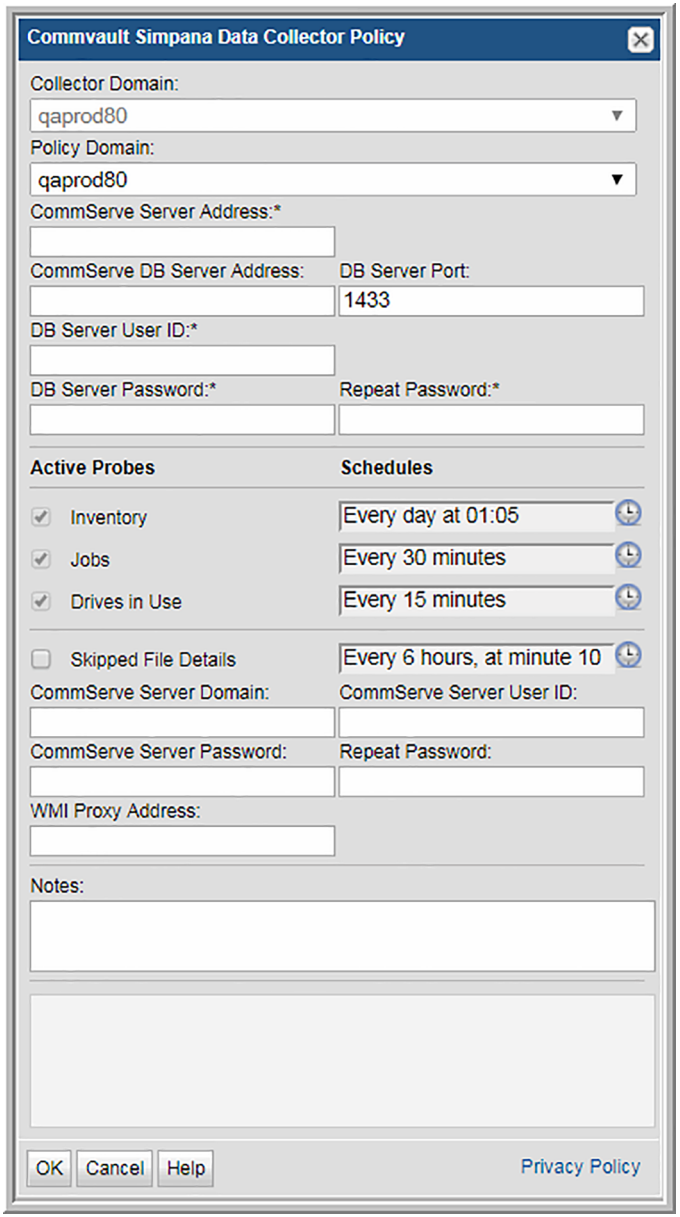
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy** and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name select **My Profile** in the User Account menu.
CommServe Server Address*	Specify the IP address or host name of the CommServe server. This field is required.
CommServe DB Server Address	Specify the IP address or host name of the CommServe database system. This field may be empty. The CommServe database hostname defaults to the CommServe server if the field is empty.
DB Server Port	Specify the port used by the CommServe database. The default is 1433. This port is not enabled by default on the SQL server. Once this port is configured on the SQL server, the server must be restarted before data collection can occur.
DB Server User ID*	Specify the read-only user ID (with a non-expiring password) for the CommServe database. This is a SQL authentication login with at least the following roles and permissions in the CommServe database: db_datareader - EXECUTE dbo.GetDateTime - EXECUTE dbo.GetUnixTime - EXECUTE dbo.GetJobFailureReason - EXECUTE dbo.JMGetLocalizedMessageFunc This field is required.

Field	Description
DB Server Password*	The non-expiring password associated with the User ID. This field is required.
Repeat Password	The password associated with the User ID.
Active Probes	
Inventory	Click the clock icon to create a schedule frequency for collecting data relating to system details such as system, disk, tape, VTL and filesystem compression. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. Optimize performance by scheduling less frequent collection. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Jobs	Click the clock icon to create a schedule frequency for collecting data relating to backup jobs. The default collection is every 30 minutes. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. The default maximum number of hours that will be collected is 168 (7 days). **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Drives in Use	Click the clock icon to create a schedule frequency for collecting data relating to the drives in use for backup. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Skipped File Details	Activates skipped file collection details - this collects which files had problems during backup/restore and needed to be skipped. It collects client logs and may require WMI proxy information. Click the clock icon to create a schedule frequency for collecting data relating to the skipped files during backup. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted. **Note:** By default, this field is not selected. Activating this field will cause another collection to run periodically that may take hours (depending on the number of clients). You can also access the CommCell GUI for additional information.
CommServe Server Domain	Specify the domain associated with the User ID. This field must be combined the CommServe Server User ID. If this field is blank, a local user account (.\username) will be used.
CommServe Server User ID	Specify the user ID with administrative privileges on the CommServe server. This field must be combined the CommServe Server Domain. If this field is blank, a local user account (.\username) will be used.The User ID and Password fields are required for the Skipped File Details collection.
CommServe Server Password	The password associated with the CommServe Server User ID. The User ID and Password fields are required for the Skipped File Details collection.
Repeat Password	The password associated with the User ID.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6. Click **OK** to save the policy.
7. On the Data Collector server, install/update the Data Collector software.

Chapter 8

Configuration for EMC Avamar

This chapter includes the following topics:

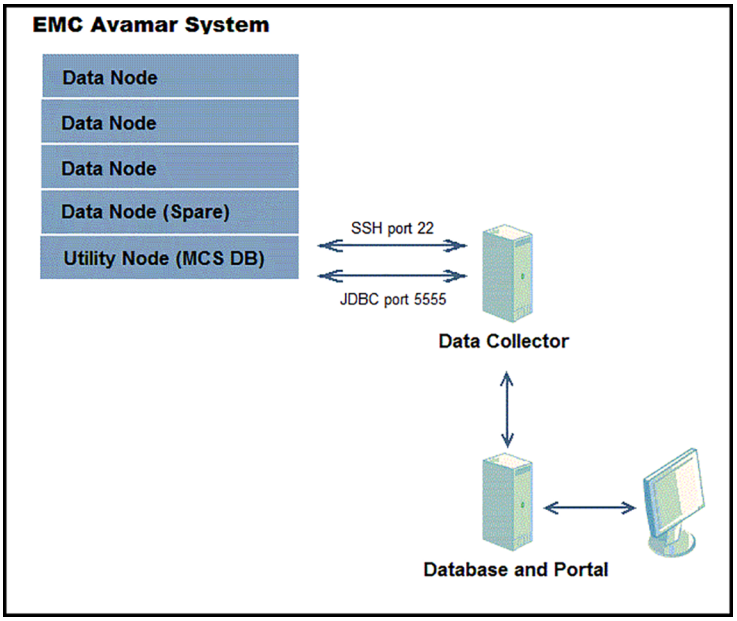
- Introduction
- Architecture overview (EMC Avamar)
- Prerequisites for adding Data Collectors (EMC Avamar)
- Installation overview (EMC Avamar)
- Add EMC Avamar servers
- Adding an EMC Avamar Data Collector policy
- Testing the collection
- Add/Configure an Avamar Server within the Data Collector policy window
- Import EMC Avamar server information
- Export EMC Avamar server information

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Architecture overview (EMC Avamar)

The following diagram provides an example of how the EMC Avamar Data Collector could be deployed in your environment.



The Data Collector connects to the Avamar system and via JDBC, extracts data from the Management Console Server (MCS) Database. The Avamar connection information is retrieved from the Portal. This connection information includes parameters such as the user ID, password, and server address. The Avamar version is retrieved from the Avamar server. Open ports: 22 for SSH and 5555 for JDBC to MCS DB.

Prerequisites for adding Data Collectors (EMC Avamar)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- TCP ports 5555 and 22.
- An Avamar Utility Node server must be configured in the Data Collector Policy. The login credentials must have **admin** or **dpn** access to the Avamar utility node so that the Data Collector can invoke command-line programs in the /usr/local/avamar/bin directory.
- One Data Collector can be used to include all of these backup products: Commvault Simpana, EMC Avamar, EMC NetWorker, EMC Data Domain, Backup Exec, Cohesity NetBackup, HP Data Protector, and Generic Backup products. And, you also can include other enterprise objects, such as storage arrays, in this Data Collector.
- The Data Collector uses JDBC as a read-only user to collect point-in-time data from the Avamar Management Console Server (MCS) database. In addition, command-line-interface (CLI) commands access the utility node for Avamar server status details.

Installation overview (EMC Avamar)

1. Update the Local Hosts file. This enables Portal access.
2. Add EMC Avamar Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the EMC Avamar data collector policy.
5. On the Data Collector Server, install the Data Collector software.
6. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal—that is, a HOSTED installation (perhaps for a product evaluation)—skip this section and contact your hosting organization's representative to configure the hosted Portal for your Data Collector.

Add EMC Avamar servers

Add Avamar servers to NetBackup IT Analytics using the Inventory or add an Avamar server directly from the data collector policy window.

1. Note the ports used by the Avamar Data Collector: TCP 5555 and SSH 22.
2. In the Inventory, add an Avamar server (Utility Node).
   - Internal Host Name - Must match the Avamar Utility Node fully qualified domain name (FQDN).
   - IP Address - IP address of the Utility Node.
   - Backup Type - EMC Avamar Server.
3. Configure a view-only User ID and Passcode in the Data Collector policy.

Note: You can also add EMC Avamar servers directly from the Data Collector policy screen.

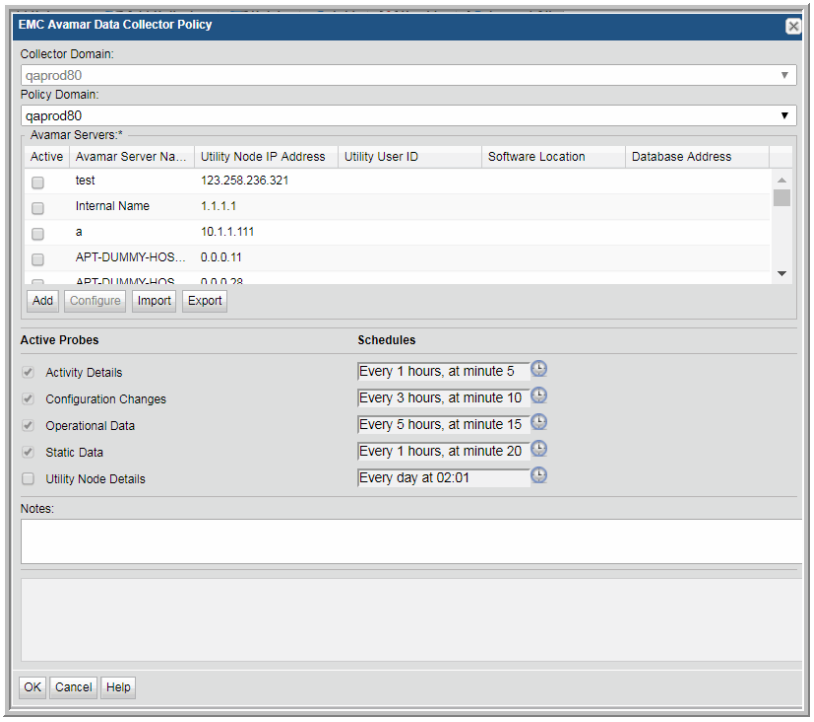
See "Add/Configure an Avamar Server within the Data Collector policy window" on page 120.

Adding an EMC Avamar Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5. Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Avamar Servers*	You can add Avamar servers by clicking **Add**. You can also import multiple servers using a .CSV file. You can also do this using the Inventory. The **Avamar Servers** table is populated using any of these methods. The servers added to this table using **EMC Avamar Data Collector Policy** screen are also displayed under **Inventory**. You must indicate which servers are active.
Active	Click **Active** to indicate the Avamar server(s) to use in the data collection policy. For Avamar, this is the Utility Node. If additional fields must be configured, the **Configure Server** dialog is automatically displayed when you make your selection.
Add	Click **Add** to add an Avamar server type. The added servers are also displayed under **Inventory**. **Note:** Data Collector policies can be in place for multiple servers, but a server cannot have multiple policies. See “Add/Configure an Avamar Server within the Data Collector policy window” on page 120.
Configure	Click **Configure** to revise or add information to the Avamar server you selected. See “Add/Configure an Avamar Server within the Data Collector policy window” on page 120.
Import	Click **Import** to browse for the CSV file in which you entered the Avamar server configuration details. See “Import EMC Avamar server information” on page 122.

Field	Description
Export	Click **Export** to create and download a comma-separated values (CSV) file containing all the server information listed in the **Avamar Servers** table. See "Export EMC Avamar server information" on page 123.
Active Probes	Click the clock icon to set a schedule frequency. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. You can set a schedule to collect on: ■ Activity Details ■ Configuration Changes ■ Operational Data ■ Static Data **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Activity Details	Collects backup events/activities from the Avamar server.
Configuration Changes	Collects datasets, retention policies, schedules, Avamar clients, groups and group members from the Avamar server.
Operational Data	Collects node utilization, node space, events, DPN statistics, Garbage Collection (GC) status, current Global Storage Area Network (GSAN) status from the Avamar.
Static Data	Collects the Axion systems, event catalog and plugin catalog entries from the Avamar server.
Utility Node Details	Collects chassis information for the Avamar Utility Node.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Click **OK** to save the Policy.

7 Install/update the Data Collector software on the Data Collector server.

Testing the collection

You can test the collection of data using the **Run** functionality available in **Admin**>**Data Collection**>**Collector Administration**. This test run performs a

high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

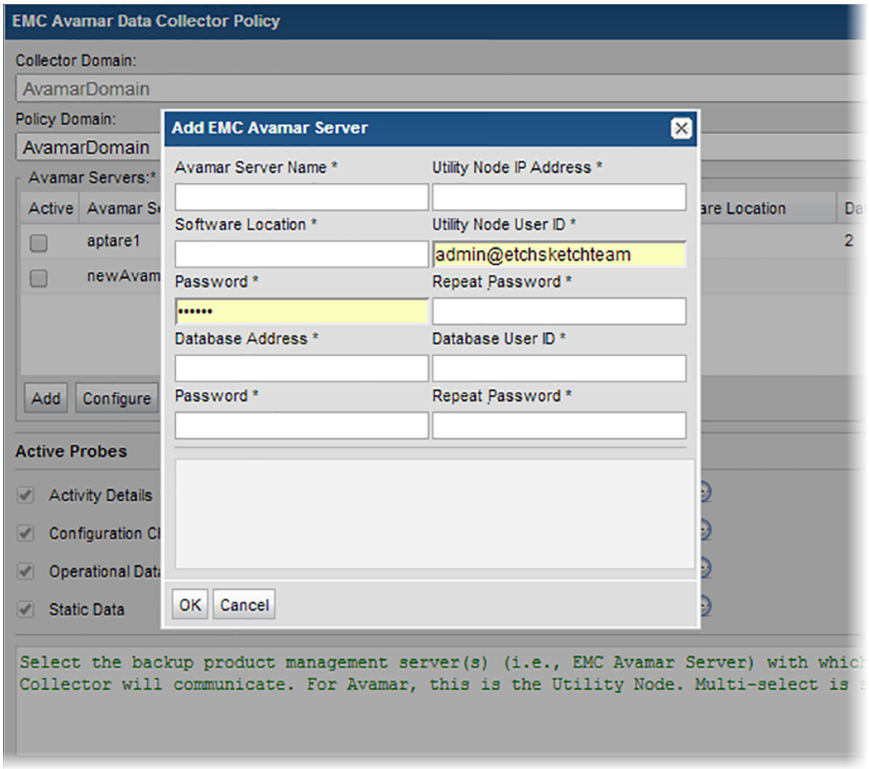
Add/Configure an Avamar Server within the Data Collector policy window

Add Avamar servers by clicking **Add**, by importing using a .CSV file, or by using the Inventory. The **Avamar Servers** table is populated using any of these methods. Servers added to this table are also displayed under **Inventory**. The Avamar Servers table only displays available servers. These servers are not assigned to other policies within the domain.

Note: Data Collector policies can be in place for multiple servers, but a server cannot be assigned multiple policies within the same domain. If you try add a server that is already assigned to another Data Collector policy, you will be prompted to remove it from its current policy and reassign it.

---

1. Click **Add** on the **EMC Avamar Data Collector Policy** screen. The **Add EMC Avamar Server** screen displays.



2. Enter the values:

Field	Description
Avamar Server Name	The Avamar Utility Node server name. This is displayed on the **Inventory** page under the **Host Name** column. This is displayed on the **Host Administration** dialog under **Internal Name**. This is a required field.
Utility Node IP Address	IP address of the Avamar Utility Node. This is management server with which the Data Collector will communicate. This is displayed on the Host Management page under the **Primary IP** column. This is a required field.
Software Location	Directory under which all Avamar binaries and configuration files are kept. This field is pre-populated with a default location: /usr/local/avamar. You can edit the field, but it must contain a value.

Field	Description
Utility Node User ID	The login credentials must have admin or dpn access to the Avamar utility node so that the Data Collector can invoke command-line programs in the /usr/local/avamar/bin directory.
Password	Password for the utility node username that has root-level access to the Avamar utility node. This is a required field.
Database Address	Hostname or IP address used to connect to the Avamar Management Console database. This field is pre-populated with a default address: the Utility Node IP address. You can edit the field, but it must contain a value.
Database User ID	User name to log into the EMC Avamar Management Console database for reporting access. This field is pre-populated with a default Avamar user ID: viewuser. You can edit the field, but it must contain a value.
Password	Password for credentials required to log into the EMC Avamar management console database for reporting access. This field is pre-populated with a default Avamar user password: viewuser1. You can edit the field, but it must contain a value.

Import EMC Avamar server information

You can quickly add a list of EMC Avamar servers using the **Import** function. The information is displayed in the **Avamar Servers** table on the **EMC Avamar Data Collector Policy** screen. Because the import is done within a policy, the host group/domain selected for the policy is used for server location.

CSV Format Specifications

Before importing, create a comma-separated values (CSV) file of Avamar server data. The CSV file must use the following order to populate the fields correctly when importing:

1. Avamar Server Name - maximum 128 characters. Null is not accepted
2. Utility Node IP Address - maximum 40 characters. Null is not accepted
3. Utility Node User ID - maximum 64 characters. Null is not accepted
4. Utility Node Password - maximum 256 characters. Null is not accepted
5. Software Location - maximum 256 characters. If this field is blank, the following default is used: /usr/local/avamar.

6. Database Address - maximum 128 characters. If the Avamar database is resident on the Utility Node, this should contain the Utility Node's IP Address.
7. Database User ID - maximum 64 characters. If this field is blank, the following default is used: viewuser.
8. Database Password - maximum 64 characters. If this field is blank, the following default is used: viewuser1.

Import Notes

If the same Avamar Server already exists in the specified host group, the details are updated when an import occurs.

To Import EMC Avamar Servers

1 Prepare the CSV according to CSV Format Specifications.

See "CSV Format Specifications" on page 122.

2 Select **Admin** > **Data Collection** > **Collector Administration**.

3 Click **Add Policy**.

4 Select **EMC Avamar**. The **EMC Avamar Data Collector Policy** screen is displayed.

5 Click **Import**. The **Import EMC Avamar Servers** window is displayed. You can browse for the CSV file you created.

Export EMC Avamar server information

Use **Export** to create a comma-separated values (CSV) file containing all the server information listed in the Avamar Servers table.

Click **Export** to download the CSV file to your local system.

Chapter 9

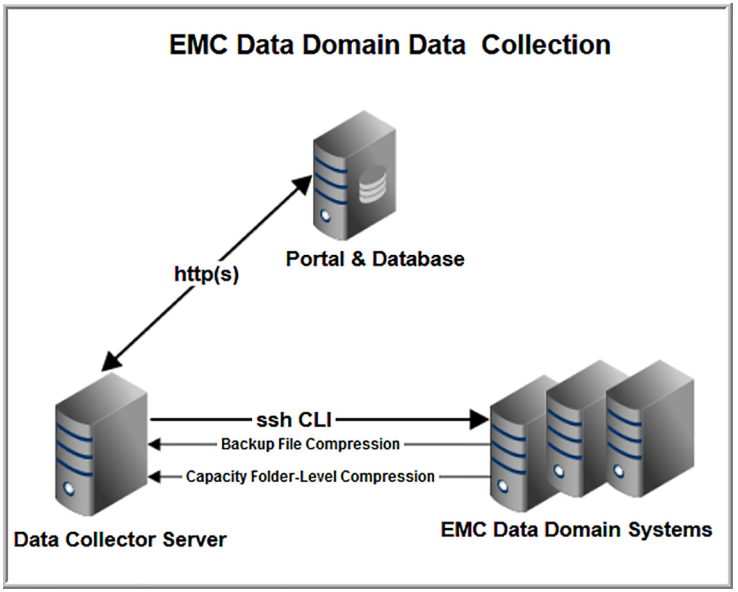
Configuration for EMC Data Domain backup

This chapter includes the following topics:

- Architecture overview (EMC Data Domain Backup)
- Prerequisites for adding Data Collectors (EMC Data Domain Backup)
- Installation overview (EMC data domain Backup)
- Add EMC data domain servers
- Add an EMC data domain backup Data Collector policy
- Adding/Configuring an EMC data domain server within the Data Collector policy window
- Configure a data domain server for file-level compression collection

Architecture overview (EMC Data Domain Backup)

The following diagram provides an example of how the EMC Data Domain Data Collector could be deployed in your environment.



The Data Collector connects to the Data Domain system via SSH to issue data-gathering commands from the command-line interface (CLI).

Data Domain systems straddle the backup and storage capacity worlds. When addressing data protection challenges, Data Domain provides backup, archive, and disaster recovery solutions. In support of these solutions, Data Domain appliances supply deduplication and storage management systems. These systems provide storage in the following ways:

- Native storage device for backup systems
- Virtual tape library (VTL) for backup systems
- NFS mount or CIFS share folders for file storage

Collection related to backups retrieves Data Domain system details such as file system and virtual tape library (VTL) usage. If NetBackup collection also is enabled, a file-level compression probe can collect data that links NetBackup backup images with Data Domain file-level compression ratios, enabling reports by NetBackup client or policy. Data collection gathers information regarding the actual size of the backup image that was sent to the Data Domain system, along with the size of the backup image that is stored on disk after deduplication and compression. NetBackup IT Analytics maps the backup image back to the backup system file catalog. This data helps in identifying backup sets, clients, and policies that are best suited for the deduplication/compression features offered by Data Domain storage. In addition, chargeback reporting can use the actual disk space used (size of the backup image).

Prerequisites for adding Data Collectors (EMC Data Domain Backup)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Port used by the Data Domain Data Collector: **Port 22 for SSH.**
- If collecting File-Level Compression metrics, Cohesity NetBackup collection must be enabled.
- Aggregated global and local compression rates for all Cohesity NetBackup backup images can be collected for all active Data Domain Server MTrees connected (via DDBOOST) to NetBackup Primary Servers. These Primary Servers must have an active Data Collector that has successfully completed an initial data collection. Initiate compression rate collection by selecting File-Level Compression in the Data Domain Data Collector Policy.

Installation overview (EMC data domain Backup)

It is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment. The following lists the high-level steps required to install a data collector for a specific vendor subsystem.

1. Update the Local Hosts file. This enables Portal access.

2. Add EMC Data Domain Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the EMC Data Domain data collector policy.
5. On the Data Collector Server, install the Data Collector software.
6. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal, that is, a HOSTED installation (perhaps for a product evaluation) skip this section and contact your hosting organization's representative to configure the hosted portal for your Data Collector.

Add EMC data domain servers

Add or edit EMC Data Domain servers to NetBackup IT Analytics directly from the data collector policy window or through the Inventory.

Note: When adding an EMC Data Domain Server, in the Inventory select **Hosts**, not Backup Servers.

---

1. Add a host for each Data Domain server.
   - External Host Name - Displayed in the Portal.
   - Internal Host Name - Must match the host name of the Data Domain server; fully qualified domain name (FQDN).
   - Backup Type - Data Domain Server
2. If collecting File-Level Compression data, refer to the following section.

   See " Add an EMC data domain backup Data Collector policy" on page 127.

Add an EMC data domain backup Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add an EMC data domain backup Data Collector policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu**.**
5. Optionally, add an EMC Data Domain server from the policy screen. This action can also be completed in the Inventory.

   See "Adding/Configuring an EMC data domain server within the Data Collector policy window" on page 131.

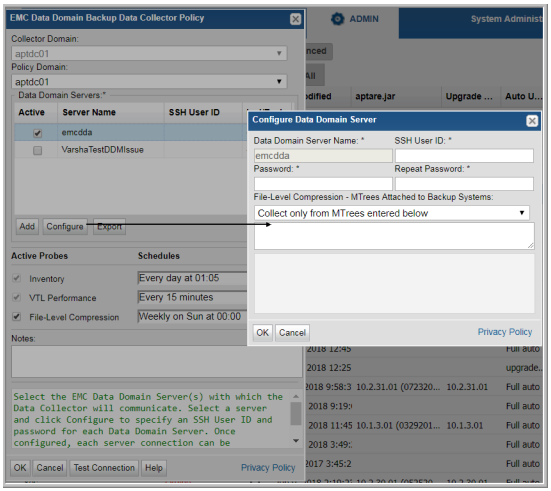
6 When selecting the File-Level Compression probe, additional configuration is required, as follows:

Select a Data Domain Server.

Select the File-Level Compression probe.

Click **Configure**.

See “Configure a data domain server for file-level compression collection” on page 132.



7 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

See See Table 9-1 on page 129.

Table 9-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 9-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Data Domain Servers*	When you check **Active** for a server shown in the list, a dialog window prompts for the SSH credentials. Alternatively, select a server and click **Configure**. You must indicate which servers are active. You must configure each server with a **Backup Type** of **Data Domain Server**. See “Add EMC data domain servers” on page 127.
Add	Click **Add** to add a Data Domain servers. The added servers are also displayed under **Inventory**. See “Adding/Configuring an EMC data domain server within the Data Collector policy window” on page 131. **Note:** If the hosts already exists, NetBackup IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.
Configure	Select a Data Domain server and click **Configure** to enter the SSH credentials that will be used to access the server. This allows provides access to setting up file-level compression. Refer to the following for additional setup information. See “Configure a data domain server for file-level compression collection” on page 132.
Export	Click **Export** to retrieve a list of all the Data Domain servers in a comma-separated values file.
Inventory Probe	Inventory details such as system, disk, tape, and VTL details are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 9-1 Policy Parameters *(continued)*

Field	Description
VTL Performance	Data associated with the performance of the Data Domain system virtual tape libraries (VTL) is collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available.
File-Level Compression Probe	When this probe is selected, MTrees can be entered into the File-Level Compression list configured for a Data Domain Server. The Data Domain Servers will then display an Include/Exclude column, with negative numbers indicating MTrees are excluded and positive numbers indicating MTrees are included. Hover your mouse over the Incl/Excl column to view the MTrees.If the column displays +0, it indicates no Mtrees have been included in the collection, and -0 indicates no Mtrees have been excluded, so all Mtrees will be collected from. For additional setup information refer to the following section. This section also contains information about RMAN and NetBackup jobs. See "Configure a data domain server for file-level compression collection" on page 132.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Adding/Configuring an EMC data domain server within the Data Collector policy window

Add and edit Data Domain servers directly from the data collector policy. This functionality is also available in the **Inventory**.

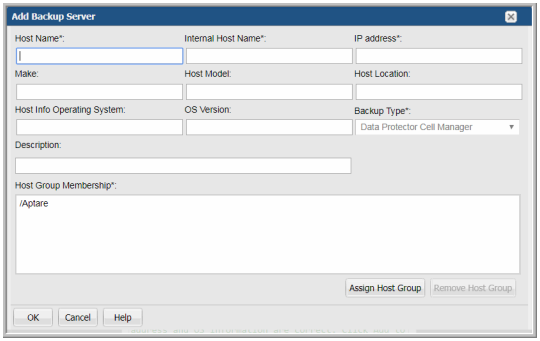
The **Data Domain Servers** table, shown in the policy, is populated using either of these methods. Servers added to this table are also displayed under **Inventory**. The Data Domain Servers table only displays available servers. These servers are not assigned to other policies within the domain.

Note: Data Collector policies can be in place for multiple servers, but a server cannot be assigned multiple policies within the same domain. If you try add a server that is already assigned to another Data Collector policy, you will be prompted to remove it from its current policy and reassign it.

---

1. Click **Add** on the EMC Data Domain Backup Data Collector Policy screen.
2. Select a Data Domain Server and click **Configure**.

   The **Add Backup Server** screen displays.



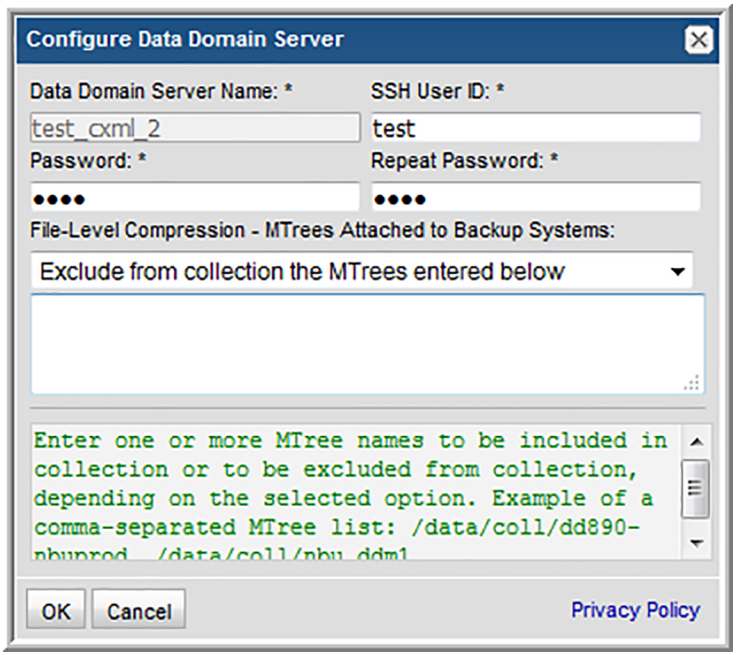
3. Enter or update values. Required fields are denoted by *.
4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups.

Configure a data domain server for file-level compression collection

In addition to the Names and Backup Type that were entered when an EMC Data Domain server was created, credentials are required to access and collect from the server. Also, if File-Level Compression collection from NetBackup systems is desired, MTree data must be listed.

File-Level Compression information can be instrumental in determining efficient storage strategies and identifying storage that can be reclaimed, thereby reducing

archive storage expenses. This data can be used to identify clients with inefficient de-duplication ratios, highlighting where de-deduplication is not an effective approach for certain backed-up files. For example, some hosts may be running database applications that are constantly producing unique bits of data. These hosts can consume much of the expensive Data Domain storage. Data Domain collection now can identify the largest offenders, which can then be moved to less expensive storage to avoid paying premium rates for de-duplication. Use the following report templates to take advantage of this collected data: Data Domain NetBackup File Compression Summary and the Data Domain NetBackup File Compression Detail.



1. Enter the following details and click **OK**.

Field	Description
Data Domain Server Name*	In order for Data Domain Servers to be listed in the policy window, they must be configured with a **Backup Type** of **Data Domain Server**. See "Add EMC data domain servers" on page 127.
SSH User ID*	The command-line interface (CLI) via SSH is used to gather Data Domain system data. This requires the SSH Service to be enabled and a Data Domain user that has a management role of 'user'. This User ID must be the same for all addresses listed in the System Addresses entry field for the Data Domain systems.

Field	Description
Password*	The password associated with the User ID.
Repeat Password*	The password associated with the User ID.
File-Level Compression - MTrees Attached to Backup Systems*	This selection is relevant only when the File-Level Compression probe is selected in the EMC Data Domain Backup Policy. Select the option to either include or exclude collection from the MTrees entered in the list. If the `exclude` option is selected with an empty MTree list, data from all MTrees will be collected. If the `include` option is selected with an empty MTree list, no file-level compression data will be collected. **Note:** Warning: Choosing to exclude file-level collection with an empty MTree list may cause collection to take several hours to complete.

Field	Description
Exclude from collection the MTrees entered below*	
OR	
Collect only from MTrees entered below	

Field	Description
	Enter one or more MTree names to be included in collection or to be excluded from collection, depending on the selected option. When compression information is collected from the MTree, an attempt is made to connect the file with a backup job that has previously been collected. A 'hint' must be specified to allow this to occur. Currently Oracle RMAN, Veritas NetBackup, and EMC Avamar are supported. For this probe to collect data, the RMAN / NetBackup / Avamar jobs must have been previously collected and all RMAN or NetBackup collection probes must have been run. **Note:** The **Exclude from collection the MTrees entered below** field will not collect for Avamar. To specify an MTree to which RMAN is sending backup files to, enter: RMAN:[MTree Name]. For NetBackup, enter: NBU:[MTree Name]. For Avamar, enter: AVM:[MTree Name]. Example of a comma-separated MTree list: RMAN:/data/col1/rman_su1, NBU:/data/col1/nbu_ddm1 AVM:/data/col1/avamar-1629802442 If you do not specify a hint, it is assumed that the Data Domain MTree contains files created by Veritas NetBackup. To run File-Level compression across all Mtrees on a Data Domain system, with a 'hint' to specify that the database attempt to link files with Backup jobs, enter: RMAN:* or NBU:* or AVM:* depending on the Backup system using the MTree. Mixed use of wildcards is not supported. Aggregated global and local compression rates for all NetBackup backup images are collected for all MTrees that are connected to the Active Data Domain servers via DDBOOST and where the NetBackup Data Collector is active and has successfully completed an initial data collection. **Warning:** Choosing to exclude collection with an empty MTree list may cause

Field	Description
	collection to take several hours to complete.

2. Click **OK** to save the policy.
3. On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.

Chapter 10

Configuration for Dell EMC NetWorker backup & recovery

This chapter includes the following topics:

- Introduction
- Prerequisites for adding Data Collectors (Dell EMC NetWorker Backup & Recovery)
- Installation overview (Dell EMC Networker Backup & Recovery)
- Adding a Dell EMC Networker Backup & Recovery Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Dell EMC NetWorker Backup & Recovery)

- EMC NetWorker data collection policies are implemented based on vendor version number. For EMC NetWorker versions post 9.2.1.x, collection is done using the policy titled: DELL EMC NetWorker Backup & Recovery.

See “Adding a Dell EMC Networker Backup & Recovery Data Collector policy ” on page 140.

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- The NetWorker REST API is installed with the NetWorker installation. As part of the installation process, an Apache Tomcat instance is installed and a nonroot -user, nsrtomcat, is created. If your system has special user security requirements, ensure that proper operational permissions are granted to the nsrtomcat users.
- With the NetWorker REST API, all endpoints other than initial landing endpoint (https://your-server-name:9090/nwrestapi/) require authentication. Once a user has been authenticated by the API, permissions to NetWorker resources will be based on the NetWorker permissions for that user.
- Default port number to connect to NetWorker REST API is 9090. This value is configurable in the policy.

Installation overview (Dell EMC Networker Backup & Recovery)

1. Update the Local Hosts file. This enables portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Dell EMC Networker Backup & Recovery data collector policy.

4. On the Data Collector Server, install the Data Collector software.
5. Validate the data collector installation.

Adding a Dell EMC Networker Backup & Recovery Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal to which you will add Data Collector policies. For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported. On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1 Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a collector if required.

3 Click **Add Policy**, and then select the vendor-specific entry in the menu.

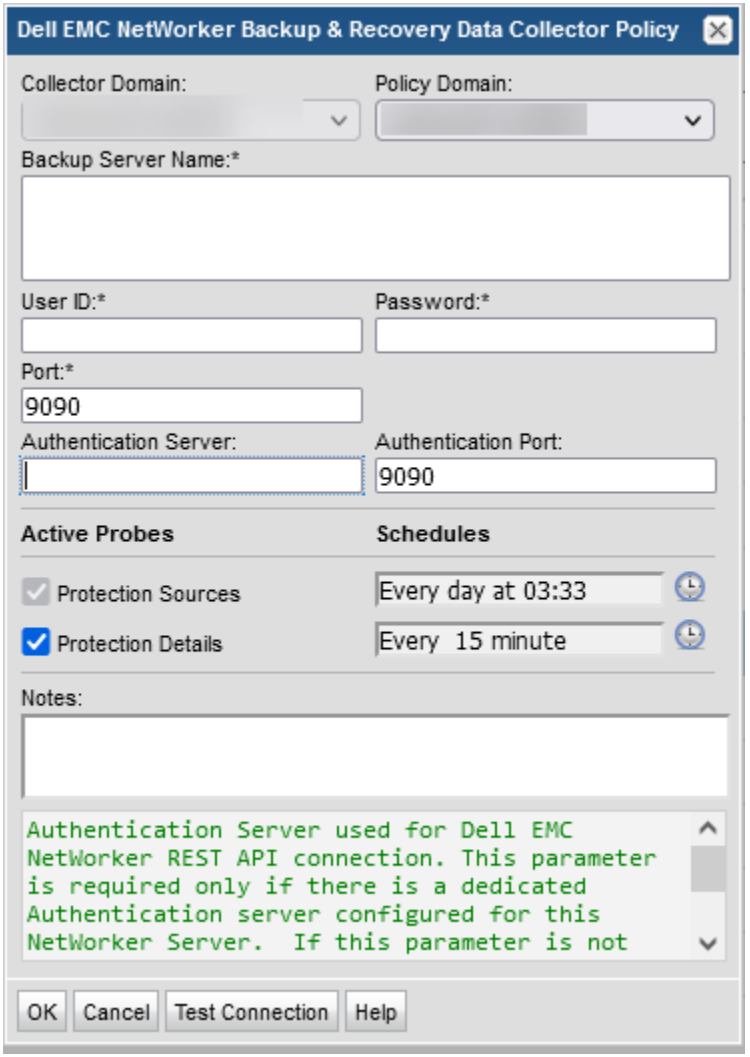


Table 10-1 Dell EMC Networker Backup and Recovery Data Collector policy

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 10-1 Dell EMC Networker Backup and Recovery Data Collector policy *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Backup Server Name*	Enter one or more Dell EMC NetWorker Backup & Recovery server host names to probe. Comma-separated host names are supported, for example: myhost1, myhost2. This field is required.
User ID*	View-only User ID for Dell EMC NetWorker REST API. This field is required.
Password*	Password for Dell EMC NetWorker REST API. This field is required.
Port*	Port used for Dell EMC NetWorker REST API connection. Default: 9090. This field is required.
Authentication Server	Authentication Server used for DELL EMC NetWorker REST API connection. **Note:** This parameter is required only if there is a dedicated authentication server configured for this NetWorker Server. If this parameter is not specified, collection assumes this NetWorker server uses its own local authentication service.
Authentication Port	Authentication Port used for DELL EMC REST API connection. Default value is 9090
Active Probes	
Protection Sources	Collects Storage Nodes, Devices, Protection Groups, Protection Policies, Workflows and their Actions.
Protection Details	Collects job and backup details.

Table 10-1 Dell EMC Networker Backup and Recovery Data Collector policy *(continued)*

Field	Description
Schedule	Click clock icon to create a schedule. By default, it is collected at 3.33 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the **Collector Administration** page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in**Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 11

Configuration of Dell EMC PowerProtect Data Manager (PPDM)

This chapter includes the following topics:

- Introduction
- Prerequisites for adding Data Collectors (Dell PowerProtect Data Manager)
- Installation overview (Dell PowerProtect Data Manager)
- Add a Dell PowerProtect Data Manager Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Dell PowerProtect Data Manager)

Identify a server where the Data Collector software will be installed.

Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- The user for Dell PowerProtect Data Manager data collection policy must be assigned the Administrator role. All the REST API requests executed are made using the GET method.

Installation overview (Dell PowerProtect Data Manager)

Use the following list to ensure that you complete each step in the order indicated:

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. On the Data Collector Server, install the Data Collector software.
4. Validate the Data Collector Installation.

Add a Dell PowerProtect Data Manager Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add the Data Collector policy.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, you can run collection on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data similar to that of a scheduled run and also collects logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add a Dell PowerProtect Data Manager policy:

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Select a Data collector from the list. Search for a collector if required.
3. Click **Add Policy** and then select **Dell PowerProtect Data Manager** from the menu.
4. Enter the policy parameters based on the description below and click **OK** to create and save the policy.

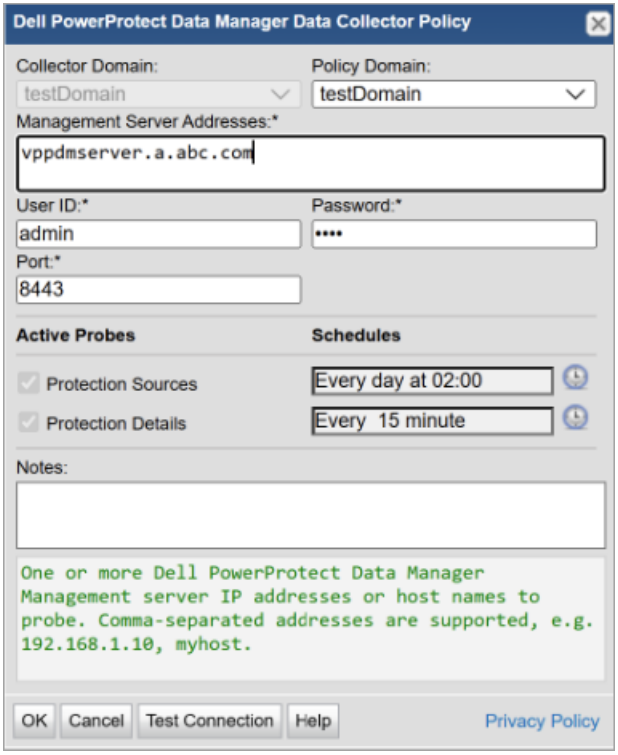


Table 11-1 Dell PowerProtect Data Manager Data Collector policy

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	Hostname or IP Address of the Dell PowerProtect Data Manager Server. Comma-separated host names are supported.
Port*	Server port number for REST API communication. The default port number is 8443 for SSL communications.
User ID*	Specify the user which has administrator role.
Password*	The password associated with the User ID.
Protection Sources	This probe focuses on APIs related to the collection of data protection information like System Configuration, Licenses, Node, Disks, Protection Policies, Protection Rules, Policies for disaster recovery and etc. By default, it is collected at 02:00 daily.
Protection Details	This probe focuses on APIs that help in collecting the information about Assets, Hosts, Activities, etc. By default, it is collected every 15 mintes.

Table 11-1 Dell PowerProtect Data Manager Data Collector policy *(continued)*

Field	Description
Schedules	Click the clock icon to create a schedule. By default, it is collected at 02:00 daily and every 15mins daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: ■ */30 * * * * means every 30 minutes ■ */20 9-18 * * * means every 20 minutes between the hours of 9 am and 6 pm ■ */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a collector policy are relative to the time on the collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your Data Collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Table 11-1 Dell PowerProtect Data Manager Data Collector policy *(continued)*

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services to be running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin** > **Data Collection** > **Collector Administration**. This on-demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 12

Importing generic backup data

This chapter includes the following topics:

- About generic backup data collection
- Configuring generic backup data collection
- CSV Format Specification
- Manually loading the CSV file

About generic backup data collection

Backup Manager can report on data from backup products that are not native to NetBackup IT Analytics--such as PureDisk, BakBone, and BrightStor. Using the backup vendor's export feature, create a comma-separated values (CSV) file. The NetBackup IT Analytics Data Collection process will import the data into the Portal database, to be included in NetBackup IT Analytics reports, such as the Job Summary report. The data can be scheduled for regular collection intervals.

Note: In addition to the regularly scheduled data collection, the CSV file also can be imported manually.

See "Manually loading the CSV file" on page 153.

Considerations

- Files can be imported more than once. Importing will not result in duplicate entries.

- Data is job-centric only--that is, no tape media or tape library information is imported.
- When checking Data Collection Status, the indicator may display a red error status, which for generic backup data collection, may not be a true error condition. The Generic Backup Data Collector checks the timestamp of the CSV file and if it is the same as the last collection, it does not attempt to re-import the data. In this regard, the Generic Backup data collection process differs from other collectors, as it expects to have data provided via the CSV file.
- Data is stored securely and can be used for historical tracking and trending.

Configuring generic backup data collection

The following tasks must be performed as part of the Generic Backup Data Collection setup:

- In the NetBackup IT Analytics Portal, create a host of type: Generic Backup Server. This is the server that is managing the backups of the clients for which you will be importing backup data.
- In the NetBackup IT Analytics Portal, add a Data Collector Policy of Product Type: Generic Backup. In this policy, supply the path to the CSV file.
  See " Add a generic backup Data Collector policy " on page 157.
- Create a comma-separated file of the backup/restore data--typically, a file that has been exported using the backup software utilities.
  See "CSV Format Specification" on page 151.

CSV Format Specification

Using the backup software, create a comma-separated file that contains the following 15 data elements from the backup/restore job(s). Note that each field must have an entry, even if it is a null entry within the commas. Field values cannot contain embedded commas. All string fields must be enclosed within single straight quotes.

Note: The CSV file must be UTF-8 encoded, however be sure to remove any UTF-8 BOMs (Byte Order Marks). The CSV cannot be properly parsed with these additional characters.

Table 12-1 CSV file with data elements.

Data Elements	Data Type	Value
VendorName	STRING	The name of the backup application used to perform the backup, enclosed in single straight quotes.
ClientName	STRING	The host name of the machine being backed up, enclosed in single straight quotes.
ClientIPAddress	NUMBER	The IP address of the machine being backed up. If an IP address is not available, simply use two single straight quotes (") or 'null' to indicate a blank/missing value.
VendorJobType	STRING	Valid values include: BACKUP or RESTORE--enclosed in single straight quotes.
StartDateString	DATE	The start date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). **Note:** Adhere to the specific date format--number of digits and special characters--as shown above.
FinishDateString	DATE	The end date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). **Note:** Adhere to the specific date format--number of digits and special characters--as shown above.
BackupKilobytes	NUMBER	The numeric size of the backup in kilobytes (otherwise use 0). Remember NetBackup IT Analytics uses 1024 for a KiB.
NbrOfFiles	NUMBER	The number of files that were backed up (otherwise use 0).
MediaType	STRING	The type of media that was used: T for Tape or D for Disk, enclosed within single straight quotes.
VendorStatus	NUMBER	A numeric job status: 0=Successful, 1=Partially Successful, or 2=Failed.
VendorJobId	STRING	Vendor job ID, enclosed in single straight quotes.
VendorPolicyName	STRING	Vendor policy name, enclosed in single straight quotes.
JobLevel	STRING	Job level, enclosed in single straight quotes. Example: Incremental, Full.
TargetName	STRING	File system backed up by the managed backup system (MBS), enclosed in single straight quotes.

Table 12-1 CSV file with data elements. *(continued)*

Data Elements	Data Type	Value
ScheduleName	STRING	Name of the backup schedule, enclosed in single straight quotes.

EXAMPLE: genericBackupJobs.csv

```
'Mainframe Backup','mainframe_name','10.10.10.10','BACKUP','2008-03-24
 10:25:00', '2008-03-24
11:50:00',3713,45221,'D',0,'413824','Retail_s01002030','Incremental','/I:/Shared/','Daily'
'UNIX tar backup','host_xyz.anyco.com','null','BACKUP','2008-03-24
10:22:00','2008-03-24
12:50:00',1713,45221,'T',1,'5201','HQ_Finance','Full','/D:/Backups/','Daily'
'ArcServe','host_123.anyco.com','null','RESTORE','2008-03-24
8:22:00','2008-03-24
9:12:00',0,0,'T',0,'2300','Retail_s03442012','Incremental','/I:/Shared/','EOM'
```

Manually loading the CSV file

Use the following procedure to manually load the Generic Backup CSV file into the Portal database.

Prerequisites:

- These scripts must be run on the **Collector Server**.
- The **checkinstall** script must be run first to register the event collector ID.

1. List the Data Collectors to get the **Event Collector ID** and the **Server ID**, which will be used in step 2.

   Windows:

   ```
   C:\opt\APTARE\mbs\bin\listcollectors.bat
   ```

   Linux:

   ```
   /opt/aptare/mbs/bin/listcollectors.sh
   ```

   In the output, look for the Event Collectors section associated with the Software Home--the location of the CSV file (the path that was specified when the Data Collector Policy was created). Find the **Event Collector ID** and **Server ID**.

   ```
   ==== Event Collectors ===
   ```

Event Collector Id: EVENT_1029161_9

```
Active: true
Active: true
Software Home: C:\gkgenericBackup.csv
Server Address: 102961
Domain: gkdomain
Group Id: 102961
Sub-system/Server Instance/Device Manager Id: 102961
Schedule: */10 * * * *
```

2. Use the following commands to load the data from the CSV file into the Portal database.

   Windows:

   ```
   C:\opt\APTARE\mbs\bin\loadGenericBackupData.bat <EventCollectorID>
    <ServerID> [verbose]
   ```

   Linux:

   ```
   /opt/aptare/mbs/bin/loadGenericBackupData.sh <EventCollectorID>
   <ServerID> [verbose]
   ```

Note: If you run the command with no parameters, it will display the syntax.

The load script will check to see if the backup server and client already exist; if not, they will be added to the database. The script then checks for a backup job with the exact same backup server, client, start date and finish date. If no matches are found, the job will be added; otherwise, it will be ignored. This prevents duplicate entries and allows the import of the script to be repeated, if it has not been updated. Once the load is complete, these clients and jobs will be visible via the NetBackup IT Analytics Portal and the data will be available for reporting.

Chapter 13

Configuration for generic backup

This chapter includes the following topics:

- Introduction
- Generic backup data collection
- Prerequisites for adding Data Collectors (Generic Backup)
- Installation overview (generic backup)
- Add generic backup servers
- Add a generic backup Data Collector policy
- Adding/Editing a generic backup server within the Data Collector policy
- Manually load the CSV file (generic backup)
- CSV format specification

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Generic backup data collection

Backup Manager can report on data from backup products that are not native to NetBackup IT Analytics—such as PureDisk, BakBone, and BrightStor. Using the backup vendor's export feature, create a comma-separated values (CSV) file. The Data Collection process will import the data into the Portal database, to be included in NetBackup IT Analytics reports, such as the Job Summary report. The data can be scheduled for regular collection intervals.

Note: In addition to the regularly scheduled data collection, the CSV file also can be imported manually.

See "Manually load the CSV file (generic backup)" on page 161.

Note: If the hosts already exists, NetBackup IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.

Prerequisites for adding Data Collectors (Generic Backup)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.

- Create a comma-separated file of the backup/restore data--typically, export the data using the backup software utilities.
  See “CSV format specification” on page 163.

Installation overview (generic backup)

1. Update the Local Hosts file. This enables Portal access.
2. Add Generic Backup Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the Generic Backup data collector policy.
5. On the Data Collector Server, install the Data Collector software.
6. Validate the Data Collector Installation.

Add generic backup servers

Add or edit Generic Backup servers to NetBackup IT Analytics using the data collector policy screen or through the Inventory.

Add a generic backup Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

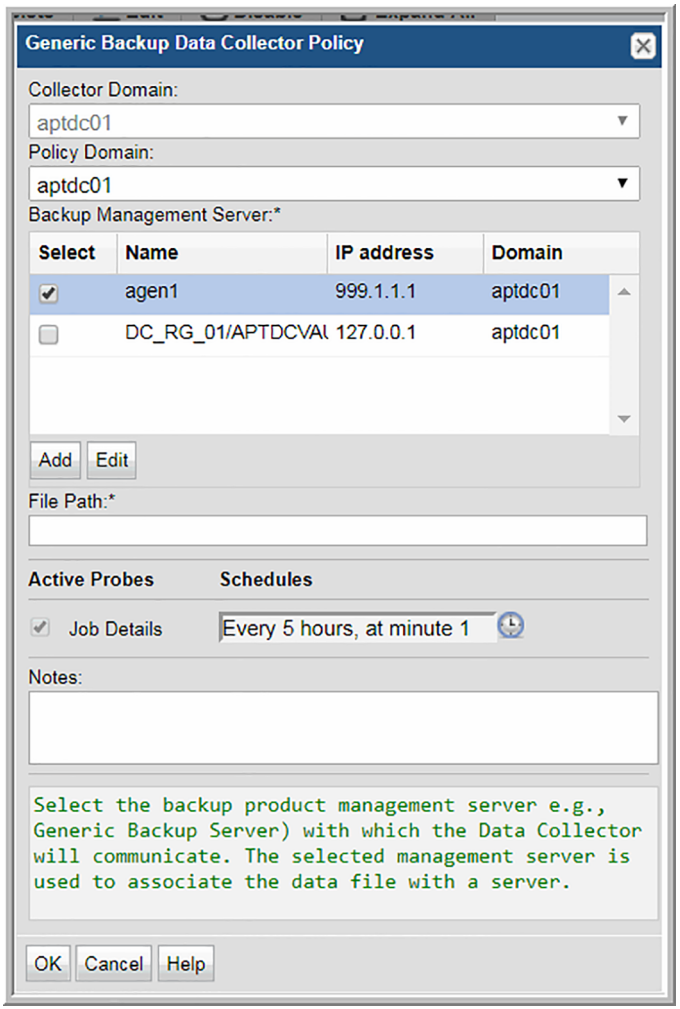
1 Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

Note: In this instance, select Generic Backup.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

See See Table 42-1 on page 418.

6 Optionally, add/edit a Generic Backup server from the policy screen. These operations can also be completed in the Inventory.

7 Click **OK** to save the policy.

Table 13-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Backup Management Server*	Select the backup product management server, e.g., Generic Backup Server with which the Data Collector will communicate. The selected management server is used to associate the data file with a server.
Add	Click **Add** to add a Generic Backup server. Added servers are also displayed in the Inventory. See “Adding/Editing a generic backup server within the Data Collector policy” on page 160.
Edit	Select a server and click **Edit** to update the server values.

Table 13-1 Policy Parameters *(continued)*

Field	Description
File Path*	The absolute file path on the Data Collector Server where the CSV data file is located. Typically, `C:\\Program Files\\Aptare\\mbs\\logs\\genericBackups.csv` for Windows, or `/opt/aptare/mbs/logs/genericBackups.csv` for Linux. Example: `/opt/aptare/mbs/logs/genericBackups.csv`
Job Details	Check the box to activate details collection. Click the clock icon to create a schedule frequency. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Adding/Editing a generic backup server within the Data Collector policy

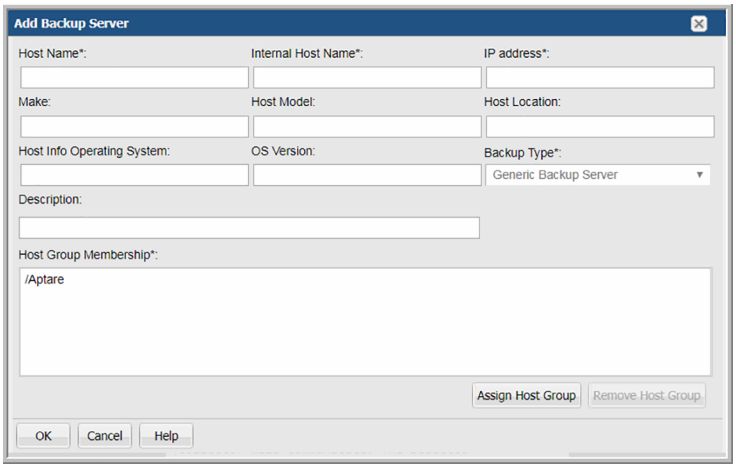
Add and edit Generic Backup servers directly from the data collector policy. This functionality is also available in the **Inventory**.

The **Backup Management Server** table, shown in the policy, is populated using either of these methods. Servers added from the policy are also displayed under **Inventory**. The **Backup Management Server** table only displays available servers. These servers are not assigned to other policies within the domain.

Note: Data Collector policies can be in place for multiple servers, but a server cannot be assigned multiple policies within the same domain. If you try add a server that is already assigned to another Data Collector policy, you will be prompted to remove it from its current policy and reassign it.

1. Click **Add** on the Generic Backup Data Collector Policy screen.
   - Select a Backup Management Server and click **Edit**.
2. The **Add Backup Server** screen displays.

Note: If the hosts already exists, NetBackup IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.



3. Enter or update values. Required fields are denoted by *.
4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups.

Manually load the CSV file (generic backup)

Use the following procedure to manually load the Generic Backup CSV file into the Portal database.

Pre-requisites:

- These scripts must be run on the **Data Collector server**.
- The `checkinstall` script must be run first to register the event collector ID.

1. List the Data Collectors to get the **Event Collector ID** and the **Host ID**, which will be used in step 2.

   Windows:

```
C:\opt\APTARE\mbs\bin\listcollectors.bat
```

Linux:

```
/opt/aptare/mbs/bin/listcollectors.sh
```

In the output, look for the Event Collectors section associated with the Software Home—the location of the CSV file (the path that was specified when the Data Collector Policy was created). Find the **Event Collector ID** and **Host ID**.

```
==== Event Collectors ===
          Event Collector Id: EVENT_1029161_9
          Active: true
          Active: true
          Software Home: C:\gkgenericBackup.csv
          Server Address: 102961
          Domain: gkdomain
          Group Id: 102961
          Server Id: 102961
          Schedule: */10 * * * *
```

2. Use the following commands to load the data from the CSV file into the Portal database.

   Windows:

   ```
   C:\opt\APTARE\mbs\bin\loadGenericBackupData.bat <EventCollectorID>
    <HostID>
   ```

   Linux:

   ```
   /opt/aptare/mbs/bin/loadGenericBackupData.sh <EventCollectorID>
   <HostID>
   ```

Note: If you run the command with no parameters, it will display the syntax.

The load script will check if the backup server and client already exist; if not, they will be added to the database. The script then checks for a backup job with the exact same backup server, client, start date and finish date. If no matches are found, the job will be added; otherwise, it will be ignored. This prevents duplicate entries and allows the import of the script to be repeated, if it has not been updated. Once the load is complete, these clients and jobs will be visible via the NetBackup IT Analytics Portal and the data will be available for reporting.

CSV format specification

Using the backup software, create a comma-separated file that contains the following 15 data elements from the backup/restore job(s). Note that each field must have an entry, even if it is a null entry within the commas. Field values cannot contain embedded commas. All string fields must be enclosed within single straight quotes.

Note: The CSV file must be UTF-8 encoded, however be sure to remove any UTF-8 BOMs (Byte Order Marks). The CSV cannot be properly parsed with these additional characters.

Table 13-2 CSV format specification

Name	Type	Value
VendorName	STRING	The name of the backup application used to perform the backup, enclosed in single straight quotes.
ClientName	STRING	The host name of the machine being backed up, enclosed in single straight quotes.
ClientIPAddress	NUMBER	The IP address of the machine being backed up. If an IP address is not available, simply use two single straight quotes ('') or 'null' to indicate a blank/missing value.
VendorJobType	STRING	Valid values include: BACKUP or RESTORE—enclosed in single straight quotes.
StartDateString	DATE	The start date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). **Note:** Adhere to the specific date format—number of digits and special characters—as shown above.

Table 13-2 CSV format specification *(continued)*

Name	Type	Value
FinishDateString	DATE	The end date and time of the backup job in the format: YYYY-MM-DD HH:MI:SS (enclosed in single straight quotes). **Note:** Adhere to the specific date format—number of digits and special characters—as shown above.
BackupKilobytes	NUMBER	The numeric size of the backup in kilobytes (otherwise use 0). Remember NetBackup IT Analytics uses 1024 for a KiB.
NbrOfFiles	NUMBER	The number of files that were backed up (otherwise use 0).
MediaType	STRING	The type of media that was used: T for Tape or D for Disk, enclosed within single straight quotes.
VendorStatus	NUMBER	A numeric job status: 0=Successful, 1=Partially Successful, or 2=Failed.
VendorJobId	STRING	Vendor job ID, enclosed in single straight quotes.
VendorPolicyName	STRING	Vendor policy name, enclosed in single straight quotes.
JobLevel	STRING	Job level, enclosed in single straight quotes. Example: Incremental, Full.
TargetName	STRING	File system backed up by the managed backup system (MBS), enclosed in single straight quotes.

Table 13-2 CSV format specification *(continued)*

Name	Type	Value
ScheduleName	STRING	Name of the backup schedule, enclosed in single straight quotes.

EXAMPLE: genericBackupJobs.csv

```
'Mainframe Backup','mainframe_name','10.10.10.10','BACKUP','2008-03-24
 10:25:00', '2008-03-24
11:50:00',3713,45221,'D',0,'413824','Retail_s01002030','Incremental',
'/I:/Shared/','Daily'
UNIX tar backup','host_xyz.anyco.com','null','BACKUP','2008-03-24
10:22:00','2008-03-24
12:50:00',1713,45221,'T',1,'5201','HQ_Finance','Full','/D:/Backups/','Daily'
ArcServe','host_123.anyco.com','null','RESTORE','2008-03-24
8:22:00','2008-03-24
9:12:00',0,0,'T',0,'2300','Retail_s03442012','Incremental',
'/I:/Shared/','EOM'
```

Chapter 14

Configuration for HP Data Protector

This chapter includes the following topics:

- Introduction
- Architecture overview (HP Data Protector)
- Prerequisites for adding Data Collectors (HP Data Protector)
- Installation overview (HP Data Protector)
- Identify HP Data Protector collection requirements
- Cell Manager commands for data collection
- Preparing for centralized data collection on a remote Cell Manager
- Configure the Data Collector server in Cell Manager (HP Data Protector)
- Configure an HP Data Protector admin user
- Validate HP Data Protector setup
- Add HP Cell Manager servers to NetBackup IT Analytics
- Add an HP Data Protector Data Collector policy
- Add/Edit a HP Data Protector server within the Data Collector policy
- Tune the configuration

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Architecture overview (HP Data Protector)

The HP Data Protector (HPDP) backup environment, known as a Data Protector Cell, is a network of systems with a common backup policy that is in the same time zone and on the same LAN/SAN. An HPDP Cell will usually include a Cell Manager, Installation Servers, Clients, and Backup Devices.

Cell Manager

HP Data Protector bases its backup management on the Cell Manager, which provides a central point for managing backup and restore sessions. Cell Manager executes Data Protector Software and Session Managers and also contains the Data Protector Internal Database (IDB). This database includes such details as backup duration, session IDs, and media IDs. Multiple cells can be configured into a group, enabling a single-point manager of cell managers.

Disk agent (backup agent)

Client systems that are being backed up must have an HP Data Protector Disk Agent installed. The disk agent manages the reads/writes from a disk on a system and also communicates with the media agent. The disk agent also is installed on the Cell Manager, enabling backup of its data, configuration details, and IDB.

Media agent

The media agent communicates with the disk agent and also reads/writes data on the media device.

Client systems

The client systems are the systems that are being backed up. These systems have the HP Data Protector Disk Agent installed on them.

User interface (UI)

The UI provides access to the Data Protector functionality and is used for configuration and administration tasks. It must be installed on the systems that are performing backup administration. Note that in addition to the graphical user interface, HPDP also has a command-line interface.

Prerequisites for adding Data Collectors (HP Data Protector)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 5555, WMI range of ports, Linux ssh 22
- The HP Data Protector (HPDP) client software version must match the specific version (major and minor) of the HPDP server being probed.

Installation overview (HP Data Protector)

1. Update the Local Hosts file. This enables Portal access.
2. Identify the specific HP Data Protector elements required for the Data Collector configuration:
   - See "Identify HP Data Protector collection requirements" on page 169.

- See "Configure the Data Collector server in Cell Manager (HP Data Protector)" on page 172.
- See "Configure an HP Data Protector admin user" on page 173.
- See "Validate HP Data Protector setup" on page 174.

3. In the NetBackup IT Analytics Portal, configure the HP Data Protector servers that are needed for data collection.

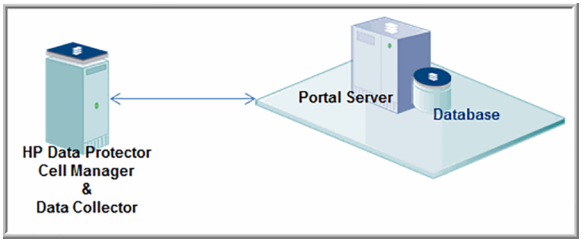
   See "Add HP Cell Manager servers to NetBackup IT Analytics" on page 174.
4. In the Portal, add a Data Collector, if one has not already been created.
5. Configure an HP Data Protector data collection policy.
6. On the Data Collector Server, install the Data Collector software.
7. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal--that is, a HOSTED installation (perhaps for a product evaluation)--skip this section and contact your hosting organization's representative to configure the hosted Portal for your Data Collector.

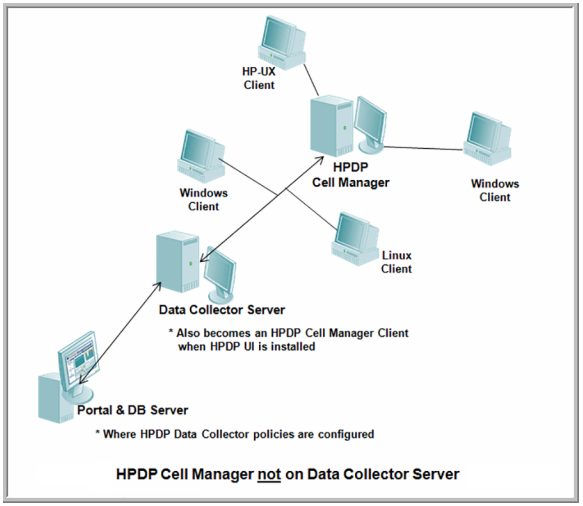
Identify HP Data Protector collection requirements

Two approaches can be taken when configuring collection from the HP Data Protector Cell Manager:

- Distributed Configuration: HP Data Protector Cell Manager and NetBackup IT Analytics Data Collector on the same server



- Centralized Configuration (Preferred): HP Data Protector Cell Manager and NetBackup IT Analytics Data Collector on different servers.



Cell Manager commands for data collection

When gathering data from HP Data Protector Cell Manager, several commands are executed, both on the Cell Manager server and on the Data Collector server. These commands are referenced later in this document.

For the purpose of preparing your environment for data collection, refer to the following table:

On the Data Collector Server	On the HPDP Cell Manager Server
omnicc	**omnidbutil**
omnicellinfo	
omnidb	
omnidownload	
omnimm	
omnirpt	

Preparing for centralized data collection on a remote Cell Manager

Assumption: The following steps assume that HP Data Protector Cell Manager has been installed on a server that is not the same as the NetBackup IT Analytics Data Collector server.

The following information will be used later when you configure a Data Collection Policy via the Portal.

On the HP Data Protector Cell Manager server:

1. Identify the Cell Manager Server's Name:

   _____

2. Identify the OS of the Cell Manager Server:

   _____

3. Identify the directory where the Cell Manager is installed. This path will be used later to fill in the Remote Software Location field when you configure the Data Collector policy in the NetBackup IT Analytics Portal:

   _____

   Typically, this location will be:

   Windows: C:\Program Files\Omniback

   Linux: /opt/omni

4. If the Data Collector is installed on a Linux OS, a WMI Proxy Server must be installed on a Windows system in order to collect data from a Cell Manager that is installed on a Windows system.

5. Configure the Data Collector server to be an HPDP Client.

   See "Configure the Data Collector server in Cell Manager (HP Data Protector)" on page 172.

6. The **omnidbutil** command is executed on the Cell Manager server to obtain drive status. Therefore, the following configuration is required:

   The user defined in the Data Collector must be an Admin user that the Cell Manager Server recognizes--either as a local user account or a Windows domain user account--that has execute rights to the **omnidbutil** command.

   See "Configure an HP Data Protector admin user" on page 173.

On the NetBackup IT Analytics Data Collector Server:

1. Make sure the Data Collector server has become the HPDP client with the HPDP User Interface component installed.

Find the directory (default is: `C:\Program Files\omniback\bin`) where the following commands are located and verify that the following commands exist in that directory. This validates that the User Interface was installed correctly.

```
omnicc
omnicellinfo
omnidb
omnidownload
omnimm
omnirpt
```

Configure the Data Collector server in Cell Manager (HP Data Protector)

When a Data Collector is configured in HPDP Cell Manager, it becomes a Client of Cell Manager. Therefore, the following requirements need to be considered.

Requirements for the Data Collector (Windows)

- Microsoft implementation of the TCP/IP protocol must be installed and running. The protocol must be able to resolve hostnames; and the computer name and hostname must be the same.
- Ensure that network access user rights are set under the Windows local security policy for the account performing the installation.

Steps to Configure the Data Collector Server in Cell Manager

The HP Data Protector UI can be deployed in a number of ways. The steps you take depend on whether you are using the original Data Protector UI (Windows only) or the Data Protector Java UI. Details for both user interfaces are provided in the steps below.

On the HP Data Protector Cell Manager Server:

1. Start the HP Data Protector UI (choose one of the following User Interfaces).
   - Original Data Protector UI (Windows only):
     Start > Programs > HP Data Protector > Data Protector Manager
   - Data Protector Java UI (Windows):
     Start > Programs > HP Data Protector > Data Protector Java GUI Manager

Then, in the Connect to Cell Manager dialog, select or type the name of the Cell Manager and click **Connect**.

- Data Protector Java UI (Linux):

```
/opt/omni/java/client/bin/javadpgui.sh
```

2. Make sure that you have a user that is a **Local System Administrator account from the Data Collector Server**.

   See “Configure an HP Data Protector admin user” on page 173.

3. Validate the conditions.

   See “Validate HP Data Protector setup” on page 174.

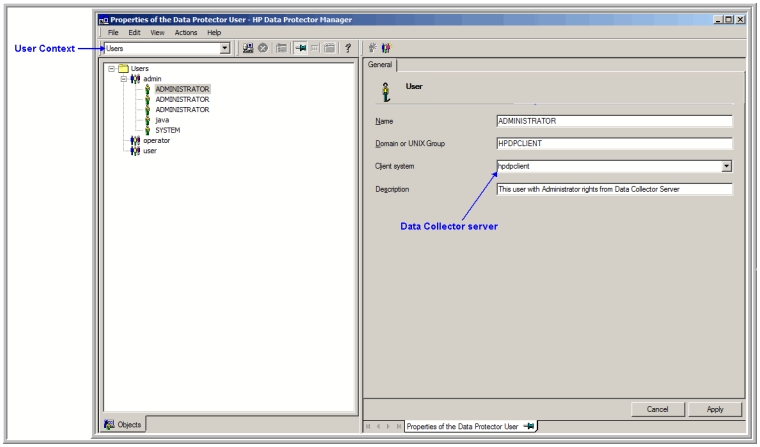
Configure an HP Data Protector admin user

Note: If the Data Collector is installed on the same server as Cell Manager, skip this section.

If the Data Collector is installed on a different server from the Cell Manager server, the following tasks must be performed.

On the HP Data Protector Cell Manager server:

1. Open the HP Data Protector UI.
2. Make sure you have a user that is a **Local System Administer account from the Data Collector Server.**
   - Switch to the User context and add the user under an “Admin” class.



Validate HP Data Protector setup

On the Data Collector Server:

1. Execute the following commands from the HP Data Protector backup software location to validate that the setup conditions have been meet:

   ```
   omnicc -version -server <CellManagerServerName>
   omnicc -check_licenses -server <CellManagerServerName>
   ```

   - If the first command does not run correctly, it means that the User Interface component has not been installed correctly.
   - If the first command runs, but the second command displays, “Insufficient permissions. Access denied,” it means that the configuration of the Data Collector Server in the HP Cell Manager server has failed.

Add HP Cell Manager servers to NetBackup IT Analytics

On the Portal, repeat these steps for each HP Data Protector Cell Manager server.

1. Open a browser window and point it to your instance of the Portal (for example: http://aptareportal.yourdomain.com).
2. Login as an admin user (e.g. admin@yourdomain.com).
3. Add a Backup Server. This can be done directly from the data collector policy or from the Inventory.
4. Enter values for all required fields (denoted by an *) and click **OK**. The field, Internal Host Name, needs to match the host name of the HP Cell Manager Server. Ensure you select **HP Cell Manager Server** as the Type. The fields External Name, Make and Model are not used by the application for anything other than display purposes.
5. Select the Host Group while you are adding the backup server.

Note: If a server group hierarchy has already been established in the application, you can select the host group to which you would like the **HP Cell Manager Server** to belong, although it is recommended that you add the **HP Cell Manager Server** to the top-level folder.

Add an HP Data Protector Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu**.**

5 Optionally add an HP Data Protector Backup Server from the policy screen. This action can also be completed in the Inventory.

See “Add/Edit a HP Data Protector server within the Data Collector policy” on page 180.

6 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

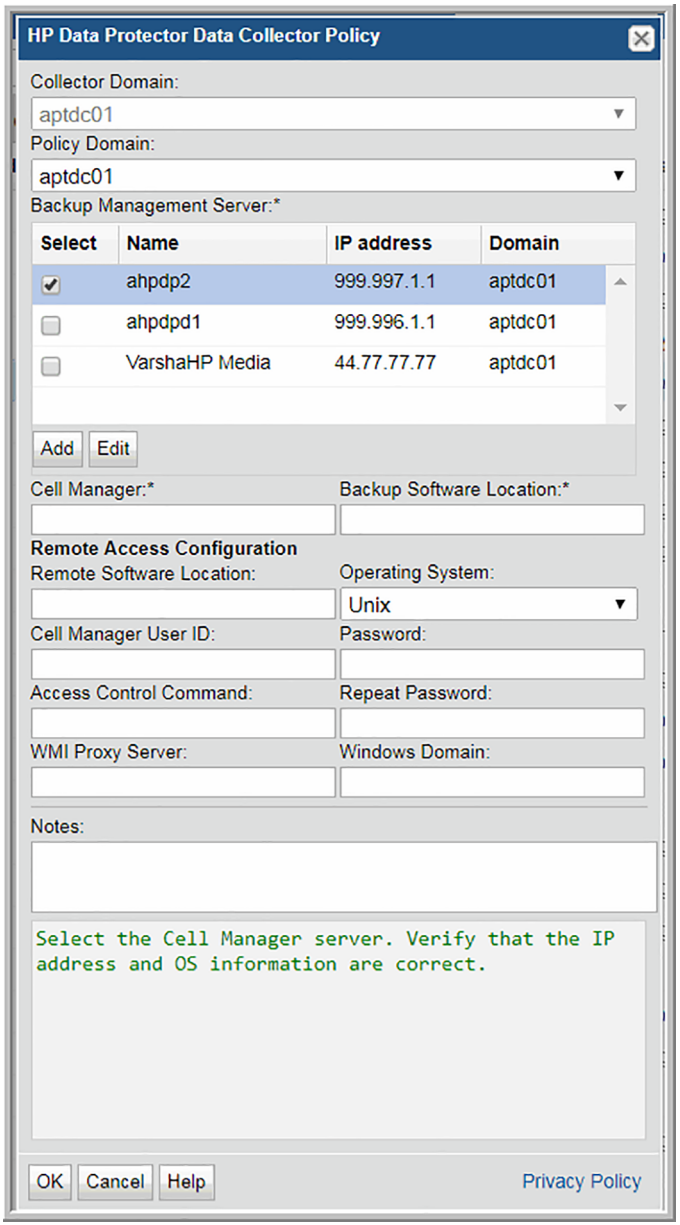


Table 14-1

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Backup Management Server*	Select the Cell Manager server. Verify that the IP address and OS information are correct.
Add	Click **Add** to add a Cell Manager server. Added servers are also displayed in the **Inventory**. **Note:** If the hosts already exists, NetBackup IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click Ok to update Host details / Host Type.
Edit	Select a Cell Manager server and click **Edit** to update the values.

Table 14-1 *(continued)*

Field	Description
Cell Manager*	The Cell Manager is the server that runs session managers and core software to manage the backup details in the HP Data Protector database. Enter the name or IP address of the HPDP Cell Manager server. In the majority of cases, this field should contain the same server that you selected from the above Backup Management Server list; however, for special-case situations, an alias may be entered. Example: HPSERVER
Backup Software Location*	On the Data Collector server, this is the home directory of the HP Data Protector Admin Client software—that is, the location of the omni commands, such as omnicellinfo and omnireport—to be used by the Data Collector server.
Remote Access Configuration The following parameters are required only when the Data Collector server is different from the Cell Manager server.	
Remote Software Location	The home directory on the HP Data Protector server where Cell Manager is installed. Typically C:\Program Files\Omniback for Windows, or /opt/omni for Linux; only required for remote access to Cell Manager.
Operating System	The operating system on which the HP Data Protector Data Collector is running; only required for remote access to Cell Manager.
Cell Manager User ID	An Admin User that the Cell Manager server recognizes--either a local user account or a Windows domain user account--that has execute rights to the omnidbutil command. This command is used to obtain drive status. Required only when the Data Collector is on a server that is different from the Cell Manager server.
Password/Repeat Password	Password for the Cell Manager User ID on the remote system.
Access Control Command	For Linux hosts: If the user ID is not root, provide the full path to access control; Example: /usr/bin/sudo

Table 14-1 *(continued)*

Field	Description
WMI Proxy Server	Enter the server name or IP address where the WMI Proxy is installed. Only needed if collecting from Windows hosts and when the Data Collector is on a server that is different from the Cell Manager server. If the Data Collector is installed on a Linux OS, a WMI Proxy Server must be installed on a Windows system in order to collect data from a Cell Manager that is installed on a Windows system.
Windows Domain	The Windows domain, if applicable.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Add/Edit a HP Data Protector server within the Data Collector policy

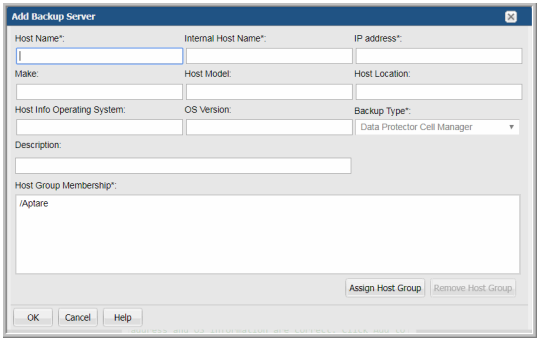
Add and edit HP Data Protector Cell Manager servers directly from the data collector policy. This functionality is also available using the **Inventory**.

The **Backup Management Servers** table, shown in the policy, is populated using either of these methods. Servers added to this table are also displayed under **Inventory**. The Backup Management Servers table only displays available servers. These servers are not assigned to other policies within the domain.

Note: Data Collector policies can be in place for multiple servers, but a server cannot be assigned multiple policies within the same domain. If you try add a server that is already assigned to another Data Collector policy, you will be prompted to remove it from its current policy and reassign it.

---

1. Click **Add** on the HP Data Protector Data Collector Policy screen.
   - Select a Cell Manager server and click **Edit**.
2. The **Add Backup Server** screen displays.



3. Enter or update values. Required fields are denoted by *.
4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups.
5. Click **OK** to save the policy.
6. On the Data Collector server, install/update the Data Collector software.

Tune the configuration

By default, the HP Data Protector Data Collector does not collect data for Not Configured File Systems for Backup Specifications. This collection feature is disabled because, in certain environments, it may impact performance.

To enable collection: edit the following file and make the modifications via the command-line interface.

1. Edit the file: <aptare_home>/mbs/bin/aptarecron.sh|bat

   Locate the **jvm** line and add: **-DenableFS=true**

Chapter 15

Configuration for IBM Spectrum Protect (TSM)

This chapter includes the following topics:

- Introduction
- Architecture overview (IBM Spectrum Protect -TSM)
- Prerequisites for adding data collectors (IBM Spectrum Protect - TSM)
- Installation overview (IBM Spectrum Protect - TSM)
- Add IBM Spectrum Protect (TSM) servers
- Adding an IBM Spectrum Protect (TSM) Data Collector policy
- Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy
- Import IBM Spectrum Protect (TSM) information
- Export IBM Spectrum Protect (TSM) server information

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed. This enables you to determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Architecture overview (IBM Spectrum Protect -TSM)

For each IBM Spectrum Protect (TSM) Instance, the Data Collector will establish connections to the database using the command, dsmadmc. The Data Collector Configuration file contains all the connection information for each instance including such parameters as the user name and password for login, the instance name, IP address of the IBM Spectrum Protect (TSM) server, and port.

The Data Collector will use various QUERY and SELECT commands via dsmadmc to obtain its information from each separate IBM Spectrum Protect (TSM) Instance. The information is then sent via http(s) to the Portal. A user can then launch a web browser to use the Portal to see a global view of all of their IBM Spectrum Protect (TSM) servers and IBM Spectrum Protect (TSM) Instances.

IBM Spectrum Protect (TSM) - servers and instances defined

IBM Spectrum Protect (TSM) Server- The system that is running the server software. This system will be known by its host name. It is the physical or virtual host onto which one or more IBM Spectrum Protect (TSM) instances reside.

IBM Spectrum Protect (TSM) Instance - A separate instance of the server software running on a TSM server. A single TSM server can run multiple TSM Instances. This is normally implemented by setting up a separate set of client and administration ports for each TSM Instance. In the architecture illustration, there are two TSM servers—one has a single TSM Instance running on it and the other Host has two TSM Instances running on it.

Prerequisites for adding data collectors (IBM Spectrum Protect - TSM)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same

server, verify that the Portal and Data Collector software do not reside in the same directory.

- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- A IBM Spectrum Protect (TSM) client must be installed on the Data Collector server with the dsmadmc command available.
- Ports to IBM Spectrum Protect (TSM) instances must be open. Each instance will have a unique port. Make note of these instance/port combinations for data collection. Typically, TCP 1500 is the default port.
- The Data Collector server can be any server within your network that is Java 1.7 compatible and with **dsmadmc** installed. For Linux platforms, this server must be added to **dsm.sys** so the Data Collector can use the **dsmadmc** command.
- For a data collector installed on Windows, the parameter variable **DSM_CONFIG** *MUST* be configured. The value of the variable should be the full path and filename for the `dsm.opt` file.

Note: For a default installation of the Windows TSM client, the location is: `C:\Program Files\Tivoli\TSM\baclient\dsm.opt`

To add the parameter, navigate to *Admin* > *Advanced* > *Parameters*. Click **Add** and **Add Advanced Parameter** dialog box is displayed. Click **Add** to add the parameter.

Installation overview (IBM Spectrum Protect - TSM)

1. Update the local hosts file.
2. Add IBM Spectrum Protect (TSM) Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the IBM Spectrum Protect (TSM) data collector policy.
5. On the Data Collector Server, install the Data Collector software.
6. Validate the Data Collector Installation.

Add IBM Spectrum Protect (TSM) servers

Repeat these steps for each IBM Spectrum Protect (TSM) server:

1. In the Inventory, add a host for each IBM Spectrum Protect (TSM) server.
   - Host Name - Displayed in the Portal.
   - Internal Host Name - Must match the host name of the IBM Spectrum Protect (TSM) server.
   - IP Address
   - Backup Type = IBM Spectrum Protect (TSM) Server

Note: If a host group hierarchy has already been established in the application, you can find the host group to which you would like the IBM Spectrum Protect (TSM) server to belong, although it is recommend adding the TSM server to the top-level folder.

Note: You can also add IBM Spectrum Protect (TSM) servers directly from the Data Collector policy screen.

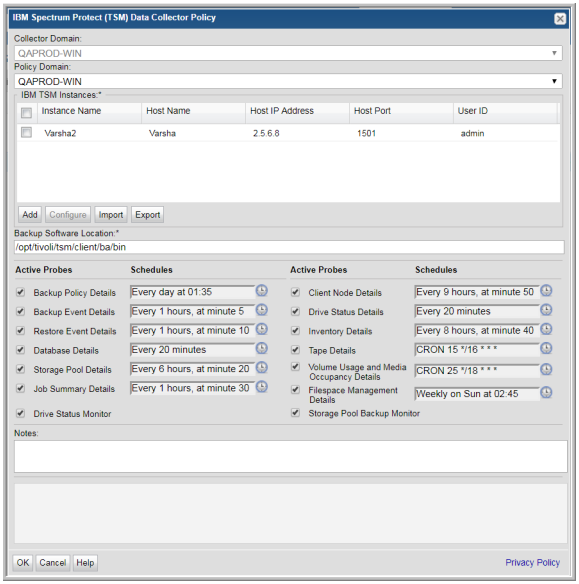
See "Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy" on page 190.

Adding an IBM Spectrum Protect (TSM) Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5. Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

   See See Table 15-1 on page 186.
6. Click **OK** to save the policy.
7. On the Data Collector server, install/update the Data Collector software.

Table 15-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 15-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. (The Collector Domain is the domain that was supplied during the Data Collector installation process.) The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
IBM Spectrum Protect (TSM) Instances	
Active	Click **Active** to indicate the IBM Spectrum Protect (TSM) server/instances to use in the data collection policy. Multi-select is supported. If additional fields must be configured, the **Configure Server** dialog is automatically displayed when you make your selection.
Add	Click **Add** to add an IBM Spectrum Protect (TSM) server/instance. The IBM Spectrum Protect (TSM) servers added to this table using **IBM Spectrum Protect (TSM) Data Collector Policy** screen are also displayed in the Inventory **Note:** Data Collector policies can be in place for multiple instances, but an instance cannot exist in multiple policies. See “Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy” on page 190.
Configure	Select a row in the **IBM Spectrum Protect (TSM) Instances** table. Double-click or click **Configure** to revise or add information to the TSM server/instance you selected. See “Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy” on page 190.

Table 15-1 Policy Parameters *(continued)*

Field	Description
Import	Click **Import** to browse for the CSV file in which you entered the IBM Spectrum Protect (TSM) server/instance configuration details. This enables you quickly add a list of IBM Spectrum Protect (TSM) instances or servers. See "Import IBM Spectrum Protect (TSM) information" on page 192.
Export	Click **Export** to create and download a comma-separated values (CSV) file containing all the host/instance information listed in the **IBM Spectrum Protect (TSM) Instances** table. This enables you to extract your IBM Spectrum Protect (TSM) server information and transfer it easily into a spreadsheet or some other media. See "Export IBM Spectrum Protect (TSM) server information" on page 193.
Backup Software Location*	The home directory of the TSM Admin Client software--that is, the dsmadmc command on the Data Collector server. Typically `C:\Program Files\Tivoli\TSM\baclient` for Windows, or /opt/tivoli/tsm/client/ba/bin for Linux
Active Probes and Schedules	
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Backup Policy Details	Collects backup policy details including policy name, policy identifier, date and time as it relates to the specified IBM Spectrum Protect (TSM) instances/servers.
Backup Event Details	Collects backup event details including backup type, client names, duration, dates, size, files, directories and so on.
Restore Event Details	Collects restore event details such as job duration, number of files backed up and also skipped, amount of data restored, and restore job status.

Table 15-1 Policy Parameters *(continued)*

Field	Description
Database Details	Collects IBM Spectrum Protect (TSM) backup database details, such as total capacity, available space, cache hit percentages, and buffer requests.
Storage Pool Details	Collects IBM Spectrum Protect (TSM) storage pool information, such as migration and reclamation details.
Job Summary Details	Collects IBM Spectrum Protect (TSM) job summary details including client name, node name, backup type, dates, duration and so on, as it relates to the specified IBM Spectrum Protect (TSM) instances/servers.
Client Node Details	Collects client node details covered by the selected policy domain as they relate to the specified IBM Spectrum Protect (TSM) instances/servers.
Drive Status Monitor	Continuously monitors the IBM Spectrum Protect (TSM) console for drive status messages, there is no schedule.
Drive Status Details	Collects drive status details including, drive name, library name, status, start and end times as it relates to the specified IBM Spectrum Protect (TSM) instances/servers.
Inventory Details	Collects IBM Spectrum Protect (TSM) host details including host name, IP Address, Host ID, and port number. Also collects from drives and paths such as device type, device name, library name, and ACS drive ID.
Tape Details	Collects the tape details including media type name, media status, storage pool name, and estimated capacity.
Volume Usage and Media Occupancy Details	Collects client and node information, and then for each node it retrieves the volume usage details from the IBM Spectrum Protect (TSM) instance or server. For each volume, collects details of media occupying the storage pool. Details include the type and size of the media.
Filespace Management Details	Collects filespace details such as capacity, backup start/finish dates, and the percentage of the filespace that is occupied.
Storage Pool Backup Monitor	Continuously monitors the IBM Spectrum Protect (TSM) console for storage pool migration messages, there is no schedule.

Table 15-1 Policy Parameters *(continued)*

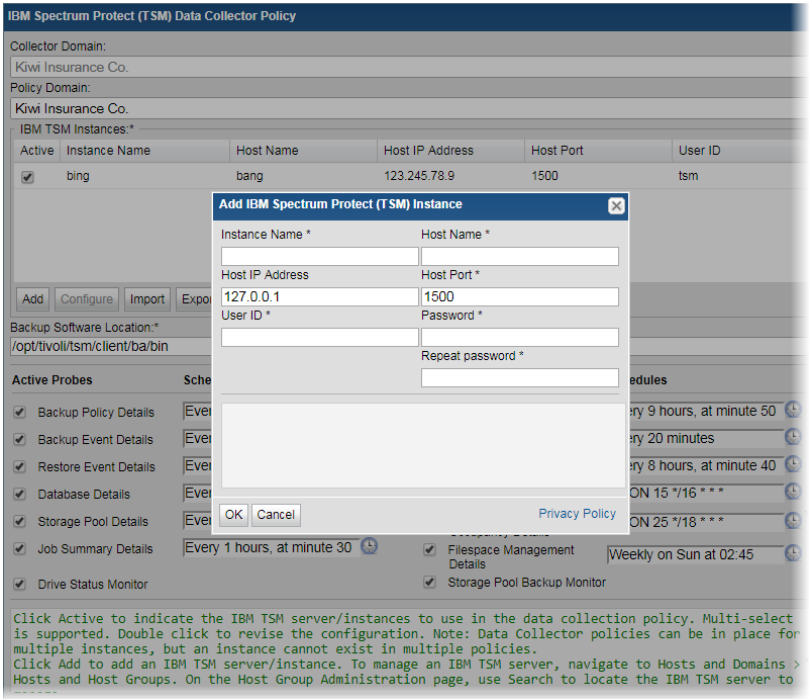
Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy

Add IBM Spectrum Protect (TSM) servers/instances by clicking **Add**, or by importing using a .CSV file. The **IBM TSM Instances** table is populated using this method. Servers added to this table are also displayed under **Host Management** and **Host Group Administration**. The **IBM TSM Instances** table only displays available Instances that are not assigned to other policies within the domain.

Note: Data Collector policies can be in place for multiple instances but an instance cannot be assigned multiple policies within the same domain. If you try add an instance that is already assigned to another Data Collector policy, you will be prompted to remove it from its current policy and reassign it.

1. Click **Add** on the **IBM Tivoli Storage Manager Data Collector Policy** screen. The **Add IBM Tivoli Storage Manager Instance** screen displays.



2. Enter the values:

Field	Description
Instance Name	The name assigned to the IBM Spectrum Protect (TSM) instance. This is a separate instance of the server software running on a IBM Spectrum Protect (TSM) server. A single server can run multiple instances. An instance is defined by instance name, host name, and port number.
Host Name	The name of the IBM Spectrum Protect (TSM) server. This is the host running the IBM Spectrum Protect (TSM) server software. This system will be known by its host name. If you do not know the Host Name, you can enter the IP Address in this field.
Host IP Address	The IP address of the host running the IBM Spectrum Protect (TSM) server software. By default it is set to 127.0.0.1. You can revise it as required and this field is not mandatory.
Host Port	Port number used by dsmadmc to communicate with the IBM Spectrum Protect (TSM) Instance. Each instance will have its own specific port. By default it is set to 1500. You can revise it, but the field is required.
User ID	IBM Spectrum Protect (TSM) user ID with query and select privileges.

Field	Description
Password	Password associated with the IBM Spectrum Protect (TSM) administrator account credentials.

Import IBM Spectrum Protect (TSM) information

You can quickly add a list of IBM Spectrum Protect (TSM) servers/instances using the Import function. The information is displayed in the IBM TSM Instances table on the IBM Spectrum Protect (TSM) Data Collector Policy screen. Because the import is done within a policy, the host group/domain selected for the policy is used for server location.

CSV format specifications

Before importing, create a comma-separated values (CSV) file of IBM Spectrum Protect (TSM) server data. The CSV file must use the following order to populate the fields correctly when importing:

1. Instance Name
2. Host Name
3. Host IP Address
4. Admin Port
5. User ID
6. Password

To import IBM Spectrum Protect (TSM) hosts

1 Prepare the CSV according to CSV format specifications.

See "CSV format specifications" on page 192.

2 Select **Admin > Data Collection > Collector Administration.**

3 Search for a Collector if required.

4 Select a collector.

5 Click **Add Policy** and select **IBM Spectrum Protect (TSM)**. The **IBM Spectrum Protect (TSM) Data Collector Policy** screen is displayed.

6 Click **Import**. The **Import IBM Spectrum Protect (TSM) Instances** dialog is displayed. You can browse for the CSV file you created.

Export IBM Spectrum Protect (TSM) server information

Use **Export** to create a comma-separated values (CSV) file containing all the server information listed in the **IBM TSM Instances** table.

Click **Export** to download the CSV file to your local system.

Chapter 16

Configuration for NAKIVO Backup & Replication

This chapter includes the following topics:

- Introduction
- Prerequisites for adding data collectors (NAKIVO Backup & Replication)
- Installation overview (NAKIVO Backup & Replication)
- Add a NAKIVO Backup & Replication Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (NAKIVO Backup & Replication)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- NAKIVO Backup & Replication Server must have the license that allows access to NetBackup IT Analytics reporting REST APIs. User credentials to access NetBackup IT Analyticsreporting REST APIs are also required.
- Install only one Data Collector on a server (or OS instance).
- Default port 4443 - Director Web UI port (used during NAKIVO Backup & Replication installation.

Installation overview (NAKIVO Backup & Replication)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the NAKIVO Backup & Replication data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector Installation.

Add a NAKIVO Backup & Replication Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.
5. Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

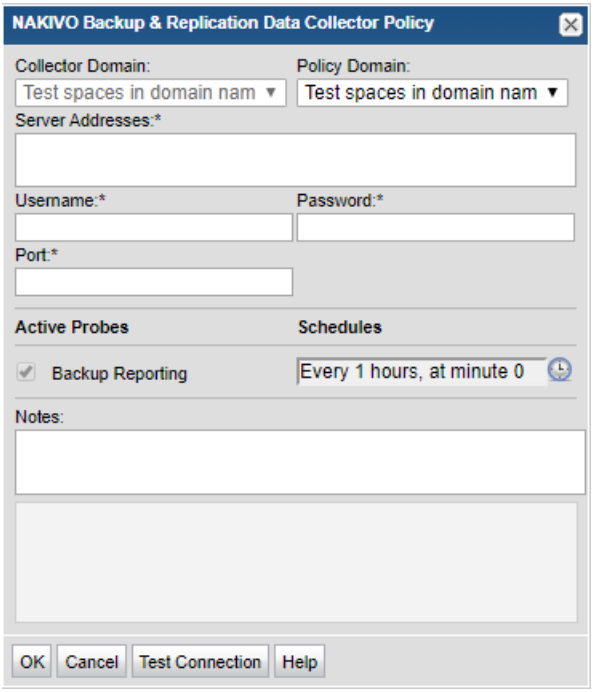


Table 16-1 NAKIVO Backup & Replication Data Collector Policy

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Server Address	Enter one or more NAKIVO Backup & Replication server IP addresses to probe. Comma-separated addresses are supported.
Port	Enter the value for NAKIVO server's Director Web UI port. Default port is 4443.
Username	Enter the user name used for the NAKIVO Backup & Replication system.
Password*	Password for NAKIVO Backup & Replication Server associated with the Username.
Active Probes	
Backup Reporting	Probe for NAKIVO Backup & Replication system.
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 16-1 NAKIVO Backup & Replication Data Collector Policy *(continued)*

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in**Admin>Data Collection>Collector Administration** . This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See Working with On-Demand Data Collection for details.

Chapter 17

Configuration for Oracle Recovery Manager (RMAN)

This chapter includes the following topics:

- Introduction
- Prerequisites for adding data collectors (Oracle Recovery Manager - RMAN)
- Installation overview (Oracle Recovery Manager - RMAN)
- Add an Oracle Recovery Manager (RMAN) Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (Oracle Recovery Manager - RMAN)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Database Host and Port: Identify the hostname of the server where the database in which the RMAN data resides as well as the port this database is listening on. The default port is 1521.
- The configured user must exist in all configured instances with the same password. The user should the CREATE SESSION privilege and have the following permissions in the schemas to be collected from:
  - User must have the SELECT_CATALOG_ROLE to retrieve RMAN data from the Dynamic Performance (V$) views:

    ```
    GRANT SELECT_CATALOG_ROLE TO <user>;
    ```

  - User requires the RECOVERY_CATALOG_OWNER (or RECOVERY_CATALOG_USER role in Oracle 12c or later) for example:

    ```
    GRANT RECOVERY_CATALOG_OWNER TO <user>;
    ```

    or

    ```
    GRANT RECOVERY_CATALOG_USER TO <user>;
    ```

    or have a virtual private catalog set up for the user (see Oracle documentation).
  - User must have SELECT permission to V$INSTANCE and V$DATABASE (which is included in SELECT_CATALOG_ROLE).

Installation overview (Oracle Recovery Manager - RMAN)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Oracle Recovery Manager (RMAN) data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Add an Oracle Recovery Manager (RMAN) Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the*Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

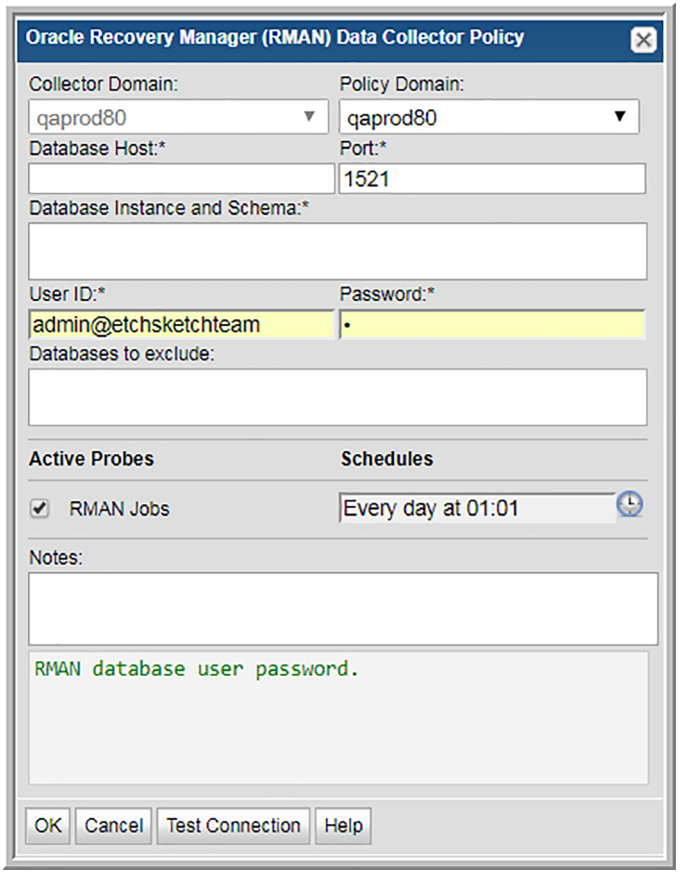
To add the policy

1 Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

See See Table 17-1 on page 202.

Table 17-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 17-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Database Host	RMAN database server.
Port	Database listener port. By default the port is 1521.
Database Instance and Schema	RMAN database instance names and optional schemas, each formatted as INSTANCE.SCHEMA and separated by commas or spaces. If a schema is not specified then all Recovery Catalog schemas in the instance accessible to the user ID will be collected. If there are no accessible Recovery Catalog schemas then the Dynamic Performance (V$) views will be collected. Use the PUBLIC schema to force collection from the V$ views, or a Recovery Catalog schema name to only collect from that schema. Example (to collect both from a Recovery Catalog schema and the V$ views in the DB1 instance): DB1.RMAN, DB1.PUBLIC
User ID*	This field is required. RMAN database user name. This must be a user with SELECT permission for the Dynamic Performance (V$) views and any Recovery Catalog schema views being collected from.
Password*	This field is required. RMAN database user password.
Databases to exclude	RMAN numeric database IDs to exclude from collection, separated by commas or spaces.
Active Probes	
RMAN Jobs	Probe for Oracle Recovery Manager (RMAN) jobs.

Table 17-1 Policy Parameters *(continued)*

Field	Description
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin**>**Data Collection**>**Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. Refer to Working with On-Demand Data Collection for details.

Chapter 18

Configuration for Rubrik Cloud Data Management

This chapter includes the following topics:

- Introduction
- Prerequisites for adding Data Collectors (Rubrik Cloud Data Management)
- Installation overview (Rubrik Cloud Data Management)
- Add a Rubrik Cloud Data Management Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Rubrik Cloud Data Management)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Read-only Rubrik user account

Installation overview (Rubrik Cloud Data Management)

Use the following list to ensure that you complete each step in the order indicated.

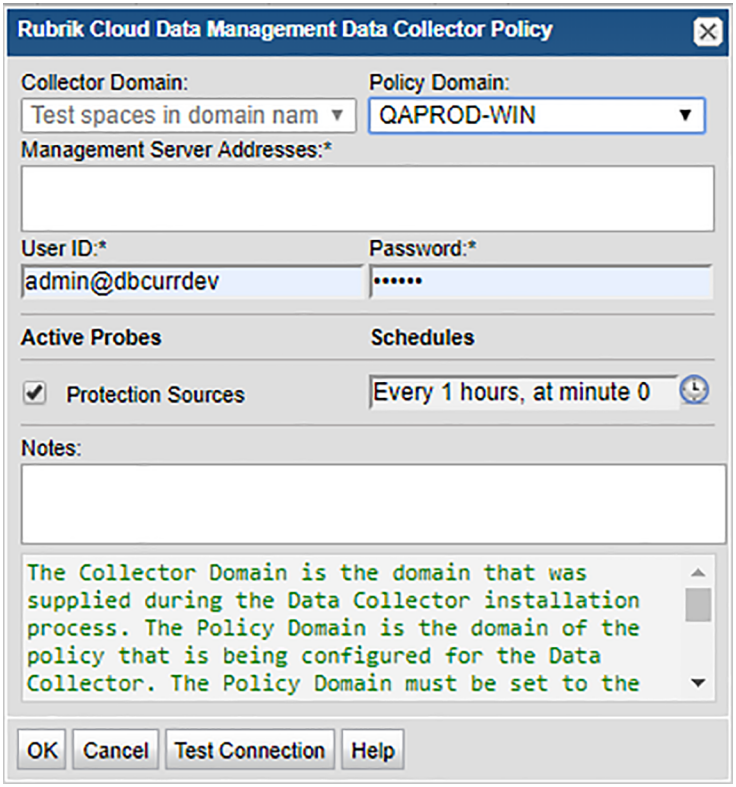
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Rubrik Cloud Data Management data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Add a Rubrik Cloud Data Management Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide* .
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5. Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

   See

Table 18-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more Cloud Data Management's server IP addresses or host names to probe. Comma-separated addresses are supported, e.g. 192.168.1.10, myhost NOTE: To collect from a Cluster, enter the IP address of only one of the management servers.
User ID*	Read-only userID for the Rubrik Cloud Data Management system.
Password*	Password for the Rubrik Cloud Data Management system. The password associated with the User ID.
Protection Sources	Probe for Rubrik Cloud Data Management Protection Details.
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 18-1 Policy Parameters *(continued)*

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 19

Configuration for Veeam Backup & Replication

This chapter includes the following topics:

- Introduction
- Prerequisites for adding data collectors (Veeam Backup & Replication)
- Verifying Data Collector servers can connect to Veeam servers
- Known issues and limitations (Veeam Backup & Replication)
- Installation overview (Veeam Backup & Replication)
- Add a Veeam Backup & Replication Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (Veeam Backup & Replication)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Requires a Microsoft Windows Data Collector server
- Requires Microsoft PowerShell 4.0 or above. Veeam Backup & Replication comes with a PowerShell extension - a snap-in to Microsoft Windows PowerShell. The Veeam Backup PowerShell snap-in enables most operations that are available in the user interface. For version 11.0, Veeam Backup & Replication comes with a PowerShell module which can be used on any machine with the backup console installed.
- Veeam Requirement: User credentials with a Veeam Backup Administrator role are required to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in or PowerShell module (version 11.0).
- Veeam Backup & Replication Console must be installed on the system where the Data Collector service is running.
- Default port is 9392.

Verifying Data Collector servers can connect to Veeam servers

Basic PowerShell commands for Veeam

- Add Veeam Snapin

```
Add-PSSnapin -PassThru VeeamPSSnapIn
```

Note: Skip this command for Veeam version 11.0, as it supports the PowerShell module.

- Connect to Veeam Backup Server

```
Connect-VBRServer -User <user> -Password <password> -Server
<server>
```

- Disconnect from Previous Connection

```
Disconnect-VBRServer
```

Verification steps

In this section, we'll use a scenario to illustrate the verification steps. The task is to connect to Veeam Servers Server-A and Server-B from the same Veeam Data Collector Server, where the Veeam Backup & Replication Console is installed.

1 From Microsoft PowerShell Console (in Administrator mode), add Veeam SnapIn.

```
Add-PSSnapin -PassThru VeeamPSSnapIn
```

Note: Skip this step for Veeam version 11.0, as it supports the PowerShell module.

---

2 Log into the Veeam Backup & Replication Console using Server-A credentials.

3 Open a PowerShell Console and connect to Server-A.

```
Connect-VBRServer -User ServerAUserId -Password ServerAPassword
-Server Server-A
```

The Server -A connection should be successful.

4 Open a PowerShell Console and disconnect from Server-A.

```
Disconnect-VBRServer
```

5 Open a PowerShell Console and connect to Server-B.

```
Connect-VBRServer -User ServerBUserId -Password ServerBPassword
-Server Server-B
```

If the Server-B connection is successful, it means: both Servers are on the same software version (including minor patch releases/ updates).

If the Server-B connection fails with the following error:

```
Connect-VBRServer: Cannot connect to backup server because some
of its components are out of date.
```

it means: Server-A and Server-B are on different software versions. The Veeam Backup & Replication Console is only in sync with Server-A.

Known issues and limitations (Veeam Backup & Replication)

- Backup File Names
  Veeam allows a backup job to have different backup and retention policies. For certain configuration types such as, Synthetic Full Backup or Forever Forward Incremental Backup Retention Policy, one of the *.vib files is renamed as *.vbk at regular intervals by Veeam. In NetBackup IT Analytics, the Veeam Data Collector retrieves backup information for a specified period of time at regular intervals. This set of backup information may contain file names with a *.vib extension (instead of *.vbk) and display in the Job Details report.
  For details about the various use cases, https://helpcenter.veeam.com/docs/backup/vsphere/backup_files.html?ver=95.
  As you compare NetBackup IT Analytics reports to native Veeam reports, if there are discrepancies in the files, you can force a historic data collection to examine the details. Additionally, when validating NetBackup IT Analytics reports against Veeam reports, focus on the file names and not the file extensions.
- Successful Endpoint Backup Jobs Displaying Size = 0.00 Bytes
  Occasionally, Veeam will create additional maintenance jobs such as Full backup file merge completed successfully and there is not a data size associated with the job. These jobs will be displayed with a status of Successful but without an associated data size.

- Veeam Collection does not support collection of jobs or backup data which are based on VMware Tags.

Installation overview (Veeam Backup & Replication)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Veeam Backup & Replication data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Add a Veeam Backup & Replication Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

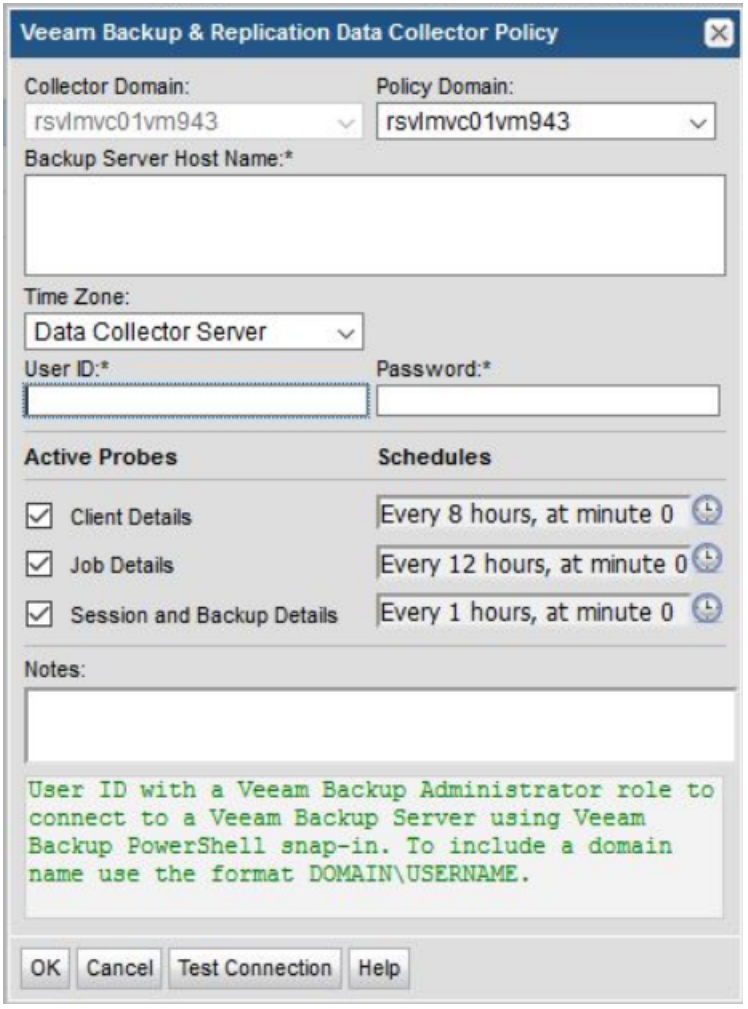
To add the policy

1 Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

Table 19-1

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Backup Server Host Name*	One or more Veeam Backup Server Host Names to probe. IP Address is not supported. Comma-separated host names are supported. Example, VeeamServer1, VeeamServer2.
Time Zone	Select the time zone of Veeam Backup Server. By default, the data collector server time zone is used.
User ID*	User ID with a Veeam Backup Administrator role to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in or PowerShell module (version 11.0). To include a domain name, use the format **DOMAIN\USERNAME**.
Password*	Password for Veeam Backup Server associated with the User ID.
Active Probes	
Client Details	Probe for collecting clients to be backed up using Veeam Backup & Replication.
Job Details	Probe for collecting jobs scheduled for Veeam Backup & Replication.
Session and Backup Details	Probe for collecting session details and backups created by Veeam Backup & Replication.

Table 19-1 *(continued)*

Field	Description
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin**>**Data Collection**>**Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. Refer to Working with On-Demand Data Collection for details.

Section 3

Storage (Capacity)

- Chapter 20. Configuration for Compute Resources
- Chapter 21. Configuration for DELL EMC Elastic Cloud Storage (ECS)
- Chapter 22. Configuration for Dell EMC Unity
- Chapter 23. Pre-installation setup for Dell PowerStore
- Chapter 24. Configuration for EMC data domain storage
- Chapter 25. Configuration for EMC Isilon
- Chapter 26. Configuration for EMC Symmetrix
- Chapter 27. Configuration for EMC VNX Celerra
- Chapter 28. Configuration for EMC VNX CLARiiON
- Chapter 29. Configuration for EMC VPLEX
- Chapter 30. Configuration for EMC XtremIO
- Chapter 31. Configuration for FUJITSU ETERNUS Data Collector
- Chapter 32. Configuration for Hitachi Block
- Chapter 33. Configuration for Hitachi Content Platform (HCP)
- Chapter 34. Configuration for Hitachi NAS

- Chapter 35. Configuration for Hitachi Vantara All-Flash and Hybrid Flash Storage
- Chapter 36. Configuration of Host inventory
- Chapter 37. Configuration for HP 3PAR
- Chapter 38. Configuration for HP EVA
- Chapter 39. Configuration for HPE Nimble Storage
- Chapter 40. Configuration for HPE StoreOnce
- Chapter 41. Configuration for IBM Enterprise
- Chapter 42. Configuration for IBM COS
- Chapter 43. Configuration for IBM SVC
- Chapter 44. Configuration for IBM XIV
- Chapter 45. Configuration for Microsoft Windows server
- Chapter 46. Configuration for NetApp-7
- Chapter 47. Configuration for NetApp StorageGRID
- Chapter 48. Configuration for NetApp Cluster
- Chapter 49. Configuration for NetApp E-Series
- Chapter 50. Configuration for NEC HYDRAstor
- Chapter 51. Configuration for Pure Storage FlashArray

Chapter 20

Configuration for Compute Resources

This chapter includes the following topics:

- Overview
- Prerequisites for adding Data Collectors - Compute Resources
- Installation overview
- Add a Compute Resources policy

Overview

A single instance of Data Collector can support any number of enterprise objects in most cases. However, each environment has its own unique deployment and configuration requirement. It is therefore important to correctly assess the environment to determine the ideal location and the optimal number of Data Collectors to be installed.

Prerequisites for adding Data Collectors - Compute Resources

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.
  Example:

  ```
  172.16.2.2 aptareportal.<yourdomain>.com

  172.16.2.3 aptareagent.<yourdomain>.com
  ```

- Gather the following required configuration details:
  - Host name for the server which would be sending the Compute Resources Data.
  - Ensure that each server added in policy can communicate with the Data Collector Server.

Installation overview

Use the following list to ensure that you complete each step in the order indicated:

- Update the Local Hosts file. This enables Portal access.
- In the Portal, add a Data Collector, if one has not already been created.
- In the Portal, add the Compute Resources policy. A single policy is allowed per collector.
- On the Data Collector Server, install the Data Collector software.
- For Windows Data Collector, install WMI Proxy Service
- Validate the Data Collector installation.

Add a Compute Resources policy

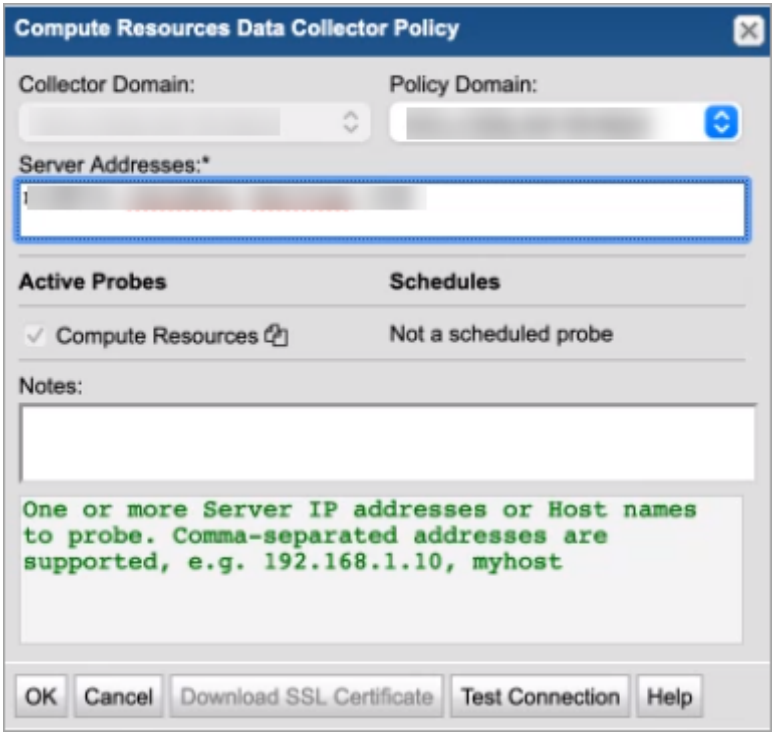
Before adding a policy:

- A Data Collector must exist in the Portal, to which you will add the Data Collector policies. For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- A single policy is allowed per collector.
- Users can manually add a policy using **Add Policy** menu on the Collector Administration screen.
- An existing Compute Resources policy's server address would get updated with the Internal Host Name of Primary Server from a Cohesity NetBackup Data Collector Policy, when the NetBackup Resources Monitor probe is enabled. For further details, refer to the help for Adding a Cohesity NetBackup Data Collector policy. A new policy for Compute Resources will get added if there is no existing policy.

To add a Compute Resources policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy** and then select the vendor-specific entry from the menu.



5 Enter or select the parameters based on the description below and click **OK** to save the policy.

The mandatory parameters are denoted by an asterisk (*).

Table 20-1 Compute Resources Data Collector Policy field description

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 20-1 Compute Resources Data Collector Policy field description *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Server Addresses	One or more host names specified as a comma separated list. This server address must match the host name of the server with NetBackup IT Analytics Exporter.
Compute Resources	This probe collects OS and hardware metrics from servers. No schedule is associated with this probe. It collects data received from NetBackup IT Analytics Exporter installed on the server configured in the policy. To install and configure NetBackup IT Analytics Exporter, see*NetBackup IT Analytics Exporter Installation and Configuration Guide*.
Schedules	Compute Resources probe is not a scheduled probe. It is always up and running and gathers data as it receives it from the NetBackup IT Analytics Exporter configured on the server.
Sender ID	Click on the icon next to the Compute Resources probe name to copy the Sender ID. This ID is required during the setup of NetBackup IT Analytics Exporter on the host. The value of a Sender ID is same for all the servers configured in a single policy. Refer *NetBackup IT Analytics Exporter Installation and Configuration Guide* for further details on its usage.

Table 20-1 Compute Resources Data Collector Policy field description *(continued)*

Field	Description
Download SSL Certificate	Downloads the SSL certificate required to setup NetBackup IT Analytics Exporter on the host. Refer *NetBackup IT Analytics Exporter Installation and Configuration Guide* for further details on its usage.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 21

Configuration for DELL EMC Elastic Cloud Storage (ECS)

This chapter includes the following topics:

- Pre-Installation setup for DELL EMC Elastic Cloud Storage (ECS)
- Prerequisites for adding Data Collectors - DELL EMC Elastic Cloud Storage (ECS)
- Installation overview - DELL EMC Elastic Cloud Storage (ECS)
- Add a DELL EMC Elastic Cloud Storage (ECS) Data Collector policy

Pre-Installation setup for DELL EMC Elastic Cloud Storage (ECS)

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors - DELL EMC Elastic Cloud Storage (ECS)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- User must belong to Management Users with System Monitor privileges.

Installation overview - DELL EMC Elastic Cloud Storage (ECS)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the DELL EMC Elastic Cloud Storage (ECS) data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Add a DELL EMC Elastic Cloud Storage (ECS) Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

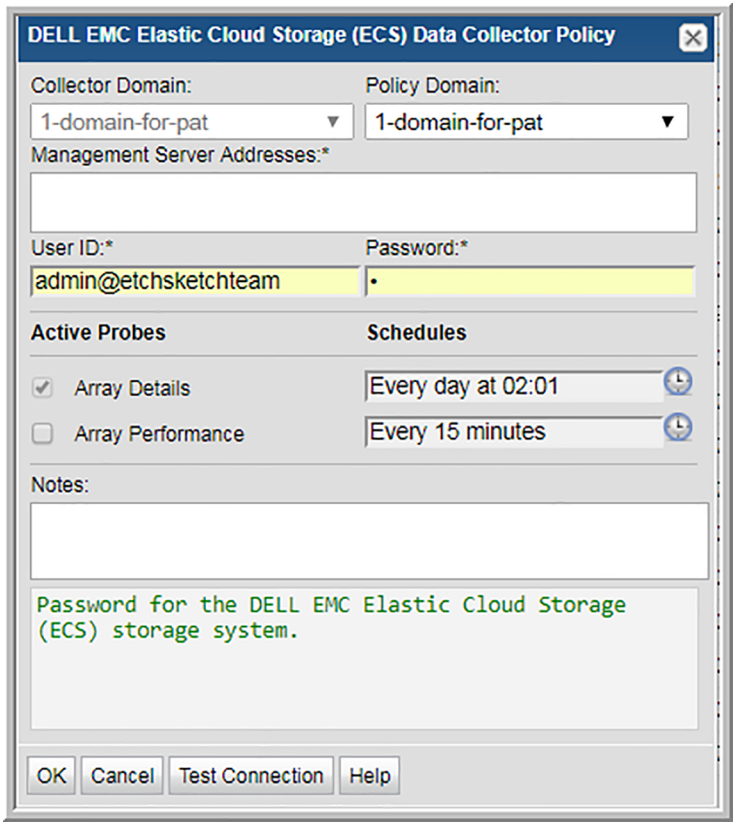
For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*

- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more DELL EMC Elastic Cloud Storage (ECS) Management server IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost To collect from a Cluster, enter the IP address of only one of the management servers.
User ID*	This field is required. View-only User ID and password for the DELL EMC Elastic Cloud Storage (ECS) storage system.
Password*	This field is required. Password for the DELL EMC Elastic Cloud Storage (ECS) storage system.
Active Probes	
Array Details	Click to activate the collection of array details.
Array Performance	Click to activate the probe for performance metrics for DELL EMC Elastic Cloud Storage (ECS) storage system.

Field	Description
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See “Working with on-demand Data Collection” on page 624.

Chapter 22

Configuration for Dell EMC Unity

This chapter includes the following topics:

- Pre-Installation setup for Dell EMC Unity
- Prerequisites for adding Data Collectors (Dell EMC Unity)
- Installation overview (Dell EMC Unity)
- Add a Dell EMC Unity Data Collector policy

Pre-Installation setup for Dell EMC Unity

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Dell EMC Unity)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Data collector must be installed on a system accessible to DELL EMC Unity storage array.
- Data collector supports DELL EMC Unity REST API version 4.3.0 for collecting capacity information from DELL EMC Unity storage array.
- User credentials with "security administrator" role is required to connect to Dell EMC Unity storage array using REST API.

Installation overview (Dell EMC Unity)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Dell EMC Unity data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Add a Dell EMC Unity Data Collector policy

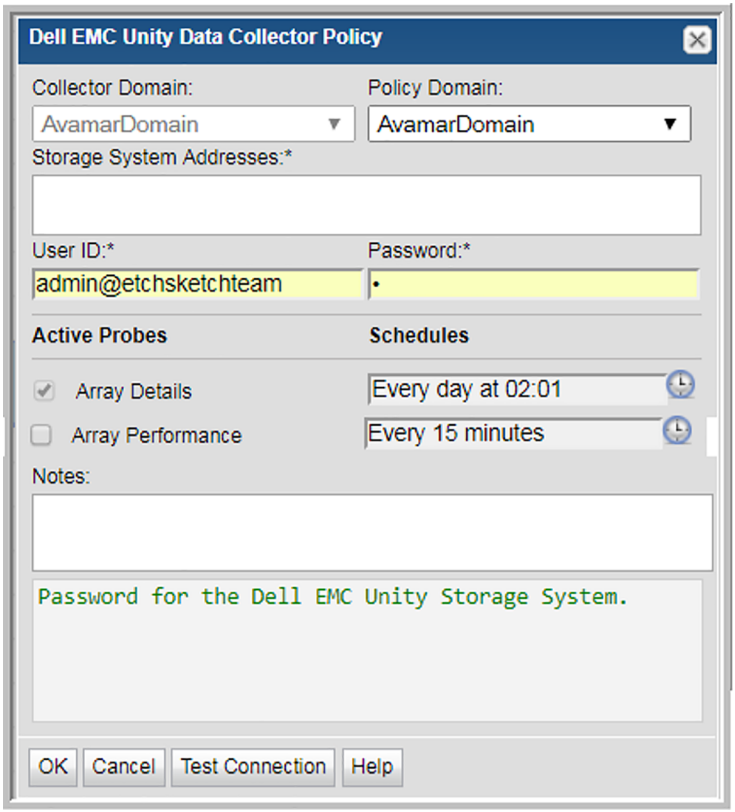
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Storage System Addresses*	One or more DELL EMC Unity storage system host name or IP address to probe. Comma separated values are supported.
User ID*	View-only User ID for the Dell EMC Unity storage system.
Password*	Password for the Dell EMC Unity storage system. The password associated with the User ID.
Array Details	Click the check box to activate array details collection.
Array Performance	Click to activate array performance data collection. By default, it is collected every 15 minutes. Do not schedule this probe for more than one hour, as by default, the maximum duration for which performance data is collected is an hour. The first time the probe is executed, 15 minutes of performance data will be collected.

Field	Description
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See “Working with on-demand Data Collection” on page 624.

Chapter 23

Pre-installation setup for Dell PowerStore

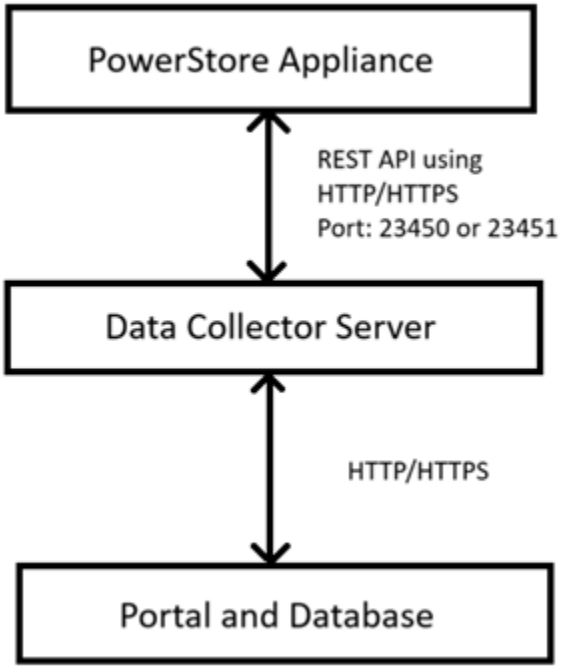
This chapter includes the following topics:

- Overview
- Prerequisits for adding Dell PowerStore data collector
- Add a Dell PowerStore policy

Overview

Dell PowerStore connector uses REST API with read-only access to PowerStore appliance to collect capacity, volumes, physical disk, cluster, and policy details.

This information helps to monitor and report capacity related information about the PowerStore appliances in PowerStore system.



Prerequisits for adding Dell PowerStore data collector

- A 64-bit OS. See NetBackup IT Analytics Certified Configurations Guide for the supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory

- Install only one Data Collector on a server (or OS instance).
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.

Example:

172.16.2.2 aptareportal.<yourdomain>.com

172.16.2.3 aptareportal.<yourdomain>.com

Add a Dell PowerStore policy

Before adding the policy

A data collector must exist on the portal to which you will add data collector policies.

For specific prerequisites and supported configurations, see Certified configuration guide.

After adding the policy

On-demand collections allows you to select which probes and devices to run collection. The action collects data the same way as scheduled job run.

Note: Refer Certified Configuration guide for supported vendors. The Run button is only displayed if the policy vendor is supported.

To add a policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search and select the required data collector.
3. Click **Add Policy** and then select **Dell PowerStore** policy.
4. Click **Ok** to save the policy.

Table 23-1 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 23-1 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*): *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings. Example: yourdomain
Management Server Address*	Hostname or IP Address for the PowerStore REST API Server.
User ID*	Specify the Username with Storage Administrator (View Only) role. Refer section Pre-installation setup for more details.
Password*	The password associated with the User ID.
Data Protection	This probe focuses on APIs related to the management of data protection features like snapshots, replications, and policies which are critical for disaster recovery and data safety. By default, it is collected at 01:01 daily.
Data Utilization	This probe would focus on APIs that help in monitoring and managing storage resource utilization, providing insights into how storage is being used and helping optimize performance. By default, it is collected at 01:01 daily.
Performance	Enables API driven collection of performance metrics at various levels such as volumes and ports. The collection is triggered based on the configured schedule.

Table 23-1 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*): *(continued)*

Field	Description
Schedules	Click the clock icon to create a schedule. By default, it is collected at 1:01 daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 24

Configuration for EMC data domain storage

This chapter includes the following topics:

- Architecture overview (EMC data domain storage)
- Prerequisites for adding data Collectors (EMC data domain storage)
- Installation overview (EMC data domain storage)
- Add EMC data domain servers
- Adding an EMC data domain storage Data Collector policy

Architecture overview (EMC data domain storage)

The following diagram provides an example of how the EMC Data Domain Data Collector could be deployed in your environment.

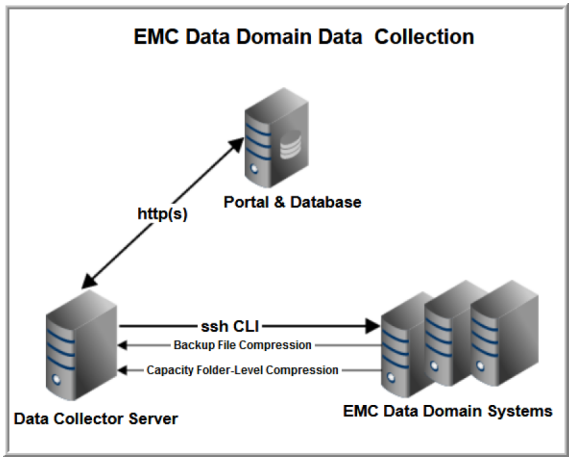


Figure 2 Data Collector in an EMC Data Domain Environment

The NetBackup IT Analytics Data Collector connects to the Data Domain system via SSH to issue data-gathering commands from the command-line interface (CLI).

Data Domain systems straddle the backup and storage capacity worlds. When addressing data protection challenges, Data Domain provides backup, archive, and disaster recovery solutions. In support of these solutions, Data Domain appliances supply deduplication and storage management systems. These systems provide storage in the following ways:

- Native storage device for backup systems
- Virtual tape library (VTL) for backup systems
- NFS mount or CIFS share folders for file storage

data domain collected storage data

Data Domain storage collection can be configured to collect CIFS shares, NFS mounts, and folder-level compression rates, enabling a consolidated view of storage utilization. For folder-level compression collection, a probe collects file-level compression ratios for both folders and files stored on Data Domain CIFS or NFS mounts. Folder-level data compression rates enable chargeback on used disk space associated with shares and mounts, and folders within those shares and mounts. In the data collection policy, define the share folder depth to be interrogated. For example, a single share may have individual folders for business units. Data about these folders and files is collected and collated, based on the folder depth specified.

Prerequisites for adding data Collectors (EMC data domain storage)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Port used by the Data Domain Data Collector: **Port 22 for SSH.**
- Ensure that you have data domain version 5.7 and above supported for collecting Physical Capacity Measurement (PCM) per mtree for Data Domain.
  On the Data Domain Operating System, execute the following two commands with admin privileges:

  Note: By default PCM is disabled.

  - Command to enable PCM: `compression physical-capacity-measurement enable and-initialize`
  - Command to scheduled PCM job per day for mtree: `compression physical-capacity-measurement schedule create jf_sched2 mtrees /data/col1/backup time 1400`

Installation overview (EMC data domain storage)

1. In the Portal, add a Data Collector, if one has not already been created.

2. In the Portal, add the EMC Data Domain data collector policy.
3. On the Data Collector Server, install the Data Collector software.
4. Validate the Data Collector Installation.

Note: These steps apply only if you are performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal, that is, a HOSTED installation (perhaps for a product evaluation) skip this section and contact your hosting organization's representative to configure the hosted portal for your Data Collector.

Add EMC data domain servers

For each EMC Data Domain server specified in the NetBackup IT Analytics Data Collector Pre-Installation worksheet, add the Data Domain server(s) to NetBackup IT Analytics by following the steps outlined in this section.

Note: When adding an EMC Data Domain Server, in the Inventory select **Hosts**, not Backup Servers.

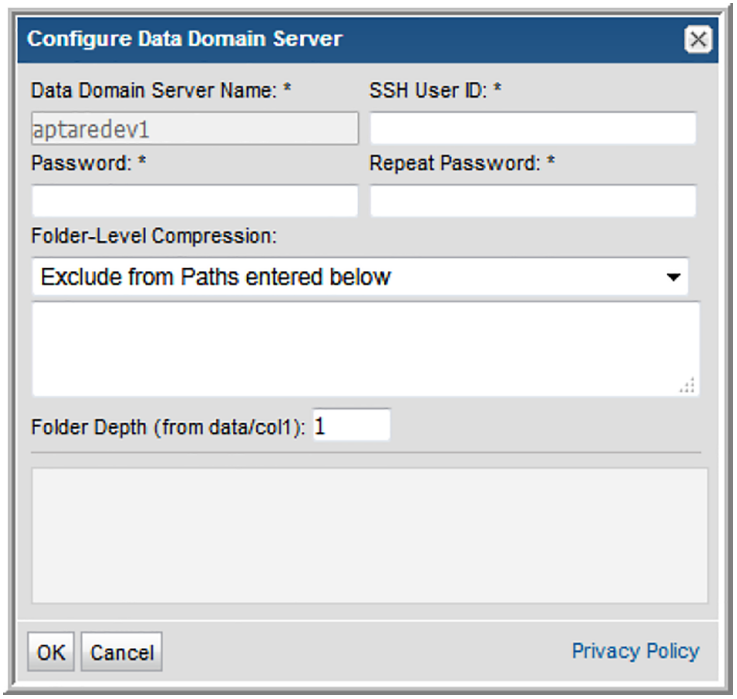
---

1. In the Portal, add a host for each Data Domain server.
   - External Host Name - Displayed in the Portal.
   - Internal Host Name - Must match the host name of the Data Domain server; fully qualified domain name (FQDN).
   - Backup Type - Data Domain Server
2. If collecting Folder-Level Compression data, refer to the following section.

Configure a data domain server for folder-level compression collection

In addition to the values that were entered when an EMC Data Domain server was created, credentials are required to access and collect from the server. Also, if Folder-Level Compression collection is desired, folder paths can be specified.

Folder-level data compression rates enable reporting on used disk space associated with shares and mounts, and folders within those shares and mounts. In the data collection policy, define the share folder depth to be interrogated. For example, a single share may have individual folders for business units. Data about these folders and files is collected and collated, based on the folder depth specified.



1. Enter the following details and click **OK**.

Field	Description	Sample Value
Data Domain Server Name*	In order for Data Domain Servers to be listed in the policy window, they must have been created via the Inventory and configured with a **Backup Type** of **Data Domain Server**. See "Add EMC data domain servers" on page 246.	`DDM-HQ`
SSH User ID*	The command-line interface (CLI) via SSH is used to gather Data Domain system data. This requires a view-only Data Domain User ID that must be a member of the Data Domain system Admin group. This User ID must be the same for all addresses listed in the System Addresses entry field for the Data Domain systems.	`Administrator`
Password	The password associated with the User ID.	`Pwd1`
Repeat Password	The password associated with the User ID.	`Pwd1`

Field	Description	Sample Value
Folder-Level Compression	Select the option to either include or exclude collection and then enter folders to the list. If the exclude option is selected with an empty folder list, compression data from all folders will be collected. If the include option is selected with an empty folder list, no folder-level compression data will be collected. The folders should start with /data/col1 **Warning:** Choosing to exclude compression collection with an empty folder list may cause collection to take several hours to complete.	`/data/col1/dd890-nbuprod`
Folder Depth (from data/col1)	Specify the folder depth to be interrogated. For example, a single share may have individual folders for business units. Data about these folders and files is collected and collated, based on the folder depth specified. The folder depth starts from the folder path name that is specified in the include list or from /data/col1, if no include folders are specified. An empty value means that data collection will collect all the sub-folders within each folder specified in the include list.	`1`

Adding an EMC data domain storage Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

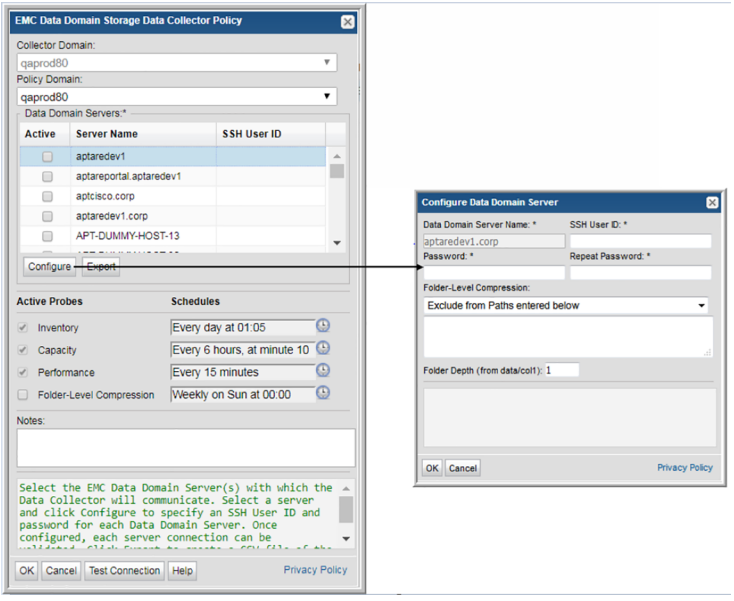
To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

Note: Only one Data Domain Storage policy can be added to a Data Collector for the same Policy Domain. Activate multiple Data Domain servers within a single policy.

Data Domain Storage collection can be configured to collect CIFS shares, NFS mounts, and folder-level compression rates, enabling a consolidated view of storage utilization. A Capacity Manager probe collects file-level compression ratios for both folders and files stored on Data Domain CIFS or NFS mounts. Folder-level data compression rates enable chargeback on used disk space associated with shares and mounts, and folders within those shares and mounts. In the data collection policy, define the share folder depth to be interrogated. For example, a single share may have individual folders for business units. Data about these folders and files is collected and collated, based on the folder depth specified. This feature augments the existing Data Domain Backup data collection, which includes an option to collect file-level compression ratios associated with NetBackup backup images.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name select **Admin > Domains > Domains**.	`yourdomain`
Data Domain Servers*	When you check **Active** for a server shown in the list, a dialog window prompts for the SSH credentials. Alternatively, select a server and click **Configure**. In order for Data Domain Servers to be listed in the policy window, they must have been created via the Inventory and configured with a **Backup Type** of **Data Domain Server**. See "Add EMC data domain servers" on page 246.	
SSH User ID*	The command-line interface (CLI) via SSH is used to gather Data Domain system data. This requires a view-only Data Domain User ID that must be a member of the Data Domain system Admin group. This User ID must be the same for all addresses listed in the System Addresses entry field for the Data Domain systems.	`Administrator`
Password	The password associated with the User ID.	`Pwd1`
Configure	Select a Data Domain server and click **Configure** to enter the SSH credentials that will be used to access the server.	
Export	Click **Export** to retrieve a list of all the Data Domain servers in a comma-separated values file.	

Field	Description	Sample Value
Inventory Probe	Inventory details such as system, enclosure, disk, MTree, Licensing, DD Boost, snapshot and file system compression are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Capacity Probe	Data associated with system capacities, such as file system capacity, LSU compression and replication information, is collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Performance Probe	Data associated with the performance of the Data Domain system, such as CPU and disk burst indicators and disk performance indicators, is collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Folder-Level Compression Probe	To enable folder-level compression collection, check the box and double-click a Data Domain server above to specify the folder paths to exclude or include in collection. This probe collects folder-level compression ratios for both folders and files stored on CIFS shares or NFS mounts. When this probe is selected, DataDomain configured CIFS or NFS pathnames can be entered into the Folder-Level Compression list configured for a Data Domain Server. The Data Domain Servers will then display an Include/Exclude column, with negative numbers indicating pathnames that are excluded and positive numbers indicating pathnames that are included. Hover your mouse over the Incl/Excl column to view the pathnames. If the column displays +0, it indicates no pathnames have been included in the collection, and -0 indicates no pathnames have been excluded, so all configured CIFS or NFS pathnames will be collected from. **Note:** In order to collect folder level compression information, the CIFS shares or NFS mounts data needs to collected using the Inventory Probe. **Warning:** Choosing to exclude compression collection with an empty folder list may cause collection to take several hours to complete.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Field	Description	Sample Value
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin > Data Collection > Collectors**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

6. Click **OK** to save the policy.
7. On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.

Chapter 25

Configuration for EMC Isilon

This chapter includes the following topics:

- Pre-Installation setup for EMC Isilon
- Prerequisites for adding Data Collectors (EMC Isilon)
- Configure the Isilon SNMP service
- Configure Isilon sudo access
- Installation overview (EMC Isilon)
- Adding an EMC Isilon Data Collector policy

Pre-Installation setup for EMC Isilon

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC Isilon)

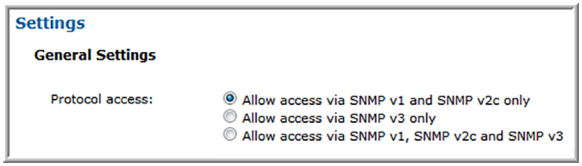
- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Configure the Isilon SNMP service

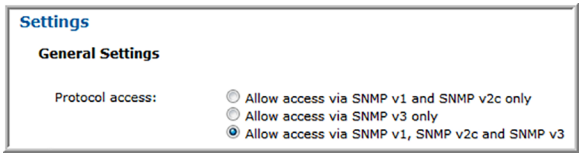
The Isilon Data Collector requires the Isilon SNMP service to be running. SNMP data is collected using the **sudo snmpbulkwalk** command in an SSH session. This does not require any additional ports to be opened for SNMP.

1. In the Isilon administrative web interface, **Access Management/Users**, select **Cluster Management > SNMP Monitoring** to enable/configure SNMP. Note that the SNMP configuration is specific to an SNMP version.
2. Configure SNMP using the following tables to determine the protocol access required for your environment. Be sure to click **Submit** on the **SNMP Monitoring** page to save your configuration.

SNMP v1 and v2c only	■ Enable access:  ■ If SNMP v2c is allowed, then the **read-only community** string must be set. 

SNMP v1, v2c, and v3

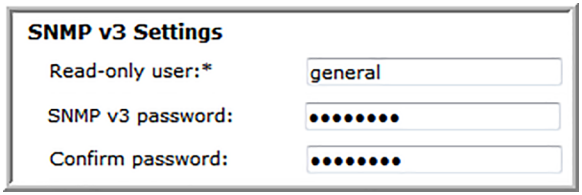
- Enable access:



- When SNMP v2c is allowed, the **read-only community** string must be set.



- When SNMP v3 is allowed, the **read-only user**and **SNMP v3 password** must both be set. The SNMP password for Isilon must be at least 8 characters long.

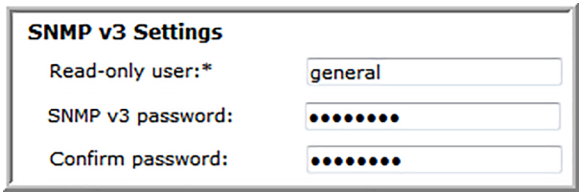


SNMP v3 is allowed, but SNMP v2c is not allowed

- Enable access.



- When SNMP v3 is allowed, the **read-only user** and **SNMP v3 password** must both be set. The the SNMP password for Isilon must be at least 8 characters long.



- The following additional configuration is required at the command line, on each cluster node that is configured in the Data Collector policy.

1. Log in to the node as **root** and change to the root user home directory.

```
# cd /root
```

2. Create the **.snmp** directory and make it accessible only to the **root** user.

```
# mkdir .snmp
# chmod 700 .snmp
# ls -ld .snmp
drwx------ 2 root 512 Sep 18 15:00 .snmp
```

3. Modify or create.**snmp/snmp.conf**, using **nano** or another editor, to add the following line, replacing **<snmp v3 password>** with the password entered in the SNMP v3 Settings.

```
defAuthPassphrase <snmp v3 password>
```

4. Save .**snmp/snmp.conf** and make it accessible only to the **root** user.

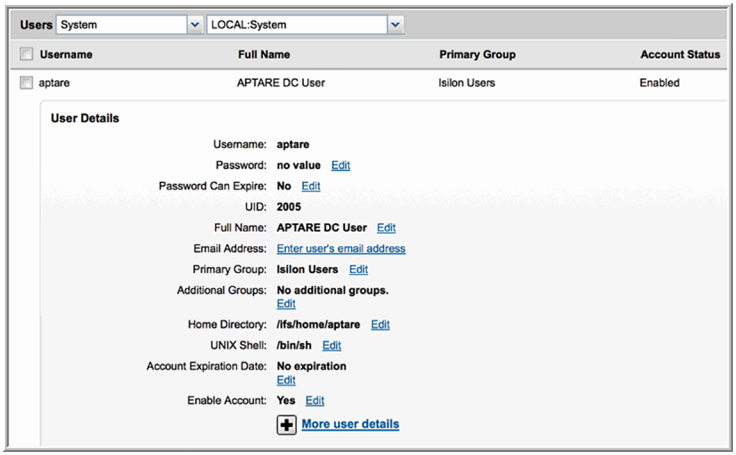
```
# chmod 600 .snmp/snmp.conf
# ls -l .snmp/
total 1
-rw------- 1 root 129 Sep 18 15:02 snmp.conf
```

Configure Isilon sudo access

If your security requirements require sudo access to provide temporary, elevated privileges, use the instructions in this section unless you are using an account with root privileges for the collection.

The commands in this section are for Isilon OneFS v7.0 and later. Verify command path names for the respective versions.

1. Using the Isilon administrative web interface, **Access Management/Users**, create a local user on the Isilon cluster, similar to the details shown in the following example.



2. Log in to any node of the cluster.
3. At the command line, grant this new user **AuditAdmin** privileges to enable SSH access to the cluster.

```
# isi auth roles modify AuditAdmin --add-user aptare
```

Modify the Sudo configuration

Depending on your version of EMC Isilon, you may either run the `isi_visudo` command, or create a drop-in `sudoers` file in the correct directory to restrict the commands that a user can execute.

1. Configure `visudo` to modify the `sudoers` file. The **visudo** will use the editor specified in the $EDITOR variable, or vi, by default.

   Specify your preferred editor. For example, to use nano as your editor, execute the following:

```
# export EDITOR=nano
```

2. Once your editor is configured, execute one of the following commands to edit the `sudoers` file.

   For OneFS versions lower than 9.1:

   ```
   # isi_visudo
   # visudo -f /usr/local/etc/sudoers.d/aptare
   ```

   ```
   # isi_visudo
   # isi_visudo -f /etc/mcp/override/sudoers
   ```

3. Add the following lines to the sudoers file, substituting the name of the user you created for **<username>**.

   ```
   <username> ALL=(ALL) NOPASSWD: /usr/local/bin/snmpbulkwalk, \
                  /usr/bin/isi, /usr/bin/isi_for_array,
   /usr/bin/isi_hw_status
   ```

4. Save the `sudoers` file.
5. If you have upgraded OneFS to version 9.1 or later, run these commands to using your user credentials to resume the data collection:

   ```
   # sudo isis version
   # isi version
   # sudo -A isi version
   ```

Installation overview (EMC Isilon)

Use the following list to ensure that you complete each step in the order indicated. Each item in this list corresponds to a section in this guide that contains the step-by-step instructions.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC Isilon data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an EMC Isilon Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

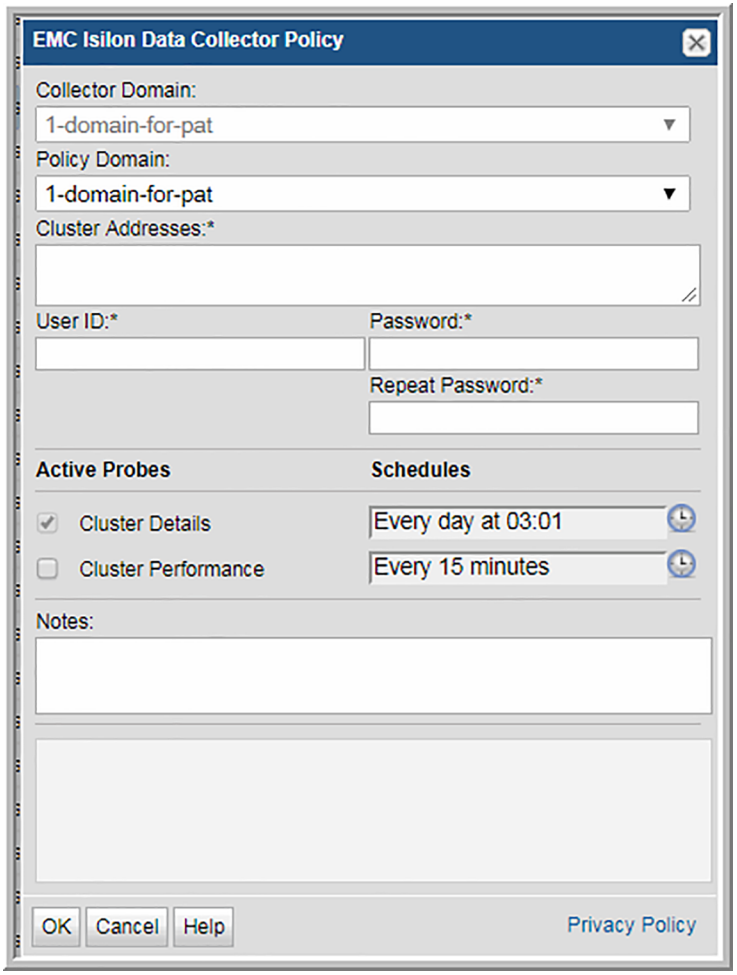
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

:

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
Domain	The domain identifies the top level of your host group hierarchy. The name was supplied during the installation process. All newly discovered hosts are added to the root host group associated with this domain. Typically, only one Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Cluster Addresses*	Enter one or more EMC Isilon cluster address(es) separated by commas. For each cluster enter the address of a single externally accessible node. Do not enter multiple nodes per cluster.	
User ID and Password*	SSH User ID and password for accessing the EMC Isilon cluster.	

Field	Description	Sample Value
Cluster Details Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	Every day at 03:01
Cluster Performance Schedule	Check the check box to activate cluster performance collection to populate performance metrics for EMC Isilon clusters. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	Every 15 minutes
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

6. Click **OK** to save the policy.
7. On the Data Collector server, install/update the Data Collector software.

Chapter 26

Configuration for EMC Symmetrix

This chapter includes the following topics:

- Pre-Installation setup EMC Symmetrix
- Prerequisites for adding Data Collectors (EMC Symmetrix)
- Installation overview (EMC Symmetrix)
- Adding an EMC Symmetrix Data Collector policy

Pre-Installation setup EMC Symmetrix

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC Symmetrix)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- The Data Collector must be installed on the server that manages the Symmetrix array.
- **Recommended**: EMC Solutions Enabler should be running on a server that is not the Data Collector server; the SYMAPI server daemon (storsrvd) must be running on this server. See the Data Collector installation guide for steps to verify this configuration.
- Set the EMC Solutions Enabler user account to **StorageAdmin** instead of Monitor.
- SymCLI must be installed on the Data Collector server.
- For additional specific prerequisite details and supported configurations, see the *Certified Configurations Guide*.
- A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

Installation overview (EMC Symmetrix)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC Symmetrix data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an EMC Symmetrix Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

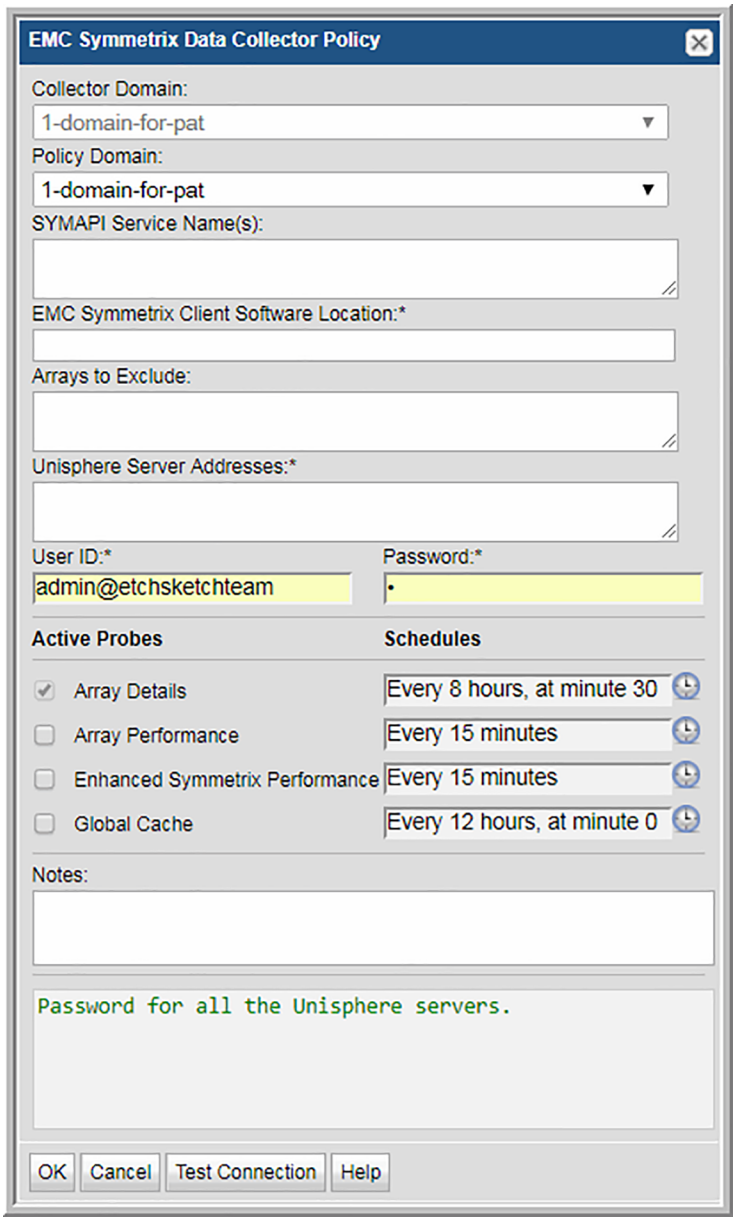
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

Note: Only one EMC Symmetrix policy is permitted per Data Collector.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
SYMAPI Service Names	Enter a comma-separated list of SYMAPI service names, such as SYMAPI_SECURE. These names are defined in $EMC_HOME\SYMAPI\config\netcnfg of the Data Collector server. Typically, $EMC_HOME on Windows is C:\Program File\EMC and on Linux it is /usr/ This option is only used with remote host configuration, not when the Data Collector is the primary Solutions Enabler host. See also: See "If the EMC solutions enabler is on a remote server (Recommended)" on page 270.	SYMAPI_SECURE
EMC Symmetrix Client Software Location *	This location refers to the location on the Data Collector. Linux: `/usr/symcli/bin` Windows: `C:\Program Files\EMC\symCLI\bin` On Windows, the short name for the directory path may be required when spaces are included in a path: `C:\PROGRA~2\EMC\symCLI\bin`. The short name can be determined with the "`dir /x`"command in the parent directory.	
Arrays to Exclude	Enter one or more Symmetrix SymIDS to be excluded. Comma-separated SymIDs are supported. Example: 000190102500, 000190102501	

Field	Description	Sample Value
Unisphere Server Addresses*	Comma-separated list of Unisphere server IP addresses (or host names) to probe. If the port number is different from the default 8443, specify it after a colon character (for example: 127.0.0.1:8444).	
User ID/Password*	User ID and password required for Unisphere servers/hosts.	
Active Probes and Schedules		
Array Details	Click the check box to activate array details collection. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Array Performance	Click check box to activate array performance collection. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Enhanced Symmetrix Performance	Click the check box to collect performance data for EMC Symmetrix storage systems using Unisphere for VMAX. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.	

Field	Description	Sample Value
Global Cache	Click the check box to collect Global Cache data for EMC Symmetrix storage systems. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

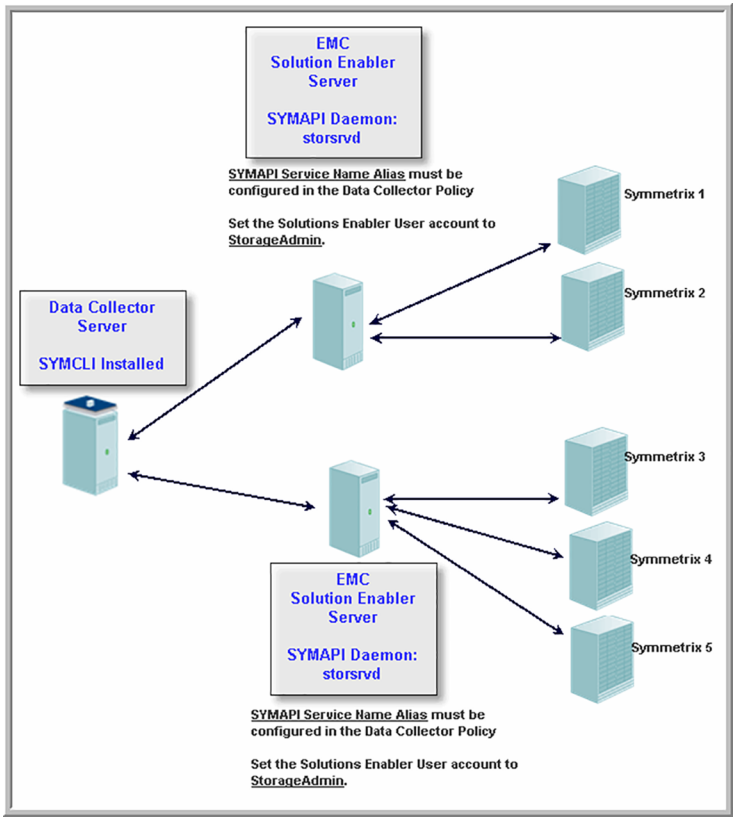
6. Click **OK** to save the policy.
7. On the Data Collector server, install/update the Data Collector software.

If the EMC solutions enabler is on a remote server (Recommended)

If the EMC Solutions Enabler is running on a server that is not the Data Collector Server, then you must:

- Verify that the Solutions Enabler on the remote host is the same version that is installed on the Data Collector. In EMC Solutions Enabler, select the SMCLI_COMPONENT and BASE_COMPONENT software.
- Verify that the SYMAPI server daemon is running on the Solutions Enabler server. The following diagram illustrates this configuration.
- For the Solutions Enabler User account, set it to **StorageAdmin** instead of Monitor.

- In the Data Collector policy, configure the SYMAPI Service Name Alias.
- The SYMCLI_CONNECT variable on the SYMCLI server must be set to match NETCNFG alias.



To check if the SYMAPI storsrvd daemon is running on each of the EMC Solutions Enabler Servers:

1. Log on to the server as root (Linux) or as a user with Administrative privileges (Windows).
2. At the command prompt, type: **stordaemon list**

   A list of available and running daemons will be listed in the command's output. Running daemons are prefaced with an asterisk in square brackets: [*]

   Example:

```
[*]   storapid EMC Solutions Enabler Base Daemon
    storgnsd EMC Solutions Enabler GNS Daemon
```

```
   storevntd EMC Solutions Enabler Event Daemon
[*]   storwatchd EMC Solutions Enabler Watchdog Daemon
   storsrvd EMC Solutions Enabler SYMAPI Server Daemon
```

3. If the storesrvd daemon is not running, type: **stordaemon start storsrvd**

Chapter 27

Configuration for EMC VNX Celerra

This chapter includes the following topics:

- Pre-Installation setup for EMC VNX Celerra
- Prerequisites for adding Data Collectors (EMC VNX Celerra)
- Setup for EMC VNX Celerra arrays
- Configure a Read-Only user with an Operator role
- Start the XML API server
- Installation overview (EMC VNX Celerra)
- Adding an EMC VNX Celerra Data Collector policy

Pre-Installation setup for EMC VNX Celerra

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC VNX Celerra)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Enable statistics logging on the VNX system to collect LUN performance information.
- See "Setup for EMC VNX Celerra arrays" on page 274.
- See "Configure a Read-Only user with an Operator role" on page 275.
- See "Start the XML API server" on page 276.

Setup for EMC VNX Celerra arrays

1. Note the port used by the EMC Celerra Data Collector: **XML API 443/2163/6389/6390/6391/6392**.
2. On the VNX server, in EMC Unisphere, configure a Read-Only User with an Operator Role.
3. On the VNX server, start the XML API Server (**/nas/sys/nas_mcd.cfg)**.
4. Gather the following required configuration details:
   - Array Addresses: List of VNX (Celerra) storage array addresses, only one Control Stations address per array.
   - Celerra Array User ID & Password: Credentials for a view-only user with an Operator role.
5. If using Active Directory for verbose user names, for quota reporting purposes, the following are required:
   - Fully qualified Domain Name for the root of the LDAP directory tree.

- IP address or host name of the primary directory host that is used for authentication.
- Active Directory restricted user login name(with directory search/read privileges) that binds to the directory server.
- If using SSL, the explicit path and file name for the SSL primary certificate file is required.

6. Enable statistics logging on the VNX system to collect LUN performance information.

Configure a Read-Only user with an Operator role

A read-only user with an operator role is required to access the EMC VNX server for data collection.

1. On the VNX server, launch EMC Unisphere and login as root.
2. Select the **Celerra server** from the drop-down list at the top of the EMC Unisphere toolbar.
3. Click the **Settings** icon in the EMC Unisphere toolbar and then click **Security**.
4. Select **Local Users**.
5. From the **Groups** tab, click **Create** to create a new group.
6. In the new group window:
   - Enter a **Group Name.**
   - For **Role**, select **Operator**.
   - Keep the other default values.
   - Click **OK**.
     Once you click OK, the group will appear in the Groups list as a Local User, a Group Type of Local, and a Role of Operator.
7. Click the **Users** tab at the top of the EMC Unisphere window.
8. Click **Create**, configure the values for the following fields, and click **OK**:
   - User Name
   - Password
   - Primary Group (select the group you just created)
   - Group (Role) Membership (check the group with the Operator role that you just created)
   - CLI access allowed (check the box to enable access)

Once you click OK, the new user will appear in the list as a State of Enabled, Account Type of Local, and a Role of Operator.

Start the XML API server

Before collecting data from the EMC VNX (Celerra) server, the XML API server must be enabled (By default, the XML API server is disabled.). The XML API provides a communication protocol that supports authentication and XML requests.

To start the XML API server, take the following steps on the VNX server.

1. Login as root.
2. In the **/nas/sys/nas_mcd.cfg** file, **uncomment** the following lines:

```
daemon "XML API Server"
    executable "/nas/sbin/start_xml_api_server"
    optional yes
    canexit yes
    autorestart yes
    ioaccess no
```

3. Restart the NAS services:

```
service nas start
```

   At this point, the XML API is started and is controlled by the primary control daemon.

Installation overview (EMC VNX Celerra)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC VNX Celerra data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an EMC VNX Celerra Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

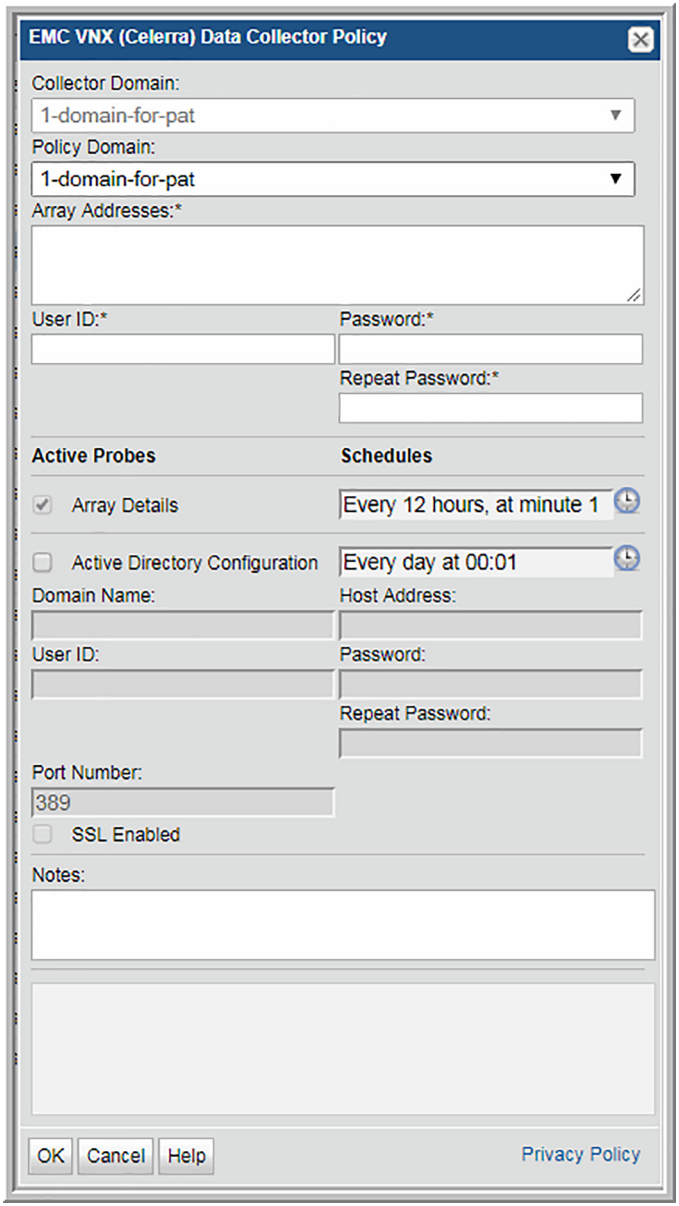
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu **EMC VNX (Celerra).**



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
Array Addresses*	Enter one or more VNX (Celerra) storage array address(es) separated by commas. List only one Control Station IP address per array. Make sure that XML API server is running. Click Help to view the steps to start the XML API server on VNX (Celerra) arrays. See Adding an EMC VNX (Celerra) Data Collector and Start the XML API Server.	
User ID*	Enter a User ID for the VNX array. This ID must have an Operator role, which enables read-only privileges.	
Password*	Password associated with the User ID	
Repeat Password*	Password associated with the User ID	

Field	Description	Sample Value
Array Details	Check the box to activate the collection of array details. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Active Directory Configuration	Check this box if you want the Data Collector to gather the verbose User Name from Active Directory and associate it with the appropriate VNX User ID for quota reporting purposes. **Note:** Once a single EMC VNX (Celerra) Data Collector policy has been configured to use Active Directory, there is no need to configure Active Directory in other VNX (Celerra) Data Collector policies, if they are all using the same directory server. Click the clock icon to create a schedule.	
Domain Name	Enter a fully qualified Domain Name for the root of the LDAP directory tree. Use a period-separated format (example: ldap.emc.com). This example will be translated by the system to X.509 format: dc=ldap, dc=emc, dc=com. Only a single LDAP domain is supported. This is a mandatory field, if you have checked Active Directory Configuration.	
Host Address	Enter the IP address or host name of the primary directory host that is used for authentication. This value is based on the format of the subject in the host's certificate. This is a mandatory field if you have checked Active Directory Configuration.	
User ID	Enter the Active Directory login name of the user account that binds to the directory server. This should be a restricted user account, such as a Domain Guest account, with directory read and search privileges. This is a mandatory field if you have checked Active Directory Configuration.	
Password/Repeat Password	Enter the Password for the Active Directory account. This credential is used to authenticate the account. This is a mandatory field if you have checked Active Directory Configuration.	
Port Number	Enter the network port used by Active Directory. This is a mandatory field if you have checked Active Directory Configuration.	

Field	Description	Sample Value
SSL Enabled	Check this box if your LDAP protocol uses SSL for encryption and authentication.	
SSL Primary Certificate File	Enter the explicit path and file name for the SSL primary certificate file. Example: C:\SSL\primaryCert.cer. This certificate is used for authentication when connecting to Active Directory.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

6 Click **OK** to save the policy.

7 On the Data Collector server, install/update the Data Collector software.

Chapter 28

Configuration for EMC VNX CLARiiON

This chapter includes the following topics:

- Pre-Installation setup for EMC VNX
- Prerequisites for adding Data Collectors (EMC VNX)
- Installation overview (EMC VNX)
- Adding an EMC VNX Data Collector policy

Pre-Installation setup for EMC VNX

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC VNX)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Note the port used by the EMC VNX Data Collector: NaviCLI 443/2163/6389/6390/6391/6392.
- NaviSecCLI must be installed on the Data Collector server.
- A low security level for certificates is required. Ensure this setting by using the following command:

```
naviseccli security -certificate -setLevel low
```

- Gather the following required configuration details:
  - Array Addresses: List of IP addresses to be probed, only one storage processor address per array.
  - EMC Navi Client Software Location: Path of the software installation.
  - NaviSuite User ID & Password: Credentials for a view-only user ID.
- Enable performance data logging on the VNX system to collect LUN performance information.

Installation overview (EMC VNX)

Use the following list to ensure that you complete each step in the order indicated. Each item in this list corresponds to a section in this guide that contains the step-by-step instructions.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC VNX data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on oneof the Windows hosts.

6. Validate the Data Collector installation.

Adding an EMC VNX Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

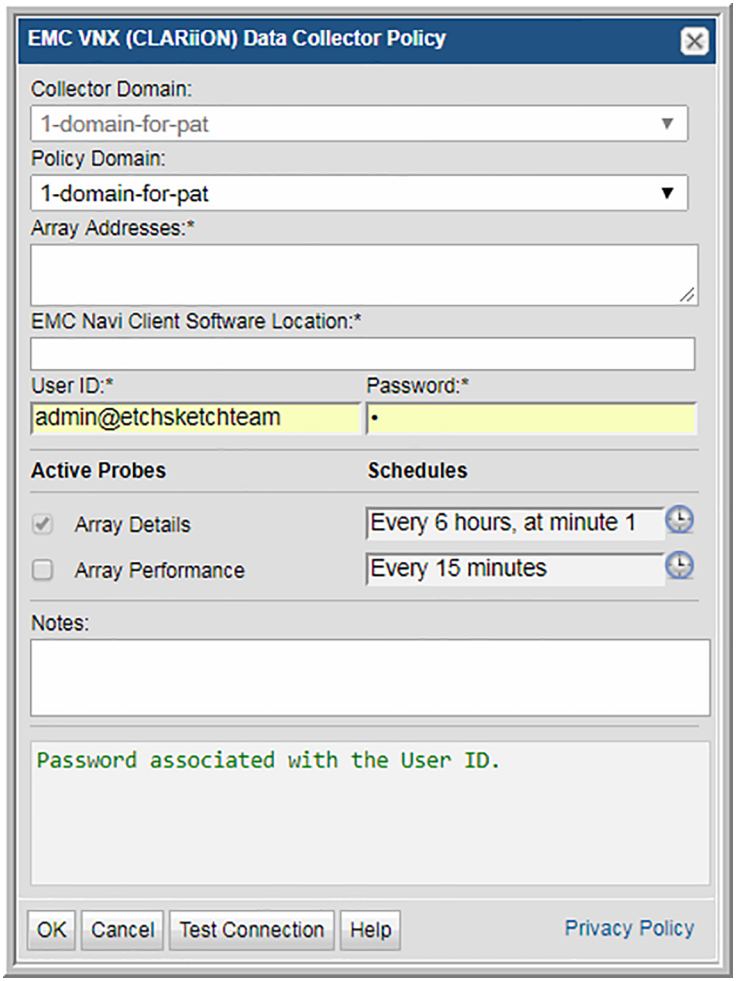
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Array Addresses*	Enter one or more storage array addresses separated by commas. List only one SP (storage processor) IP address per array. Typically, only the IP addresses are required, with port 443 used as the default. To change the port that the Data Collector uses to communicate with the array, use the format: `<IP address>:<port number>`	`172.16.1.1:445`
EMC Navi Client Software Location *	For example: Linux: `/opt/Navisphere/bin` Windows: `C:\Program Files\EMC\NavisphereCLI\`	
User ID*	Create a Global user with operator privileges for NaviSuite (VNX Block).	`Administrator`
Password*	The password is encrypted prior to saving in the NetBackup IT Analytics database and is never visible in any part of the application.	Password1
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Field	Description	Sample Value
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See "Working with on-demand Data Collection" on page 624.	
Array Details	Activate array details collection. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Array Performance	Activate array performance collection. Note that at least two collections from this array must be performed BEFORE array performance data can be reported on. Array performance collection requires FLARE code version 05.31.000.5.006 A01 (VNX Block) or higher and current supported versions of NaviCLI for each. Click the clock icon to create a schedule.	

6 Click **OK** to save the policy.

7 On the Data Collector server, install/update the Data Collector software.

Chapter 29

Configuration for EMC VPLEX

This chapter includes the following topics:

- Pre-Installation setup for EMC VPLEX
- Prerequisites for adding Data Collectors (EMC VPLEX)
- Installation overview (EMC VPLEX)
- Adding a EMC VPLEX Data Collector policy

Pre-Installation setup for EMC VPLEX

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC VPLEX)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation overview (EMC VPLEX)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC VPLEX data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding a EMC VPLEX Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

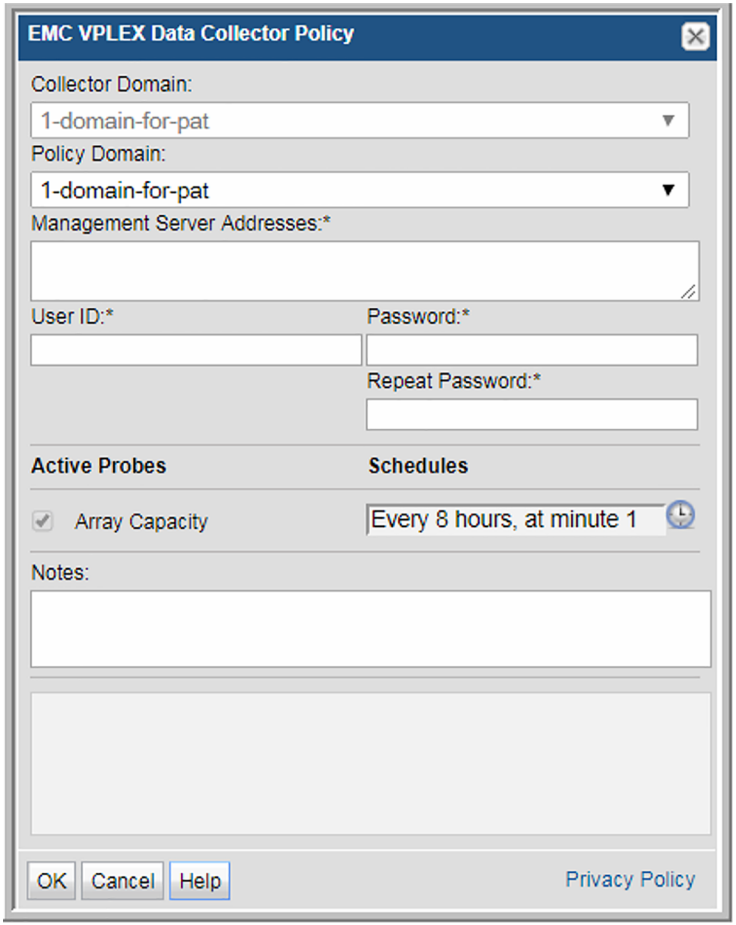
To add the policy

1 **Select Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	One or more VPLEX IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10,myhost. **Note:** To collect from a Cluster, enter the IP address of only one of the management servers.
User ID*	View-only user ID and password for the EMC VPLEX storage system.
Password*	The password associated with the User ID.
Array Capacity (Active Probe)	This collection is enabled by default to collect array capacity data from your EMC VPLEX environment.
Schedule	Click the clock icon to create a schedule. By default, it is collected every 8 hours. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 30

Configuration for EMC XtremIO

This chapter includes the following topics:

- Pre-Installation setup for EMC XtremIO
- Prerequisites for adding Data Collectors (EMC XtremIO)
- Installation overview (EMC XtremIO)
- Add an EMC XtremIO Data Collector policy

Pre-Installation setup for EMC XtremIO

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (EMC XtremIO)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation overview (EMC XtremIO)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the EMC XtremIO data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Add an EMC XtremIO Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

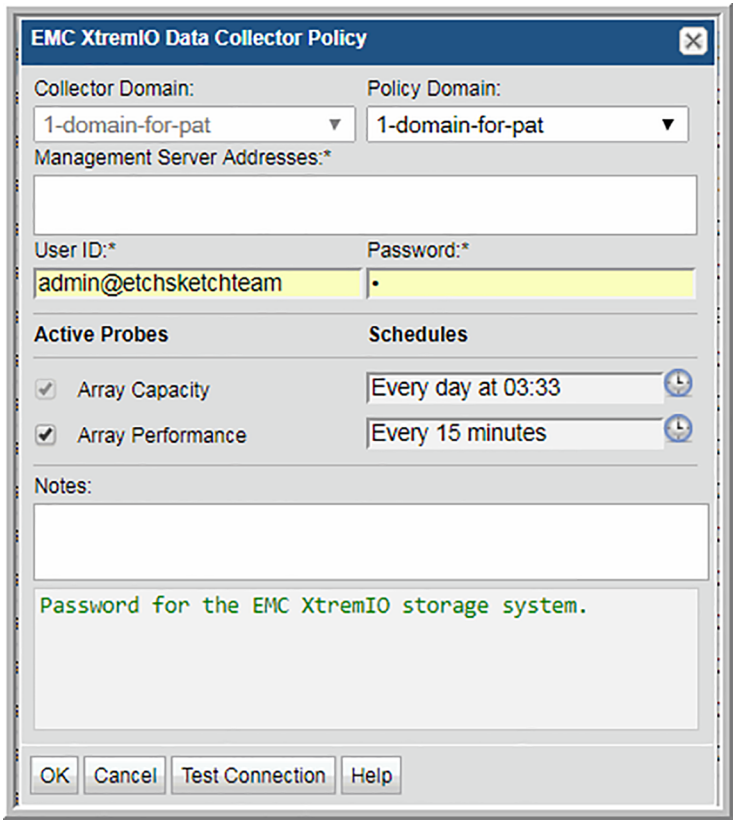
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	One or more XtremIO Management server IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost
User ID*	View-only User ID for the EMC XtremIO storage system.
Password*	Password for the EMC XtremIO storage system. The password associated with the User ID.
Array Capacity (Active Probe)	This collection is enabled by default to collect array capacity data from your EMC XtremIO environment. Click the clock icon to create a schedule. By default, collection occurs at 3:33 am daily.
Array Performance	Click the checkbox to activate array performance collection. By default, collection is every 15 minutes. Collected performance data will be 15 minutes older than the current time. To avoid memory issues with large sets of performance data, set a collection schedule for no more than 1 hour.

Field	Description
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See “Working with on-demand Data Collection” on page 624.

Chapter 31

Configuration for FUJITSU ETERNUS Data Collector

This chapter includes the following topics:

- About data collector
- Pre-installation setup
- Prerequisites for adding Data Collectors
- Installation overview
- Adding a FUJITSU ETERNUS Data Collector policy

About data collector

NetBackup IT Analytics now supports Fujitsu ETERNUS data collection. The following models are supported.

- **CS8000**: ETERNUS CS8000 model of FUJITSU is a unified data protection platform which simplifies backup and archiving for open systems and mainframes. Industry standard VTL and NFS/CIFS interfaces allow one unified data protection approach and optimize backup and archive infrastructures.
- **DX/AF**: The FUJITSU Storage ETERNUS AF delivers the advantages of flash storage to the max, supporting all tier-1 applications. With ultra-low response times that set performance records, mirroring and transparent failover, selective deduplication/compression and easily-configurable automated quality of service to minimize admin work, this system transforms your data center, saving you people, time and money.

Pre-installation setup

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

ETERNUS CS8000 provides IT departments with multi-site, multi-tier protection that is easy to manage – both for near-term restore and long-term retention in any backup environment. The end results are improved protection, streamlined management, and lower overall costs.

Prerequisites for adding Data Collectors

- 64-bit OS. See *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation overview

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables the Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the **FUJITSU ETERNUS** Data Collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

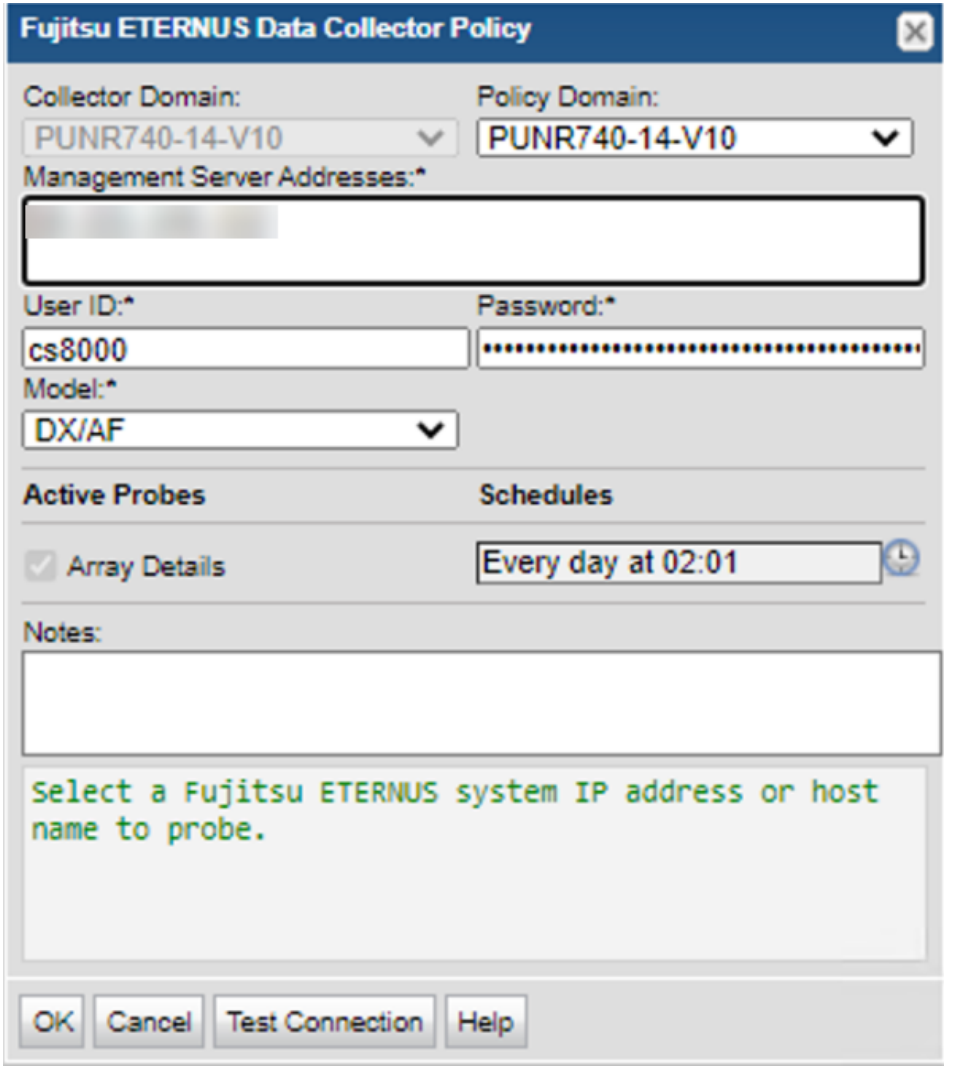
Adding a FUJITSU ETERNUS Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide* > *Capacity Manager configurations* > *Supported storage arrays and access requirements* section.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported. On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



Specify the required parameters. Mandatory parameters are denoted by an asterisk (*)

Table 31-1 FUJITSU ETERNUS Data Collector policy parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	Hostname or IP Address of the Fujitsu Eternus System
User ID*	View-only User ID for the Fujitsu ETERNUS system.
Model*	Select the appropriate model. The following models are supported: ■ Eternus CS8000 ■ DX/AF
Password*	Password for the Fujitsu ETERNUS system
Active Probes	
Array Details	This probe is enabled by default to collect the data for Fujitsu Eternus System. **Note:** By default, it is collected at 02:01 daily.
Schedule	Click **Clock** icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 31-1 FUJITSU ETERNUS Data Collector policy parameters *(continued)*

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See Working with on-demand Data Collection.

Chapter 32

Configuration for Hitachi Block

This chapter includes the following topics:

- Pre-Installation setup for Hitachi Block
- Prerequisites for adding Data Collectors (Hitachi Block)
- Installation overview (Hitachi Block Storage)
- Adding a Hitachi Block Storage Data Collector policy
- Configuring a Hitachi Device manager user
- Configuring a Collector for Hitachi NAS block storage
- Adding an HP command view advanced Data Collector policy

Pre-Installation setup for Hitachi Block

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Hitachi Block)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Note the port used by the Hitachi (Block) Data Collector: TCP 2001. The HIAA probe uses 22015 for Http and 22016 for Https.
- If collecting performance data, the Data Collector must be installed on the same server as HTnM (Tuning Manager). And, a single Data Collector policy must be used to collect both the capacity data from the Device Manager server and the performance data from the Tuning Manager server.
- Gather the following required configuration details:
  - HDvM Name or IP Address
  - HDvM User ID & Password: For HDvM 7.1.1 and 7.2, the user ID must have view permissions to HRpM and HTSM.
  - HTnM Install Location: Location of the HTnM (Tuning Manager) server installation directory.

Installation overview (Hitachi Block Storage)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Hitachi Block Storage data collection policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector Installation.

Adding a Hitachi Block Storage Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

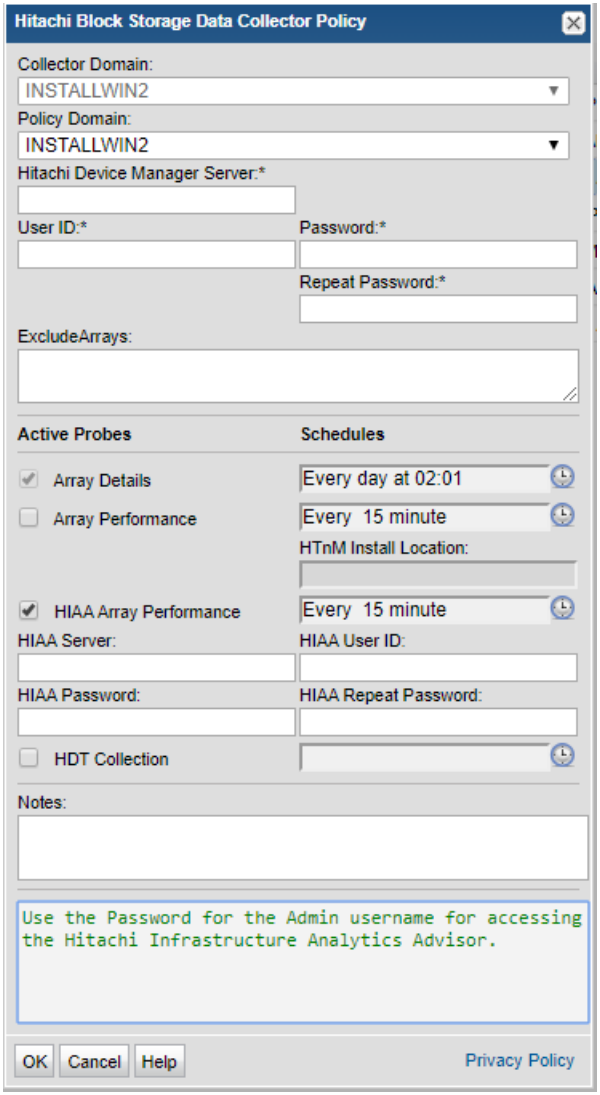
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. **Select Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

   For HP Command View Advanced Edition, HP XP arrays are treated as Hitachi Block Storage. To add a policy to collect from HP StorageWorks XP arrays (HP Command View Advanced Edition), use this Hitachi Block Storage Data Collector Policy.

5 Specify Data Collector Properties.



6 Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Hitachi Device Manager Server*	The address of the Hitachi Device Manager Server--either the IP address or server name. For HP Command View Advanced Edition, use the IP address or server name of the Command View Server. If this policy is being created to collect block storage shared with Hitachi NAS (HNAS), you must specify the IP address of the Hitachi Device Manager that manages the array that shares capacity with HNAS. See "Configuring a Collector for Hitachi NAS block storage" on page 315.
User ID*	Use the User ID and passcode as defined in Hitachi Device Manager (HDvM). This typically would be an administrator privilege, but must be a minimum privilege of a view-only user. Create a new user with view-only privileges and add the user to ViewGroup, a built-in HDvM group. See "Configuring a Hitachi Device manager user" on page 312. For Hitachi Device Manager 7.1.1 and 7.2, the user ID configured to access HDvM must have view permissions to HRpM and HTSM.
Password*	**Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.

Field	Description
Exclude Arrays	Enter one or more array names to be excluded. Comma-separated names are supported. Example: USPV1_172.16.1.13, USPV1_172.16.1.14, AMS - Corporate(5100)@172.16.1.43
Array Details	Click the check box to activate array details collection. Click the clock icon to set the schedule. For example: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri.
Array Performance	Click the check box to activate performance collection and enable entries and selections for the HTnM Install Location and the Performance Schedule. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Requirement: To collect performance data from Hitachi Tuning Manager, the Data Collector must be installed on the same server as Tuning Manager. And, a single Data Collector policy must be used to collect both the capacity data from the Device Manager server and the performance data from the Tuning Manager server.
HTnM Install Location	Specify the Tuning Manager server installation directory. By default, the Tuning Manager server will be installed in the following locations: Windows Server 2003 (x86) and Windows Server 2008 (x86): %SystemDrive%\Program Files\HiCommand\TuningManager Windows Server 2003 (x64) and Windows Server 2008 (x64): %SystemDrive%\Program Files (x86)\HiCommand\TuningManager Solaris: /opt/HiCommand/TuningManager
HIAA Array Performance	Click the check box to activate performance collection using Hitachi Infrastructure Analytics Advisor (HIAA) . Note that at least one collection from this array must be performed BEFORE array performance data can be collected. This probe collects LUN and Port performance information.

Field	Description
HIAA Server	The IP address of the Infrastructure Analytics Advisor management server. Typically, only the IP address/Host name is required, with port 22015 for HTTP, and 22016 for HTTPS used as the default. To change the port that the Data Collector uses to communicate with the array, use the format: <ipaddress>:<port number>. For example: 172.16.1.1:443.
HIAA User ID	Admin username for accessing the Hitachi Infrastructure Analytics Advisor.
HIAA Password	Password for the Admin username (User ID) for accessing the Hitachi Infrastructure Analytics Advisor.
HDT Collection	Activate HDT Collection. An HDT Schedule is not required if your HDvM is not managing VSP arrays running HDT. Click the clock icon to create a schedule frequency. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

7. Click **OK** to save the Policy and return to the Collection Administration window where the Policy will be listed under the Data Collector.
8. On the Data Collector server, install/update the Data Collector software.

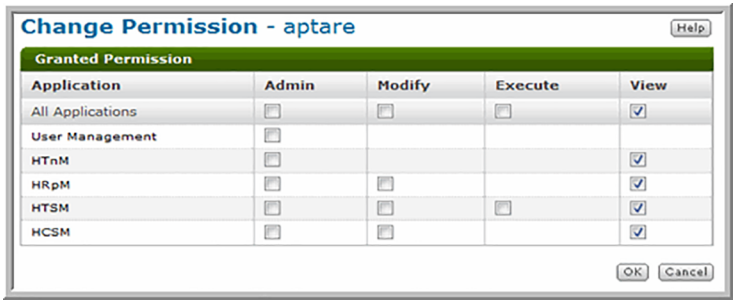
Configuring a Hitachi Device manager user

The Data Collector requires read-only permission to gather data from Hitachi Device Manager (HDvM). This requires an HDvM read-only user. To configure a read-only user, take the following steps.

1. Login to Hitachi Device Manager.
2. From the Administration tab, click **Users and Permissions**.
3. Under Users and Permissions, select **Users** and click **Add User**.
4. For the User ID, enter **aptare** and fill in the required user fields and click **OK**.

5. Under Users and Permissions, select **Users**again to verify the account that you just created.
6. Click the **Change Permission** tab for the **aptare** user only.
7. Check the boxes under the View column to configure read-only permission for each licensed component. Options are: HTnM, HRpM, HTSM, and HCSM.

Note: You may not have all (or any) components licensed in your environment, therefore you may not see all the components.



8. Click **OK** to save the permissions for the **aptare** user.
9. From the Administration tab, click **User Groups**.
10. Select **ViewGroup**, which is a built-in user group.
11. In the ViewGroup window, click **Add Users**.
12. Select the **aptare** user and click **OK**.

Validate the User ID access

1. To list the **aptare** user configured on Hitachi Device Manager, use the Hitachi Device Manager XML API, connecting via:
2. http://<DeviceManagerIP>:2001/service/ServerAdmin

   where:

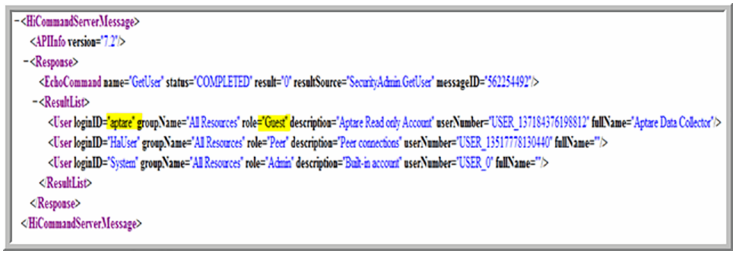
DeviceManagerIP	Hitachi Device Manager IP address
2001	Default port number allocated to this server

3. Copy and paste the following XML request into the Server Administration Service API window and click **Submit**.

```
    <?xml version="1.0"?>
    <HiCommandServerMessage>
    <APIInfo version="7.2"/>
    <Request>
    <SecurityAdmin>
    <Get target="User">
    <User>
    </User>
    </Get>
    </SecurityAdmin>
    </Request>
</HiCommandServerMessage>
```



Sample output from this request:



This XML response lists the **aptare** user as a Guest role. The Guest role has read-only permission, sufficient for collecting data from Hitachi storage arrays.

Configuring a Collector for Hitachi NAS block storage

If you are configuring a Hitachi Data Systems policy to collect block storage shared with Hitachi NAS (HNAS), you will need the IP address of the Hitachi Device Manager server.

1. In the HNAS UI, go to: **Home > Storage Management > Hitachi Device Managers**.
2. Use the Device Manager's default user name and password.

Adding an HP command view advanced Data Collector policy

For HP Command View Advanced Edition, HP XP arrays are treated as Hitachi Block Storage. To add a policy to collect from HP StorageWorks XP arrays (HP Command View Advanced Edition),

See "Adding a Hitachi Block Storage Data Collector policy" on page 308.

Chapter 33

Configuration for Hitachi Content Platform (HCP)

This chapter includes the following topics:

- Pre-Installation setup for Hitachi Content Platform (HCP)
- Prerequisites for adding Data Collectors (Hitachi Content Platform)
- Installation overview (Hitachi Content Platform)
- Add a Hitachi Content Platform (HCP) Data Collector policy
- Setting up permissions for an HCP local user or active directory user
- Hitachi content platform system management console
- Hitachi content platform tenant management console

Pre-Installation setup for Hitachi Content Platform (HCP)

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Hitachi Content Platform)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Create an HCP system Local user or Active Directory user with specific permissions using the Hitachi Content Platform System Management Console and the Hitachi Content Platform Tenant Management Console. Additional security settings must also be enabled. This enables data collection for HCP namespaces and namespace statistics.

Installation overview (Hitachi Content Platform)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Hitachi Content Platform (HCP) data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Add a Hitachi Content Platform (HCP) Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

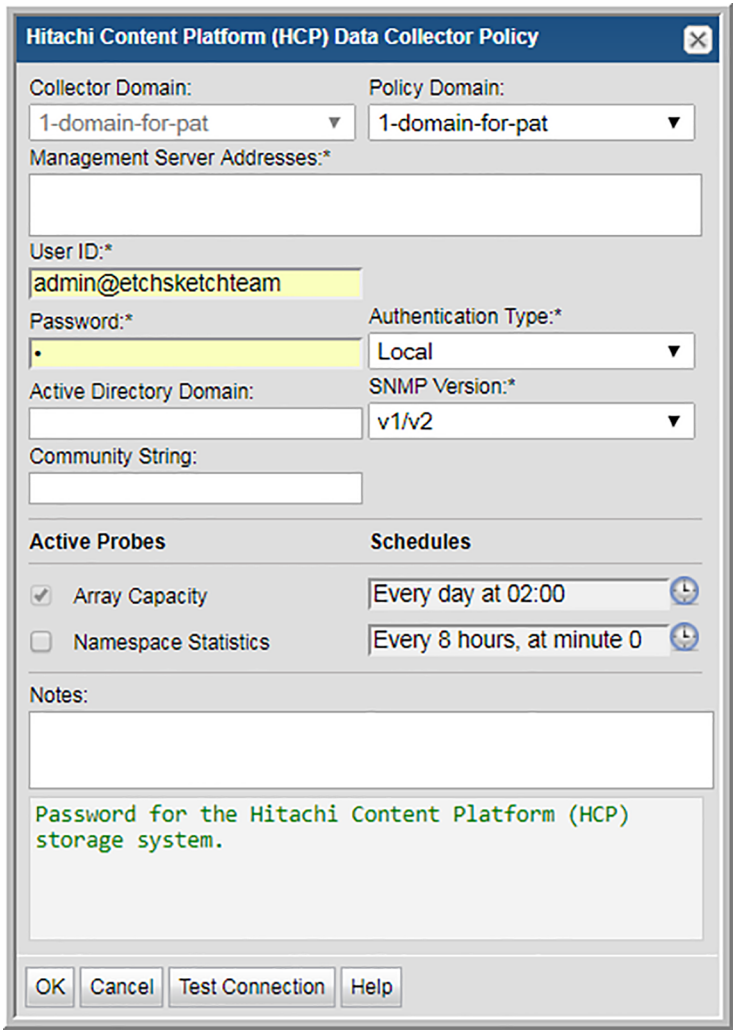
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

Note: The Data Collector retrieves data only from the HCP object array. It has no visibility into the physical capacity supporting the HCP array. Therefore, capacity values potentially could be double counted, for example, if data from a supporting array is also being collected.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	One or more HCP Management server IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost.
User ID*	User ID for the Hitachi Content Platform (HCP) storage system. This ID is also used for MAPI and SNMPv3. Set specific permissions using the Hitachi Content Platform System Management Console and the Hitachi Content Platform Tenant Management Console. Additional security settings must also be enabled. See "Setting up permissions for an HCP local user or active directory user" on page 322.
Password*	Password for the Hitachi Content Platform (HCP) storage system. This password is also used for MAPI and SNMPv3.
Authentication Type*	Select either Local or Active Directory Authentication.
Active Directory Domain	The Active Directory Domain Name for the Hitachi Content Platform (HCP) storage system is an optional field, required only when Active Directory is selected as the Authentication Type.
SNMP Version*	SNMP version.
Community String	Community string for SNMP.

Field	Description
Array Capacity/Schedule	This collection is enabled by default to collect array capacity data from your Hitachi Content Platform (HCP) environment. Click the clock icon to create a schedule. By default, it is collected at 3:33 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Namespace Statistics/Schedule	A Hitachi Content Platform (HCP) repository is partitioned into namespaces. A namespace is a logical grouping of objects. Namespaces provide a mechanism for separating the data stored for different applications, business units, or customers. **Note:** The minimum interval size maintained by the array is one hour, and NetBackup IT Analytics collects namespace statistics based on the length of time since the last collection cycle, to a maximum of 8 hours. One collection per hour is recommended. However, if for example, you schedule one collection every 4 hours, NetBackup IT Analytics will maintain the 4 hour increments and so on. Click the clock icon to create a schedule. By default, it is collected every 8 hours. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See “Working with on-demand Data Collection” on page 624.

Setting up permissions for an HCP local user or active directory user

An HCP repository is partitioned into namespaces. Each namespace consists of a distinct logical grouping of objects with its own directory structure. Namespaces provide a mechanism for separating the data stored for different applications, business units, or customers. Namespaces are owned and managed by tenants.

To enable data collection for HCP namespaces and namespace statistics, a user must be created with certain permissions using the Hitachi Content Platform System Management Console and the Hitachi Content Platform Tenant Management Console. Additional security settings must also be enabled.

Note: Data collection will still occur without these settings, but namespace and namespace statistics will not be included.

Hitachi content platform system management console

Hitachi Content Platform supports two user types:

- Local - User accounts defined and authenticated in the HCP system
- Active Directory - The users, passwords stored in Active Directory and authenticated remotely by AD.

You can create new users to match the user profile in the data collector policy or use existing users with the following roles set.

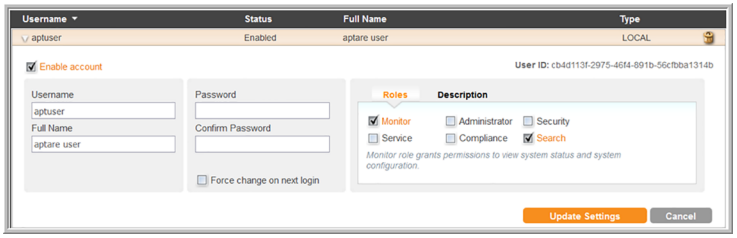
Local users

Use the Hitachi Content Platform System Management Console to create a user and enable the Monitor and Search roles. You must also define Security settings to enable the management API to allow access to some of the HCP system settings.

This user ID must be a system-level user and match the User ID entered in the data collector policy.

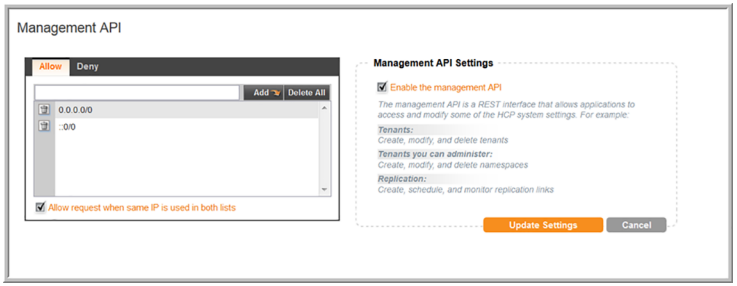
Monitor grants permission to use the System Management Console to view the HCP system status and most aspects of the system configuration, including tenant configurations.

Search grants permission to use the metadata query API and Search Console to query or search the default namespace and any namespaces owned by HCP tenants that are configured to allow system-level users to manage them and search their namespaces.



Local users and active directory users

Use the Security settings in the Hitachi Content Platform System Management Console to enable the Management API Settings (MAPI). This should be enabled at the cluster level.



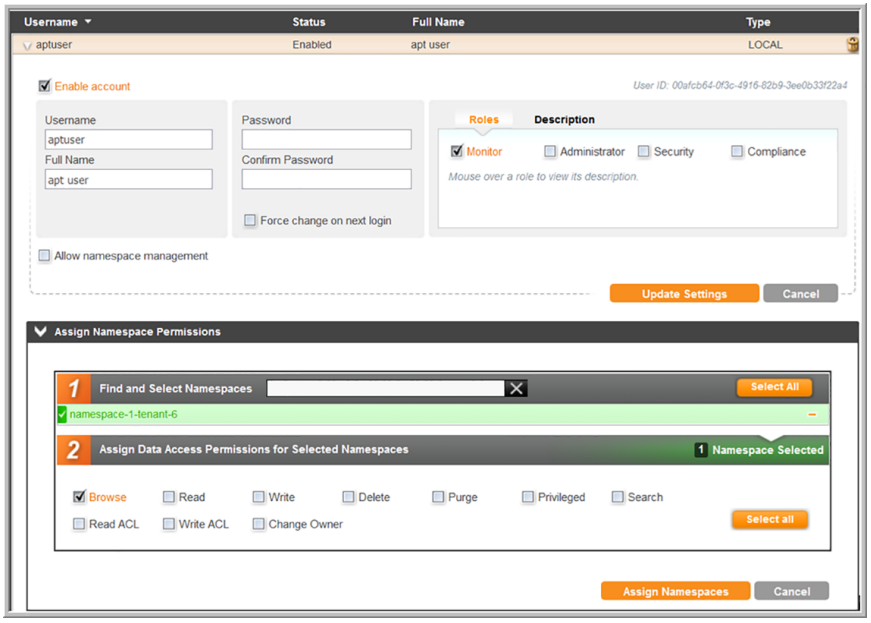
Hitachi content platform tenant management console

Namespaces are owned and managed by administrative entities called tenants. A tenant typically corresponds to an organization, such as a company or a division or department within a company.

Use the Hitachi Content Platform Tenant Management Console to create a user account that matches the user created using the Hitachi Content Platform System Management Console. Enable Monitor and Browse permissions for each namespace under a tenant.

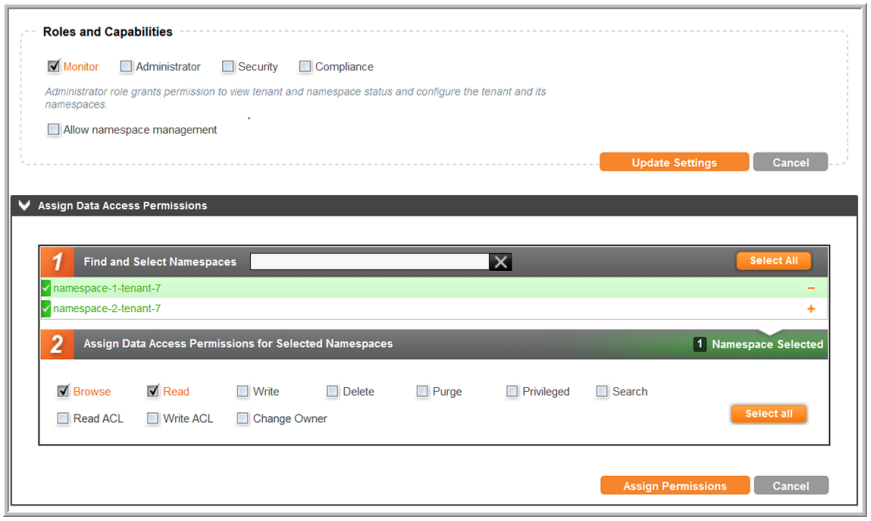
You must also define Security settings to enable the management API to allow access to some of the HCP system settings. This user ID must match the User ID entered in the data collector policy.

Local users



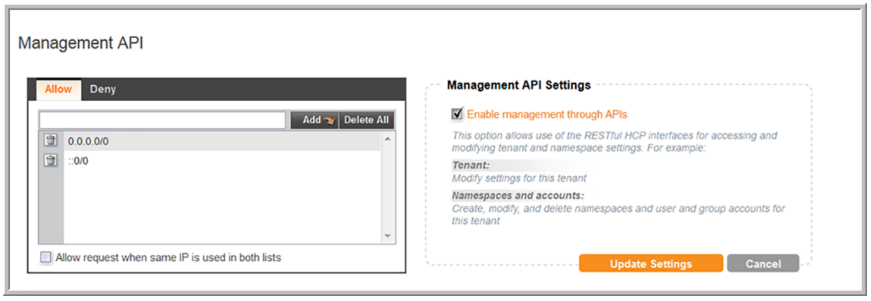
For each tenant, click the Allow system level users to manage this tenant and search its namespaces check box.

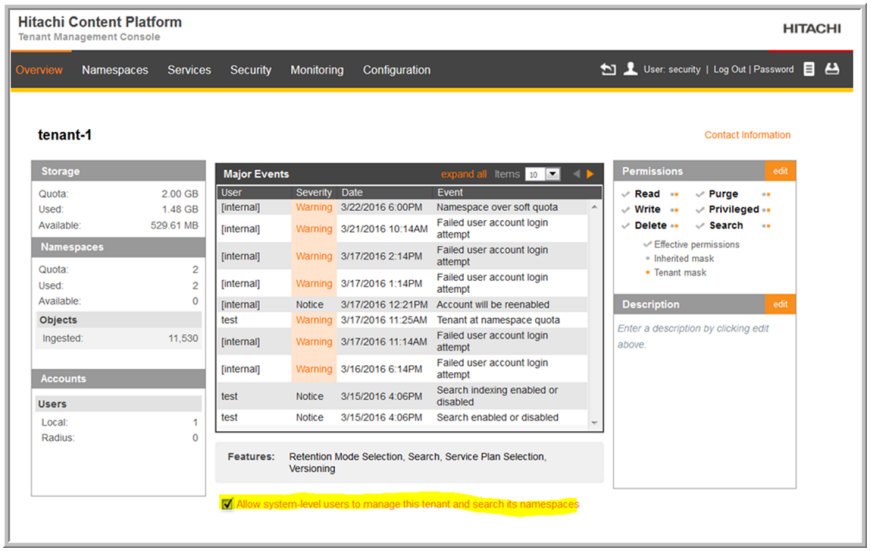
Active directory users



Local users and active directory users

Use the Security settings in the Hitachi Content Platform Tenant Management Console to enable the Management API Settings (MAPI).




Hitachi Content Platform
Tenant Management Console
HITACHI
Overview
Namespaces
Services
Security
Monitoring
Configuration
User: security | Log Out | Password
tenant-1
Contact Information
Storage
Quota: 2.00 GB
Used: 1.48 GB
Available: 529.61 MB
Namespaces
Quota: 2
Used: 2
Available: 0
Objects
Ingested: 11,530
Accounts
Users
Local: 1
Radius: 0
Major Events
expand all
Items 10
User Severity Date Event
[internal] Warning 3/22/2016 6:00PM Namespace over soft quota
[internal] Warning 3/21/2016 10:14AM Failed user account login attempt
[internal] Warning 3/17/2016 2:14PM Failed user account login attempt
[internal] Warning 3/17/2016 1:14PM Failed user account login attempt
[internal] Notice 3/17/2016 12:21PM Account will be reenabled
test Warning 3/17/2016 11:25AM Tenant at namespace quota
[internal] Warning 3/17/2016 11:14AM Failed user account login attempt
[internal] Warning 3/16/2016 6:14PM Failed user account login attempt
test Notice 3/15/2016 4:06PM Search indexing enabled or disabled
test Notice 3/15/2016 4:06PM Search enabled or disabled
Features: Retention Mode Selection, Search, Service Plan Selection, Versioning
Allow system-level users to manage this tenant and search its namespaces
Permissions
edit
Read
Write
Delete
Purge
Privileged
Search
Effective permissions
Inherited mask
Tenant mask
Description
edit
Enter a description by clicking edit above.

Chapter 34

Configuration for Hitachi NAS

This chapter includes the following topics:

- Pre-Installation setup Hitachi NAS
- Prerequisites for adding Data Collectors (Hitachi NAS - HNAS)
- Installation overview (Hitachi NAS - HNAS)
- Adding a Hitachi NAS (HNAS) Data Collector policy
- HNAS configuration requirements
- Adding the collector

Pre-Installation setup Hitachi NAS

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Hitachi NAS - HNAS)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Reside in the same time zone as the subsystem from which data will be collected
- For performance reasons, Data Collectors should not be installed on the same server as the Portal. If, for some reason, you require both to be on the same server, the Portal and Data Collector software should not reside in the same directory on the server.
- If collecting performance data, the Data Collector must be installed on the same server as HTnM (Tuning Manager). And, a single Data Collector policy must be used to collect both the capacity data from the Device Manager server and the performance data from the Tuning Manager server.

Gather the following required configuration details:

- HNAS Admin EVS Address
- User ID & Password: Credentials with supervisor privileges for accessing the Hitachi NAS.
- Server Control (SSC) Utility Location: Location of the SSC command-line utility.

Installation overview (Hitachi NAS - HNAS)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Hitachi NAS data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector Installation.

Adding a Hitachi NAS (HNAS) Data Collector policy

Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

For specific prerequisites and supported configurations refer to the ,*Certified Configurations Guide*.

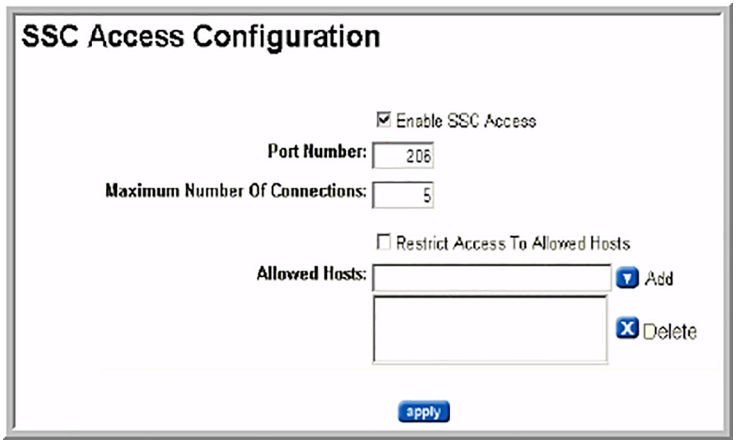
This Data Collector policy collects from Hitachi NAS. To collect block storage shared with HNAS, you must also create a separate data collector policy for the relevant supported vendor storage; for example, Hitachi Storage. If that policy is a Hitachi Block Storage policy, you must specify the IP address of the Hitachi Device Manager that manages the array that shares capacity with HNAS.

HNAS configuration requirements

1. The SSC Utility must be copied to a location on the Data Collector server. Note this location, as it is required when you configure a NetBackup IT Analytics HNAS Data Collector policy.
2. The Data Collector uses the SiliconServer Control (SSC) CLI to access the Hitachi NAS CLI via Admin EVS (a public network). Therefore, a server administration IP address must be assigned to at least one of the Gigabit Ethernet (GE) interfaces. Refer to the “IP Network Setup” section of the HNAS System Administration Guide.
3. SSC Access must be enabled via the SSC Admin utility on the Hitachi NAS server:

Configuring SSC access

In the SSC Admin utility, enable SSC Access. The default port number is 206. You also can use this configuration to restrict access to only certain users.



Adding the collector

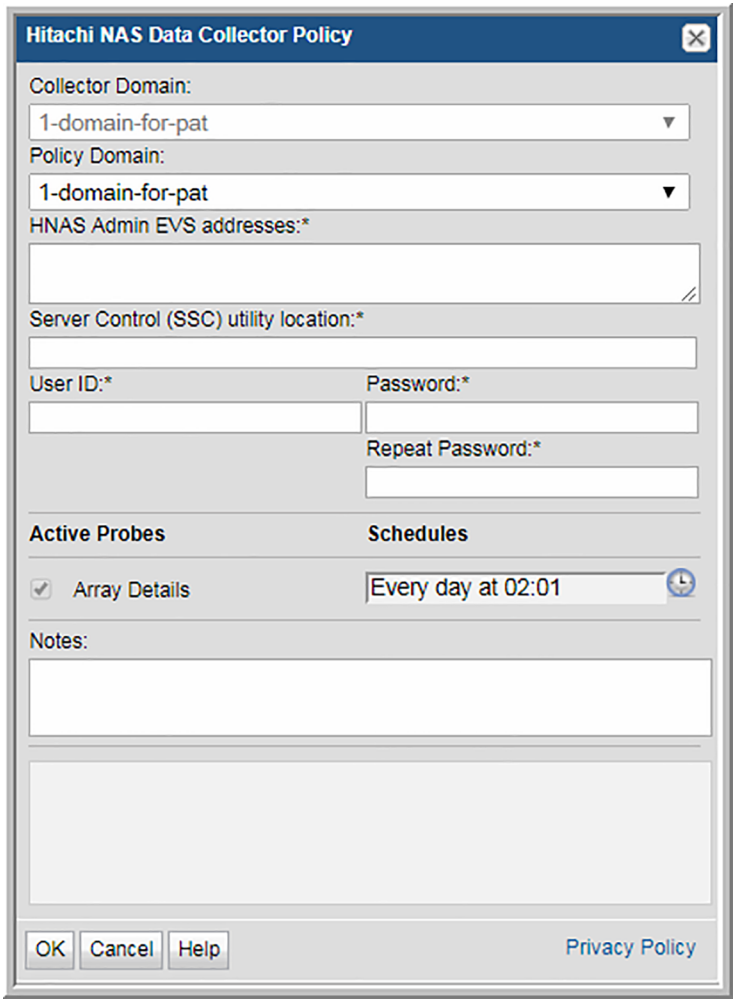
Note: The Data Collector retrieves data only from the HCP object array. It has no visibility into the physical capacity supporting the HCP array. Therefore, capacity values potentially could be double counted, for example, if data from a supporting array is also being collected.

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
HNAS Admin EVS Addresses*	Enter one or more Hitachi NAS Admin EVS addresses separated by commas. **Note:** You must also create a separate Data Collector policy to collect the block storage that shares the space with Hitachi NAS (HNAS). Choose a relevant supported storage vendor policy such as Hitachi Block Storage.	
Server Control (SSC) utility location*	The location of the SiliconServer Control (SSC) CLI. See "HNAS configuration requirements" on page 330. Linux: `/usr/bin` Windows: `c:\program files\ssc`	
User ID*	Create a user with supervisor privileges for accessing the Hitachi NAS.	`Administrator`
Password*	Password associated with the User ID. The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Array Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

6 Click **OK** to save the Policy.

Chapter 35

Configuration for Hitachi Vantara All-Flash and Hybrid Flash Storage

This chapter includes the following topics:

- Pre-Installation setup for Hitachi Vantara All-Flash and Hybrid Flash Storage
- Prerequisites for adding Data Collectors (Hitachi Vantara All-Flash and Hybrid Flash Storage)
- Installation overview
- Adding a Hitachi Vantara All-Flash and Hybrid Flash Storage policy

Pre-Installation setup for Hitachi Vantara All-Flash and Hybrid Flash Storage

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Hitachi Vantara All-Flash and Hybrid Flash Storage)

- A 64-bit OS. See the *NetBackup IT Analytics Certified Configurations Guide* for the supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.
  Example:

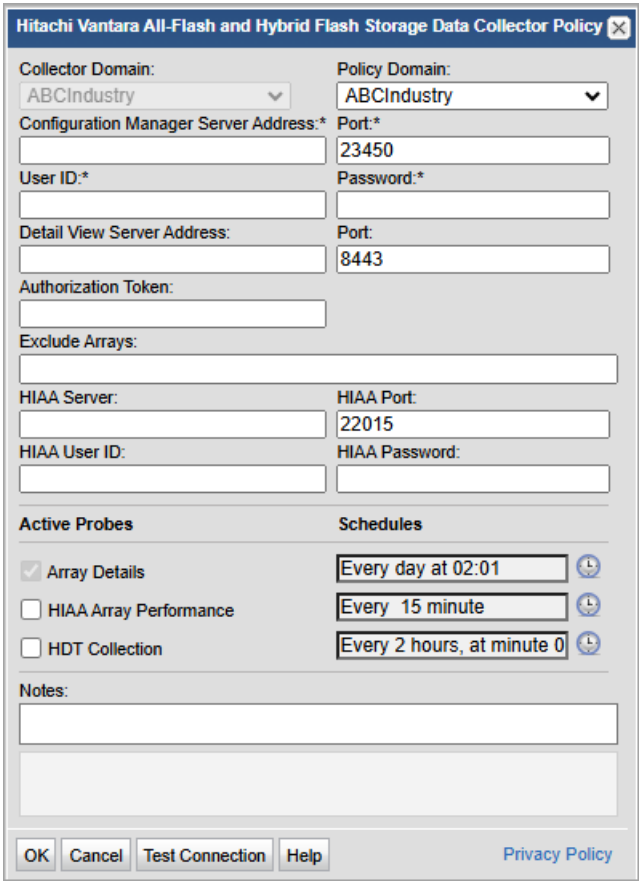
  ```
  172.16.2.2 aptareportal.<yourdomain>.com
  172.16.2.3 aptareagent.<yourdomain>.com
  ```

- Obtain the following required configuration details:
  - For Array Details Probe and HDT Probe
    - Host name or IP Address for the Hitachi Ops Center Configuration Manager REST API Server.
    - User ID (Storage Administrator View Only role) and Password to connect to Configuration Manager via REST API.
    - To create a User with Storage Administrator (View Only) permissions, follow the below steps.
      - Step-1: Create a new (use an existing) User Group with Storage Administrator (View Only) role.
      - Step-2: Assign all the Resource Groups to this User Group that you want APTARE to report on. It is recommended that all the Resource Groups are added so that APTARE is able to get the information.

        - Step-3: Create a new User with User Group created in Step 1

    - For HIAA Performance Probe:
        - Hitachi Infrastructure Analytics Advisor (HIAA) Server address.
        - Admin User ID and Password to connect to HIAA Server using REST API.

- Before adding a new Hitachi Vantara All-Flash and Hybrid Flash Storage policy, ensure that any existing Hitachi Block Storage policies (Hitachi Device Manager based collection) is not collecting data for same arrays. If this scenario is possible:
    - Disable the existing Hitachi Block Storage policy from **Admin** > **Data Collection** > **Collector Administration** screen.
      Or
    - Exclude such arrays from Hitachi Block Storage Policy using the **Exclude Arrays** feature.



- Collection for Hitachi Arrays should be done either via Hitachi Block (Hitachi Device Manager based collection) or using Hitachi Vantara All-Flash and Hybrid Flash Storage policy (via Hitachi Ops Center Configuration Manager REST API). Users should not collect same array from both policies, this can result in double counting for licensing.

Installation overview

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.

3. In the Portal, add the Hitachi Vantara All-Flash and Hybrid Flash Storage data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. See Installing the WMI Proxy Service (Windows Host Resources only).
7. Validate the Data Collector installation.

Adding a Hitachi Vantara All-Flash and Hybrid Flash Storage policy

Before adding the policy

A Data Collector must exist in the Portal, to which you will add Data Collector Policies. For specific prerequisites and supported configurations for a specific vendor, see the *NetBackup IT AnalyticsCertified Configurations Guide*.

After adding the policy

For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported. On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same way as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1 Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Configuration Manager Server Address*	Hostname or IP Address for the Hitachi Ops Center Configuration Manager REST API Server.
Port*	Configuration Manager Server port number for REST API communication. The default port number is 23451 for SSL communications, and 23450 for non-SSL communications.
User ID*	Specify the username with Storage Administrator (View Only) role.
Password*	The password associated with the User ID.
Detail view server address	Hitachi Ops Center API Detail view Server Address (IP address or Host Name) for Array Details probe
Port	Hitachi Ops Center API Detail view server port number for REST API communication. The default port number is 8443.
Authorization token	Hitachi Ops Center detail view server authorization token for the Hitachi Vantara Flash Storage system.
Exclude Arrays	Enter one or more Array Serial Number to be excluded. Comma-separated list is supported. Example: 10127, 410100
HIAA Server Address	Hostname or IP Address of the Hitachi Infrastructure Analytics Advisor management server. This is required only when HIAA Array Performance probe is enabled.

Field	Description
HIAA Port	Port number for Hitachi Infrastructure Analytics Advisor management server. The default port number is 22015 for HTTP, and 22016 for HTTPS. This is required only when HIAA Array Performance probe is enabled.
HIAA User ID	Specify the Admin username for accessing the Hitachi Infrastructure Analytics Advisor (HIAA). This is required only when HIAA Array Performance probe is enabled.
HIAA Password	Use the Password for the Admin username for accessing the Hitachi Infrastructure Analytics Advisor (HIAA). This is required only when HIAA Array Performance probe is enabled.
Array Details	This probe is enabled by default to collect array capacity data from your Hitachi environment. By default, it is collected at 02:01 daily.
HIAA Array Performance	This probe is used to collect the array performance details. The default schedule is every 15mins. Note that at least one collection from this array must be performed BEFORE array performance data can be collected.
HDT Collection	This probe is used to collect the Dynamic Tiering information. The default schedule is every 2 hours.
Schedules	Click the clock icon to create a schedule. By default, it is collected at 1:01 daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: Examples of CRON expressions: ■ */30 * * * * means every 30 minutes ■ */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm ■ */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Click **OK** to save the Policy.

Chapter 36

Configuration of Host inventory

This chapter includes the following topics:

- Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements
- Host Inventory pre-installation setup
- Plan host Data Collection
- WMI Proxy requirements for Windows host Data Collection
- Host access requirements
- Verify command paths
- Host Inventory configuration steps
- Host Inventory setup overview
- Host Inventory maintenance overview
- Before discovering hosts
- Configure / Search the host Inventory
- Manage credentials
- Manage WMI proxy
- Manage paths
- Manage access control
- Host Inventory management

- Configure host Discovery policies to populate the host Inventory
- Execute and monitor host Discovery
- Validate host connectivity
- Show errors
- Filter the host Inventory - hide / un-hide, remove
- Host Inventory search and host Inventory export
- Export the host Inventory
- Configure and edit host probes
- Propagate Probe Settings: Copy Probes, Paste Probes

Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements

If you are using sudo to elevate access to root privileges, update the sudoers file:

- Sudoers file: /etc/sudoers
- Use the lists of the sudo commands (per OS) that are located on the Portal server in:

  ```
  <Home>/opt/aptare/updates
  ```

- Comment out this line in the sudoers file: **Defaults requiretty**

Access Requirements by OS

Table 36-1 Host Resources Prerequisites by Operating System

Host OS	Host Access Requirements	Port Requirements	Notes
Linux RH Linux SUSE CentOS AIX Solaris	ssh or telnet must be enabled Some commands may require an account with super-user root privileges. **sudo**, **sesudo**, and **pbrun** are supported; ensure the user ID has required sudo, sesudo, or pbrun privileges.	ssh: 22 telnet: 23	Collection uses ssh/telnet to execute commands. OS and application commands require root privileges for HBA API access. The **sysstat** utility must be installed on Linux servers or storage nodes for Linux host performance data collection.
Windows	A WMI Proxy is required to collect from Windows hosts. All Windows hosts require a user ID with Administrator privileges for WMI.	RPC: TCP Port 135 for WMI DCOM: TCP/UDP 1024-65535 TCP/IP 1248, if WMI Proxy server is not the same as the Data Collector server	When the Data Collector Policy is configured to include file-level data, the Data Collector and WMI need to use a Windows Domain Administrator ID.

Host Inventory pre-installation setup

Capacity Manager can collect data and then report on storage that is allocated to and consumed by hosts in your enterprise. Host capacity and utilization reports enable you to optimize existing storage resources and more accurately forecast usage.

Host Resources Data Collection can gather the following information by probing hosts:

- Host Probes: Capacity (HBA, iSCSI, Volume Manager, Multi-pathing)
- Host Probes: Memory, Network, Process, Processor, System
- Application Probes: Exchange, SQL Server, Oracle, Oracle ASM
- File Analytics Probes

Note: Host Resources data collection does not require a dedicated Data Collector for each resource. If you have a Storage Array Data Collector, the Host Resources collector is inherently part of that Data Collector. However, if for some reason you do not have a Storage Array Data Collector, you can explicitly create just a Host Resources Data Collector.

Several key steps comprise the Host Data Collection Process. These steps are summarized here, with details provided in the descriptions of specific tasks.

- Add Hosts to the Host Inventory - This initial setup phase requires some pre-planning to ascertain which hosts and credentials will be needed for successful host authentication. Then, you'll take this information and create several configuration settings--credentials, WMI proxies, paths, and access control commands--required to discover hosts in your environment. The Host Discovery process attempts to find hosts using these configuration settings and then populates the host inventory.
- Configure & Validate Hosts - Once hosts have been added to the inventory, specific probe settings can be configured to tailor the type of data to be collected from a host. The Validate step provides feedback to troubleshoot host connectivity and data collection issues. In addition, you can hide/remove hosts that do not belong in your inventory--for example, IP addresses of non-host devices such as tape drives. This is an iterative process to verify the collection settings for each host in your host inventory.
- Enable & Manage On-going Collection - Once a host has been validated, enable on-going data collection. Subsequent changes to the host in your enterprise may impact data collection. As changes and collection issues arise, updates to host data collection configurations will be required.

Plan host Data Collection

Prior to configuring NetBackup IT Analytics to discover your host inventory, you must identify the hosts for which you will be collecting data. Because each enterprise has a unique inventory of hosts with specific access requirements and restrictions, the process of ensuring successful host data collection requires an assessment of the hosts in your environment and several configuration steps.

WMI Proxy requirements for Windows host Data Collection

A WMI Proxy server is required for collecting data from Windows hosts.

- WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service. To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.
- When installing the WMI Proxy, if the installer detects that Microsoft .NET is not already installed, it notes this dependency and then installs .NET for you. Microsoft .NET contains several necessary libraries.

Data Collector Server OS	WMI Proxy Requirements	Notes
Windows	WMI Proxy will be installed on the Data Collector server by default	
■ Red Hat Linux ■ CentOS	Identify a Windows machine on which to install the WMI Proxy	Note the IP address of the server on which the WMI Proxy resides, as you will use it during the Portal configuration process.

Host access requirements

This section lists the access requirements for host resource data collection. You will use this information to populate the configurations used by the Host Discovery, Validation, and Collection processes.

- Create a list of the name or IP address for each host for which you want to collect data.
- User ID & Password Credentials: Root-level, read-only access is required for host data collection.
  See "Manage credentials" on page 354.
  See "Manage access control" on page 360.
- Access Control: For security reasons, most enterprise environments mandate access control where a new non-root account is created, with temporarily elevated access to the required commands provided via an access control command, such as sudo. Otherwise, the root user is required for host access. For Linux Hosts in access control environments, if a command such as sudo is used and the absolute path is not in the interactive ssh, identify the absolute path of the access control command.

See “Verify command paths” on page 348.
See “Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements” on page 344.

- Path: NetBackup IT Analytics must have knowledge of the correct paths to access commands. An overview of the requirements is listed here, with the details provided in
  See “Verify command paths” on page 348.
  For Windows hosts, a path is required for fcinfo, hbacmd, and scli commands. For Linux hosts, if the Data Collector is installed on a Windows server, use plink.exe to determine the path; if the Data Collector is installed on a Linux server, determine the path by executing ssh.
- HBA Prerequisites: NetBackup IT Analytics uses an internal probing mechanism to gather Host Bus Adapter (HBA) data from Windows hosts. It is critical for the Data Collector to probe the HBA in order to establish a host’s relationship with storage. Without the HBA information, all storage for a host will be listed as local storage.

  Note: Do not enable HBA probes for VMware guest host collection.

  Windows: One of the following mechanisms is required to collect Windows HBA information. The Data Collector actually uses all of the mechanisms that are available and then merges the data collected from all. A collection error is reported only if all of the following methods fail.
  - hbaverify is provided by default with the Data Collector WMI Proxy installation.
  - scli - SANsurfer Command Line Interface (SCLI) for Windows from QLogic (SCLI is a separate install from the base install of SANsurfer and often is not installed with the SANsurfer utility).
  - hbacmd (HBAnyware from Emulex) is required for both LUN Mapping and HBA data collection. This is typically provided by default as part of the driver software.
  - fcinfo - Fibre Channel Information Tool from Microsoft is not typically used, as the previously listed methods are preferred.

  Linux: scli or hbacmd (required only for HBA information)
  Solaris: scli or hbacmd (required only for HBA information)

Verify command paths

Verify the command paths that will be used by the Data Collector.

Both Linux & Windows:

- If Veritas Volume Manager is installed on any hosts, note the path to the vxprint command.
- If any multi-pathing software is installed on hosts, note the path to the command.

Linux: Verify the non-interactive SSH path for Linux users for several sample hosts:

```
ssh <user>@<hostname> env
```

where <user> is the credential the collector will use to access the host.

To determine the Linux path from a Windows server, you can use a command-line interface to telnet/ssh client software. The following example shows Plink, which is a command-line interface to PuTTY (a telnet/ssh client):

To determine the Linux path from a Windows server, you can use a command-line interface to ssh client software. The following example shows Plink, which is a command-line interface to PuTTY (a ssh client):

```
plink <user>@<hostname> env
```

Example of a PATH for commands:

```
/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
```

Windows: Make a note of the paths for the executables identified for HBA data collection. Note that in Windows, multiple paths are separated by a semi-colon (;). For example:

```
C:\Program Files\Emulex\Util\HBAnyware;C:\Program
Files\QLogic\SANSurfer
```

Host Inventory configuration steps

This section contains:

- See “Host Inventory setup overview” on page 350.
- See “Host Inventory maintenance overview” on page 351.

Read this section first for a high-level overview, then follow the specific steps in the following to configure your system for Host Data Collection.

See “Before discovering hosts” on page 353.

See “Host Inventory management” on page 362.

Host Inventory setup overview

Note that some steps typically are required only as part of the initial configuration and rarely require additional maintenance. For the purpose of this document, these initial steps are treated as requirements:

See “Before discovering hosts” on page 353.



Note: Each step is summarized in this section. To access detailed descriptions, click the links for each step. The buttons at the bottom of the window--**Hide, Remove, Show Errors, Validate, Edit Probes, Copy Probes, Paste Probes**--are described in the following section.

See “Host Inventory maintenance overview” on page 351.

1. Prior to discovering hosts, a data collector policy must be configured. You can use an existing policy--for example, a data collector policy that has been created for Storage Array data collection--or create a new data collector policy.
2. See “Configure / Search the host Inventory” on page 353.

   Using the Host Inventory window, you can search for hosts in the inventory; or you can set up configurations in preparation for discovering and configuring hosts.

   - See “Configure and edit host probes” on page 375.
     Many of the probes may not be applicable to your enterprise. It is essential that you identify the probes that are relevant to your hosts.
3. See “Manage credentials” on page 354.

   Configure user IDs and passwords for authentication when the data collector is accessing hosts.
4. See “Manage WMI proxy” on page 357.

   A WMI Proxy is required to collect data from Windows hosts. Use this option to define one or more WMI Proxies.

5. See “Manage paths” on page 358.

   Configure the paths that data collectors will use to execute commands on hosts.

6. See “Manage access control” on page 360.

   Data Collectors require read-only access to execute non-intrusive commands on hosts. It is strongly recommended that a separate login account used strictly for NetBackup IT Analytics be established and using Active Directory for Windows systems and the sudo command for Linux systems, restrict the commands that NetBackup IT Analytics can issue. To accommodate this security approach, you can optionally specify access control commands like sudo, sesudo, or pbrun.

   See “Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements” on page 344.

7. See “Configure host Discovery policies to populate the host Inventory” on page 363.

   Host Discovery attempts to find hosts and populate your NetBackup IT Analytics host inventory. Create Host Discovery Policies that use the credentials, WMI proxies, and paths that you configured.

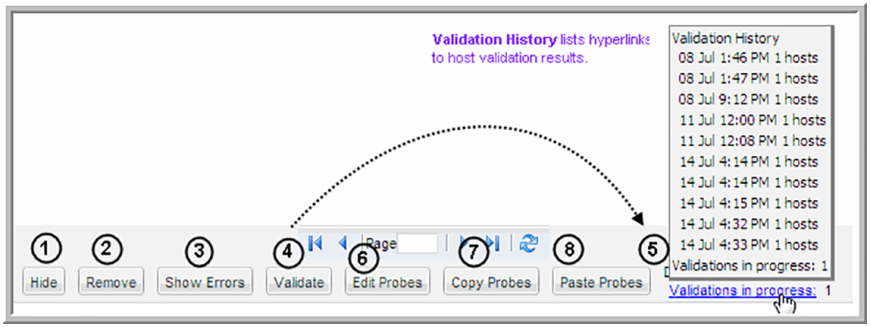
   - See “Validate host connectivity” on page 370.
     Host validation must take into account host access for a wide variety of conditions and environments. As the discovery process accesses hosts, informative messages will provide clues to connectivity issues. In addition, devices that don’t belong in a host inventory--for example, printers in the IP address range that you specified--may have been discovered and need to be hidden or removed from the inventory.

8. See “Host Inventory setup overview” on page 350.

   To facilitate data collection troubleshooting, you can create log requests and be notified when the logs are available. These logs can also be transferred to support for additional analysis.

Host Inventory maintenance overview

Once hosts have been discovered and they are listed in the Host Inventory, several options are provided to filter the list and also to manage the probes.



1. **Hide/Unhide Hosts**- Host Discovery may find devices that are not hosts that you want to manage; for example, printers.

   See “Filter the host Inventory - hide / un-hide, remove” on page 372.

2. **Remove Hosts**- Some IP addresses may be associated with devices that simply should be removed from the inventory, although if you execute a host discovery policy, the devices will return.

   See “Filter the host Inventory - hide / un-hide, remove” on page 372.

3. **Show Errors** - Use this feature to troubleshoot connectivity and validation issues.

   See “Show errors” on page 371.

4. **Validate** - Use this feature in combination with the Show Errors feature to troubleshoot host data collection issues.

   See “Validate host connectivity” on page 370.

5. **Show Validations** -

   See “Validation history” on page 370.

6. Edit Probes:

   See “Configure and edit host probes” on page 375.

7. Copy Probes:

   See “Propagate Probe Settings: Copy Probes, Paste Probes” on page 378.

8. Paste Probes

   See “Propagate Probe Settings: Copy Probes, Paste Probes” on page 378.

Before discovering hosts

If this is the first time you are collecting data from hosts, you will need to look at each of these steps to determine what configurations are required.

Before collecting host data for the first time, several configurations must be set up:

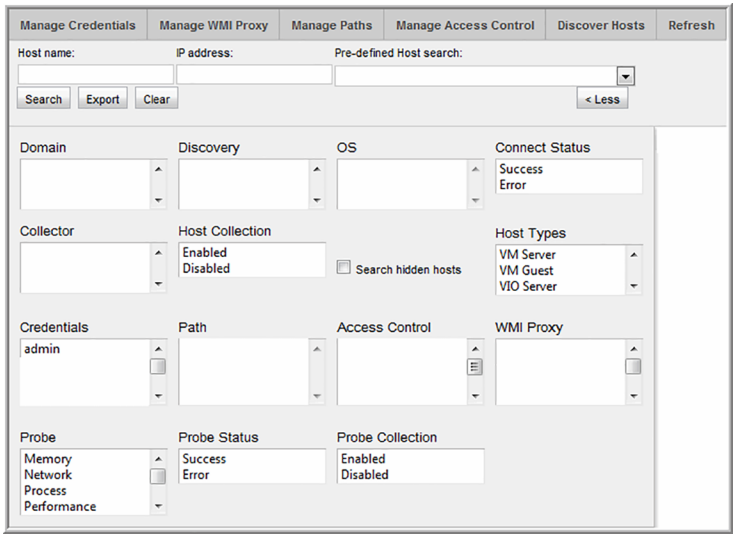
- See “Configure / Search the host Inventory” on page 353.
- See “Configure / Search the host Inventory” on page 353.
- See “Manage credentials” on page 354.
- See “Manage WMI proxy” on page 357.
- See “Manage paths” on page 358.
- See “Manage access control” on page 360.

Configure / Search the host Inventory

Before Host Discovery: Use the Host Inventory window to set up configurations--credentials, WMI proxy, paths, and access control--as described in the following sections.

After Host Discovery: Use the Host Inventory window to help you find hosts in your inventory and configure probes. Also, export the list of hosts to a comma-separated-values (.csv) file.

See “Host Inventory search and host Inventory export” on page 373.



Note: A search with no specified criteria returns all hosts in your inventory.

Manage credentials

Multiple credential sets can be created, typically for groups of hosts with common credentials and/or hosts grouped by operating system (Linux/Windows). These credential sets are then selected and applied to specific Host Discovery policies. In fact, multiple credential sets can be listed, allowing the Data Collector to attempt authentication in a specific order until it is successful.

At the very least, you should have one credential set for Linux hosts and another for Windows hosts. Each defined set of credentials will have a name, to enable relevant selection when configuring Host Discovery policies.

For additional prerequisite details:

See “Host access requirements” on page 347.

See “Host Inventory configuration steps” on page 349.

To Manage Host Credentials, select:

Admin > Data Collection > Host Inventory

1. In the Host Inventory toolbar at the top of the browser window, click **Manage Credentials**.
2. Add, Edit, or Delete credentials using the buttons at the bottom of the window.

Example of credentials for Windows hosts

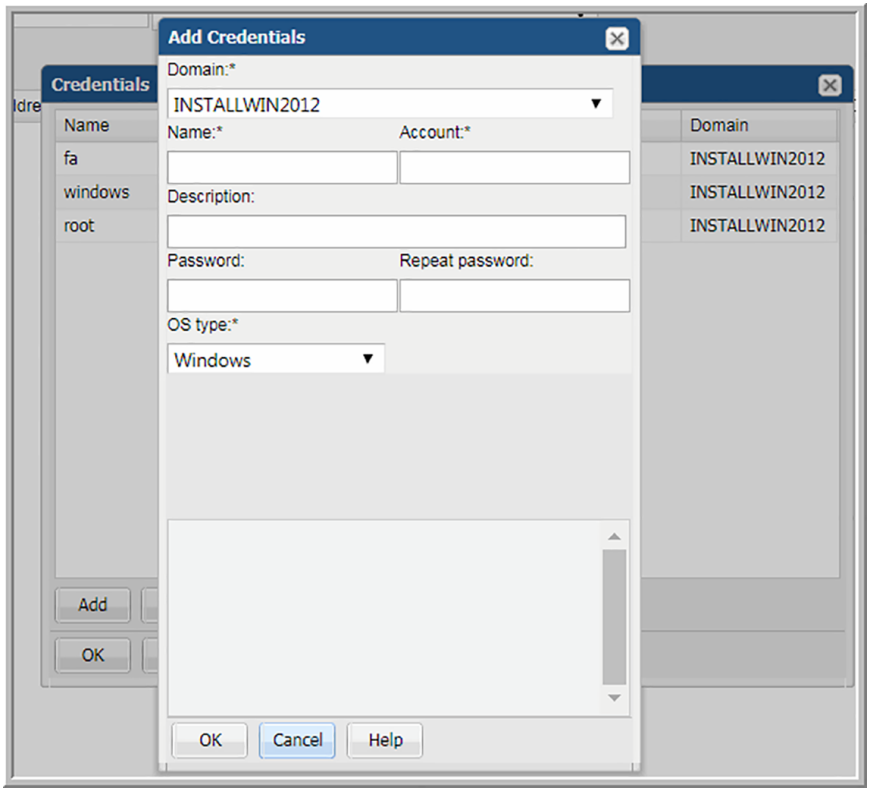


Table 36-2 Windows credentials field descriptions.

Field	Description	Sample Values
Domain*	Select the NetBackup IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).	
Name*	Assign a name to identify this set of credentials that you are defining.	

Table 36-2 Windows credentials field descriptions. *(continued)*

Field	Description	Sample Values
Account*	Enter the login account name used to log in to the hosts. If the policy includes a group of Windows hosts, use the Windows domain user id. This user id must have administrative privileges. For Linux hosts, super user root privileges are required. You also could use an access control command, such as **sudo, sesudo**, or **pbrun**. If using any of these access commands, ensure that the user ID has sudo, sesudo, or pbrun privileges. Some enterprises prefer to create a new user and provide access to commands via an access control command. See "Manage access control" on page 360. and See "Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements" on page 344.	**root**
Description	Enter a note to help identify this type of credential	**Linux logins for Corporate**
Password	Enter the password for the account	**Password1**
OS type*	Select either Linux, Windows, or NAS.	
Windows Domain	For Windows hosts only: If any of the hosts specified in the Host address field are Windows hosts, you need to specify the Windows domain name. If the host is not a member of a domain, or to specify a local user account, use a period (.) to substitute the local host SSID for the domain.	**win2kdomain**
Private Key File	For Linux hosts only: If you have configured Public Key/Private Key between your Data Collector Server and the Hosts you intend to monitor, use this field to specify the location of the Private Key file on the Data Collector Server.	**/root/.ssh/id_rsa or C:\Program Files\Aptare\mbs\conf\id_rsa**
Known Hosts File	For Linux hosts only: If you have configured Public Key/Private Key between your Data Collector Server and the Hosts you intend to monitor, use this field to specify the location of the Known Hosts file on the Data Collector Server.	**/root/.ssh/known_hosts or C:\Program Files\ Aptare\mbs\conf \known_hosts**

Manage WMI proxy

Note: A WMI Proxy configuration is needed only if you are collecting data from Windows servers in your environment.

Multiple WMI Proxy settings can be created to manage access to Windows hosts.

For additional prerequisite details:

See “Host access requirements” on page 347.

See “Host Inventory configuration steps” on page 349.

To Manage WMI Proxy settings, in the toolbar select:

Admin > Data Collection > Host Inventory

1. In the Host Inventory toolbar at the top of the browser window, click **Manage WMI Proxy**.
2. Add, Edit, or Delete settings using the buttons at the bottom of the window.
3. Click **Add** to configure settings and then click **OK**.

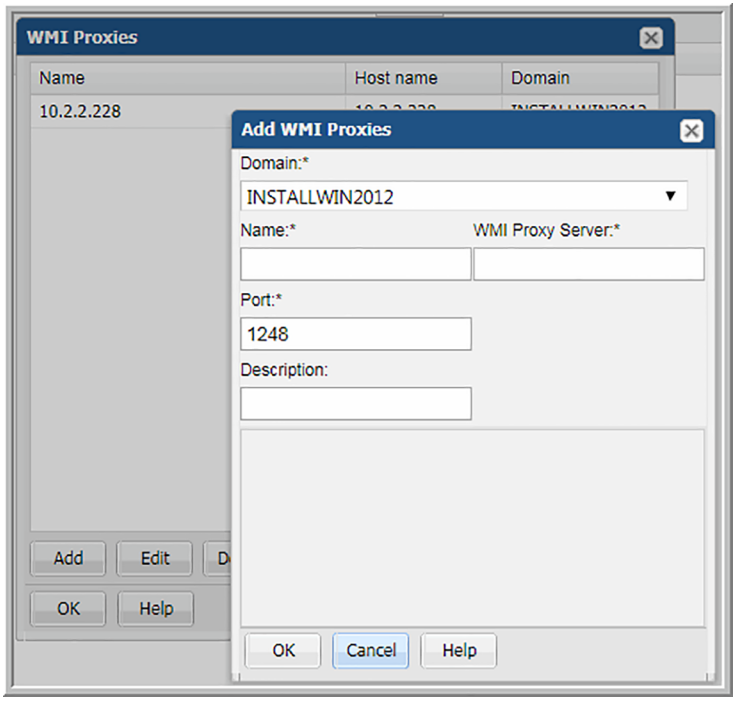


Table 36-3 WMI Proxies field descriptions.

Field	Description	Sample Values
Domain*	Select the NetBackup IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).	
Name*	Assign a name to identify this set of credentials that you are defining.	
WMI Proxy Server*	This is the **server** address of the WMI proxy, which collects data on Windows hosts. Enter either the server's IP address or name.	**CorpWin2k**
Port*	The port that the Data Collector will use to contact the WMI Proxy; usually, there is no need to change the default setting (1248).	**1248**
Description	Enter a note to help identify this WMI Proxy setting	

Manage paths

Multiple path settings can be created to designate specific paths to commands on hosts.The specified path is appended to the existing path and is used to search for commands (for example, /usr/bin:/usr/sbin). Certain commands, such as scli, require an absolute path.

For additional prerequisite details:

See "Host access requirements" on page 347.

See "Host Inventory configuration steps" on page 349.

To Manage Paths select:

Admin > Data Collection > Host Inventory

1. In the Host Inventory toolbar at the top of the browser window, click **Manage Paths**.
2. Add, Edit, or Delete settings using the buttons at the bottom of the window.
3. Click **Add** to configure settings and then click **OK**.

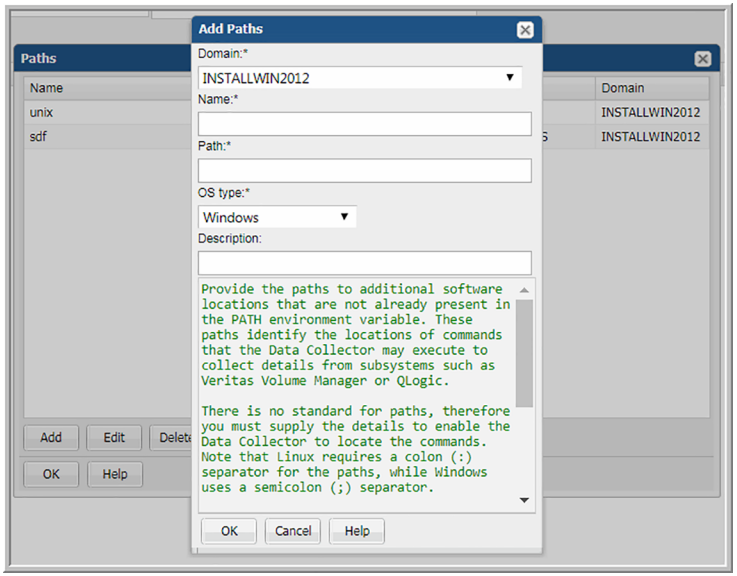


Table 36-4 Paths field descriptions.

Field	Description	Sample Values
Domain*	Select the NetBackup IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).	
Name*	Assign a name to identify this Paths setting that you are defining.	
Path*	Provide the path(s) that you want prefixed to the PATH environment variable. Note that there is no standard for the paths, therefore you must supply the details to enable the Data Collector to connect. If the Data Collector is installed on a Linux server, use the following command to determine the path to Linux servers: `ssh <userId> @<hostServer> env` If the Data Collector is installed on a Windows server, use the following, freely available executable (plink.exe) to determine the path to Linux servers: `plink <userId> @<hostServer> env`	Linux: `/opt/QLogic_Corporation /SANsurferCLI:/usr/local /sbin:/usr/local/bin: /sbin:/bin:/usr/sbin: /usr/bin:/root/bin:/opt /EMLXemlxu/bin:/usr/sbin /hbanyware:/opt/HBAnyware` Windows: `C:\Program Files\Emulex \Util\HBAnyware; C:\Program Files \QLogic\SANSurfer`

Table 36-4 Paths field descriptions. *(continued)*

Field	Description	Sample Values
OS type*	Select either Linux or Windows	
Description	Enter a note to help identify this Path setting	

Manage access control

For Linux hosts, root-level privileges are required. Data Collectors require read-only access to execute non-intrusive commands on hosts. It is strongly recommended that a separate login account used strictly for NetBackup IT Analytics be established and using Active Directory for Windows systems and the sudo command for Linux systems, restrict the commands that NetBackup IT Analytics can issue. To accommodate this security approach, you can optionally specify access control commands like sudo, sesudo, or pbrun.

See "Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements" on page 344.

Multiple Access Control settings can be created to manage access control commands for Linux hosts. For Linux systems, you must specify the path to an access control command such as sudo in order to execute certain OS commands with root-level privileges.

For additional prerequisite details:

See "Host access requirements" on page 347.

See "Host Inventory configuration steps" on page 349.

To Manage Access Control settings, select:

Admin > Data Collection > Host Inventory

1. In the Host Inventory toolbar at the top of the browser window, click **Manage Access Control**.
2. Add, Edit, or Delete settings using the buttons at the bottom of the window.
3. Click **Add** to configure settings and then click **OK**.

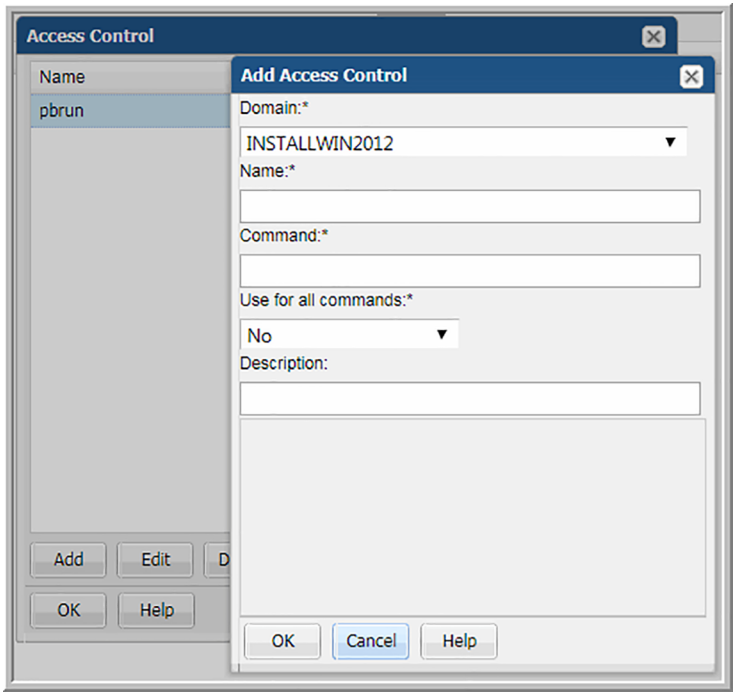


Table 36-5 Access Control field descriptions.

Field	Description	Sample Values
Domain*	Select the NetBackup IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).	
Name*	Assign a name to identify this Access Control setting.	
Command*	Linux hosts only: Provide the full path to the access control command, such as **sudo, sesudo**, or **pbrun**. See "Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements" on page 344. You can configure sudo to prompt for a password using a custom prompt (the default is "Password"). NetBackup IT Analytics expects the prompt to be "Password." If the hosts have a custom password prompt, you'll need to specify **-p Password:** after the path to sudo. See the example to the right.	**/usr/bin/sudo** **/user/local/bin/sudo -p Password:**

Table 36-5 Access Control field descriptions. *(continued)*

Field	Description	Sample Values
Use for all command*	Select Yes to have the Data Collector use the access command for all commands.	
Description	Enter a note to help identify this Access Control setting	

Host Inventory management

Now that you've set up the prerequisites, you'll use the steps described in this section for on-going Host Inventory Management. For additional prerequisite details:

See "Host access requirements" on page 347.

See "Host Inventory configuration steps" on page 349.

Once the prerequisite settings have been configured, a Host Discovery Policy must be created to enable the process of finding hosts in your environment and populating your inventory of hosts.

The Host Inventory Management processes include:

- Configure and validate hosts in the inventory
- Enable and manage on-going collection

Several tools facilitate Host Inventory Management, as described in the following sections:

- See "Configure host Discovery policies to populate the host Inventory" on page 363.
- See "Execute and monitor host Discovery" on page 368.
- See "Validate host connectivity" on page 370.
- See "Host Inventory search and host Inventory export" on page 373.
- See "Export the host Inventory" on page 374.
- See "Configure and edit host probes" on page 375.

Configure host Discovery policies to populate the host Inventory

Host Discovery begins with a Discovery Policy, which identifies the Data Collector that will gather information about hosts in your environment. In addition, a policy has an associated set of credentials, WMI proxies, and paths to access commands on the hosts. For additional prerequisite details,:

- See “Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements” on page 344.
- See “Host access requirements” on page 347.
- See “Host Inventory configuration steps” on page 349.

A Discovery Policy typically is used once to initially populate your host inventory. Executing a discovery policy more than once has no effect for hosts that were previously discovered. To identify and resolve connectivity issues refer to the following:

See “Validate host connectivity” on page 370.

Although all hosts can be included in a single policy, you might want to create one or more Host Discovery Policies in the following recommended groupings:

- by OS (Windows or Linux) - This grouping is essential, as the probes and parameters are OS-specific.
- by common attributes, such as User ID, password, access control commands (sudo, pbrun, sesudo), PATH
- by application, such as Oracle or Exchange

Discovery policy considerations

If your enterprise configures hosts to lock out access after multiple failed authentication attempts, take the following tips into consideration:

- If you choose more than one credential in the Discovery Policy credentials list, you risk host authentication failure lock-out. The discovery process will try the first credentials and if they fail, discovery will try the next credentials that you’ve selected. Therefore, if your hosts are configured to prevent multiple authentication retries, multiple failed attempts may cause a lock-out.
- If multiple Discovery Policies are running simultaneously, with one policy using an IP address to access the host and the other policy using a name to access the host, the multiple access attempts may cause a lock-out. Note that if the authentication attempts are successful, only one host record is added to the inventory.

Configure a Discovery policy

Note: A Discovery Policy typically is used once to initially populate your host inventory. Executing a discovery policy more than once has no effect for the subsequent runs for hosts that have already been discovered and added to the inventory.

For additional information about Host Inventory Discovery and Management,

- See “Before discovering hosts” on page 353.
- See “Execute and monitor host Discovery” on page 368.
- See “Validate host connectivity” on page 370.
- See “Host Inventory search and host Inventory export” on page 373.

To create/edit Host Discovery Policies, select **Admin > Data Collection > Host Inventory**

1. In the Host Inventory toolbar at the top of the browser window, click **Discover Hosts**.
2. Add, Edit, or Delete settings using the buttons at the bottom of the window.
3. Click **Add** to configure settings and then click **OK**.

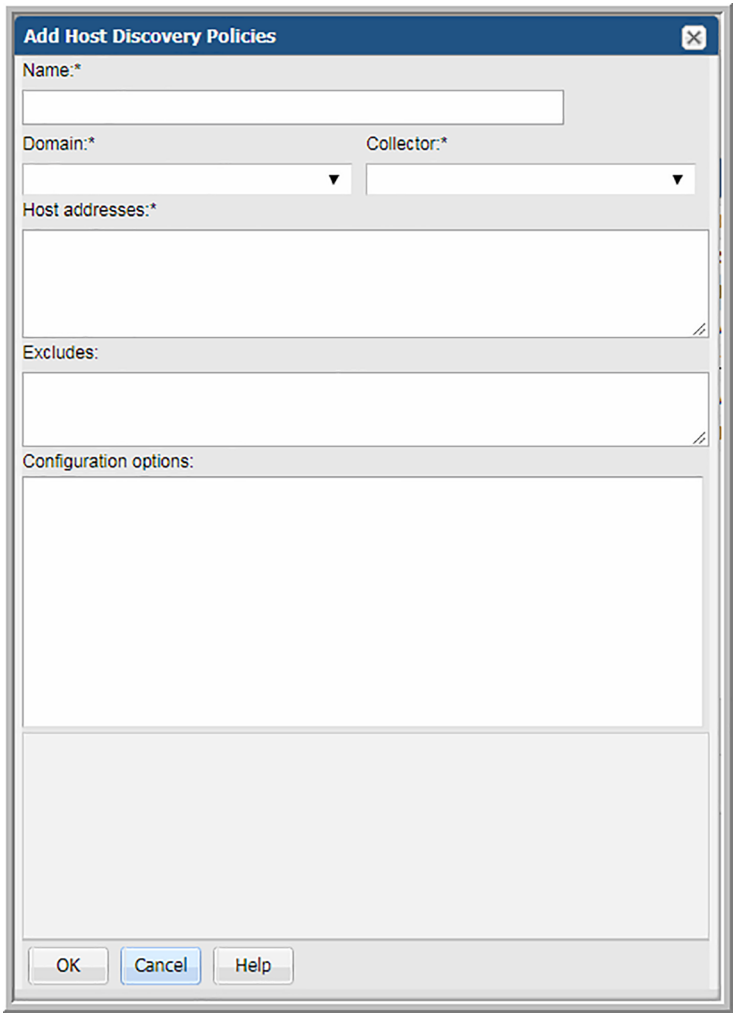


Table 36-6 Host Discovery Policy field descriptions.

Field	Description	Sample Values
Name*	Assign a name to identify this Discovery Policy.	
Collector*	Select the data collector from the drop-down list	
Domain*	Select the NetBackup IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).	

Table 36-6 Host Discovery Policy field descriptions. *(continued)*

Field	Description	Sample Values
Host addresses*	■ A range of IP addresses can be specified ■ Hostnames and/or IP addresses can be listed, separated by commas See "Collecting from Clustered SQL server and Oracle applications" on page 366.	**192.168.0.1-250** **172.168.1.21, ABChost1, ABChost2, 172.168.1.58**
Excludes	List any known IP addresses that you know are not valid for host collection; for example, the IP address of a printer. IP address ranges are also supported.	
Configuration options	This list gets populated when you select a Domain at the top of the Host Discovery Policies window. ■ Credentials ■ WMI Proxies ■ Paths Expand these lists to select the configurations to be used by this Discovery Policy. **Note:** If you choose more than one credential in the list, you risk host authentication failure lock-out. The discovery process will try the first credentials and if they fail, discovery will try the next credentials that you've selected. Therefore, if your hosts are configured to prevent multiple authentication retries, multiple failed attempts may cause a lock-out.	

Collecting from Clustered SQL server and Oracle applications

Collection from clustered SQL Server and Oracle applications requires a specific data collection configuration. Typically, when configuring a Host Discovery Policy, the IP address of the specific host/node should be configured in the policy for direct access to the host's data.

See "Configure a Discovery policy" on page 364.

In a clustered environment, however, the following configurations are required to gather the host data.

- Host collection requires the IP address or host name of the Cluster (not the IP address or host name of the Cluster Node) in the Host Discovery Policy.
  See Figure 36-1 on page 367.
- The Application Probe requires the IP address or host name of the Cluster (not the IP address or host name of the Cluster Node).

See Figure 36-2 on page 367.

Note: If Cluster Nodes already have been discovered, they should be removed from the Host Inventory.

Figure 36-1 Host Discovery Policy Configuration Steps

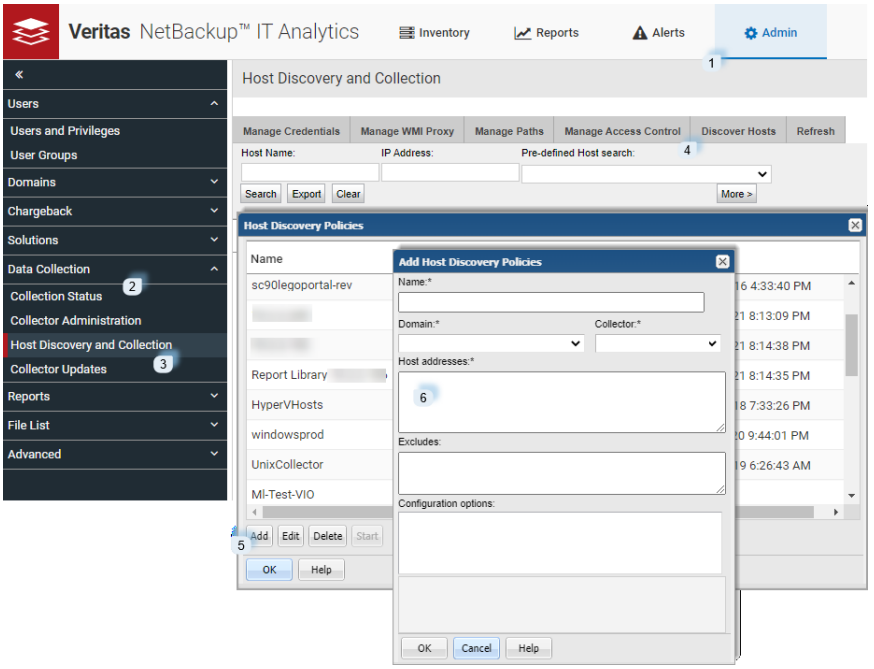
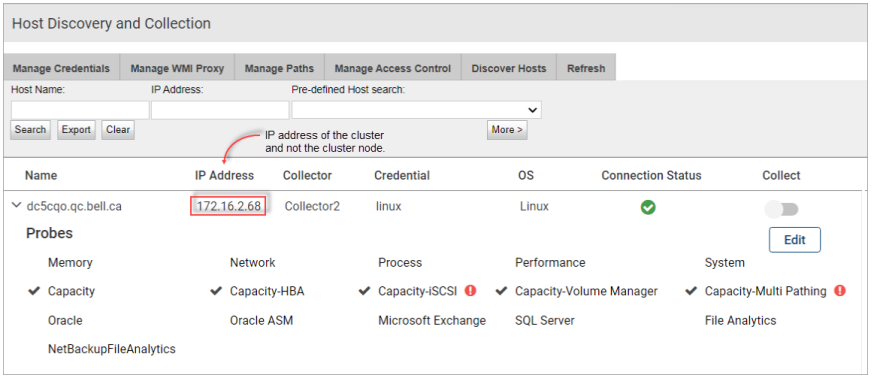
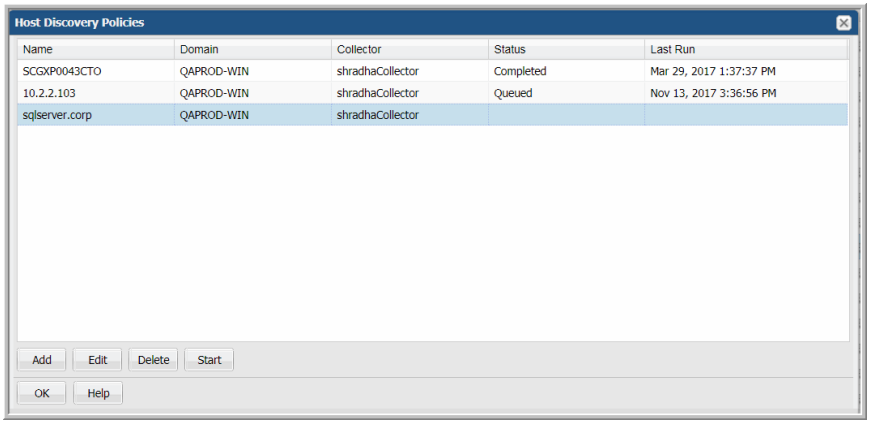


Figure 36-2 Application Probe Example



Execute and monitor host Discovery

Execute a Discovery Policy



1. In the Host Inventory toolbar, click **Discover Hosts** to list the Host Discovery Policies.
2. In the Host Discovery Policies window, select the Discovery Policy.
3. Click **Start**.

   At this point, the discovery process will begin. It may take a few minutes for the background processes to initiate the discovery.
4. Click **OK**.
5. To verify that the discovery process is running, refresh the view you launched in step 1 or go to Monitor Discovery Processes.

   Monitor Discovery processes

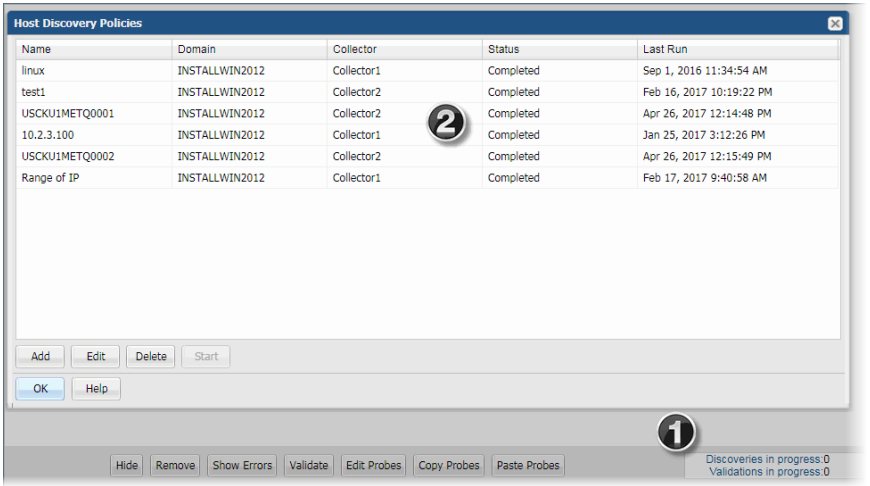
Monitor Discovery processes

Several methods can be used to monitor progress:

Method 1:

1.
2. At the bottom of the Host Inventory window, double-click the **Discoveries in progress** link to launch the Host Discovery Policies window.

   Note the Status at the right of the window.
3. Double-click the Discovery Policy to view the settings.

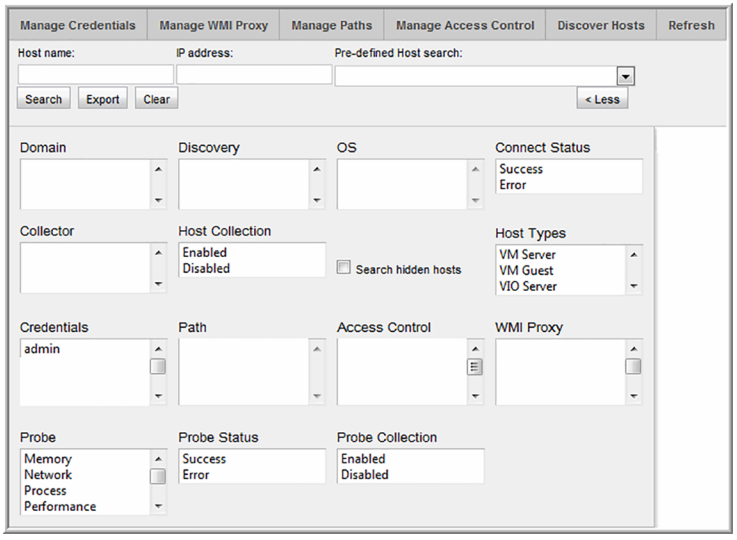


Method 2:

1. Using the Host Inventory

   See “Advanced search parameters” on page 374.

   function, search for hosts associated with a Discovery policy to see what hosts have been found.



Validate host connectivity

The Validate step executes the necessary validation steps and provides a summary of the overall success/failure. The Validation process steps through a handshake process, executing the preliminary steps that will occur during data collection. The informative messages enable you to pro-actively identify issues prior to initiating the data collection process.

Validate hosts

The Validation process identifies issues such as:

- Credential Validation Failures - Verify account IDs and passwords.
- Probe Errors - For example, an HBA probe may fail on a host that does not have an HBA. Other similar errors include iSCSI port not found or LUN not found.
- Connection Failures - The host may not be reachable.
- DNS Lookup Failures - IP addresses may not have been configured correctly.
- OS Verification Failures - Check the Access Control or WMI Proxy settings. In addition, verify that the paths are valid for the host's operating system.
- Server Command Errors - Verify that the Path and Access Control settings are correct.

Validation automatically occurs when the Data Collection processes are initiated; however, you can manually start the processes to get immediate feedback so that you can troubleshoot issues.

1. In the Host Inventory window, search for hosts. You can search by a Discovery Policy to see the results of a discovery.

   See "Execute and monitor host Discovery" on page 368.

2. Click on one or more hosts and then click **Validate** at the bottom of the window.
3. To verify that the validation has begun, click **Show Validations**at the bottom right of the window.

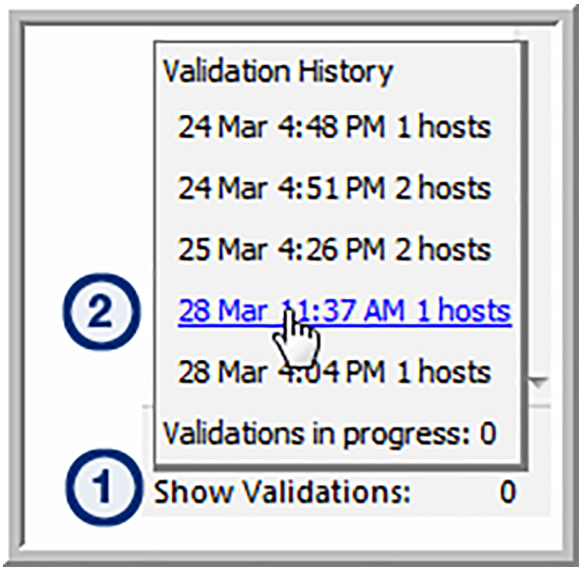
   A list of the hosts that are currently being validated will be displayed.

   See "Validation history" on page 370.

Validation history

Once a set of hosts have been selected for validation the current status, as well as the history, can be viewed in a pop-up box.

1. At the bottom right of the Host Inventory window, click **Show Validations**.



- Validation History: A list of the past 10 validations is displayed. These are hyperlinks that can be used to access the list of hosts associated with that validation process.
- Validations in progress: Click this link to view the status of the current validation process.

2. Click the link to either display validations in progress or the hosts that were included in previous validations.

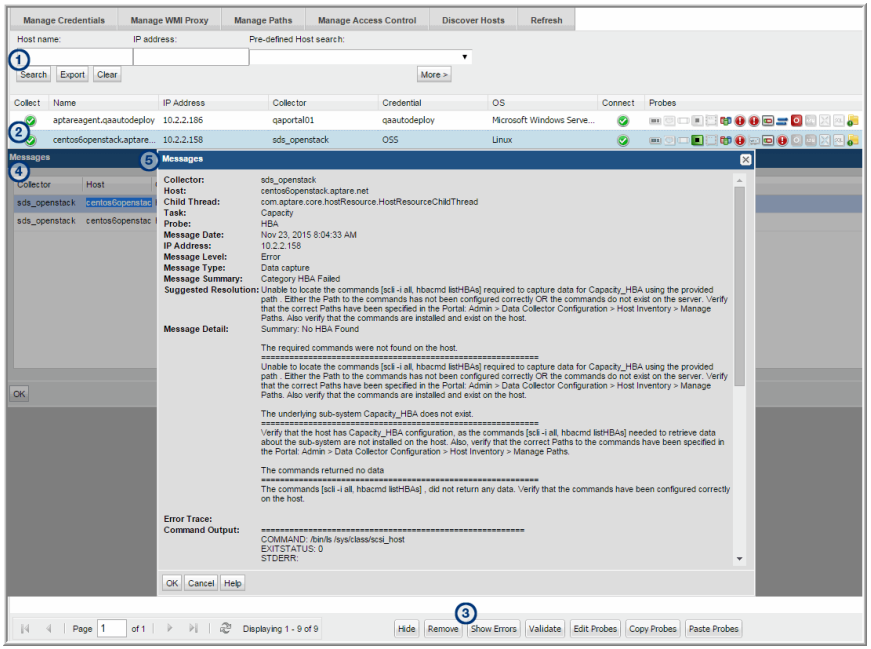
Show errors

Before host data can be successfully collected, a number of configuration steps need to be taken. The **Show Errors** button enables you to identify details to help you troubleshoot host inventory collection issues.

Show Errors lists issues specific to:

- Connectivity
- Probes
- Validation

Use the following example and steps to view troubleshooting messages.



1. Search the Host Inventory to view a list of hosts.
2. Select a host in the list that displays failure icons (in the above example, three probes have exclamation points in red circles).
3. Click **Show Errors**to display the Messages window for the selected host.
4. Double-click a message in the Messages window to view the details.
5. Take the recommended steps provided in the message details to rectify the issue. Then, re-validate the host.

Filter the host Inventory - hide / un-hide, remove

The Host Discovery process populates your inventory with hosts it finds. Often, discovery policies are designed to discover an IP address range. Host Discovery creates a record for every IP address in the range, even if it's not in use. Therefore, invalid IP addresses will appear in your Host Inventory. In addition, Discovery may find printers, routers, or switches, or other devices that aren't relevant for host data collection.

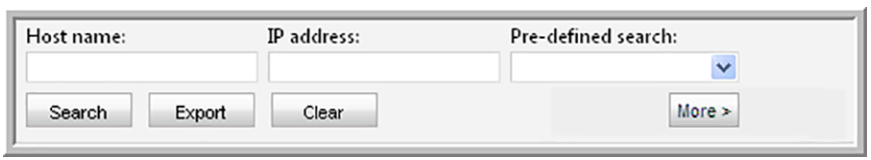
To filter your host inventory to include only hosts for which you want data collected, use the following options:

- Hide - Select a host in the inventory and click **Hide** at the bottom of the window. When you Hide a host, it will not appear in your search results.
- Unhide - If you list hosts that have been hidden, the **Hide** button will be toggled to Unhide. Use the Advanced Search Parameters option, Search hidden hosts, to view a list of hidden hosts.
  See "Advanced search parameters" on page 374.
- Remove - Select a host in the inventory and click **Remove** at the bottom of the window. When you choose to remove a host, if you execute the Discovery Policy again, it will re-add it to the inventory. You may have an IP address that is now associated with a device that is different from the one that was discovered.

Host Inventory search and host Inventory export

The Host Inventory window offers a Search feature to help you find hosts that have been discovered.

Basic search



Note: A search with no specified criteria returns all hosts in your inventory.

Pre-Defined search

Several pre-defined searches enable easy access to host lists that are useful for troubleshooting.

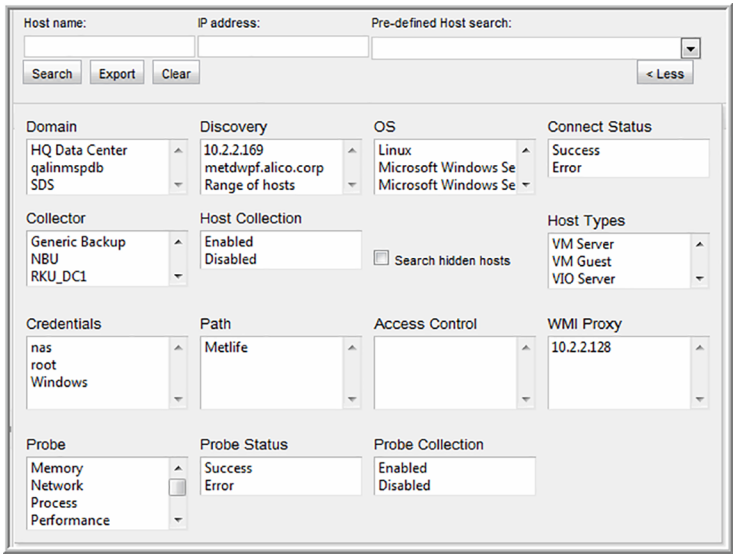
- Active policy but not collected since...

  Note: (When you select this option, a calendar pop-up enables date selection.)

- No active policy but was previously active (This means host data was successfully collected at an earlier time.)
- Credentials failing but were previously successful
- Collections failing but were previously successful

- For more specific search parameters, click **More** (once clicking More, the button displays **Less**) to enter Advanced Search Parameters.
  See "Advanced search parameters" on page 374.

Advanced search parameters



- Select specific search criteria to narrow the list of hosts displayed in the inventory.
- When you check the Search hidden hosts box, only hidden hosts will be displayed in the Host Inventory window. Also, the Hide button in the Host Inventory window will toggle to Unhide.
- When searching on Probes, if a probe was at some point activated, but then de-activated, it will appear in the search results because there is an entry in the database table.

Export the host Inventory

To export the details of the Host Inventory to a comma-separated-values file (.csv):

1. Search the host inventory without supplying any values in the search criteria fields.

   See "Host Inventory search and host Inventory export" on page 373.
2. In the Search area at the top of the Host Inventory list, click **Export**.

The resulting file will include values for the status of each of the available probes. For example, the values will be similar to N/U or Y/S, as described in the following table.

E	Error
F	Failure
N	No - Not Active
S	Success
U	Unknown
W	Warning
Y	Yes - Active Probe

Configure and edit host probes

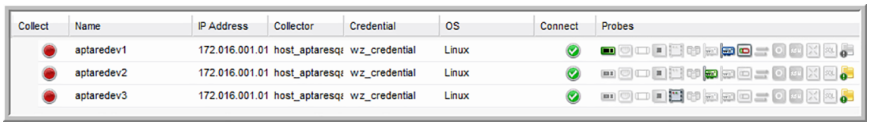
Host Resources Data Collection can gather the following information by probing hosts:

- Host Probes: Capacity (HBA, iSCSI, Volume Manager, Multi-pathing)
- Host Probes: Memory, Network, Process, Processor, System
- Application Probes: Exchange, SQL Server, Oracle, Oracle ASM
- File Analytics Probes

Note: Do not enable HBA probes for VMware guest host collection.

To configure probes for a host

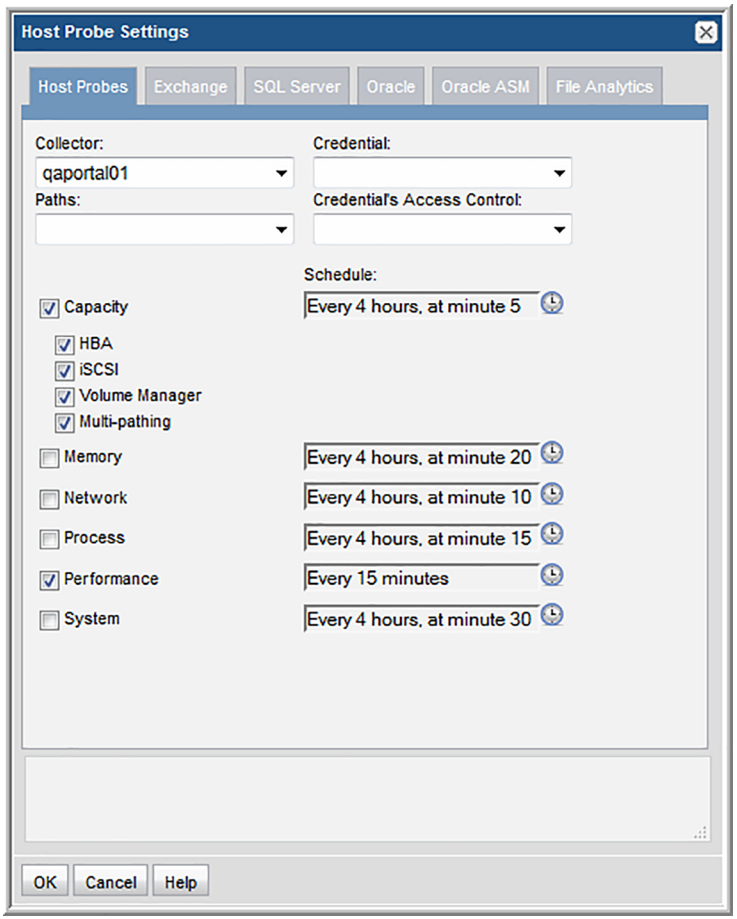
1 Search for hosts in your inventory. A search with no specified criteria returns all hosts in your inventory.



2 Mouse over each of the Probe icons at the right of the Host Inventory list to view the probe type.

3 Double-click a host in the inventory or select a host and click **Edit Probes** to configure/view the Host Probe Settings window.

See "Probe settings" on page 379.



Probe settings must be configured to ensure successful communication with the hosts. In addition, the frequency of each probe can be customized.

4. Click each tab to updated the configuration settings for the specific probes.
5. For the SQL Server and Oracle probes, you can create multiple instances, using the following steps:

   Click **Add**.

   Enter the mandatory configuration.

   See "Probe settings" on page 379.

   Click **OK**.

Host Inventory File Analytics probe

Using Host Resources data collection, hosts are discovered and added to the Host Inventory. Once a host is listed in the inventory, it can be selected and the File Analytics probe can be configured. To access the Host Inventory to enable File Analytics probes: **Admin > Data Collection > Host Inventory**

Note that by design, File Analytics host resources data collection occurs via activation of the probe in the Host Inventory window in the Portal. Collection does not occur under the following circumstance:

- The **Validate** option in the Portal's Host Inventory window only runs a connectivity check. It does not collect File Analytics data.

File Analytics Probe configurations by operating system

Windows servers: A Data Collector must be running on a Windows 2008 server. A Domain Administrator ID is required when collecting file-level data for File Analytics.

Linux servers: Only Linux is supported (Solaris, Linux, and AIX, but not HP-UX), with the following requirements:

- Root user access is supported.
- Non-root user access with sudo access control is supported.
- Non-root user access without sudo is not supported.
- Running collection with a sudo user on a Linux server requires the addition of a an access control command for the server in the Host Inventory's Manage Access Control window:
  Admin > Data Collection > Host Inventory
  Also, an advanced parameter must be created: FA_USE_SUDO set to Y.
  To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Both Windows and Linux servers

If running collection via the checkinstall utility, verify the following:

- An advanced parameter must be created: FA_HOST_VALIDATE set to Y. To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Best practices for Host Inventory File Analytics probes

- File Analytics should be configured to run daily for all hosts/servers.
- Since most environments have hundreds, even thousands of hosts, it is recommended that File Analytics probes be configured in a staggered schedule so as not to overload the Data Collector server.

Propagate Probe Settings: Copy Probes, Paste Probes

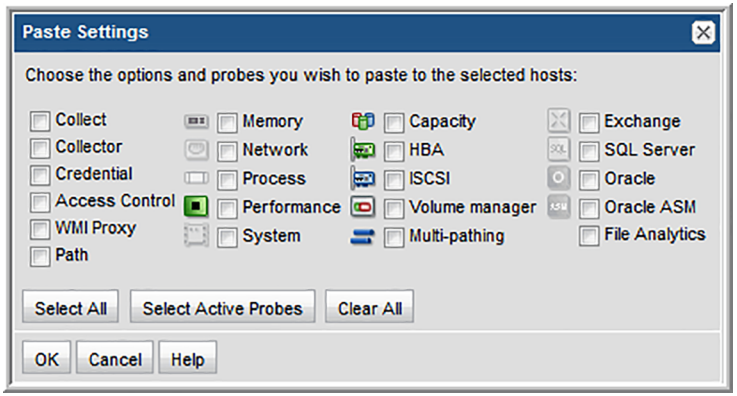
Whenever you have hosts with common attributes, you can save time by configuring probe settings for one host and then copying and pasting those settings to other hosts.

A key advantage to using the probe copy/paste feature is the ability to propagate the probe schedules to multiple hosts. In addition, you can explicitly select the probes you want to activate.

Note: You only can copy/paste probes that are within the same Domain. This mainly impacts Managed Services Providers with multi-domain environments. Use the Advanced Search function to list probes within a specific Domain.

Example of probe copy / paste

1. Search for all Linux hosts.
2. Configure the probes for one of the hosts in your Linux list and click **Copy Probes**.
3. Finally, select the remaining Linux hosts and click **Paste Probes**.



- The icons of configured Probes will be highlighted in the Paste Probes window; however, you must explicitly check those probes to copy the probe schedules and to activate the probes. Use the **Select Active Probes** button to select active probes.
- By default, the probe checkboxes will be unchecked, enabling you to explicitly select the probes that you want to paste. Or, click **Select All** to turn on all the probes for the selected host.

Probe settings

Table 36-7 Probe Settings

Probe Type	Parameters	Description
Capacity HBA iSCSI Volume Manager Multi-pathing **Note:** Do not enable HBA probes for VMware guest host collection.	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”

Table 36-7 Probe Settings *(continued)*

Probe Type	Parameters	Description
Memory	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
Network	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
Process	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
Processor	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
System	Probe schedule*	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
Exchange	Collect	Check this box to activate collection on an on-going basis. When it is unchecked, only initial validation will attempt this probe.

Table 36-7 Probe Settings *(continued)*

Probe Type	Parameters	Description
	Probe schedule	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
	Active Directory Host	Host name or address
	Active Directory Port	For example: 389
	Active Directory Base DN*	The starting point for the Active Directory. For example: CN=Services,CN=Configuration, DC=contoso2003,DC=com Several tools are available to help you identify the Base DN: **Ldp.exe** - http://support.microsoft.com /kb/224543 **adsiedit.msc** - http://technet.microsoft.com /en-us/library/cc773354(WS.10).aspx
	Active Directory User Name	Active Directory User Name This username must have privileges to search under the base DN within the Active Directory. Typically, this is an Administrator.
	Password	Active Directory Password
SQL Server	Collect	Check this box to activate collection on an on-going basis. When it is unchecked, only initial validation will attempt this probe.

Table 36-7 Probe Settings *(continued)*

Probe Type	Parameters	Description
	Probe schedule	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”
	Database*	The name of the database within the SQL server.
	Instance	The system identifier to identify the SQL server database instance--for example: BKUPEXEC. Specify either an instance name or a port. If an instance name is not specified, MSSQLSERVER is substituted.
	Port	To identify the SQL server instance, provide either an instance name or a database port number; for example: 1433. If a port number is not specified, the port is determined automatically from the instance name.
	Account*	Database access user name The data collector requires a user account with permissions to execute the stored procedures
	Password*	Database access password
	Windows Authentication	Check this box if you want Windows authentication rather than SQL server authentication.
Oracle	Collect	Check this box to activate collection on an on-going basis. When it is unchecked, only initial validation will attempt this probe.

Table 36-7 Probe Settings *(continued)*

Probe Type	Parameters	Description
	Probe schedule	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 20 minutes between the hours of 9 a.m. and 6 p.m.”
	SID*	The system identifier to identify the database instance.
	Port*	Database port number; default: 1521
	Username*	The Oracle user must have the following role granted: SELECT_CATALOG_ROLE To grant this access, use: GRANT SELECT_CATALOG_ROLE TO ‘user’ where user is the database Username that you’ll provide here.
	Password*	Database access password
Oracle ASM	Collect	Check this box to activate collection on an on-going basis. When it is unchecked, only initial validation will attempt this probe.
	Probe schedule	A schedule in cron format; for example: */20 9-18 * * * which translates to “every 20 minutes between the hours of 9 a.m. and 6 p.m.”
	Account*	The Oracle user privileges required: SYSDBA privilege if 10g sysasm in 11g
	Password*	Database access password

Table 36-7 Probe Settings *(continued)*

Probe Type	Parameters	Description
	Port*	Database port number; default: 1521
	ASM Instance*	The name that identifies the database instance.
File Analytics	Collect	Check this box to activate collection on an on-going basis. When it is unchecked, only initial validation will attempt this probe.
	Probe schedule	Default is once a month. A schedule in cron format; for example: */20 9-18 * * * which translates to “every 20 minutes between the hours of 9 a.m. and 6 p.m.”

Chapter 37

Configuration for HP 3PAR

This chapter includes the following topics:

- Pre-Installation setup for HP 3PAR
- Prerequisites for adding Data Collectors (HP 3PAR)
- Installation Overview (HP 3PAR)
- Adding an HP 3PAR Data Collector Policy
- Adding an HP command view advanced Data Collector policy

Pre-Installation setup for HP 3PAR

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (HP 3PAR)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation Overview (HP 3PAR)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the HP 3PAR data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an HP 3PAR Data Collector Policy

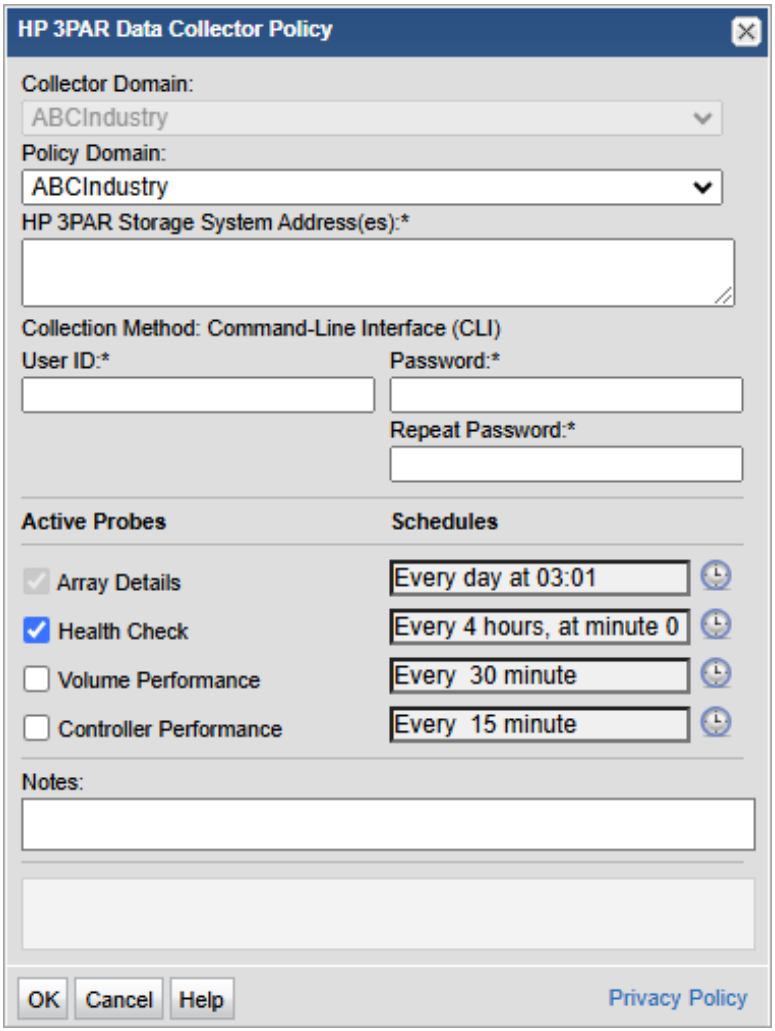
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
HP 3PAR Storage System Address(es)*	Enter a comma-separated list of IP addresses or host names of the HP 3PAR Storage Systems from which you want to collect data.

Field	Description
Collection Method	The Command Line Interface (CLI) is the only available method for HP 3PAR data collection. This method logs in to the HP 3PAR Storage System via SSH and uses the command line for data collection.
User ID*	Specify the User ID for the HP 3PAR Storage Systems. The User ID and Password must be the same for all systems identified in the Host Address field. The HP 3PAR user account should have been created with Browse rights.
Password*	Enter the password associated with the User ID. **Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.
Array Details	Select the check box to activate the array details collection. Click the clock icon to create a schedule frequency. You schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Health Check	This probe collects physical disk, event log, space and replication information. Note that to perform the collection of the array health check data, at least one Array Details collection from this array must be complete. Default scheduled: Every 4 hours.
Volume Performance	This probe collects performance metrics for Virtual Volumes and VLUNs. Note that at least one Array Details collection from this array must be performed before this data can be collected.
Controller Performance	The probe collects performance metrics for Controllers, Nodes, and Ports. Note that at least one Array Details collection from this array must be performed before this data can be collected.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Click **OK** to save the Policy and return to the Collection Administration window where the Policy will be listed under the Data Collector. From here you can add an additional Policy record (for example, if the data collector needs to communicate with other servers), or make changes to the Policy you just created.

Adding an HP command view advanced Data Collector policy

For HP Command View Advanced Edition, HP XP arrays are treated as Hitachi Block Storage. To add a policy to collect from HP StorageWorks XP arrays (HP Command View Advanced Edition), refer to the following.

See “Adding a Hitachi Block Storage Data Collector policy” on page 308.

Chapter 38

Configuration for HP EVA

This chapter includes the following topics:

- Pre-Installation setup for HP EVA
- Prerequisites for adding Data Collectors (HP EVA)
- Installation overview (HP EVA)
- Adding an HP EVA Data Collector policy

Pre-Installation setup for HP EVA

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (HP EVA)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same

server, verify that the Portal and Data Collector software do not reside in the same directory.

- Install only one Data Collector on a server (or OS instance).
- Note the port used by the HP EVA Data Collector: TCP 2372.
- Gather the following required configuration details:
  - HP EVA Management Server: IP addresses or host name.
  - SSSU Home: Location of the SSSU (Storage System Scripting Utility) command-line utility on the Data Collector.
  - Array User ID & Password: Credentials for a view-only user for the HP EVA Management System.

Installation overview (HP EVA)

Use the following list to ensure that you complete each step in the order indicated.

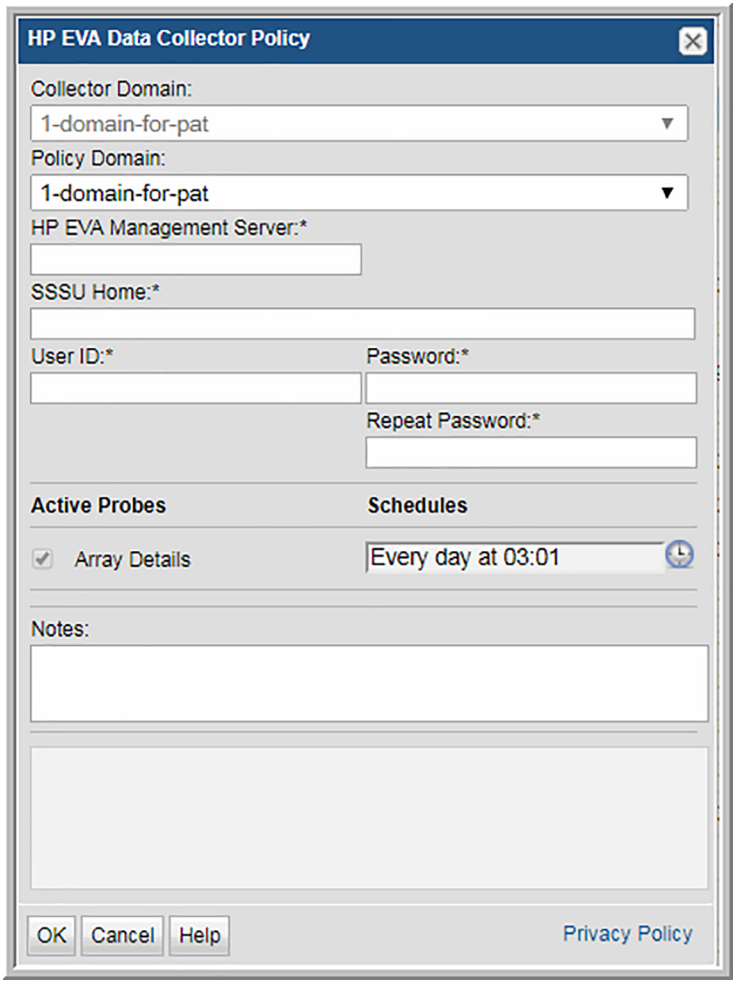
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the HP EVA data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an HP EVA Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
HP EVA Management Server*	The address of the HP EVA Management Server--**either a single IP address or server name**	eva_server1
SSSU Home*	The location of the SSSU (Storage System Scripting Utility) command-line utility. For example: `C:\\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks`	
User ID*	Use the User ID and passcode for accessing the HP-EVA Management Server. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user.	`Administrator`
Password*	The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Array Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

6 Click **OK** to save the policy.

7 On the Data Collector server, install/update the Data Collector software.

Chapter 39

Configuration for HPE Nimble Storage

This chapter includes the following topics:

- Pre-Installation setup for HPE Nimble Storage
- Prerequisites for adding Data Collectors (HPE Nimble Storage)
- Installation overview (HPE Nimble Storage)
- Adding an HPE Nimble Storage Data Collector policy

Pre-Installation setup for HPE Nimble Storage

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (HPE Nimble Storage)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Note the port used by the HPE Nimble Storage Data Collector: TCP 5392.
- Gather the following required configuration details:
  - HPE Nimble Storage Management Server: IP addresses or host name.
  - SSSU Home: Location of the SSSU (Storage System Scripting Utility) command-line utility on the Data Collector.
  - Array User ID & Password: Credentials for a view-only user for the HPE Nimble Storage Management System.

Installation overview (HPE Nimble Storage)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the portal, add a Data Collector, if one has not already been created.
3. In the portal, add the HPE Nimble Storage data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

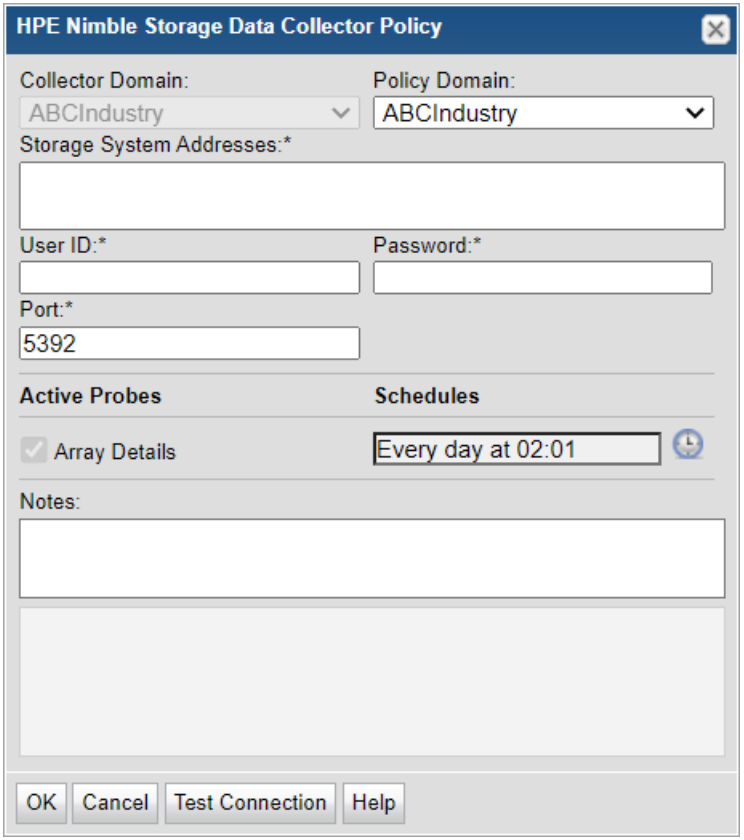
Adding an HPE Nimble Storage Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Storage System Addresses	One or more HPE Nimble Storage system host names, or IP addresses to probe. Comma separated values are supported.
User ID	Use the User ID and passcode for accessing the Nimble Storage Management Server. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user.
Password*	Password for the HPE Nimble Storage system. The password associated with the User ID.
Port	Default communication port number.

Field	Description
Array Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin** > **Data Collection** > **Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See “Working with on-demand Data Collection” on page 624.

6 Click **OK** to save the policy.

7 On the Data Collector server, install/update the Data Collector software.

Chapter 40

Configuration for HPE StoreOnce

This chapter includes the following topics:

- Pre-Installation setup for HPE StoreOnce
- Prerequisites for adding Data Collectors (HPE StoreOnce)
- Installation overview
- Adding a HPE StoreOnce policy

Pre-Installation setup for HPE StoreOnce

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (HPE StoreOnce)

- A 64-bit OS. See the *NetBackup IT Analytics Certified Configurations Guide* for the supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.
  Example:

```
172.16.2.2 aptareportal.<yourdomain>.com
172.16.2.3 aptareagent.<yourdomain>.com
```

Installation overview

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the HPE StoreOnce data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. See Installing the WMI Proxy Service (Windows Host Resources only).
7. Validate the Data Collector installation.

Adding a HPE StoreOnce policy

Before adding the policy

A Data Collector must exist in the Portal, to which you will add Data Collector Policies. For specific prerequisites and supported configurations for a specific vendor, see the *NetBackup IT AnalyticsCertified Configurations Guide*.

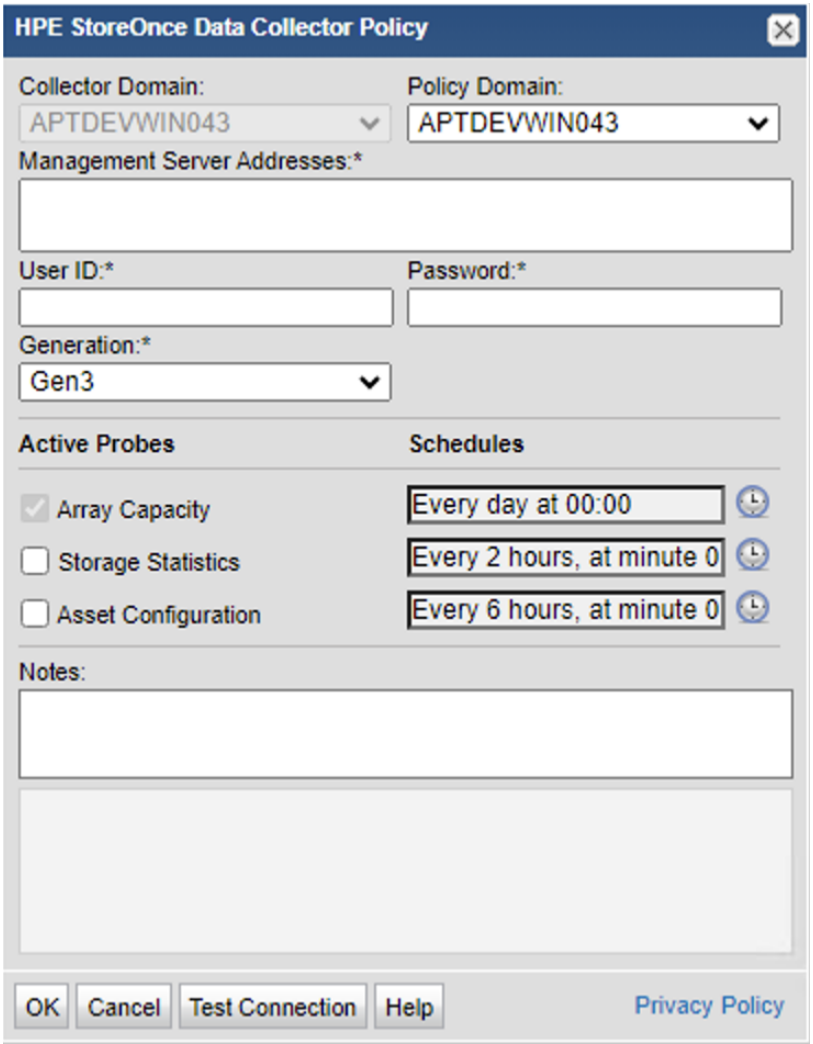
After adding the policy

For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported. On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same way as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the **HPE StoreOnce** policy from the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses*	Hostname or IP Address for the Hitachi Ops Center Configuration Manager REST API Server.
User ID*	Specify the username with Storage Administrator (View Only) role.
Password*	The password associated with the User ID.
Generation*	Select the required Generation. The available options are: ■ Gen3: It supports data collection from 6600,6500, B6200, and VSA. ■ Gen4: It supports data collection from 56xx, 52xx, and 36xx.
Array Capacity	This probe is enabled by default to collect array capacity data from your HPE StoreOnce storage environment. By default, it is collected at 00:00 daily.
Storage Statistics	Collects storage utilization specific to the entire HPE StoreOnce storage, irrespective of its nodes. Collection is performed via REST APIs exposed by the HPE StoreOnce storage.
Asset Configuration	Collects the status of each data service and high level data from data services, such as catalyst stores and VTL. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. By default, the probe is scheduled to run every 6 hours.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Click **OK** to save the Policy.

Chapter 41

Configuration for IBM Enterprise

This chapter includes the following topics:

- Pre-Installation setup for IBM Enterprise
- Prerequisites for adding Data Collectors (IBM Enterprise)
- Installation overview (IBM Enterprise)
- Adding an IBM Enterprise Data Collector policy

Pre-Installation setup for IBM Enterprise

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (IBM Enterprise)

NetBackup IT Analytics supports the following IBM Enterprise storage arrays, running DSCLI 5.2.2.272 & above: DS6000 and DS8000.

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Ports used: TCP 1751, 1750, 1718
- The IBM Enterprise Data Collector Policy is restricted to one array per policy.
- DSCLI must be installed on the Data Collector server.
- Gather the following required configuration details:
  - Array Addresses: IP addresses or name of the IBM DS Storage Frame.
  - Profile Name: The dscli.profile file name with its absolute path.
  - DSCLI Client Software Location: Location of the DSCLI executable on the Data Collector server.
  - User ID & Password: Credentials with monitor group privileges on the storage array.
- Edit the DSCLI profile file (dscli.profile) and set the output format to XML. Locate the profile file, typically in the **/profile** sub-directory and named **dscli.profile**. In this file, un-comment the Output Format property and set it to XML, as shown in the following example.

```
# Output format type for ls commands, which can take one of the
following values:
#   default: Default output
#   xml    : XML format
#   delim  : delimit columns using a character specified by "delim"
#   stanza  : Horizontal table format
# "format" is equivalent to option "-fmt default|xml|delim|stanza".
format: xml
```

Installation overview (IBM Enterprise)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the IBM Enterprise data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector Installation.

Adding an IBM Enterprise Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

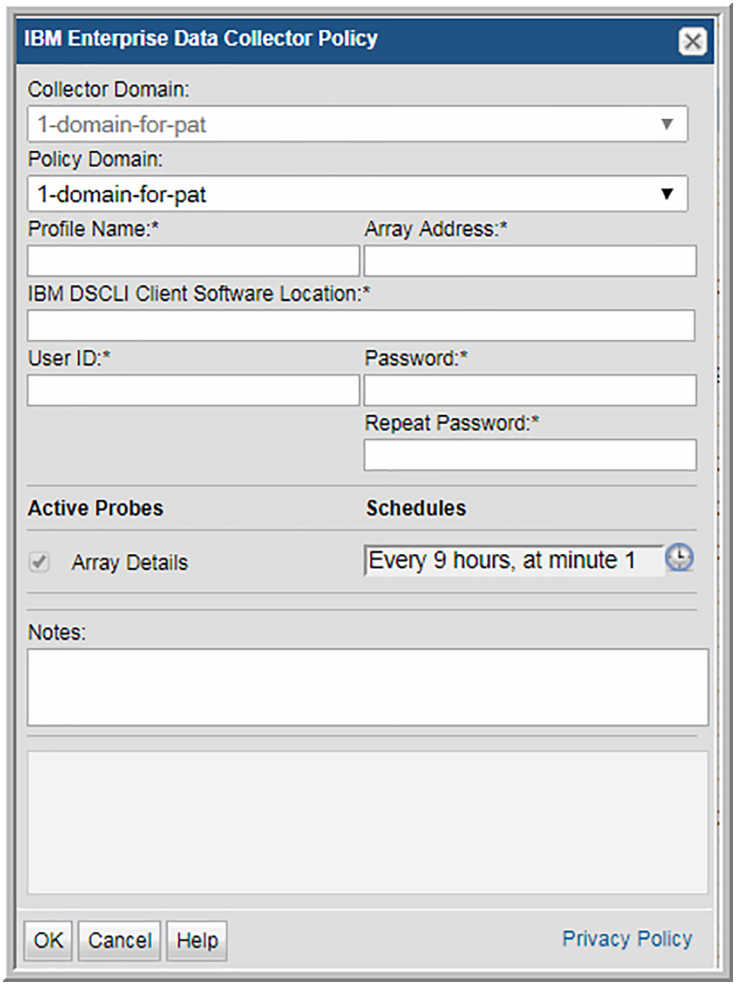
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Profile Name*	Specify the profile filename, including the absolute path. e.g. Windows: `C:\Program Files\ibm\dscli\profile\dscli.profile` Linux: `/opt/ibm/dscli/profile/dscli.profile`	
Array Address*	Enter host name or IP address of the Storage Array from which you want to collect data.	
IBM DSCLI client software location *	The location of the DSCLI executable on the Data Collector server, for example: Linux: `/opt/ibm/dscli` Windows: `C:\Program Files\IBM\dscli`	
User ID*	Specifies the user ID for the account that has monitor group privileges on the storage array.	`Monitor`
Password*	The password is encrypted prior to saving in the NetBackup IT Analytics database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Array Details	Check the box to collect array details. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Chapter 42

Configuration for IBM COS

This chapter includes the following topics:

- Introduction
- Prerequisites for adding data collectors (IBM COS)
- Installation overview (IBM COS)
- Add IBM COS Data Collector policy

Introduction

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (IBM COS)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same

server, verify that the Portal and Data Collector software do not reside in the same directory.

- Install only one Data Collector on a server (or OS instance).
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.
  Example:
  172.16.2.2 aptareportal.<yourdomain>.com
  172.16.2.3 aptareagent.<yourdomain>.com
  Gather the following required configuration details:
  Hostname for the IBM COS Manager device
  User ID & Password to login to IBM COS Manager.

Installation overview (IBM COS)

Use the following list to ensure that you complete each step in the order indicated.

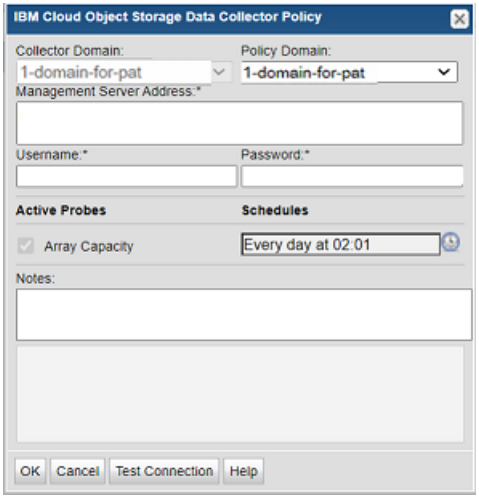
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the IBM Cloud Object Storage data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. See Installing the WMI Proxy Service (Windows Host Resources only).
7. Validate the Data Collector Installation.

Add IBM COS Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5. Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*).

   See See Table 42-1 on page 418.
6. Click **OK** to save the policy.

Table 42-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 42-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Management Server Address*	Hostname for the IBM COS Manager device
Username*	Specify the Username with Super User role
Password*	The password associated with the Username
Array Capacity	This probe is enabled by default to collect array capacity data from your IBM Cloud Object Storage environment. By default, it is collected at 02:01 daily.

Table 42-1 Policy Parameters *(continued)*

Field	Description
Schedules	Click the clock icon to create a schedule. By default, it is collected at 2:01 daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 43

Configuration for IBM SVC

This chapter includes the following topics:

- Pre-Installation setup for IBM SVC
- Prerequisites for adding Data Collectors (IBM SVC)
- Installation overview (IBM SVC)
- Adding an IBM SVC Data Collector policy

Pre-Installation setup for IBM SVC

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (IBM SVC)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).

- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Ports: TCP 5988, 5989, SSH 22
- SSPC (System Storage Productivity Center) with the CIMOM agent is required.
- Gather the following required configuration details:
  - IBM SVC Master Console Server: IP addresses or name of the server. For embedded CIMOM, this is the node's IP address and a separated Data Collector policy must be created for each node.
  - User ID & Password: Credentials to access the IBM SVC Master Console Server: Super User ID and password for CIMOM. The same user is used to execute CLI commands via ssh.

Installation overview (IBM SVC)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the IBM SVC data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an IBM SVC Data Collector policy

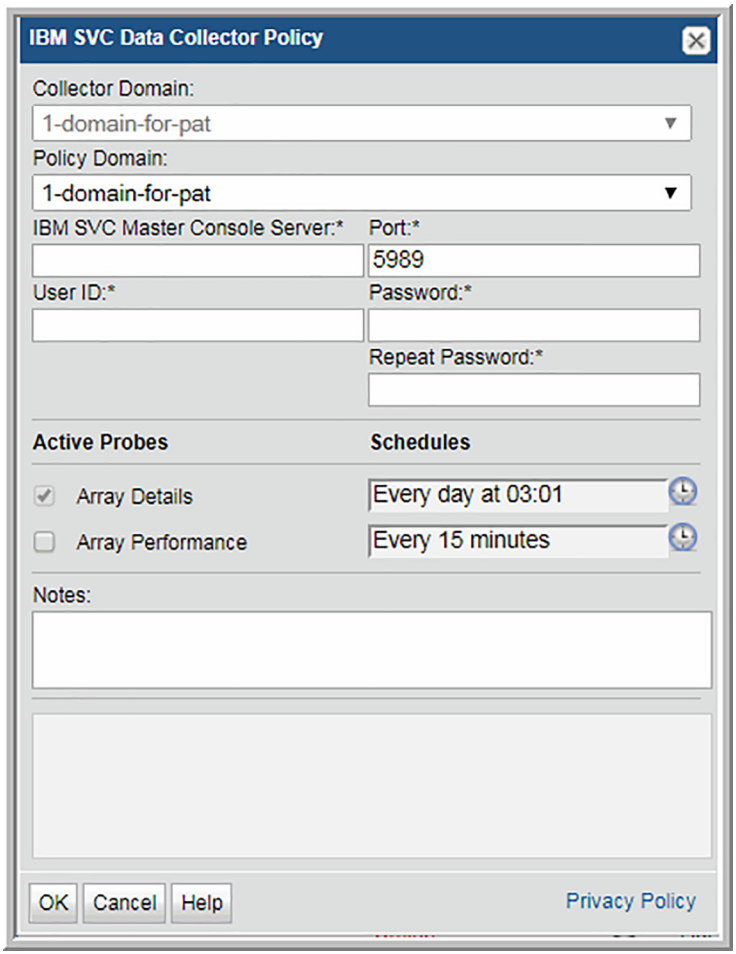
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Specify Data Collector Properties.

Note: SSPC (System Storage Productivity Center) with the CIMOM agent is required. For embedded CIMOM (versions 5.1 and 6.1), create a separate Data Collector policy for each node, where you'll enter the node's IP address in the IBM SVC Master Console Server field. A known issue in version 5.1.08 causes vdisk data to be excluded from collection.



6 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
IBM SVC Master Console Server*	The address of the IBM SVC Master Console Server--either the IP address or server name. For embedded CIMOM, enter the node's IP address (create a Data Collector policy for each node).	eva_server1
Port*	The port of the IBM SVC Server. The default SVC port is 5989.	5989
User ID*	Enter the User ID for the IBM SVC Master Console Server. This is the Super User ID and password for CIMOM. The same user is used to execute CLI commands via ssh.	`Administrator`
Password*	This is the Super User ID and password for CIMOM. **Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Array Details	Click the check box to activate the collection of array details. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Array Performance	Click the checkbox to activate performance collection. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Also, statistics collection must be enabled via the IBM SVC user interface: **Manage Clusters > Start Statistics Collection** Click the clock icon to create a schedule.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

7 Click **OK** to save the policy.

8 On the Data Collector server, install/update the Data Collector software.

Chapter 44

Configuration for IBM XIV

This chapter includes the following topics:

- Pre-Installation Setup for IBM XIV
- Prerequisites for adding Data Collectors (IBM XIV)
- Installation overview (IBM XIV)
- Adding an IBM XIV Data Collector policy

Pre-Installation Setup for IBM XIV

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (IBM XIV)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same

server, verify that the Portal and Data Collector software do not reside in the same directory.

- Install only one Data Collector on a server (or OS instance).
- XCLI must be installed on the Data Collector server.
- On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.
  Example:
  - 172.16.2.2 aptareportal.<yourdomain>.com
  - 172.16.2.3 aptareagent.<yourdomain>.com

Installation overview (IBM XIV)

Use the following list to ensure that you complete each step in the order indicated.

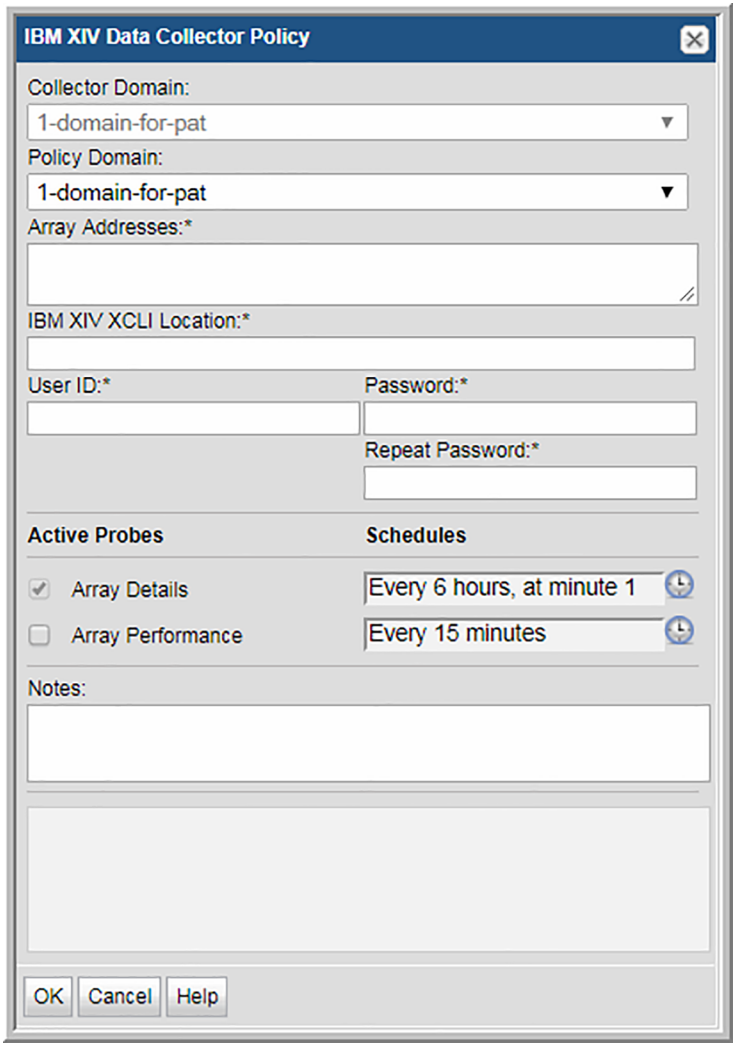
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the IBM XIV data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding an IBM XIV Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.
5. Specify Data Collector Properties.



Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings. Alternatively, you can find the domain name from **Admin** > **Domains** > **Domains**.	
Array Addresses	Enter a comma-separated list of host names or IP addresses of the IBM XIV Storage Arrays from which you want to collect data.	
IBM XIV XCLI Location	The location for the XCLI executable on the Data Collector server. Examples: Linux: `/opt/ibm/xch` Windows: `C:\Program Files (x86)\XIV\GUI10` or `C:\Program Files\XIV\GUI10`, `C:\Program Files\IBM\Storage\XIV\XIVGUI`	
User ID	Specify the user ID for the account that has monitor group privileges on the storage array.	
Password	The password for the User ID with monitor group privileges.	Pwd1

Field	Description	Sample Value
Array Details	Click the check box to activate performance collection. Click the Clock to configure a schedule for this Data Collector policy: ■ Frequency in minutes ■ Hourly ■ Daily ■ Weekly ■ Monthly ■ Cron Expression For example: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri..	
Array Performance	Click the check box to activate performance collection. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Click the Clock to configure a schedule for this Data Collector policy.	`1 */5 * * *`
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

6 Click **OK** to save the Policy.

7 On the Data Collector server, install/update the Data Collector software.

Chapter 45

Configuration for Microsoft Windows server

This chapter includes the following topics:

- Pre-Installation setup for Microsoft Windows server
- Prerequisites for adding Data Collectors (Microsoft Windows server)
- Collecting from applications and services logs
- Installation overview (Microsoft Windows Server)
- Add a Microsoft Windows server Data Collector policy

Pre-Installation setup for Microsoft Windows server

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Microsoft Windows server)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
  - The collector must have WMI network access to the Windows servers. User credentials must allow access to the root\cimv2, root\Microsoft\Windows\Storage, root\Microsoft\Windows\SMB and root\Microsoft\Windows\NFS WMI namespaces.
  - The Data Collector Service that is initially installed uses the Local System as the Login account. Sometimes this account does not have permissions to run remote WMI commands. Change the Service configuration to use a Login account that has Local Administrative privileges.
  - The collector uses a PowerShell script that uses WMI to communicate with the Windows Server, and makes a number of read-only calls to gather the information. PowerShell script execution must be enabled on the system running this script. The PowerShell version on the system must be 5.0 or above.
  - A full collection path to Windows server attached SAN or NAS storage requires that Host Resource collection be run first against the Windows servers.
  - WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service.

To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.

Collecting from applications and services logs

By default, the Windows Event Logs probe collects event messages from the Windows Logs. All events of the type Information and Audit Success are excluded from collection.

On the first collection, the Windows Event Logs probe collects all events that have occurred over the past one hour. Subsequent collections will collect starting from the time of the most current event.

Starting with release 10.2.01 P10, the Windows Event Logs probe has been enhanced to provide the collection of Events from the Applications and Services Logs.

To enable this collection, set two Advanced Parameters:

- WINDOWS_EVENTLOGS_NAME_FILTER
- WINDOWS_EVENTLOGS_INFO_EVENTID_FILTER (optional)

The parameter WINDOWS_EVENTLOGS_NAME_FILTER is set to the log name or group of logs to collect from. Wild card characters are supported. For example, to collect from the Windows SMB logs (which are presented by Windows Event Viewer in the folder structure Applications and Services Logs/Microsoft/Windows/SMBClient and Applications and Services Logs/Microsoft/Windows/SMBServer etc.) enter Microsoft-Windows-SMB* as the parameter value.

See https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent in the LogName section regarding what type of values are supported.

By default only Critical, Error and Warning events are collected. To also collect Information Events, set the WINDOWS_EVENTLOGS_INFO_EVENTID_FILTER parameter. Setting the value to '*' enables all Information Events to be collected. You can specify certain Event IDs by entering values such as 'EventID=30811 or EventID=1012' which will only collect Information events that match these EventIDs.

Installation overview (Microsoft Windows Server)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Microsoft Windows Server data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Add a Microsoft Windows server Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

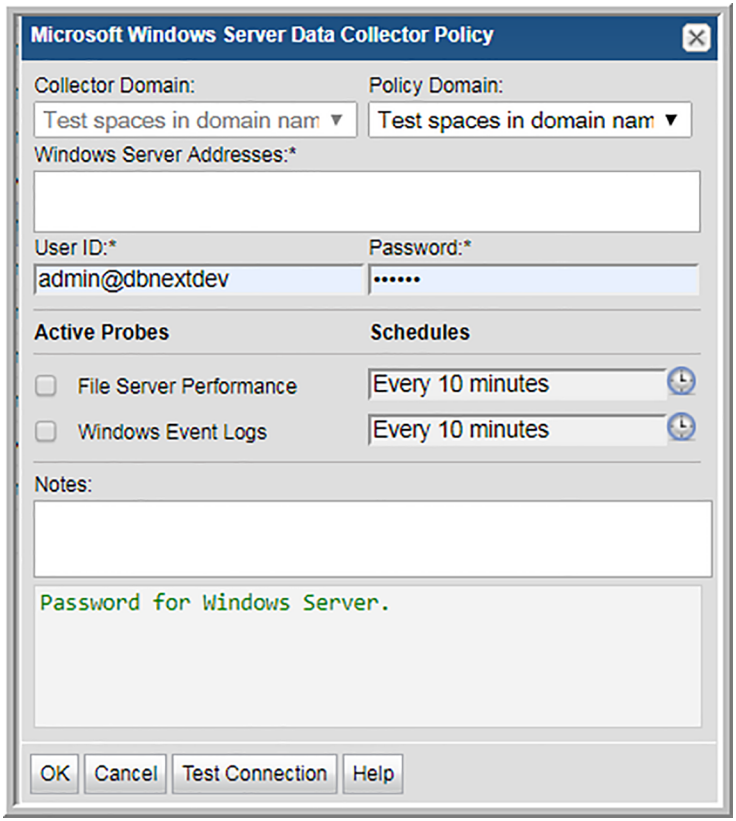
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Windows Server Addresses*	One or more Windows Server addresses to probe. Comma-separated host names are supported. Example, 10.2.3.4,10.5.3.1.
User ID*	User ID for the Windows Server.
Password*	Password for the Windows Server.
File Server Performance	Select this probe to collect the Windows File Server file share and performance information.
Windows Event Logs	Select the probe to collect Windows Event Log errors and warnings. See “Collecting from applications and services logs” on page 433. for additional information about collection options.
Schedule	Click the clock icon to create a schedule. By default, it is collected every 10 minutes. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See "Working with on-demand Data Collection" on page 624.

Chapter 46

Configuration for NetApp-7

This chapter includes the following topics:

- Pre-Installation setup for NetApp-7
- Prerequisites for adding Data Collectors (NetApp-7)
- Data Collector configurations specific to NetApp-7
- Installation overview (NetApp-7)
- Adding a NetApp Data Collector policy
- Testing the collection
- Creating a NetApp user with API privileges

Pre-Installation setup for NetApp-7

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (NetApp-7)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Data Collector configurations specific to NetApp-7

- Note the port used by the NetApp 7-Mode Data Collector: TCP 443.
- Gather the following required configuration details:
  - NetApp Addresses: IP addresses or names.
  - User ID & Password: Read-only user ID and password.
- Create a NetApp User with API privileges:

```
filer> useradmin role add apirole -a login-http-admin,api-*
filer> useradmin group add apigroup -r apirole
filer> useradmin user add apiuser -g apigroup
```

Note: For the **role** command, do **not** include a space after the comma.

If HTTP access is disabled on the vFiler

Some environments with vFilers (7-mode) disable HTTP access to the vFiler. In this situation, the Data Collector must use tunneling to retrieve data from the vFiler.

To enable access via tunneling, add the **security-api-vfiler** parameter to the api role, as shown in the following example:

```
filer> useradmin role add apirole -a
login-http-admin,api-*,security-api-vfiler
```

For additional details,

See "Creating a NetApp user with API privileges" on page 445.

Installation overview (NetApp-7)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the NetApp data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding a NetApp Data Collector policy

Note: Data collection requires a NetApp user with the necessary privileges to access the API.

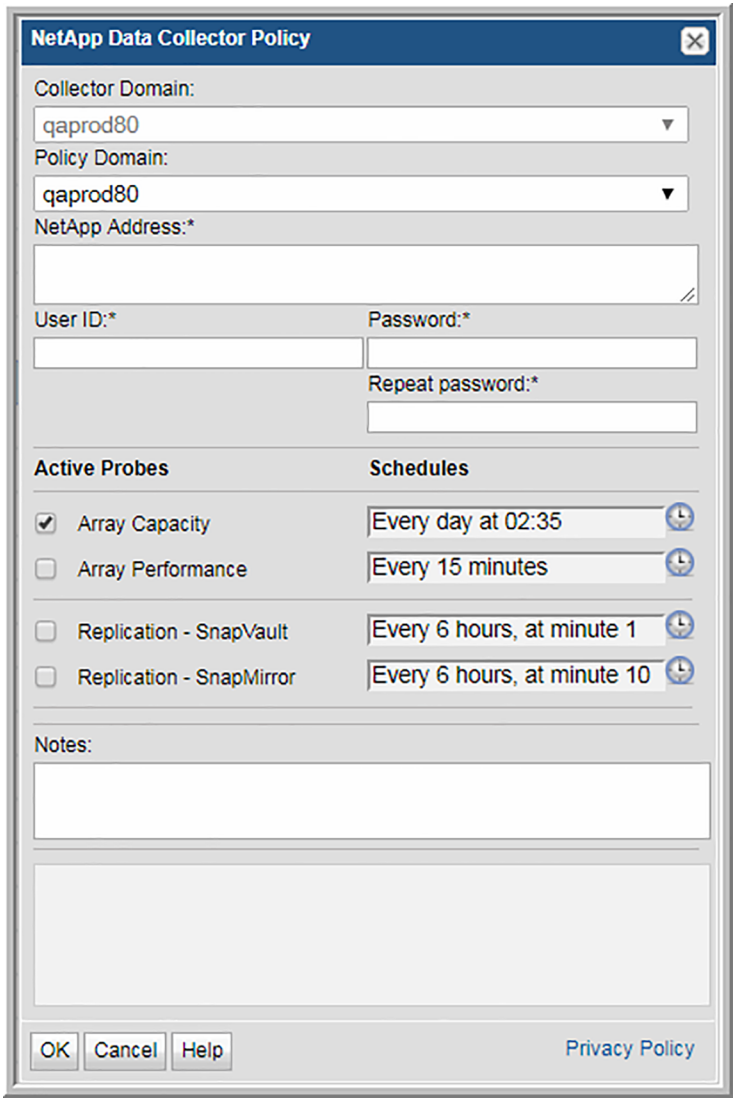
See "Creating a NetApp user with API privileges" on page 445.

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
NetApp Address*	One or more IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported.	192.168.0.1-250, 192.167.1.10, myhost
User ID*	The view-only user ID for NetApp storage.	
Password*	The password associated with the User ID.	
Array Capacity	Check the box to collect array capacity data. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Array Performance	Check the box to collect array performance data. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Click the clock icon to create a schedule.	
Replication -SnapVault	Click the check box if you are collecting data from your NetApp SnapVault environment. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. This field is specific to environments licensed for Replication Manager. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Replication - SnapMirror	Click the check box if you are collecting data from your NetApp SnapMirror environment. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. This field is specific to environments licensed for Replication Manager. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Testing the collection

You can test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

See "Working with on-demand Data Collection" on page 624.

Creating a NetApp user with API privileges

Use an existing NetApp user or create one with the necessary privileges to access the application programming interface (API). This role and user is required for collection from NetApp-7 systems. Typically, the root, admin user has all the capabilities, but it is not advisable to use root or admin passwords.

To create a new user, with the required privileges, on a NetApp system, use the following Command Line Interface (CLI) steps. For the **role** command, do **not** include a space after the comma.

```
filer> useradmin role add apifarole -a login-http-admin,api-*
filer> useradmin group add apifagroup -r apifarole
filer> useradmin user add apifauser -g apifagroup
```

If api-* does not meet your security requirements, additional File Analytics privileges can be configured using the following steps:

```
filer> useradmin role add apifarole -a
api-volume-list-info,api-nfs-exportfs-list-rules,
api-cifs-share-list-iter-start,api-cifs-share-list
-iter-next,api-cifs-share-list-iter-end,api-snapdiff
-iter-start,api-snapdiff-iter-next,api-snapdiff-iter
-end,login-http-admin,api-volume-options-list-info,
api-snapshot-list-info,api-snapshot-delete,api-
snapshot-create,api-nameservice-map-uid-to-user-name
filer> useradmin group add apifagroup -r apifarole
filer> useradmin user add apifauser -g apifagroup
```

Note: For the **role** command, do **not** include a space after the comma.

Chapter 47

Configuration for NetApp StorageGRID

This chapter includes the following topics:

- NetApp StorageGRID overview
- Prerequisites for adding Data Collectors (NetApp StorageGRID)
- Data Collector configuration specific to NetApp StorageGRID
- Installing NetApp StorageGRID
- Adding a NetApp StorageGRID Data Collector policy
- Testing the collection

NetApp StorageGRID overview

NetApp StorageGRID is a software-defined, object-based storage solution that supports industry standard API object, including the Amazon Simple Storage Service (S3) and the OpenStack Swift API.

The NetApp StorageGRID uses intelligent policy-driven data management to store, protect, and preserve fixed-content data over long periods of time, seamlessly moving data between on-premises and public cloud storage to optimize its availability, protection, performance, and cost.

Prerequisites for adding Data Collectors (NetApp StorageGRID)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Data Collector configuration specific to NetApp StorageGRID

- Execute Grid Management Policies Probe before Tenant Management Policies and Performance Management Policies Probe.
- Create a user with the same username and password for every Tenant account.
- The Grid users and the Tenant users should have Read only permissions.

Note: If SSL certificate error is displayed, import the certificate. For more information to import SSL certificate, see **System Administrator Guide** >> **SSL certificate configuration** >> **Import a certificate into the Data Collector Java keystore** section of the document.

Installing NetApp StorageGRID

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the NetApp data collector policy.

4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding a NetApp StorageGRID Data Collector policy

Note: Data collection requires a NetApp StorageGRID user with the necessary privileges to access the API.

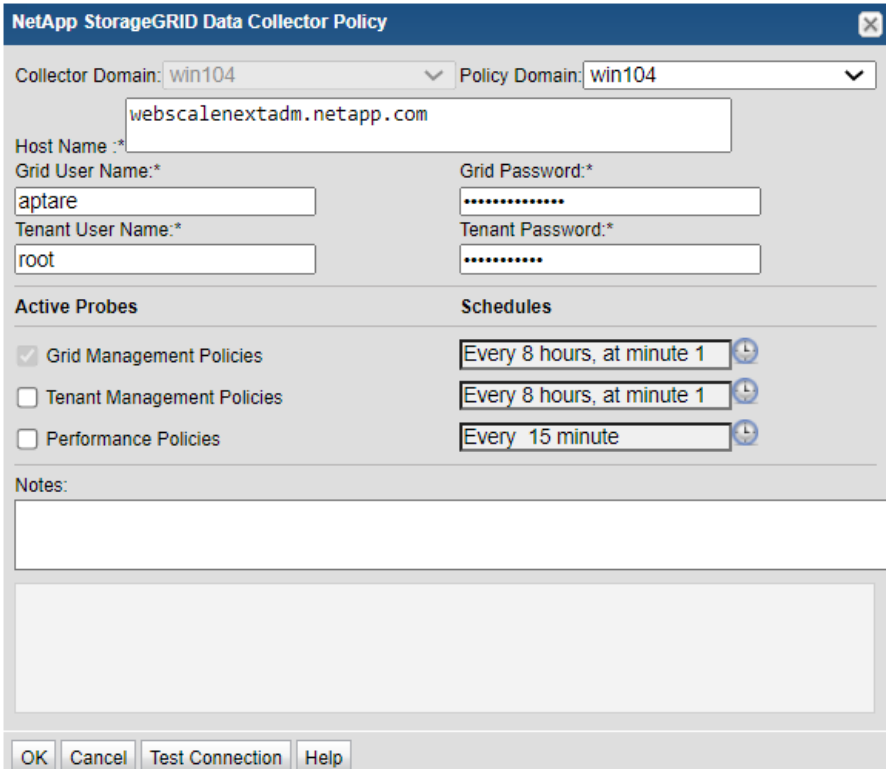
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
- For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
- On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1 Navigate to Admin >> Data Collection >> Collector Administration >> Add Policy.

2 Click Add Policy.

3 Click NetApp StorageGRID from storage column.



4 Specify the parameters. Mandatory parameters are denoted by an asterisk (*):

Table 47-1 NetApp StorageGRID parameters

Field	Description	Sample Value
Host Name *	Server IP to which data collector is going to communicate via REST on http / https to collect respective probe data.	10.12.145.50
Grid User Name *	Grid User name to communicate with the Server for REST calls.	
Grid Password *	Grid password to communicate with the Server for REST calls.	
Tenant User Name *	Tenant User name to communicate with the Server for REST calls.	

Table 47-1 NetApp StorageGRID parameters *(continued)*

Field	Description	Sample Value
Tenant Password *	Tenant password to communicate with the Server for REST calls.	
Active Probes	The probes which are to be executed. Below are the available options: ■ Grid Management Policies - Default. ■ Tenant Management Policies -Optional. ■ Performance Policies - Optional.	
Schedule:	Relevant schedule at which the probe must trigger.	

Testing the collection

You can test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

See "Working with on-demand Data Collection" on page 624.

Chapter 48

Configuration for NetApp Cluster

This chapter includes the following topics:

- Pre-Installation setup for NetApp Cluster
- Prerequisites for adding Data Collectors (NetApp Cluster)
- Installation overview (NetApp Cluster-Mode)
- Adding a NetApp Cluster-Mode Data Collector policy
- Testing the collection
- Creating a NetApp Cluster-Mode Read-Only user

Pre-Installation setup for NetApp Cluster

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (NetApp Cluster)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Create a NetApp Cluster-Mode read-only user.
  See "Creating a NetApp Cluster-Mode Read-Only user" on page 457.
- Port used by the NetApp Cluster-Mode Data Collector: TCP 443

Installation overview (NetApp Cluster-Mode)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the NetApp Cluster-Mode data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding a NetApp Cluster-Mode Data Collector policy

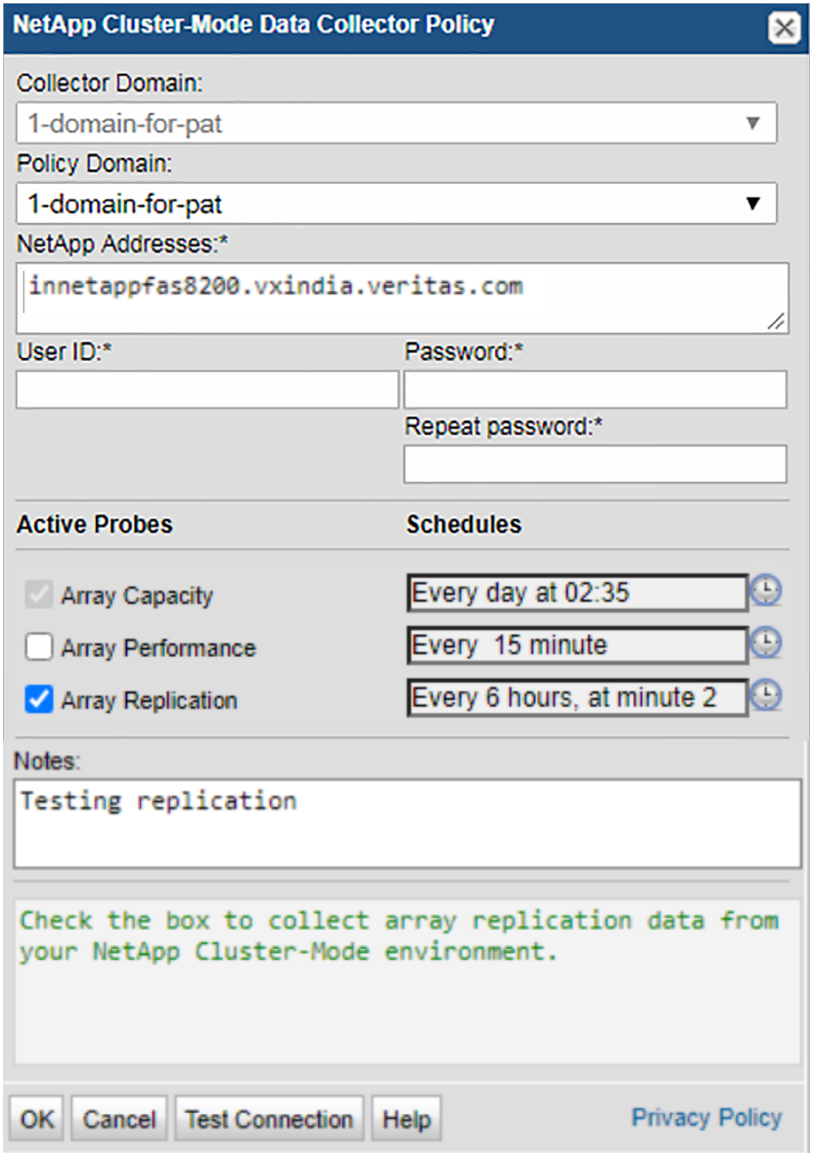
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
NetApp Address*	One or more Cluster-Mode IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, for example, 192.168.0.1-250, 192.168.1.10, myhost. If you use VMs in a management server configuration, be sure to connect to the filer node IPs and not the VM. Note that these are for ONTAP Cluster-Mode and ONTAP 7 addresses cannot be used.	192.168.0.1-250, 192.167.1.10, myhost
User ID*	The view-only user ID for accessing NetApp ONTAP Cluster-Mode storage.	
Password*	The password associated with the User ID.	

Field	Description	Sample Value
Array Capacity	Check the box to collect array capacity data from your NetApp Cluster-Mode environment. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	**1 */4 * * ***
Array Performance	Check the box to collect array performance data. Note that at least one collection from this array must be performed BEFORE array performance data can be collected. Click the clock icon to create a schedule.	
Array Replication	Select to collect array replication data from your NetApp Cluster-Mode environment.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Field	Description	Sample Value
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to Amazon Web Services using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to Amazon Web Services. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin** > **Data Collection** > **Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

Testing the collection

You can test the collection of data using the Run functionality available in Admin>Data Collection>Collectors. This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

Creating a NetApp Cluster-Mode Read-Only user

Data collection of NetApp Cluster-Mode requires a specific read-only role and user in order to collect data for a cluster.

To create a new user account with the required privileges, use the following Command Line Interface (CLI) steps. This set of commands creates a role as **apt_readonly** and then a user named **apt_user** with read-only access.

1. Create a read-only role using the following two commands.

```
security login role create -role apt_readonly -cmddirname DEFAULT
 -access readonly
security login role create -role apt_readonly -cmddirname security
 -access readonly
```

2. Create the read-only user using the following command. Once you have executed the create command, you will be prompted to enter a password for this user.

```
security login create -username apt_user -application ontapi
-authmethod password -role apt_readonly
```

The resulting role and user login will look something like this:

```
      Role            Command/                          Access
Vserver    Name          Directory                    Query Level
---------- ------------- --------- ------------------ --------
cluster1   apt_readonly  DEFAULT                       readonly
cluster1   apt_readonly  security                      readonly
cluster1::security login> show
Vserver: cluster1
                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
apt_user         ontapi      password       apt_readonly     no
```

Chapter 49

Configuration for NetApp E-Series

This chapter includes the following topics:

- Pre-Installation setup for NetApp E-Series
- Prerequisites for adding Data Collectors (NetApp E-Series)
- Installation overview (NetApp E-Series)
- Adding a NetApp E-Series Data Collector policy

Pre-Installation setup for NetApp E-Series

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (NetApp E-Series)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Locate the SMCLI executable.
- Port: TCP 2436.

Installation overview (NetApp E-Series)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the NetApp E-Series data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding a NetApp E-Series Data Collector policy

NetApp E-Series refers to arrays formerly branded as IBM Modular, which includes the 3000, 4000, and 5000 series arrays.

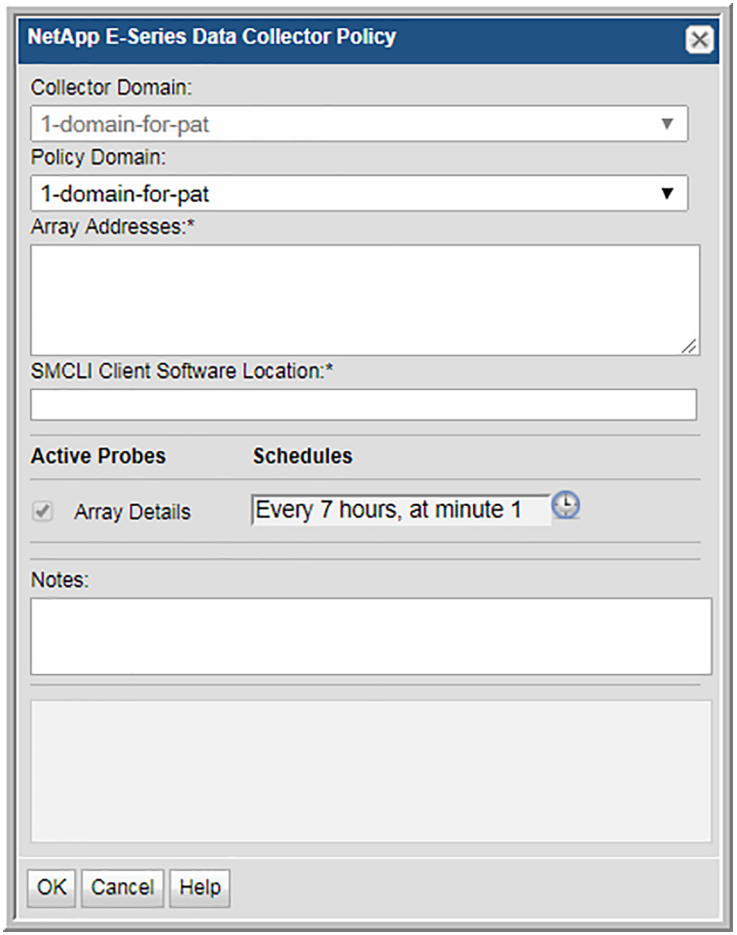
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	

Field	Description	Sample Value
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	
Active Probes Schedule*	Array details are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted. Examples: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri.	`1 */9 * * *`
Array Address*	Comma-separated list of IP addresses and/or names of the storage arrays.	
SMCLI client software location *	The location of the SMCLI executable. Examples: Linux: `/opt/SM8/client/` Windows: `C:\Program Files\SM8\client\` Windows: `C:\Program Files (x86)\StorageManager\client`	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Field	Description	Sample Value
	Test Connection initiates a Data Collector process that attempts to connect to AWS using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to AWS. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin**> **Data Collection**> **Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

Chapter 50

Configuration for NEC HYDRAstor

This chapter includes the following topics:

- Introduction
- Architecture overview
- Supported models and versions
- Prerequisites for adding a Data Collector
- Installation overview
- Adding a policy

Introduction

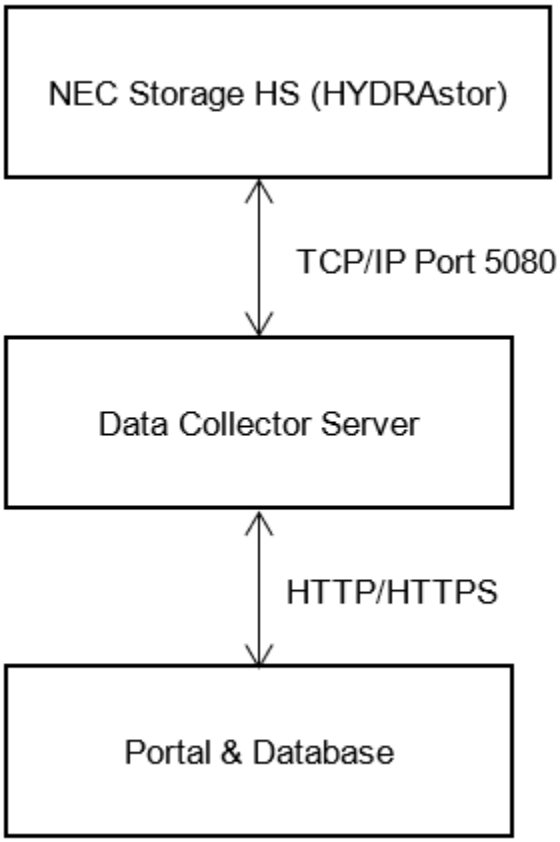
The NEC Storage HYDRAstor Virtual Appliance (HS VA) is a virtual data protection appliance that combines the flexibility of virtual machines.

The HS VA provides low-cost data protection at remote branch offices, replicating data to HS VA or HS3/HS8 appliances. HS VA also enables datacenters to provide cloud-based data protection services.

Architecture overview

The HYDRAstor Virtual Appliance is a software version of NEC HYDRAstor which runs on a virtual machine with most of the same functionalities as physical appliances. After deployment and configuration, its services can be managed by using the graphical user interface (GUI) or command-line interface (CLI).

Figure 50-1 Architecture



Supported models and versions

Version	■ V5.7.0 + P5.7.0-N002 ■ V5.7.1

Model	■ Japan ■ iStorage HS3-50, HS3-50S ■ iStorage HS6-50A, HS6-50AS ■ iStorage HS8-50, HS8-50S ■ iStorage HS Lite ■ Except for Japan ■ NEC Storage HS6-50A, HS6-50AS ■ NEC Storage HS8-50, HS8-50S ■ NEC Storage HS Virtual Appliance(HSVA)

Prerequisites for adding a Data Collector

The following are the prerequisites:

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name / value pairs to be in US English, and requires the installation by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For NEC Storage HS (HYDRAstor) collection, the Data Collector server and the subsystem can be in different time zones.
- The port which is used by the NEC Storage HS (HYDRAstor) Data Collector: Port 5080 for REST API.
- The user must have an administrator role in NEC Storage HS (HYDRAstor).

Installation overview

Steps for installation

1. Update the local hosts file to enable the portal access.
2. In the Portal, add a Data Collector, if one has not already been created.

3 In the Portal, add the **NEC storage HS (HYDRAstor)** data collector policy.

4 On the Data Collector Server, install the Data Collector software.

5 Validate the Data Collector Installation.

Note: These steps apply only while performing an IN-HOUSE installation. If a third-party service provider is hosting your Portal, that is, a HOSTED installation (perhaps for a product evaluation) skip this section and contact your hosting organization's representative to configure the hosted portal for your Data Collector.

Adding a policy

Validation before adding the policy

- A Data Collector must exist in the Portal for the Data Collector Policies.
  For specific prerequisites and supported configurations, see the **Certified Configurations Guide**.

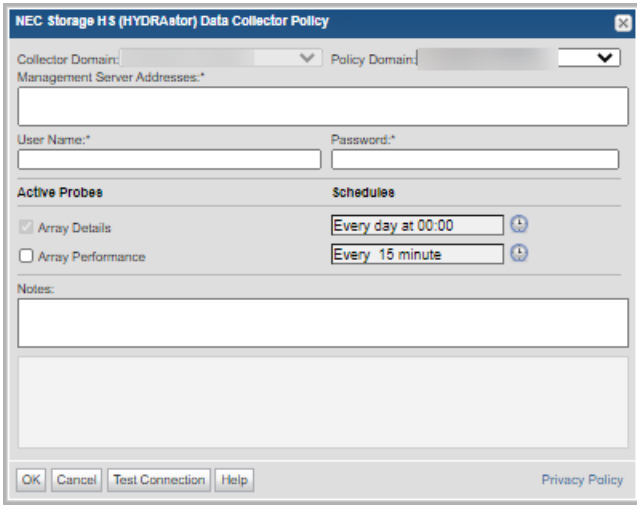
After adding the policy

- For some policies, the collections can be run on-demand using the **Run** at **Collector Administration** page action bar, provided that if the policy vendor is supported. On-demand collection lets you select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes.

  Note: Refer to the policy for probe descriptions.

To add the policy.

1. Navigate to **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select the Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



5. Specify the parameters. The mandatory parameters are denoted by an asterisk(*) symbol.

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is added. The Collector Domain is a read-only field. By default, the domain for a new policy is the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group which is associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers should have a unique domain with its own host group hierarchy. To find your Domain name, click your logon name and select My Profile from the menu. Your Domain name is displayed in your profile settings. Example: yourdomain
Management Server Addresses*	One or more NEC Storage HS (HYDRAstor) Floating IP addresses or host names to probe. Comma-separated addresses are supported. For example 192.168.1.10, myhost

Username*	Administrator username for the NEC Storage HS (HYDRAstor).
Password*	Administrator password for the NEC Storage HS (HYDRAstor).
Array Details Probe	Array details such as system, file system, user are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week, and month. Advanced use of native CRON strings is also available. If NEC Storage HS (HYDRAstor) has no data (Data Reduction ratio is N/A), NASFileServer operation and SystemCapacity operation fail. SystemCapacity operation can collect data for “data and metadata” and “parity”, but not for “data” and “parity and metadata”. **Note:** The explicit schedules that are set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Array Performance	The data that is associated with the performance of the NEC Storage HS (HYDRAstor) system to be collected. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week, and month. Advanced use of native CRON strings is also available. File-System capacity detail will be collected once a day.
Notes	Specify or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and the credentials in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there can be a delayed connection to the subsystem. Likewise, there can be a delayed response, due to other processing threads running on the Data Collector. You can also test the collection of data using the Run functionality available in **Admin** > **Data Collection** > **Collector Administration**. This *on-demand* data collection initiates a high-level validation of the installation at the individual policy level, including the domain, host group, URL, Data Collector policy, and database connectivity. You can also select individual probes and servers to test the collection run.

6. Click **OK** to save the policy.

7. On the Data Collector server, add entries to the local hosts file, both resolving to the Portal server IP address.

Chapter 51

Configuration for Pure Storage FlashArray

This chapter includes the following topics:

- Pre-Installation setup for pure Storage FlashArray
- Prerequisites for adding Data Collectors (pure Storage FlashArray)
- Installation overview (Pure storage FlashArray)
- Add a pure storage FlashArray Data Collector policy

Pre-Installation setup for pure Storage FlashArray

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (pure Storage FlashArray)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation overview (Pure storage FlashArray)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Pure Storage FlashArray data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

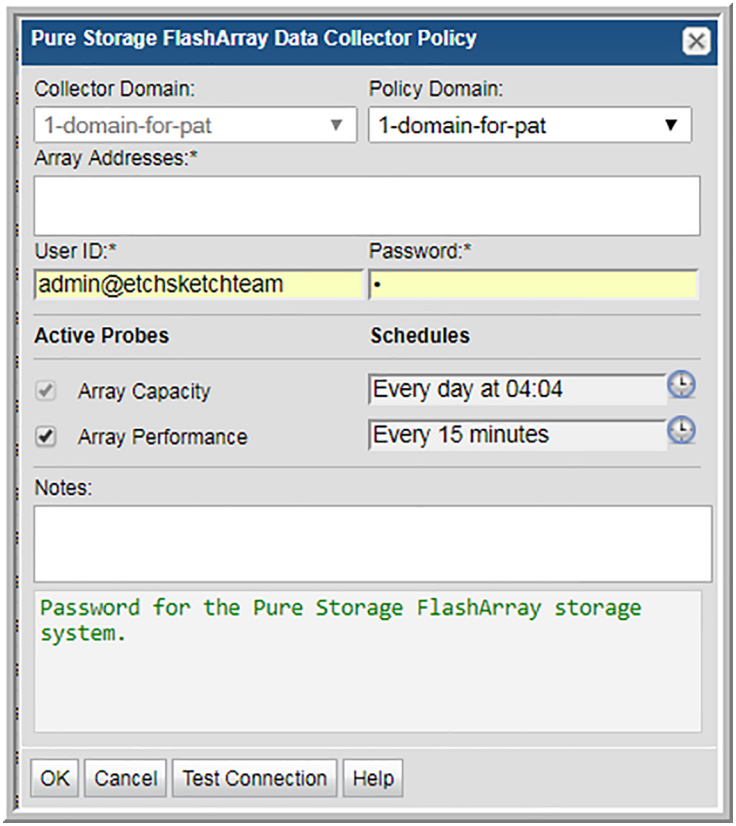
Add a pure storage FlashArray Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Array Addresses*	One or more FlashArray IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, pure01.
User ID*	View-only User ID for the Pure Storage FlashArray storage system.
Password*	Password for the Pure Storage FlashArray storage system. The password associated with the User ID.
Array Capacity	This collection is enabled by default to collect array capacity data from the Pure Storage FlashArray environment.
Array Performance	This collection is enabled by default to collect array performance data from the Pure Storage FlashArray environment. Statistics are persisted in the database as the last 3 hours in 30 second intervals. It is recommend to set a collection schedule for no more than every 3 hours.
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run. See "Working with on-demand Data Collection" on page 624.

Section 4

Compute (Virtualization and Host Collection)

- Chapter 52. Configuration for VMware
- Chapter 53. Configuration for IBM VIO
- Chapter 54. Configuration for Microsoft Hyper-V

Chapter 52

Configuration for VMware

This chapter includes the following topics:

- Pre-Installation setup for VMware
- VMware Data Collection
- Prerequisites for adding data collectors (VMware)
- Installation overview (VMware)
- Add a VMware Data Collector policy
- Datastore scan collection

Pre-Installation setup for VMware

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

VMware Data Collection

VMware Data Collection offers two options for collecting data:

- Collect data from vSphere (formerly vCenter) and/or
- Collect data from specific ESX servers that are not managed by vSphere

When you create a Data Collection policy, you can specify host names and/or IP addresses or range of addresses. In addition, you can enter a comma-separated list of any combination of host names and addresses to be probed.

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (VMware)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Port 443 must be open. Data collection uses HTTPS without certificates for secure connections.

Virtualization Manager: Collection of VMware Data

- This Data Collector policy can be incorporated with an existing Data Collector Policy. A Data Collector can collect data from Virtual Center (vCenter) or from specific ESX servers that are not managed by vCenter.
- The VMware Data Collector is multi-threaded enabling it to poll up to five vCenters in one polling cycle. Therefore, multiple vCenter collections can be configured in one Data Collector policy.

Configure VMware Access

The VMware Data Collector uses the VMware Infrastructure SDK and REST APIs over HTTPS to retrieve data from ESX servers. The VMware Data Collector is multi-threaded, enabling it to poll up to five vCenters in one polling cycle.

VMware requires the following access for data collection:

1. View-only VMware User ID that has a role with the following privileges:
   - **Read-Only**
   - **Browse Datastore**
   - **View VM storage policies**

   Note: Permissions can be granted to an existing local account or domain/AD user.

2. Assign the user to the root-level folder permissions of vSphere.

   The administrator user who provisions the read-only role for collection must be an administrator at the root level, not just at a data center or other level. If multiple vCenters are available for administration in the client (Linked Mode), that administrator user must be provisioned at the root level for each vCenter Server from which data is collected.
3. Port 443 must be open. Data collection uses HTTPS without certificate validation for encrypted connections. This allows the use of a self-signed certificate on the VMware server.

Pre-requisites for vSAN Data Collection

Currently vSAN data collection supports only the virtual center server.

vSAN configuration should be enabled on the VMWare Cluster of Virtual Center to perform vSAN data collection.

vSAN configurations

The following vSAN services should be enabled on the VMWare Cluster of virtual center to collect the **vSAN details** of each cluster.

- vSAN iSCSI Target Service
- Historical Health Service
- Data Service
- Network
- File Service

The following service should be enabled on the VMWare cluster of virtual center to collect the **vSAN performance details**.of each cluster.

- Performance service

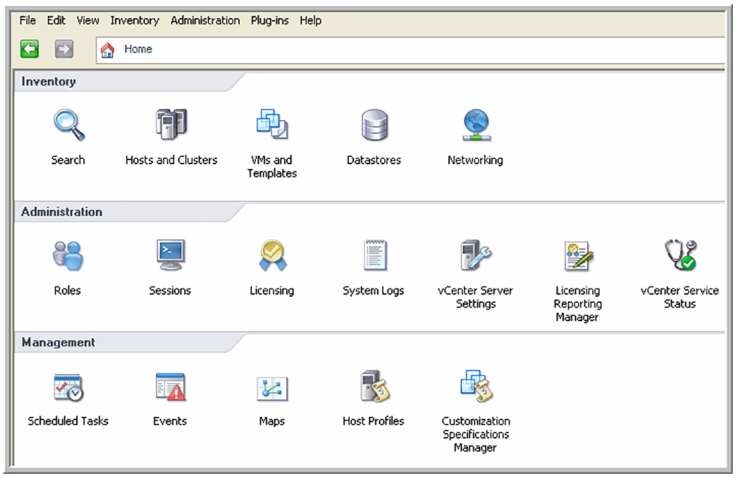
Creating a VMware Read-Only User with Required Permissions

The following procedure provides the steps for creating and configuring a vSphere user with the necessary permissions for Virtualization Manager data collection access.

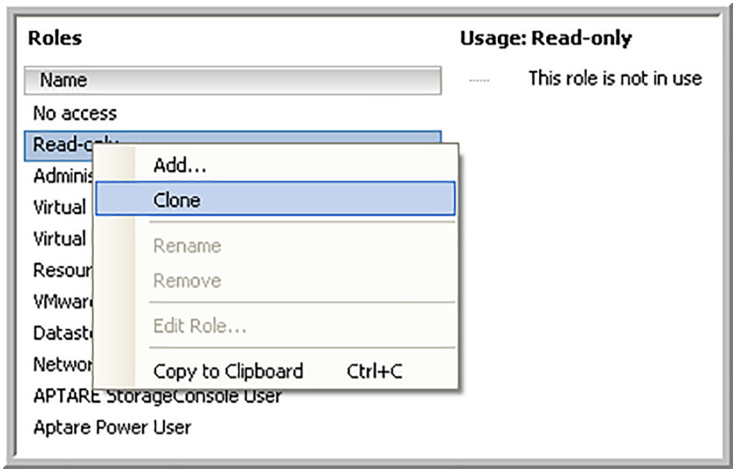
Note: Permissions can be granted to an existing local account or domain/AD user. The following VMware user-creation steps are required only if you do not want to grant permissions to an existing user.

---

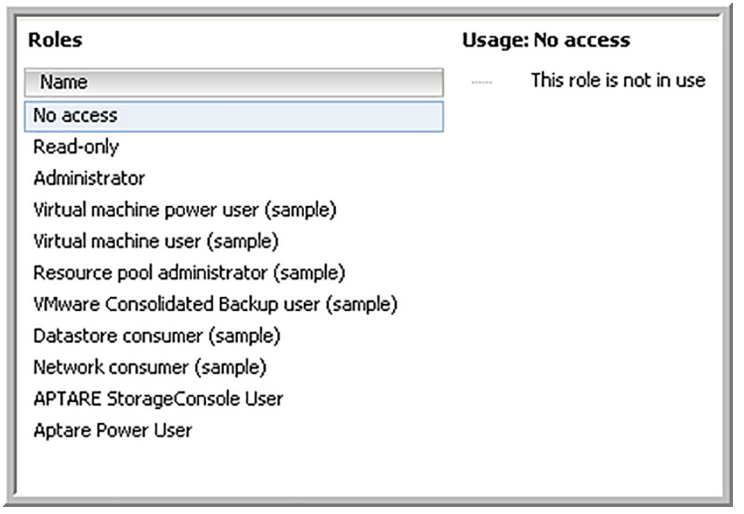
1. Create a new vCenter user to be used with NetBackup IT Analytics. For the purpose of the examples in this document, we'll name the user **aptare**.
2. Log in to vSphere with Administrator credentials to create a user with new permissions.
3. In the Home page (Alt+Home), click **Roles** under the **Administration** heading.



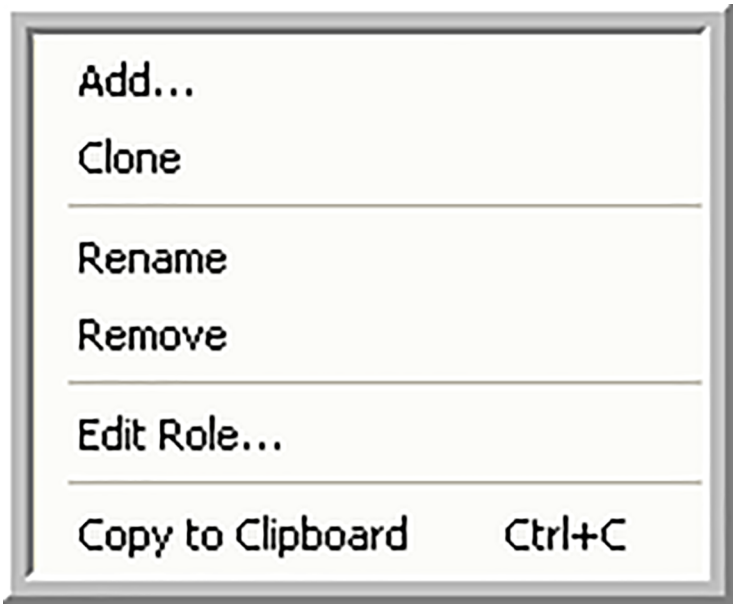
4. In the Roles window, right-click on **Read Only** and select **Clone**.



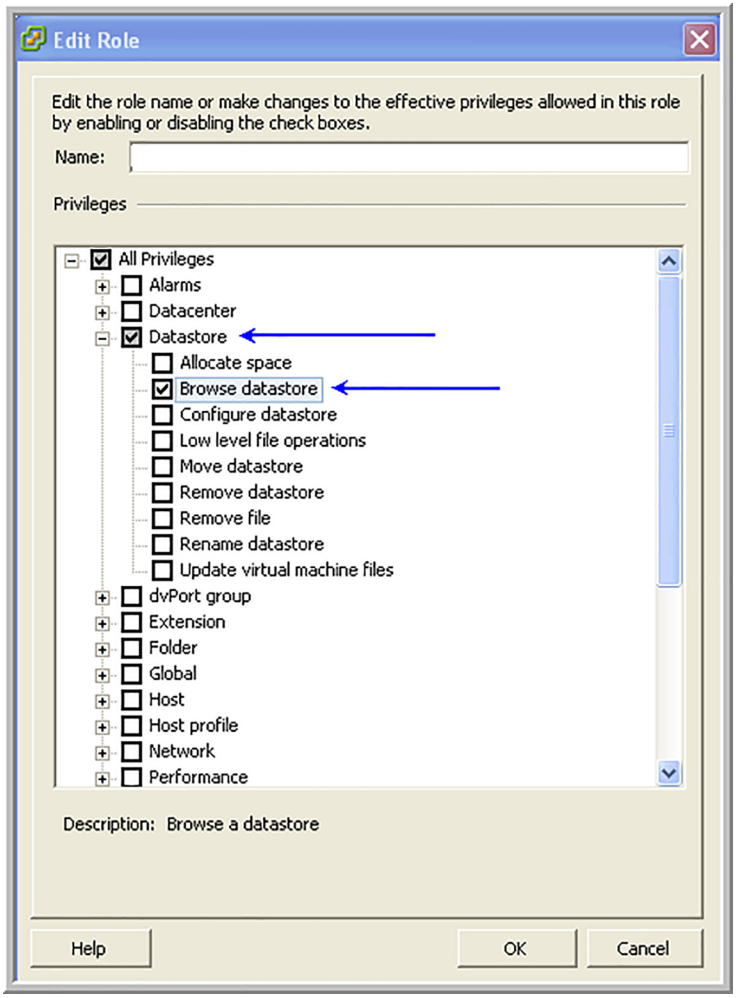
5. Name the role **NetBackup IT Analytics User**.



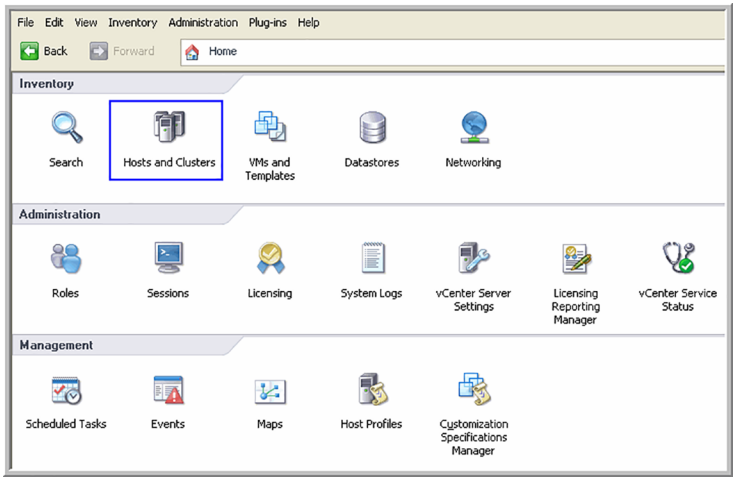
6. Right-click on the Role you just created--**NetBackup IT Analytics User**-- and select **Edit Role**.



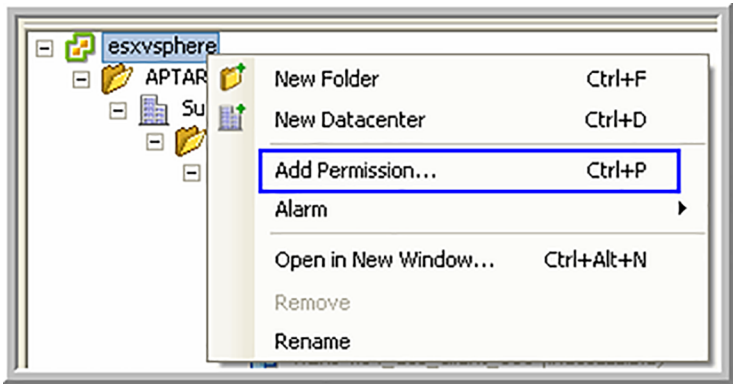
7. The only permission that is required beyond the Read-Only role is Browse Datastore and View VM storage policies. Select **Browse Datastore**, click **View VM storage policies** and then click **OK**.



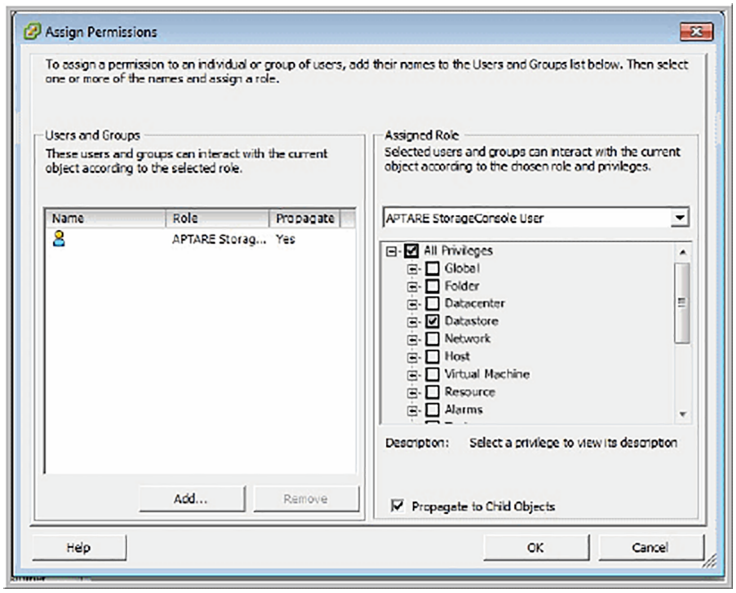
8. At the top of the vSphere window, select **Administration** > **Inventory** > **Hosts and Clusters**.



9. At the left of the vSphere window, right-click on the Root of the tree--in this example, esxvsphere--and then select **Add Permission**.



10. In the Assign Permissions window, under Assigned Role, select **NetBackup IT Analytics User** and under Users and Groups, add the user that you created and click **OK**.



11. Once the user has been added, you should see it listed under the **Permissions** tab.



12. Now you are ready to add the user to the NetBackup IT Analytics Portal. Be sure to enter the user name exactly as it is displayed in the Permissions tab (it is case sensitive). If you are using a Domain account, also include the Domain in the User ID field (for example: domain.com\aptare).

Installation overview (VMware)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the VMware data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector installation.

Add a VMware Data Collector policy

To improve performance, if you configure the vCenter 5-minute summaries for level 3 or higher, the Data Collector will use this configuration to reduce the load on the Portal during data collection. In vCenter, go to **Administration > vCenter Server Settings > Statistics**. Edit the 5-minute statistics interval and set the statistics to level 3. Note that when using level 3, some per-instance data (such as CPU core) may be missed or incomplete.

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Configure the VMware Data Collector policy.

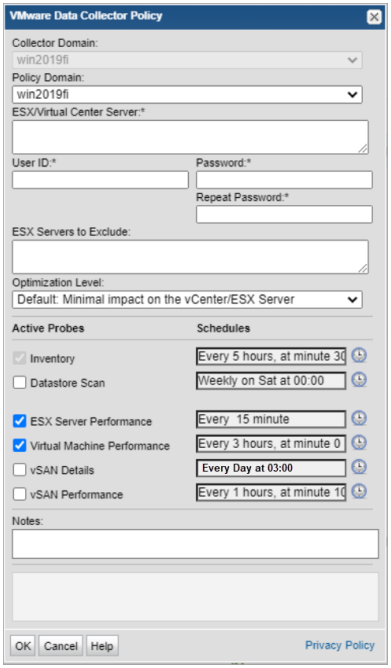


Table 52-1 VMware Data Collector Policy

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.

Table 52-1 VMware Data Collector Policy *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
ESX/Virtual Center Server*	One or more IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported. If the server requires an SSL certificate, refer to Adding a Certificate to the Java Keystore for instructions. Sample value: **192.168.0.1-250, 192.167.1.10, myhost**
User ID*	The view-only VMware user ID that has a role with the following privileges: **Read-Only** and **Browse Datastore**.
Password*	The password associated with the User ID.
ESX Servers to Exclude	Enter one or more ESX server names or IP addresses. Comma-separated names/addresses or IP ranges are supported.
Optimization Level	Select an optimization level for your VMWare data collection. Choose from default, aggressive, or none. Each selection impacts runtime differently. Effects will be most noticeable when running the Datastores collection.

Table 52-1 VMware Data Collector Policy *(continued)*

Field	Description
Inventory	By default, this probe collects data from VMware using the defined schedule. VMware tags and custom attributes are collected as part of this probe. Tags are only available when collecting from vCenter and not directly from an ESX server. Custom attributes are available from both vCenter and directly from ESX server. For performance reasons, this collection only gathers information on files currently in use by VMs collected by this probe. This includes VM disk files, suspended state, etc. Due to limitations in the data returned from VMware, this probe may miss certain files, such as ISO files that are attached to virtual DVD drives. To capture all datastore file information including the files associated with VMs in the inventory, select the check box: **Datastore Scan**. If the Datastore Scan probe is not regularly run, the Datastore Usage Breakdown report is likely to have a large Unknown category. For additional information, See "Datastore scan collection" on page 495. and See "Reports impacted by Datastore Collection" on page 496. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 52-1 VMware Data Collector Policy *(continued)*

Field	Description
Datastore Scan	Select **Datastore Scan** to perform a complete scan and capture all datastore file information. This probe may take several hours to complete and should be configured to run when VMWare is less active (for example on weekends). This probe will find files that are not discoverable using the Inventory probe but are consuming space on the datastore. After this probe has run the Datastore Usage Breakdown report will normally only have a small Unknown category, however, there usually will be some Unknowndata, representing file system overhead and internal VMWare disk structures that are not reported as files. Only enable this probe when actively looking for files that may be wasting space in the datastores. For additional information, See "Datastore scan collection" on page 495. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
ESX Server Performance	Select ESX Server Performance to collect performance data for ESX servers. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 52-1 VMware Data Collector Policy *(continued)*

Field	Description
Virtual Machine Performance	Select this probe to collect performance data from virtual machines. This probe may need to be run less often than the ESX Server Performance probe because there are usually more virtual machines than ESX servers. This probe may be disabled if it is not necessary to monitor the performance of individual virtual machines. When the default schedule of once every 3 hours is used, the Data Collector will use vCenter's 5-minute summaries for part of the data or, if collecting directly from an ESX server, there may be gaps in the data. To ensure that real-time data is always used (subject to the statistics level that is set), or if collecting from an ESX server, change the schedule of this probe to every hour (or more frequently). Click Help to view the statistics level settings in the Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
vSAN Details	Select vSAN Details probe to collect vSAN configuration details, along with health and policy. Schedule will execute daily at 03:00 hours by default and collects: ■ Configuration information ■ Cluster health information ■ vSAN disk information ■ vSAN storage policy information This probe executes on vCenter configuration and does not perform collection for ESX configuration. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 52-1 VMware Data Collector Policy *(continued)*

Field	Description
vSAN Performance	Select this probe to collect vSAN performance information. By default, the probe executes every hour at 10 minutes and collects information from the previous one hour. If you change the schedule to a duration less than an hour (less than 60 minutes), the probe executes at the specified schedule and also collects information of the time specified in the schedule. In case you set the schedule for a duration longer than one hour, the probe executes at the scheduled interval but collects data only of the past one hour from the time of execution. This behavior continues for all collections scheduled more than one hour apart. Hence as a best practice, you must schedule the probe to execute in less than or equal to one hour to be able to collect and report all the information within that hour. This probe executes on vCenter configuration and does not perform collection for ESX configuration. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Datastore scan collection

By default, Inventory collection only captures information about the files referenced by a collected virtual machine (VM files), and only using the information available without directly contacting the datastore. Examples of large files that will not be collected during the default Inventory collection are .iso files (such as, DVD images) and disk images (.vmdk) that are not attached to any collected VM. Data collection runtime is reduced when using the default Inventory collection, but only files for VMs in the inventory are collected. Therefore, a considerable amount of consumed space in the datastore may not be captured. Choose the **Datastore Scan** option to gain visibility into the storage that is not associated with a VM.

When you check **Datastore Scan**, a more detailed collection is performed by scanning the datastore to discover files resident on the datastore, but not associated with a VM in the inventory. This option, although it may impact performance, finds files that may be invisible to VMware, but that are consuming space on the datastore. For example, a VM may have been removed without deleting files from the datastore. Similarly, log files or user-stored files may be taking up space not apparent from the VM inventory's perspective.

See "Reports impacted by Datastore Collection" on page 496.

Note: If an error occurs during the Datastore Scan, then only the files available with the default Inventory collection will be collected for the Datastore. It is also possible that individual files may be found via the Inventory collection, but not via the Datastore Scan.

Reports impacted by Datastore Collection

The following reports may be impacted by the Datastore Scan collection configuration in the data collector policy.

Table 52-2 Reports impacted by Datastore Collection

Report	Default Inventory	Collect all files on datastore
VM Files Summary (drilldown)	■ No Last Modified date. ■ Total # files collected will usually be less than with an all files collection.	Last Modified date will be missing for files not found in the datastore scan.
Datastore Usage Breakdown	■ Non-VM Files and VM Not In Inventory will be zero. ■ Total VM Used will be reduced by the amount that would have been collected as VM Not In Inventory if an all files collection had been done. ■ Unknown category in the pie chart will often be significantly higher than if an all files collection had been done.	The Unknown category in the pie chart will usually be non-zero and will often be significantly higher than the default inventory collection.
Datastore Utilization	■ VM Not In Inventory will be zero. ■ Total VM Used will be reduced by the amount that would have been collected as VM Not In Inventory if an all files collection had been done.	

Table 52-2 Reports impacted by Datastore Collection *(continued)*

Report	Default Inventory	Collect all files on datastore
Datastore Detail	■ Non-VM Files and VM Not In Inventory will be zero. ■ Total VM Used will be reduced by the amount that would have been collected as VM Not In Inventory if an all files collection had been done.	VMDK and Other VM Files values typically will not be impacted by the datastore collection type.
VM Server Detail	■ VM Not In Inventory will be zero ■ Total VM Used will be reduced by the amount that would have been collected as VM Not In Inventory if an all files collection had been done.	Last Modified date will be missing for files not found in the datastore scan.
VM Detail	■ No Last Modified date. ■ Total # files collected will usually be less than with an all files collection.	
VM Snapshot Summary	■ No Last Modified date.	

Chapter 53

Configuration for IBM VIO

This chapter includes the following topics:

- Pre-Installation setup for IBM VIO
- Prerequisites for adding data collectors (IBM VIO)
- Installation overview (IBM VIO)
- Adding servers for the IBM VIO Data Collector policy
- VIO servers (IBM Virtual I/O Servers)
- LPAR clients (IBM Logical Partitioning Clients) managed by VIO servers
- HMC (IBM Hardware Management Console)
- Add an IBM VIO Data Collector policy

Pre-Installation setup for IBM VIO

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (IBM VIO)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Note the port used by the IBM VIO Data Collector: SSH 22, telnet 23.
- Data Collection retrieves data from servers in the following order:
  - VIO Servers (Virtual I/O Servers): Enable Capacity, HBA, Volume Manager, and Multi-pathing probes in Host Discovery and Collection. To use the VIO restricted shell to execute commands to collect data, configure the advanced parameter, USE_VIO_RESTRICTED_SHELL.
  - LPAR Clients (Logical Partitioning Clients) Managed by VIO Servers: Enable Capacity, HBA, Volume Manager, and Multi-pathing probes in Host Discovery and Collection.

    For newly discovered LPAR Clients, probes can be configured directly from the data collector policy.
- Gather the following required configuration details for the VIO Data Collector Policy:
  - LPAR Management Server: IP address or server name of the IBM LPAR Management Server (HMC or IVM).
  - User ID & Password: Credentials for the LPAR Management Server.
  - For the VIO server: **Private Key File** and **Known Hosts File** and **Path**.

Installation overview (IBM VIO)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the IBM VIO data collector policy.
4. On the Data Collector Server, install the Data Collector software.

5. Validate the Data Collector Installation.

Adding servers for the IBM VIO Data Collector policy

IBM VIO Data Collection requires collection from servers in the following order:

1. See "VIO servers (IBM Virtual I/O Servers)" on page 500.
2. See "LPAR clients (IBM Logical Partitioning Clients) managed by VIO servers" on page 501.
3. See "HMC (IBM Hardware Management Console)" on page 501.

As an Administrator, you may not have a complete list of the server combinations in your enterprise. Enable HBA and Multipath Probes for the servers, monitor error messages, and then disable probes, as needed.

VIO servers (IBM Virtual I/O Servers)

To configure collection for IBM VIO Servers:

1. On the VIO Servers, create a normal AIX user instead of a padmin user.
2. Access the Host Inventory window.

   Admin > Data Collection > Host Discovery and Collection
3. In the Host Discovery and Collection window, either use Discover Hosts to collect the initial data for the VIO Servers or search for the VIO Servers.
4. Configure capacity probes for each of the VIO Servers according to the following guidelines:
   - Capacity: enable.
   - HBA Probe: enable, since the VIO Servers are connected directly to the SAN.
   - Volume Manager: enable.
   - Multipathing:
     If the VIO Servers have any third-party multipathing software such as EMC PowerPath or Hitachi HDLM Multipathing, the Multipath Probe should be enabled.
     If the VIO Servers are using native AIX multipathing, the Multipath Probe should be disabled.

LPAR clients (IBM Logical Partitioning Clients) managed by VIO servers

By configuring collection for IBM LPAR clients through the data collector policy, all newly discovered LPARs found using the collector policy will automatically have the host probes activated. The eliminates the requirement of manually enabling the probes using Host Discovery.

1. On the IBM VIO data collector policy, click the checkbox **Enable Host Collection**. This activates the **Configure Host Collection** button.
2. Click **Configure Host Collection**.
3. Configure capacity probes for each of the LPAR Clients according to the following guidelines:

- Capacity: enable.
- HBA Probe:
  - If the disks are given to LPAR Clients using VSCSI, the HBA Probe should be disabled since the LPAR Clients are not connected directly to the SAN.
  - If the disks are given to LPAR Clients using NPIV, the HBA Probe should be enabled.
- Volume Manager: enable.
- Multi-pathing:
  - If the LPAR Clients have any third-party multi-pathing software such as EMC PowerPath or Hitachi HDLM Multipathing, the Multipath Probe should be enabled.
  - If the LPAR Clients are using native AIX multi-pathing, the Multi-path Probe should be disabled.

HMC (IBM Hardware Management Console)

To configure data collection from the HMC (the LPAR management server), refer to the following.

See “Add an IBM VIO Data Collector policy” on page 502.

Add an IBM VIO Data Collector policy

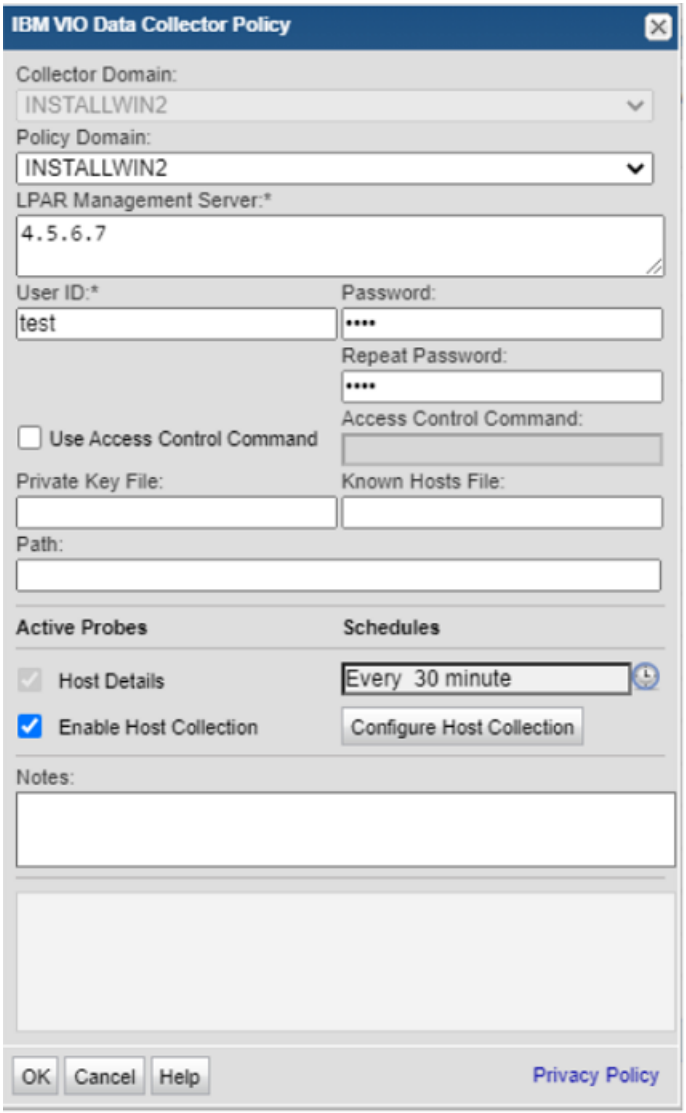
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Specify Data Collector Properties.



6 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
LPAR Management Server*	The address of the IBM LPAR Management Server of either HMC or IVM--either the IP address or server name. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost.
User ID*	Username and password for the LPAR Management Server. For HMC, the username should have at least HMC Viewer permissions.
Password*	**Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.
Use Access Control Command	Click the check box to indicate access control commands
Access Control Command	Access control command for the IBM VIO server, either sudo, pbrun, or sesudo.
Private Key File	The private key file for the IBM VIO server
Known Hosts File	Known hosts file for the IBM VIO Server.

Field	Description
Path	The path used by the VIO server
Host Details	Host details are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Enable Host Collection	Click the checkbox to activate the button: **Configure Host Collection**.
Configure Host Collection	Enables the configuration of various host probes for each of the newly discovered LPAR Clients. By configuring collection for IBM LPAR clients through the data collector policy, all newly discovered LPARs found using the collector policy will automatically have the host probes activated. This eliminates the requirement of manually enabling the probes.See "LPAR clients (IBM Logical Partitioning Clients) managed by VIO servers" on page 501.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

7 Click **OK** to save the policy.

8 On the Data Collector server, install/update the Data Collector software.

Chapter 54

Configuration for Microsoft Hyper-V

This chapter includes the following topics:

- Pre-Installation setup for Microsoft Hyper-V
- Prerequisites for adding data collectors (Microsoft Hyper-V)
- Installation overview (Microsoft Hyper-V)
- Add a Microsoft Hyper-V Data Collector policy

Pre-Installation setup for Microsoft Hyper-V

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding data collectors (Microsoft Hyper-V)

Identify a server where the Data Collector software will be installed. Server requirements include:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- The collector must have WMI network access to the Hyper-V servers. User credentials must allow access to the root\cimv2, root\virtualization\v2 and root\MSCluster WMI namespaces.
- The Data Collector Service that is initially installed uses the Local System as the Log in account. Sometimes this account does not have permissions to run remote WMI commands. You should instead change the Service configuration to use a Log in account that has Local Administrative privileges.
- The collector uses a PowerShell script that uses WMI to communicate with the Hyper-V, and makes a number of read-only calls to gather the information. PowerShell script execution must be enabled on the system running this script. The version of PowerShell on the system must be 5.0 or above.
- A full collection path to Hyper-V server attached SAN or NAS storage requires that Host Resource collection be run first against the Hyper-V servers.
- WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service.

To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.

Installation overview (Microsoft Hyper-V)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Microsoft Hyper-V data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector installation.

Add a Microsoft Hyper-V Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

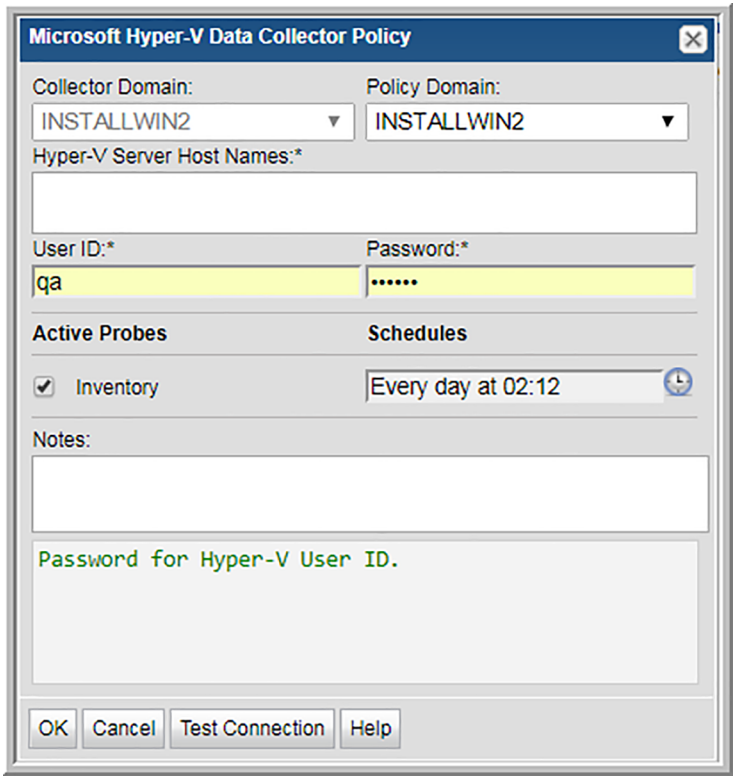
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Specify Data Collector Properties.



6 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	**yourdomain**

Field	Description	Sample Value
Hyper-V Server Host Names	One or more Hyper-V Server Host Names to probe. IP Address is not supported. Comma-separated host names are supported. For example, HyperV1, HyperV2.	
User ID/Password	View only WMI User ID for Hyper-V Server. To include a domain name use the format DOMAIN\USERNAME.	
Active Probes		
Inventory	Probe for collecting Hyper-V server and Hyper-V guest information.	
Schedule	The default is every day at 2:12. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Field	Description	Sample Value
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

7 Click **OK** to save the policy.

8 On the Data Collector server, install/update the Data Collector software.

Section 5

Cloud

- Chapter 55. Configuration for Amazon Web Services (AWS)
- Chapter 56. Configuration for Google Cloud Platform
- Chapter 57. Configuration for OpenStack Ceilometer
- Chapter 58. Configuration for OpenStack Swift
- Chapter 59. Configuration for Microsoft Azure

Chapter 55

Configuration for Amazon Web Services (AWS)

This chapter includes the following topics:

- Pre-Installation setup for Amazon Web services (AWS)
- Prerequisites for adding Data Collectors (Amazon Web services)
- Prerequisite Amazon Web services (AWS) configurations
- Configure an S3 bucket to receive billing reports
- Select cost allocation tags
- Create an AWS IAM user
- Mandatory probe user privileges
- Link AWS accounts for Collection of consolidated billing data
- Installation overview (Amazon Web Services - AWS)
- Add an Amazon Web Services (AWS) policy

Pre-Installation setup for Amazon Web services (AWS)

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Amazon Web services)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Amazon cloud computing resources are hosted in multiple locations world-wide. These locations are composed of AWS Regions. NetBackup IT Analytics enables you to configure the default region using the advance parameter.
  - **Advance parameter**: AWS_DEFAULT_REGION
  - **Value**: Veritas suggests determining the region from the following document and specify appropriate region from the Region column of the Region availability table.
    AWS Document

    Note: If no value is specified NetBackup IT Analytics considers **us-west-2** as the default value.

Prerequisite Amazon Web services (AWS) configurations

The Amazon Web Services Data Collector can collect from the following AWS entities:

- **S3 Bucket (Details and Usage)**- Simple Storage Service (S3) for storage in the cloud

- **EC2 Details** - Elastic Cloud Compute (EC2) for computing services, much like virtual servers
- **Billing Records** - Usage and corresponding charges, by service

For additional information about the type of data that is collected, refer to the Data Collector Policy configuration.

Note: Due to limitations on API request rates, multiple simultaneous processes may interfere with collection. Multiple Amazon Web Services (AWS) Data Collection processes as well as other AWS scripts should not be scheduled for the same period.

The following steps must be taken in Amazon Web Services (AWS) before a Data Collector can gain read-only access to retrieve data.

1. Configure an S3 Bucket to receive billing reports. See "Configure an S3 bucket to receive billing reports" on page 516.
2. Select cost allocation tags.See "Select cost allocation tags" on page 517.
3. Create an AWS IAM user and generate access keys.See "Create an AWS IAM user" on page 518.
4. Link AWS acccounts for collection of consolidated billing data.See "Link AWS accounts for Collection of consolidated billing data" on page 523.
5. On the portal, install a collector.
6. On the portal, add a data collector policy.

See "Installation overview (Amazon Web Services - AWS)" on page 524.

Configure an S3 bucket to receive billing reports

In Amazon Web Services (AWS), an S3 Bucket (Simple Storage Service Bucket) must be configured to receive billing reports with resources and tags.

1. Create an **S3 bucket** to collect billing records that will be accessed by the AWS Data Collector.
2. In the AWS Billing and Cost Management Preferences, configure the **S3 bucket** to Receive Billing Records.
3. Copy the text from the AWS-provided sample policy.

   This policy sets the permissions that enable AWS billing to create billing record files in the S3 bucket.

4. In the S3 bucket properties, add a bucket policy by pasting the sample into the policy.
5. Verify the S3 bucket.
6. Select cost allocation tags.

   See "Select cost allocation tags" on page 517.

Select cost allocation tags

The Amazon Web Service (AWS) Data Collector supports the Cost and Usage Reports (CUR) only.

1. Once the S3 bucket for Billing Report is created, configure the report name and the report prefix.

   CUR uses the following Amazon S3 organization and naming conventions.

   - Report-prefix: The prefix you assign to the report.
   - Report-name: The name you assign to the report.
   - yyyymmdd-yyyymmdd: The range of dates that the report covers. Reports are finalized at the end of the date range.
   - assemblyId: An ID that AWS creates each time when the report is updated.
   - file-number: If the update includes a large file, AWS might split it into multiple files. The file-number tracks the different files in an update.
   - CSV: The file format of the report.
   - ZIP / GZ: The type of compression applied to the report files.

2. Select Cost Allocation Tags that have been assigned to your AWS resources so that they appear in the billing report and also so that they will be collected by the Data Collector. Tags are user-defined and enable groupings and totals for billing and reporting.

   User-defined tags are used for collection of EC2 and S3 resources. These tags are required for cost allocation reporting of the total cost of EC2 instances and S3 buckets.

Note: Amazon Web Services generates a report once or more daily, with additions made daily over the month. Therefore, it may take up to 24 hours until a billing records file appears in the S3 bucket that is being collected by the NetBackup IT Analytics Data Collector.

---

3. Create an AWS IAM user.

   See "Create an AWS IAM user" on page 518.

Create an AWS IAM user

Data collection requires an Amazon Web Services (AWS) Identity and Access Management (IAM) user with restricted permissions. This user must have read-only permission to collect billing records from the S3 bucket and also to access the AWS API methods to retrieve data about EC2 resources and any S3 bucket.

See "Link AWS accounts for Collection of consolidated billing data" on page 523.

1. In Amazon Web Services IAM Management Console, create an IAM user, specifically for use by the NetBackup IT Analytics Data Collector.

   Click **Users > Create New Users >** enter a user name.

   Ensure that Generate an access key for each user is selected.

   This configuration results in the following security credentials: Access Key ID and Secret Access Key.

   Note: Ensure to provide mandatory credentials for the required policy probes.

   Note: For more information, See "Mandatory probe user privileges" on page 519.

   ---

2. Download the credentials, which you will need later when configuring a Data Collector Policy.

   These credentials are required when configuring the NetBackup IT Analytics AWS Data Collector Policy. The access key and secret access key will be used by the Data Collector to make read-only requests to AWS APIs.

3. In the IAM window, select the IAM User you just created and grant permissions by attaching the AWS-supplied ReadOnlyAccess policy.

   This read-only policy allows the Data Collector to retrieve data about EC2 resources and S3 buckets.

4. If you want to link AWS accounts, refer to the following.

   See "Link AWS accounts for Collection of consolidated billing data" on page 523.

Mandatory probe user privileges

The IAM users needs certain mandatory user privileges for each probes while executing data collecting from AWS policy.

It is required for IAM user to have one or more policy attached having required Actions.

Below is the sample policy for each probe and all probes.

Note: The character "*" in the attribute `"Resource":"*"` of the below sample policy denotes that the provided privilege's are for all resources in all geographical regions. For providing resource and region specific access, specify the value accordingly.

For all probes

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListAccountAliases",
                "iam:GetAccountAuthorizationDetails",
                "organizations:DescribeOrganization",
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeTags",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeVolumes",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSubnets",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeTags",
```

```
                "glacier:ListVaults",
                "s3:GetBucketLogging",
                "s3:GetBucketTagging",
                "s3:GetBucketPolicy",
                "s3:GetBucketVersioning",
                "s3:GetReplicationConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

For independent probes

- EC2 Details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeTags",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeHosts",
                "ec2:DescribeImages",
                "ec2:DescribeNetworkInterfaces",
                "organizations:DescribeOrganization",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeVolumes",
                "ec2:DescribeAccountAttributes",
```

```
                "iam:ListAccountAliases",
                "iam:GetUser",
                "ec2:DescribeSubnets",
                "iam:GetAccountAuthorizationDetails"
            ],
            "Resource": "*"
        }
    ]
}
```

- S3 Details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "organizations:DescribeOrganization",
                "s3:ListAllMyBuckets",
                "iam:ListAccountAliases",
                "s3:ListBucket",
                "iam:GetUser",
                "iam:GetAccountAuthorizationDetails"
            ],
            "Resource": "*"
        }
    ]
}
```

- Storage Usage

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:GetUser",
                "iam:GetAccountAuthorizationDetails",
```

```
                "organizations:DescribeOrganization",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketTagging",
                "s3:GetBucketLogging",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:GetBucketVersioning",
                "s3:GetBucketPolicy",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeTags",
                "glacier:ListVaults"
            ],
            "Resource": "*"
        }
    ]
}
```

- Billing Records

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "organizations:DescribeOrganization",
                "s3:ListAllMyBuckets",
                "iam:ListAccountAliases",
                "s3:ListBucket",
                "iam:GetUser",
                "iam:GetAccountAuthorizationDetails"
            ],
            "Resource": "*"
        }
```

```
        ]
    }
```

Link AWS accounts for Collection of consolidated billing data

Some large organizations create separate AWS accounts for different cost centers and then link these accounts to a Payer Account. In this case, the billing records for all of these accounts are accumulated in the billing records for the Payer Account. If you want to have a single AWS IAM user to collect these billing records and all other information about EC2 and S3 buckets, you will need to grant the user cross-account API access. By linking accounts, you establish a trust relationship between the accounts.

Ensure that the account used in AWS policy has the user access privilege to perform call to the **describeOrganization** API

Create a role for NetBackup IT Analytics Data Collection

1. Log in to the AWS account that is not the Payer Account.
2. In the AWS IAM window, select **Roles**.
3. Enter a role name that identifies it as the role specifically for data collection, such as readOnlyAccessForCollection. The name you enter cannot be changed once the role is created.
4. Select the Role Type: **Role for Cross-Account Access > Provide access between AWS accounts you own**.
5. Establish Trust using the Account ID of the Payer Account, but do not require the MFA.
6. Attach the AWS-supplied ReadOnlyAccess policy.
7. Before creating the role, review the role information to ensure that the following information is correct:
   - **Role Name**: Role named specifically for NetBackup IT Analytics data collection.
   - **Trusted Entity**: ID of the Payer Account.
   - **Policy**: ReadOnlyAccess.
8. Copy the **Role ARN** to the clipboard. You will use this copied ARN (Amazon Resource Name) when you add the role to the IAM user.

See “Add the role to the IAM user” on page 524.

9. Click **Create Role** to link the accounts.
10. Add the roles to the IAM user.

Add the role to the IAM user

1. Log in to the AWS Payer Account.
2. In the AWS IAM window, select the User that you created.

   See “Create an AWS IAM user” on page 518.
3. Under the user’s permissions, in addition to the ReadOnlyAccess policy that is listed, create an **Inline Policy**.
4. Select Custom Policy and enter a **Policy Name**.
5. Customize permissions by editing the policy, replacing the Resource example (shown in **red** below) with the **Role ARN** that you copied to the clipboard, enclosed in straight quotes.

```
{"Statement":[
  {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource":
"arn:aws:iam::123456789012:role/accessForAPTAURECollector"
  }
 ]
}
```

6. The AWS configuration is now complete. Proceed with the Data Collection Configuration.

Installation overview (Amazon Web Services - AWS)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Amazon Web Services Policy Data Collector policy.
4. On the Data Collector Server, install the Data Collector software.

5. Validate the Data Collector installation.

Add an Amazon Web Services (AWS) policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

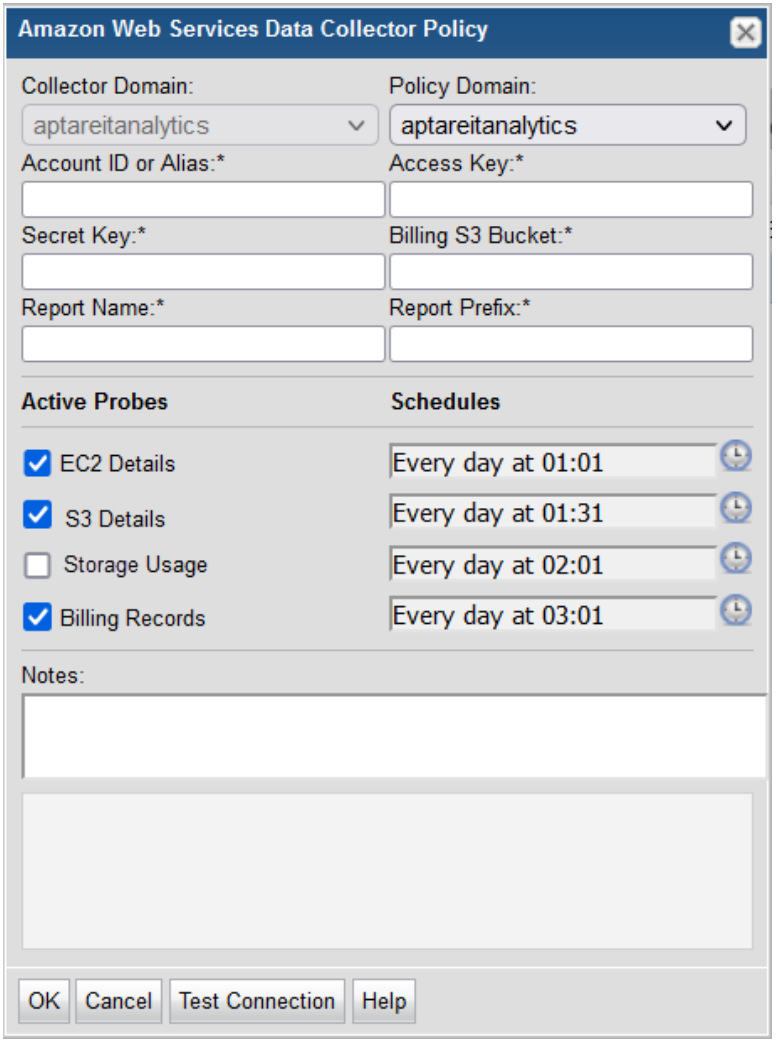
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Note: Due to limitations on API request rates, multiple simultaneous processes may interfere with collection. Multiple Amazon Web Services (AWS) Data Collection processes as well as other AWS scripts should not be scheduled for the same period.

Table 55-1 Amazon Web Services Data Collector Policy

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name select **My Profile** in the User Account menu.
Account ID or Alias	Enter the AWS account ID number, as shown in the AWS Management Console. This is the ID of the account that pays for the Amazon account. If an account alias has been created, it can be used in lieu of the account ID.
Access Key	Enter the access key ID for the AWS IAM user.
Secret Key	Enter the secret access key for the AWS IAM user.
Billing S3 Bucket	This is the name of the S3 bucket that was created to specifically collect billing records for the NetBackup IT Analytics AWS Data Collector policy.
Report Name	The name you have assigned to the billing report in the AWS billing configuration.
Report Prefix	The prefix you have assigned to the billing report in the AWS billing configuration.
EC2 Details	Collect EC2 instances, EBS volumes, and EBS volume snapshots (and the relationships among these objects), including details such as: ■ EC2 instance: name, tags, region, availability zone, when launched, status, type, virtualization, monitoring configuration. ■ EBS volumes: name, tags, region, availability zone, when created, status, type, size. ■ EBS volume snapshots: name, tags, region, when creation started, progress, status, volume size. **Note:** Ensure to provide mandatory credentials for the required policy probes. For more information, See "Mandatory probe user privileges" on page 519.
S3 Details	Collect S3 bucket details, such as name, tags, region, owner, when created, and version information. **Note:** Ensure to provide mandatory credentials for the required policy probes. For more information, See "Mandatory probe user privileges" on page 519.

Table 55-1 Amazon Web Services Data Collector Policy *(continued)*

Field	Description
Storage Usage	Collect S3 storage bucket, EFS, and glacier usages such as number of current objects, total size of current objects, number of versions, total size of all versions, number of delete markers, oldest modified current object, and newest modified current object. **Note:** For buckets that have a large number of objects, this collection may take a long time. Tracking of storage bucket usage is supported in these AWS regions: ■ us-east-1 ■ us-east-2 ■ us-west-1 ■ us-west-2 ■ af-south-1 ■ ap-east-1 ■ ap-south-1 ■ ap-northeast-3 ■ ap-northeast-2 ■ ap-southeast-1 ■ ap-southeast-2 ■ ap-northeast-1 ■ ca-central-1 ■ eu-central-1 ■ eu-west-1 ■ eu-west-2 ■ eu-west-3 ■ eu-south-1 ■ eu-north-1 ■ me-south-1 ■ sa-east-1 ■ us-gov-east-1 ■ us-gov-west-1 **Note:** Ensure to provide mandatory credentials for the required policy probes. For more information, See "Mandatory probe user privileges" on page 519.

Table 55-1 Amazon Web Services Data Collector Policy *(continued)*

Field	Description
Billing Records	Collect all fields from the detailed billing report with resources and tags, such as invoice, resource, payer, linked account, usage type, and costs. **Warning:** The AWS data collection process was suspended from 11.3.0 till 11.4.xx version. If you choose to upgrade the portal with the feature enablement, there is a risk of data loss for the preceding months. Veritas recommends configuring an advanced parameter to recover any lost data during the probe execution. ■ **Advance parameter**: AWS_BILLING_LOOKBACK_MONTHS ■ **Value**: Number of months (numeric value) For instance, if the advanced parameter value is set to 5, data collection will span the previous 5 months as well as the current month. **Note:** Ensure to provide mandatory credentials for the required policy probes. For more information, See "Mandatory probe user privileges" on page 519.
Schedule	**Note:** AWS billing records are updated once or more every 24 hours; therefore, it may take 24 hours after configuring this Data Collector Policy before billing records are available in NetBackup IT Analytics. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Table 55-1 Amazon Web Services Data Collector Policy *(continued)*

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to AWS using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to AWS. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Note: For details about the initial data collection period, refer to the following.

See the section called “Modifying the AWS Collection Period” on page 530.

Modifying the AWS Collection Period

On the first collection of Amazon Web Services (AWS) billing data, the Data Collector collects one month’s worth of data. To override this period, set the AWS_BILLING_LOOKBACK_MONTHS advanced parameter to the number of months of billing history that should be retrieved during the first collection.

Note: To set the parameter, navigate to **Admin** > **Advanced** and then click **Parameters**. Parameters page is displayed.

Chapter 56

Configuration for Google Cloud Platform

This chapter includes the following topics:

- Overview
- Pre-installation setup for GCP
- Prerequisites for adding Data Collectors (GCP)
- Installation GCP
- Adding policy
- Testing the collection
- Creating an IAM role
- Billing Data Access Role
- Cloud API
- Project access

Overview

Google Cloud Platform (GCP) provides infrastructure, platform as a service, and serverless computing environments for business agility.

GCP stores any amount of data and can be retrieved as requested in a secure and customizable services. GCP enables to create and execute virtual machines on Google's infrastructure.

Pre-installation setup for GCP

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (GCP)

- Must have Google account to log in to Google Cloud Platform.
- Must have administrative access to create new projects / existing project.
- Must have an IAM Service Account User and create key in .JSON format which will be used as private key while authentication.

Note: For more information to create IAM Service Account user, See “Creating an IAM role” on page 534.

- Enable Billing Account Access to the service account and enable billing export option.
- The APTARE projects requires the billing API enabled.

Note: For more information on billing API, See “Cloud API” on page 540.

Installation GCP

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the **Google Cloud Platform** Data Collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Adding policy

The following procedure details to add policy to Google Cloud Platform

1. Navigate to **Admin** >> **Data Collection** >> **Collector Administration**.
2. Click **Add Policy** and select **Google Cloud Platform** from cloud column.

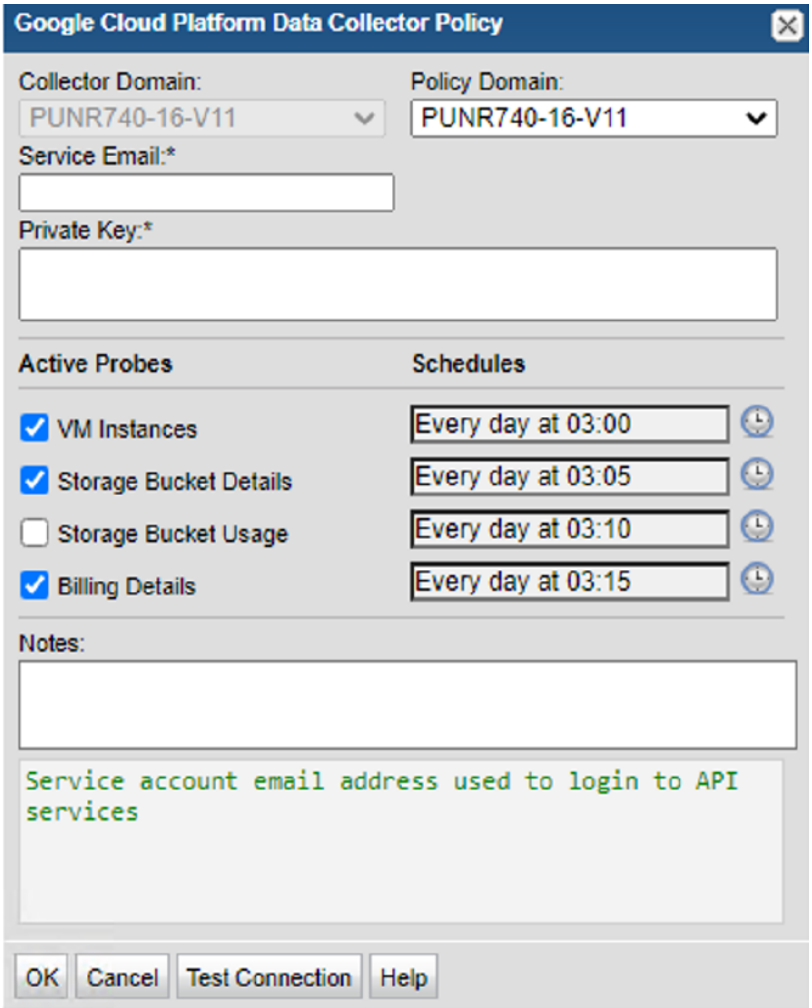


Table 56-1 GCP Data Collector Policy parameters

Field	Description
Service Email*	Client email for the service account which data collector is going to communicate via REST on http / https to collect respective probe data.
Private Key*	Communicating with the Server for REST calls.
Active Probes	The probes which are to be executed. Following are the available options: ■ VM Instances. ■ Storage Bucket Details. ■ Storage Bucket Usage. ■ Billing Details.
Schedule	Relevant schedule at which the probe must trigger.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the Service email and private key supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector

Testing the collection

Verify the connection using **Test Connection**. Once the connection is successful, you can test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**.

This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

Creating an IAM role

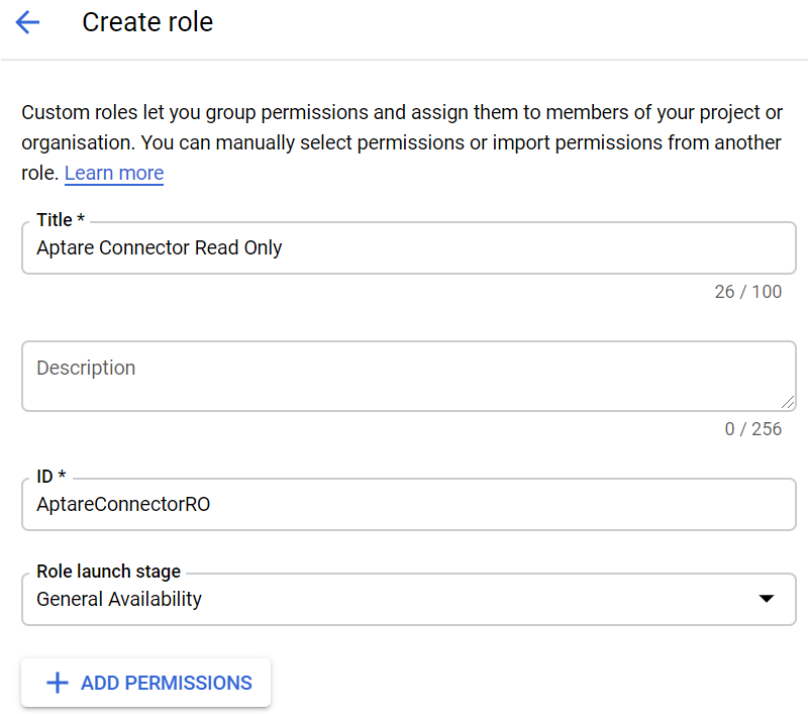
This role is intended to be used at the organization level so that it can be easily shared between projects.

If the collector is intended to only monitor a single project then the role can be added at the project level.

Create a new role.

To create an IAM role

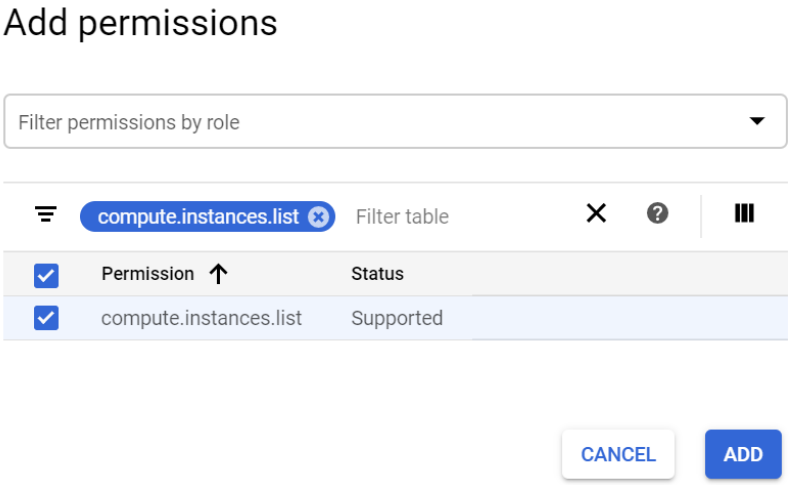
1. Choose the organization from the project selector.
2. Navigate to IAM & Admin > Roles.
3. Choose **CREATE ROLE**.
4. Specify title and description.



Adding permissions to the role

1. After completing the above steps, continue with the following.
2. Select **General Availability**.
3. Click **Add Permissions**.
4. In the **Filter permission by role** field to find and add the following permissions.
   - compute.instances.list
   - compute.machineTypes.get
   - compute.snapshots.list
   - compute.zones.list

- resourcemanager.projects
- .get resourcemanager.projects.list
- storage.buckets.list
- storage.objects.list



Assigning permission to the role

Note: IAM administrative access required to assign the permissions.

Billing Data Access Role

The following process allows to:

- Billing data access role
- Create an IAM Service Account User
- Enable Billing Account Access
- Enable Billing Export

Creating Billing Data Access role

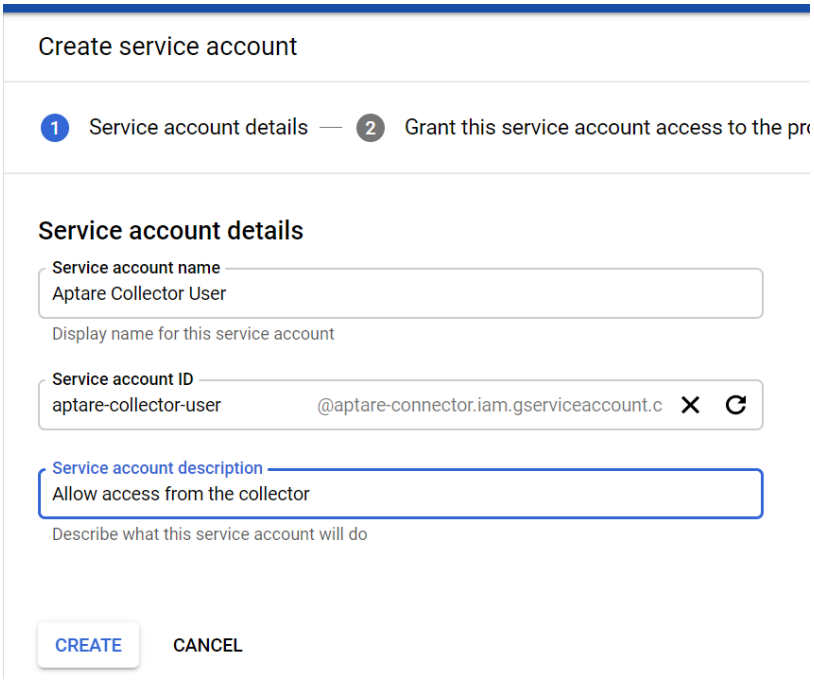
To access billing data tables a role, a user must exist within the master APTARE project. Typically, an administrator user of an individual project will not have permissions to create roles who can access Billing Data records.

1. Select the **Aptare Connector Project**.
2. Select **IAM & ADMIN** > **Roles**.
3. Choose **CREATE ROLE**.
4. Specify title and description.
5. Select **General Availability**.
6. Click **Add Permissions**.
7. Specify **bigquery** in the **Filter permission by role** field to find and add the following permissions.
   - bigquery.datasets.get
   - bigquery.jobs.create
   - bigquery.tables.get
   - bigquery.tables.getData
   - bigquery.tables.list

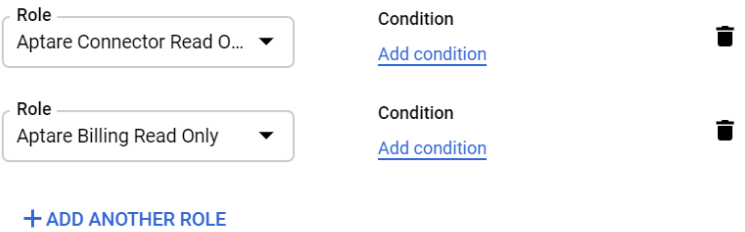
Creating an IAM Service Account User

Create an account used to access GCP from the connector.

1. Select the previously created **Aptare Connector** project.
2. Navigate to **IAM & Admin** > **Service Accounts**.
3. Choose **CREATE SERVICE ACCOUNT**.
4. Specify the required details and click **CREATE**.



5. Choose the **Aptare Connector Read Only**.
6. Click **ADD ANOTHER ROLE** and select the **Aptare Billing Read Only**.

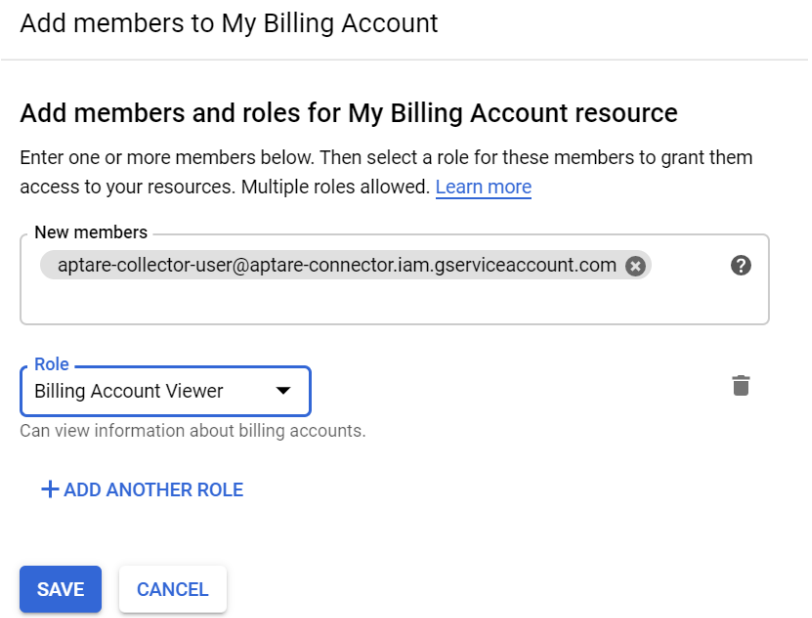


7. Click **CONTINUE**.
8. Click **CREATE KEY** and choose the default JSON format.
9. A .JSON file will be downloaded.
10. Click **CLOSE**.

Enable billing account access

The service account needs access to list the available billing accounts.

1. Navigate to **Billing** > **Manage Billing Accounts**.
2. Select the box next to the billing account which opens the permissions panel on the right side.
3. Click **Add Members**.
4. Specify email address for the service user account.
5. Choose the **Billing Account Viewer** role.
6. Click **Save**.



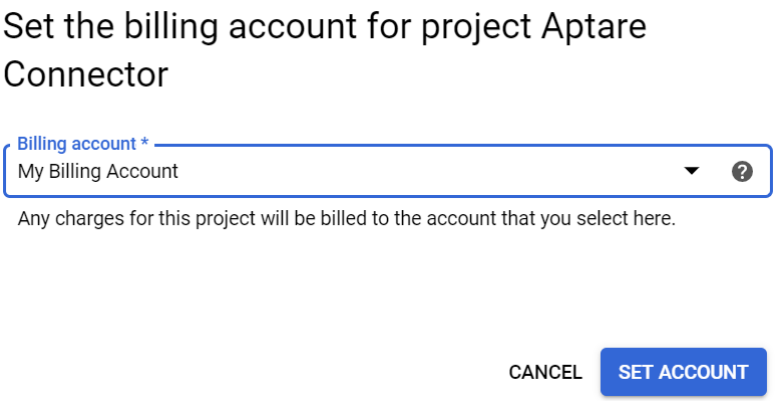
Enable billing export

To collect billing data, the billing account needs to be exported to the 'Aptare Collector Project' using a BigData table.

Following is the procedure to enable billing export option.

1. Navigate to (Big Data) BigQuery
2. Under resources, select **aptare-connector**.

3. Choose **Create Dataset** on the right panel.
4. Specify title and click **Create Dataset**.
5. From the main menu, select **Billing**.
6. Link the project to a Billing Account.



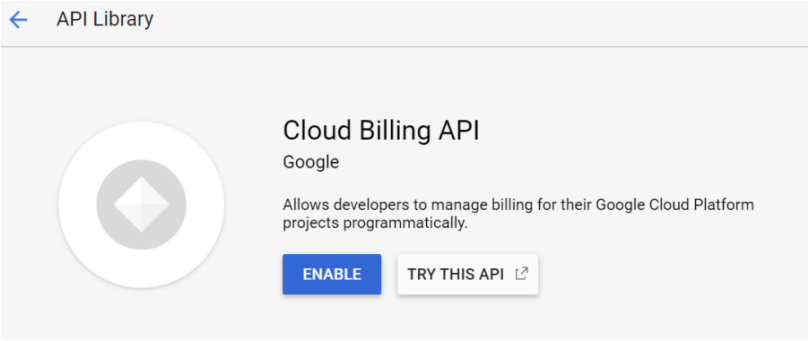
7. Select **Billing Export** from the menu item.
8. Select **BIGQUERY** Export option.
9. Select the project and the data set.
10. Click **SAVE**

Cloud API

The 'Aptare Collector Project' requires the billing API enabled.

The following procedure details to enable cloud API

1. Select the **Aptare Collector Project**.
2. Navigate to **API & Services** > **Library**.
3. Search for the **Billing** API's.
4. Select **Google Cloud Billing API**.



5. Click **ENABLE**.
6. Search for the **Resource** API's.
7. Select **Google Cloud Resource Manager API**.
8. Click **ENABLE**.
9. Search for Compute API's and then select **Google Compute Engine API**.
10. Click **ENABLE**.

Project access

The following procedure details to grant access to the project.

Grant Access to Projects

For each project, the data collector to track, access needs to be granted to the service account.

1. Select the project that you want to monitor.
2. Navigate to **IAM & Admin** > **IAM**.
3. Click **ADD**.
4. Specify the email for the service account previously created.
5. Select **Aptare Collector Read Only** role.
6. Click **SAVE**.

Note: Repeat the above steps for all projects which needs to be tracked.

Chapter 57

Configuration for OpenStack Ceilometer

This chapter includes the following topics:

- Pre-Installation setup for OpenStack Ceilometer
- Prerequisites for adding Data Collectors (OpenStack Ceilometer)
- Installation Overview (OpenStack Ceilometer)
- Adding an OpenStack Ceilometer Data Collector policy

Pre-Installation setup for OpenStack Ceilometer

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (OpenStack Ceilometer)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation Overview (OpenStack Ceilometer)

As a part of cloud-based data collection, NetBackup IT Analytics supports OpenStack Ceilometer, which exposes metrics provided by the various other projects within OpenStack into a common retrieval mechanism for chargeback billing. Note, currently NetBackup IT Analytics only captures metrics for OpenStack Compute (Nova). Ceilometer views are available for use in the SQL Template Designer and the Data Collector policy is classified under Cloud.

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the OpenStack Ceilometer data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

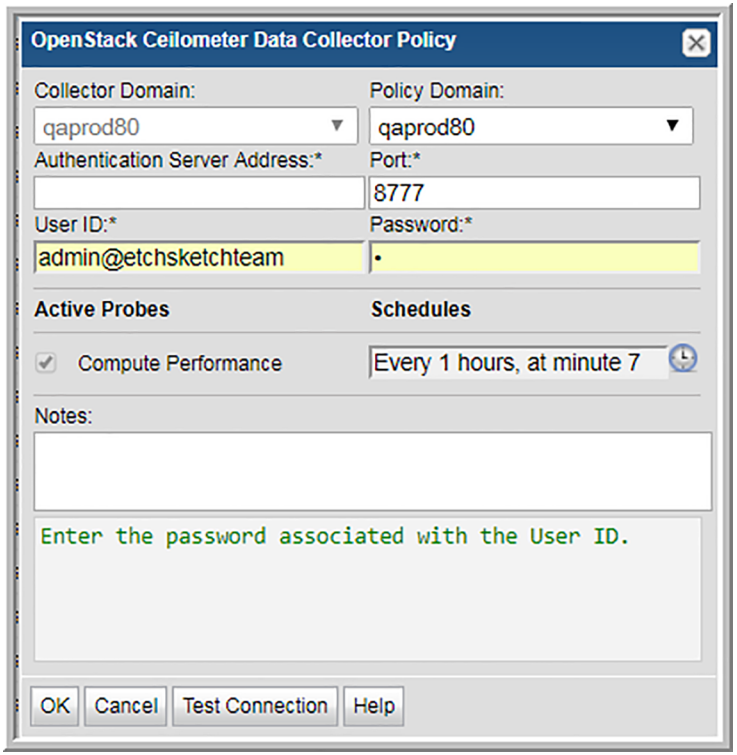
Adding an OpenStack Ceilometer Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Authentication Server Address*	Enter the IP address of the server with Identity Service and port number in the format: <ip address>:<port_number>. The port number is NOT required if you are running on the default port 35357. However, if you are running on a port other than the default, you must specify the port number.
Port	Ceilometer API service port.
User ID*	Enter a user ID that has access to the tenants/projects. This user must have an Admin role, which has access to all projects.
Password*	Enter the password associated with the User ID.
Compute Performance	Collect metrics based on the length of time since the last collection cycle to a maximum of one hour. One collection per hour is the recommended time period.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 58

Configuration for OpenStack Swift

This chapter includes the following topics:

- Pre-Installation setup for OpenStack Swift
- Prerequisites for adding Data Collectors (Dell compellent)
- Installation overview (OpenStack Swift)
- Adding an OpenStack Swift Data Collector policy

Pre-Installation setup for OpenStack Swift

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Dell compellent)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

Installation overview (OpenStack Swift)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the OpenStack Swift data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Adding an OpenStack Swift Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

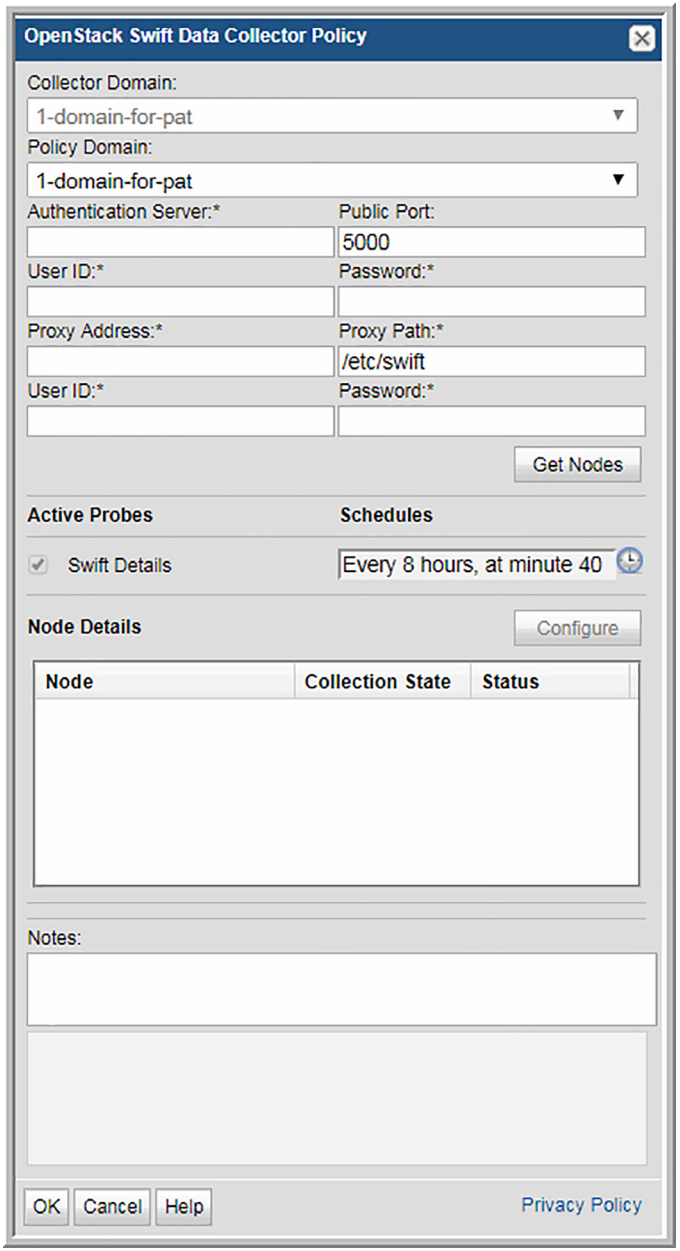
To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Authentication Server*	Enter the IP address of the Authentication Server and port number in the format: <ip address>:<port_number>. For V1, the port number is NOT required if you are running on the default port. However, if you are running on a port other than the default, you must specify the port number. If using V2 authentication, this port number is the Admin port of the authentication server with the default value of 35757.
Public Port	The public port for V2 authentication. Typically, the default value is 5000.
User ID*	Enter a user ID that has access to the tenants/projects. This user must have an Admin role, which has access to all projects. When you click Get Nodes, the credentials are verified to ensure this is a valid user.
Password*	Enter the password associated with the User ID.
Proxy IP*	Enter an IP address or host name for the OpenStack proxy server. This address/name may be the same as what is configured for the Controller.
Proxy Path*	This path identifies the location of the OpenStack Swift configuration files. Default: /etc/swift
User ID*	Enter a user ID for the Swift Proxy server. This user must have super-user root privileges (sudo, sesudo, and pbrun are supported). When you click Get Nodes, an SSH connection is made to the Proxy server and a list of node IP addresses is returned.
Password*	Enter the password associated with the Proxy's User ID.

Field	Description
Get Nodes	When you click **Get Nodes**, the Authentication Server credentials are verified. Next, an SSH connection is made to the Proxy server to return a list of node IP addresses that will be listed in the table. This process can take up to a minute to complete. When this processing is complete, click the **Details** link to list status and any errors, such as authentication failures, that prevented collection of the list of nodes. **Get Nodes** requires that Agent Services are running.
Configure	When you click **Configure**, the Data Collector policy is saved and the Host Inventory window is displayed so that you can take the following actions before collection can take place for the listed nodes: Manage Credentials, Manage Paths, and Manage Access Control. **Note:** Although a list of nodes has been identified, node collection will not complete successfully until all configurations have been set and collection is activated in the Host Inventory window. The following message may appear in the metadata log file, if configurations are not correct: “Could not find a host for this IP address: <ip_address>”
Active Probes	
Schedule	Click the clock icon to create a schedule. By default, it is collected every 8 hours. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Collection State	Values listed for a storage node represent the state of the main Capacity probe for the host: On, Off, or N/A. After the initial Get Nodes action, the state will always be N/A because the Configure step must occur before data collection can be attempted.
Status	Values listed for a storage node represent the status of all probes for the host: Error, Success, or N/A. After the initial Get Nodes action, the state will always be N/A because the Configure step must occur before data collection can be attempted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 59

Configuration for Microsoft Azure

This chapter includes the following topics:

- Pre-Installation setup for Microsoft Azure
- Setting up credentials for Microsoft Azure Data Collection
- Install the Azure PowerShell client on a Windows computer
- Find your tenant and subscription ID
- Register a new application for the Data Collector
- Create a principal and assign role to the application
- Prerequisites for Adding Data Collectors (Microsoft Azure)
- Installation overview (Microsoft Azure)
- Add a Microsoft Azure Data Collector policy
- Reconfigure an Existing Azure Role for Azure Storage Access

Pre-Installation setup for Microsoft Azure

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

As a part of cloud-based data collection, NetBackup IT Analytics supports Microsoft Azure. Policies identify backup, storage accounts, billing and VMs for Azure

resources. To work with Azure, you need one or more Azure subscriptions. Azure reports are available for billing, capacity and virtual machines. Azure database views are available in the SQL Template Designer to construct custom reports. Azure enterprise objects are also defined in the Dynamic Template Designer.

Note: The Data Collector only supports Azure resources deployed with the Resource Manager model.

Setting up credentials for Microsoft Azure Data Collection

To setup credentials for Azure data collection:

1. See "Install the Azure PowerShell client on a Windows computer" on page 554.
2. See "Find your tenant and subscription ID" on page 554.
3. See "Register a new application for the Data Collector" on page 555.
4. See "Create a principal and assign role to the application" on page 556.

Install the Azure PowerShell client on a Windows computer

Use the Azure with Windows PowerShell to access the information required for data collection. You must execute Windows PowerShell as administrator.

To install the Azure Client with Windows PowerShell

1 Navigate to http://go.microsoft.com/fwlink/p/?linkid=320376&clcid=0x409

2 Install and at the prompt enter the following to import modules:

```
Install and at the prompt enter the following to import modules:
Install-Module PowerShellGet -Force
Install-Module -Name AzureRM -AllowClobber
Import-Module -Name AzureRM
```

Find your tenant and subscription ID

1. Execute Azure Windows PowerShell as an administrator.
2. Log into your Azure account:

```
Login-AzureRMAccount
```

3. View the Tenant ID and Subscription ID in the output:

```
Get-AzureRmSubscription
```

Register a new application for the Data Collector

Azure requires a new Application be registered before you can interact with it.

To register a new Application for the Data Collector

You must be logged into your account within Azure Windows PowerShell. The following steps are performed at the Microsoft Azure PowerShell prompt.

1 Set the context using your Tenant ID and Subscription ID by entering:

```
Set-AzureRMContext -SubscriptionId <SUBSCRIPTIONID> -TenantId
<TENANTID>
```

2 Set the Password in a SecureString:

```
$securePwd = ConvertTo-SecureString "<PASSWORD>" -AsPlainText -Force
```

3 Revise the DisplayName, Hostname, and Azure Default Directory. Copy/paste the following at the prompt:

Note: Azure Default Directory can be found in your Azure account under Subscription>Overview.

```
$azureAdApplication = New-AzureRmADApplication -DisplayName
"<DISPLAYNAME>" -HomePage
"https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>" -IdentifierUris
"https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>" -Password
$securePwd -AvailableToOtherTenants $true
```

4 Enter the following to display your application parameters:

```
$azureAdApplication
```

5 Write down the Subscription ID, Tenant ID, Application ID, and the Password you chose. The Application ID is displayed in the output. The Data Collector requires those four parameters.

Create a principal and assign role to the application

To enable access rights to the subscription, assign a combination of the Reader role and a custom Azure Storage read-only RBAC role to the application.

To create a combination of Reader and RBAC role for access:

1. Create a Principal for the application:

```
New-AzureRmADServicePrincipal -ApplicationId <APPLICATIONID>
```

2. Assign a Reader role ot the application. This role is required for Azure Resource Manager (ARM) discovery.

```
New-AzureRmRoleAssignment `
-RoleDefinitionName Reader `
-ServicePrincipalName <APPLICATIONID> `
-Scope "/subscriptions/<SubscriptionID>"
```

3. Create a `.json` file template with the required permissions. The permissions set in this template ensure read-only access to Azure Storage services using RBAC. Storage Account keys are no used.

```
{
"Name": "<Role-Name>",
"Id": null,
"IsCustom": true,
"Description": "<Role Description>",
"Actions": [ "Microsoft.Storage/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/read" ],
"NotActions": [],
"DataActions": [ "Microsoft.Storage/*/read" ],
"NotDataActions": [],
"AssignableScopes": [ "/subscriptions/<Subscription ID>" ]
}
```

4. Create a custom role with `.json` file template .

```
New-AzRoleDefinition -InputFile "C:\CustomRoles\customrole.json"
```

5 Assign the custom role to the application.

```
New-AzureRmRoleAssignment `
-RoleDefinitionName <customRoleName> `
-ServicePrincipalName <APPLICATIONID> `
-Scope "/subscriptions/<SubscriptionID>"
```

6 Add below advance parameter in NetBackup IT Analytics.

- Parameter name: AZURE_STORAGE_AUTH_MODE
- Parameter value: RBAC

Prerequisites for Adding Data Collectors (Microsoft Azure)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Requires Port 443.

Installation overview (Microsoft Azure)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Microsoft Azure data collector policy.
4. On the Data Collector Server, install the Data Collector software.

5. Validate the Data Collector Installation.

Add a Microsoft Azure Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

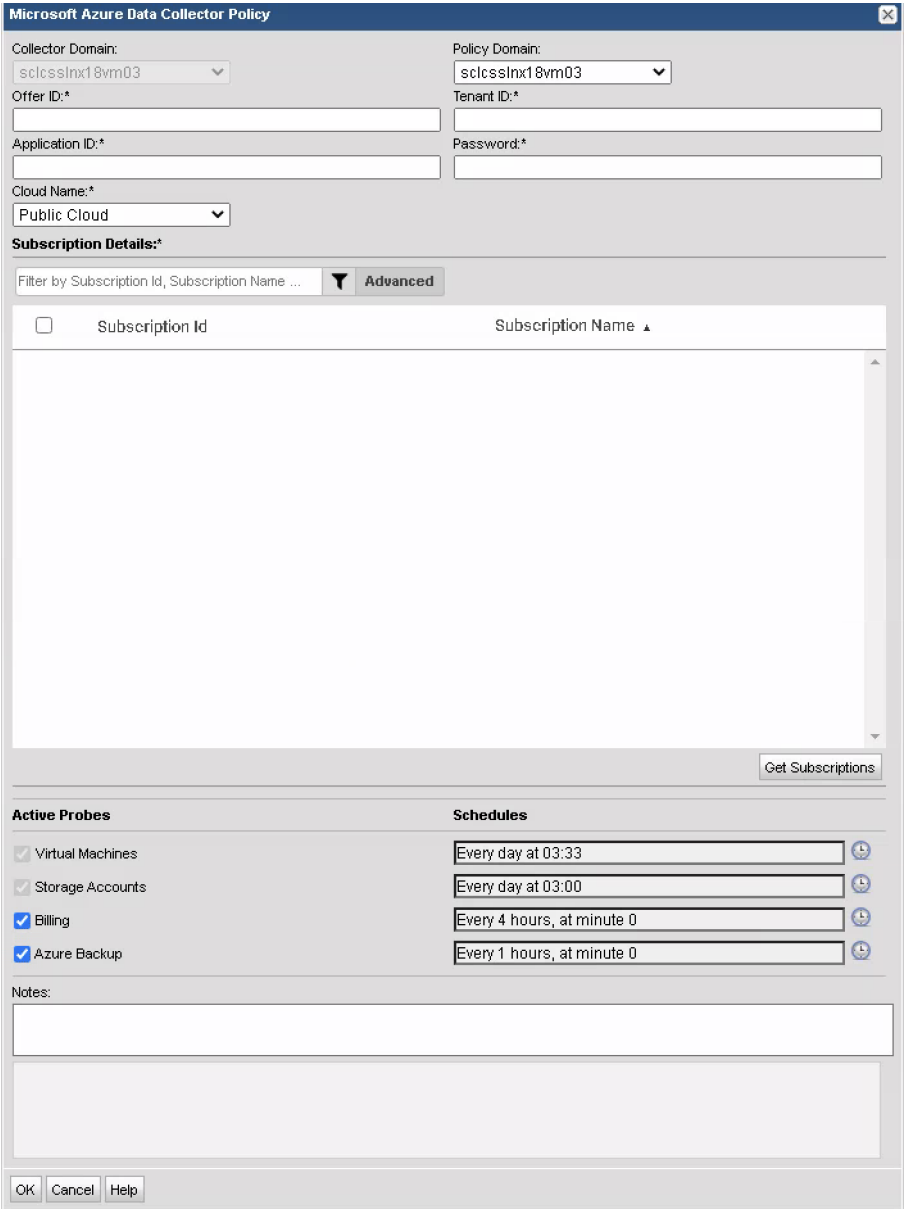
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Offer ID*	Offer ID of your Microsoft Azure Cloud Subscription. To locate your Offer ID, log into your Azure portal and the Offer ID is listed as a parameter under your Subscription service.
Tenant ID*	Tenant ID of your Microsoft Azure Cloud account. Also known as the GUID.
Application ID*	Application ID associated with the registered Microsoft Azure application. Azure requires an application for the data collector to interact with it. Refer to See "To register a new Application for the Data Collector" on page 555.
Password*	Password associated with the Application ID (the registered Microsoft Azure application).
Cloud Name	Select cloud name. **Note:** Default value is **Public Cloud**.
Subscription ID*	Subscription ID of your Microsoft Azure Cloud account. **Note:** A maximum of 105 subscriptions can be selected in a policy.
Subscription Details*	Subscription Details of your Microsoft Azure Cloud account. **Note:** Subscription list will not update automatically. User will have to manually update the list by clicking on the **Get Subscriptions** button, in case a subscription gets added or deleted.
Virtual Machines	Select to set a collection schedule for Azure virtual machines.
Storage Accounts	Select to set a collection schedule for Azure storage accounts.
Billing	Select to set a collection schedule for Azure billing.

Field	Description
Azure Backup	Select to set a collection schedule for Azure Backup.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Reconfigure an Existing Azure Role for Azure Storage Access

This procedure describes how to reconfigure an existing role with Azure RBAC-based authentication for Azure Storage collection without using storage account keys. This procedure allows you to edit the permissions of an existing role and restrict the it with read-only permissions to storage discovery, file shares, and storage data plane.

To reconfigure an existing role with RBAC-based authentication:

1 Create a custom RBAC role (minimal and read-only) using the following .json sample.

```
Azure-Storage-RBAC-ReadOnly.json
{
"properties": {
"roleName": "Azure-Storage-RBAC-ReadOnly",
"description": "Minimum permissions for Azure Storage collection
 using RBAC only (no storage keys).",
"assignableScopes": [
"/subscriptions/<SUBSCRIPTION_ID>"
```

```
],
"permissions": [
{ "actions": [ "Microsoft.Storage/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/read" ],
"notActions": [], "dataActions": [ "Microsoft.Storage/*/read" ],
 "notDataActions": [] }
]
}
}
```

This role gets the following permissions/restrictions:

- ARM read access for storage discovery and file shares.
- Storage data-plane read access for Blob/Queue/Table.
- No access to storage keys.
- No write or delete permissions.

2 Create the role in Azure using CLI:

```
az role definition create \
--role-definition Azure-Storage-RBAC-ReadOnly.json
```

3 Assign the role at Subscription Scope.

If you assign a resource group or a storage account, the scope will cause ARM discovery to fail.

```
az role assignment create \
--assignee <SERVICE_PRINCIPAL_OBJECT_ID> \
--assignee-principal-type ServicePrincipal \
--role "Azure-Storage-RBAC-ReadOnly" \
--scope /subscriptions/<SUBSCRIPTION_ID>
```

4 Add below advance parameter in NetBackup IT Analytics.

- Parameter name: AZURE_STORAGE_AUTH_MODE
- Parameter value: RBAC

Note: To switch to the default mode (ListKey), set the advanced parameter {{AZURE_STORAGE_AUTH_MODE=KEY}} or remove the {{AZURE_STORAGE_AUTH_MODE}} advance parameter.

Section 6

Fabric

- Chapter 60. Configuration for Brocade switch
- Chapter 61. Configuration for Cisco switch
- Chapter 62. Configuration for Brocade Zone alias
- Chapter 63. Configuration for Cisco Zone alias

Chapter 60

Configuration for Brocade switch

This chapter includes the following topics:

- Pre-Installation setup for Brocade switch
- Prerequisites for adding Data Collectors (Brocade switch)
- Upgrade troubleshooting: Brocade BNA SMI-S (CIM) server and Java 11
- Supported switches
- Brocade switches: Default ports and firewall considerations
- Installation overview (Brocade switch)
- Brocade switch Data Collector policy

Pre-Installation setup for Brocade switch

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

Prerequisites for adding Data Collectors (Brocade switch)

General prerequisites:

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- Verify the rpm fontconfig is installed. Fontconfig is a library designed to provide system-wide font configuration, customization and application access. If the rpm fontconfig is not installed, the installer will not be able to load User Interface Mode. This is a prerequisite for a new Data Collector installation.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

While the general requirements to configure the policy are listed above, the prerequisites specific to the collection method are categorized below.

Prerequisites for SMI-S

The following are the prerequisites for is **SMI-S** is selected for **Collection method**:

- A single Data Collector can include all supported switches--Brocade, and Cisco. In fact, this single Data Collector can be used for other enterprise objects, such as backup products and storage arrays.
- The Data Collector accesses the SMI agent server to retrieve data, so the user ID and password for that server is required. This is true only when collection type in policy is SMI-S.
- A single Data Collector can be installed for multiple backup, storage, and fabric products.
- Verify that a host-based SMI agent is installed. The SMI agent must be installed on a host that can communicate with the Fabric. See the relevant switch vendor documentation for details.

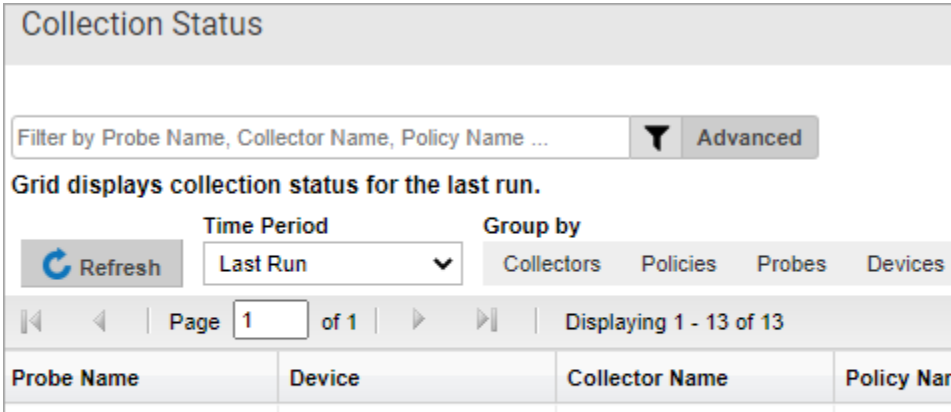
Prerequisites for REST APIs

The following are the prerequisites if **REST API** option is selected for **Collection method**:

- Same user ID and password should be configured on all the switches in the Fabric. Users with Read-Only access can login.
- To collect the Simple Network Management Protocol (SNMP) responses, client must be registered on each Brocade switch from which traps are to be collected.
- In Brocade REST API / *Command Line Interface* Server Address(es), in Brocade Switch Data Collector policy, configure switch IP address / fully qualified switch name.

Note: For Configured Switch, Collector also collects Switch information from all other Switches in the Fabric. Collector uses the same User ID and Password, as configured in the Policy, to connect to other Switches.

- Enable session-based connection. The REST API Collection Method uses session-based approach to connect to the switch. If the login session is successful, it utilizes the session to collect the required data and then logs out to release the session.
- The following URIs should be accessible on Switches:



  - /rest/running/fabric/fabric-switch OR /rest/running/brocade-fabric/fabric-switch
  - /rest/running/switch/fibrechannel-switch OR /rest/running/brocade-fibrechannel-switch/fibrechannel-switch
  - /rest/running/brocade-interface/fibrechannel

- /rest/running/brocade-chassis/chassis
- /rest/running/brocade-fru/blade
- /rest/running/brocade-fibrechannel-trunk/trunk
- /rest/running/brocade-fru/fan
- /rest/running/brocade-fru/power-supply
- /rest/running/brocade-media/media-rdp
- /rest/running/brocade-name-server/fibrechannel-name-server
- /rest/running/zoning/defined-configuration OR /rest/running/brocade-zone/defined-configuration
- /rest/running/zoning/effective-configuration OR /rest/running/brocade-zone/effective-configuration
- /rest/running/brocade-fibrechannel-configuration/fabric
- /rest/brocade-fru/sensor
- /rest/running/brocade-interface/fibrechannel-statistics/
- /rest/running/brocade-chassis/ha-status
- /rest/running/logical-switch/fibrechannel-logical-switch OR /rest/running/brocade-fibrechannel-logical-switch/fibrechannel-logical-switch

Note: The Status column of Collection Status page displays warning message if any of the following URLs is not accessible.

Prerequisites for Command Line Interface method

The following are the prerequisites for **Command Line Interface** option of **Collection method**. This method is supported for Brocade Switch FOS version 7.4.2 and later.

The following are the prerequisites to collect for Switch Details probe: TCP port 22 (all SAN switches)

1. Use IP address of the principal switch only - one principal switch per policy while configuring the Brocade policy.
2. The following list of commands must be accessible:

```
fabricshow, lscfg --show -n, switchshow, dnsConfig -show,
bannershow, uptime, portshow -i %min-index%-%max-index% -f,
ipaddrshow, chassisshow, trunkshow, fanshow, psshow, sfpshow -all,
```

```
 nsshow -t, zoneshow, configure -show, fabricPrincipal --show,
sensorshow, haShow, firmwareshow, islshow, errdump, agshow, ag
-show, licenseshow, configshow, mapsdb -show, seccertmgmt show
-cert https, ldapcfg -show, userconfig --show -a, seccertutil
show, license -show
```

3. Minimum role required is switchadmin with default permissions for all RBAC classes for the Home LF and Chassis Roles:

	Home LF Role	Chassis Role	Remarks
Option-1	switchadmin (default RBAC)	switchadmin (default RBAC)	Works for most deployments, excluding AD and User config data collection (ldapcfg –show & userconfig --show -a will not work and data collection will end with warnings)
Option-2	switchadmin (default RBAC)	admin (default RBAC)	Required for deployments, excluding User config data collection (userconfig --show -a will not work and data collection will end with warnings).
Option-3	admin (default RBAC)	admin (default RBAC)	Covers complete data collection (all commands will be executed, without warnings)

4. If a physical switch chassis is shared between multiple fabrics, create a single NetBackup IT Analytics Data Collector policy (including single principal switch) to avoid overlap. For example, the usplsansw510 & usplsansw520 are considered “shared” physical chassis.

The following are the prerequisites to collect FC Port Statistics using SNMP: UDP port 161 must be accessible from the Data Collector:

1. This account must have a home Virtual Fabric and access to a list of Virtual Fabric IDs.
   - The minimum role required is switchadmin with default set of permissions for all RBAC classes.
   - It is possible to leverage the switchadmin or admin user configured for **Switch details** data collection as long as that user exists on all switches within the fabric (if shared, all fabrics), it has necessary SNMP privileges assigned and the username matches the SNMP v3 account.
2. This account name must match the SNMP V3 username (= SNMP v3 account mentioned in the below section) and comes in addition to the CLI/SSH account used by **Switch details** probe.
3. To retrieve FC Port Statistics from Brocade virtual fabrics / virtual switches:
   - Create a dedicated CLI user account with a role such that it has access to all virtual fabrics.
     - Add the user with the command:

       ```
       userconfig --add <snmp_user> -r <role> -l
       <list_of_virtual_fabric_ids> -h <home_fabric> -c
       <chassis_role>
       ```

     - If the user already exists, use:

       ```
       userconfig --addlf <snmp_user> -l
       <list_of_virtual_fabrics_ids> -r <role>
       ```

4. Configure SNMP (Version 1, 2c or 3) on all the switches:
   - Set the IP address or Subnet in the SNMP access control on all the switches.
   - Configure SNMP v3 account on all the switches.
   - Security Level of v3 (AuthNoPriv, noAuthNoPriv)
5. The following OIDs must be accessible to the SNMP user:

OIDs for IF-MIB	ifIndex, ifHCOutOctets, ifHCInOctets

OIDs for FCMGMT-MID	connUnitPortIndex, connUnitPortStatIndex, connUnitPortNodeWwn, connUnitPortStatCountFBSYFrames, connUnitPortStatCountPBSYFrames, connUnitPortStatCountFRJTFrames, connUnitPortStatCountPRJTFrames, connUnitPortStatCountClass1RxFrames, connUnitPortStatCountClass2RxFrames, connUnitPortStatCountClass3RxFrames, connUnitPortStatCountClass3Discards, connUnitPortStatCountRxMulticastObjects, connUnitPortStatCountTxMulticastObjects, connUnitPortStatCountRxLinkResets, connUnitPortStatCountTxLinkResets, connUnitPortStatCountRxOfflineSequences, connUnitPortStatCountTxOfflineSequences, connUnitPortStatCountLinkFailures, connUnitPortStatCountTxObjects, connUnitPortStatCountInvalidCRC, connUnitPortStatCountInvalidTxWords, connUnitPortStatCountPrimitiveSequenceProtocolErrors, connUnitPortStatCountLossofSignal, connUnitPortStatCountLossofSynchronization, connUnitPortStatCountInvalidOrderedSets, connUnitPortStatCountFramesTooLong, connUnitPortStatCountFramesTruncated, connUnitPortStatCountAddressErrors, connUnitPortStatCountDelimiterErrors, connUnitPortStatCountRxObjects, connUnitPortStatCountEncodingDisparityErrors, connUnitPortStatCountBBCreditZero, connUnitPortStatCountInputBuffersFull
OIDs for SW-MIB	swFCPortIndex, swConnUnitBadEOF, swConnUnitLCRX, swFCPortTxWords, swFCPortRxWords, swFCPortTxFrames, swFCPortRxFrames, swFCPortTooManyRdys, swFCPortNoTxCredits, swFCPortRxEncInFrs, swFCPortRxCrcs, swFCPortRxTruncs, swFCPortRxTooLongs, swFCPortRxBadEofs, swFCPortRxEncOutFrs, swFCPortC3Discards, swFCPortMcastTimedOuts

6. Access to MIBs can be checked using `snmpconfig --show mibcapability` command as follows:
   - `snmpconfig -snmpconfig --show snmpv3` shows the configured user with auth and priv protocol.

- `snmpconfig-show accesscontrol` shows access list configuration.
- `snmpconfig --set accesscontrol` asks prompts to update accesscontrol list and add collector IP or subnet.
- `snmpconfig -show mibcapability` must show sw-mib, if-mib, and fcmgmt-mib as enabled.

Upgrade troubleshooting: Brocade BNA SMI-S (CIM) server and Java 11

With the introduction of support for Java 11, older versions of Brocade BNA may encounter compatibility issues. The following section covers potential workarounds. Collection occurs from the SMI-S (CIM) server component of the BNA the data collector is collecting from. The version of Java used by NetBackup IT Analytics disables some insecure TLS algorithms by default. If collection fails with the following error in the collector logs, the version of Brocade BNA may be incompatible and not allow collection using the TLS algorithms enabled by default with Java 11.

```
Failed to establish JDBC connection to: jdbc:jtds:sqlserver://...
java.sql.SQLException: Network error IOException: null
at net.sourceforge.jtds.jdbc.JtdsConnection.<init>
(JtdsConnection.java:437)
```

Upgrade Brocade BNA to the latest version to enable secure collection. If upgrade is not possible, a workaround can be attempted to restore compatibility. If the following steps do not resolve the issue, your version of Brocade BNA is not supported.

1. Edit <collector install dir>/java/conf/security/java.security.
2. Search for jdk.tls.disabledAlgorithms.
3. Copy the existing lines and comment (to have a backup for easy restore).

```
#jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
#    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

4. One at a time, remove an algorithm from the jdk.tls.disabledAlgorithms and test the collection, starting at the last algorithm and working backward. Stop once you reach an algorithm containing 'keySize <'.

- Remove one algorithm - for example NULL

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
    EC keySize < 224, 3DES_EDE_CBC, anon
```

- Save the file.
- Run `checkinstall` and verify collection succeeds.
- If `checkinstall` does not succeed, restore jdk.tls.disabledAlgorithms to its original state.

5. Change to DH keySize<768 - for example.

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 768, \
EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

- Save the file.
- Run `checkinstall` and verify collection succeeds.

6. If a working configuration is found, restart the collector service.

Supported switches

Refer to the *Certified Configurations Guide* for a complete list.

Brocade switches: Default ports and firewall considerations

The default ports for NetBackup IT Analytics collection of Brocade switch data include:

- HTTP - 5988
- HTTPS - 5989

The following ports are not an NetBackup IT Analytics specific requirement, however, the Brocade SMI agent contacts the switch via RPC on port mapper port 111. Other RPC calls use ports 897 (non-secure) and 898 (secure). If a firewall exists between the Brocade SMI agent and the Brocade fabric, the following ports must be open:

- RPC on port mapper - 111
- RPC (non-secure) - 897

- RPC (secure) - 898

Installation overview (Brocade switch)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Brocade Switch data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector Installation.

Brocade switch Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the Run button on the Collector Administration page action bar. The Run button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.
- If the Collection method is REST API */ Command Line Interface*:
  - Collection Method using Brocade Switch supports Fabric OS version v8.2.1 and above.
  - Collection Method using Command Line Interface supports Brocade Switch version is v7.4.2h and above.
  - If the Indications Probe checkbox is selected, SNMP traps are collected instead of Brocade CIM indications. The following four SW traps are supported:
    - `swFCPortScn`
    - `swStateChangeTrap`

- swDeviceStatusTrap
- swEventTrap

- Once the Indications Probe is running, any change in the SNMP fields of the policy will take about 2 minutes to reflect in the probe.
- In Brocade REST API Server Address(es), in Brocade Switch Data Collector policy, configure switch IP address / fully qualified switch name.
- Configured switch should be accessible. If switch is not accessible, collection fails. When any switch in the fabric is not accessible, collector collects basic information of that switch which it can collect without connecting to the switch.

Note: For Configured Switch, Collector also collects Switch information from all other Switches in the Fabric. Collector uses the same User ID and Password, as configured in the Policy, to connect to other Switches.

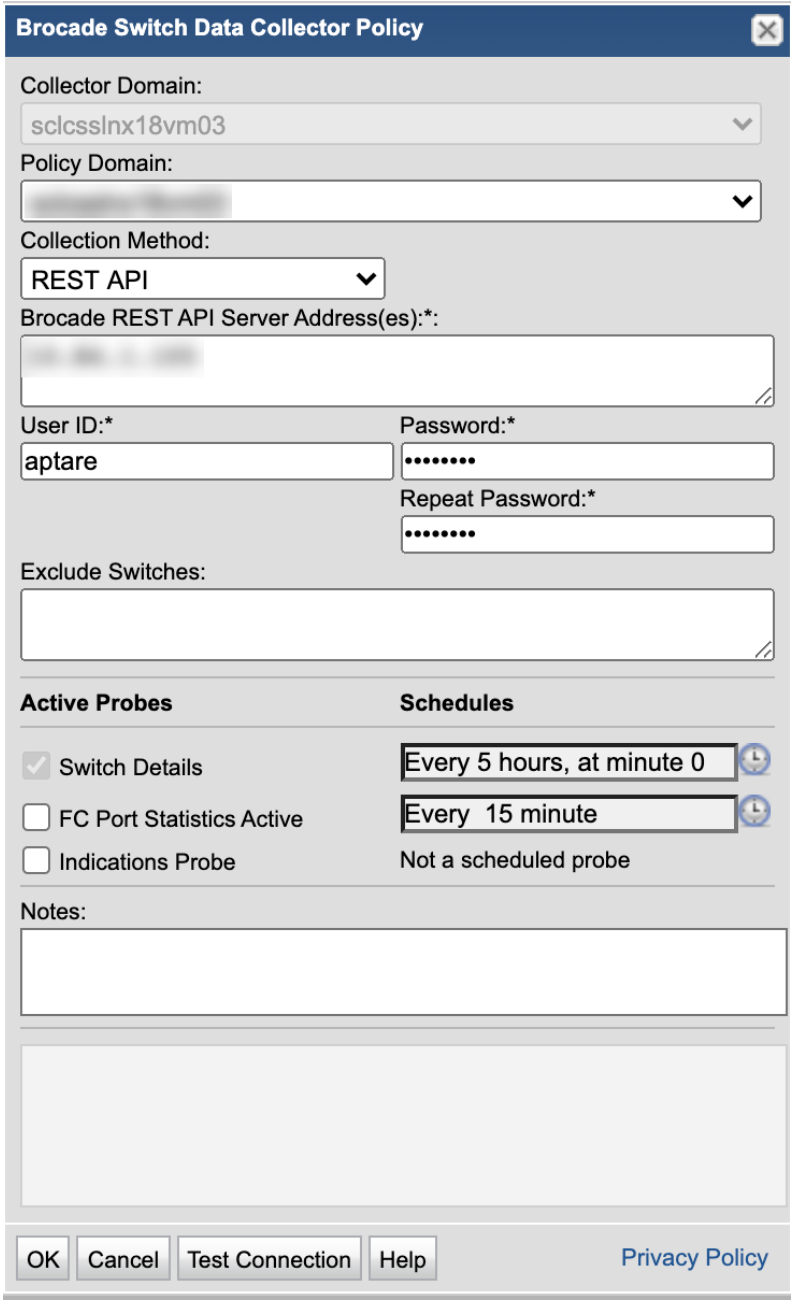
- When the Collection Method is Command Line Interface, add switch IP Address / fully qualified switch name of Principal switch in **Brocade Server Address** field.
- When collection method is Command Line Interface, TCP port 22 and UDP port 161 on Brocade Switch must be open, and those must be accessible to Data Collector.
- While retrieving logical switches, if a switch is not accessible, collector logs a warning message for that switch.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

Best Practices: Interconnected switches should be configured in the same Data Collector policy.


Brocade Switch Data Collector Policy
Collector Domain:
sclcsslnx18vm03
Policy Domain:
Collection Method:
REST API
Brocade REST API Server Address(es):*:
User ID:*
aptare
Password:*
Repeat Password:*
Exclude Switches:
Active Probes
Schedules
Switch Details
Every 5 hours, at minute 0
FC Port Statistics Active
Every 15 minute
Indications Probe
Not a scheduled probe
Notes:
OK
Cancel
Test Connection
Help
Privacy Policy

5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Collection Method	The Collection Method sets the interface to connect to Brocade Switch. The available options are: **1** **SMI-S**: If SMI-S options is selected, specify Brocade SMI agent Address. **2** **REST API**: If REST API option is selected, specify Brocade REST API Server Address(es). **3** **Command Line Interface**: If Command Line Interface is selected, then specify Brocade Switch Server Address.	
Brocade Server Address*:	This field is enabled if Collection Method is Command Line Interface. Specify only one Principal Switch IP address or fully qualified one Switch name for the Brocade Switch. **Note:** The port number is optional. The format should be: <ip_address>[:port_number].	

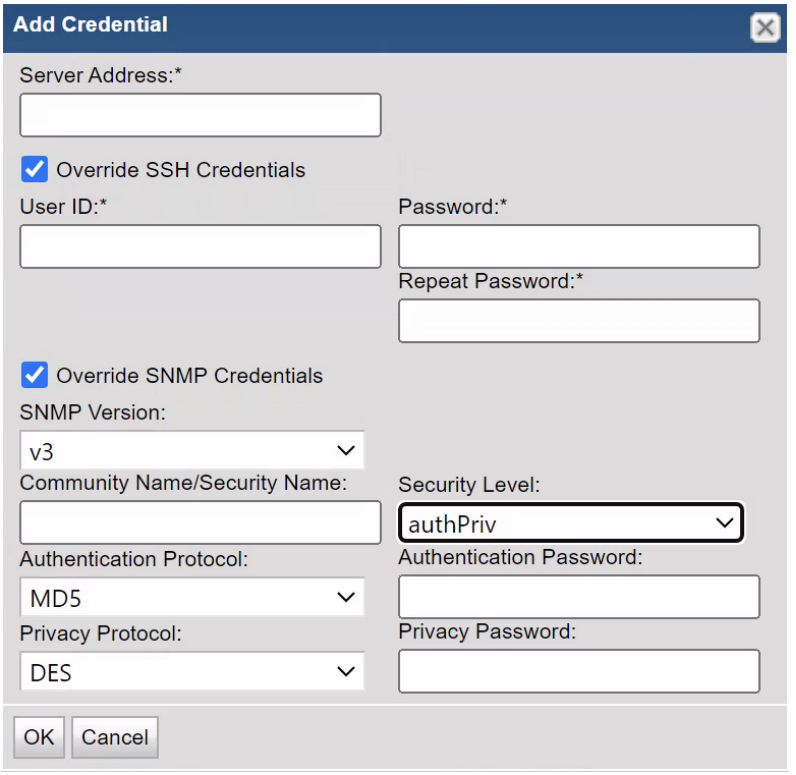
Field	Description	Sample Value
Brocade SMI agent address*	This field is enabled if Collection Method is SMI-S. Enter the IP address of the Brocade SMI agent and port number in the format: <ip_address>:port_number The port number is NOT required if you want to use the default port numbers: 5988 (http) or 5989 (https).	192.1.1.1
Brocade REST API Server Address(es)*	This field is enabled if Collection Method is REST API. Specify the Principal Switch IP address or fully qualified Switch name for the Brocade Switch. **Note:** Port number is optional. The format should be: <ip_address>[:port_number]	192.1.1.1:8080
User ID*	Use the User ID and passcode for accessing the switch. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user.	`Administrator`
Password*	Specify the password. **Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1
Repeat Password	Re-type the password you have specified in the **Password** field.	
Exclude Switches	Enter a switch WWN - e.g., 10:00:00:60:69:90:04:9F, 100000606990049F Colons within the WWN are NOT required. A comma-separated list is supported. **Note:** For the REST API, principal switch cannot be excluded.	10:00:00:60:69:90:04:9F, 100000606990049F
SNMP Version	SNMP version is enabled if the Collection Method is **REST API** and **Indications Probe** / **FC Port Statistics Active** is selected. Select the SNMP version configured on the switch to receive SNMP traps. The available options are: ■ v1 ■ v2c ■ v3	
Indications Probe	■ If collection method is REST API, SNMP traps details are collected. ■ If collection method is SMI-S, CIM indication details are collected.	

Field	Description	Sample Value
Community Name/Security Name	This field is enabled if the Collection Method is REST API and Indications Probe is turned on. Specify the SNMP community name if the SNMP Version is v1/v2c or the SNMP security name if SNMP Version is v3, as configured on the switch.	public, snmpadmin1
Switch Details	Click the check box to collect switch details. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
FC Port statistics Active	Click the check box to collect FC Port statistics. This may have a performance impact, which can be optimized with the FC Port statistics schedule. Click the clock icon to create a schedule.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	
SNMP Port	SNMP port is enabled if the Collection Method is REST API and Indications Probe is turned on. Specify the UDP port number of the collector configured on the switch at which SNMP traps will be received.	8163

Field	Description	Sample Value
Security Level	This field is enabled if the Collection Method is REST API, Indications Probe is turned on and SNMP version is v3. Select the SNMP security level as configured on the switch. The available options are: ■ **noAuthNoPriv**: If noAuthNoPriv option is selected, authentication and privacy are disabled. ■ **authNoPriv**: If authNoPriv option is selected, specify the Authentication Protocol and Authentication Password. Privacy is disabled. ■ **authPriv**: If authPriv option is selected, specify the Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password.	
Authentication Protocol	This field is enabled if the Collection Method is REST API, Indications Probe is turned on and Security Level is authNoPriv or authPriv. Select the SNMP authentication protocol. The available options are: MD5 and SHA	
Authentication Password	This field is enabled if Collection Method is REST API, Indications Probe is turned on and Security Level is authNoPriv. Specify the SNMP authentication password.	Password1
Privacy Protocol	This field is enabled if Indications Probe is turned on and if Security Level is authPriv. Select the SNMP privacy protocol. The available options are: DES and AES128	
Privacy Password	This field is enabled if Indications Probe is turned on and if Security Level is authPriv. Specify the SNMP privacy password.	Password1
Credentials Override	Configure switches to override the default credentials. Click **Add** to add credentials for a switch. Select a switch and click **Edit** to update the credentials. **Note:** To delete the switch credentials, select the appropriate switch and click **Delete** to delete the credentials.	

Field	Description	Sample Value
Test Connection	Test Connection is supported if REST API option is selected as Collection Method. Test connection message displays the details of the Data Collector connected to the switches as configured in the policy.	

6 If the collection method is Command Line Interface (CLI), then the Credentials Override can be added to the policy. Click Add or Edit and specify the parameters.



Field	Description	Sample Value
Server Address	Specify the IP address or fully qualified switch name for the Brocade switch	
Override SSH credentials	Select to enable override for SSH credentials.	

Field	Description	Sample Value
User ID	Specify the User ID.	Administrator
Password / Repeat password	Specify the password. Repeat the same password in the Repeat password field. **Note:** The password is encrypted.	
Override SNMP credentials	Select to enable overriding of the SNMP credentials.	
SNMP version	Select the appropriate SNMP version from the following: ■ V1 ■ V2c ■ V3	
Community name / Security name	■ **Community name**: Specify if the version selected is V1 / V2c. ■ **Security name**: Specify is the version select is V3.	public snmpadmin1
Security level	The field is enabled only if the SNMP version selected is V3. Select the appropriate security level as configured on the switch. Following are the available options: ■ **noAuthNoPriv**: If noAuthNoPriv option is selected, authentication and privacy are disabled. ■ **authNoPriv**: If authNoPriv option is selected, specify the Authentication Protocol and Authentication Password. Privacy is disabled. ■ **authPriv**: If authPriv option is selected, specify the Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password.	
Authentication protocol	The field is enabled if the security level **authNoPriv** or **authPriv** is selected. Select the appropriate SNMP authentication protocol from the following options: ■ MD5 ■ SHA	
Authentication password	Once the authentication protocol is configured, specify the SNMP authentication password.	password1

Field	Description	Sample Value
Privacy protocol	The field is enabled if the security level **authPriv** is selected. Select the appropriate SNMP privacy protocol from the following options: ■ DES ■ AES128	
Privacy password	Once the privacy protocol is configured, specify the SNMP privacy protocol password.	password1

Chapter 61

Configuration for Cisco switch

This chapter includes the following topics:

- Pre-Installation setup for Cisco switch
- Prerequisites for adding Data Collectors (Cisco switch)
- Upgrade troubleshooting: Cisco DCNM SMI-S (CIM) server and Java 11
- Cisco switches: Default ports and firewall considerations
- Installation overview (Cisco switch)
- Cisco switch Data Collection policy
- Before you start Cisco switch Data Collection

Pre-Installation setup for Cisco switch

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Cisco switch)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- A single Data Collector can include all supported switches--Brocade and Cisco. In fact, this single Data Collector can be used for other enterprise objects, such as backup products and storage arrays.
- The Data Collector accesses the SMI agent server to retrieve data, so the user ID and password for that server is required.
- A single Data Collector can be installed for multiple backup, storage, and fabric products.
- For Interconnected Cisco switches: Interconnected switches, which share the same VSAN, must all be configured in the same Data Collector policy.
- Verify that a host-based SMI agent is installed. The SMI agent must be installed on a host that can communicate with the Fabric. See the relevant switch vendor documentation for details.

Upgrade troubleshooting: Cisco DCNM SMI-S (CIM) server and Java 11

With the introduction of support for Java 11, older versions of Cisco DCNM may encounter compatibility issues. The following section covers potential workarounds. Collection occurs from the SMI-S (CIM) server component of the DCNM the data collector is collecting from. The version of Java used by NetBackup IT Analytics disables some insecure TLS algorithms by default. If collection fails with the following error in the collector logs, the version of Cisco DCNM may be incompatible and not allow collection using the TLS algorithms enabled by default with Java 11.

```
Failed to establish JDBC connection to: jdbc:jtds:sqlserver://...
java.sql.SQLException: Network error IOException: null
at net.sourceforge.jtds.jdbc.JtdsConnection.<init>
(JtdsConnection.java:437)
```

Upgrade Cisco DCNM to the latest version to enable secure collection. If upgrade is not possible, a workaround can be attempted to restore compatibility. If the following steps do not resolve the issue, your version of Cisco DCNM is not supported.

1. Edit <collector install dir>/java/conf/security/java.security.
2. Search for jdk.tls.disabledAlgorithms.
3. Copy the existing lines and comment (to have a backup for easy restore).

```
#jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
#    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
DH keySize < 1024, \
    EC keySize < 224, 3DES_EDE_CBC, anon, NULL
```

4. One at a time, remove an algorithm from the jdk.tls.disabledAlgorithms and test the collection, starting at the last algorithm and working backward. Stop once you reach an algorithm containing 'keySize <'.
   - Remove one algorithm - for example NULL

     ```
     jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
     DH keySize < 1024, \
         EC keySize < 224, 3DES_EDE_CBC, anon
     ```

   - Save the file.
   - Run `checkinstall` and verify collection succeeds.
   - If `checkinstall` does not succeed, restore jdk.tls.disabledAlgorithms to its original state.
5. Change to DH keySize<768 - for example.

   ```
   jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA,
   DH keySize < 768, \
   EC keySize < 224, 3DES_EDE_CBC, anon, NULL
   ```

   - Save the file.
   - Run `checkinstall` and verify collection succeeds.
6. If a working configuration is found, restart the collector service.

Cisco switches: Default ports and firewall considerations

The default ports for NetBackup IT Analytics collection of Cisco switch data include:

- HTTP - 5988
- HTTPS - 5989

Installation overview (Cisco switch)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Cisco Switch data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Cisco switch Data Collection policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the Collector Administration page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1 Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.

2 Search for a Collector if required.

3 Select a Data Collector from the list.

4 Click **Add Policy**, and then select the vendor-specific entry in the menu.

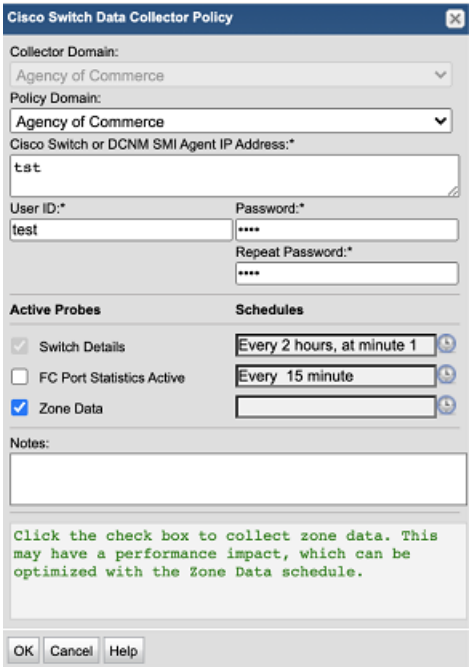
Requirement: Interconnected switches, which share the same VSAN, must be configured in the same Data Collector policy for Cisco Switches.

Note: Data collection for Cisco switches uses SMI, however, a non-default port number is not configurable.

See "Before you start Cisco switch Data Collection" on page 591.

---

5 Specify Data Collector Properties.



6 Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain identifies the top level of your host group hierarchy. The name was supplied during the installation process. All newly discovered hosts are added to the root host group associated with this domain. Typically, only one Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy.	192.1.1.1
Cisco switch or DCNM SMI Agent IP address*	Enter the IP address of the Cisco switch. Multiple switch IP addresses, separated by commas, can be entered for this field. Interconnected switches, which share the same VSAN, must be included in the same Data Collector policy. If you are using the Data Center Network Manager (DCNM) for central control, a separate Data Collector policy is needed for each DCNM. Enter the DCNM SMI agent address (and optionally, its port number) in the format: <ip_address>:<port_number> For DCNM v6.2.x, you will need a valid (or temporary) license in order for the SMI agent to be able to get data.	192.1.1.1
User ID*	Use the User ID and passcode for accessing the switch. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user.	`Administrator`
Password*	**Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Switch Details	Check the box to collect switch details. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
FC Port Statistics Active	Check the box if you want to collect FC Port statistics. This may have a performance impact, which can be optimized with the FC Port schedule.	
Zone Data	Check the box if you want to collect the zone related data. This may have a performance impact, which can be optimized with the zone data schedule.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Before you start Cisco switch Data Collection

The Data Collector uses SMI-S to communicate with the Cisco switches to gather data. To ensure that the SMI-S provider is running, be sure to enable the Common Information Model (CIM) Server on the switch using the following CLI commands:

- cimserver status: To execute this command, you need to be in enable mode.
- show cimserver
- config t - This puts you into configuration mode.
- comserver enable - Once you are in configuration mode, this command turns on the SMI-S provider.

Chapter 62

Configuration for Brocade Zone alias

This chapter includes the following topics:

- Pre-Installation setup for Brocade zone alias
- Prerequisites for adding Data Collectors (Brocade zone alias)
- Brocade switches: Default ports and firewall considerations
- Installation overview (Brocade zone alias)
- Brocade zone alias Data Collector policy

Pre-Installation setup for Brocade zone alias

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Brocade zone alias)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- A single Data Collector can include all supported switches--Brocade and Cisco. In fact, this single Data Collector can be used for other enterprise objects, such as backup products and storage arrays.
- The Data Collector accesses the SMI agent server to retrieve data, so the user ID and password for that server is required.
- A single Data Collector can be installed for multiple backup, storage, and fabric products.
- Verify that a host-based SMI agent is installed. The SMI agent must be installed on a host that can communicate with the Fabric. See the relevant switch vendor documentation for details.

Brocade switches: Default ports and firewall considerations

The default ports for NetBackup IT Analytics collection of Brocade switch data include:

- HTTP - 5988
- HTTPS - 5989

The following ports are not an NetBackup IT Analytics-specific requirement, however, the Brocade SMI agent contacts the switch via RPC on port mapper port 111. Other RPC calls use ports 897 (non-secure) and 898 (secure). If a firewall exists between the Brocade SMI agent and the Brocade fabric, open the following ports:

- RPC on port mapper - 111
- RPC (non-secure) - 897
- RPC (secure) - 898

Installation overview (Brocade zone alias)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Brocade Zone Alias data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

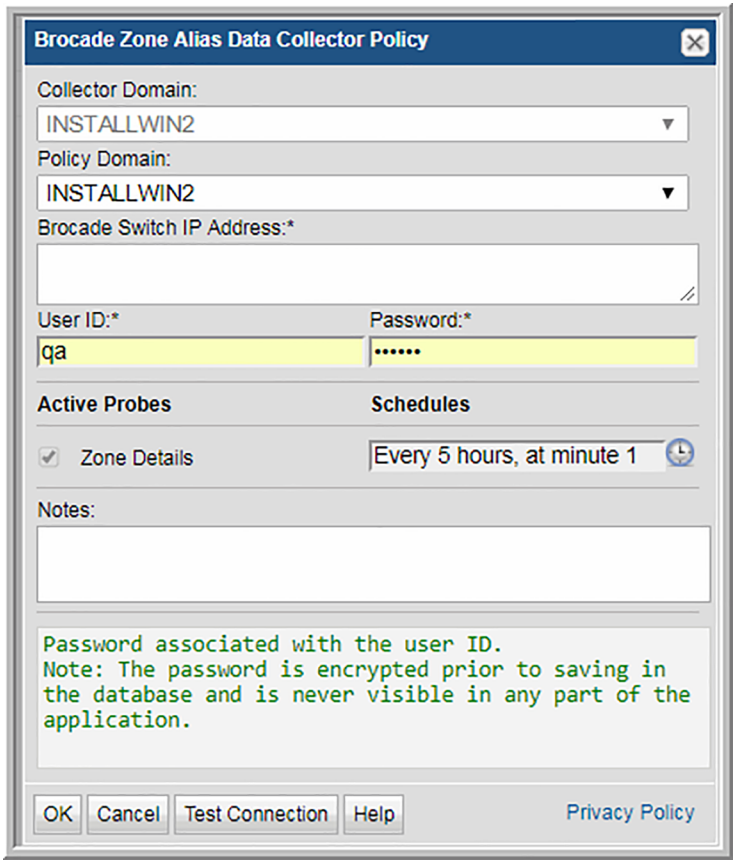
Brocade zone alias Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.
  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

5 Specify Data Collector Properties.



6 Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the host alias policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	`yourdomain`
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	192.1.1.1
Brocade Switch IP Addresses*	Enter the IP address of the Brocade switch. A comma-separated list of addresses may be entered for multiple switches that have the same credentials.	
User ID*	Enter the User ID and passcode for accessing the Brocade switch. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user.	`Administrator`
Password*	Password associated with the user ID. **Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the switches using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the switch. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. Test Connection requires that Agent Services are running.	

Field	Description	Sample Value
Zone Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Chapter 63

Configuration for Cisco Zone alias

This chapter includes the following topics:

- Pre-Installation setup Cisco zone alias
- Prerequisites for adding Data Collectors (Cisco zone alias)
- Cisco switches: Default ports and firewall considerations
- Installation overview (Cisco Zone Alias)
- Cisco zone alias Data Collector policy

Pre-Installation setup Cisco zone alias

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

Prerequisites for adding Data Collectors (Cisco zone alias)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English,

and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- A single Data Collector can include all supported switches--Brocade and Cisco. In fact, this single Data Collector can be used for other enterprise objects, such as backup products and storage arrays.
- The Data Collector accesses the SMI agent server to retrieve data, so the user ID and password for that server is required.
- For Interconnected Cisco switches: Interconnected switches, which share the same VSAN, must all be configured in the same Data Collector policy.
- Verify that a host-based SMI agent is installed. The SMI agent must be installed on a host that can communicate with the Fabric. See the relevant switch vendor documentation for details.

Cisco switches: Default ports and firewall considerations

The default ports for NetBackup IT Analytics collection of Cisco switch data include:

- HTTP - 5988
- HTTPS - 5989

Installation overview (Cisco Zone Alias)

Use the following list to ensure that you complete each step in the order indicated.

1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Cisco Zone Alias data collector policy.
4. On the Data Collector Server, install the Data Collector software.

5. If collecting from Windows hosts, install the WMI Proxy Service on one of the Windows hosts.
6. Validate the Data Collector installation.

Cisco zone alias Data Collector policy

- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

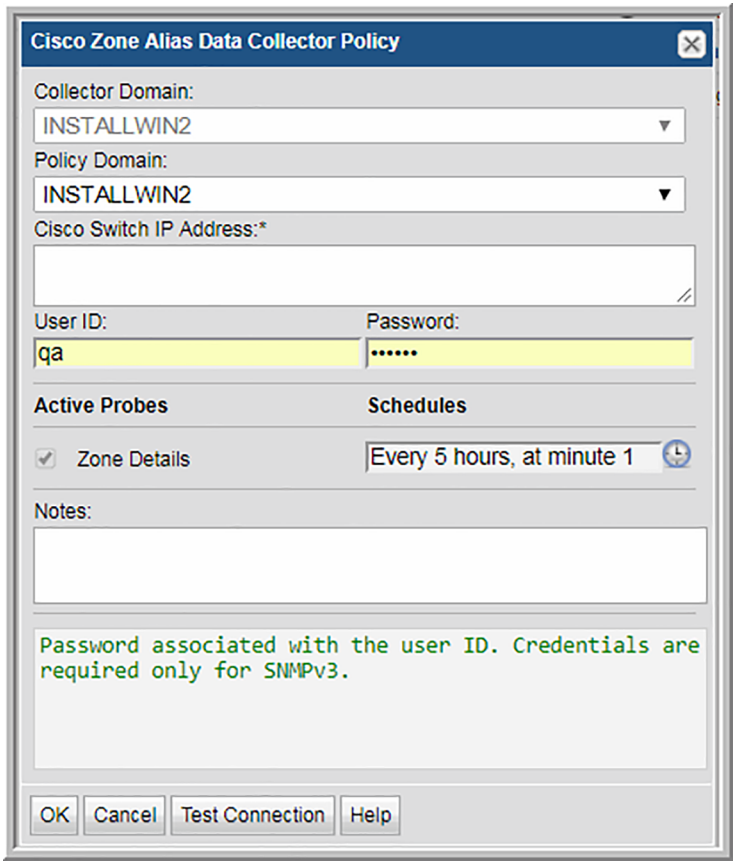
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only displayed if the policy vendor is supported.

  On-demand collection allows you to select which probes and devices to run collection against. This action collects data the same as a scheduled run, plus logging information for troubleshooting purposes. For probe descriptions, refer to the policy.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu**.**

5 Specify Data Collector properties.



6 Add or select the parameters. Mandatory parameters are denoted by an asterisk (*):

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the host alias policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	`yourdomain`
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy.	192.1.1.1
Cisco Switch IP Addresses*	Enter the IP address of the Cisco switch. A comma-separated list of addresses may be entered for multiple switches that have the same credentials.	
User ID	Use the User ID and passcode for accessing the Cisco switch. This typically would be an administrator privilege, but must be a minimum privilege of a view-only user. Credentials are not mandatory because depending on the version of the Cisco switch software, a user ID and password may not be required.	`Administrator`
Password	Password associated with the user ID. Credentials are not mandatory because depending on the version of the Cisco switch software, a user ID and password may not be required. **Note:** The password is encrypted prior to saving in the database and is never visible in any part of the application.	Password1

Field	Description	Sample Value
Zone Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to switches using the IP addresses and credentials supplied in the policy. Credentials are not mandatory because depending on the version of the Cisco switch software, a user ID and password may not be required. This validation process returns either a success message or a list of specific connection errors. Several factors affect the response time of this validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the switch. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. Test Connection requires that Agent Services are running.	

Section 7

File Analytics

- Chapter 64. Configuration for File Analytics
- Chapter 65. File Analytics Export Folder Size and Folder Depth

Chapter 64

Configuration for File Analytics

This chapter includes the following topics:

- Pre-Installation setup for File Analytics
- File Analytics Data Collection overview
- File Analytics Data Collection architecture
- File Analytics Data Collector policies
- Prerequisites for adding Data Collectors (File Analytics)
- CIFS shares
- Host Discovery and Collection File Analytics probe
- Adding a File Analytics Data Collector policy
- Set up FIPS compliant Data Collector for File Analytics

Pre-Installation setup for File Analytics

In most cases, a single instance of the Data Collector can support any number of enterprise objects. However, each environment has its own unique deployment configuration requirements, so it is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires

the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.

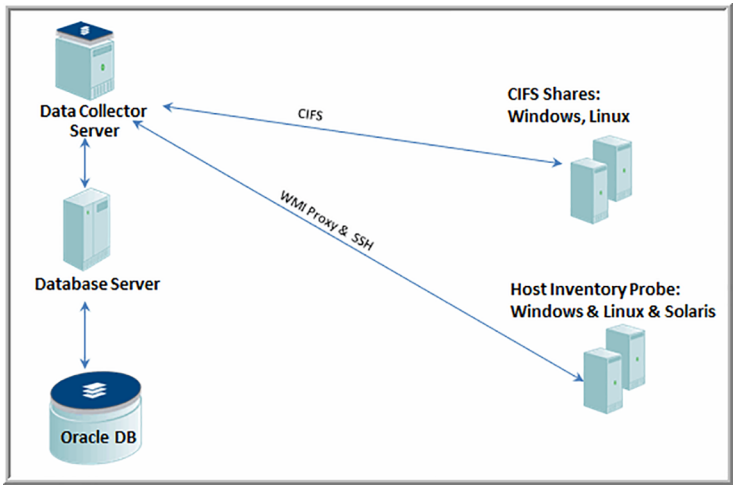
File Analytics Data Collection overview

File Analytics offers a highly optimized, lightweight data collector that uncovers files that are needlessly consuming storage. The bulk of wasted space often can be attributed to unstructured data--that is, files that contain data such as email, word processing documents, presentations, and digital media. Unlike structured data, which is managed by database administrators, unstructured data tends to proliferate with reckless abandon, resulting in stagnant and duplicated data. To assess the value of data files, whether they are critical to operations or are merely forgotten files, File Analytics provides data profiling. This data classification enables aggregation of file types and data growth forecasting. In addition, storage administrators can make archiving decisions based on the age of the data and its relevance to business objectives.

Once data collection completes, a number of reports provide insight into file profiles in your enterprise. Using built-in categorization and also file categories that you can customize, File Analytics becomes part of your arsenal of storage management tools. File Analytics aggregates the data, making it easy for you to identify offenders, such as:

- Deduplication candidates
- File ownership (or lack thereof)
- Largest files
- File Categories (Top file types by volume)

File Analytics Data Collection architecture



File Analytics Data Collector policies

File Analytics data collection can be configured in different ways, depending on the location of the files you want to profile in your enterprise. Determine which of the following approaches is relevant for your environment:

- Create a File Analytics Data Collector policy to configure a file shares probe. This Data Collector traverses the network CIFS shares to collect and categorize filesystem storage consumption metadata. This highly optimized traversal profiles unstructured data to enable you to identify storage that can be reclaimed. Use this for any CIFS share that is serving up files that you want to profile, regardless of manufacturer of the appliance.
- Host Discovery and Collection option directly interrogates hosts' attached storage to profile files. Configure a host probe for Windows (WMI Proxy) and Linux (SSH) collection of a host's locally attached storage.
  See "Host Discovery and Collection File Analytics probe" on page 609.
- Create a Veritas NetBackup Collection policy and configure File Analytics in it to collect file information of backed up clients from the NetBackup Primary Server. Refer to the *Configuring File Analytics in NetBackup Data Collector Policy* section of the *Data Collector installation Guide for Backup Manager* for the configuration steps.

Prerequisites for adding Data Collectors (File Analytics)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

CIFS shares

- This Data Collector can collect both Linux and Windows shares. The recommended Windows Data Collector server operating system is Windows Server. See the *Data Collector Supported Operating Systems* sections of the *NetBackup IT Analytics Certified Configurations Guide* for supported OS versions.
- The Windows LAN Manager authentication level, in the local security policy security options, must be modified to: Send LM & NTLM - use NTLMv2 session security if negotiated. This allows the Data Collector to invoke the **net use** command with the password supplied on the command line. Without this setting, later versions of Windows will terminate with a system error 86 (invalid password).
- Windows CIFS Shares collection requires the Windows Domain User ID. This User ID must have Administrative privileges.
- Linux CIFS Shares collection requires super-user root privileges. Access control commands, such as sudo, sesudo, and pbrun are also supported. If using any of the access control commands, verify that the User ID has sudo, sesudo, or pbrun privileges.
- Collection of owner data for Windows and CIFS is configurable via Advanced Parameters. Data collection completes faster when owner data is not collected (the default). Although not recommended, you can configure an Advanced Parameter, FA_RESOLVE_OWNERS set to Y, to enable owner collection. To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Host Discovery and Collection File Analytics probe

Using Host Resources data collection, hosts are discovered and added to the Host Discovery and Collection list. Once a host is listed in the inventory, it can be selected and the File Analytics probe can be configured. To access the Host Inventory to enable File Analytics probes: **Admin > Data Collection > Host Discovery and Collection**

Note that by design, File Analytics host resources data collection occurs via activation of the probe in the Host Discovery and Collection window in the Portal.

File Analytics Probe Configurations by operating system

Refer to the *Certified Configurations Guide* for complete details.

Windows servers: A Domain Administrator user ID is required when collecting file-level data for File Analytics.

Linux servers: Linux is only supported with the following requirements:

- Root user access is supported.
- Non-root user access with sudo access control is supported.
- Non-root user access without sudo is not supported.
- Running collection with a sudo user on a Linux server requires the addition of an access control command for the server in the Host Discovery and Collection's Manage Access Control window: **Admin > Data Collection > Host Discovery and Collection**
  Also, an advanced parameter must be created: FA_USE_SUDO set to Y.
  To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Both Windows and Linux servers

If running collection via the checkinstall utility, verify the following:

- An advanced parameter must be created: FA_HOST_VALIDATE set to Y. To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Best practices for host Inventory File Analytics probes

Since most environments have hundreds, even thousands of hosts, it is recommended that File Analytics probes be configured in a staggered schedule so as not to overload the Data Collector server.

Adding a File Analytics Data Collector policy

One of the types of data collection that can be configured for File Analytics is collection of CIFS shares. The Data Collector will take the configuration that you specify, including the share names and credentials, and then traverse the file system structure to identify these shared resources on your network and collect the relevant metadata.

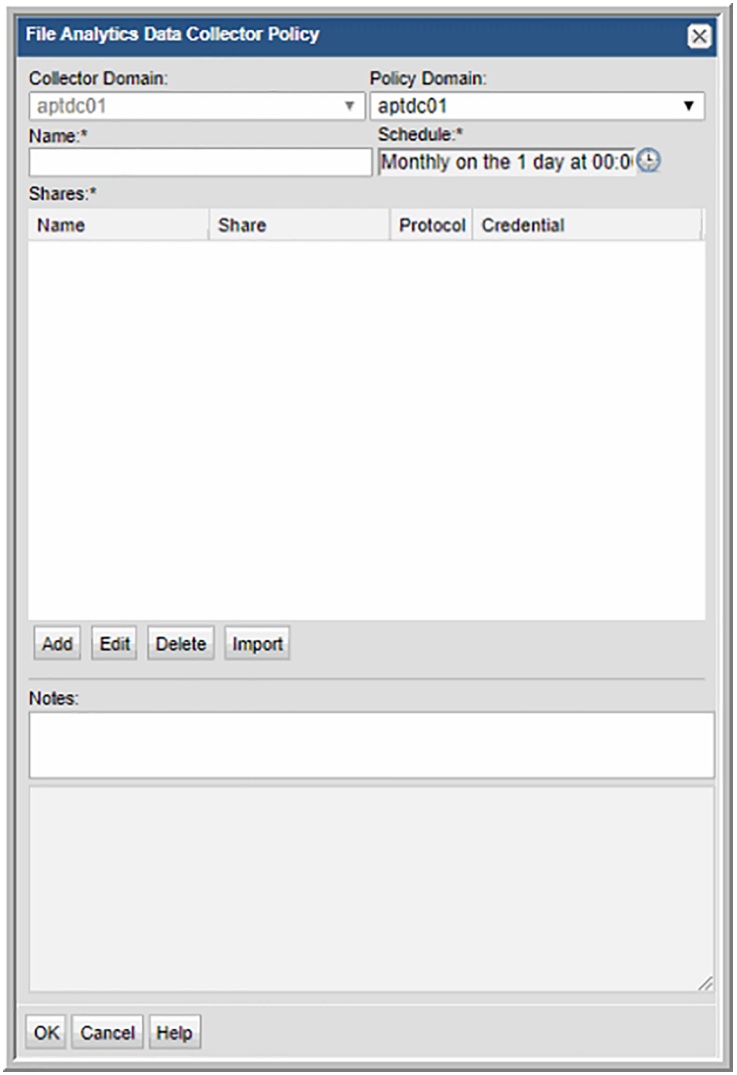
Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

To add the policy

1. Select **Admin > Data Collection > Collector Administration**. Currently configured Portal Data Collectors are displayed.
2. Search for a Collector if required.
3. Select a Data Collector from the list.

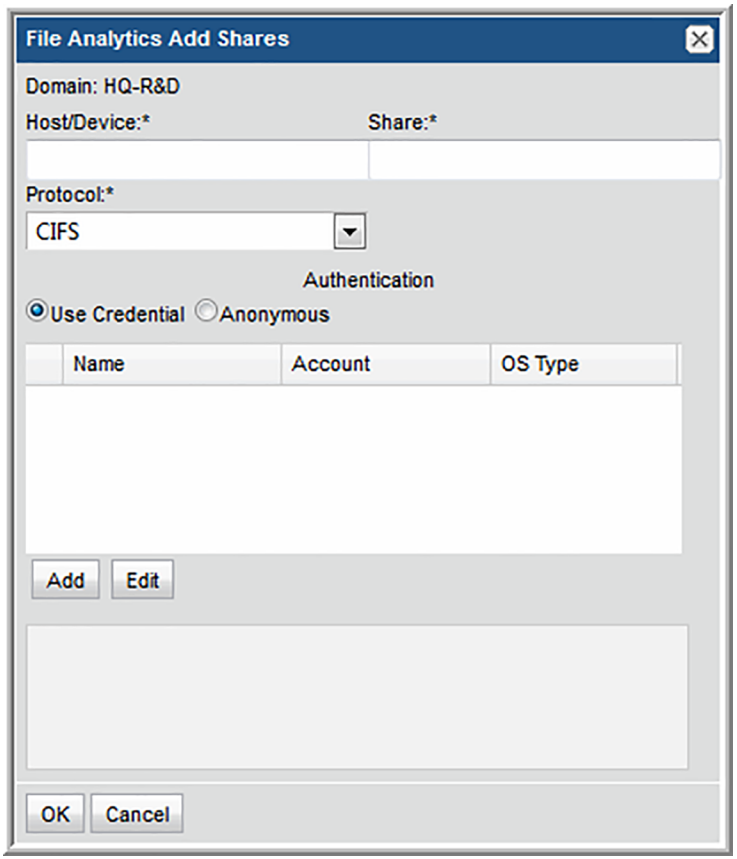
4 Click **Add Policy**, and then select File Analytics policy.



5 Enter or select the parameters. Mandatory parameters are denoted by an asterisk (*):

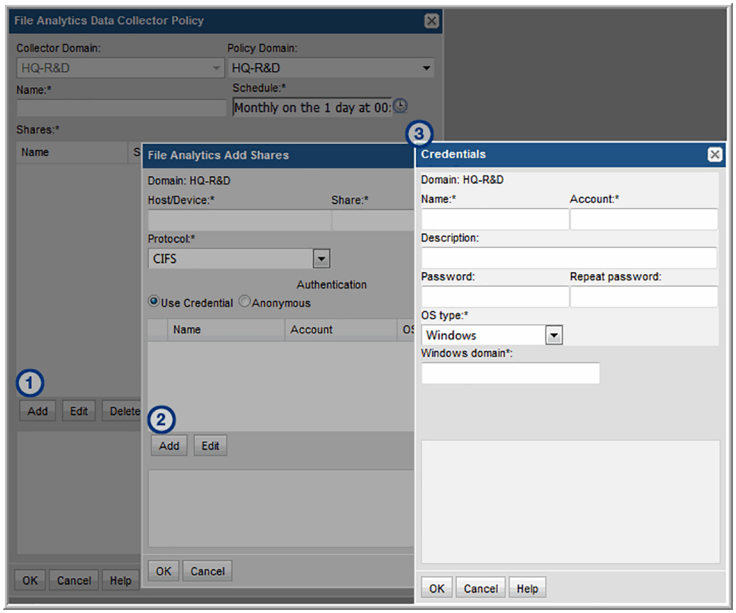
Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Name*	Enter a name that will be displayed in the list of Data Collector policies.
Schedule*	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Shares*	Click **Add** to configure the CIFS shares that the collector will probe. Click **Edit** to modify a CIFS share configuration. Note that the Import button in this window enables bulk loading of CIFS shares. See “Importing the CIFS share configuration” on page 615.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Enter or select CIFS shares configuration parameters in the **File Analytics Shares** window.



Field	Description	Sample Value
Host/Device*	Enter the host IP address or host name for the device that is being probed for CIFS shares. This also could be a non-host device, such as a NetApp array.	**172.1.1.1**
Share*	Enter the name of the CIFS share that the Data Collector will probe.	HOME
Protocol*	CIFS is currently the only option.	
Authentication	Click either Anonymous or Use Credentials. If you are using credentials, click **Add** to configure the CIFS share credentials, or select an existing credential definition and click **Edit**.	

7 Enter credentials in the **Credentials** window.



Field	Description	Sample Value
Name*	Assign a name to identify the set of credentials that you are defining.	
Account*	Enter the login account name used to log in to the hosts. If the policy includes a group of Windows hosts, use the Windows Domain user ID. This user ID must have administrative privileges. For Linux hosts, super-user root privileges are required. You also could use an access control command, such as sudo, sesudo, or pbrun. If using any of these access commands, ensure that the user ID has sudo, sesudo, or pbrun privileges. Some enterprises prefer to create a new user and provide access to commands via an access control command.	root
Description	Enter a note to help identify the credential.	
Password	Enter the password for the account	
OS Type*	Select either Windows, Linux, or NAS	
Windows Domain*	For Windows hosts only: Specify the Windows domain name. If the host is not a member of a domain, or to specify a local user account, use a period (.)	

Field	Description	Sample Value
Private Key File	For Linux hosts only: If you have configured a Public/Private Key between your Data Collector server and the hosts you intend to monitor, specify the location of the Private Key file on the Data Collector Server.	
Known Hosts File	For Linux hosts only: If you have configured a Public Key/Private Key between your Data Collector server and the hosts you intend to monitor, specify the location of the Known Hosts file on the Data Collector Server.	

8 Click **OK** to close and save the configuration in each window.

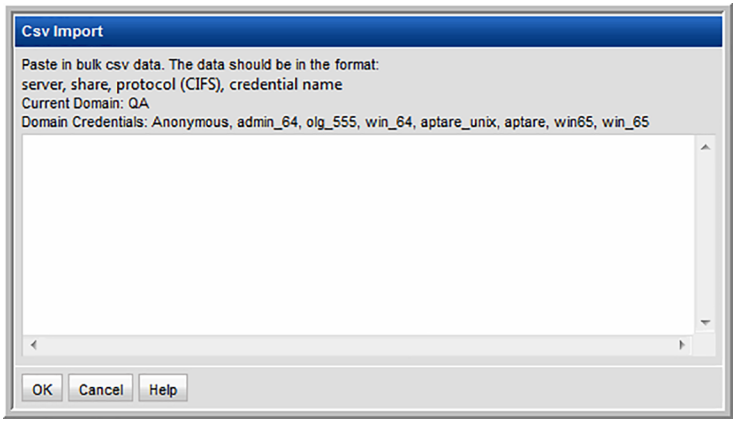
Importing the CIFS share configuration

The import feature facilitates entry of a large number of CIFS shares. Simply paste the details in comma-separated format into the window and click **OK**.

Data Format:

```
host, share, protocol (CIFS), credential name
```

The Credential Names, already configured for the current Domain, are displayed at the top of the window.



Set up FIPS compliant Data Collector for File Analytics

To become FIPS 140-2 compliant, you must configure the Data Collector for File Analytics as recommended below:

1. To enable FIPS compliance, you must install the Data Collector on a FIPS-compliant system.
2. Ensure that the Data Collector and the target Windows file server both are configured in FIPS mode.
3. Specify **vers=2** as the protocol version used between the collector and the target system.
4. Ensure Kerberos authentication is used on the target system.

Note: Steps to set up Windows file server in FIPS and Kerberos are beyond the scope of this document. You can refer the relevant product documentation for the same.

Chapter 65

File Analytics Export Folder Size and Folder Depth

This chapter includes the following topics:

- Extracting File Analytics export folder size
- Specifying the File Analytics folder depth

Extracting File Analytics export folder size

To extract the first-level folder size information from the File Analytics database:

1. At the Linux command prompt, run the following command:

```
 java -classpath
/opt/aptare/portal/WEB-INF/lib/*:/opt/aptare/portal/WEB-INF/classes/
 -DAPTARE_HOME="<ita-install-path>/aptare"
com.aptare.sc.service.fa.FaSubDirectoryReport
```

   where the value of `APTARE_HOME` property is the absolute path of the `aptare` directory.

   For example:

```
 java -classpath
/opt/aptare/portal/WEB-INF/lib/*:/opt/aptare/portal/WEB-INF/classes/
 -DAPTARE_HOME="/opt/aptare"
com.aptare.sc.service.fa.FaSubDirectoryReport
```

   This generates an output file: **report.csv**

Output format:

```
Server Name, Volume Name, Folder name, Size in MB, Last Modified
```

Where:

- Folder name: The root-level folders in the volume
- Size in MB: Sum of all the file sizes in the folder (recursively)
- Last Modified: Maximum modified time stamp from within all the files in the folder (recursively)

Specifying the File Analytics folder depth

A parameter, **Dfa.export**, is available to specify folder depth for File Analytics.

- To specify the folder depth for the report summary, add the following parameter when executing the command `-Dfa.export.folderDepth=x` where `"x"` is the depth. By default the depth is set to 1.
- To turn off reporting on parents, add the following parameter when executing the command `-Dfa.export.includeParents=No`. By default reporting on parents is turned on.
- To specify the name of the output file use `-Dfa.export.reportFileName=SomeReportName.csv`. If this parameter is not specified the default output file will be report.csv.

For example:

```
java -classpath  /opt/aptare/portal/WEB-INF/lib/*:/opt/aptare/portal/
WEB-INF/classes/ -Dfa.export.folderDepth=2 -Dfa.export.includeParents=No
-Dtest.resourceLocation=opt/aptare/portal/WEB-INF/classes/
com.aptare.sc.service.fa.FaSubDirectoryReport
```

Sample Directory Structures and Results

As an example, the table that follows, uses these directory structures to show the results of different parameter values:

- D1
- D1/SD1
- D1/SD1/SD2
- D2/SD3
- D3

This table illustrates the expected results given the different parameter values:

Table 65-1

fa.export.folder Depth	fa.export.include Parents	Directories Included in Report
0	N/A	D1 D2 D3
1	N/A	D1 D1/SD1 D2 D2/SD3 D3
2	No	D1/SD1 D1/SD1/SD2 D2/SD3 D3

Section 8

Data Collection Validation and Troubleshooting

- Chapter 66. Validate data collection
- Chapter 67. Data Collector Troubleshooting
- Chapter 68. Uninstalling the Data Collector

Chapter 66

Validate data collection

This chapter includes the following topics:

- Validation methods
- Data Collectors: Vendor-Specific validation methods
- Working with on-demand Data Collection
- Collect historic data on-demand
- Using the CLI check install utility
- List Data Collector configurations

Validation methods

Validation methods are initiated differently based on subsystem vendor associated with the Data Collector policy, but perform essentially the same functions. Refer to the following table for vendor-specific validation methods.

- Test Connection - Initiates a connection attempt directly from a data collector policy screen that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors.
- On-Demand data collection run - Initiates an immediate end-to-end run of the collection process from the Portal without waiting for the scheduled launch. This on-demand run also serves to validate the policy and its values (the same as Test Connection), providing a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. This is initiated at the policy-level from **Admin>Data Collection>Collector Administration.**
  See “Working with on-demand Data Collection” on page 624.

- CLI Checkinstall Utility- This legacy command line utility performs both the Test Connection function and On-Demand data collection run from the Data Collector server.
  See "Using the CLI check install utility" on page 631.

Note: NetBackup IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

Data Collectors: Vendor-Specific validation methods

Table 66-1 Vendor-specific validation requirements.

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Amazon Web Services (AWS)	x	x	
Brocade Switch		x	
Brocade Zone Alias	x	x	
Cisco Switch		x	
Cisco Zone Alias	x	x	
Cohesity DataProtect	x	x	
Commvault Simpana			x
Compute Resources	x		
Dell Compellent			x
Dell EMC Elastic Cloud Storage (ECS)	x	x	
Dell EMC NetWorker Backup & Recovery	x		
Dell PowerProtect Data Manager	x	x	x
Dell EMC Unity	x	x	
EMC Avamar		x	
EMC Data Domain Backup	x	x	

Table 66-1 Vendor-specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
EMC Data Domain Storage	x	x	
EMC Isilon		x	
EMC Symmetrix	x	x	
EMC VNX	x	x	
EMC VNX Celerra			x
EMC VPLEX			x
EMC XtremIO	x	x	
HDS HCP	x	x	
HDS HNAS		x	
HP 3PAR			x
HP Data Protector			x
HP EVA			x
HPE Nimble Storage	x	x	
Hitachi Block			x
Hitachi Content Platform (HCP)	x	x	
Hitachi NAS	x	x	
IBM Enterprise			x
IBM SVC			x
IBM Spectrum Protect (TSM)		x	
IBM VIO	x	x	
IBM XIV			x
Microsoft Azure	x	x	
Microsoft Hyper-V	x	x	
Microsoft Windows Server	x	x	

Table 66-1 Vendor-specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
NAKIVO Backup & Replication	x	x	
NetApp E Series			x
Netapp		x	
Netapp Cluster Mode		x	
OpenStack Ceilometer	x	x	
OpenStack Swift	x Test Connection is included with the Get Nodes function.	x	
Oracle Recovery Manager (RMAN)	x	x	
Pure FlashArray	x	x	
Rubrik Cloud Data Management	x	x	
VMWare			x
Veeam Backup & Replication	x	x	
Veritas Backup Exec			x
Veritas NetBackup	x	x	
Veritas NetBackup Appliance	X	x	

Working with on-demand Data Collection

Collections can run on a schedule or on-demand using the **Run** button on the action bar. On-demand allows you to select which probes and devices to run. The on-demand run collects data just like a scheduled run plus additional logging information for troubleshooting. A stopped Policy still allows an on-demand collection run, provided the policy is assigned to one of the specified vendors and the collector is online.

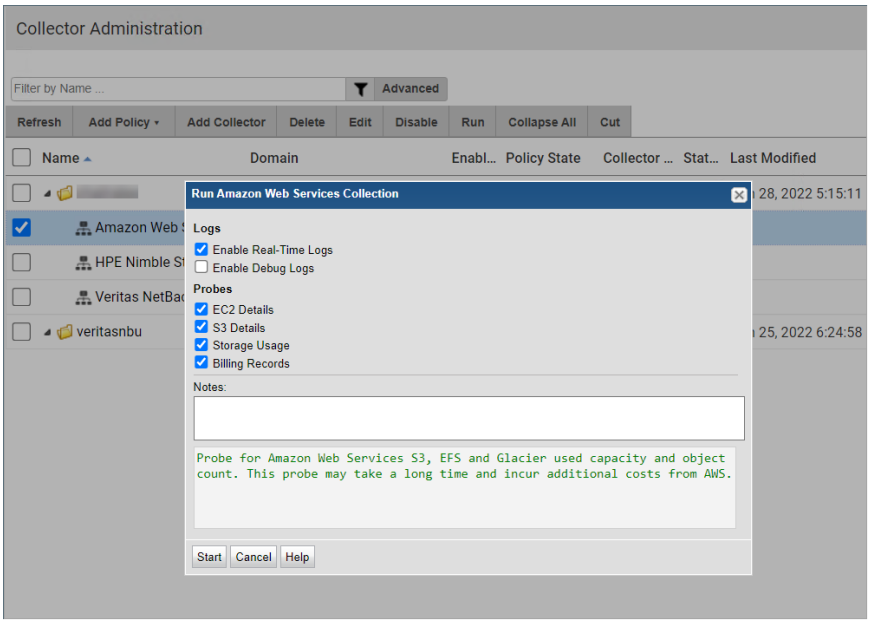
Note: On-demand data collection is not available for all policies.

On-Demand data collection serves multiple purposes. You can use it to:

- Validate the collection process is working end-to-end when you create a data collector policy
- Launch an immediate run of the collection process without waiting for the scheduled run
- Populate your database with new/fresh data
- Choose to view the collection logs on the portal while performing an on-demand run.

To initiate an on-demand data collection

1. Select **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Click **Expand All** to browse for a policy or use **Search**.
3. Select a data collector policy from the list. If the vendor is supported, the **Run** button is displayed on the action bar.
4. Click **Run**. A dialog allowing you to select servers and individual probes to test the collection run is displayed. The following example shows the Amazon Web Services dialog. See the vendor specific content for details on probes and servers.



5 Select the servers and probes for data collection.

6 The portal enables the user to log the messages at various level during the collection process. Following are the available options:

- **Enable Real-Time Logs**: This option enables the user to log generally useful information in real-time when the collection is in progress, select **Enable Real-Time Logs**.
- **Enable Debug Logs**: This option enables the user to log information at a granular level, select **Enable Debug Logs**

7 Click **Start**. Data is collected just like a scheduled run plus additional logging information for troubleshooting. Once started, you can monitor the status of the run through to completion.

Note: If there is another data collection run currently in progress when you click **Start**, the On-Demand run will wait to start until the in-progress run is completed.

See "View real-time logging during an on-demand collection" on page 626.

See "Generating debug level logs during an on-demand collection" on page 627.

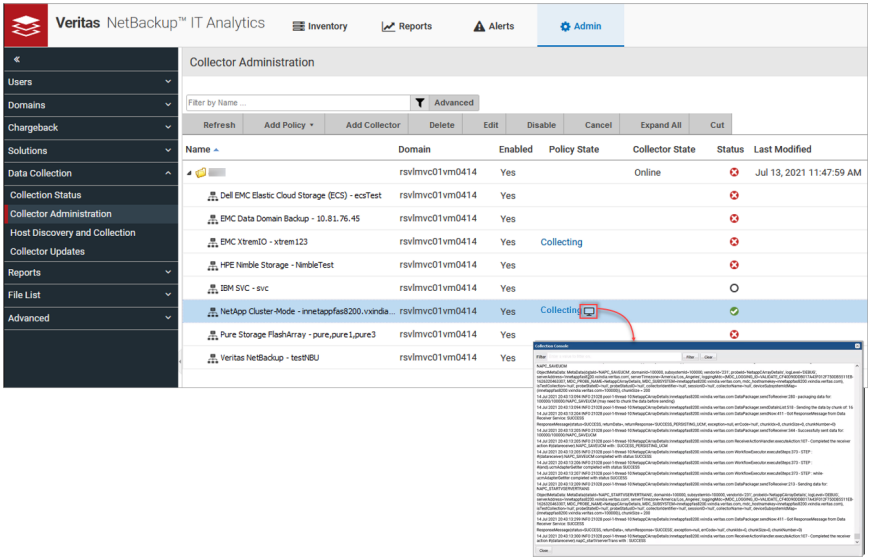
View real-time logging during an on-demand collection

By default, real-time logging is enabled when you initiate an on-demand collection for a data collector. **Admin** > **Data Collection** > **Collector Administration** provides a window to view the logs in real-time as the collection progresses.

The following steps help you to view the real-time logging:

1. Go to **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Initiate an on-demand data collection as described under Working with on-demand Data Collection with **Enable Real-Time Logs** selected.

   The **Policy State** column displays status as **Collecting** and an icon to open the **Collection Console** pop-up.
3. Click the icon next to the **Collecting** link to view the real-time logs in the **Collection Console**. Real-time logs are visible as long as the data collection is in progress and the **Collection Console** is open.



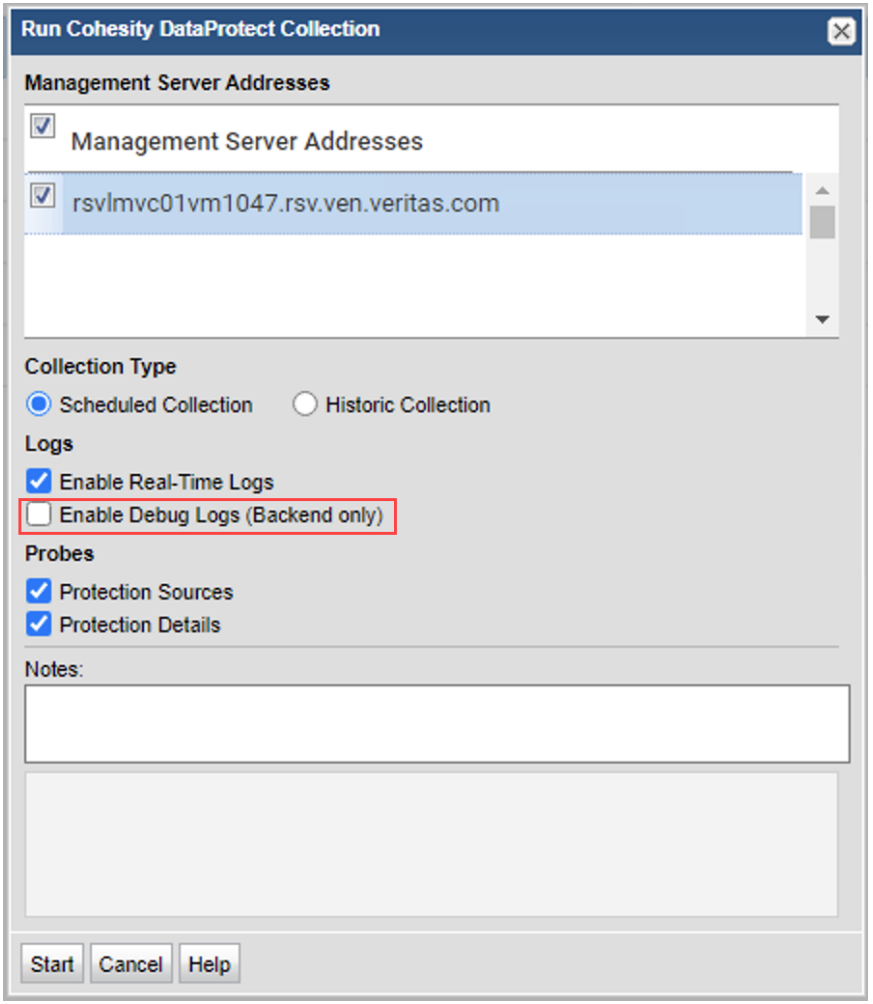
   You can use the filter on the console to selectively view the logs of your choice. The **Collection Console** icon is not visible if the data collection is not in progress.

Generating debug level logs during an on-demand collection

By default, **Enable Debug Logs (Backend only)** option is not selected when you initiate an on-demand collection for a data collector. The **Collector Administration** provides a window to generate debug level information as the collection progresses.

The following steps to enable debug level log file generation:

1. Go to **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Initiate an on-demand data collection as described under Working with on-demand Data Collection with **Enable Debug logs (Backend only)** option selected.



Note: The path for generated log file on data collector server:
`<APTARE_HOME>/mbs/logs/validation/`

Collect historic data on-demand

You can follow this procedure to run an on-demand historic data collection of the supported vendor policies and load historic events on the NetBackup IT Analytics Portal.

Ensure you have an existing supported vendor policy configured with a Data Collector and the Data Collector must be online before you initiate a on-demand historic data collection.

Table 66-2 Supported vendors for historic data collection

Vendor name	Supported collection
Veritas NetBackup	Date range
Cohesity	Time period (in hours) and date range

To initiate a on-demand historic data collection:

1. Select **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Click **Expand All** to browse for a supported vendor policy or use **Search**.
3. Select the supported data collector policy from the list.
4. From the action bar, click **Run**. A dialog allowing you to select individual probes and servers to run the collection is displayed. See the vendor specific content for details on probes and servers.

   A dialog allowing you to specify the collection type is displayed.



5 Select **Historic Collection** and specify other details based on the field descriptions below:

NetBackup Primary Servers (for NetBackup policies) Management Server Addresses (for Cohesity policies)	Select the servers from which the policy must collect the historic data.
Probes	Applicable probes are enabled by default. If you disable any probes, ensure you keep at least one probe in enabled state.
Time Period	The on-demand function retrieves historic data collected within the duration specified under this.
Lookback Hours (for Cohesity policies)	Enter the duration in hours. The moment you initiate the on-demand collection, historic data from the collection performed within the Lookback Hours is retrieved, based on the policy and the probe.
Start Date and Time	Specify the start date and time of the historic data collection.
End Date and Time	Specify the end date and time of the historic data collection.
Client Names (for NetBackup policies)	Specify one or more client names for NetBackup historic collection. Separate the names by commas. This field appears if only one primary server is selected in **NetBackup Primary Servers**.
Notes	Enter your comments about the on-demand historic data collection.

Note: The Start Date/Time and End Date/Time are calculated based on the time zone of the server specified while adding the primary server on the policy screen. Also, the Scheduled Collection interface remains disabled until the on-demand collection is in progress.

6 Click **Start**. Data is collected just like a scheduled run plus additional logging information for troubleshooting. You can monitor the collection progress of the run through **Collection Status** page. The collection is queued if another data collection run is in progress.

Using the CLI check install utility

This legacy utility performs both the Test Connection function and On-Demand data collection run from a command line interface launched from the Data Collector server.

Note: NetBackup IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

The following directions assume that the Data Collector files have been installed in their default location:

- **Windows**:`C:\Program Files\Veritas\AnalyticsCollector`
- **Linux**:`/usr/openv/analyticscollector`

If you have installed the files in a different directory, make the necessary path translations in the following instructions.

Note: Some of the following commands can take up to several hours, depending on the size of your enterprise.

To run Checkinstall

1 Open a session on the Data Collector server.

Windows: Open a command prompt window.

Linux: Open a terminal/SSH session logged in as root to the **Data Collector Server**.

2 Change to the directory where you'll run the validation script.

Windows: At the command prompt, type:

```
cd C:\Program Files\Veritas\AnalyticsCollector <enter>
```

Linux: In the SSH session, type:

```
cd /usr/openv/analyticscollector <enter>
```

3 Execute the validation script.

Windows: At the command prompt, type: `checkinstall.bat` <enter>

Linux: In the SSH session. type: `./checkinstall.sh` <enter>

The **checkinstall** utility performs a high-level check of the installation, including a check for the domain, host group and URL, Data Collector policy and database connectivity. For a component check, specifically for Host Resources, run the **hostresourcedetail.sh|bat**utility.

This utility fails if :

- The Data Collector policy has **NOT** been configured in the Portal.
  OR
- The version of the Data Collector **doesn't match** with the version of NetBackup IT Analytics Portal.

To upgrade Data Collector version to match with the version of NetBackup IT Analytics Portal.

Login to portal.

Navigating to *Admin* > *Data Collection* > *Collector Updates* page.

Trigger the upgrade.

Ensure that the Data Collector services are online.

Checkinstall includes an option to run a probe for one or more specific devices. Note that certain Data Collectors will not allow individual selection of devices. Typically these are collectors that allow the entry of multiple server addresses or ranges of addresses in a single text box.

These collectors include: Cisco Switch, EMC Data Domain, EMC VNX arrays, HP 3PAR, IBM XIV arrays and VMware.

Data Collectors that probe all devices that are attached to a management server also do not allow individual selection of devices: EMC Symmetric, File Analytics, Hitachi arrays and IBM VIO.

4 If the output in the previous steps contains the word **FAILED** and the reason of failure is **NOT** because of version mismatch, then contact Support and have the following files ready for review:

- **Windows**: `C:\Program Files\Veritas\AnalyticsCollector\mbs\logs\validation\`
- **Linux**: `/usr/openv/analyticscollector/mbs/logs/validation/`

List Data Collector configurations

Use this utility to list the various child threads and their configurations encapsulated within a data collector configuration. This utility can be used in conjunction with other scripts, such as **checkinstall.[sh|bat]**.

On Linux: **./listcollectors.sh**

On Windows: **listcollectors.bat**

Chapter 67

Data Collector Troubleshooting

This chapter includes the following topics:

- Resolving Data Collectors connections issues - Linux specific
- Resolving Data Collectors connections issues - Windows specific
- Portal upgrade performance issues
- Verify the Data Collector configuration
- Verify Connectivity
- Configuring web proxy updates
- Collecting missed events for Veritas Backup Exec
- Substituting ODBC for JDBC to connect to SQL server for Veritas Backup Exec
- Useful Data Collection scripts for capacity
- Host resources troubleshooting
- Host resources: Check the status of the WMI proxy server
- Host resources: Post-Installation verification
- Host resources: Check host connectivity using standard SSH
- Host resources: Check host connectivity
- Host resources: Check host connectivity using Host Resource Configuration file
- Host resources: Generating host resource configuration files

- Host resources: Check the execution of a command on a remote server
- Host resources Data Collection
- Host resources: Collection in stand-alone mode
- Configuring parameters for SSH
- Identifying Windows file system access errors (File Analytics)
- Collect from remote shares (File Analytics)
- Adding a certificate to the Java keystore

Resolving Data Collectors connections issues - Linux specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal.
2. Verify that the key file is generated when the data collector was created.
3. On the portal, perform `wget` to the URL of the data receiver. The expected response is: `Index.html` file.

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify that the data receiver URL resolves via `NSLOOKUP`. If not then specify the data receiver IP address and name to the data collector's host file.

   Verify using `wget` from the data collector that a response back, index.html page, is received. If not then ,verify if the firewall is blocking the access to port 80/443, depending upon configurations.

5. Execute the command `../mbs/bin/updateconfig`. The expected response is: quick return to the command prompt. If not then: verify that the /opt/aptare/datarcvrconf/collectorConfig.global.properties on the portal has the correct URL.
6. Execute the `checkinstall`. If there is initial communication but errors, confirm the data collector name, passcode, and URL are correct.

7. Examine the `<Data Collector home>/mbs/conf/collector.properties` file and verify that the collector name, collector password, and URL were specified appropriately during the installation.
8. Verify that the collector service is started, and **Watchdog** is running.
9. Ensure the understanding that if the portal is running a later upgrade than the GA data collector that upgrade will initiate right after DC connects, and the data collector will go offline for a period during the upgrade.

Resolving Data Collectors connections issues - Windows specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal
2. Verify that the key file generated when the data collector was created.
3. On the portal, access a web browser to the URL of the data receiver. Expected response: `Veritas NetBackup IT Analytics Data Receiver`.

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify the data receiver URL resolves via `NSLOOKUP`. If not, specify the data receiver IP address and name to the data collector's host file.
5. Verify the response by a browser session on the data collector to the URL. If not, verify if firewall is blocking access to port 80/443, based on the configuration.
6. Execute `<DC HOME>\mbs\bin\updateconfig`. The expected response is, quick return to the command prompt. If not, verify that the **<APTARE PORTAL HOME>datarcvrconf\collectorConfig.global.properties** on the portal has the correct URL.
7. Execute `checkinstall`. If there is initial communication with errors, verify the data collector name, passcode, and URL are correct.
8. Examine the `<Data Collector home>\mbs\conf\collector.properties` file and confirm the collector name, collector password, and URL were keyed in correctly at installation.
9. Verify that the collector service is started and running.

10. Ensure the understanding that if the portal is running a later upgrade than the GA data collector that upgrade will initiate right after DC connects, and the data collector will go offline for a period during the upgrade.

Portal upgrade performance issues

When the entropy of the system is very low, cryptographic functions takes considerable amount of time.

Following are the examples of low entropy:

- while adding new data collector on Portal, takes longer time to generate the key file.
- Upgrade of Portal hangs when upgrading internal objects.
- Aptare agent service takes longer time when started to get the `collectorconfig.xml` from data receiver side.
- `checkinstall.sh` file execution takes longer time than expecting.

These issues are observed on **Linux Platform**.

The following solution is recommended:

Note: Download and install **rng-tools rpm** on the Portal.

For **RHEL/OEL**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `yum install rng-tools` to install the rng-tools.
3. Type `systemctl start rngd` to start the services.
4. Type `systemctl enable rngd` to enable the services.

For **Suse**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `zypper install rng-tools` to install the rng-tools.
3. Type `systemctl start rng-tools` to start the services.
4. Type `systemctl enable rng-tools` to enable the services.

Verify the Data Collector configuration

The Data Collector configuration file contains key information captured during the installation process. If the information was entered incorrectly, this may be the cause of the failure.

To check the configuration file

1 Edit the configuration file.

Windows:

```
edit C:\Program Files\Aptare\mbs\conf\wrapper.conf”
```

Linux:

```
edit /opt/aptare/mbs/bin/startup.sh” and
"/opt/aptare/mbs/bin/updateconfig.sh"
```

2 Verify the values of the following parameters and update them, if necessary.

wrapper.app.parameter.2	Should match the Collector Name you specified when adding a collector policy.
wrapper.app.parameter.3	Should match the Passcode you specified when adding a collector policy.
wrapper.app.parameter.4	For IN-HOUSE installations: http://itanalyticsagent.yourdomain.com where: yourdomain.com has the appropriate value. For third-party HOSTED installations: http://itanalyticsagent.yourdomain.com where: domain.com has the appropriate value.

3 If you changed any of the configuration file parameters, you’ll need to:

- Restart the Data Collector service.
- Re-run the installation validation utility.

Verify Connectivity

To verify that the Data Collector Server can access the Portal Server:

1. Ping the Data Collector URL:

```
ping itanalyticsagent.yourdomain.com
```

2. Verify that the URL has been set up correctly in DNS or in the local hosts file, to resolve to the Portal Server.

Configuring web proxy updates

If you are using a proxy server to connect to the Portal, the Data Collector was configured during installation to use the proxy to connect to the Portal. If the web proxy configuration changes in your environment, the Data Collector must be aware of those changes in order to maintain connectivity. These settings can be found in:

```
/opt/aptare/mbs/conf/collectorsystem.properties
```

Collecting missed events for Veritas Backup Exec

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Backup Exec Data Collector software.

To capture data from a specific period, use the following utility:

```
buehistoricevents.{sh/bat} {AdministratorDomain} {AdministratorUser}
 {AdministratorPassword} [{Start Date} {End Date}] [verbose]
```

Where:

- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Backup Exec commands called to the eventcollector.log file.

Note: If the Start and End Dates are not specified, the utility will capture Events that occurred in the last 24 hours.

Substituting ODBC for JDBC to connect to SQL server for Veritas Backup Exec

The Backup Exec data collector, by default, uses JDBC (Java Database Connectivity) to connect to the SQL Server database. In most cases, this is the preferred mechanism for communicating with the SQL Server. However, in some

instances--for example, TCP/IP is disabled for the SQL Server--JDBC will not be feasible.

In these rare situations, you can configure ODBC (Open Database Connectivity) to connect. The main limitation of this option is that it requires that a DSN (Data Source Name) be set up for each Backup Exec server for which the data collector needs access.

Note: The data collector can be configured to use a mixture of JDBC and ODBC for specific servers.

Use the following steps to turn on ODBC for specific servers:

1. Obtain a copy the **servers.csv** file from the Portal Server (the one that you created to load the Backup Exec servers into the database).
2. Edit **servers.csv**anddelete those servers that you do not want to use ODBC. The format of the entry in the CSV file is:

   ```
   <windows_domain>, <host or ipaddress>, <ipaddress>, , , BKUPEXEC
   ```

3. Save the file to **$APTARE_HOME/mbs/conf** as **odbcservers.conf**on the Data Collector server.
4. Launch the ODBC Data Source Administrator window:

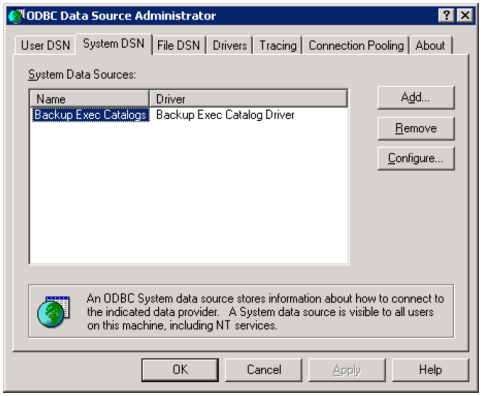
   ```
   Control Panel > Administrative Tools > Data Sources (ODBC)
   ```

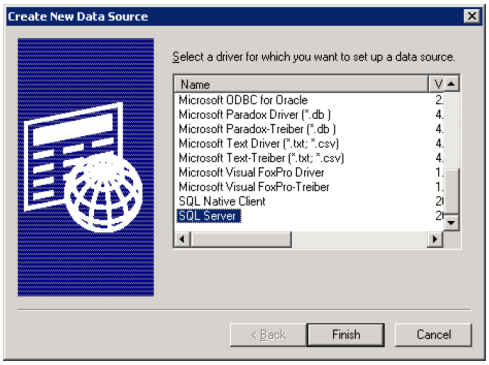
5. Set up the ODBC DSN for each of the Backup Exec servers in **odbcservers.conf**, as depicted in the following sequence of windows.

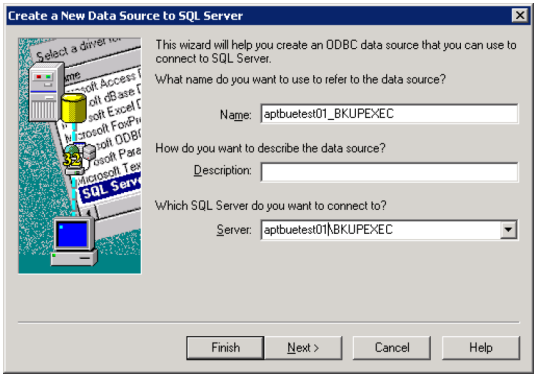
   The DSN needs to be of the form **hostname_BKUPEXEC**, where hostname is the second token in **odbcservers.conf**.

   Note: If the **hostname_BKUPEXEC** form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

   ```
   <windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
   ```



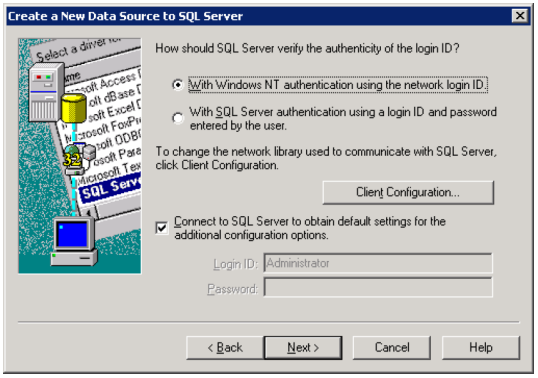


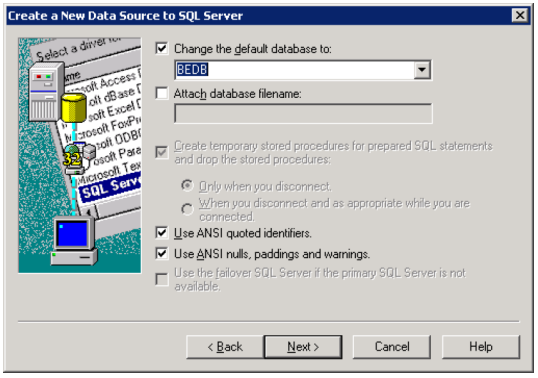


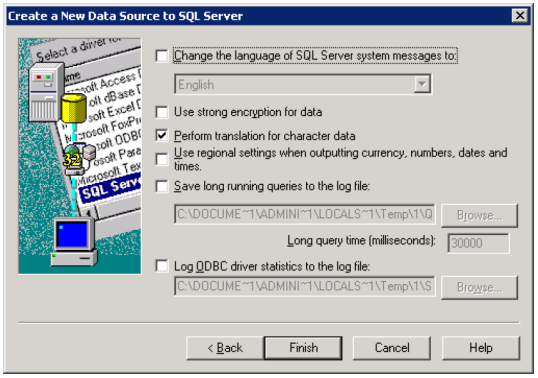
The DSN needs to be of the form hostname_BKUPEXEC, where hostname is the second token in **odbcservers.conf**.

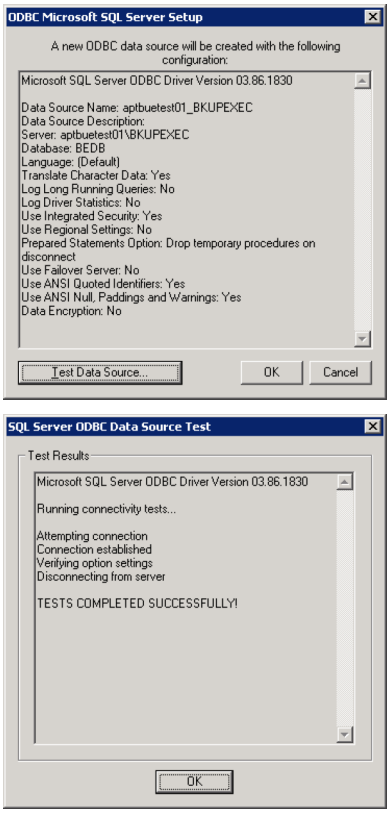
Note: If the **hostname_BKUPEXEC** form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

```
<windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
```









Useful Data Collection scripts for capacity

The following data collection scripts are available by capacity product. These scripts execute the data collection threads to capture the data. These scripts typically are used only when working with the support and services teams while troubleshooting data collection issues.

Capacity Product	Scripts	Location
EMC VNX	emccheckinstall emcvnxactivedirectorydetails emcvnxarraydetails	Windows: C:\Program Files\Aptare\mbs\bin\emc
EMC Symmetrix	emcsymmetrixarrayperfdetails	Linux: /opt/<home_dir>/mbs/bin/emc

Capacity Product	Scripts	Location
EMC CLARiiON	emcclariionarrayperfdetails	
Hitachi	hitachicheckinstall	Windows:
	hitachiarrayperfdetails	C:\Program Files\Aptare\mbs\bin\hitachi
	hitachiarrayhdtdetails	Linux:
	hitachiarraydetails	/opt/<home_dir>/mbs/bin/hitachi
Host Resources	hostvalidate	Windows:
	hostresourcevalidate	C:\Program Files\Aptare\mbs\bin\hostresources
	hostresourcediscover	Linux:
	hostresourcedetail	/opt/<home_dir>/mbs/bin/hostresources
	hostresourhostresourceasmcollectorcecheckinstall	
HP EVA	hpevaarraydetails	Windows:
		C:\Program Files\Aptare\mbs\bin\hp
		Linux:
		/opt/<home_dir>/mbs/bin/hp
HP 3PAR	hp3parperf	Windows:
	hp3pardetails	C:\Program Files\Aptare\mbs\bin\hp3Par
		Linux:
		/opt/<home_dir>/mbs/bin/hp3Par
IBM XIV	ibmxivarrayperfdetails	Windows:
	ibmxivarraydetails	C:\Program Files\Aptare\mbs\bin\ibm
IBM VIO	ibmviodetail	Linux:
		/opt/<home_dir>/mbs/bin/ibm
IBM SVC	ibmsvcarrayperfdetails	
	ibmsvcarraydetails	
IBM Enterprise Arrays	ibmenterprisearraydetails	

Capacity Product	Scripts	Location
NetApp	netappsnapvaultdetails netappsnapmirrordetails netappcheckinstall netapparrayperfdetails netapparraydetails	Windows: C:\Program Files\Aptare\mbs\bin\netapp Linux: /opt/<home_dir>/mbs/bin/netapp

Host resources troubleshooting

Use the following sequence of steps to determine the source of host resources data collection issues. All commands--except for the SSH commands and the WMI Proxy command--report errors to **metadata.log**. After executing a command, check the **metadata.log** file for error messages. If there is an error noted, correct the problem and then re-issue the command. If the command succeeds, proceed to the next command in this sequence:

1. See "Host resources: Check the status of the WMI proxy server" on page 645.
2. See "Host resources: Post-Installation verification" on page 648.
3. See "Host resources: Check host connectivity using standard SSH" on page 648.
4. See "Host resources: Check host connectivity" on page 650.
5. See "Host resources: Check the execution of a command on a remote server" on page 653.
6. See "Host resources: Collection in stand-alone mode" on page 654.

Host resources: Check the status of the WMI proxy server

Use the following **checkwmiproxy**utility to verify that the WMI Proxy Server is up and running.

The WMI Proxy logs are written to:

```
C:\Program Files\Aptare\WMIProxyServer\logs\aptarewmiserver.log
```

Prerequisites

Either **checkinstall** or **updateconfig** must have been run before running **checkwmiproxy**. Otherwise, **checkwmiproxy** will not have access to the proxy server settings that are saved in the collector configuration file.

Usage

```
checkwmiproxy.[sh|bat] [wmiProxyServer wmiProxyPort remoteWinHost
DomainOfUserId UserId Password "Command"]
```

Where:

wmiProxyServer is the name of the WMI Proxy Server

wmiProxyPort is the proxy's port (default is 1248)

Simple usage

```
checkwmiproxy.[sh|bat]
```

By default, this utility will look for the WMI Proxy Server details in the Host Resources Collector section of the collector configuration file. If it does not find a Host Resources Collector section, the **checkwmiproxy** will terminate with an error and a recommendation to pass explicit parameters, as shown in the usage statement above.

Example 1:

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00
Connection to APTARE WMI Proxy server successfully validated.
```

Example 2: Remote WMI queries

This utility also can be used to execute remote WMI queries, as shown in the following example.

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh 172.16.1.152
Administrator password 172.16.1.152 "select * from
Win32_OperatingSystem"
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
   APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00

    Connection to APTARE WMI Proxy server successfully validated.

    APTAREWMIServer Response:
    instance of Win32_OperatingSystem
    {
         BootDevice = "\\Device\\HarddiskVolume1";
         BuildNumber = "3790";
```

```
        BuildType = "Multiprocessor Free";
        Caption = "Microsoft(R) Windows(R) Server 2003, Standard
Edition";
        CodeSet = "1252";
        CountryCode = "1";
        CreationClassName = "Win32_OperatingSystem";
        CSCreationClassName = "Win32_ComputerSystem";
        CSDVersion = "Service Pack 1";
        CSName = "APTARESTGRPT1";
        CurrentTimeZone = -420;
        DataExecutionPrevention_32BitApplications = TRUE;
        DataExecutionPrevention_Available = TRUE;
        DataExecutionPrevention_Drivers = TRUE;
        DataExecutionPrevention_SupportPolicy = 2;
        Debug = FALSE;
        Description = "aptarestgrpt1";
        Distributed = FALSE;
        EncryptionLevel = 168;
        ForegroundApplicationBoost = 2;
        FreePhysicalMemory = "160264";
        FreeSpaceInPagingFiles = "1967860";
        FreeVirtualMemory = "2084508";
        InstallDate = "20070212110938.000000-480";
        LargeSystemCache = 1;
        LastBootUpTime = "20080507115419.343750-420";
        LocalDateTime = "20080520142117.484000-420";
        Locale = "0409";
        Manufacturer = "Microsoft Corporation";
        MaxNumberOfProcesses = 4294967295;
        MaxProcessMemorySize = "2097024";
        Name = "Microsoft Windows Server 2003 R2 Standard
Edition|C:\\WINDOWS|\\Device\\Harddisk0\\Partition1";
        NumberOfLicensedUsers = 10;
        NumberOfProcesses = 90;
        NumberOfUsers = 8;
        Organization = "Aptare";
        OSLanguage = 1033;
        OSProductSuite = 272;
        OSType = 18;
        OtherTypeDescription = "R2";
        PAEEnabled = TRUE;
        Primary = TRUE;
        ProductType = 3;
```

```
        QuantumLength = 0;
        QuantumType = 0;
        RegisteredUser = "Aptare";
        SerialNumber = "69712-OEM-4418173-93136";
        ServicePackMajorVersion = 1;
        ServicePackMinorVersion = 0;
        SizeStoredInPagingFiles = "2039808";
        Status = "OK";
        SuiteMask = 272;
        SystemDevice = "\\Device\\HarddiskVolume1";
        SystemDirectory = "C:\\WINDOWS\\system32";
        SystemDrive = "C:";
        TotalVirtualMemorySize = "3256472";
        TotalVisibleMemorySize = "1363400";
        Version = "5.2.3790";
        WindowsDirectory = "C:\\WINDOWS";
};
```

Host resources: Post-Installation verification

Execute this utility to verify that the host resources installation was successful.

```
hostresourcecheckinstall.{sh|bat}
```

Host resources: Check host connectivity using standard SSH

NetBackup IT Analytics uses SSH to communicate with devices to run SSH commands. Sometimes, a connectivity issue is simply an incorrect path to a host.

Note: Use the following SSH commands before attempting to collect data.

To check host connectivity using standard SSH:

1. Check that the connection to a Host is successful, using the credentials provided.

   ```
   [user@host ~] ssh <user>@<host> ls
   ```

   Similarly, if you are using Telnet, check your host access via Telnet and run **sudo** commands, as shown in the following step.

2. In access-controlled environments such as **sudo**, a sudo user must be set up. Ensure that the sudo user can run the commands required for the host operating system platform.

   To verify **sudo** access:

   ```
   [user@host ~] ssh <sudouser>@<host> "sudo <command>"
   ```

   If this command results in errors, such as command not found, set up the paths correctly and re-run this command.

   See "Checking Paths for SSH" on page 649.

   on page 11.

3. Paths should be set correctly for the commands to run.

Checking Paths for SSH

If you find messages in the metadata.log file that indicate that some of the commands are not found, then most likely the reason for it is the paths have not been set properly.

NetBackup IT Analytics uses a non-interactive login shell to execute ssh commands on devices.

1. Check the environment setting for the shell by running the command.

   ```
   [user@host ~] ssh <user>@<host> "env"
   ```

   Check the PATH shown in the output and make sure that it contains the path to all the commands required for NetBackup IT Analytics for the OS platform of the host.

   Sample PATH for each of the host operating system platforms:

   Linux: /bin:/sbin:/usr/bin:/usr/sbin

   Solaris: /usr/xpg4/bin:/usr/sbin:/usr/bin

   AIX: /usr/bin:/usr/sbin

   HPUX: /usr/bin:/usr/sbin:/opt/fcms/bin:/sbin

   Note: Since Veritas Volume Manager is supported, its path needs to be included in the PATH env variable.

   ---

2. In **sudo** environments, make sure that the sudo path is also in the PATH shown in the output of the above command.

Environment setting for bash users

1. Define all your settings in the file: **~/.bashrc**
2. Make sure that the file **~/.bash_profile** only contains the line: **source ~/.bashrc**

Host resources: Check host connectivity

This utility displays information on the connection status of a list of host names, IP addresses, or a range of IP addresses.

```
chkHostConnection.{sh|bat} HostAddresses userId password
[domain <domain>]
[exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

Table 67-1 Hosts resources and their values.

Host Addresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

As a result: for each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} HostAddresses userId password [domain
<domain>] [exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
```

```
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Host resources: Check host connectivity using Host Resource Configuration file

This utility provides information on the connection status of a list of Host Addresses that are provided in the Host Resource Configuration file.

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>]
[cto <connectTimeout>] [sto <socketTimeout>]
```

Table 67-2 Hosts resources and their values.

HostResourceFile	The file should be located under the home directory: /mbs/conf/hostresourceconf
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds

Table 67-2 Hosts resources and their values. *(continued)*

HostResourceFile	The file should be located under the home directory: /mbs/conf/hostresourceconf
sto	Socket time-out in milliseconds

Result: For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ..... SUCCESS
172.16.1.12 ..... SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>] [cto <connectTimeout>] [sto <socketTimeout>]
```

HostResourceFile	The file should be located under the home directory: **/mbs/conf/hostresourceconf**
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ..... SUCCESS
172.16.1.12 ..... SUCCESS
```

Host resources: Generating host resource configuration files

This utility automatically generates the host resource configuration files and collector configuration file for each valid line provided in the input file.

```
genHostResourceConf.{sh|bat} {CollectorID} {fileName}
```

CollectorID	Identifier name used for the configuration files

filename	File containing the list of parameters--one per line--in the format: `HostAddresses:userId:password:domain:excludeHostAddress` Comments are allowed by using a # at the beginning of the line.
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Sample lines in an input file

```
# Sample configuration file to generate Host Resource Conf files
172.16.1.11-13,aptarelab3:root:adminpwd::172.16.1.12-13,apataredlab3
aptareaix1:root:superpwd::
apatrewin2k:samuel:adminpwd:aptarewin2kdomain:
```

Results

- For each valid line, a host resource configuration is created under the home directory: **/mbs/conf/hostresourceconf**. Lines that are not valid are sent to standard output.
- Creates a collector configuration xml file with Meta Data Collector child thread tags for each successfully created host resource configuration file. The file is saved in the home directory under **/mbs/conf**. The collector configuration xml is named in the following format:
  collectorconfig-<date>.xml where date is in DDMMMYYYHHMM format

Host resources: Check the execution of a command on a remote server

This utility provides the output of a command by running it on the specified remote server.

```
remoteExecCommand.{sh|bat} HostAddress [enc] userId password
[domain=<domain>]
[wmiserver=<wmiserver>] [cto=<connectTimeout>] [sto=socketTimeout>]
 [accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.

userId password	Use the [enc] option to provide encrypted user ID and password arguments.
domain	The Domain for the Windows hosts (only for connecting to a Windows server)
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Example

```
remoteExecCommand.sh 172.16.1.21 myuser mypasswd /usr/bin/df -k
remoteExecCommand.sh 172.16.1.21 myuser mypasswd accessCmd=sudo
cto=10000 /usr/bin/df -k
```

Host resources Data Collection

NetBackup IT Analytics can collect the following types of host resources:

- Capacity
- Oracle
- SQL Server
- Exchange
- Network
- Processor
- Memory
- Process
- System

Host resources: Collection in stand-alone mode

This utility executes the data collection process against the specific host resources files.

Usage (3 options)

```
hostresourceDetail.{sh|bat} all
hostresourceDetail.{sh|bat} <MetaCollectorID> <HostResourcePolicyName>
hostresourceDetail.{sh|bat} HostAddresses uid=userId pwd=password
[<domain>]
[<excludeHostAddresses>]
```

all	This option runs host resource policies against all Meta Collectors.
MetaCollectorID	The ID used to identify the MetaCollector within the collector configuration xml file.
HostResourcePolicyName	The Policy ID within the Meta Collector ID specified.
HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.

Configuring parameters for SSH

To add any configurable SSH parameters, modify the following scripts:

```
hostResourceDetail.{sh|bat} and aptarecron.{sh|bat}
```

For example, to add the **channelWaitTime**parameter, insert the following after java:

```
-DchannelWaitTime=5000
```

Configure channelWaitTime

If you are experiencing slow connectivity from the Data Collector Server to the Host, update the scripts with this Configurable Parameter. This parameter is specified in milliseconds.

```
-DchannelWaitTime=5000 // This will set the wait time for data from
 the server.
```

Configure singleChannelSession

This will run each command in a separate session.

```
-DsingleChannelSession=true // This will run the each command in a
separate session.
```

Configure sudoWithPassword

In sudo environments, this will send the password without waiting for a prompt.

```
-DsudoWithPassword=true // This will allow running sudo with -S option
 to send the password without waiting for a prompt.
```

Identifying Windows file system access errors (File Analytics)

While profiling the Windows primary file table and file systems, a number of error messages may appear in the **MFT.Aptare_File_Inventory.log** file

These errors actually may require no follow-up actions. Typically, the errors are legitimate, such as a file being locked for exclusive use. Therefore, some files in the C:\Windows\System32 directory will not be profiled.

Example of a Log Error Message:

```
Unable To Access File C:\Windows\System32\Boot. Error 2. Skipping!!!
```

The following table lists System Errors with descriptions.

Table 67-3 Windows file system errors and its description

System Error	Description
2	System cannot find the file specified; This error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.

Table 67-3 Windows file system errors and its description *(continued)*

System Error	Description
3	System cannot find the path specified; This system error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.
5	Access Denied; The file is accessible only to SYSTEM; for example, C:\Windows\System32\LogFiles\WMI\RtBackup
32	Another process has the file opened in exclusive mode; for example, database files used by the SQL server

Collect from remote shares (File Analytics)

The functionality of the host File Analytics probe excludes remote shares that are mounted to the target host, thereby capturing only local files and folders.

To collect from remote shares, an advanced parameter must be configured.

1. In the Portal, navigate to **Admin > Advanced > Parameters**.
2. Click **Add** to add an advanced parameter with a value of **FA_HOST_CAPTURE_REMOTE_SHARES** with a default value of **Y**, along with the target server host name.

Adding a certificate to the Java keystore

Use the following steps to add an SSL certificate to the Java keystore for a Data Collector. Some servers, such as VSphere, require a certificate for connection while communicating with SSL.

Keystore file location

Note: For the following commands, if you are not running in the default collector location (/usr/openv/analyticscollector or \Program Files\Veritas\AnalyticsCollector), substitute the appropriate APTARE_HOME in the command path.

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Copy the certificate file (certfile.txt) to the Data Collector. Run the following command to add the certificate:

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -import
 -alias "somealias" -file certfile.txt -keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -import -alias
"somealias" -file certfile.txt -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

When prompted, enter the default password to the keystore:

```
changeit
```

The results will be similar to the following example:

```
Enter keystore password:
......
Certificate Shown here
......
......
......
Trust this certificate? [no]: yes
```

Once completed, run the following keytool command to view a list of certificates from the keystore and confirm that the certificate was successfully added. The certificate fingerprint line displays with the alias name used during the import.

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -list
-keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -list -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Sample Linux Output

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
```

```
Your keystore contains 79 entries
digicertassuredidrootca, Apr 16, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
trustcenterclass2caii, Apr 29, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
.....
```

Chapter 68

Uninstalling the Data Collector

This chapter includes the following topics:

- Uninstall the Data Collector on Linux
- Uninstall the Data Collector on Windows

Uninstall the Data Collector on Linux

This uninstall process assumes that the Data Collector was installed using the standard installation process.

To uninstall the Data Collector software from a Linux host:

1. Login to the Data Collector server as root.
2. For NetBackup IT Analytics Data Collector version 10.6 or lower, execute the `Uninstall APTARE IT Analytics Data Collector Agent` script located at `<Data Collector home folder>/UninstallerData`

   For example:

   ```
   /opt/aptare/UninstallerData/Uninstall APTARE IT Analytics Data Collector Agent
   ```

3. For NetBackup IT Analytics Data Collector version 11.0 or later, execute `uninstall_dc.sh script` located at `<Data Collector home folder>/UninstallerData/uninstall_dc.sh`

   For example:

   ```
   /opt/aptare/UninstallerData/uninstall_dc.sh
   ```

Uninstall the Data Collector on Windows

This uninstall process assumes that the Data Collector was installed using the standard installation process.

To uninstall the Data Collector software from a Windows host:

1. Login to the Data Collector server as an administrator.
2. Go to **Control Panel** > **Add and Remove Program** > **Programs and Features** and uninstall **NetBackup IT Analytics Data Collector**.

The uninstaller may not delete the entire Data Collector directory structure. Sometimes new files that were created after the installation are retained along with their parent directories. If the Data Collector was upgraded from version 10.6 or older, you may find entries of Kafka and Zookeeper services on the services panel (default `C:\Program Files\Aptare`), even after the uninstallation of the Data Collector. You must manually delete the services and reboot the system.

Appendix A

Firewall Configuration: Default Ports

This appendix includes the following topics:

- Firewall configuration: Default ports

Firewall configuration: Default ports

The following table describes the standard ports used by the Portal servers, the Data Collector servers, and any embedded third-party software products as part of a standard “out-of-the-box” installation.

Table A-1 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139

Table A-1 Components: Default Ports *(continued)*

Component	Default Ports
Oracle Oracle TNS listener port	1521
Tomcat - Data Receiver Apache connector port and shutdown port for Data Receiver instance of tomcat	8011, 8017
Tomcat - Portal Apache connector port and shutdown port for Portal instance of tomcat	8009, 8015
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445
ZooKeeper	2181 **Note:** NetBackup IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the local host where NetBackup IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table A-2 Storage Vendors: Default Ports

Storage Vendor	Default Ports and Notes
Dell Compellent	1433 SMI-S http (5988) SMI-S https (5989)
Dell EMC Elastic Cloud Storage (ECS)	REST API 4443

Table A-2 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
Dell EMC Unity	REST API version 4.3.0 on 443 or 8443
EMC Data Domain Storage	SSH 22
EMC Isilon	SSH 22
EMC Symmetrix	SymCLI over Fibre Channel 2707
EMC VNX	NaviCLI 443, 2163, 6389, 6390, 6391, 6392
EMC VNX (Celerra)	XML API 443, 2163, 6389, 6390, 6391, 6392
EMC VPLEX	https TCP 443
EMC XtremIO	REST API https 443
HP 3PAR	22 for CLI
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0
Hitachi Block Storage	TCP 2001 For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
Hitachi Vantara All-Flash and Hybrid Flash Storage	Hitachi Ops Center Configuration Manager REST API: 23450 for HTTP and 23451 for HTTPS. HIAA : 22015 for HTTP, and 22016 for HTTPS
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778

Table A-2 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
Microsoft Windows Server	2016 WMI 135 DCOM TCP/UDP > 1023
NetApp E-Series	SMCLI 2436
NetApp ONTAP 7-Mode and Cluster-Mode	ONTAP API 80/443
Pure Storage FlashArray	REST API https 443

Table A-3 Data protection: Default ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023
Dell EMC Networker Backup & Recovery	Port used for Dell EMC NetWorker REST API connection. Default: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
HP Data Protector	5555 WMI ports SSH 22 (Linux)
IBM Spectrum Protect (TSM)	1500
NAKIVO Backup & Replication	Director Web UI port (Default: 4443)
Oracle Recovery Manager (RMAN)	1521
Rubrik Cloud Data Management	REST API 443
Veeam Backup & Replication	9392
Veritas Backup Exec	1433

Table A-4 Network & Fabrics: Default Ports

Network & Fabrics Vendor	Default Ports and Notes
Brocade Switch	SMI-S 5988/5989
Cisco Switch	SMI-S 5988/5989

Table A-5 Virtualization Vendors: Default Ports

Virtualization Vendor	Default Ports and Notes
IBM VIO	SSH 22
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESX or ESXi,vCenter,vSphere	vSphere VI SDK https TCP 443

Table A-6 Replication Vendors: Default Ports

Replication Vendor	Default Ports and Notes
NetApp ONTAP 7-Mode	ONTAP API 80/443

Table A-7 Cloud Vendors: Default Ports

Cloud Vendor	Default Ports and Notes
Microsoft Azure	https 443
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22
Google Cloud Platform	https 443

Appendix B

Load historic events

This appendix includes the following topics:

- Introduction
- Load Commvault Simpana events
- Load Dell PowerProtect Data Manager jobs
- Load EMC Avamar events
- Load EMC NetWorker events
- Load HP Data Protector events
- Load IBM Spectrum Protect (TSM) events
- Load Oracle Recovery Manager (RMAN) events
- Load Veeam Backup & Replication events
- Load Veritas NetBackup events
- Load Veritas Backup Exec events
- Corrections in duplication of clients
- Cohesity
- Dell EMC NetWorker Backup & Recovery

Introduction

After installing the backup Data Collectors, you may want to capture historical backup events for inclusion in the NetBackup IT Analytics database.

Note: If the scheduled data collection process oversights the data, the Historic Event Collection should be used.

Note: For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Data Collector software.

Load Commvault Simpana events

Commvault Simpana Historic Collection uses a JDBC connection to collect jobs data from the Commvault Simpana database for a given look back hours.

Configure **COMMVAULT_OLDEST_JOB_HOURS** parameter for historic data collection.

Note: The allowed maximum number of hours to look back for historic data collection is 168 hours. Historic collection is normally used on first time collection. It retrieves the details of the backup jobs, restore jobs, and job failures from the database using the SQL queries.

Windows:

```
C:\Program Files\Aptare\mbs\bin\commvault\cvsimpanadetails.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/commvault/cvsimpanadetails.sh
```

To capture data from a specific period, use the following utility:

```
cvsimpanadetails.{sh|bat} <output_dir> <cvdb_username> <cvdb_password>
<cvdb_hostname>[:port] [max_hours [cv_username cv_password
[cv_hostname]]]
```

Where:

- This utility will write data to a set of files in the output directory specified in `output_dir`.
- The cvdb_username, cvdb_password and cvdb_hostname refer to the CommServ database system (this is usually the same as the CommServ server) from which you are collecting data.
- [Optional]Port Number can be appended to the cvdb_hostname, separated by a colon.

Note: If a port number is not specified, default 1433 port is assigned.

- [Optional]Maximum number of hours from which to start the collection can be specified. This value is used to calculate the current time minus the number of hours that was entered.
  If you do not enter a maximum number of hours, then all details retained by the Commvault Simpana database will be retrieved.
- The last set of cv_username, cv_password and cv_hostname are required only if you are collecting Skipped File Details from a Windows-based CommServ Server.

Load Dell PowerProtect Data Manager jobs

To enable historic collection for Dell PowerProtect Data Manager, you must add the Advanced parameter. Once the parameter is set, it gets applied in every collection run. Ensure that parameter is deleted after collecting the historical data.

To add an advance parameter, see NetBackup IT Analytics User Guide > Customize with advanced parameters > Adding an advance parameter section.

- DPDM_LOOKBACK_HOURS
- Host: Add Dell PowerProtect Data Manager servers for which this advanced parameter must be applied.

If the above parameters are not set, the default look-back time is 3 days (36 hours).

REST API

/api/v2/activities - This call is used in REST API to collect all activities.

/api/v2/protection-details - This call is used in REST API to retrieve a list of existing protections such as backups and replications.

Load EMC Avamar events

EMC Avamar Historic Data Collection uses JDBC as a read-only user to collect point-in-time data of backup events / activities from the Avamar Management Console Server (MCS) database within a given time frame.

It retrieves backup information from Avamar MCS database using the following views:

- `v_repl_activities` - extracts record for each replication activity.
- `v_plugin_catalog` - extracts record for each known plug-in.

- `v_activities_2` - extracts record for each backup, restore, or validation activity.
- `v_datasets` - extracts record for each data set known to the MCS.
- `v_retention_policies` - extracts record for each retention policy known to the MCS.

Windows:

```
C:\Program Files\Aptare\mbs\bin\avamar\avamarhistoricdetails.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/avamar/avamarhistoricdetails.sh
```

To capture the data from a specific period, use the following utility:

```
avamarhistoricdetails.{sh|bat} <MetadataCollectorID> <SubSystemID>
["<Start Date>" "<End Date>"] [verbose]
```

Where:

- The MetadataCollectorID and the SubSystemID can be found by executing the utility:
  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Avamar commands called to the metadata.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last two weeks.

Load EMC NetWorker events

NetWorker Historic Collection uses `mminfo` command to extract backup information and save sets for a given time frame.

By default, the `mminfo` command gets information about the Backup media and save sets that were completed during the last 24 hours. This includes: the volume name, client name, creation date, amount of data saved to the volume, level of backup performed, and the name of the save set.

Windows:

```
C:\Program Files\Aptare\mbs\bin\networker\nwhistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/networker/nwhistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
nwhistoricevents.{sh|bat} <EventCollectorID> <ServerID> ["<Start
Date>" "<End Date>"] [verbose]
```

Where:

- The EventCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the NetWorker commands called to the `eventcollector.log` file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours.

Load HP Data Protector events

The HP Data Protector (HPDP) Historic event collection captures backup details for all the sessions within a given time frame which is present in HPDP System. It uses the HPDP omnidb and omnirpt CLIs to query the data protector internal database for detailed backup information.

- `omnidb` - Queries the data protector internal database. This command is available on systems with the data protector user interface component installed.
- `omnirpt` - Generate various reports of the data protector environment, for example, about backup, object copy, object consolidation and object verification sessions in a specific time phase, session specification, media, data protector configuration, and single sessions. This command is available on systems with the data protector user interface component installed.

Windows:

```
C:\Program Files\Aptare\mbs\bin\dataprotector\hpdphistoricevents.bat
```

Linux:

```
 <APTARE HOME>/mbs/bin/dataprotector/hpdphistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
hpdphistoricevents.{sh|bat} <EventCollectorID> <ServerID> ["<Start
Date>" "<End Date>"] [verbose]
```

Where:

- The EventCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the Data Protector commands called to the `eventcollector.log` file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the previous 24 hours. HP Data Protector commands ignore the time segment of the start and end date values. In addition, the end date value is used as an “until” value.

Note: For example, a value of "2015-05-11 23:59:59" will only collect historic values up to 2015-05-11 00:00:00. To collect values for the date of 2015-05-11 you should enter a end date of "2015-05-12 00:00:00".

Load IBM Spectrum Protect (TSM) events

TSM Historic collection uses `dsmadmc` command with SQL query as one of the parameters to collect all historic data.

Windows:

```
C:\Program Files\Tivoli\TSM\baclient\dsmadmc  -id= <userId>
-password= <password> -tcpserveraddress= <server> -tcpport= <serverPort>
-DISPLaymode=LIst -noconfirm  <query>
```

Linux:

```
C:\Program Files\Tivoli\TSM\baclient\dsmadmc  -id= <userId>
-password= <password> -se= <configInstanceName> -DISPLaymode=LIst
-noconfirm  <query>
```

SQL queries utilizes the following database tables:

- sessions
- EVENT
- actlog
- summary
- summary_extended

Windows:

```
C:\Program Files\Aptare\mbs\bin\tsm\tsmhistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/tsm/tsmhistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
tsmhistoricevents.{sh/bat} <MetadataCollectorID> <ServerID> ["<Start
Date>" "<End Date>" [verbose]]
```

Where:

- The MetadataCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the IBM Spectrum Protect (TSM) commands called to the `metadata.log` file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the previous 24 hours.

Load Oracle Recovery Manager (RMAN) events

RMAN Historic collection fetches Jobs data over JDBC connection from RMAN database. It uses Dynamic Performance (V$) views for fetching backups in individual instances, or Recovery Catalog views for fetching backups from a central Recovery Catalog.

1. Set Advanced Parameter `RMAN_BACKUP_LOOKBACK_DAYS=#`, where # must be a positive numeric value that indicates the days to load (from current day).
2. Set Advanced Parameter `RMAN_BACKUP_LOOKBACK_OVERRIDE=Y`.

   Note: For more information on RMAN_BACKUP_LOOKBACK_OVERRIDE and RMAN_BACKUP_LOOKBACK_DAYS, see *NetBackup IT Analytics User Guide* > *Customize with advanced parameters* >> *Adding an advance parameter* section.

3. Navigate to *Admin* >> *Data Collection* >> *Collector Administration*.
4. Select **Oracle RMAN Data Collection** policy and click **Run**.

   You can also wait for the scheduled collection to complete.
5. Reset RMAN_BACKUP_LOOKBACK_DAYS and RMAN_BACKUP_LOOKBACK_OVERRIDE to their original values (or the default values) once the Collection Run is complete. Do not delete the advanced parameters.

Load Veeam Backup & Replication events

Veeam Historic collection uses PowerShell commands to get client, job, session and backup data for a given time span defined by advanced parameters.

The following are the advanced parameters used in the process.

1. Set Advanced Parameter `VEEAM_BACKUP_LOOKBACK_DAYS` to the number of days. Also specify the Data Collector and the Host Name(s) for which the historical data must be collected.
2. Set Advanced Parameter `VEEAM_BACKUP_LOOKBACK_OVERRIDE=Y`. Also specify the Data Collector and the Host Name(s) for which the historical data must be collected.

Note: For more information on RMAN_BACKUP_LOOKBACK_OVERRIDE and RMAN_BACKUP_LOOKBACK_DAYS, see *NetBackup IT Analytics User Guide* >> *Customizing with Advance Parameter* >> *Adding an advance parameter* section.

Configuring these parameters, the normal collection (scheduled or on-demand) works as a historic collection. With these parameters, collection probes such as Client Details, Job Details, Session, and Backup Details can be executed to get the historic data.

3. Navigate to **Admin** >> **Data Collection** >> **Collector Administration**.
4. Select Veeam Backup & Replication Data Collection policy and then click **Run**.

   See "Working with on-demand Data Collection" on page 624.
5. Reset `VEEAM_BACKUP_LOOKBACK_OVERRIDE=N` (or the default values) once the Collection Run is complete to avoid historic data collection on future scheduled or On Demand runs,

Load Veritas NetBackup events

The Cohesity NetBackup Historic collection is limited to capturing details on successful backup images that are still present in the NetBackup catalog (i.e. unexpired backup images). This historic information is captured using the NetBackup `bpimagelist` command.

The failed jobs are not:

- the part of the historic collection as they are not present in the catalog
- point-in-time metrics such as job throughput.

The following are the steps to execute historic collection from the portal:

1. Log in to the portal.
2. Navigate to *Admin* >> *Data Collection* >> *Collector Administration*.
3. Expand the collector and then select the **NetBackup Policy**.
4. Click **Run**. The **Run Cohesity NetBackup Collection** dialog box is displayed.
5. Click **Historic Collection**.
6. Clear the **Enable Real-Time Logs** check box.
7. Clear the **Enable Debug Logs** check box.
8. Select the appropriate **Start Date** and **End Date**.

9. Specify one or more **Client Name(s)**, separated by commas, to limit historic collection to only these specified clients. For example, Client_a, Client_b
10. Click **Start**.

NetBackup IT Analytics gathers backup events from both the NetBackup catalog and the NetBackup activity log. Specify the date range for the backup jobs that occurred during a given time period.

To minimize the impact on performance, upload the backup events for each individual client. However, in many cases, this is not practical. Therefore, several methods are provided to accommodate various needs. Only successful jobs are retrieved from the NetBackup environment.

Load events for individual NetBackup clients

To retrieve historic data from a NetBackup client, execute the following command-line scripts.

Windows:

```
C:\Program Files\Aptare\mbs\bin\veritas\load_nbu_backups.bat
<metaDataCollectorId> <primaryServerName> <client_name> "<Start_Date>"
 "<End_Date>"
```

Linux:

```
<APTARE HOME>/mbs/bin/symantec/load_nbu_backups.sh
<metaDataCollectorId> <primaryServerName> <client_name> "<Start_Date>"
 "<End_Date>"
```

Note: Start_Date and End_Date must be in the format: **YYYY-MM-DD HH:MM:SS**

Where:

- The MetadataCollectorID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Load events for a group of NetBackup clients

To load the historic events for a group of NetBackup clients, execute the following command-line scripts.

Note: This process will only load data for clients that are listed in standard policies. It will not retrieve data for clients not explicitly listed in policies. For example, VMware VMs that are part of a VMware Intelligent Policy will not be included.

Linux

1. Create a NetBackup client list:

```
/usr/openv/netbackup/bin/admincmd/bpplclients -noheader -allunique
 > /tmp/client_list.txt
```

2. Load the list into a for loop:

```
            for i in `awk '{print $3}' /tmp/client_list.txt`
            do
            /<APTARE HOME>/mbs/bin/veritas/load_nbu_backups.sh
<metaDataCollectorId> <primaryServerName> $i "<Start_Date>"
"<End_Date>"
            done
```

Note: Start_Date and End_Date must be in the format: **YYYY-MM-DD HH:MM:SS**

Where:

- The MetadataCollectorID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Windows

1. Create a NetBackup client list:

```
C:\program files\Veritas\netbackup\bin\admincmd\bpplclients
-noheader -allunique > c:\client_list.txt
```

2. Load the list into a for loop:

```
            for /F "tokens=3" %A in (c:\client_list.txt) do
"c:\program files\aptare\mbs\bin\veritas\load_nbu_backups.bat"
```

```
<metaDataCollectorId> <primaryServerName> %A "<Start_Date>"
"<End_Date>"
```

Start_Date and End_Date must be in the format: **YYYY-MM-DD HH:MM:SS**

Note: If the path C:\Program Files fails, try it as C:\Progra~1 or C:\Progra~2

Load Veritas Backup Exec events

Cohesity Backup Exec Historic collection uses JDBC connection to query Backup Exec database for capturing all Backup Events data for a specific given time period.

SQL queries utilizes the following Backup Exec Database tables:

- JobHistorySummary
- JobHistoryDetail, Resource
- ResourceContainer
- Jobs
- TaskDefinition
- Policy
- Device
- Schedule
- ComplexTask

Windows:

```
C:\Program Files\Aptare\mbs\bin\backupexec\buehistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/backupexec/buehistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
buehistoricevents.{sh|bat} <AdministratorDomain> <AdministratorUser>
 <AdministratorPassword> ["<Start Date>" "<End Date>"] [verbose]
```

Where:

- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the Backup Exec commands called to the `metadata.log` file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours.

Corrections in duplication of clients

This section applies to those clients that are being reported by Veritas NetBackup's VMware policy.

A VMware backup policy in NetBackup can be configured in several ways with Virtual Machine (VM) Primary identifier set to one of

- Hostname
- Display Name
- DNS Name
- Instance UUID
- BIOS UUID

Due to which the name of the same VM reported by NetBackup may differ depending on how the policy is created, which may result in the same VM getting persisted in Aptare database with different name resulting in duplicates.

To fix the historic data having duplicate clients, execute the following command-line scripts on Data Collector.

Warning: The command should be executed only after upgrading to version 10.6 P14 or 11.0.02.

Windows:

```
C:\Program Files\Aptare\mbs\bin\veritas\correct_vm_dup_clients.bat
<metaDataCollectorId> <primaryServerName>
```

Linux:

```
<APTARE HOME>/mbs/bin/symantec/correct_vm_dup_clients.sh
<metaDataCollectorId> <primaryServerName>
```

Where: The MetadataCollectorID can be found by executing the following utility:

- For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

- For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Cohesity

Cohesity Historic collection uses REST APIs to collect the session and backup information.

To execute the Cohesity Historic data collection from the portal, configure the following advanced parameters within the specific time frame.

- COHESITY_BACKUP_LOOKBACK_HOURS
- COHESITY_BACKUP_START_TIMESTAMP (Unix epoch time in microseconds) Example: 1590488100000000 for (May 26, 2020 10:15:00 AM GMT)
- COHESITY_BACKUP_END_TIMESTAMP (Unix epoch time in microseconds) Example: 1590922800000000 (May 31, 2020 11:00:00 AM GMT)

Note: If the above parameters are not set, then the default look-back time is 36 hours

---

REST APIs

- `GET /irisservices/api/v1/public/protectionRuns`
  All the parent and child data
- `GET /irisservices/api/v1/public/restore/tasks`
  All the recovery-related data
- `GET /irisservices/api/v1/public/protectionSources/objects/`
  Returns the Protection Source objects corresponding to the specified IDs.
- `GET /irisservices/api/v1/public/protectionJobs/`
  All Protection Jobs currently on the Cohesity Cluster are returned
- `GET /irisservices/api/v1/public/protectionPolicies/`
  Returns the created Protection Policy

Dell EMC NetWorker Backup & Recovery

To enable Historic Collection for Dell EMC Networker, Advanced parameters need to be added.

Note: To add an advance parameter, see *NetBackup IT Analytics User Guide >> Customize with advanced parameters >> Adding an advance parameter* section.

- DELLEMC_NETWORKER_START_TIME
- DELLEMC_NETWORKER_END_TIME
- Date
  Format - 'yyyy-MM-ddTHH:mm:ss'.
  Example: 2018-05-10T16:00:03. This will be Dell EMC NetWorker server time.
- Host
  Add Dell EMC NetWorker servers, for which this advanced parameter should be applied.

REST API

global/jobs - This call is used in REST API to collect job details.

Appendix C

CRON Expressions for Policy and Report Schedules

This appendix includes the following topics:

- CRON expressions for policy probe schedules
- CRON expressions for scheduling reports

CRON expressions for policy probe schedules

Many Data Collector policy configurations require a schedule. Native CRON expressions are supported for fine-tuning a schedule. The CRON expression format for the policy configurations follows strings with five single space-separated time and date fields:

*	*	*	*	*
minutes	hours	day of month	month	day of the week

The following are the general guidelines when using special characters during the CRON expressions.

Table C-1 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
minutes	0-59 (0 is “on the hour”)

Table C-1 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)

- NetBackup IT Analytics supports a maximum of 80 characters in a CRON expression.

Special Characters:

- A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the seconds and minutes position is not permitted, as this would excessively trigger the probe—every second or minute.
- A forward slash (/) can be used to specify intervals.
- Use a dash (-) to specify a range.
- The CRON expression for the last day of the month, denoted by the letter L, is not supported.

Table C-2 Probe Schedule field examples of string with five single space-separated time and date fields

Probe Schedule Examples	Scheduled Run Time
0 14-15 * * 1	On the hour, every Monday, between 2 and 3pm **Note:** A zero in the minutes position denotes the beginning of the hour.
30 9-13 * * 1-5	9:30, 10:30, 11:30, 12:30, and 13:30, Monday through Friday.
0 */2 * * *	To run the probe every 2 hours, put */2 in the hour position. This schedules the probe at 2am, 4am, 6am, 8am, 10am, 12pm, 2pm, and so on.
*/30 * * * *	Every 30 minutes
*/20 9-18 * * *	Every 20 minutes between 9 am and 6 pm
*/30 * * * 1-5	Every 30 minutes, Monday through Friday

Table C-2 Probe Schedule field examples of string with five single space-separated time and date fields *(continued)*

Probe Schedule Examples	Scheduled Run Time
1 2 * * *	2:01 every day
30 9,11 * * *	9:30 and 11:30 every day

CRON expressions for scheduling reports

Many reports and dashboards may require a email or export schedule. Native CRON expressions are supported for fine-tuning a email or schedule. The format for scheduling reports and dashboard email and exports follows string with six single space-separated time and date fields:

*	*	*	*	*	*
second	minute	hour	day of the month	month	day of the week

The following are the general guidelines when using special characters during the CRON expressions.

Table C-3 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
second	0-59 in string with six single space-separated time and date fields
minutes	0-59 (0 is “on the hour”)
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)
■ NetBackup IT Analytics supports a maximum of 80 characters in a CRON expression.	
Special Characters:	

Table C-3 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
■ A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the seconds and minutes position is not permitted, as this would excessively trigger the probe—every second or minute.	
■ A forward slash (/) can be used to specify intervals.	
■ Use a dash (-) to specify a range.	
■ Use ? (“no specific value”) when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, to schedule the trigger on a particular day of the month (the 10th), but irrespective of the day-of-the-week that happens to be, specify “10” in the day-of-month field, and “?” in the day-of-week fie	
■ You can use forward slash (/) can be used to specify increments. For example, “0/15” in the seconds field means “the seconds 0, 15, 30, and 45”. And “5/15” in the seconds field means “the seconds 5, 20, 35, and 50”. You can also specify ‘/’ after the ‘’ character - in this case ‘’ is equivalent to having ‘0’ before the ‘/’. ‘1/3’ in the day-of-month field means “fire every 3 days starting on the first day of the month”.	
■ The CRON expression for the last day of the month, denoted by the letter L, is not supported.	

Table C-4 Report Schedule field examples of string with six single space-separated time and date fields

Report Schedule Examples	Schedule Run Time
0 0 * * * *	the top of every hour of every day.
*/10 * * * * *	every ten seconds.
0 0 8-10 * * *	8, 9 and 10 o'clock of every day.
0 0 6,19 * * *	6:00 AM and 7:00 PM every day.
0 0/30 8-10 * * *	8:00, 8:30, 9:00, 9:30, 10:00 and 10:30 every day.
0 0 0 25 12 ?	every Christmas Day at midnight.
0 15 10 * * ? 2010	run at 10:15 AM every day during the year 2010.

Table C-4 Report Schedule field examples of string with six single space-separated time and date fields *(continued)*

Report Schedule Examples	Schedule Run Time
0 0 12 1/5 * ?	run at 12 PM (noon) every 5 days every month, starting on the first day of the month.
0 0 0 1W * *	first weekday of the month at midnight
0 11 11 11 11 ?	run every November 11th at 11:11 AM.
0 0-5 14 * * ?	run every minute starting at 2 PM and ending at 2:05 PM, every day.

Appendix D

Maintenance Scenarios for Message Relay Server Certificate Generation

This appendix includes the following topics:

- Regenerate authentication certificate nearing expiry (or already expired)
- Recover inadvertently deleted aptare.ks file
- Authenticate new database with existing SSL certificates
- SSL certificate authentication for a new data collector

Regenerate authentication certificate nearing expiry (or already expired)

Data exporters and data senders, installed on the hosts from where data is collected, require certificates to establish authentic communication with message relay server and data sender installed on the data collector system. This section provides the procedure to regenerate such a certificate that has either expired or is nearing expiry.

To regenerate a certificate:

1. Login to the data collector system and navigate to its installation path: `/aptare/mbs/conf`.
2. Identify these files inside `/aptare/mbs/conf`:
   - `aptare_message_relay_certificate.pem`

- `aptare_message_relay_keystore.ks`
- `aptare_message_relay_keystore.properties`

3. Stop the Aptare Agent service on the data collector system.

   On a Windows system, you can stop the service from the Services Console, whereas you can use `./aptareagent stop` command on Unix.

4. Delete `aptare_message_relay_certificate.pem` and `aptare_message_relay_keystore.ks` files from `/aptare/mbs/conf`.

5. Start the Aptare Agent service on the data collector system.

   The `aptare_message_relay_certificate.pem` and `aptare_message_relay_keystore.ks` files are regenerated and will reappear inside the `/aptare/mbs/conf` folder.

   The data collector sends a REST request to the data receiver and publishes the new certificate in the database. The certificate is essential to enable communication between the message relay server and the data sender trust store. Hence, you must download the new certificate as described in the steps below and copy it to all the data senders.

To download the new certificate:

1. Login to the NetBackup IT Analytics Portal.

   Since the certificate was changed, the portal will display a notification which states:

   ```
   Data Collector SSL certificate has not been downloaded
   for collector(s): <data_collector_name>.
   ```

2. Go to **Admin** > **Data Collection** > **Collector Administration** and click the collector name to view its policies.
3. Double-click the policy name for which SSL certificate needs to be downloaded. The policy configuration window is displayed.
4. Click **Download SSL Certificate**. The certificate is downloaded to your system.
5. Copy the certificate to the data sender trust store.

Recover inadvertently deleted `aptare.ks` file

When `aptare.ks` gets deleted, there are no ways to encrypt/decrypt the keys stored in `aptare_message_relay_keystore.properties`. This procedure provides the steps to recover an inadvertently deleted keystore (aptare.ks) file.

To recover a keystore file:

1. Login to the data collector system and navigate to its installation path: `/Aptare/mbs/conf`.
2. Identify these files inside `/Aptare/mbs/conf`:
   - `aptare_message_relay_certificate.pem`
   - `aptare_message_relay_keystore.ks`
   - `aptare_message_relay_keystore.properties`
3. Stop the Aptare Agent service on the data collector system.

   On a Windows system, you can stop the service from the Services Console, whereas you can use `./aptareagent stop` command on Unix.
4. Delete these files from `/Aptare/mbs/conf`.
   - `aptare_message_relay_certificate.pem`
   - `aptare_message_relay_keystore.ks`
   - `aptare_message_relay_keystore.properties`
5. Login to the NetBackup IT Analytics Portal to generate a new keystore file.

   Since the certificate was changed, the portal will display a notification which states:

   ```
   Data Collector SSL certificate has not been downloaded
   for collector(s): <data_collector_name>.
   ```

6. Go to **Admin** > **Data Collection** > **Collector Administration** and click the collector name to view its policies.
7. Double-click the collector to invoke the **Edit Collector** window.
8. Copy the **Passcode** value and save it for later use.
9. Click **Generate Key** and download the key file.
10. Copy the key file to `/Aptare/mbs/conf` folder on the data collector system. Ensure the file name is same as that of the data collector on the portal.
11. On the data collector system, open the collector.properties file from `/Aptare/mbs/conf` and replace the **COLLECTOR_PASSWORD** value with the **Passcode** value copied from the **Edit Collector** window.
12. Save the `collector.properties` file and start the Aptare Agent service.

    After the service starts:

- A new `aptare.ks` is generated inside `/Aptare/mbs/conf` which consumes the new key file.
- . The `aptare_message_relay_certificate.pem`, `aptare_message_relay_keystore.ks`, and `aptare_message_relay_keystore.properties` files are generated later shortly.
- Since the certificate was changed, the portal will display a notification which states:

  ```
  Data Collector SSL certificate has not been downloaded
  for collector(s): <data_collector_name>.
  ```

13. On the NetBackup IT Analytics Portal, go to **Admin** > **Data Collection** > **Collector Administration** and click the collector name to view its policies.
14. Double-click the policy name for which SSL certificate needs to be downloaded. The policy configuration window is displayed.
15. Click **Download SSL Certificate**. The certificate is downloaded to your system.
16. Copy the certificate to the data sender trust store.

Authenticate new database with existing SSL certificates

When you install a new database, the SSL certificate entry is lost on the database host. Since the data collector runs on a separate system, it is unaware about the DB import and does not update certificate to the DB.

Perform the following steps to regenerate the `aptare_message_relay_certificate.pem` file and authenticate the new database:

1. Login to the data collector system and navigate to its installation path: `/Aptare/mbs/conf`.
2. Login to the data collector system and stop the Aptare Agent service on the data collector system.

   On a Windows system, you can stop the service from the Services Console, whereas you can use `./aptareagent stop` command on Unix.
3. Delete `aptare_message_relay_certificate.pem`
4. Start the Aptare Agent service on the data collector system.

Note: The `aptare_message_relay_certificate.pem` file need not be copied on the data sender as the same certificate file is just regenerated.

SSL certificate authentication for a new data collector

Whenever an old data collector is removed, you must replace it with a new data collector to maintain continuity. The new data collector creates new `aptare_message_relay_certificate.pem`, `aptare_message_relay_keystore.ks`, and`aptare_message_relay_keystore.properties` files. The certificate file is also regenerated during the collector installation and the certificate file in the database is refreshed. Administrator must download the SSL certificate from the respective policy configuration screens of the NetBackup IT Analytics Portal and copy it to the trust store of every data sender.