

APTARE IT Analytics Data Collector Installation Guide for Capacity Manager

Release 10.4.00

VERITAS™

APTARE IT Analytics Data Collector Installation Guide for Capacity Manager

Last updated: 2020-09-30

Legal Notice

Copyright © 2020 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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. VERITAS TECHNOLOGIES LLC 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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive.
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

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 Veritas website.

Veritas Services and Operations Readiness Tools (SORT)

Veritas 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

Chapter 1	Data Collection for Capacity Overview	12
	Data Collection for Capacity Overview	12
	Capacity Manager: Collection of Array Capacity Data	13
	Capacity Architecture Overview	13
	Which Data Collector Policies Are Needed?	15
	Planning Worksheets	16
	Storage Array Details	16
	Host Resources Details	17
Chapter 2	Pre-Installation Setup for Dell Compellent	18
	Pre-Installation Setup for Dell Compellent	18
	Prerequisites for Adding Data Collectors (Dell Compellent)	18
	Upgrade Troubleshooting: Microsoft SQL Server and Java 11	19
	Installation Overview (Dell Compellent)	20
	Adding a Dell Compellent Data Collector Policy	21
Chapter 3	Pre-Installation Setup for DELL EMC Elastic Cloud Storage (ECS)	25
	Pre-Installation Setup for DELL EMC Elastic Cloud Storage (ECS)	25
	Prerequisites for Adding Data Collectors - DELL EMC Elastic Cloud Storage (ECS)	26
	Installation Overview - DELL EMC Elastic Cloud Storage (ECS)	26
	Add a DELL EMC Elastic Cloud Storage (ECS) Data Collector Policy	27
Chapter 4	Pre-Installation Setup for EMC Data Domain Storage	32
	Architecture Overview (EMC Data Domain Storage)	32
	Prerequisites for Adding Data Collectors (EMC Data Domain Storage)	34
	Installation Overview (EMC Data Domain Storage)	34
	Add EMC Data Domain Servers	35

	Adding an EMC Data Domain Storage Data Collector Policy	37
Chapter 5	Pre-Installation Setup for EMC Isilon	47
	Pre-Installation Setup for EMC Isilon	47
	Prerequisites for Adding Data Collectors (EMC Isilon)	47
	Required Prerequisite: Configure the Isilon SNMP Service	48
	Optional Prerequisite: Configure Isilon Sudo Access	51
	Modify the sudo Configuration	51
	Installation Overview (EMC Isilon)	52
	Adding an EMC Isilon Data Collector Policy	52
Chapter 6	Pre-Installation Setup EMC Symmetrix	59
	Pre-Installation Setup EMC Symmetrix	59
	Prerequisites for Adding Data Collectors (EMC Symmetrix)	59
	Installation Overview (EMC Symmetrix)	60
	Adding an EMC Symmetrix Data Collector Policy	61
	If the EMC Solutions Enabler is on a Remote Server (Recommended)	67
Chapter 7	Pre-Installation Setup for Dell EMC Unity	70
	Pre-Installation Setup for Dell EMC Unity	70
	Prerequisites for Adding Data Collectors (Dell EMC Unity)	70
	Installation Overview (Dell EMC Unity)	71
	Add a Dell EMC Unity Data Collector Policy	72
Chapter 8	Pre-Installation Setup for EMC VNX Celerra	76
	Pre-Installation Setup for EMC VNX Celerra	76
	Prerequisites for Adding Data Collectors (EMC VNX Celerra)	76
	Setup for EMC VNX Celerra Arrays	77
	Configure a Read-Only User with an Operator Role	78
	Start the XML API Server	79
	Installation Overview (EMC VNX Celerra)	79
	Adding an EMC VNX Celerra Data Collector Policy	80
Chapter 9	Pre-Installation Setup for EMC VNX CLARiiON	87
	Pre-Installation Setup for EMC VNX CLARiiON	87
	Prerequisites for Adding Data Collectors (EMC VNX CLARiiON)	87
	Installation Overview (EMC VNX CLARiiON)	88
	Adding an EMC VNX (CLARiiON) Data Collector Policy	89

Chapter 10	Pre-Installation Setup for EMC VPLEX	96
	Pre-Installation Setup for EMC VPLEX	96
	Prerequisites for Adding Data Collectors (EMC VPLEX)	96
	Installation Overview (EMC VPLEX)	97
	Adding a EMC VPLEX Data Collector Policy	97
Chapter 11	Pre-Installation Setup for EMC XtremIO	102
	Pre-Installation Setup for EMC XtremIO	102
	Prerequisites for Adding Data Collectors (EMC XtremIO)	102
	Installation Overview (EMC XtremIO)	103
	Add an EMC XtremIO Data Collector Policy	103
Chapter 12	Pre-Installation Setup for Hitachi Block	108
	Pre-Installation Setup for Hitachi Block	108
	Prerequisites for Adding Data Collectors (Hitachi Block)	108
	Installation Overview (Hitachi Block Storage)	109
	Adding a Hitachi Block Storage Data Collector Policy	110
	Configuring a Hitachi Device Manager User	116
	Validate the User ID Access	117
	Configuring a Collector for Hitachi NAS Block Storage	119
	Adding an HP Command View Advanced Data Collector Policy	119
Chapter 13	Pre-Installation Setup for Hitachi Content Platform (HCP)	120
	Pre-Installation Setup for Hitachi Content Platform (HCP)	120
	Prerequisites for Adding Data Collectors (Hitachi Content Platform)	121
	Installation Overview (Hitachi Content Platform)	121
	Add a Hitachi Content Platform (HCP) Data Collector Policy	122
	Setting Up Permissions for an HCP Local User or Active Directory User	128
	Hitachi Content Platform System Management Console	129
	Local Users	129
	Local Users and Active Directory Users	130
	Hitachi Content Platform Tenant Management Console	130
	Local Users	131
	Active Directory Users	131
	Local Users and Active Directory Users	132

Chapter 14	Pre-Installation Setup Hitachi NAS	133
	Pre-Installation Setup Hitachi NAS	133
	Prerequisites for Adding Data Collectors (Hitachi NAS - HNAS)	133
	Installation Overview (Hitachi NAS - HNAS)	134
	Adding a Hitachi NAS (HNAS) Data Collector Policy	135
	HNAS Configuration Requirements	135
	Configuring SSC Access	135
	Adding the Collector	136
Chapter 15	Host Inventory Pre-Installation Setup	141
	Host Access Privileges, Sudo Commands, Ports, and WMI Proxy	
	Requirements	142
	Access Requirements by OS	143
	Host Inventory Pre-Installation Setup	143
	Plan Host Data Collection	144
	WMI Proxy Requirements for Windows Host Data Collection	144
	Host Access Requirements	145
	Verify Command Paths	147
	Host Inventory Configuration Steps	147
	Host Inventory Setup Overview	148
	Host Inventory Maintenance Overview	149
	Before Discovering Hosts	150
	Configure/Search the Host Inventory	151
	Manage Credentials	152
	Example of Credentials for Windows Hosts	153
	Manage WMI Proxy	155
	Manage Paths	157
	Manage Access Control	158
	Host Inventory Management	161
	Configure Host Discovery Policies to Populate the Host Inventory	
	162
	Discovery Policy Considerations	162
	Configure a Discovery Policy	163
	Collecting from Clustered SQL Server and Oracle Applications	
	166
	Execute and Monitor Host Discovery	167
	Execute a Discovery Policy	167
	Monitor Discovery Processes	168
	Validate Host Connectivity	169
	Validate Hosts	169
	Validation History	170
	Show Errors	170

	Filter the Host Inventory - Hide/Unhide, Remove	171
	Host Inventory Search and Host Inventory Export	172
	Basic Search	172
	Pre-Defined Search	172
	Advanced Search Parameters	173
	Export the Host Inventory	173
	Configure and Edit Host Probes	174
	Host Inventory File Analytics Probe	176
	File Analytics Probe Configurations by Operating System	176
	Both Windows and Linux Servers	177
	Best Practices for Host Inventory File Analytics Probes	177
	Propagate Probe Settings: Copy Probes, Paste Probes	177
	Example of Probe Copy/Paste	177
	Probe Settings	178
Chapter 16	Pre-Installation Setup for HP 3PAR	184
	Pre-Installation Setup for HP 3PAR	184
	Prerequisites for Adding Data Collectors (HP 3PAR)	184
	Installation Overview (HP 3PAR)	185
	Adding an HP 3PAR Data Collector Policy	185
	Adding an HP Command View Advanced Data Collector Policy	191
Chapter 17	Pre-Installation Setup for HP EVA	192
	Pre-Installation Setup for HP EVA	192
	Prerequisites for Adding Data Collectors (HP EVA)	192
	Installation Overview (HP EVA)	193
	Adding an HP EVA Data Collector Policy	193
Chapter 18	Pre-Installation Setup for Huawei OceanStor	199
	Pre-Installation Setup for Huawei OceanStor	199
	Prerequisites for Adding Data Collectors (Huawei OceanStor)	199
	Installation Overview	200
	Add a Huawei OceanStor Data Collector Policy	200
Chapter 19	Pre-Installation Setup for IBM Enterprise	205
	Pre-Installation Setup for IBM Enterprise	205
	Prerequisites for Adding Data Collectors (IBM Enterprise)	205
	Installation Overview (IBM Enterprise)	207
	Adding an IBM Enterprise Data Collector Policy	207

Chapter 20	Pre-Installation Setup for NetApp E-Series	211
	Pre-Installation Setup for NetApp E-Series	211
	Prerequisites for Adding Data Collectors (NetApp E-Series)	211
	Installation Overview (NetApp E-Series)	212
	Adding a NetApp E-Series Data Collector Policy	212
Chapter 21	Pre-Installation Setup for IBM SVC	219
	Pre-Installation Setup for IBM SVC	219
	Prerequisites for Adding Data Collectors (IBM SVC)	219
	Installation Overview (IBM SVC)	220
	Adding an IBM SVC Data Collector Policy	221
Chapter 22	Pre-Installation Setup for IBM XIV	227
	Pre-Installation Setup for IBM XIV	227
	Prerequisites for Adding Data Collectors (IBM XIV)	227
	Installation Overview (IBM XIV)	228
	Adding an IBM XIV Data Collector Policy	228
Chapter 23	Pre-Installation Setup for INFINIDAT InfiniBox	234
	Pre-Installation Setup for INFINIDAT InfiniBox	234
	Prerequisites for Adding Data Collectors (INFINIDAT InfiniBox)	234
	Installation Overview	235
	Add an INFINIDAT InfiniBox Data Collector Policy	235
Chapter 24	Pre-Installation Setup for NetApp-7	240
	Pre-Installation Setup for NetApp-7	240
	Prerequisites for Adding Data Collectors (NetApp-7)	240
	Data Collector Configurations Specific to NetApp-7	241
	If HTTP Access is Disabled on the vFiler	241
	Installation Overview (NetApp-7)	242
	Adding a NetApp Data Collector Policy	242
	Testing the Collection	248
	Creating a NetApp User with API Privileges	248

Chapter 25	Pre-Installation Setup for Microsoft Windows Server	250
	Pre-Installation Setup for Microsoft Windows Server	250
	Prerequisites for Adding Data Collectors (Microsoft Windows Server)	250
	Collecting from Applications and Services Logs	252
	Installation Overview (Microsoft Windows Server)	252
	Add a Microsoft Windows Server Data Collector Policy	253
Chapter 26	Pre-Installation Setup for NetApp Cluster	257
	Pre-Installation Setup for NetApp Cluster	257
	Prerequisites for Adding Data Collectors (NetApp Cluster)	257
	Installation Overview (NetApp Cluster-Mode)	258
	Adding a NetApp Cluster-Mode Data Collector Policy	259
	Testing the Collection	264
	Creating a NetApp Cluster-Mode Read-Only User	264
Chapter 27	Pre-Installation Setup for Pure Storage FlashArray	266
	Pre-Installation Setup for Pure Storage FlashArray	266
	Prerequisites for Adding Data Collectors (Pure Storage FlashArray)	266
	Installation Overview (Pure Storage FlashArray)	267
	Add a Pure Storage FlashArray Data Collector Policy	267
Chapter 28	Pre-Installation Setup for Veritas NetBackup Appliance	272
	Overview	272
	Prerequisites for Adding Data Collectors (Veritas NetBackup Appliance)	272
	Installation Overview (Veritas NetBackup Appliance)	273
	Adding a Veritas NetBackup Appliance Data Collector Policy	274
Chapter 29	Installing the Data Collector Software	278
	Introduction	278
	Installing the WMI Proxy Service (Windows Host Resources only)	279
	Testing WMI Connectivity	283
	Installing Data Collector Software: From the Internet	286

	Installing Data Collector Software: No Internet Available from the Data Collector Server	286
	Installing Data Collector Software: UI Deployment	287
	Installing Data Collector Software: From the Console	289
Chapter 30	Validating Data Collection	293
	Validation Methods	293
	Data Collectors: Vendor-Specific Validation Methods	294
	Working with On-Demand Data Collection	296
	Using the CLI Checkinstall Utility	298
	List Data Collector Configurations	299
Chapter 31	Uninstalling the Data Collector	300
	Uninstall the Data Collector on Linux	300
	Uninstall the Data Collector on Windows	301
Chapter 32	Manually Starting the Data Collector	302
	Introduction	302
Appendix A	Firewall Configuration: Default Ports	304
	Firewall Configuration: Default Ports	304

Data Collection for Capacity Overview

This chapter includes the following topics:

- [Data Collection for Capacity Overview](#)
- [Capacity Manager: Collection of Array Capacity Data](#)
- [Capacity Architecture Overview](#)
- [Which Data Collector Policies Are Needed?](#)
- [Planning Worksheets](#)
- [Storage Array Details](#)
- [Host Resources Details](#)

Data Collection for Capacity Overview

The Data Collector is a centralized and remotely managed data collection mechanism. This Java application is responsible for interfacing with enterprise objects, such as backup servers and storage arrays, gathering information related to storage resource management.

The APTARE 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 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.

The APTARE Data Collector obtains all of its monitoring rules from a APTARE Data Collector configuration file. This file resides in the Reporting Database in XML format. When the APTARE 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.

Capacity Manager: Collection of Array Capacity Data

- The Data Collector communicates with the storage array's system service processor (SSP) and hosts to gather storage capacity data.
- A single Data Collector can include all supported storage types--Dell, EMC, NetApp, IBM, HP, or Hitachi. In fact, this single Data Collector can be used for other enterprise objects, such as backup jobs.
- The EMC Symmetrix Data Collector needs to be installed on the servers that manage the Symmetrix arrays.
- Host Resources do 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 install a Host Resources Data Collector independently.
- Host probes can be configured to gather data and statistics--Memory, Network, Processes, Processor, System, Capacity, Capacity-HBA, Capacity-ISCSI, Capacity-Volume Manager, Capacity-Multi-Pathing, Oracle, Oracle ASM, Microsoft Exchange, SQL Server, File Analytics.

Capacity Architecture Overview

Capacity Manager provides end-to-end storage capacity reporting from the hosts to the storage arrays. The Data Collector is a software component that is responsible for interfacing with one or many storage arrays for information related to the capacity management environment. In most cases, the Data Collector software module can reside on any server within your network that is Java 1.8 compatible and, where applicable, has a working copy of specific storage array command line utilities already installed. The exception is EMC Symmetrix, which requires the Data Collector to reside on the server that manages the arrays. The following diagram illustrates how the Capacity Manager Data Collector could be deployed in your environment:

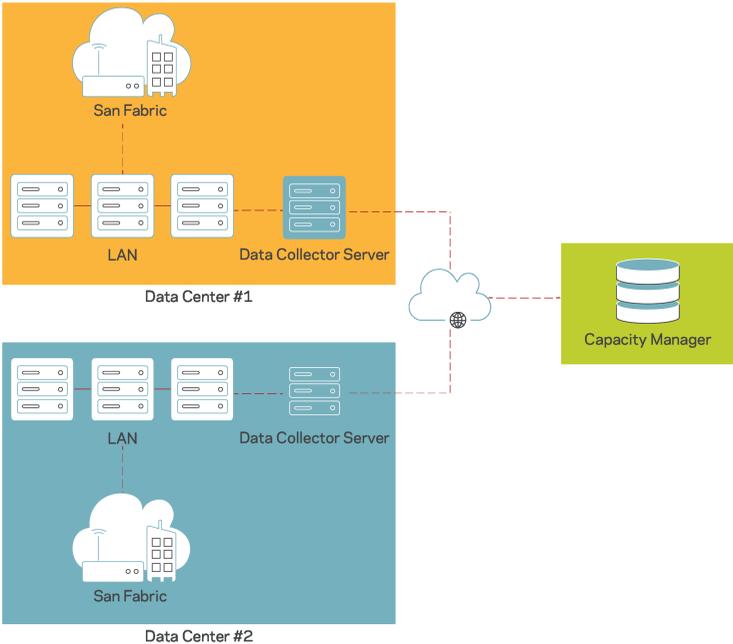


Figure 1.1 Data Collector for Capacity Manager

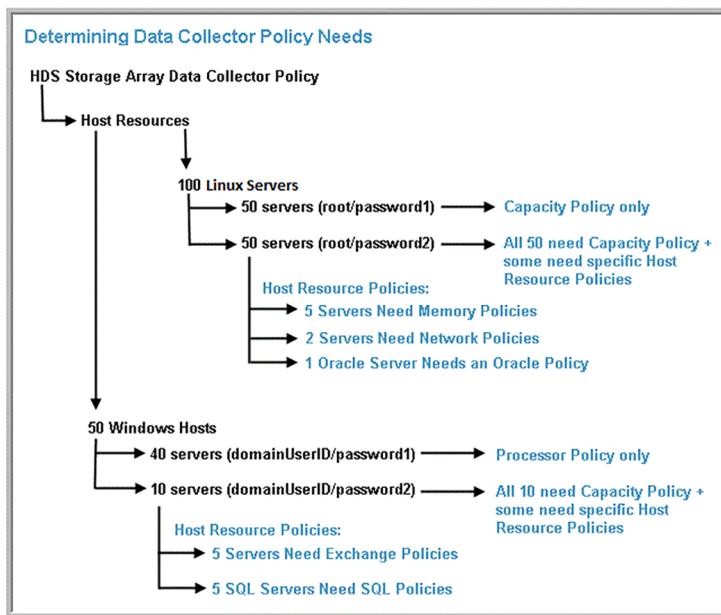
The Data Collector obtains all of its monitoring rules from a configuration file maintained in the database. This file is called the Data Collector Configuration File and is stored in the database in XML format. When the Data Collector is first started, it downloads the Data Collector Configuration File from the database. The Data Collector uses this file to determine the list of storage arrays that are to be monitored and included in its data polling.

In most cases, a single instance of the Data Collector can support any number of storage arrays. The only real limitation is the memory and CPU processing power of the server on which the Data Collector resides. For each storage array, the Data Collector will establish connections to the database. The Data Collector Configuration file contains all the connection information for each server including such parameters as the host name / IP address of the server.

The Data Collector communicates with the storage array's system service processor (SSP) to gather storage capacity data. The information is then sent via http(s) to the Portal. Users can then access the Portal via a web browser.

Which Data Collector Policies Are Needed?

Policies need to be configured via the Portal to establish communication with the installed Data Collectors. The following example illustrates a typical Capacity Manager deployment for array and host data collection.



In this example of 100 Linux servers:

- 50 servers will have only capacity information collected
- Another 50 servers will have capacity information collected, plus some of those servers will also have Host Resources data collected:
 - 5 Memory
 - 2 Network
 - 1 Oracle Server

Planning Worksheets

Use the following worksheets to gather the configuration information required for Data Collector deployment.

IMPORTANT NOTES:

- The EMC Symmetrix Data Collector needs to be installed on the servers that manage the Symmetrix arrays.
- EMC CLARiiON NaviSuite requires a view-only user ID. User IDs may be different for each array.
- NetApp storage requires a view-only User ID, which may be different for each array set.

Storage Array Details

List all storage arrays for which you want to collect data.

#	Array Type	Array Name	Storage Array IP Address	Device Manager Server (Hitachi)	Data Collector Server IP Address	User ID & Password
Ex:	Hitachi	HD1000	203.23.100	203.100	203.10.5	
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Host Resources Details

List all hosts for which you want to collect data.

#	Host Name	Storage Array IP Address	User ID	OS	Applications /Databases
Example Host	kiwi	203.23.10.1	Admin	AIX	Oracle
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

Pre-Installation Setup for Dell Compellent

This chapter includes the following topics:

- [Pre-Installation Setup for Dell Compellent](#)
- [Prerequisites for Adding Data Collectors \(Dell Compellent\)](#)
- [Upgrade Troubleshooting: Microsoft SQL Server and Java 11](#)
- [Installation Overview \(Dell Compellent\)](#)
- [Adding a Dell Compellent Data Collector Policy](#)

Pre-Installation Setup for Dell Compellent

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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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).

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 APTARE 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 (Dell Compellent)

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 Compellent 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.

Validate the Data Collector installation.
6. See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

Adding a Dell Compellent 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.

The screenshot shows a configuration window titled "Dell Compellent Data Collector Policy". The window contains several sections for configuring data collection:

- Collector's Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Enterprise Manager Address:***: An empty text input field.
- SMI-S Port:***: A text input field containing "5988".
- Use HTTPS:**: An unchecked checkbox.
- SMI-S User ID:***: An empty text input field.
- Password:***: An empty text input field.
- Repeat Password:***: An empty text input field.
- Enterprise Manager DB Address:***: An empty text input field.
- DB Port:***: A text input field containing "1433".
- DB User ID:***: An empty text input field.
- Password:***: An empty text input field.
- Repeat Password:***: An empty text input field.

Below the configuration fields are two sections:

- Active Probes:** A list of checkboxes. "Array Details" is checked, and "Array Performance" is unchecked.
- Schedules:** Two dropdown menus. The first is set to "Every 5 hours, at minute 1" and the second is set to "Every 15 minutes".

At the bottom of the window, there is a "Notes:" section with a large empty text area, and a row of buttons: "OK", "Cancel", "Help", and a "Privacy Policy" link.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>To find your Domain name select Admin > Domains > Domains.</p>
Enterprise Manager Address*	Specify the IP address or host name of the Dell Compellent Enterprise Manager.
SMI-S Port*	The port value defaults to 5988. This is the port for access to the Enterprise Manager SMI-S Provider.
Use HTTPS	This option is turned off by default. Check it to have the Data Collector use HTTPS to connect to the Enterprise Manager SMI-S Provider.
SMI-S User ID*	The user ID for logging into Enterprise Manager SMI-S Provider to collect Compellent data.
Password*	The password associated with the User ID. Current versions of Compellent Enterprise Manager have an 8-character limit for SMI-S passwords. This limit may be changed in future versions of Enterprise Manager.
Repeat Password*	Repeat the password associated with the User ID.
Enterprise Manager DB Address*	Specify the IP address or host name of the Compellent Enterprise Manager database.

Field	Description
DB Port*	Specify the port used by the Enterprise Manager database (defaults to 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 User ID*	Specify the database User ID. The SQL login must be a SQL Server authentication. Using Microsoft SQL Server Management Studio, on the Server Roles screen, only public needs to be checked. On the User Mapping screen, public and db_datareader should be checked for the compsadb database.
Password*	The password associated with the User ID.
Repeat Password*	Repeat the password associated with the User ID.
Array Details	<p>Check the box if you are collecting array details.</p> <p>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.</p> <p>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.</p>
Array Performance	<p>Check the box if you are collecting performance data.</p> <p>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.</p> <p>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.</p>
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.

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

The screenshot shows a configuration dialog box titled "DELL EMC Elastic Cloud Storage (ECS) Data Collector Policy". The dialog contains the following fields and options:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Management Server Addresses:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A password input field with a single dot visible.
- Active Probes:** A section with two checkboxes:
 - Array Details
 - Array Performance
- Schedules:** A section with two time-based schedules:
 - Every day at 02:01 (with a clock icon)
 - Every 15 minutes (with a clock icon)
- Notes:** A text area containing the text: "Password for the DELL EMC Elastic Cloud Storage (ECS) storage system."
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" are located at the bottom of the dialog.

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

Field	Description
Collector Domain	<p>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.</p>
Policy Domain	<p>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.</p> <p>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.</p> <p>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.</p>
Management Server Addresses	<p>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</p> <p>To collect from a Cluster, enter the IP address of only one of the management servers.</p>
User ID*	<p>This field is required. View-only User ID and password for the DELL EMC Elastic Cloud Storage (ECS) storage system.</p>
Password*	<p>This field is required. Password for the DELL EMC Elastic Cloud Storage (ECS) storage system.</p>

Field	Description
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.
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>

Field	Description
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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.

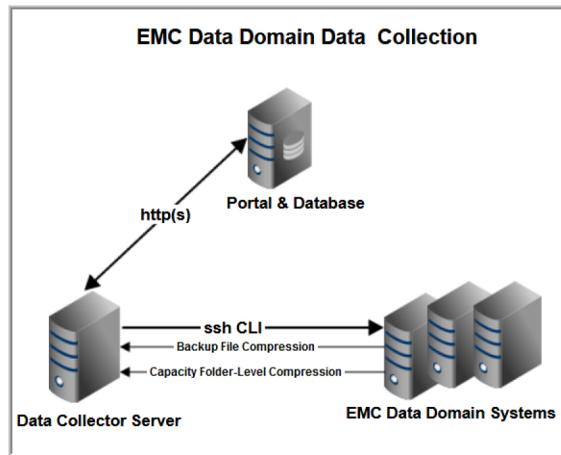


Figure 2 Data Collector in an EMC Data Domain Environment

The APTARE 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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.
- Port used by the Data Domain Data Collector: **Port 22 for SSH.**

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 APTARE IT Analytics Data Collector Pre-Installation worksheet, add the Data Domain server(s) to APTARE 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 35.	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

Field	Description	Sample Value
Repeat Password	The password associated with the User ID.	Pwd1
Folder-Level Compression	<p>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.</p> <p>The folders should start with /data/col1</p> <p>Warning: Choosing to exclude compression collection with an empty folder list may cause collection to take several hours to complete.</p>	/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.

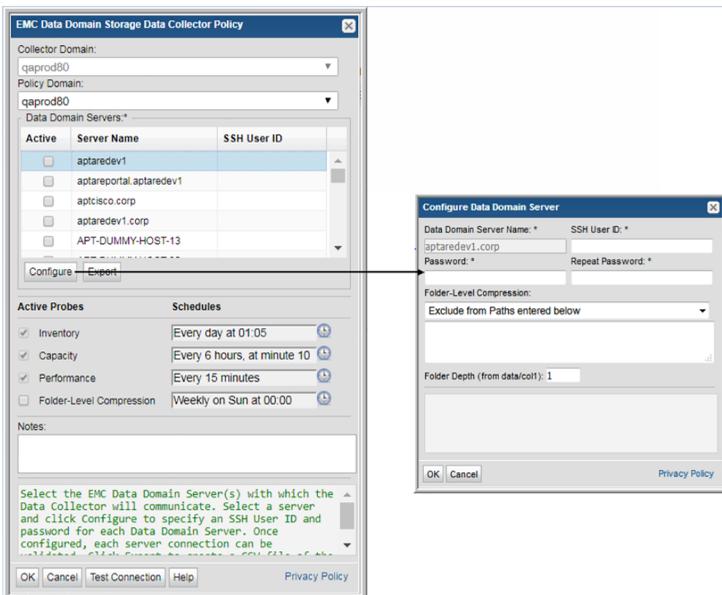
To add the policy

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>To find your Domain name select Admin > Domains > Domains.</p>	yourdomain

Field	Description	Sample Value
Data Domain Servers*	<p>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.</p> <p>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.</p> <p>See “Add EMC Data Domain Servers” on page 35.</p>	
SSH User ID*	<p>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.</p>	Administrator
Password	<p>The password associated with the User ID.</p>	Pwd1
Configure	<p>Select a Data Domain server and click Configure to enter the SSH credentials that will be used to access the server.</p>	
Export	<p>Click Export to retrieve a list of all the Data Domain servers in a comma-separated values file.</p>	

Field	Description	Sample Value
Inventory Probe	<p>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.</p> <p>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.</p>	
Capacity Probe	<p>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.</p> <p>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.</p>	

Field	Description	Sample Value
Performance Probe	<p>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.</p> <p>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.</p>	

Field	Description	Sample Value
Folder-Level Compression Probe	<p>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 Data Domain Boost connections, CIFS shares or NFS mounts.</p> <p>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.</p> <p>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.</p> <p>Warning: Choosing to exclude compression collection with an empty folder list may cause collection to take several hours to complete.</p>	

Field	Description	Sample Value
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	<p>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.</p> <p>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.</p> <p>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.</p>	

- 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.

Pre-Installation Setup for EMC Isilon

This chapter includes the following topics:

- [Pre-Installation Setup for EMC Isilon](#)
- [Prerequisites for Adding Data Collectors \(EMC Isilon\)](#)
- [Required Prerequisite: Configure the Isilon SNMP Service](#)
- [Optional Prerequisite: 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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).

Required Prerequisite: Configure the Isilon SNMP Service

Required Configuration for Isilon Data Collection

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:

Settings
General Settings

Protocol access:

- Allow access via SNMP v1 and SNMP v2c only
- Allow access via SNMP v3 only
- Allow access via SNMP v1, SNMP v2c and SNMP v3

- If SNMP v2c is allowed, then the **read-only community** string must be set.

SNMP v1/v2c Settings

Read-only community:*

- SNMP v1, v2c, and v3
- Enable access:

Settings
General Settings

Protocol access:

- Allow access via SNMP v1 and SNMP v2c only
- Allow access via SNMP v3 only
- Allow access via SNMP v1, SNMP v2c and SNMP v3

- When SNMP v2c is allowed, the **read-only community** string must be set.

SNMP v1/v2c Settings

Read-only community:*

- 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 Settings

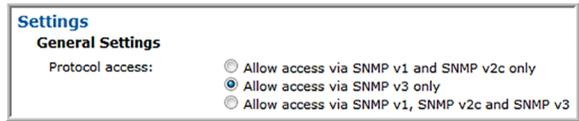
Read-only user:*

SNMP v3 password:

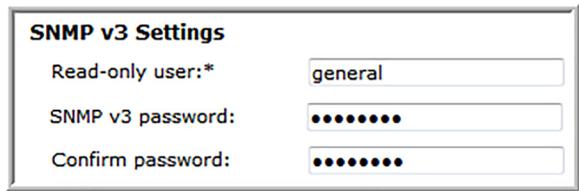
Confirm password:

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
```

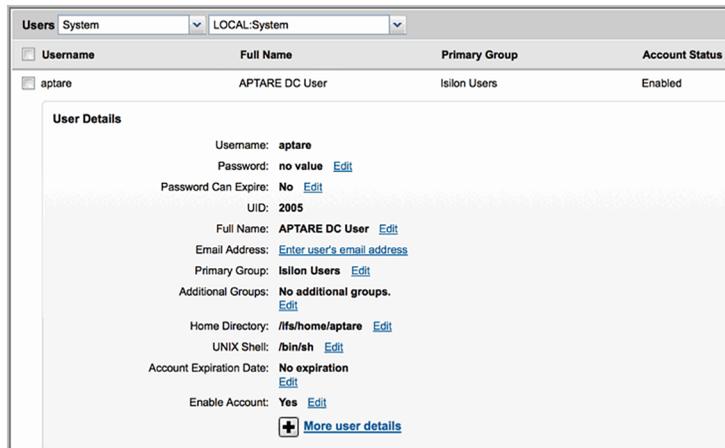
Optional Prerequisite: Configure Isilon Sudo Access

Optional Configuration for Isilon Data Collection

Collection of Isilon data requires root privileges. If your security requirements require sudo access to provide temporary, elevated privileges, use the instructions in this section.

The commands in this section are for Isilon OneFS v7.0. Verify command path names if using subsequent 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.



The screenshot shows the 'Users' management page in the Isilon administrative web interface. At the top, there are dropdown menus for 'System' (set to 'System') and 'LOCAL: System' (set to 'LOCAL: System'). Below these is a table with columns: Username, Full Name, Primary Group, and Account Status. A single user 'aptare' is listed with Full Name 'APTARE DC User', Primary Group 'Isilon Users', and Account Status 'Enabled'. Below the table is a 'User Details' section for the 'aptare' user. The details include: Username: aptare; Password: no value (with an 'Edit' link); Password Can Expire: No (with an 'Edit' link); UID: 2005; Full Name: APTARE DC User (with an 'Edit' link); Email Address: Enter user's email address (with an 'Edit' link); Primary Group: Isilon Users (with an 'Edit' link); Additional Groups: No additional groups. (with an 'Edit' link); Home Directory: /ifs/home/aptare (with an 'Edit' link); UNIX Shell: /bin/sh (with an 'Edit' link); Account Expiration Date: No expiration (with an 'Edit' link); Enable Account: Yes (with an 'Edit' link). At the bottom of the details section is a '+ More user details' link.

2. Log in to any node of the cluster as **root**.
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. **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. Use `isi_visudo` if available.

```
# isi_visudo
```

```
# visudo -f /usr/local/etc/sudoers.d/aptare
```

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.

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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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.

The screenshot shows a dialog box titled "EMC Isilon Data Collector Policy" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Collector Domain:** A dropdown menu showing "1-domain-for-pat".
- Policy Domain:** A dropdown menu showing "1-domain-for-pat".
- Cluster Addresses:*** An empty text input field.
- User ID:*** and **Password:***: Two empty text input fields.
- Repeat Password:***: An empty text input field.
- Active Probes:** A section with two checkboxes:
 - Cluster Details
 - Cluster Performance
- Schedules:** A section with two dropdown menus:
 - The first dropdown is set to "Every day at 03:01" and has a clock icon.
 - The second dropdown is set to "Every 15 minutes" and has a clock icon.
- Notes:** Two empty text input fields.
- Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom left. A "Privacy Policy" link is located at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
Domain	<p>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.</p> <p>If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy.</p> <p>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.</p>	yourdomain
Cluster Addresses*	<p>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.</p>	
User ID and Password*	<p>SSH User ID and password for accessing the EMC Isilon cluster.</p>	

Field	Description	Sample Value
Cluster Details Schedule	<p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	Every day at 03:01

Field	Description	Sample Value
Cluster Performance Schedule	<p>Check the check box to activate cluster performance collection to populate performance metrics for EMC Isilon clusters.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	Every 15 minutes
Notes	<p>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.</p>	

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

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

EMC Symmetrix Data Collector Policy

Collector Domain:
 1-domain-for-pat

Policy Domain:
 1-domain-for-pat

SYMAPI Service Name(s):

EMC Symmetrix Client Software Location:*

Arrays to Exclude:

Unisphere Server Addresses:*

User ID:* Password:*

admin@etchsketchteam •

Active Probes	Schedules
<input checked="" type="checkbox"/> Array Details	Every 8 hours, at minute 30
<input type="checkbox"/> Array Performance	Every 15 minutes
<input type="checkbox"/> Enhanced Symmetrix Performance	Every 15 minutes
<input type="checkbox"/> Global Cache	Every 12 hours, at minute 0

Notes:

Password for all the Unisphere servers.

OK Cancel Test Connection Help

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
SYMAPI Service Names	<p>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/</p> <p>This option is only used with remote host configuration, not when the Data Collector is the primary Solutions Enabler host.</p> <p>See also:</p> <p>See "If the EMC Solutions Enabler is on a Remote Server (Recommended)" on page 67.</p>	SYMAPI_SECURE
EMC Symmetrix Client Software Location *	<p>This location refers to the location on the Data Collector.</p> <p>Linux: /usr/symcli/bin</p> <p>Windows: C:\Program Files\EMC\symCLI\bin</p> <p>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.</p>	
Arrays to Exclude	<p>Enter one or more Symmetrix SymIDs to be excluded. Comma-separated SymIDs are supported. Example: 000190102500, 000190102501</p>	
Unisphere Server Addresses*	<p>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).</p>	
User ID/Password*	<p>User ID and password required for Unisphere servers/hosts.</p>	

Field	Description	Sample Value
Active Probes and Schedules		
Array Details	<p>Click the check box to activate array details collection.</p> <p>Note that at least one collection from this array must be performed BEFORE array performance data can be collected.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p>* / 30 * * * * means every 30 minutes</p> <p>* / 20 9-18 * * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>* / 10 * * * 1-5 means every 10 minutes Mon - Fri.</p> <p>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.</p>	

Field	Description	Sample Value
Array Performance	<p>Click check box to activate array performance collection.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p>* /30 * * * * means every 30 minutes</p> <p>* /20 9-18 * * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>* /10 * * * 1-5 means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Enhanced Symmetrix Performance	<p>Click the check box to collect performance data for EMC Symmetrix storage systems using Unisphere for VMAX.</p> <p>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.</p>	
Global Cache	<p>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.</p>	

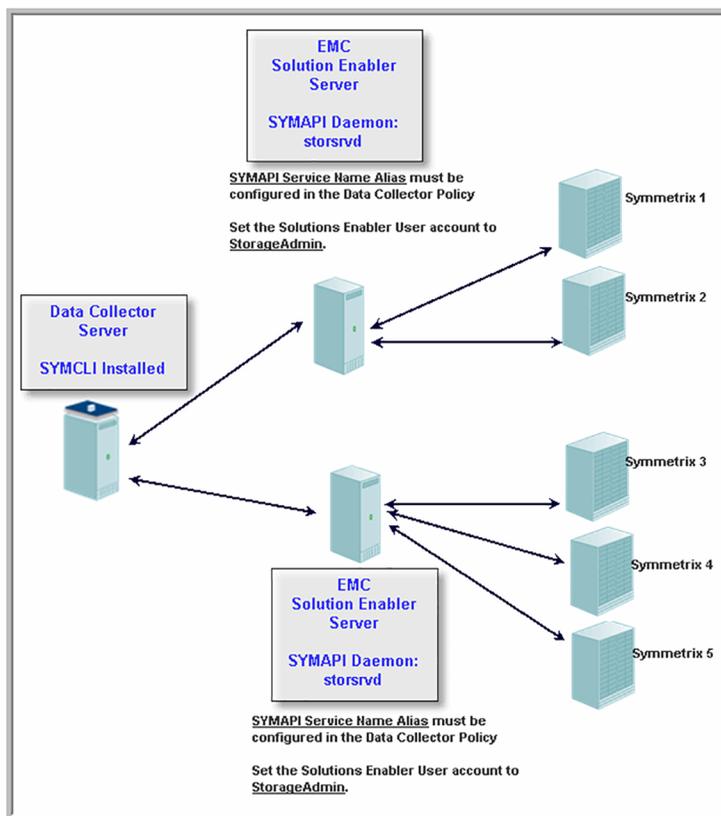
Field	Description	Sample Value
Notes	<p>Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable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

- 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: **stordaeomon 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: **stordaeomon start storsrvd**

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.
- Read-only credentials (username and password) are 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.

See ["Installing the WMI Proxy Service \(Windows Host Resources only\)"](#) on page 279.

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.

The screenshot shows a configuration window titled "Dell EMC Unity Data Collector Policy". It contains the following fields and options:

- Collector Domain:** A dropdown menu with "AvamarDomain" selected.
- Policy Domain:** A dropdown menu with "AvamarDomain" selected.
- Storage System Addresses:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A password input field with a masked character "•".
- Active Probes:** A section with two checkboxes:
 - Array Details
 - Array Performance
- Schedules:** A section with two schedule input fields:
 - Every day at 02:01 (with a plus icon)
 - Every 15 minutes (with a minus icon)
- Notes:** A text area containing the text "Password for the Dell EMC Unity Storage System." in green.
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" are located at the bottom of the dialog.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
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	<p>Click to activate array performance data collection. By default, it is collected every 15 minutes.</p> <p>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.</p>

Field	Description
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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 APTARE 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.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- 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.
- For performance reasons, do not install Data Collectors on the same server as the APTARE 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 77.
- See [“Configure a Read-Only User with an Operator Role”](#) on page 78.
- See [“Start the XML API Server”](#) on page 79.

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 master 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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)**.

The screenshot shows a configuration window titled "EMC VNX (Celerra) Data Collector Policy". The window contains the following fields and options:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Array Addresses:*** An empty text area.
- User ID:*** and **Password:*** text input fields.
- Repeat Password:*** text input field.
- Active Probes** section:
 - Array Details**
 - Active Directory Configuration**
- Schedules** section:
 - Every 12 hours, at minute 1 (with a clock icon)
 - Every day at 00:01 (with a clock icon)
- Domain Name:** text input field.
- Host Address:** text input field.
- User ID:** text input field.
- Password:** text input field.
- Repeat Password:** text input field.
- Port Number:** text input field with "389" entered.
- SSL Enabled**
- Notes:** A large empty text area.

At the bottom of the window, there are buttons for **OK**, **Cancel**, **Help**, and a **Privacy Policy** link.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
Array Addresses*	<p>Enter one or more VNX (Celerra) storage array address(es) separated by commas. List only one Control Station IP address per array.</p> <p>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.</p>	
User ID*	<p>Enter a User ID for the VNX array. This ID must have an Operator role, which enables read-only privileges.</p>	
Password*	<p>Password associated with the User ID</p>	
Repeat Password*	<p>Password associated with the User ID</p>	

Field	Description	Sample Value
Array Details	<p>Check the box to activate the collection of array details.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Active Directory Configuration	<p>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.</p> <p>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.</p> <p>Click the clock icon to create a schedule.</p>	

Field	Description	Sample Value
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.	

Field	Description	Sample Value
Port Number	Enter the network port used by Active Directory. This is a mandatory field if you have checked Active Directory Configuration.	
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.

Pre-Installation Setup for EMC VNX CLARiiON

This chapter includes the following topics:

- [Pre-Installation Setup for EMC VNX CLARiiON](#)
- [Prerequisites for Adding Data Collectors \(EMC VNX CLARiiON\)](#)
- [Installation Overview \(EMC VNX CLARiiON\)](#)
- [Adding an EMC VNX \(CLARiiON\) Data Collector Policy](#)

Pre-Installation Setup for EMC VNX CLARiiON

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 CLARiiON)

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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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 CLARiiON 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 CLARiiON)

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 CLARiiON 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
6. Validate the Data Collector installation.

Adding an EMC VNX (CLARiiON) 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.

The screenshot shows a configuration dialog box titled "EMC VNX (CLARiiON) Data Collector Policy". The dialog contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Array Addresses:*** An empty text input field.
- EMC Navi Client Software Location:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A password input field with a masked character "•".
- Active Probes:** A section with two checkboxes:
 - Array Details
 - Array Performance
- Schedules:** A section with two schedule inputs:
 - Every 6 hours, at minute 1 (with a clock icon)
 - Every 15 minutes (with a clock icon)
- Notes:** An empty text area.
- A green message box at the bottom states: "Password associated with the User ID."
- Buttons at the bottom: OK, Cancel, Test Connection, Help, and a link for 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<code>yourdomain</code>

Field	Description	Sample Value
Array Addresses*	<p>Enter one or more CLARiiON storage array address(es) separated by commas.</p> <p>List only one SP (storage processor) IP address per array.</p> <p>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:</p> <p><IP address>:<port number></p>	172.16.1.1:445
EMC Navi Client Software Location*	<p>For example:</p> <p>Linux: /opt/Navisphere/bin</p> <p>Windows: C:\Program Files\EMC\NavisphereCLI\</p>	
User ID*	<p>Create a Global user with operator privileges for CLARiiON NaviSuite (VNX Block).</p>	Administrator
Password*	<p>The password is encrypted prior to saving in the APTARE IT Analytics database and is never visible in any part of the application.</p>	Password1
Notes	<p>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.</p>	

Field	Description	Sample Value
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>	

Field	Description	Sample Value
Array Details	<p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Array Performance	<p>Activate array performance collection. Note that at least two collections from this array must be performed BEFORE array performance data can be reported on.</p> <p>Array performance collection requires FLARE code version 04.30.000.5.524 A11 (CLARiiON) or FLARE code version 05.31.000.5.006 A01 (VNX Block), or higher, and current supported versions of NaviCLI for each.</p> <p>Click the clock icon to create a schedule.</p>	

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

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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.

The screenshot shows a configuration window titled "EMC VPLEX Data Collector Policy". The window contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Management Server Addresses:*** An empty text input field.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat Password:*** An empty text input field.
- Active Probes:** A section with a checked checkbox for "Array Capacity".
- Schedules:** A section with a dropdown menu showing "Every 8 hours, at minute 1" and a plus icon.
- Notes:** Two empty text input fields.
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom left, and a "Privacy Policy" link at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
Management Server Addresses*	<p>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.</p> <p>Note: To collect from a Cluster, enter the IP address of only one of the management servers.</p>
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.

Field	Description
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected every 8 hours.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>* / 30 * * * *</code> means every 30 minutes</p> <p><code>* / 20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>* / 10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
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.

The screenshot shows a dialog box titled "EMC XtremIO Data Collector Policy". It contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Management Server Addresses:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A password input field with a masked character "•".
- Active Probes:** A section with two checked items: "Array Capacity" and "Array Performance".
- Schedules:** A section with two items: "Every day at 03:33" and "Every 15 minutes", each with a clock icon.
- Notes:** A text area containing the text "Password for the EMC XtremIO storage system." in green.
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" are located at the bottom.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> <p>To avoid memory issues with large sets of performance data, set a collection schedule for no more than 1 hour.</p>

Field	Description
Schedule	<p>Click the clock icon to create a schedule.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See “[Installing the WMI Proxy Service \(Windows Host Resources only\)](#)” on page 279.
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.

The screenshot shows a configuration window titled "Hitachi Block Storage Data Collector Policy". The window contains the following fields and sections:

- Collector Domain:** A dropdown menu with "INSTALLWIN2" selected.
- Policy Domain:** A dropdown menu with "INSTALLWIN2" selected.
- Hitachi Device Manager Server:*** An empty text input field.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat Password:*** An empty text input field.
- ExcludeArrays:** A large empty text area.
- Active Probes:** A section with three checkboxes:
 - Array Details
 - Array Performance
 - HIAA Array Performance
- Schedules:** A section with three dropdown menus:
 - Every day at 02:01
 - Every 15 minute
 - Every 15 minute
- HTnM Install Location:** An empty text input field.
- HIAA Server:** An empty text input field.
- HIAA User ID:** An empty text input field.
- HIAA Password:** An empty text input field.
- HIAA Repeat Password:** An empty text input field.
- HDT Collection
- Notes:** A large text area containing the text: "Use the Password for the Admin username for accessing the Hitachi Infrastructure Analytics Advisor."
- Buttons:** "OK", "Cancel", "Help", and "Privacy Policy".

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

Field	Description
Collector Domain	<p>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.</p>
Policy Domain	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Field	Description
Hitachi Device Manager Server*	<p>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.</p> <p>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.</p> <p>See "Configuring a Collector for Hitachi NAS Block Storage" on page 119.</p>
User ID*	<p>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.</p> <p>See "Configuring a Hitachi Device Manager User" on page 116.</p> <p>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.</p>
Password*	<p>Note: The password is encrypted prior to saving in the database and is never visible in any part of the application.</p>
Exclude Arrays	<p>Enter one or more array names to be excluded.</p> <p>Comma-separated names are supported. Example: USPv1_172.16.1.13, USPv1_172.16.1.14, AMS - Corporate(5100)@172.16.1.43</p>

Field	Description
Array Details	<p>Click the check box to activate array details collection. Click the clock icon to set the schedule.</p> <p>For example:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p>
Array Performance	<p>Click the check box to activate performance collection and enable entries and selections for the HTnM Install Location and the Performance Schedule.</p> <p>Note that at least one collection from this array must be performed BEFORE array performance data can be collected.</p> <p>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.</p>

Field	Description
HTnM Install Location	<p>Specify the Tuning Manager server installation directory. By default, the Tuning Manager server will be installed in the following locations:</p> <p>Windows Server 2003 (x86) and Windows Server 2008 (x86): %SystemDrive%\Program Files\HiCommand\TuningManager</p> <p>Windows Server 2003 (x64) and Windows Server 2008 (x64): %SystemDrive%\Program Files (x86)\HiCommand\TuningManager</p> <p>Solaris: /opt/HiCommand/TuningManager</p>
HIAA Array Performance	<p>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.</p>
HIAA Server	<p>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.</p>
HIAA User ID	<p>Admin username for accessing the Hitachi Infrastructure Analytics Advisor.</p>
HIAA Password	<p>Password for the Admin username (User ID) for accessing the Hitachi Infrastructure Analytics Advisor.</p>

Field	Description
HDT Collection	<p>Activate HDT Collection. An HDT Schedule is not required if your HDvM is not managing VSP arrays running HDT.</p> <p>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.</p> <p>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.</p>
Notes	<p>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.</p>

- 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.

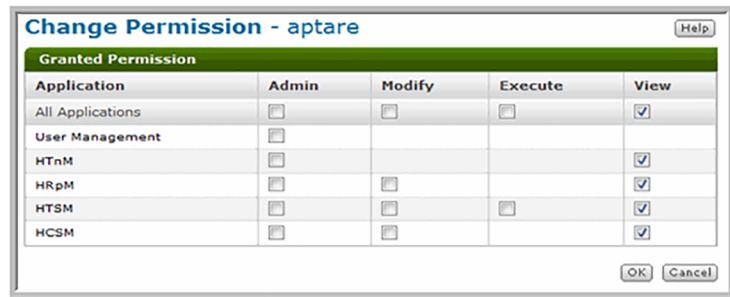
Configuring a Hitachi Device Manager User

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:

```

<HiCommandServerMessage>
<APIInfo version="7.2"/>
<Response>
<EchoCommand name="GetUser" status="COMPLETED" result="0" resultSource="SecurityAdmin.GetUser" messageId="563254492">
<ResultList>
<User loginID="aptare" groupName="All Resources" role="Guest" description="Aptare Read only Account" userNumber="USER_137184376198812" fullName="Aptare Data Collector">
<User loginID="HitUser" groupName="All Resources" role="Peer" description="Peer connections" userNumber="USER_1351778130440" fullName="">
<User loginID="System" groupName="All Resources" role="Admin" description="Built-in account" userNumber="USER_0" fullName="">
</ResultList>
</Response>
</HiCommandServerMessage>

```

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 110.

Pre-Installation Setup 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 APTARE 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.
- 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.
- Amazon Corretto 11. 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 APTARE 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.

Hitachi Content Platform (HCP) Data Collector Policy

Collector Domain: 1-domain-for-pat Policy Domain: 1-domain-for-pat

Management Server Addresses:*

User ID:* admin@etchsketchteam

Password:* • Authentication Type:* Local

Active Directory Domain: SNMP Version:* v1/v2

Community String:

Active Probes **Schedules**

Array Capacity Every day at 02:00

Namespace Statistics Every 8 hours, at minute 0

Notes:

Password for the Hitachi Content Platform (HCP) storage system.

OK Cancel Test Connection Help

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

Field	Description
Collector Domain	<p>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.</p>
Policy Domain	<p>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.</p> <p>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.</p> <p>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.</p>
Management Server Addresses*	<p>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.</p>

Field	Description
User ID*	<p>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.</p> <p>See “Setting Up Permissions for an HCP Local User or Active Directory User” on page 128.</p>
Password*	<p>Password for the Hitachi Content Platform (HCP) storage system. This password is also used for MAPI and SNMPv3.</p>
Authentication Type	<p>Select either Local or Active Directory Authentication.</p>
Active Directory Domain	<p>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.</p>
SNMP Version*	<p>SNMP version.</p>
Community String	<p>Community string for SNMP.</p>

Field	Description
Array Capacity/Schedule	<p>This collection is enabled by default to collect array capacity data from your Hitachi Content Platform (HCP) environment.</p> <p>Click the clock icon to create a schedule. By default, it is collected at 3:33 am daily.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>

Field	Description
Namespace Statistics/Schedule	<p>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.</p> <p>Note: The minimum interval size maintained by the array is one hour, and APTARE 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, APTARE IT Analytics will maintain the 4 hour increments and so on.</p> <p>Click the clock icon to create a schedule. By default, it is collected every 8 hours.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>

Field	Description
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

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.

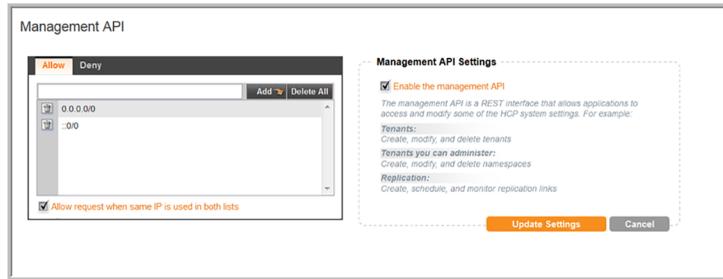
Search grants permission to use the metadata query API and Search Console to query or search the default namespace and any namespaces owned by HCP tenants that are configured to allow system-level users to manage them and search their namespaces.

The screenshot shows the user configuration interface in the Hitachi Content Platform System Management Console. The interface is divided into several sections:

- Header:** Username (apuser), Status (Enabled), Full Name (aptare user), and Type (LOCAL).
- Enable account:** A checkbox labeled "Enable account" is checked.
- Fields:** Username (apuser), Full Name (aptare user), Password, and Confirm Password.
- Force change on next login:** A checkbox that is currently unchecked.
- Roles:** A table with columns "Roles" and "Description". The roles listed are Monitor (checked), Administrator, Service, Compliance, Security, and Search (checked).
- Description:** A note stating "Monitor role grants permissions to view system status and system configuration."
- Buttons:** "Update Settings" and "Cancel".

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

The screenshot displays the configuration interface for a local user. At the top, a header shows the user's details: Username (aptuser), Status (Enabled), Full Name (apt user), and Type (LOCAL). Below this, there is a section for user settings with a sub-header "Enable account". The "Username" field contains "aptuser", and the "Full Name" field contains "apt user". There are fields for "Password" and "Confirm Password", along with a checkbox for "Force change on next login". A "Roles" section is visible, with "Monitor" selected and "Administrator", "Security", and "Compliance" unselected. A "Description" field contains the text "Mouse over a role to view its description." At the bottom of this section are "Update Settings" and "Cancel" buttons.

Below the user settings is the "Assign Namespace Permissions" section. It features a search bar for "Find and Select Namespaces" with a "Select All" button. A list of namespaces is shown, with "namespace-1-tenant-6" selected. Below the list, there is a section for "Assign Data Access Permissions for Selected Namespaces" with a "1 Namespace Selected" indicator. The permissions section includes checkboxes for "Browse" (checked), "Read", "Write", "Delete", "Purge", "Privileged", and "Search". There are also checkboxes for "Read ACL", "Write ACL", and "Change Owner". A "Select all" button is present at the bottom right of this section. At the very bottom of the "Assign Namespace Permissions" section are "Assign Namespaces" and "Cancel" buttons.

For each tenant, click the Allow system level users to manage this tenant and search its namespaces check box.

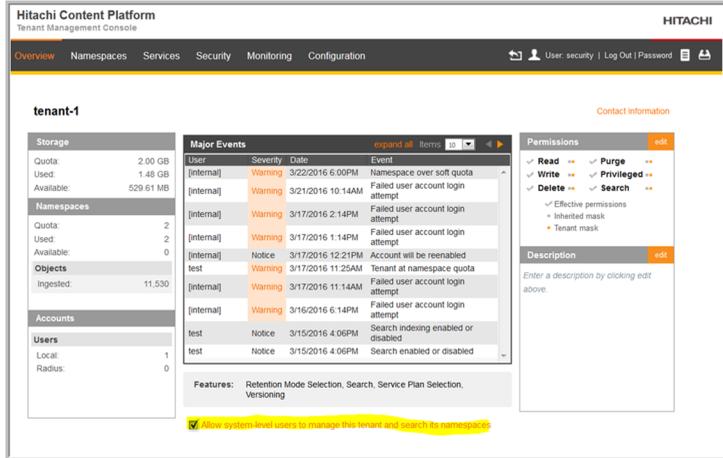
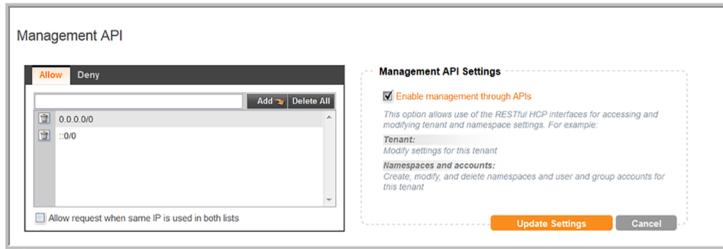
Active Directory Users

The screenshot displays the configuration interface for an Active Directory user. At the top, there is a "Roles and Capabilities" section with a sub-header. It includes checkboxes for "Monitor" (checked), "Administrator", "Security", and "Compliance". Below this, there is a description: "Administrator role grants permission to view tenant and namespace status and configure the tenant and its namespaces." There is also a checkbox for "Allow namespace management". At the bottom of this section are "Update Settings" and "Cancel" buttons.

Below the roles section is the "Assign Data Access Permissions" section. It features a search bar for "Find and Select Namespaces" with a "Select All" button. A list of namespaces is shown, with "namespace-1-tenant-7" and "namespace-2-tenant-7" selected. Below the list, there is a section for "Assign Data Access Permissions for Selected Namespaces" with a "1 Namespace Selected" indicator. The permissions section includes checkboxes for "Browse" (checked), "Read" (checked), "Write", "Delete", "Purge", "Privileged", and "Search". There are also checkboxes for "Read ACL", "Write ACL", and "Change Owner". A "Select all" button is present at the bottom right of this section. At the very bottom of the "Assign Data Access Permissions" section are "Assign Permissions" and "Cancel" buttons.

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).



Pre-Installation Setup 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.

- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- When the APTARE 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.
- 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.
- 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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 APTARE 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.

SSC Access Configuration

Enable SSC Access

Port Number:

Maximum Number Of Connections:

Restrict Access To Allowed Hosts

Allowed Hosts:

Adding the Collector

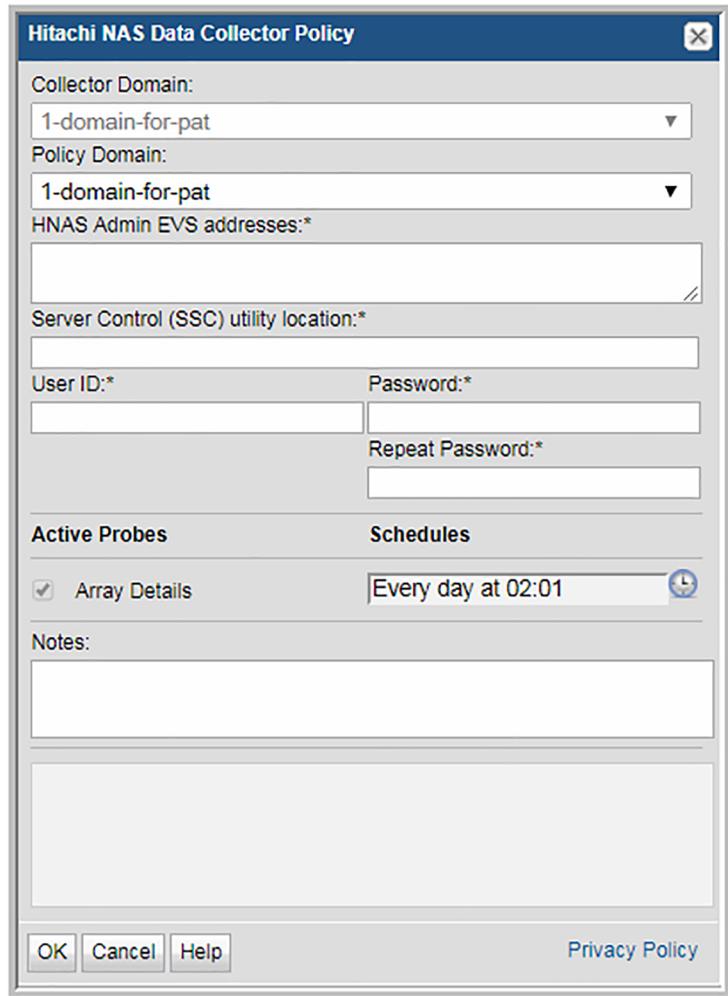
Note: The Data Collector retrieves data only from the HCP object array. It has no visibility into the physical capacity supporting the HCP array. Therefore, capacity values potentially could be double counted, for example, if data from a supporting array is also being collected.

- 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.



The image shows a dialog box titled "Hitachi NAS Data Collector Policy". It contains several fields and sections for configuring the data collector policy. The "Collector Domain" and "Policy Domain" are both set to "1-domain-for-pat". There are empty text boxes for "HNAS Admin EVS addresses:*" and "Server Control (SSC) utility location:*". The "User ID:*" and "Password:*" fields are empty, and there is a "Repeat Password:*" field below them. The "Active Probes" section has a checked checkbox for "Array Details". The "Schedules" section has a dropdown menu set to "Every day at 02:01". There is a "Notes:" section with a large empty text area. At the bottom, there are "OK", "Cancel", and "Help" buttons, and a "Privacy Policy" link.

Hitachi NAS Data Collector Policy

Collector Domain:
1-domain-for-pat

Policy Domain:
1-domain-for-pat

HNAS Admin EVS addresses:*

Server Control (SSC) utility location:*

User ID:* Password:*

Repeat Password:*

Active Probes **Schedules**

Array Details Every day at 02:01

Notes:

OK Cancel 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<code>yourdomain</code>

Field	Description	Sample Value
HNAS Admin EVS Addresses*	<p>Enter one or more Hitachi NAS Admin EVS addresses separated by commas.</p> <p>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.</p>	
Server Control (SSC) utility location*	<p>The location of the SiliconServer Control (SSC) CLI.</p> <p>See “HNAS Configuration Requirements” on page 135.</p> <p>Linux: <code>/usr/bin</code></p> <p>Windows: <code>c:\program files\ssc</code></p>	
User ID*	<p>Create a user with supervisor privileges for accessing the Hitachi NAS.</p>	Administrator
Password*	<p>Password associated with the User ID.</p> <p>The password is encrypted prior to saving in the database and is never visible in any part of the application.</p>	Password1

Field	Description	Sample Value
Array Details	<p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Notes	<p>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.</p>	

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

Host Inventory Pre-Installation Setup

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/Unhide, 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 15-1 Host Resources Prerequisites by Operating System

Host OS	Host Access Requirements	Port Requirements	Notes
Linux RH Linux SUSE CentOS AIX HP-UX 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 APTARE 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 | |
| <ul style="list-style-type: none"> ■ 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 152.
 See “[Manage Access Control](#)” on page 158.
- 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 147.

See [“Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements”](#) on page 142.

- Path: APTARE 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 147.

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: APTARE 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)

HP-UX: fcmsutil (used only for HBA information; should already be installed by default)

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):

```
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 148.
- See [“Host Inventory Maintenance Overview”](#) on page 149.

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 150.

See [“Host Inventory Management”](#) on page 161.

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 150.



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 149.

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 151.

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 174.
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 152.
Configure user IDs and passwords for authentication when the data collector is accessing hosts.
 4. See “[Manage WMI Proxy](#)” on page 155.
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 157.

Configure the paths that data collectors will use to execute commands on hosts.

6. See [“Manage Access Control”](#) on page 158.

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 APTARE IT Analytics be established and using Active Directory for Windows systems and the sudo command for Linux systems, restrict the commands that APTARE 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 142.

7. See [“Configure Host Discovery Policies to Populate the Host Inventory”](#) on page 162.

Host Discovery attempts to find hosts and populate your APTARE 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 169.

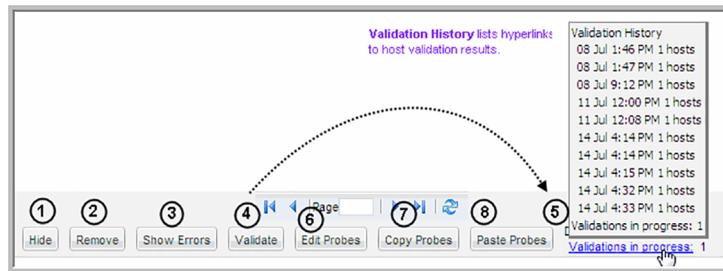
Host validation must take into account host access for a wide variety of conditions and environments. As the discovery process accesses hosts, informative messages will provide clues to connectivity issues. In addition, devices that don't belong in a host inventory--for example, printers in the IP address 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 148.

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/Unhide, Remove”](#) on page 171.
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/Unhide, Remove”](#) on page 171.
3. **Show Errors** - Use this feature to troubleshoot connectivity and validation issues.
See [“Show Errors”](#) on page 170.
4. **Validate** - Use this feature in combination with the Show Errors feature to troubleshoot host data collection issues.
See [“Validate Host Connectivity”](#) on page 169.
5. **Show Validations** -
See [“Validation History”](#) on page 170.
6. **Edit Probes**:
See [“Configure and Edit Host Probes”](#) on page 174.
7. **Copy Probes**:
See [“Propagate Probe Settings: Copy Probes, Paste Probes”](#) on page 177.
8. **Paste Probes**
See [“Propagate Probe Settings: Copy Probes, Paste Probes”](#) on page 177.

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 151.
- See [“Configure/Search the Host Inventory”](#) on page 151.
- See [“Manage Credentials”](#) on page 152.
- See [“Manage WMI Proxy”](#) on page 155.
- See [“Manage Paths”](#) on page 157.
- See [“Manage Access Control”](#) on page 158.

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 172.

The screenshot shows the Host Inventory configuration window with the following sections and settings:

- Navigation:** Manage Credentials, Manage WMI Proxy, Manage Paths, Manage Access Control, Discover Hosts, Refresh
- Search Fields:** Host name, IP address, Pre-defined Host search (dropdown)
- Buttons:** Search, Export, Clear, < Less
- Configuration Grid:**
 - Domain:** (dropdown)
 - Discovery:** (dropdown)
 - OS:** (dropdown)
 - Connect Status:** Success, Error (dropdown)
 - Collector:** (dropdown)
 - Host Collection:** Enabled, Disabled (dropdown), Search hidden hosts
 - Host Types:** VM Server, VM Guest, VIO Server (dropdown)
 - Credentials:** admin (dropdown)
 - Path:** (dropdown)
 - Access Control:** (dropdown)
 - WMI Proxy:** (dropdown)
 - Probe:** Memory, Network, Process, Performance (dropdown)
 - Probe Status:** Success, Error (dropdown)
 - Probe Collection:** Enabled, Disabled (dropdown)

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 145.

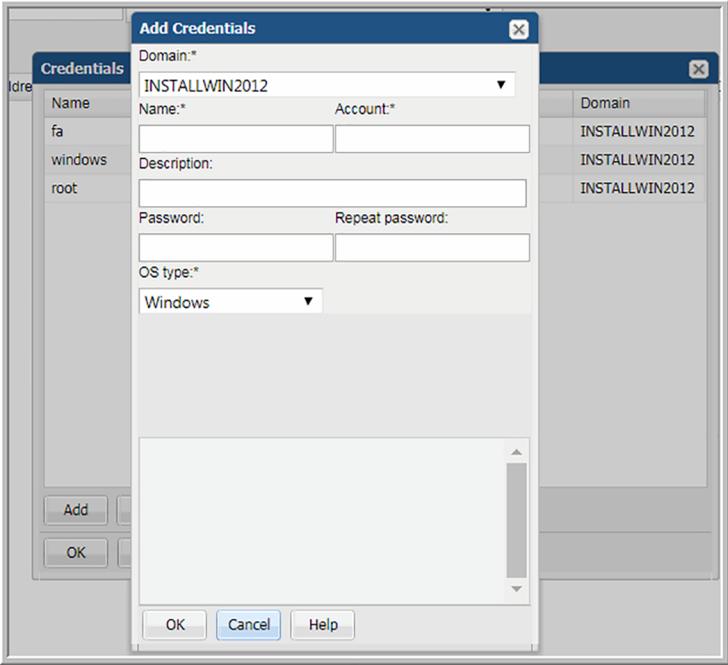
See [“Host Inventory Configuration Steps”](#) on page 147.

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



Field	Description	Sample Values
Domain*	Select the APTARE 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.	

Field	Description	Sample Values
Account*	<p>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.</p> <p>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.</p> <p>See “Manage Access Control” on page 158.</p> <p>and</p> <p>See “Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements” on page 142.</p>	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	<p>For Windows hosts only:</p> <p>If any of the hosts specified in the Host address field are Windows hosts, you need to specify the Windows domain name.</p> <p>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.</p>	win2kdomain

Field	Description	Sample Values
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.	<code>/root/.ssh/id_rsa</code> or <code>C:\Program Files\Aptare\mbs\conf\id_rsa</code>
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.	<code>/root/.ssh/known_hosts</code> or <code>C:\Program Files\Aptare\mbs\conf\known_hosts</code>

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:

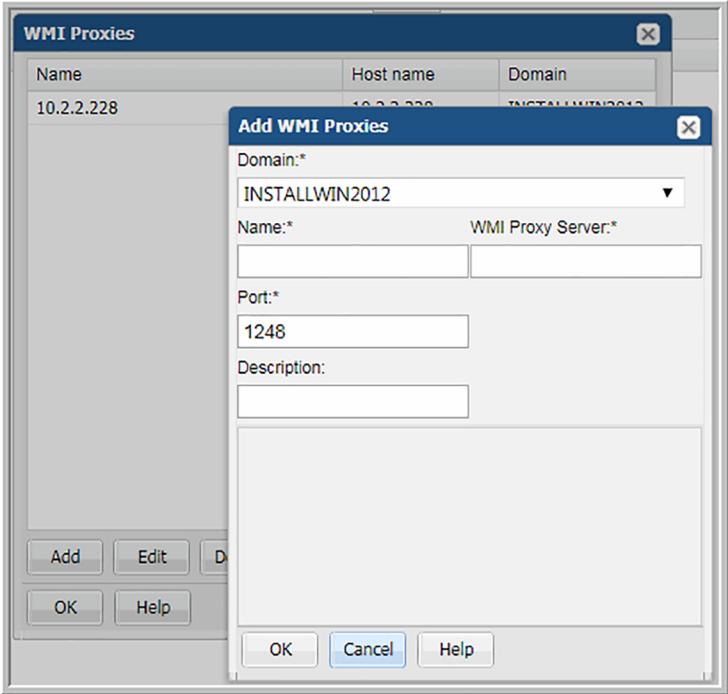
See [“Host Access Requirements”](#) on page 145.

See [“Host Inventory Configuration Steps”](#) on page 147.

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**.



Field	Description	Sample Values
Domain*	Select the APTARE 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

Field	Description	Sample Values
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:

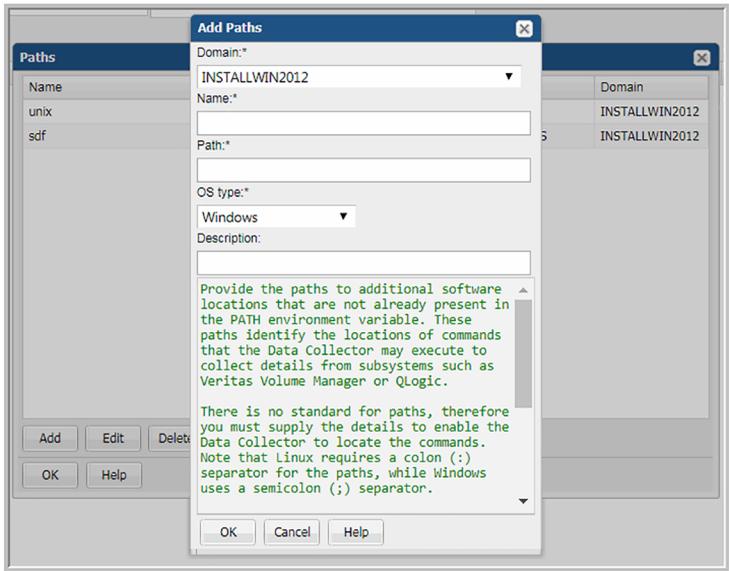
See [“Host Access Requirements”](#) on page 145.

See [“Host Inventory Configuration Steps”](#) on page 147.

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**.



Field	Description	Sample Values
Domain*	Select the APTARE 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*	<p>Provide the path(s) that you want prefixed to the PATH environment variable.</p> <p>Note that there is no standard for the paths, therefore you must supply the details to enable the Data Collector to connect.</p> <p>If the Data Collector is installed on a Linux server, use the following command to determine the path to Linux servers:</p> <pre>ssh <userId> @<hostServer> env</pre> <p>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:</p> <pre>plink <userId> @<hostServer> env</pre>	<p>Linux:</p> <pre>/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</pre> <p>Windows:</p> <pre>C:\Program Files\Emulex \Util\HBAnyware; C:\Program Files \QLogic\SANSurfer</pre>
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 APTARE IT Analytics be established

and using Active Directory for Windows systems and the sudo command for Linux systems, restrict the commands that APTARE 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 142.

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:

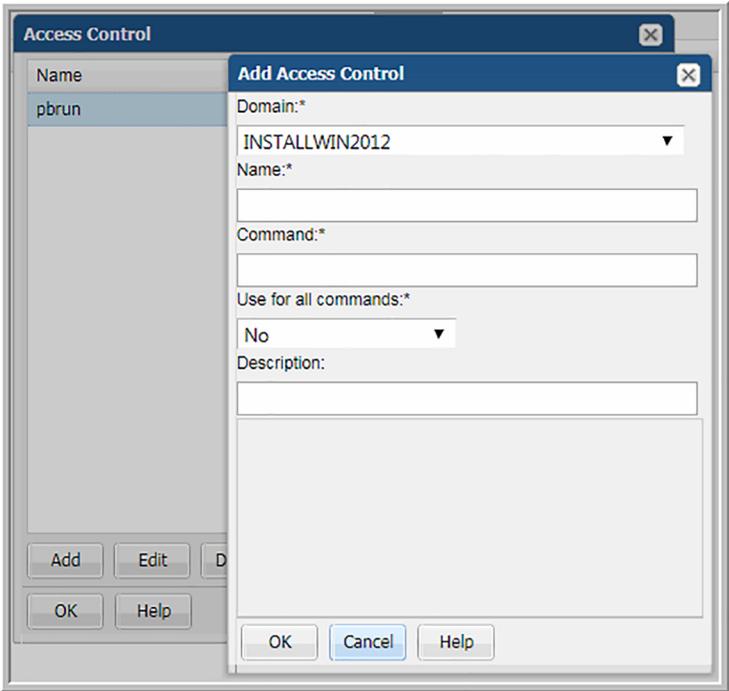
See [“Host Access Requirements”](#) on page 145.

See [“Host Inventory Configuration Steps”](#) on page 147.

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**.



Field	Description	Sample Values
Domain*	Select the APTARE 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.	

Field	Description	Sample Values
Command*	<p>Linux hosts only: Provide the full path to the access control command, such as sudo, sesudo, or pbrun.</p> <p>See “Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements” on page 142.</p> <p>You can configure sudo to prompt for a password using a custom prompt (the default is “Password”). APTARE 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.</p>	<p>/usr/bin/sudo</p> <p>/user/local/bin/sudo -p Password:</p>
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 145.

See [“Host Inventory Configuration Steps”](#) on page 147.

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 162.
- See [“Execute and Monitor Host Discovery”](#) on page 167.
- See [“Validate Host Connectivity”](#) on page 169.
- See [“Host Inventory Search and Host Inventory Export”](#) on page 172.
- See [“Export the Host Inventory”](#) on page 173.
- See [“Configure and Edit Host Probes”](#) on page 174.

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 142.
- See [“Host Access Requirements”](#) on page 145.
- See [“Host Inventory Configuration Steps”](#) on page 147.

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 169.

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 150.
- See [“Execute and Monitor Host Discovery”](#) on page 167.
- See [“Validate Host Connectivity”](#) on page 169.
- See [“Host Inventory Search and Host Inventory Export”](#) on page 172.

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**.

Add Host Discovery Policies [X]

Name:*

Domain:* Collector:*
 ▼ ▼

Host addresses:*

Excludes:

Configuration options:

OK Cancel Help

Field	Description	Sample Values
Name*	Assign a name to identify this Discovery Policy.	
Collector*	Select the data collector from the drop-down list	

Field	Description	Sample Values
Domain*	<p>Select the APTARE IT Analytics Domain from the list; for most environments, only one Domain is displayed. Multiple domains facilitate management for Managed Services Providers (MSPs).</p>	
Host addresses*	<ul style="list-style-type: none"> ■ A range of IP addresses can be specified ■ Hostnames and/or IP addresses can be listed, separated by commas <p>See “Collecting from Clustered SQL Server and Oracle Applications” on page 166.</p>	<p>192.168.0.1-250 172.168.1.21, ABChost1, ABChost2, 172.168.1.58</p>
Excludes	<p>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.</p>	
Configuration options	<p>This list gets populated when you select a Domain at the top of the Host Discovery Policies window.</p> <ul style="list-style-type: none"> ■ Credentials ■ WMI Proxies ■ Paths <p>Expand these lists to select the configurations to be used by this Discovery Policy.</p> <p>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.</p>	

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 163.

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 15-1](#) on page 166.
- 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 15-2](#) on page 167.

Note: If Cluster Nodes already have been discovered, they should be removed from the Host Inventory.

Figure 15-1 Host Discovery Policy Configuration Steps

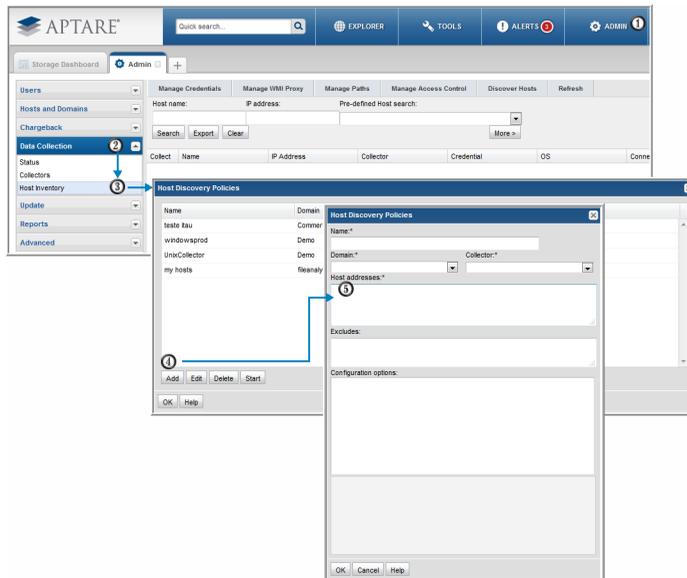
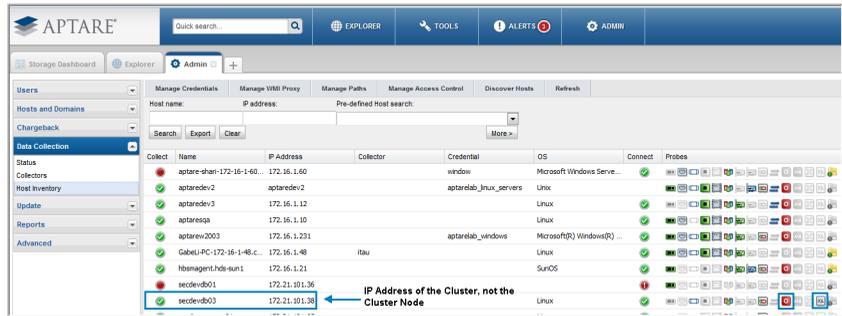
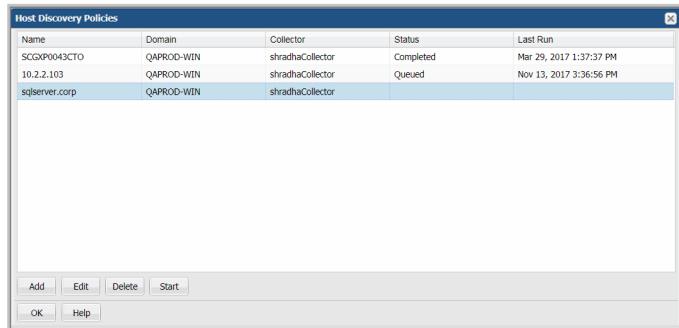


Figure 15-2 Application Probe Example



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.

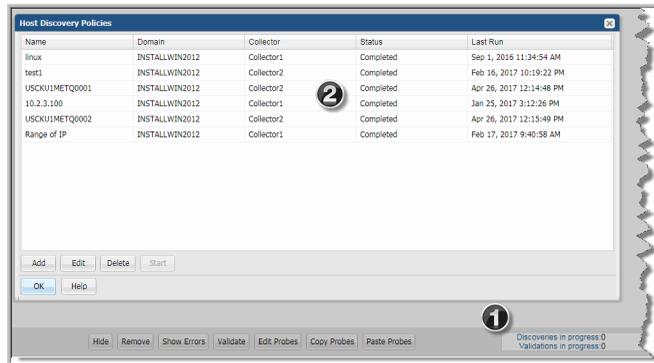
4. Click **OK**.
5. To verify that the discovery process is running, refresh the view you launched in step 1 or go to Monitor Discovery Processes.

See [“Monitor Discovery Processes”](#) on page 168.

Monitor Discovery Processes

Several methods can be used to monitor progress:

Method 1

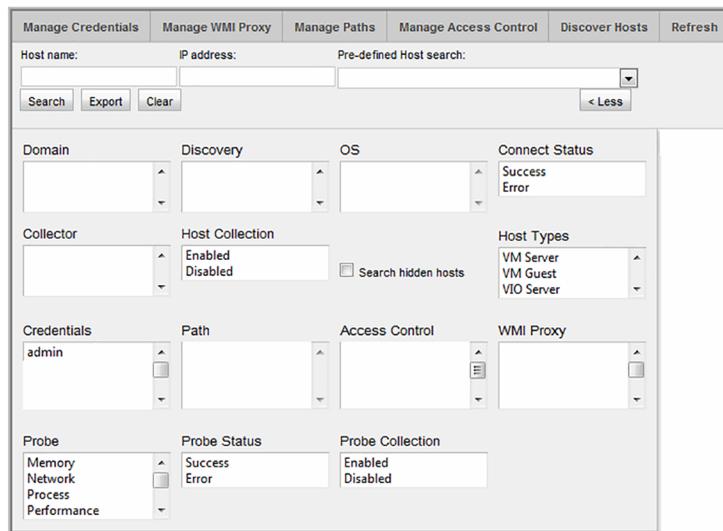


1. At the bottom of the Host Inventory window, double-click the **Discoveries in progress** link to launch the Host Discovery Policies window.

Note the Status at the right of the window.

2. Double-click the Discovery Policy to view the settings.

Method 2



1. Using the Host Inventory

See [“Advanced Search Parameters”](#) on page 173.

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 [“Monitor Discovery Processes”](#) on page 168.

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.

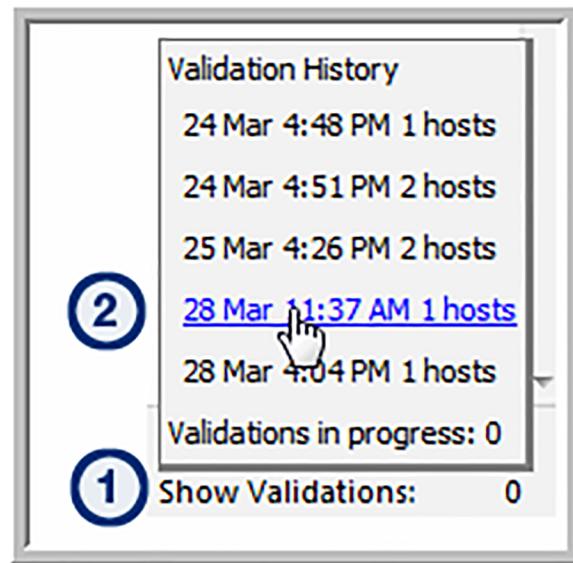
A list of the hosts that are currently being validated will be displayed.

See [“Validation History”](#) on page 170.

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

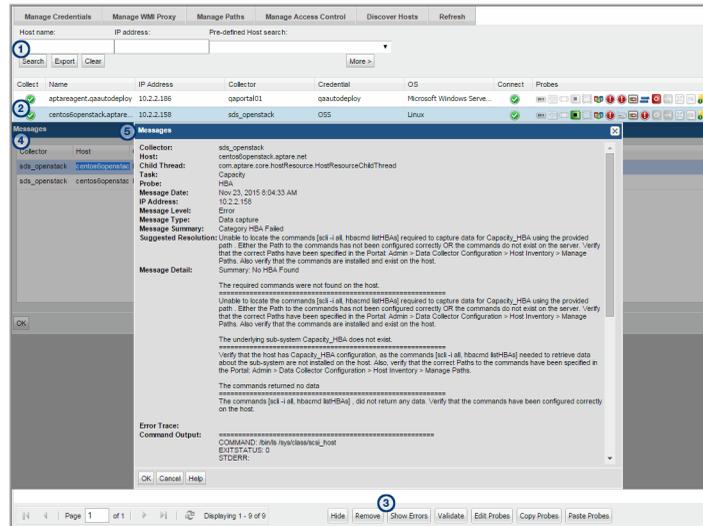
Before host data can be successfully collected, a number of configuration steps need to be taken. The **Show Errors** button enables you to identify details to help you troubleshoot host inventory collection issues.

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/Unhide, 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.

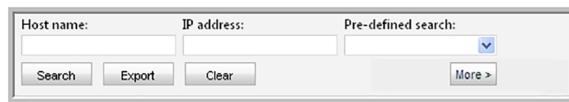
To filter your host inventory to include only hosts for which you want data collected, use the following options:

- 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 173.
- 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 173.

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 172.

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.

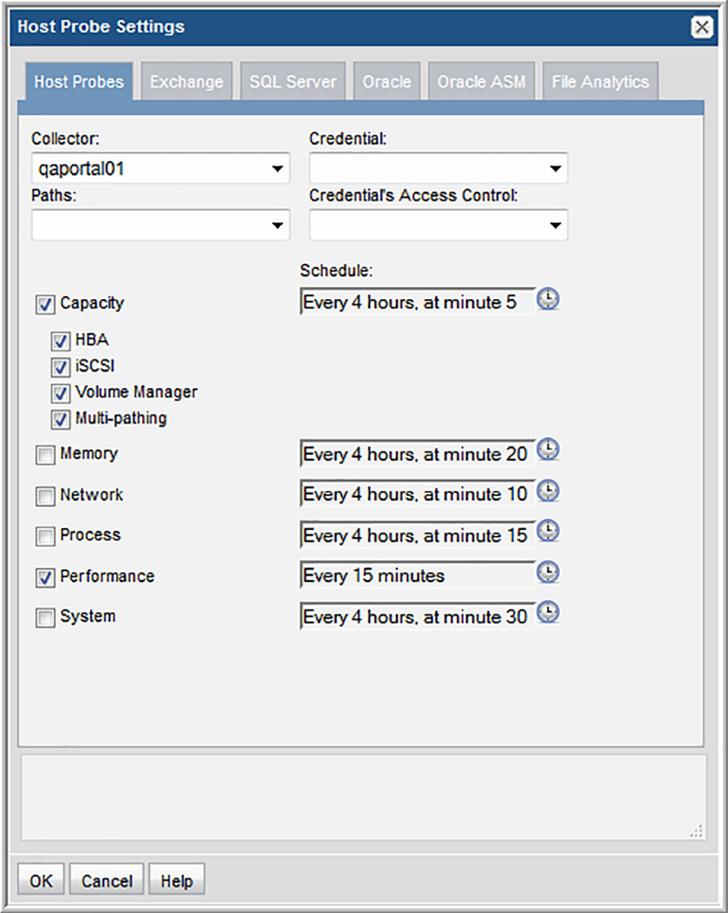
To configure probes for a host

- 1 Search for hosts in your inventory. A search with no specified criteria returns all hosts in your inventory.

Collect	Name	IP Address	Collector	Credential	OS	Connect	Probes
	aptaredev1	172.016.001.01	host_aptaresqi	wz_credential	Linux		
	aptaredev2	172.016.001.01	host_aptaresqi	wz_credential	Linux		
	aptaredev3	172.016.001.01	host_aptaresqi	wz_credential	Linux		

- 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 178.



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 178.

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

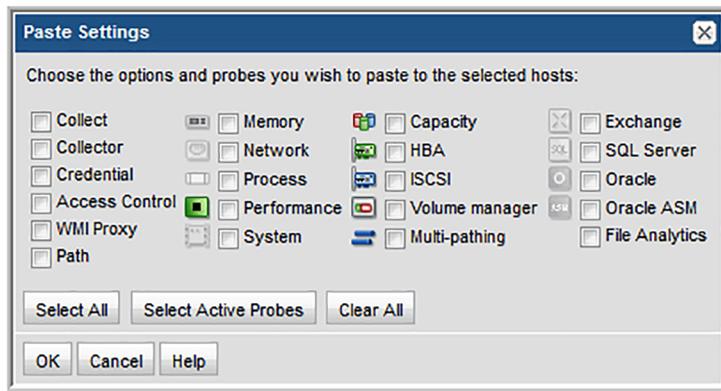
Whenever you have hosts with common attributes, you can save time by configuring probe settings for one host and then copying and pasting those settings to other hosts.

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 15-2 Table 15.3 Probe Settings

Probe Type	Parameters	Description
Capacity HBA iSCSI Volume Manager Multi-pathing	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.”
Note: Do not enable HBA probes for VMware guest host collection.		

Table 15-2 Table 15.3 Probe Settings (*continued*)

Probe Type	Parameters	Description
Memory	Probe schedule*	<p>A schedule in cron format; for example:</p> <p><code>*/20 9-18 * * *</code></p> <p>which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”</p>
Network	Probe schedule*	<p>A schedule in cron format; for example:</p> <p><code>*/20 9-18 * * *</code></p> <p>which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”</p>
Process	Probe schedule*	<p>A schedule in cron format; for example:</p> <p><code>*/20 9-18 * * *</code></p> <p>which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”</p>
Processor	Probe schedule*	<p>A schedule in cron format; for example:</p> <p><code>*/20 9-18 * * *</code></p> <p>which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”</p>
System	Probe schedule*	<p>A schedule in cron format; for example:</p> <p><code>*/20 9-18 * * *</code></p> <p>which translates to “every 0, 20 and 40th minute past the 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18th hour.”</p>

Table 15-2 Table 15.3 Probe Settings (*continued*)

Probe Type	Parameters	Description
Exchange	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 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

Table 15-2 Table 15.3 Probe Settings (*continued*)

Probe Type	Parameters	Description
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.
	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

Table 15-2 Table 15.3 Probe Settings (*continued*)

Probe Type	Parameters	Description
	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.
	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.

Table 15-2 Table 15.3 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.”
	Account*	The Oracle user privileges required: SYSDBA privilege if 10g sysasm in 11g
	Password*	Database access password
	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.”

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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.

The screenshot shows a configuration window titled "HP 3PAR Data Collector Policy". The window contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- HP 3PAR Storage System Address(es):*** An empty text input field.
- Collection Method:** Set to "Command-Line Interface (CLI)".
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat Password:*** An empty text input field.
- Active Probes:** A list with two items: "Array Details" (checked) and "Array Performance" (unchecked).
- Schedules:** Two entries: "Every day at 03:01" and "Every 15 minutes", each with a clock icon.
- Notes:** A large empty text area.
- Buttons:** "OK", "Cancel", and "Help" at the bottom left; "Privacy Policy" at the bottom right.

- 5 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<code>yourdomain</code>

Field	Description	Sample Value
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.	3PAR_server1
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.	Admin
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.	Password1

Field	Description	Sample Value
Array Details	<p>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.</p> <p>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.</p>	
Array Performance	<p>Select 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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
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 110.

Pre-Installation Setup 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 APTARE 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.
- 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.

- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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*.

- **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.

The screenshot shows a configuration window titled "HP EVA Data Collector Policy" with a close button (X) in the top right corner. The window contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- HP EVA Management Server:*** An empty text input field.
- SSSU Home:*** An empty text input field.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat Password:*** An empty text input field.
- Active Probes:** A section with a checked checkbox and the text "Array Details".
- Schedules:** A section with a dropdown menu showing "Every day at 03:01" and a clock icon.
- Notes:** A large empty text area for notes.
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom left, and a "Privacy Policy" link at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	yourdomain
HP EVA Management Server*	The address of the HP EVA Management Server-- either a single IP address or server name	eva_server1

Field	Description	Sample Value
SSSU Home*	<p>The location of the SSSU (Storage System Scripting Utility) command-line utility.</p> <p>For example: C:\Program Files\Hewlett-Packard\Software\Element Manager for StorageWorks</p>	
User ID*	<p>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.</p>	Administrator
Password*	<p>The password is encrypted prior to saving in the database and is never visible in any part of the application.</p>	Password1
Array Details	<p>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.</p> <p>Examples of CRON expressions:</p> <p>*/30 * * * * means every 30 minutes</p> <p>*/20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>*/10 * * * 1-5 means every 10 minutes Mon - Fri.</p> <p>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.</p>	

Field	Description	Sample Value
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.

Pre-Installation Setup for Huawei OceanStor

This chapter includes the following topics:

- [Pre-Installation Setup for Huawei OceanStor](#)
- [Prerequisites for Adding Data Collectors \(Huawei OceanStor\)](#)
- [Installation Overview](#)
- [Add a Huawei OceanStor Data Collector Policy](#)

Pre-Installation Setup for Huawei OceanStor

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 (Huawei OceanStor)

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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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).
- Huawei OceanStor uses a default array name, Huawei.Storage for all arrays. APTARE IT Analytics requires a unique array name for data collection and to be able to report valid capacity data. The default array name must be changed to a unique entry on the Huawei system.

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 Huawei OceanStor 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
6. Validate the Data Collector installation.

Add a Huawei OceanStor 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.

The screenshot shows a configuration window titled "Huawei OceanStor Data Collector Policy". The window contains the following fields and controls:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Server Addresses:*** An empty text input field.
- Server Port:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A password input field with a single dot visible.
- Active Probes:** A section with a checked checkbox for "Array Capacity".
- Schedules:** A dropdown menu with "Every day at 03:33" selected and a refresh icon.
- Notes:** A text area containing the text "Password for the Huawei OceanStor storage system." in green.
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" buttons at the bottom.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
Server Addresses*	<p>One or more Huawei OceanStor Server IP addresses or host names to probe. Comma-separated addresses are supported, for example 192.168.1.10, myhost</p> <p>Note: To collect from a Cluster, enter the IP address of only one of the management servers.</p>
Server Port	Server Port number for the Huawei OceanStor storage system.
User ID*	View-only User ID for the Huawei OceanStor storage system.
Password*	Password for the Huawei OceanStor storage system. The password associated with the User ID.
Array Capacity	This probe is enabled by default to collect array capacity data from your Huawei OceanStor environment. By default, it is collected at 03:33 daily.

Field	Description
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected at 1:01 daily.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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)

APTARE IT Analytics supports the following IBM Enterprise storage arrays, running DSCSI 5.2.2.272 & above: DS6000 and DS8000.

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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.

The image shows a configuration dialog box titled "IBM Enterprise Data Collector Policy". It contains several fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Profile Name:*** and **Array Address:***: Two empty text input fields.
- IBM DSCLI Client Software Location:***: An empty text input field.
- User ID:*** and **Password:***: Two empty text input fields.
- Repeat Password:***: An empty text input field.
- Active Probes** and **Schedules**: Two sections. Under "Active Probes", there is a checked checkbox for "Array Details". Under "Schedules", there is a text field containing "Every 9 hours, at minute 1" and a clock icon.
- Notes:** A large empty text area.
- Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom left. A "Privacy Policy" link is located at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	yourdomain
Profile Name*	<p>Specify the profile filename, including the absolute path. e.g.</p> <p>Windows: C:\Program Files\ibm\dscli\profile\dscli.profile</p> <p>Linux: /opt/ibm/dscli/profile/dscli.profile</p>	
Array Address*	IP address of the IBM Storage Array (IBM DS Storage Frame). Only one array per IBM Enterprise Data Collector Policy is allowed.	

Field	Description	Sample Value
IBM DSCLI client software location *	<p>The location of the DSCLI executable on the Data Collector server, for example:</p> <p>Linux: /opt/ibm/dscli</p> <p>Windows: C:\Program Files\IBM\dscli</p>	
User ID*	<p>Specifies the user ID for the account that has monitor group privileges on the storage array.</p>	Monitor
Password*	<p>The password is encrypted prior to saving in the APTARE IT Analytics database and is never visible in any part of the application.</p>	Password1
Array Details	<p>Check the box to collect array details.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p>*/30 * * * * means every 30 minutes</p> <p>*/20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>*/10 * * * 1-5 means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Notes	<p>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.</p>	

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

6. Validate the Data Collector installation.

Adding a NetApp E-Series 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.

The screenshot shows a dialog box titled "NetApp E-Series Data Collector Policy" with a close button (X) in the top right corner. The dialog contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Array Addresses:*** An empty text area.
- SMCLI Client Software Location:*** An empty text field.
- Active Probes** and **Schedules** sections:
 - Active Probes:** A checkbox labeled "Array Details" is checked.
 - Schedules:** A text field contains "Every 7 hours, at minute 1" with a clock icon to its right.
- Notes:** A large empty text area.
- At the bottom, there are three buttons: "OK", "Cancel", and "Help".

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

Field	Description	Sample Value
Collector Domain	<p>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.</p>	
Policy Domain	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
Active Probes Schedule*	<p>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</p> <p>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.</p> <p>Examples:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p>	1 */9 * * *
Array Address*	Comma-separated list of IP addresses and/or names of the storage arrays.	
SMCLI client software location *	<p>The location of the SMCLI executable.</p> <p>Examples:</p> <p>Linux: <code>/opt/SM8/client/</code></p> <p>Windows: <code>C:\Program Files\SM8\client\</code></p> <p>Windows: <code>C:\Program Files (x86)\StorageManager\client</code></p>	

Field	Description	Sample Value
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.	

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
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.

The screenshot shows the 'IBM SVC Data Collector Policy' dialog box. It contains the following fields and sections:

- Collector Domain:** A dropdown menu with '1-domain-for-pat' selected.
- Policy Domain:** A dropdown menu with '1-domain-for-pat' selected.
- IBM SVC Master Console Server:*** An empty text input field.
- Port:*** A text input field containing '5989'.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat Password:*** An empty text input field.
- Active Probes:** A section with two checkboxes:
 - Array Details
 - Array Performance
- Schedules:** A section with two dropdown menus:
 - Every day at 03:01
 - Every 15 minutes
- Notes:** A large empty text area for additional information.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons are located at the bottom left. A 'Privacy Policy' link is located at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<code>yourdomain</code>

Field	Description	Sample Value
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	<p>Click the check box to activate the collection of array details.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p>* / 30 * * * * means every 30 minutes</p> <p>* / 20 9-18 * * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>* / 10 * * * * 1-5 means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Array Performance	<p>Click the checkbox to activate performance collection.</p> <p>Note that at least one collection from this array must be performed BEFORE array performance data can be collected.</p> <p>Also, statistics collection must be enabled via the IBM SVC user interface: Manage Clusters > Start Statistics Collection</p> <p>Click the clock icon to create a schedule.</p>	

Field	Description	Sample Value
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.

Pre-Installation Setup 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 APTARE 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.
- 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.

- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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.

The screenshot shows a dialog box titled "IBM XIV Data Collector Policy" with a close button in the top right corner. The dialog is divided into several sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Array Addresses:*** An empty text input field.
- IBM XIV XCLI Location:*** An empty text input field.
- User ID:*** and **Password:***: Two empty text input fields.
- Repeat Password:***: An empty text input field.
- Active Probes:** A section with two checkboxes: "Array Details" and "Array Performance".
- Schedules:** A section with two dropdown menus. The first is set to "Every 6 hours, at minute 1" and the second is set to "Every 15 minutes".
- Notes:** A large empty text area.
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom.

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

Field	Description	Sample Value
Collector Domain	<p>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.</p>	
Policy Domain	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	
Array Addresses	<p>Enter a comma-separated list of host names or IP addresses of the IBM XIV Storage Arrays from which you want to collect data.</p>	

Field	Description	Sample Value
IBM XIV XCLI Location	<p>The location for the XCLI executable on the Data Collector server.</p> <p>Examples:</p> <p>Linux: /opt/ibm/xch</p> <p>Windows: C:\Program Files (x86)\XIV\GUI10 or C:\Program Files\XIV\GUI10, C:\Program Files\IBM\Storage\XIV\XIVGUI</p>	
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
Array Details	<p>Click the check box to activate performance collection.</p> <p>Click the Clock to configure a schedule for this Data Collector policy:</p> <ul style="list-style-type: none"> ■ Frequency in minutes ■ Hourly ■ Daily ■ Weekly ■ Monthly ■ Cron Expression <p>For example:</p> <p>* / 30 * * * * means every 30 minutes</p> <p>* / 20 9-18 * * * * means every 20 minutes between the hours of 9am and 6pm</p> <p>* / 10 * * * 1-5 means every 10 minutes Mon - Fri..</p>	

Field	Description	Sample Value
Array Performance	<p>Click the check box to activate performance collection.</p> <p>Note that at least one collection from this array must be performed BEFORE array performance data can be collected.</p> <p>Click the Clock to configure a schedule for this Data Collector policy.</p>	1 */5 * * *
Notes	<p>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.</p>	

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

Pre-Installation Setup for INFINIDAT InfiniBox

This chapter includes the following topics:

- [Pre-Installation Setup for INFINIDAT InfiniBox](#)
- [Prerequisites for Adding Data Collectors \(INFINIDAT InfiniBox\)](#)
- [Installation Overview](#)
- [Add an INFINIDAT InfiniBox Data Collector Policy](#)

Pre-Installation Setup for INFINIDAT InfiniBox

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 (INFINIDAT InfiniBox)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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 Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the INFINIDAT InfiniBox 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
6. Validate the Data Collector installation.

Add an INFINIDAT InfiniBox 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.

The screenshot shows a dialog box titled "INFINIDAT InfiniBox Data Collector Policy". It contains the following fields and options:

- Collector Domain:** A dropdown menu with "INSTALLWIN2012" selected.
- Policy Domain:** A dropdown menu with "INSTALLWIN2012" selected.
- Server Addresses:*** An empty text input field.
- User ID:*** A text input field containing "denice".
- Password:*** A password input field with masked characters "*****".
- Active Probes:** A section with two checkboxes:
 - Array Capacity
 - Array Performance
- Schedules:** A section with two dropdown menus:
 - Every day at 01:01 (with a clock icon)
 - Every 15 minutes (with a clock icon)
- A large text area containing the message: "Password for the INFINIDAT InfiniBox storage system."
- Buttons at the bottom: "OK", "Cancel", "Test Connection", and "Help".

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
Server Addresses*	One or more InfiniBox Server 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
User ID*	View-only User ID for the INFINIDAT InfiniBox storage system.
Password*	Password for the INFINIDAT InfiniBox storage system. The password associated with the User ID.
Array Capacity	This collection is enabled by default to collect array capacity data from your INFINIDAT InfiniBox environment.
Array Performance	Select to collect real-time performance information for INFINIDAT InfiniBox storage system. To avoid data loss, it is recommended to set a collection schedule for no more than 25 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.

Field	Description
Test Connection	<p data-bbox="599 282 1206 421">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.</p> <p data-bbox="599 444 1206 583">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.</p> <p data-bbox="599 605 1206 800">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.</p> <p data-bbox="599 822 1206 843">See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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 248.

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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.

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 248.

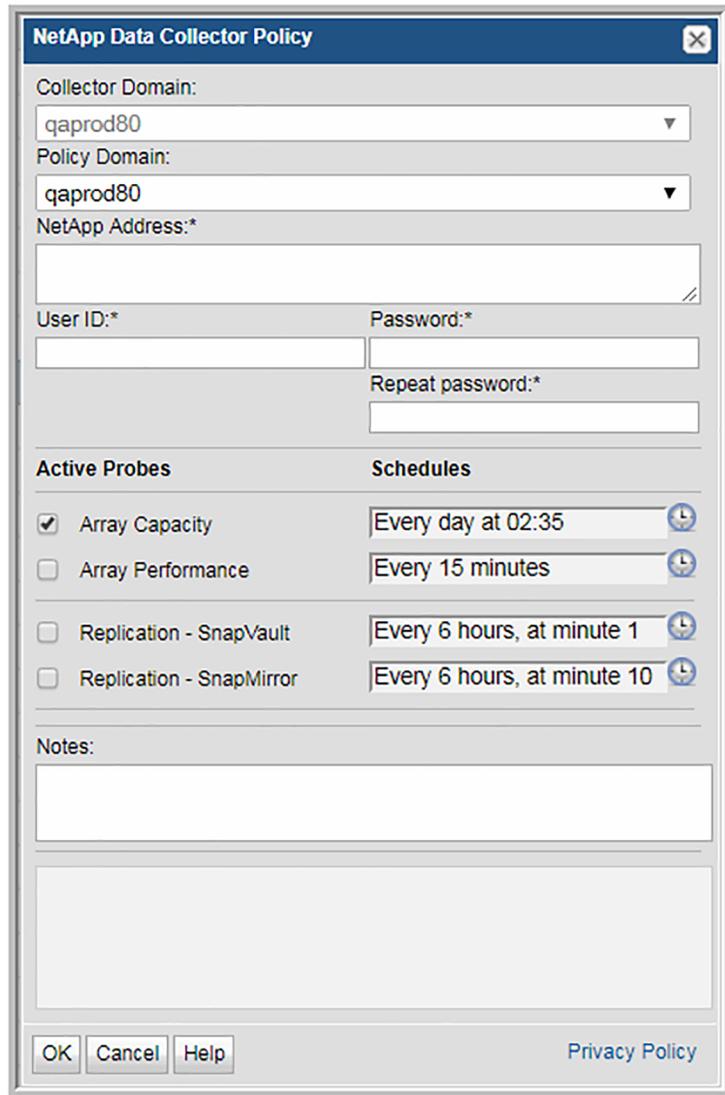
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can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



The image shows a configuration dialog box titled "NetApp Data Collector Policy". It contains several input fields and sections:

- Collector Domain:** A dropdown menu with "qaprod80" selected.
- Policy Domain:** A dropdown menu with "qaprod80" selected.
- NetApp Address:*** An empty text input field.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat password:*** An empty text input field.
- Active Probes:** A list of checkboxes:
 - Array Capacity
 - Array Performance
 - Replication - SnapVault
 - Replication - SnapMirror
- Schedules:** A list of dropdown menus with clock icons:
 - Every day at 02:35
 - Every 15 minutes
 - Every 6 hours, at minute 1
 - Every 6 hours, at minute 10
- Notes:** A large empty text area.
- Buttons:** "OK", "Cancel", and "Help" buttons are at the bottom left. A "Privacy Policy" link is at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>	
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.	

Field	Description	Sample Value
Password*	The password associated with the User ID.	
Array Capacity	<p>Check the box to collect array capacity data.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	
Array Performance	<p>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.</p> <p>Click the clock icon to create a schedule.</p>	

Field	Description	Sample Value
Replication - SnapVault	<p>Click the check box if you are collecting data from your NetApp SnapVault environment.</p> <p>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.</p> <p>This field is specific to environments licensed for Replication Manager.</p> <p>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.</p>	
Replication - SnapMirror	<p>Click the check box if you are collecting data from your NetApp SnapMirror environment.</p> <p>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.</p> <p>This field is specific to environments licensed for Replication Manager.</p> <p>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.</p>	

Field	Description	Sample Value
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 296.

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.

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

The screenshot shows a dialog box titled "Microsoft Windows Server Data Collector Policy". It contains the following fields and options:

- Collector Domain:** A dropdown menu with "Test spaces in domain nam" selected.
- Policy Domain:** A dropdown menu with "Test spaces in domain nam" selected.
- Windows Server Addresses:*** An empty text input field.
- User ID:*** A text input field containing "admin@dbnextdev".
- Password:*** A password input field with six dots.
- Active Probes:** Two checkboxes: "File Server Performance" and "Windows Event Logs", both of which are unchecked.
- Schedules:** Two dropdown menus, both set to "Every 10 minutes".
- Notes:** A text area containing the text "Password for Windows Server." in green.
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" are located at the bottom of the dialog.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
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 252. for additional information about collection options.

Field	Description
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected every 10 minutes.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup 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 APTARE 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.
- 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.
- Support Amazon Corretto 11. 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 APTARE 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 264.
- 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.

See ["Installing the WMI Proxy Service \(Windows Host Resources only\)"](#) on page 279.

6. Validate the Data Collector installation.

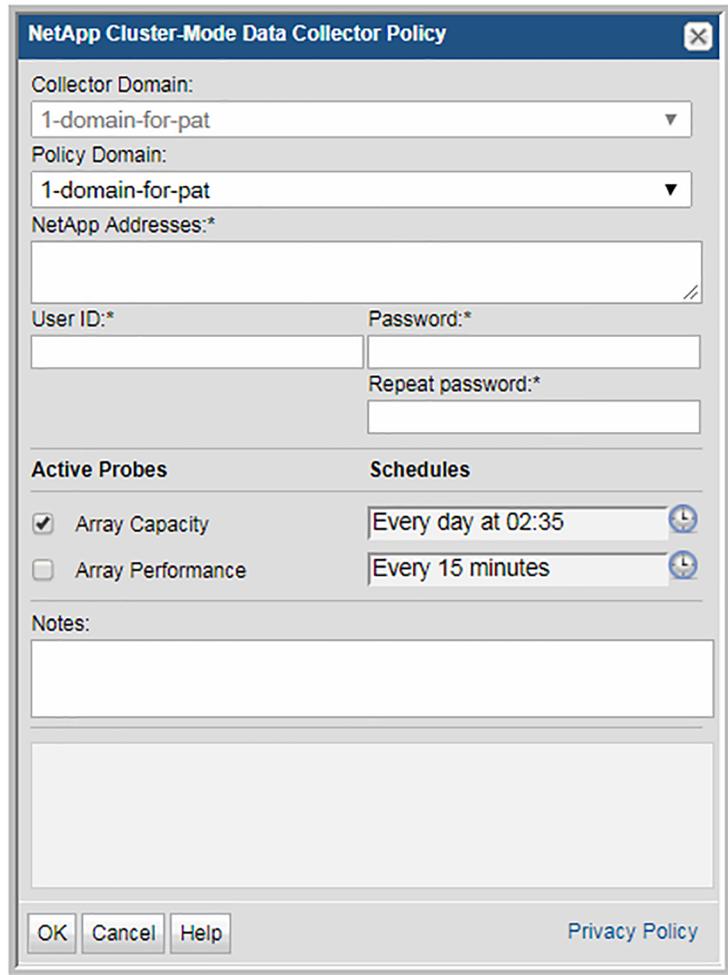
Adding a NetApp Cluster-Mode Data Collector Policy

- 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.



The image shows a dialog box titled "NetApp Cluster-Mode Data Collector Policy". It contains several fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- NetApp Addresses:*** An empty text input field.
- User ID:*** An empty text input field.
- Password:*** An empty text input field.
- Repeat password:*** An empty text input field.
- Active Probes:** A section with two options:
 - Array Capacity
 - Array Performance
- Schedules:** A section with two dropdown menus:
 - Every day at 02:35 (with a clock icon)
 - Every 15 minutes (with a clock icon)
- Notes:** A large empty text area.
- Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom left. A "Privacy Policy" link is located at the bottom right.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>	

Field	Description	Sample Value
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	<p>Check the box to collect array capacity data from your NetApp Cluster-Mode environment.</p> <p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>	1 */* * * *
Array Performance	<p>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.</p> <p>Click the clock icon to create a schedule.</p>	

Field	Description	Sample Value
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>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/
Vserver  Name                 Directory      Access
-----  -
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

```

Pre-Installation Setup 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 APTARE 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.

- 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.
- Support Amazon Corretto 11. 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 APTARE 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.

See [“Installing the WMI Proxy Service \(Windows Host Resources only\)”](#) on page 279.
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.

The screenshot shows a configuration window titled "Pure Storage FlashArray Data Collector Policy". The window contains the following fields and sections:

- Collector Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Policy Domain:** A dropdown menu with "1-domain-for-pat" selected.
- Array Addresses:*** An empty text input field.
- User ID:*** A text input field containing "admin@etchsketchteam".
- Password:*** A text input field containing a single dot ".".
- Active Probes:** A section with two checked checkboxes: "Array Capacity" and "Array Performance".
- Schedules:** A section with two dropdown menus: "Every day at 04:04" and "Every 15 minutes".
- Notes:** A text area containing the text "Password for the Pure Storage FlashArray storage system." in green.
- Buttons:** "OK", "Cancel", "Test Connection", and "Help" buttons at the bottom.

- 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	<p>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.</p> <p>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.</p> <p>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.</p>
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.

Field	Description
Schedule	<p>Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily.</p> <p>Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
Notes	<p>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.</p>
Test Connection	<p>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.</p> <p>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.</p> <p>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.</p> <p>See “Working with On-Demand Data Collection” on page 296.</p>

Pre-Installation Setup for Veritas NetBackup Appliance

This chapter includes the following topics:

- [Overview](#)
- [Prerequisites for Adding Data Collectors \(Veritas NetBackup Appliance\)](#)
- [Installation Overview \(Veritas NetBackup Appliance\)](#)
- [Adding a Veritas NetBackup Appliance Data Collector Policy](#)

Overview

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 (Veritas NetBackup Appliance)

- Install Data Collector on the same server as NetBackup Appliance.
- Minimum NetBackup Appliance 3.1.2 is recommended. If a previous version is installed, the utility `nb_monitor_util`, must be manually installed.

- Server requirements include:
- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- When the APTARE 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.
- 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.
- Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, the recommendation is that you 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).

Installation Overview (Veritas NetBackup Appliance)

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

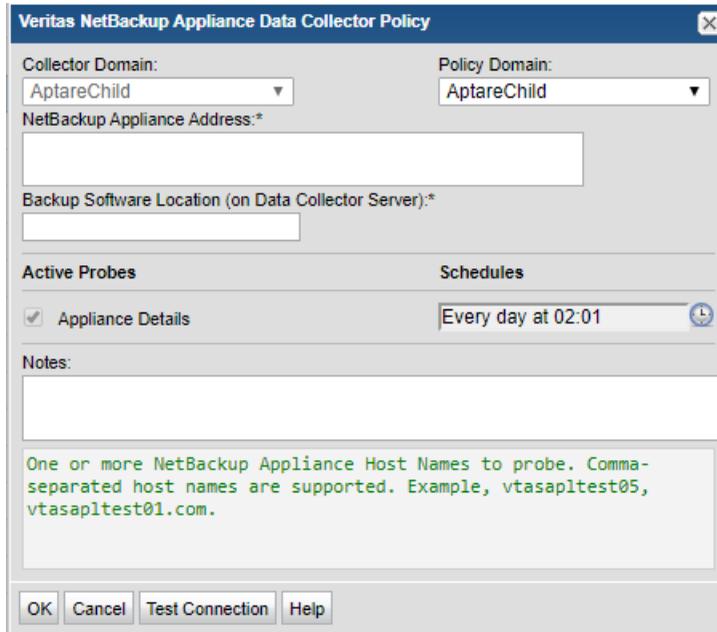
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Veritas NetBackup Appliance data collector policy.
4. On the NetBackup Appliance Server, install the Data Collector Software
5. If collecting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

Adding a Veritas NetBackup Appliance 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.

To add the policy

- 1 Select **Admin>Data Collection>Collector Administration**. Currently configured Portal Data Collectors are displayed.
- 2 Search for 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(*).
- 6 Click **OK** to save the policy.



Field

Collector Domain

Description

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.

Field	Description
NetBackup Appliance Address**	One or more NetBackup Appliance Servers to probe. Comma-separated host names are supported. For example, nbuaplttest05, nbuaplttest01.com.
Backup Software Location (on Data Collector Server)*	Backup Software Home Location should either be the root folder or directory where the NetBackup Remote Administration Console software is installed, or the root folder to the netbackup/volmgr folder(s) where the NetBackup software is installed. Default Backup Software Home location for Veritas NetBackup: For Windows: C:\Program Files\Veritas. For Linux: /usr/opensv
Appliance Details	<p>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.</p> <p>Examples of CRON expressions:</p> <p><code>*/30 * * * *</code> means every 30 minutes</p> <p><code>*/20 9-18 * * * *</code> means every 20 minutes between the hours of 9am and 6pm</p> <p><code>*/10 * * * 1-5</code> means every 10 minutes Mon - Fri.</p> <p>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.</p>
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

Test Connection

Description

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. Test Connection also checks that the utility `nb_monitor` is installed.

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.

Installing the Data Collector Software

This chapter includes the following topics:

- [Introduction](#)
- [Installing the WMI Proxy Service \(Windows Host Resources only\)](#)
- [Testing WMI Connectivity](#)
- [Installing Data Collector Software: From the Internet](#)
- [Installing Data Collector Software: No Internet Available from the Data Collector Server](#)
- [Installing Data Collector Software: UI Deployment](#)
- [Installing Data Collector Software: From the Console](#)

Introduction

This section includes the instructions for installing the Data Collector software on the Data Collector Server. In addition, 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 storage array Data Collector installation on a Windows server.

In addition to the GUI version, the installer supports a console (command line) interface for Linux systems that do not have X-Windows installed. You will be directed to the console interface instructions, if appropriate.

When the APTARE 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.

Installing the WMI Proxy Service (Windows Host Resources only)

To collect data from Windows hosts, choose a Windows host on which to install the WMI proxy.

- This is only required if you are collecting data from Windows Host Resources.
- The WMI Proxy needs to be installed on only one Windows host.
- If the Data Collector is on a Windows server, the WMI Proxy will be installed there as part of the storage array Data Collector installation.
- If the Data Collector is on a Linux server, you'll need to identify a Windows server on which to install the WMI proxy service.

1. Locate the executable on the Portal and copy it to the Data Collector server.

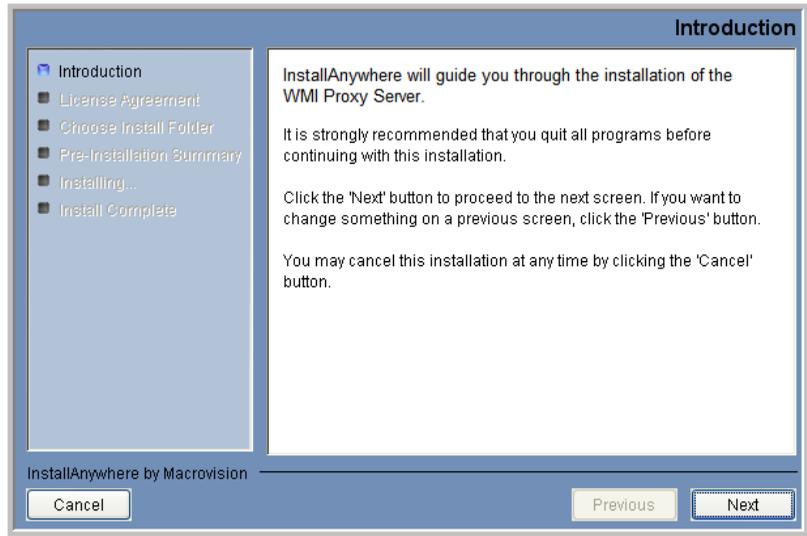
On Windows:

```
c:\opt\aptare\utils\aptarewmiproxyserver.exe
```

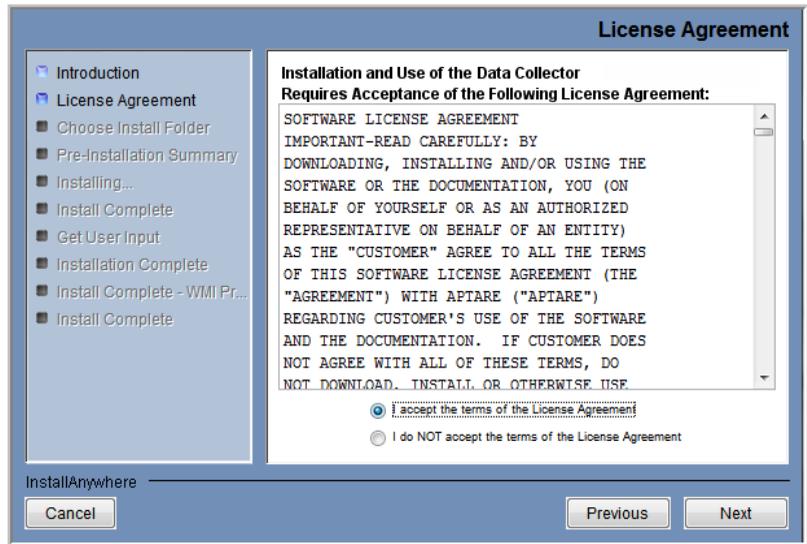
On Linux:

```
/opt/aptare/utils/aptarewmiproxyserver.exe
```

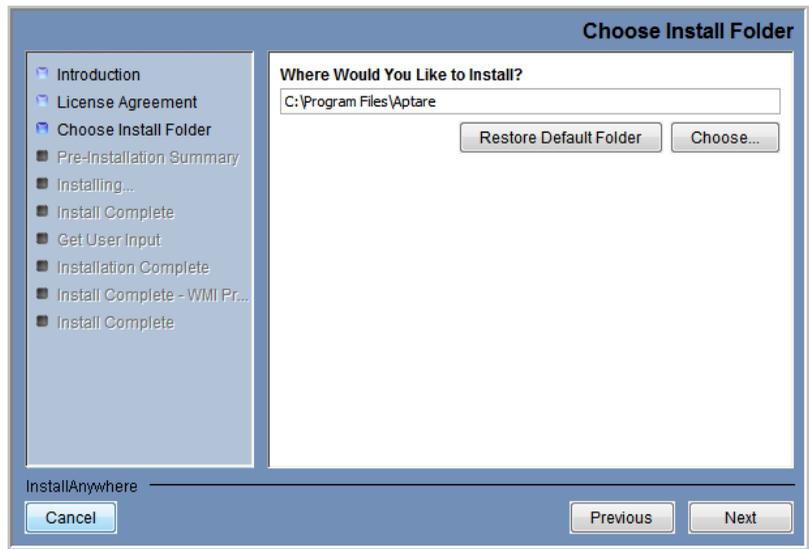
2. Install Anywhere will prepare to install the Data Collector Software. An Introduction dialog box will outline the installation process.



3. Click **Next** to view the License Agreement.



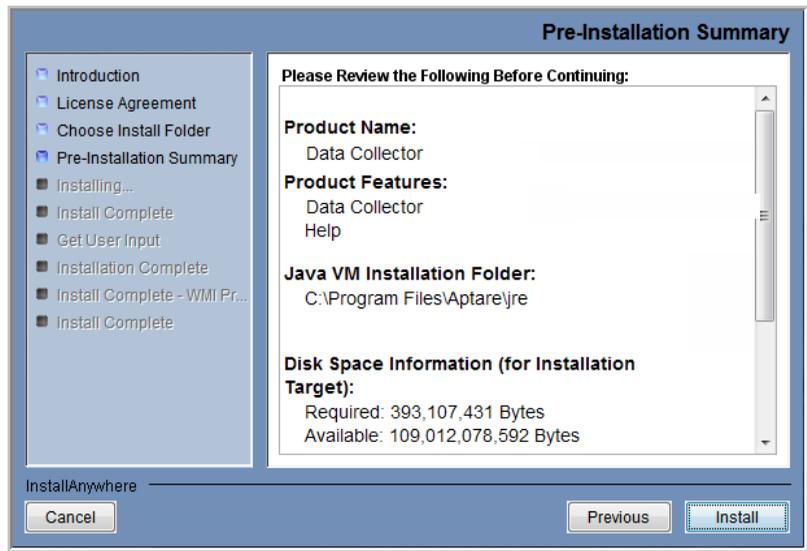
4. Read the agreement.
5. Click on the “I accept the terms of the License Agreement” radio button.
6. Click **Next** to display the window where you will choose the installation folder.



7. Specify the directory where you would like to install the Data Collector software.
 - Default for Windows: **C:\Program Files\Aptare**
 - Default for Linux: **/opt/aptare**

Note: Accepting the default path is recommended.

8. Click **Next**.
9. Verify the pre-installation summary.



10. Click **Install** to proceed with the installation.
11. If the installer detects that you do not have Microsoft .NET already installed on the server, it will notify you of this required dependency. Microsoft .NET contains several necessary libraries. Refer to the *Certified Configurations Guide* for the required version of .NET.
12. Click **OK** to enable the installer to proceed with the installation of Microsoft .NET.

The wizard will step you through the process and its progress.

When the WMI Proxy installation completes, the WMI Server will be listed in the Windows Services list with a Startup Type of Automatic, however, this first time you will need to start the service from the Services window. Each time you re-start this Windows server, the proxy services will start automatically.

13. To access the Windows Services list to start the WMI Proxy Server:

Startup > Control Panel > Administrative Tools > Services

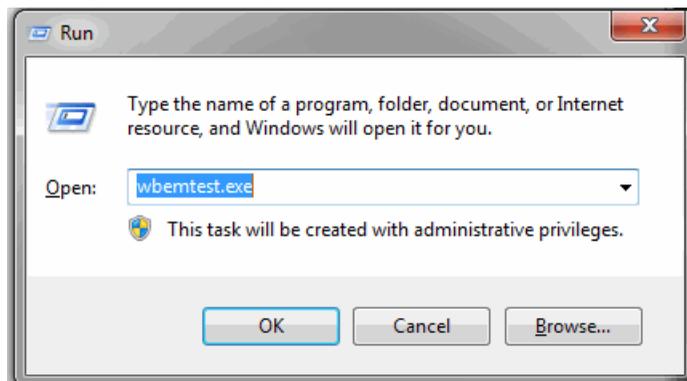
14. A window will be displayed when the installation is complete.
15. Click **Done** to complete the process.
16. It is recommended that you run the C:\Program Files\Aptare\mbs\bin\checkinstall.bat batch file to validate the Data Collector Installation.

Testing WMI Connectivity

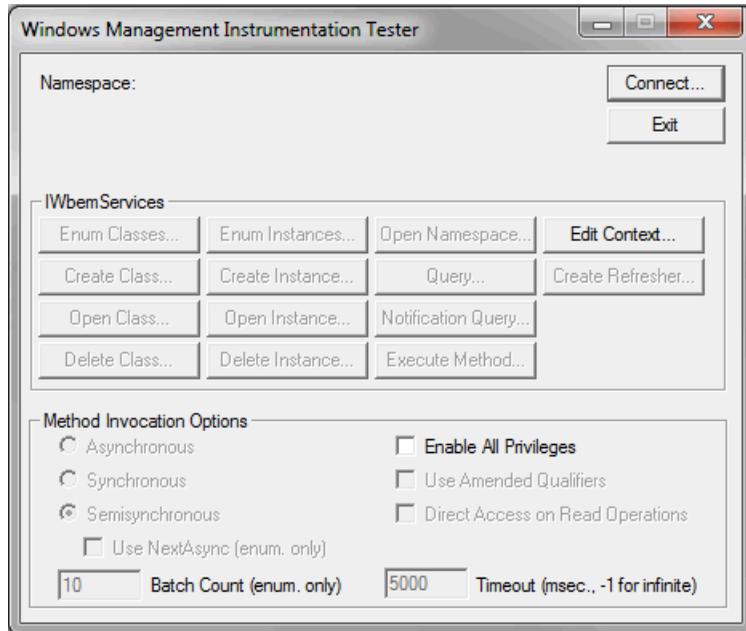
The Windows Management Instrumentation (WMI) Proxy is used by APTARE IT Analytics to collect data from Windows hosts. Should you have connectivity issues, these steps can be taken to test and troubleshoot connectivity.

To verify that WMI is working properly, take the following steps:

1. Log in to the Data Collector server as an Administrator.
2. From the Windows Start menu, type Run in the search box to launch the following window where you will enter **wbemtest.exe** and click **OK**.



3. In the Windows Management Instrumentation Tester window, click **Connect**.



4. In the Connect window, preface the Namespace entry with the IP address or hostname of the target remote server in the following format:

```
\\<IP Address>\root\cimv2
```

The image shows a 'Connect' dialog box with the following fields and options:

- Namespace:** Text box containing 'root\cimv2'. Buttons: Connect, Cancel.
- Connection:** Using: IWbemLocator (Namespaces); Returning: IWbemServices; Completion: Synchronous.
- Credentials:** User: []; Password: []; Authority: [].
- Locale:** []
- How to interpret empty password:** NULL, Blank.
- Impersonation level:** Identify, Impersonate, Delegate.
- Authentication level:** None, Packet, Connection, Packet integrity, Call, Packet privacy.

5. Complete the following fields in the Connect window and then click **Connect**.
 - User - Enter the credentials for accessing the remote computer. This may require you to enable RPC (the remote procedure call protocol) on the remote computer.
 - Password
 - Authority: Enter **NTLMDOMAIN:<NameOfDomain>** where NameOfDomain is the domain of the user account specified in the User field.
6. Click **Enum Classes**.
7. In the Superclass Info window, select the **Recursive** radio button, but do not enter a superclass name. Then, click **OK**.
8. The WMI Tester will generate a list of classes. If this list does not appear, go to the Microsoft Developer Network web site for troubleshooting help.

<http://msdn.microsoft.com/en-us/library/ms735120.aspx>

Installing Data Collector Software: From the Internet

Follow these instructions if you are installing on a Data Collector Server that has Internet access and a web browser.

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

If your Data Collector Server does not have Internet access or web browser access—for example, X-Windows not available, proceed to the following section.

See [“Installing Data Collector Software: No Internet Available from the Data Collector Server”](#) on page 286.

1. Start the web browser on the **Data Collector Server**.
2. Navigate to the Support website to access the relevant download link.
3. Select the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.
 - Linux: `sc_datacollector_linux_<releaseversion>_<MMDDYYYY>.bin`
 - Windows: `sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe`
4. Execute the OS-specific Data Collector installer.
5. Proceed to the UI Deployment of the Data Collector.

See [“Installing Data Collector Software: UI Deployment ”](#) on page 287.

Installing Data Collector Software: No Internet Available from the Data Collector Server

Use these instructions if you are installing via the Internet where Internet access is not available from the data collector server.

1. Note the Platform/OS of the **Data Collector Server** on which you want to install the Data Collector.
2. Open a browser on a client with web access (you will download the installer to this client, and then copy it to the **Data Collector Server**).
3. Navigate to the Support website to access the relevant download link.
4. Download the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.
 - Linux: `sc_datacollector_linux_<releaseversion>_<MMDDYYYY>.bin`

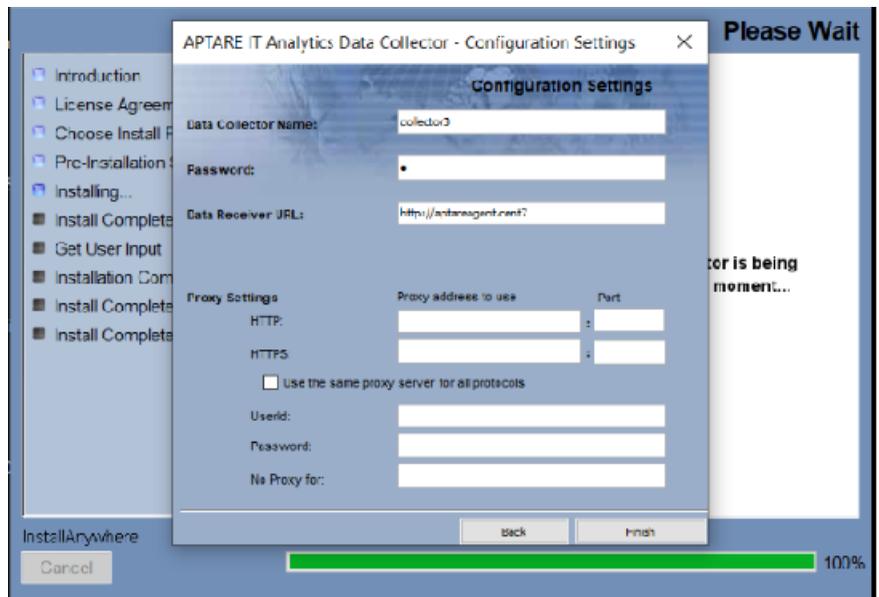
- Windows: `sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe`
- 5. At the prompt, save the Data Collector Installer to a directory on the client.
- 6. Copy the Data Collector Installer to the Data Collector Server where the Data Collector is to be installed.
- 7. Go to the Data Collector Server and run the installer.
 - **On Windows:**
Execute `sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe`
 - Proceed to the UI deployment.
See [“Installing Data Collector Software: UI Deployment”](#) on page 287.
 - **On Linux:**
If the **Data Collector Server** has X-Windows, take these steps, substituting the relevant Data Collector Installer name for `<installer_file>`
`chmod +x <installer_file>`
`sh ./<installer_file> -i swing`
 - Proceed to the UI deployment.
See [“Installing Data Collector Software: UI Deployment”](#) on page 287.
If the **Data Collector Server** does not have X-Windows:
 - Proceed to the Console Installation instructions.

Installing Data Collector Software: UI Deployment

InstallAnywhere will prepare to install the Data Collector software. After checking the available disk space and downloading the installer, an introduction dialog window outlines the installation process.

1. Review the installation process and click **Next**. The License Agreement displays for your acknowledgement.
2. Read the agreement and click the “I accept” radio button and then **Next**. The installer will display a window, which prompts you for an Install Folder.
3. Specify the directory where you would like to install the Data Collector software. Accepting the default paths is recommended. Windows default directory:
`C:\Program Files\Aptare`
4. Click **Next** to display the Pre-Installation Summary.

5. Review the summary and click **Install**. The dialog tracks the installation as it progresses.
6. A Configuration Settings window will prompt you to select a Data Collection Task. The configuration choices are: Data Collector (includes WMI Proxy) or WMI Proxy Server (only). A single Data Collector can be installed for multiple products on a single server. When you select a backup product, if you are installing on a Windows server, the WMI Proxy Server is automatically included with the installation. When you select a storage array, the Host Resources setup is automatically included in the installation. The WMI Proxy Server also can be installed individually.
7. Enter the configuration settings for your particular environment.



8. After entering the configuration settings, click **Next**. At this point, the Data Collector has been successfully installed, however, to validate the Data Collector installation, it is recommended that you run the `C:\Program Files\Aptare\mbs\bin\checkinstall.bat` batch file.
9. Choose **Run now** and click **Done** in the **Get User Input** window to validate the installation and then quit the installer. The InstallAnywhere portion of the installation is now complete and the process continues with the command-line script execution.

Field	Description
Data Collector Name *	A unique name assigned to this Data Collector. This is the name that you used during the pre-Installation setup. The Data Collector will use this value for authentication purposes.
Password *	The password assigned to this Data Collector. The password is encrypted prior to saving in the APTARE IT Analytics database and is never visible in any part of the application.
Data Receiver URL*	This is the URL the Data Collector uses to communicate to the Portal server. The format of this URL should be: http://aptareagent.yourdomain.com It is similar to the URL you use to access the web-based Portal (http://aptareportal.yourdomain.com). Note: Be sure to enter the URL with the prefix aptareagent and NOT aptareportal.
Proxy Settings (Optional)	Enter the proxy server details for both http and https, including the User ID and Password for the server. HTTP/HTTPS: Enter a hostname or IP address and a port number. Use the same proxy server for all protocols: Check this box if the proxy server is used for all. User ID & Password: Enter the credentials for the proxy server. No Proxy for: List hostnames or IP addresses that will not be proxied. Examples: 192.168.1.1/21, localhost

Installing Data Collector Software: From the Console

Follow these instructions when installing on a Linux server that does not have X-Windows. The Installer will guide you through the sequence of steps to install and configure the Data Collector. If at any time you need to go back a step, simply type 'back' at the prompt.

Note: The Data Collector installer does not support console-based installation for the Windows operating system.

1. From your telnet session **cd** to the location where the Data Collector Installer file has been saved.

2. Execute the following commands, substituting the relevant Data Collector Installer name for <installer_name>.bin.

```
chmod +x <installer_name>.bin
sh ./<installer_name>.bin -i console
```

3. InstallAnywhere will prepare to install the Data Collector software.
4. The License Agreement will be displayed.
5. Read the agreement and type **Y** to accept it.
6. The installer will prompt for the installation location.
7. A Pre-Installation Summary will be displayed.
8. The installation process will track the progress.
9. The installer will prompt for the **Data Collector Name**. This is the ID that will be used on the Portal side to authenticate the Data Collector. This value should be the same value you configured on the Portal for the field "ID" during the Pre-Installation step.
10. The installer will prompt for the **Data Collector Password**. This is the password that will be used on the Portal side to authenticate the Data Collector. This value should be the same value you configured on the Portal for the field "password" during the Pre-Installation step.
11. The installer will prompt for the **Data Receiver URL**. This is the URL the Data Collector uses to communicate to the Portal server. This is the URL the Data Collector uses to communicate to the Portal server. The format of this URL should be:

`http://aptareagent.yourdomain.com`

It is similar to the URL you use to access the web-based Portal (`http://aptareportal.yourdomain.com`).

IMPORTANT NOTE: Be sure to enter the URL with the prefix `aptareagent` and **NOT** `aptareportal`

Configuration Settings - 3

```
-----
Enter Data Receiver URL
(Required Field)
Data Receiver URL (DEFAULT: ):
http://aptareagent.yourdomain.com
The installer will perform a post-install validation:
The installer will now configure the installation.
This may take a few minutes.
```

12. Web Proxy (HTTP) settings can be configured.

```
Configuration Settings- 4
-----
Connection Settings
Use Proxies? (Y/N) (DEFAULT: N): y
```

```
Configuration Settings - 5
-----
Enter HTTP Proxy IP Address
(Please leave field empty if there is no Proxy/Firewall)

HTTP Proxy IP Address (DEFAULT: ): 10.2.2.116
```

```
Configuration Settings - 6
-----
Enter HTTP Proxy Port
(Please leave field empty if there is no Proxy/Firewall)

HTTP Proxy Port (DEFAULT: ): 3128
```

```
Configuration Settings - 7
-----
Enter HTTPs Proxy IP Address
(Please leave field empty if there is no Proxy/Firewall)

HTTPs Proxy IP Address (DEFAULT: ):
```

```
Configuration Settings - 8
-----
Enter HTTPs Proxy Port
```

(Please leave field empty if there is no Proxy/Firewall)

HTTPs Proxy Port (DEFAULT:):

Configuration Settings - 9

Enter Proxy UserId

(Please leave field empty if there is no Proxy/Firewall)

Proxy UserId (DEFAULT:):

Configuration Settings - 10

Enter Proxy Password

(Please leave field empty if there is no Proxy/Firewall)

Proxy Password:

Configuration Settings - 11

Enter comma separated IP Addresses to exclude from Proxy

(Please leave field empty if there is no Proxy/Firewall)

No Proxy for (DEFAULT:):

The installer will now configure the installation.

This may take a few minutes.

PRESS <ENTER> TO

CONTINUE:=====

Installation Complete

To validate the Data Collector installation, it is recommended that you run the

<home>/mbs/bin/checkinstall.sh script.

Validating Data Collection

This chapter includes the following topics:

- [Validation Methods](#)
- [Data Collectors: Vendor-Specific Validation Methods](#)
- [Working with On-Demand Data Collection](#)
- [Using the CLI Checkinstall 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 296.

- 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 Checkinstall Utility”](#) on page 298.

Note: APTARE 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 30-1

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
Dell Compellent			x
Dell EMC Elastic Cloud Storage (ECS)	x	x	
Dell EMC NetWorker Backup & Recovery	x		
Dell EMC Unity	x	x	
EMC Avamar		x	
EMC Data Domain Backup	x	x	
EMC Data Domain Storage	x	x	

Table 30-1 (continued)

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
EMC Isilon		x	
EMC NetWorker			x
EMC Symmetrix	x	x	
EMC VNX CLARiiON	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	
Huawei OceanStor	x	x	
IBM Enterprise			x
IBM SVC			x
IBM Spectrum Protect (TSM)		x	
IBM VIO	x	x	
IBM XIV			x
INFINIDAT Infinibox	x	x	
Microsoft Azure	x	x	

Table 30-1 (continued)

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Microsoft Hyper-V	x	x	
Microsoft Windows Server	x	x	
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

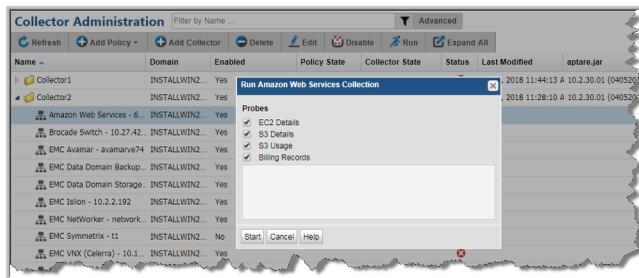
Note: On-Demand data collection is not available for all policies.

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
- 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, providing the policy is one of the specified vendors and the Collector is online.

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 individual probes and servers 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 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.

Using the CLI Checkinstall 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: APTARE 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\Aptare) or Linux (/opt/aptare).

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 telnet 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\Aptare\mbs\bin <enter>
```

Linux: In the telnet session, type:

```
cd /opt/aptare/mbs/bin <enter>
```

3 Execute the validation script.

Windows: At the command prompt, type: `checkinstall.bat <enter>`

Linux: In the telnet 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. This utility will fail if a Data Collector policy has not been configured in the Portal. For a component check, specifically for Host Resources, run the **hostresourcedetail.sh|bat** utility.

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 CLARiiON, EMC Data Domain, EMC VNX arrays, HP 3PAR, IBM mid-range arrays, 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**, then contact Support and have the following files ready for review:

```
/opt/aptare/mbs/logs/validation/
```

```
C:\Program Files\Aptare\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**

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

Note: This uninstall process assumes that the Data Collector was installed using the standard installation process.

1. Login to the **Data Collector Server** as **root**.
2. Stop the Data Collector service, using the command appropriate for the operating system.

```
[Data Collector Home Folder]/mbs/bin/aptare_agent stop
```

3. Run the `Uninstall Data Collector Agent` script, located in the following directory:

```
[Data Collector Home Folder]/UninstallerData
```

Uninstall the Data Collector on Windows

1. Login to the **Data Collector Server**. (User must have Administrator privileges.)
2. Stop the Data Collector services.
 - Click **Start > Settings > Control Panel**
 - Click **Administrative Tools**.
 - Click **Services**.
3. Click **Uninstall APTARE IT Analytics Data Collector in Start Menu/Programs/APTARE IT Analytics Data Collector**
4. Follow the prompts in the uninstall windows.

Note: The uninstaller may not delete the entire Data Collector directory structure. Sometimes new files, created after the installation, along with their parent directories, are not removed. You may need to manually remove the root install folder (default C:\Program Files\Aptare) and its sub-folders after the uninstaller completes.

Manually Starting the Data Collector

This chapter includes the following topics:

- [Introduction](#)

Introduction

The installer configures the Data Collector to start automatically, however, it does not actually start it upon completion of the installation because you must first validate the installation.

Follow these steps, for the relevant operating system, to manually start the Data Collector service:

On Windows

The installer configures the Data Collector process as a Service.

To view the Data Collector Status:

1. Click **Start > Settings > Control Panel**
2. Click **Administrative Tools**.
3. Click **Services**. The Microsoft Services dialog is displayed. It should include entries for **Aptare Agent**. Start this service if it is not running.

On Linux

The installer automatically copies the Data Collector “start” and “stop” scripts to the appropriate directory, based on the vendor operating system.

To start the data collector, use the following command:

```
etc/init.d/aptare_agent start
```

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
Linux Hosts	SSH 22, Telnet 23
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139
Oracle Oracle TNS listener port	1521

Table A-1 Components: Default Ports (*continued*)

Component	Default Ports
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

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 80/443
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 (CLARiiON)	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

Table A-2 Storage Vendors: Default Ports (*continued*)

Storage Vendor	Default Ports and Notes
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
Huawei OceanStor Enterprise Storage	8080
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778
INFINIDAT InfiniBox	REST API TCP 80, 443
Microsoft Windows Server	2012 R2, 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
Veritas NetBackup Appliance	1556

Table A-3 Data Protection: Default Ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443

Table A-3 Data Protection: Default Ports (*continued*)

Data Protection Vendor	Default Ports and Notes
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
EMC NetWorker	<ul style="list-style-type: none"> ■ NSRADMIN TCP 7937-7940 ■ WMI Proxy range of ports ■ SSH 22 (Linux)
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
Veritas NetBackup	1556, 13724 WMI ports SSH 22 (Linux)

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, Telnet 23
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
Amazon Web Services	https 443
Microsoft Azure	https 443
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22