VERITAS
APTARE IT Analytics™

Data Collector Installation Guide for Backup Manager

Contents

Chapter 1
Introduction

Chapter 2
Pre-Installation Setup for Commvault Simpana

Chapter 3
Pre-Installation Setup for Cohesity DataProtect

Chapter 4
Pre-Installation Setup for EMC Avamar

Chapter 5
Pre-Installation Setup for EMC Data Domain Backup

Chapter 6
Pre-Installation Setup for EMC NetWorker

Chapter 7
Pre-Installation Setup for Generic Backup

Chapter 8
Pre-Installation Setup for HP Data Protector

Chapter 9
Pre-Installation Setup for IBM Spectrum Protect (TSM)

Chapter 10
Pre-Installation Setup for Veritas Backup Exec

Chapter 11
Pre-Installation Setup for Veritas NetBackup

Chapter 12
Pre-Installation Setup for Oracle Recovery Manager (RMAN)

Chapter 13
Pre-Installation Setup for Rubrik Cloud Data Management

Chapter 14
Pre-Installation Setup for Veeam Backup & Replication

Chapter 15
Discovery Policies for Veritas NetBackup

Chapter 16
Installing Data Collectors

Chapter 17
Validating Data Collection

Chapter 18
Manually Starting the Data Collector

Chapter 19
Uninstalling the Data Collector

Chapter 20
Load Historic Events

Appendix A
Troubleshooting

Appendix A
CRON Expressions and Probe Schedules

Appendix B
Firewall Configuration: Default Ports

Copyrights and Trademarks

Legal Notice

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

1

Introduction

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

Backup Manager: Collection of Backup and Restore Data

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.

For Backup Manager, where you install the Data Collector also depends on the backup solution.

- For Commvault Simpana, the Data Collector should be installed on the same machine as the WMI proxy server.
- For all other backup solutions, the Data Collector can run on any server running a supported operating system.
- One Data Collector can be used to include *all* of these backup products: Commvault Simpana, EMC Avamar, EMC NetWorker, EMC Data Domain, Veritas Backup Exec, Veritas NetBackup, HP Data Protector, and Generic Backup products. And, you also can include other enterprise objects, such as storage arrays, in a single Data Collector.

Data Collection by Backup Product

The following collection mechanisms are used for the particular backup products:

- **Commvault Simpana** - The Data Collector uses JDBC as a read-only user (including executing some read-only functions) to collect point-in-time data from the Commvault Simpana CommServe database. The Data Collector also uses a Commvault Simpana command-line tool (sendLogFiles.exe - executed using WMI on the CommServe server) to collect log files from client machines managed by the CommServe server.
- **EMC Avamar** - The Data Collector uses JDBC as a read-only user to collect point-in-time data from the Avamar Management Console Server (MCS) database.
- **EMC Data Domain** - A Data Collector policy can be configured to use the command-line interface (CLI) to gather the details. Note that more details can be obtained via the CLI than with SNMP.

- **EMC NetWorker -** The Data Collector uses the NetWorker administration command-line utilities, such as mminfo, nsradmin, and nsrinfo.
- **Generic Backup Data -** APTARE Backup Manager can report on data from backup products that are *not* native to APTARE IT Analytics—such as PureDisk, BakBone, and BrightStor. Using the backup vendor's export feature, create a comma-separated values (CSV) file. The Data Collection process will import the data into the Portal database.
- **HP Data Protector -** The Data Collector communicates with the Cell Manager—the server that runs session managers and core software to manage the backup details in the HP Data Protector internal database (IDB).
- **IBM Tivoli Storage Manager (TSM) -** The Data Collector interfaces with TSM using the TSM utility, dsmadmc, collecting data from the underlying TSM databases, including TSM Archives for LAN-free backups.
- **Veritas Backup Exec -** The Data Collector uses database commands to obtain information from each Backup Exec server.
- **Veritas NetBackup -** A single, centralized Data Collector can collect from multiple NetBackup Master Servers. A variety of probes can be selected to gather details such as tape inventory and storage lifecycle policies (SLP).

2

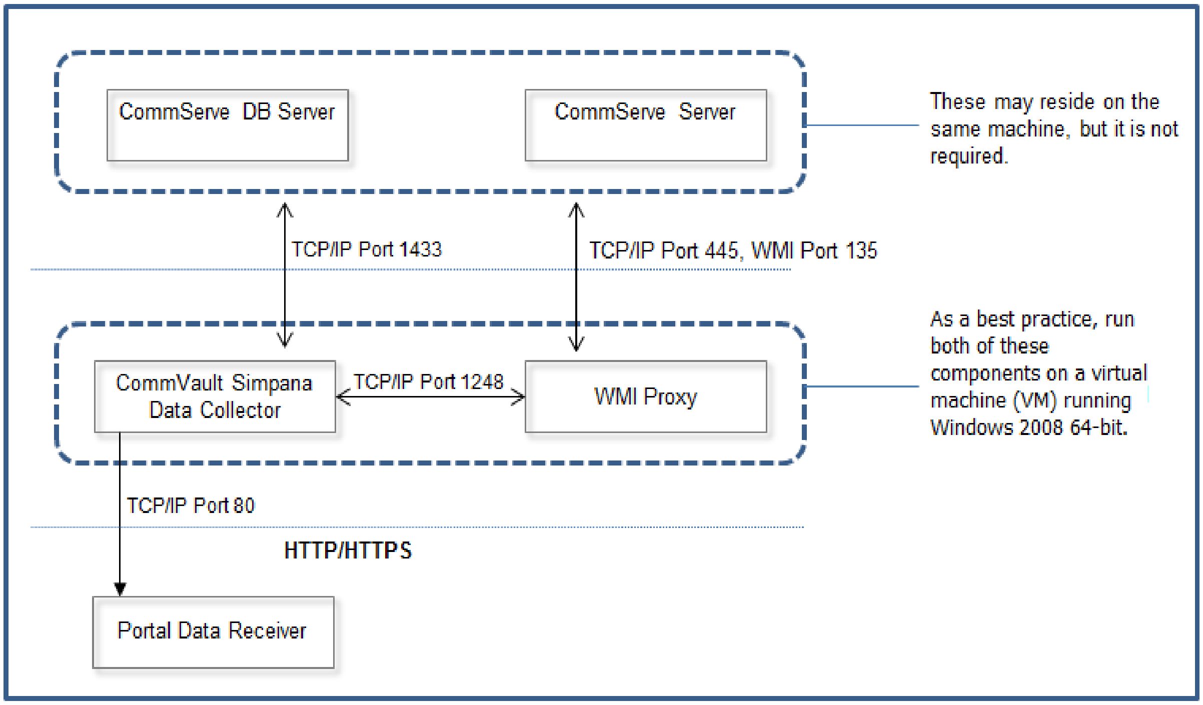
Pre-Installation Setup for Commvault Simpana

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

Architecture Overview (Commvault Simpana)

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

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



CommServe DB Server
CommServe Server
These may reside on the same machine, but it is not required.
TCP/IP Port 1433
TCP/IP Port 445, WMI Port 135
CommVault Simpana Data Collector
TCP/IP Port 1248
WMI Proxy
As a best practice, run both of these components on a virtual machine (VM) running Windows 2008 64-bit.
TCP/IP Port 80
HTTP/HTTPS
Portal Data Receiver

Prerequisites for Adding Data Collectors (Commvault Simpana)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the 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.
- Open TCP/IP access to the Commvault database on a static port (1433 recommended). See Open TCP/IP Access to the Commvault Database.
- MS SQL Server needs to be accessible to the collector on a static TCP Port (1433 recommended), requiring a restart of the SQL database service, if not already configured.
- MS SQL Server must be set to Mixed-mode authentication, and the login to be used for collection must be using SQL authentication. See https://msdn.microsoft.com/en-us/library/ms188670.aspx.
- WMI Proxy access requires the following: Port 135 is required for skipped files collection and 445 for CIFS over TCP. A fixed port can be configured for WMI as specified at: http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx
- The Data Collector should be installed on the same server as the WMI proxy server.
- Read-only user configured on the CommServe server. See Set Up a Read-Only User in the CommServe Server.
- If you want to load historical data from a CommServe database, use the utility described in Load Historical Data Prior to Initial Data Collection.
- One Data Collector can include *all* of these backup products: Commvault Simpana, EMC Avamar, EMC NetWorker, EMC Data Domain, Veritas Backup Exec, Veritas NetBackup, HP Data Protector, IBM Spectrum Protect (TSM), and Generic Backup products. And, you also can include other enterprise objects, such as storage arrays, in this Data Collector.

Upgrade Troubleshooting: Microsoft SQL Server and Java 10

With release version 10.3 introducing support for Java 10, 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 version 10.3 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 10.

```
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)
```

APTARE recommends to upgrade MS SQL Server to the latest version to enable secure collection. Your MS SQL Server version may not be supported for APTARE IT Analytics version 10.3. 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 allow communication with the data collector:

1. Edit <collector install dir>/jre/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=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
   #    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
       EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   ```
4. Remove `3DES_EDE_CBC`.

   ```
   #jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
   #    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
       EC keySize < 224, DES40_CBC, RC4_40
   ```
5. Save the file.
6. Run **checkinstall** and verify collection succeeds.

If **checkinstall** does not succeed, each of the following algorithms can be individually re-enabled in an attempt to restore compatibility.

7. If **checkinstall** does not succeed, restore, remove `RC4_40`, save, re-run **checkinstall**.

   ```
   #jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
   #    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
       EC keySize < 224, DES40_CBC, 3DES_EDE_CBC
   ```
8. If **checkinstall** does not succeed, restore, remove `DES40_CBC`, save, re-run **checkinstall**.

   ```
   #jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
   #    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
       EC keySize < 224, RC4_40, 3DES_EDE_CBC
   ```
9. If **checkinstall** does not succeed, restore, change the `DH keySize` as follows, save, re-run **checkinstall**.

   ```
   #jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
   #    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 768, \
       EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
   ```
10. After a working configuration is found, restart the collector service.

Installation Overview (Commvault Simpana)

1. Updating the Local Hosts File for Data Collection
2. Open TCP/IP Access to the Commvault Database

3. Set Up a Read-Only User in the CommServe Server
4. Add Commvault Simpana Servers
5. Load Historical Data Prior to Initial Data Collection
6. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
7. In the Portal, add the Commvault Simpana data collector policy. Adding a Commvault Simpana Data Collector Policy
8. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
9. Validate the Data Collector Installation. See Validating Data Collection.

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

Open TCP/IP Access to the Commvault Database

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

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

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

Additional Static Port Configuration Steps

If you configured a static port during the port configuration process (Open TCP/IP Access to the Commvault Database), take the following additional steps.

On the Commvault CommCell Server:

1. Start the **ODBC Data Source Administrator** tool.
2. Select the Commvault database DSN (usually a system DSN) and click **Configure**.
3. Click **Next**.
4. Select **With SQL Server authentication using a login ID and password entered by the user**.

5. Enter the required User ID and password.
6. Click **Client Configuration** and make the following changes.
   - In the Network libraries window, select **TCP/IP**.
   - Enter the server name.
   - De-select **Dynamically determine port**. ODBC uses port 1433 as a default, so it will be grayed out.
   - Click **OK**.
7. Click **Next** and change the database, if needed.
8. Click **Next**, then **Finish**.
9. Click **Test Data Source**.
10. Click **OK**.

Set Up a Read-Only User in the CommServe Server

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

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

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

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

   dbo.GetDateTime

   dbo.GetUnixTime

   dbo.GetJobFailureReason

   dbo.JMGetLocalizedMessageFunc

There are two methods for assigning EXECUTE permission.

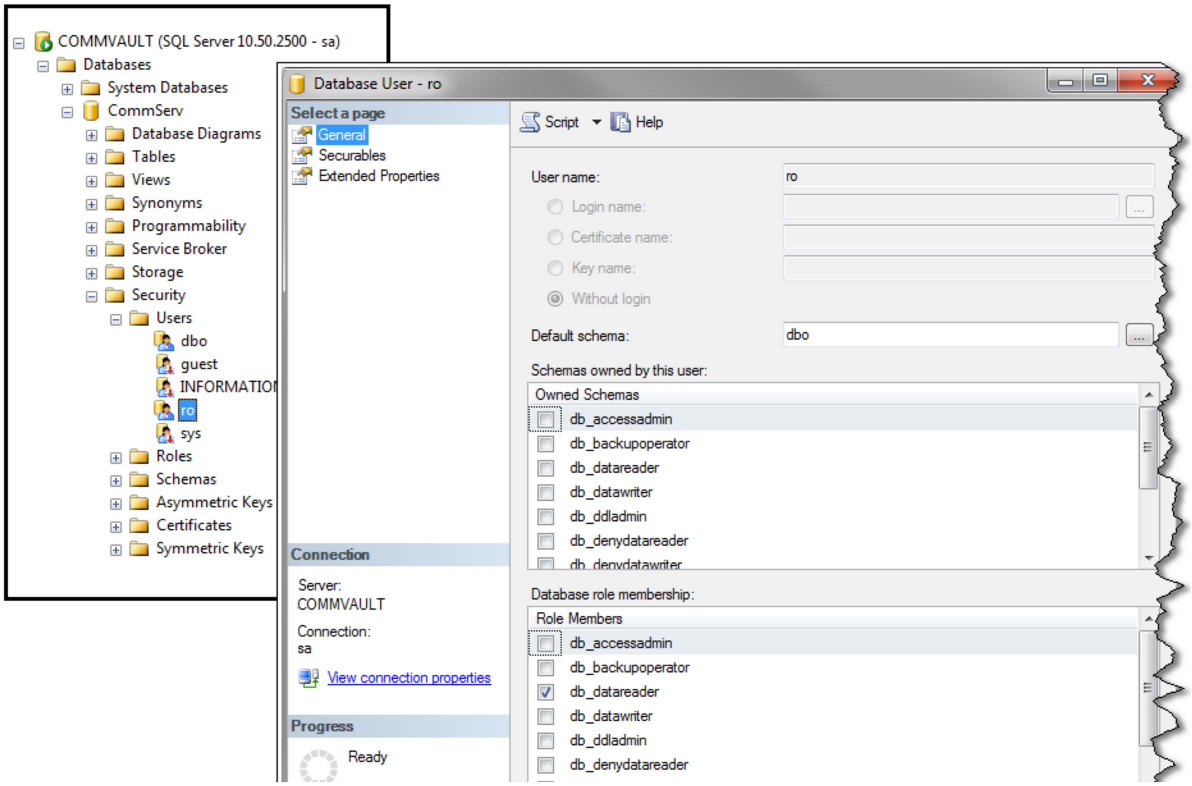
Option 1: Execute SQL commands in the CommServe database

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

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

Option 2: Use MSSQL Management Studio

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



User name: ro

○ Login name:

○ Certificate name:

○ Key name:

● Without login

Default schema: dbo

Schemas owned by this user:

Owned Schemas
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter

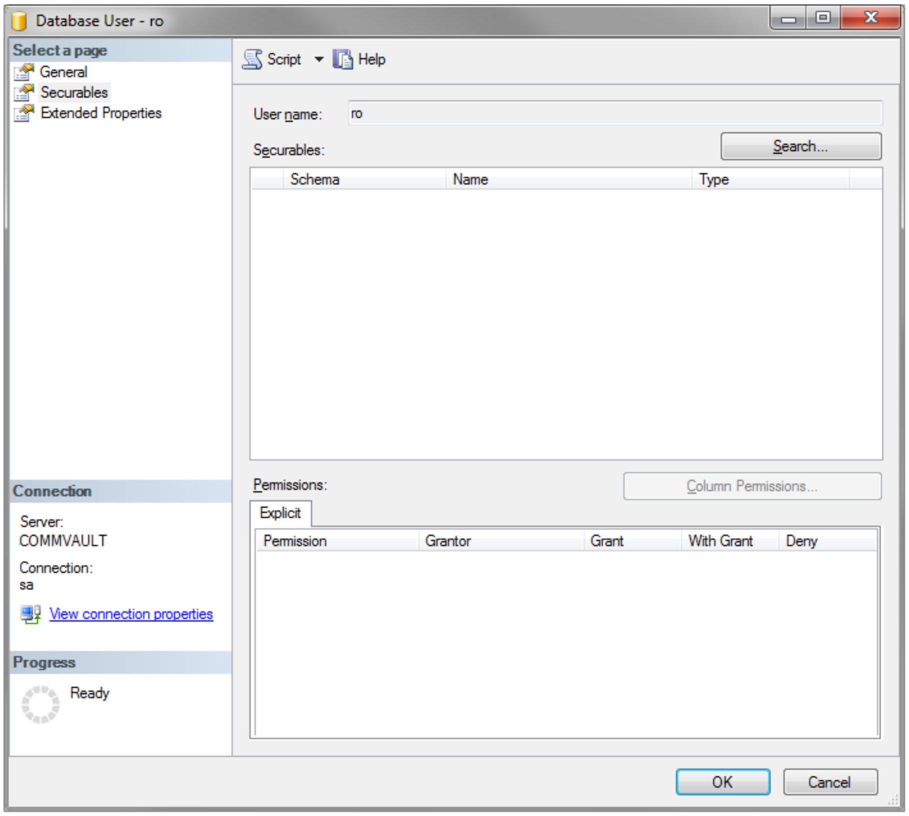
Database role membership:

Role Members
□ db_accessadmin
□ db_backupoperator
☑ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader

Server:
COMMVAULT

Connection:
sa

3. Select the **Securables** page.



User name: ro

Securables:

Schema	Name	Type

Permissions:

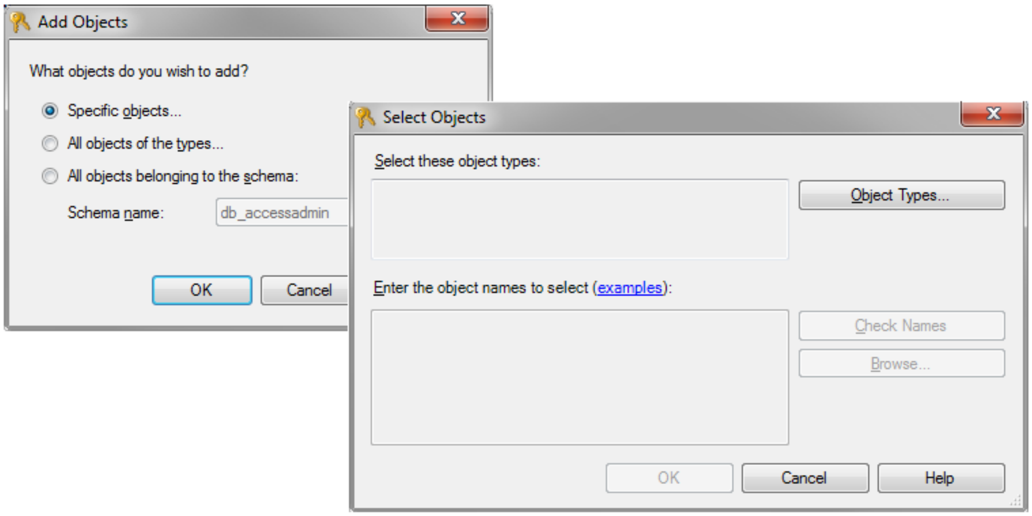
Permission	Grantor	Grant	With Grant	Deny

Server:
COMMVAULT

Connection:
sa

4. Click Search.

5. Add specific objects.



What objects do you wish to add?

● Specific objects...

○ All objects of the types...

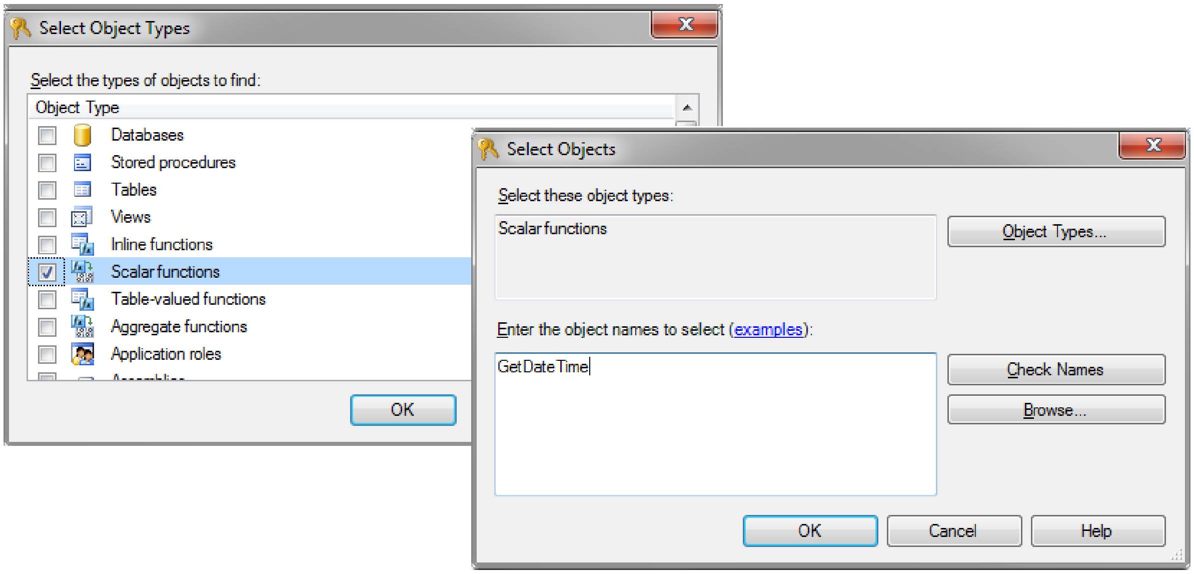
○ All objects belonging to the schema:

Schema name: db_accessadmin

Select these object types:

Enter the object names to select (examples):

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



Select the types of objects to find:

Object Type

□ Databases

□ Stored procedures

□ Tables

□ Views

□ Inline functions

☑ Scalar functions

□ Table-valued functions

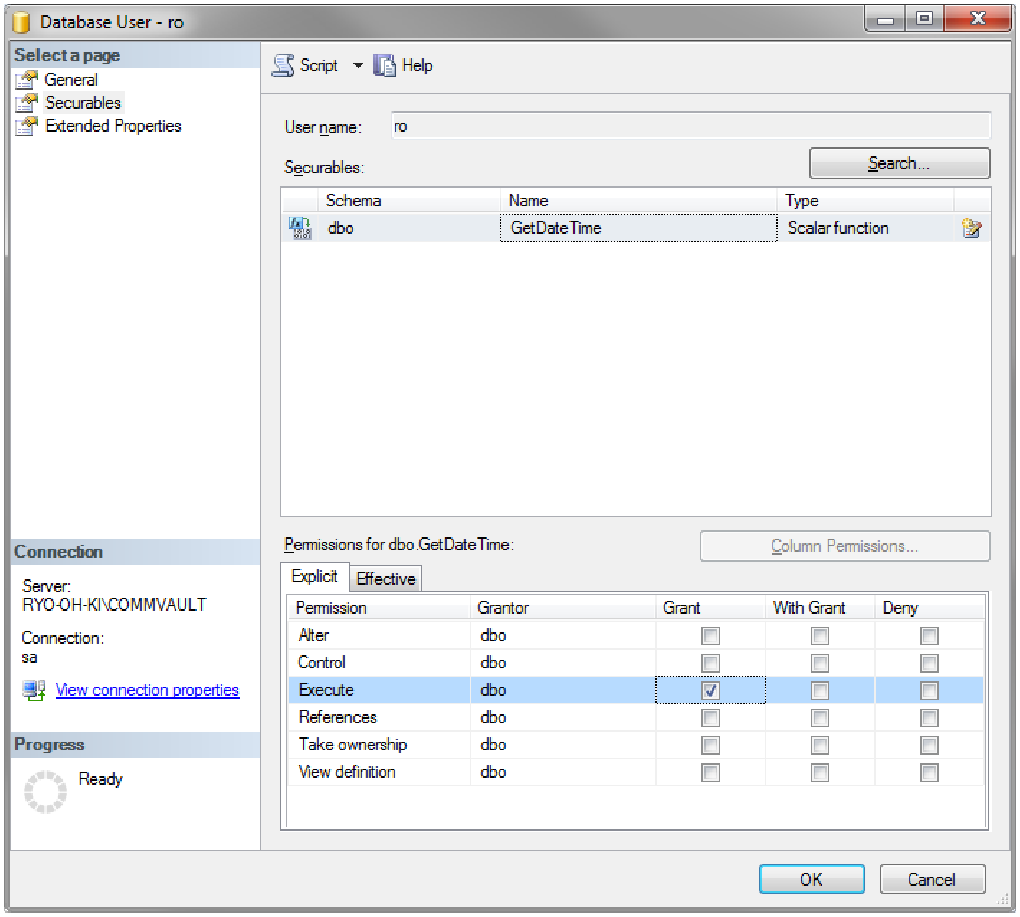
□ Aggregate functions

□ Application roles

Select these object types: Scalar functions

Enter the object names to select (examples): GetDateTime

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



User name: ro

Securables:

Schema	Name	Type
dbo	GetDateTime	Scalar function

Permissions for dbo.GetDateTime:

Permission	Grantor	Grant	With Grant	Deny
Alter	dbo	□	□	□
Control	dbo	□	□	□
Execute	dbo	☑	□	□
References	dbo	□	□	□
Take ownership	dbo	□	□	□
View definition	dbo	□	□	□

Server:
RYO-OH-KI\COMMVAULT

Connection:
sa

8. Grant execute permissions for GetDateTime by clicking **Execute**. Click **OK**.

9. Repeat steps 4-8 for each function:
   - GetUnixTime
   - GetJobFailureReason
   - JMGetLocalizedMessageFunc

10. Verify Connectivity with the Read-Only User ID

Verify Connectivity with the Read-Only User ID

Using SQL Server Management Studio, verify that you can connect and log in to the CommServe SQL database instance using this newly create User ID.

Load Historical Data Prior to Initial Data Collection

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

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

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

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

2. Login to SQL Plus.

   ```
   sqlplus portal/portal
   ```

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

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

4. Exit SQL Plus.

   ```
   SQL> exit
   ```

Add Commvault Simpana Servers

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

1. In the Inventory, add a host for each CommServe server. See Managing Hosts and Backup Servers.
   - **Host Name** - Displayed in the Portal.
   - **Internal Host Name** - Must match the host name of the CommServe Server.
   - **IP Address** - IP address of the Commserve Server.
   - **Type** - Commvault Server.

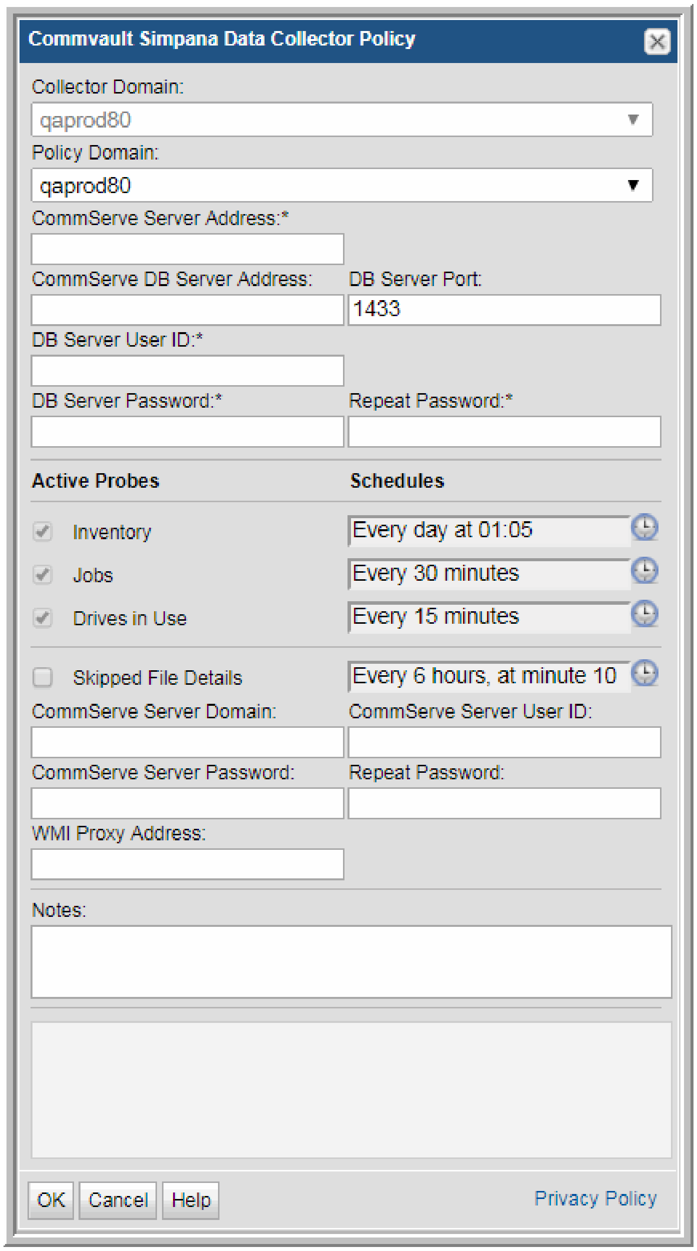
Adding a Commvault Simpana Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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 and see Working with On-Demand Data Collection for details about **Run**.

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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



Commvault Simpana Data Collector Policy

Collector Domain: qaprod80

Policy Domain: qaprod80

CommServe Server Address:*

CommServe DB Server Address:

DB Server Port: 1433

DB Server User ID:*

DB Server Password:*

Repeat Password:*

Active Probes	Schedules
☑ Inventory	Every day at 01:05
☑ Jobs	Every 30 minutes
☑ Drives in Use	Every 15 minutes
☐ Skipped File Details	Every 6 hours, at minute 10

CommServe Server Domain:

CommServe Server User ID:

CommServe Server Password:

Repeat Password:

WMI Proxy Address:

Notes:

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

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name select **My Profile** in the User Account menu.	`yourdomain`
CommServe Server Address	Specify the IP address or host name of the CommServe server. This field is required.	
CommServe DB Server Address	Specify the IP address or host name of the CommServe database system. This field may be empty. The CommServe database hostname defaults to the CommServe server if the field is empty.	`192.168.0.1-250, 192.168.1.10, myhost`
DB Server Port	Specify the port used by the CommServe database. The default is 1433. This port is not enabled by default on the SQL server. Once this port is configured on the SQL server, the server must be restarted before data collection can occur.	
DB Server User ID*	Specify the read-only user ID (with a *non-expiring password)* for the CommServe database. This is a SQL authentication login with at least the following roles and permissions in the CommServe database: db_datareader - EXECUTE dbo.GetDateTime - EXECUTE dbo.GetUnixTime - EXECUTE dbo.GetJobFailureReason - EXECUTE dbo.JMGetLocalizedMessageFunc This field is required.	
DB Server Password*	The non-expiring password associated with the User ID. This field is required.	
Repeat Password	The password associated with the User ID.	
Active Probes		

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

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

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

4

Pre-Installation Setup for EMC Avamar

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

- Architecture Overview (EMC Avamar)
- Prerequisites for Adding Data Collectors (EMC Avamar)
- Adding an EMC Avamar Data Collector Policy

Architecture Overview (EMC Avamar)

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

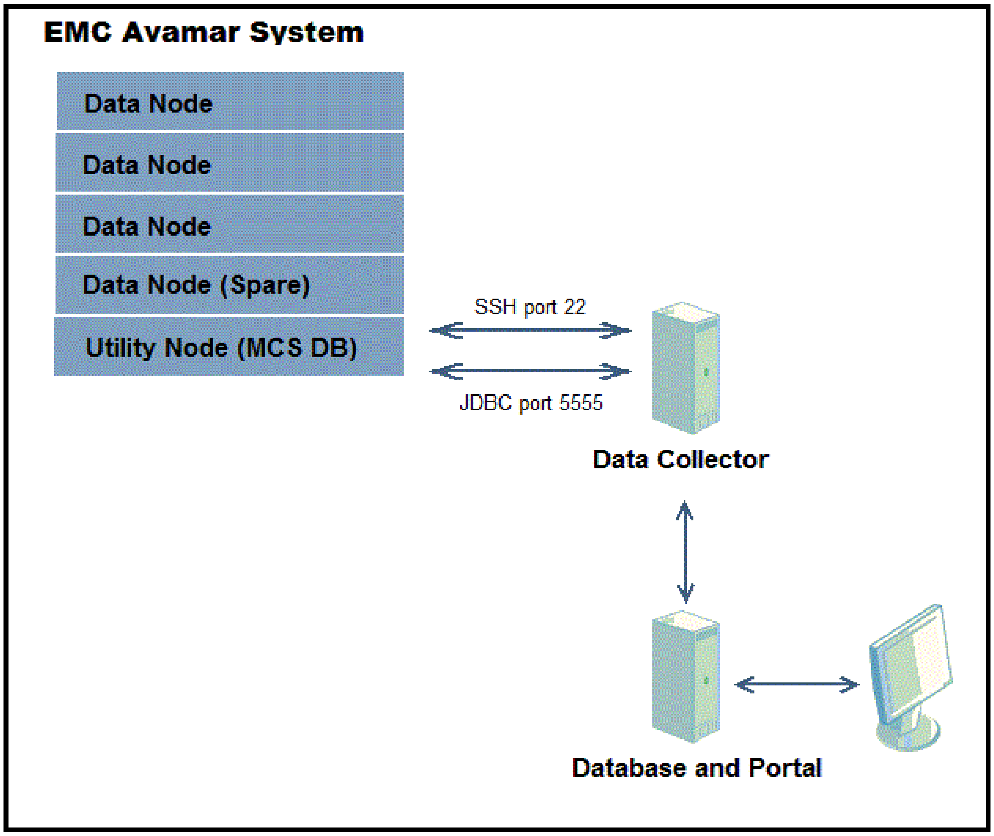


Figure 1 Data Collector in an EMC Avamar Environment

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

Prerequisites for Adding Data Collectors (EMC Avamar)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the 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.
- TCP ports 5555 and 22.
- An Avamar Utility Node server must be configured in the Data Collector Policy. The login credentials must have **admin** or **dpn** access to the Avamar utility node so that the Data Collector can invoke command-line programs in the /usr/local/avamar/bin directory.
- One Data Collector can be used to include *all* of these backup products: Commvault Simpana, EMC Avamar, EMC NetWorker, EMC Data Domain, Veritas Backup Exec, Veritas NetBackup, HP Data Protector, and Generic Backup products. And, you also can include other enterprise objects, such as storage arrays, in this Data Collector.
- The Data Collector uses JDBC as a read-only user to collect point-in-time data from the Avamar Management Console Server (MCS) database. In addition, command-line-interface (CLI) commands access the utility node for Avamar server status details.

Installation Overview (EMC Avamar)

1. Updating the Local Hosts File for Data Collection
2. Add EMC Avamar Servers
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. In the Portal, add the EMC Avamar data collector policy. Adding an EMC Avamar Data Collector Policy
5. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
6. Validate the Data Collector Installation. See Validating Data Collection.

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

Add EMC Avamar Servers

Add Avamar servers to APTARE IT Analytics using the Inventory or add an Avamar server directly from the data collector policy window. See Managing Hosts and Backup Servers.

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

Note: You can also add EMC Avamar servers directly from the Data Collector policy screen. See Adding/ Configuring an Avamar Server within the Data Collector Policy Window

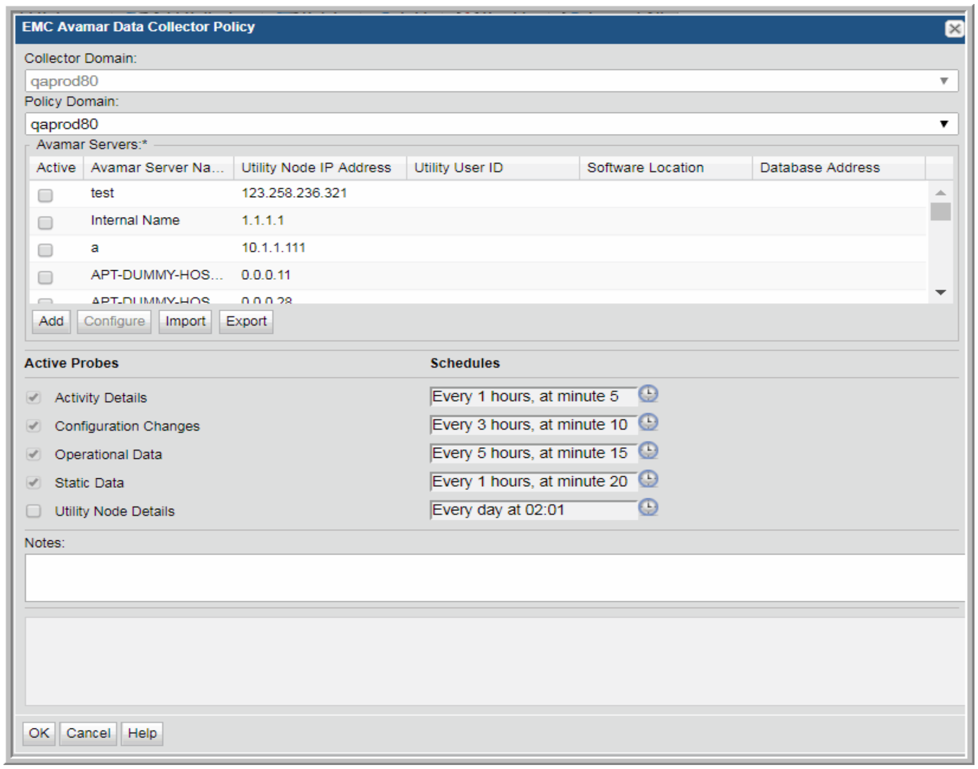
Adding an EMC Avamar Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



EMC Avamar Data Collector Policy

Collector Domain: qaprod80

Policy Domain: qaprod80

Avamar Servers:*

Active	Avamar Server Na...	Utility Node IP Address	Utility User ID	Software Location	Database Address
☐	test	123.258.236.321			
☐	Internal Name	1.1.1.1			
☐	a	10.1.1.111			
☐	APT-DUMMY-HOS...	0.0.0.11			
☐	APT-DUMMY-HOS	0.0.0.28			

Active Probes	Schedules
☑ Activity Details	Every 1 hours, at minute 5
☑ Configuration Changes	Every 3 hours, at minute 10
☑ Operational Data	Every 5 hours, at minute 15
☑ Static Data	Every 1 hours, at minute 20
☐ Utility Node Details	Every day at 02:01

Notes:

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

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

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

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

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

Testing the Collection

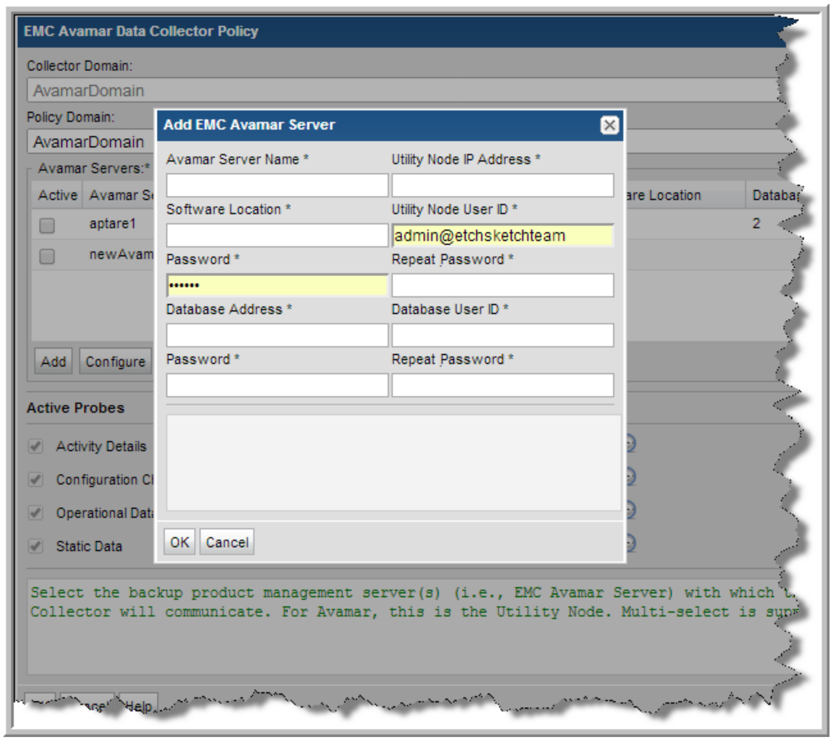
You can test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity. See Working with On-Demand Data Collection for details.

Adding/Configuring an Avamar Server within the Data Collector Policy Window

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

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

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



Collector Domain: AvamarDomain

Policy Domain: AvamarDomain

Utility Node User ID *: admin@etchsketchteam

Password *: ••••••

Select the backup product management server(s) (i.e., EMC Avamar Server) with which t Collector will communicate. For Avamar, this is the Utility Node. Multi-select is sup

2. Enter the values:

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

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

Importing EMC Avamar Server Information

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

CSV Format Specifications

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

1. **Avamar Server Name** - maximum 128 characters. Null is not accepted
2. **Utility Node IP Address** - maximum 40 characters. Null is not accepted
3. **Utility Node User ID** - maximum 64 characters. Null is not accepted
4. **Utility Node Password** - maximum 256 characters. Null is not accepted
5. **Software Location** - maximum 256 characters. If this field is blank, the following default is used: /usr/local/avamar.
6. **Database Address** - maximum 128 characters. If the Avamar database is resident on the Utility Node, this should contain the Utility Node's IP Address.
7. **Database User ID** - maximum 64 characters. If this field is blank, the following default is used: viewuser.
8. **Database Password** - maximum 64 characters. If this field is blank, the following default is used: viewuser1.

Import Notes

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

To Import EMC Avamar Servers

1. Prepare the CSV according to CSV Format Specifications.
2. Select **Admin > Data Collection > Collector Administration**.
3. Click **Add Policy**.
4. Select **EMC Avamar**. The **EMC Avamar Data Collector Policy** screen is displayed.
5. Click **Import**. The **Import EMC Avamar Servers** window is displayed. You can browse for the CSV file you created.

Exporting EMC Avamar Server Information

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

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

3

Pre-Installation Setup for Cohesity DataProtect

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

- Prerequisites for Adding Data Collectors (Cohesity DataProtect)
- Installation Overview (Cohesity DataProtect)
- Add a Cohesity DataProtect Data Collector Policy

Prerequisites for Adding Data Collectors (Cohesity DataProtect)

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

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- User must be assigned the Cohesity *Operator* role

Installation Overview (Cohesity DataProtect)

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

1. Update the Local Hosts file. This enables Portal access. See Updating the Local Hosts File for Data Collection.
2. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
3. In the Portal, add the Cohesity DataProtect data collector policy. See Add a Cohesity DataProtect Data Collector Policy
4. On the Data Collector Server, install the Data Collector software. See Data Collector Installation.
5. Validate the Data Collector Installation. See Validating Data Collection.

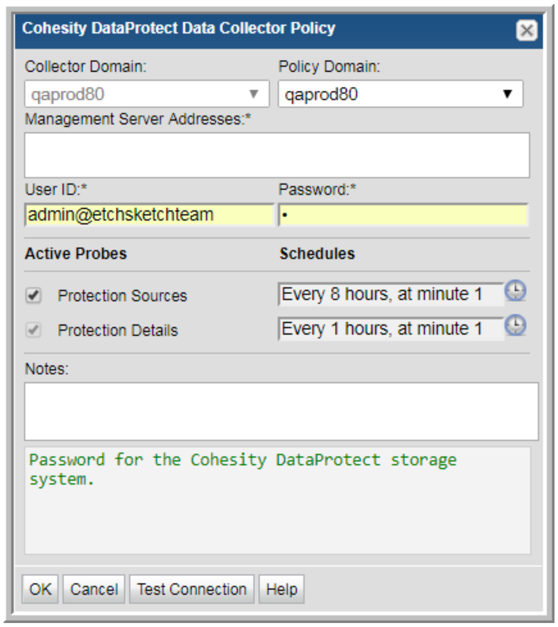
Add a Cohesity DataProtect Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



Cohesity DataProtect Data Collector Policy

Collector Domain: qaprod80

Policy Domain: qaprod80

Management Server Addresses:*

User ID:* admin@etchsketchteam

Password:* •

Active Probes	Schedules
☑ Protection Sources	Every 8 hours, at minute 1
☑ Protection Details	Every 1 hours, at minute 1

Notes:

Password for the Cohesity DataProtect storage system.

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

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

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more DataProtect Management server IP addresses or host names to probe. Comma-separated addresses or IP ranges are supported, e.g. 192.168.0.1-250, 192.168.1.10, myhost **Note:** To collect from a Cluster, enter the IP address of only one of the management servers. To collect from multiple nodes, use the master node IP.
User ID*	This field is required. View-only User ID and password for the Cohesity DataProtect storage system.
Password*	This field is required. Password for the Cohesity DataProtect storage system.
Active Probes	
Protection Sources	Probe for Cohesity DataProtect Protection Sources.
Protection Details	Probe captures data about Protection Jobs, including their policies, schedules, sessions, and backups.
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

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

5

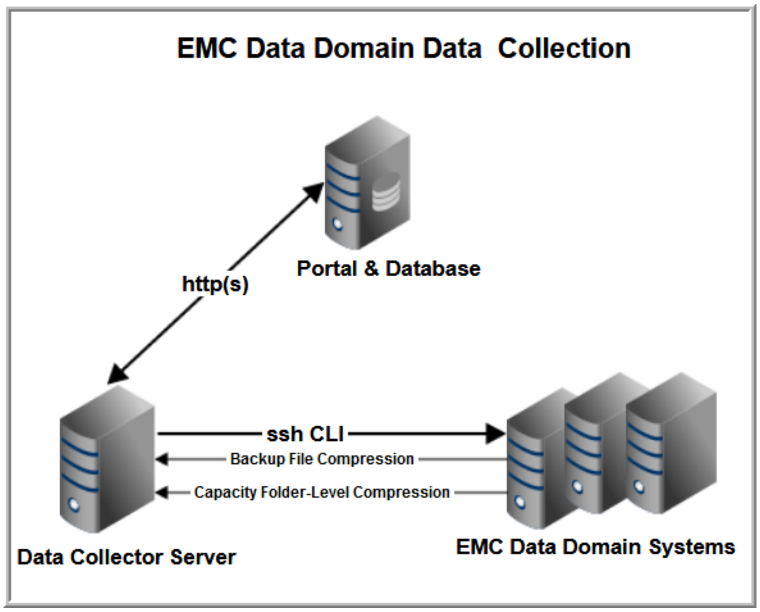
Pre-Installation Setup for EMC Data Domain Backup

It is important to understand where the Data Collector software must be installed so that you can determine how many Data Collectors must be installed and which servers are best suited for the deployment.

- Architecture Overview (EMC Data Domain Backup)
- Prerequisites for Adding Data Collectors (EMC Data Domain Backup)
- Installation Overview (EMC Data Domain Backup)
- Adding an EMC Data Domain Backup Data Collector Policy

Architecture Overview (EMC Data Domain Backup)

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



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

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

- Native storage device for backup systems
- Virtual tape library (VTL) for backup systems

- NFS mount or CIFS share folders for file storage

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

Prerequisites for Adding Data Collectors (EMC Data Domain Backup)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the 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.**
- If collecting File-Level Compression metrics, Veritas NetBackup collection must be enabled.
- Aggregated global and local compression rates for all Veritas NetBackup backup images can be collected for all *active* Data Domain Server MTrees connected (via DDBOOST) to NetBackup Master Servers. These Master Servers must have an active Data Collector that has successfully completed an initial data collection. Initiate compression rate collection by selecting File-Level Compression in the Data Domain Data Collector Policy.

Installation Overview (EMC Data Domain Backup)

1. Updating the Local Hosts File for Data Collection.
2. Add EMC Data Domain Servers.
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. In the Portal, add the EMC Data Domain data collector policy. Adding an EMC Data Domain Backup Data Collector Policy.
5. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
6. Validate the Data Collector Installation. See Validating Data Collection.

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

Add EMC Data Domain Servers

Add or edit EMC Data Domain servers to APTARE IT Analytics directly from the data collector policy window or through the Inventory. See Managing Hosts and Backup Servers.

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

1. Add a host for each Data Domain server.
    - **External Host Name** - Displayed in the Portal.
    - **Internal Host Name** - Must match the host name of the Data Domain server; fully qualified domain name (FQDN).
    - **Backup Type** - Data Domain Server
2. If collecting File-Level Compression data, see Adding an EMC Data Domain Backup Data Collector Policy.

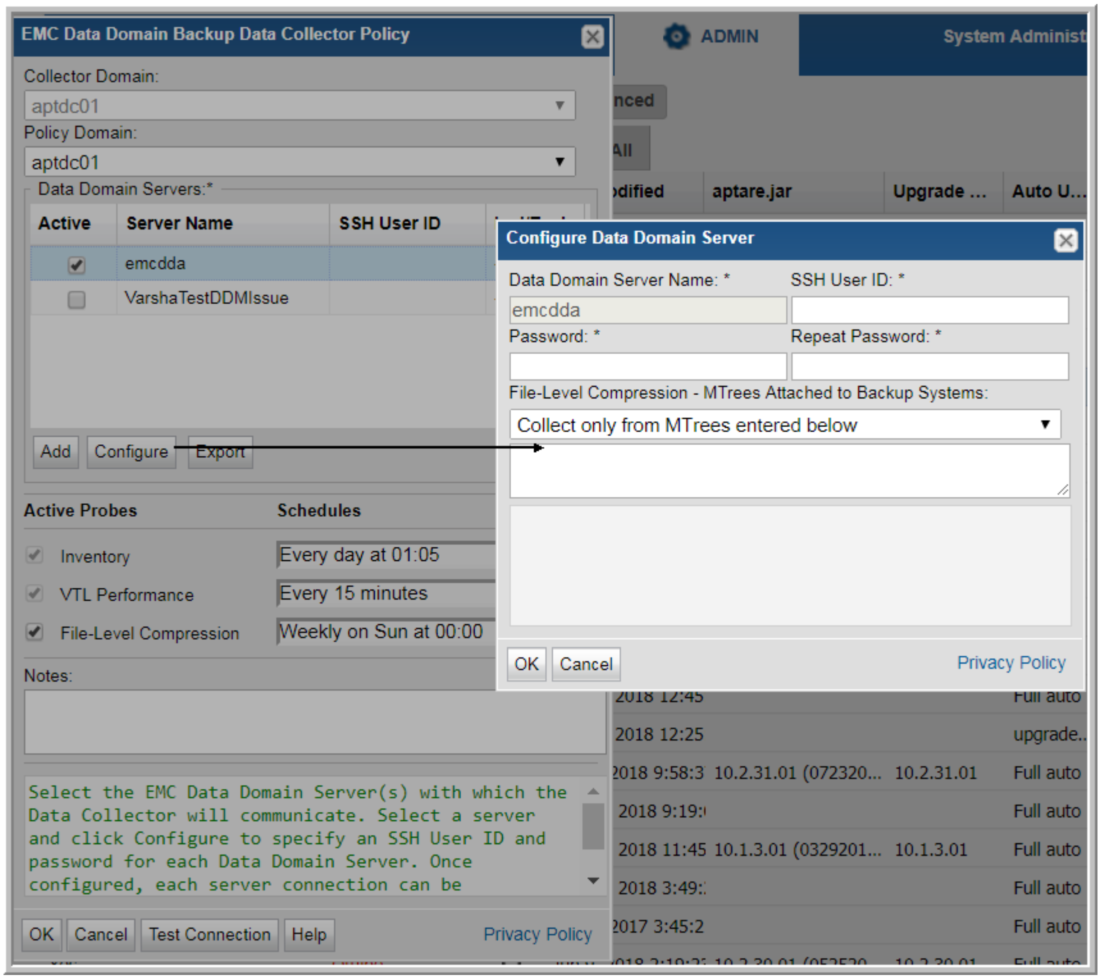
Adding an EMC Data Domain Backup Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.
5. Optionally, add an EMC Data Domain server from the policy screen. This action can also be completed in the Inventory. See Adding/Configuring an EMC Data Domain Server within the Data Collector Policy Window.
6. When selecting the File-Level Compression probe, additional configuration is required, as follows:
   a. Select a Data Domain Server.
   b. Select the File-Level Compression probe.
   c. Click **Configure**. See also, File-Level Compression Probe and Adding an EMC Data Domain Backup Data Collector Policy.



EMC Data Domain Backup Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Data Domain Servers:*

Active	Server Name	SSH User ID
☑	emcdda	
□	VarshaTestDDMIssue	

Active Probes	Schedules
☑ Inventory	Every day at 01:05
☑ VTL Performance	Every 15 minutes
☑ File-Level Compression	Weekly on Sun at 00:00

Notes:

Select the EMC Data Domain Server(s) with which the Data Collector will communicate. Select a server and click Configure to specify an SSH User ID and password for each Data Domain Server. Once configured, each server connection can be

Configure Data Domain Server

Data Domain Server Name: * emcdda

SSH User ID: *

Password: *

Repeat Password: *

File-Level Compression - MTrees Attached to Backup Systems: Collect only from MTrees entered below

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

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

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

Field	Description	Sample Value
VTL Performance	Data associated with the performance of the Data Domain system virtual tape libraries (VTL) is collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available.	

Field	Description	Sample Value
File-Level Compression Probe	When this probe is selected, MTrees can be entered into the File-Level Compression list configured for a Data Domain Server. The Data Domain Servers will then display an Include/Exclude column, with negative numbers indicating MTrees are excluded and positive numbers indicating MTrees are included. Hover your mouse over the Incl/Excl column to view the MTrees.If the column displays +0, it indicates no Mtrees have been included in the collection, and -0 indicates no Mtrees have been excluded, so all Mtrees will be collected from. Enter one or more MTree names to be included in collection or to be excluded from collection, depending on the selected option. When compression information is collected from the MTree, an attempt is made to connect the file with a backup job that has previously been collected. A 'hint' must be specified to allow this to occur. Currently Oracle RMAN and Veritas NetBackup are supported. To specify an MTree to which RMAN is sending backup files to, enter: RMAN:[MTree Name]. For NetBackup, enter: NBU:[MTree Name]. Example of a comma-separated MTree list: RMAN:/data/col1/rman_su1, NBU:/data/col1/nbu_ddm1 If you do not specify a hint, it is assumed that the Data Domain MTree contains files created by Veritas NetBackup. To run File-Level compression across all Mtrees on a Data Domain system, with a 'hint' to specify that the database attempt to link files with Backup jobs, enter: RMAN:* or NBU:* depending on the Backup system using the MTree. Mixed use of wildcards is not supported. See Adding an EMC Data Domain Backup Data Collector Policy. Aggregated global and local compression rates for all NetBackup backup images are collected for all MTrees that are connected to the Active Data Domain servers via DDBOOST and where the NetBackup Data Collector is active and has successfully completed an initial data collection. Warning: Choosing to exclude collection with an empty MTree list may cause collection to take several hours to complete.	

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

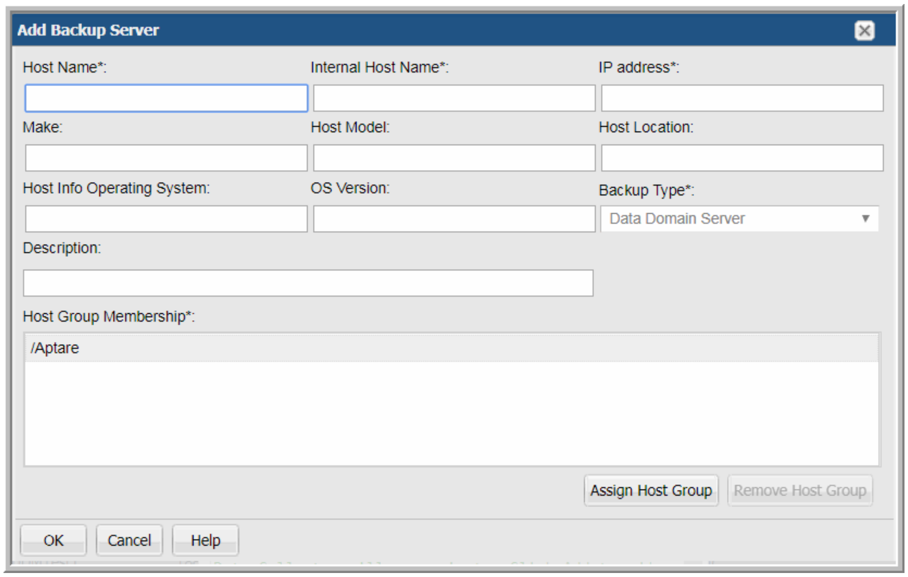
Adding/Configuring an EMC Data Domain Server within the Data Collector Policy Window

Add and edit Data Domain servers directly from the data collector policy. This functionality is also available in the **Inventory**. See Adding and Editing Hosts and Backup Servers for details.

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

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

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



Backup Type*: Data Domain Server

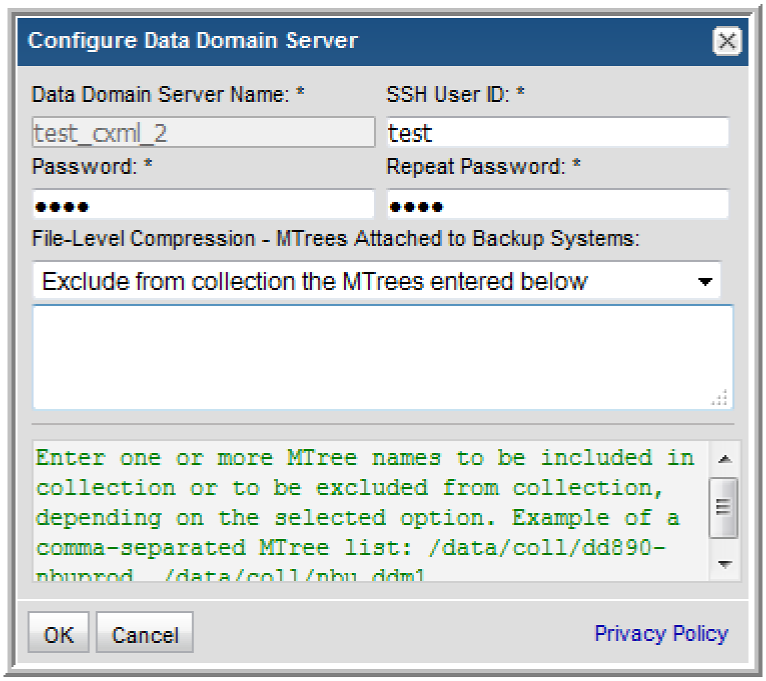
Host Group Membership*: /Aptare

3. Enter or update values. Required fields are denoted by *. See Adding and Editing Hosts and Backup Servers for details.
4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups. See Managing Host Groups for details.

Configure a Data Domain Server for File-Level Compression Collection

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

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



Data Domain Server Name: * test_cxml_2

SSH User ID: * test

Password: * ●●●●

Repeat Password: * ●●●●

File-Level Compression - MTrees Attached to Backup Systems:

Exclude from collection the MTrees entered below

```
Enter one or more MTree names to be included in
collection or to be excluded from collection,
depending on the selected option. Example of a
comma-separated MTree list: /data/coll/dd890-
nbuprod, /data/coll/nbu_ddm1
```

5. 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 be configured with a **Backup Type** of **Data Domain Server**. See Add EMC Data Domain Servers.	`DDM-HQ`
SSH User ID*	The command-line interface (CLI) via SSH is used to gather Data Domain system data. This requires a view-only Data Domain User ID that must be a member of the Data Domain system Admin group. This User ID must be the same for all addresses listed in the System Addresses entry field for the Data Domain systems.	`Administrator`
Password	The password associated with the User ID.	`Pwd1`
Repeat Password	The password associated with the User ID.	`Pwd1`

Field	Description	Sample Value
File-Level Compression - MTrees Attached to Backup Systems	This selection is relevant only when the File-Level Compression probe is selected in the EMC Data Domain Backup Policy. Select the option to either include or exclude collection from the MTrees entered in the list. If the *exclude* option is selected with an empty MTree list, data from all MTrees will be collected. If the *include* option is selected with an empty MTree list, no file-level compression data will be collected. **Warning**: Choosing to exclude file-level collection with an empty MTree list may cause collection to take several hours to complete.	
Exclude from collection the MTrees entered below OR Collect only from MTrees entered below	Enter one or more MTree names to be included in collection or to be excluded from collection, depending on the selected option. Example of a comma-separated MTree list: /data/coll/dd890-nbuprod, /data/coll/nbu_ddm1	`/data/coll/dd890-nbuprod, /data/coll/nbu_ddm1`

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.

6

Pre-Installation Setup for EMC NetWorker

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

- Architecture Overview (EMC NetWorker)
- Prerequisites for Adding Data Collectors (EMC NetWorker)
- Installation Overview (EMC NetWorker)
- Adding an EMC NetWorker Data Collector Policy
- Configure a Notification Action in EMC NetWorker

Architecture Overview (EMC NetWorker)

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

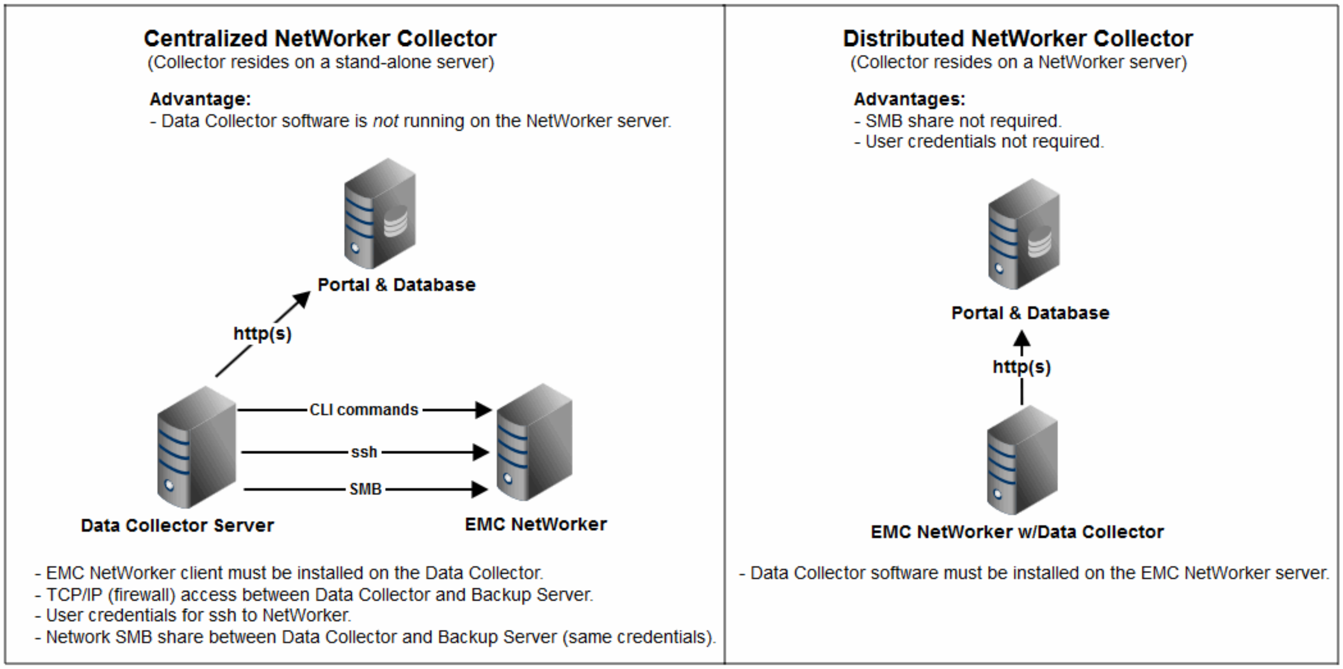

Centralized NetWorker Collector
(Collector resides on a stand-alone server)
Advantage:
- Data Collector software is *not* running on the NetWorker server.
Portal & Database
http(s)
CLI commands
ssh
SMB
Data Collector Server
EMC NetWorker
- EMC NetWorker client must be installed on the Data Collector.
- TCP/IP (firewall) access between Data Collector and Backup Server.
- User credentials for ssh to NetWorker.
- Network SMB share between Data Collector and Backup Server (same credentials).
Distributed NetWorker Collector
(Collector resides on a NetWorker server)
Advantages:
- SMB share not required.
- User credentials not required.
Portal & Database
http(s)
EMC NetWorker w/Data Collector
- Data Collector software must be installed on the EMC NetWorker server.

Figure 2 Data Collector in an EMC NetWorker Environment

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

The Data Collector will use command line utilities such as *mminfo*, *nsradmin*, and *nsrinfo* to obtain its information from each Networker Server. The Data Collector also will use ssh to connect to remote Networker servers to retrieve log file details. The information is stored in the Portal database, enabling a global view of all of the backup servers and clients.

EMC NetWorker Terminology

Networker Server - The Networker Server is the physical system that is running the EMC NetWorker server software. This system will be known by its host name or IP address.

Prerequisites for Adding Data Collectors (EMC NetWorker)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the 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.
- The ports used by the NetWorker Data Collector are: **NSRADMIN TCP 7937-7940, SSH 22** and WMI Proxy range of ports
- If NetWorker is installed on a Windows server, the Data Collector must be on a Windows server.
- Install a Backup Client on the Data Collector server to enable access to NetWorker Administrative Tools.
- For NetWorker 7.5 and 7.6, a writable, network-accessible share must be on the NetWorker server for log file transfers to the Data Collector server.
- Configure a Notification Action in EMC NetWorker.

Installation Overview (EMC NetWorker)

1. Updating the Local Hosts File for Data Collection
2. Add EMC NetWorker Servers
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. In the Portal, add the EMC NetWorker data collector policy. See Adding an EMC NetWorker Data Collector Policy.
5. Configure a Notification Action in EMC NetWorker
6. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
7. Validate the Data Collector Installation. See Validating Data Collection.

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 NetWorker Servers

Add a host for each NetWorker server (Utility Node) to APTARE IT Analytics using the data collector policy screen or through the Inventory. See Managing Hosts and Backup Servers.

- **Host Name** - Displayed in the Portal.
- **Internal Host Name** - Must match the host name of the NetWorker server; fully qualified domain name (FQDN).
- **Backup Type** - NetWorker Server

Adding an EMC NetWorker Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

   During the configuration of this Data Collector, you will provide the details for SSH or SMB access to the NetWorker log files, used to collect restore data, group details, and drive performance data.

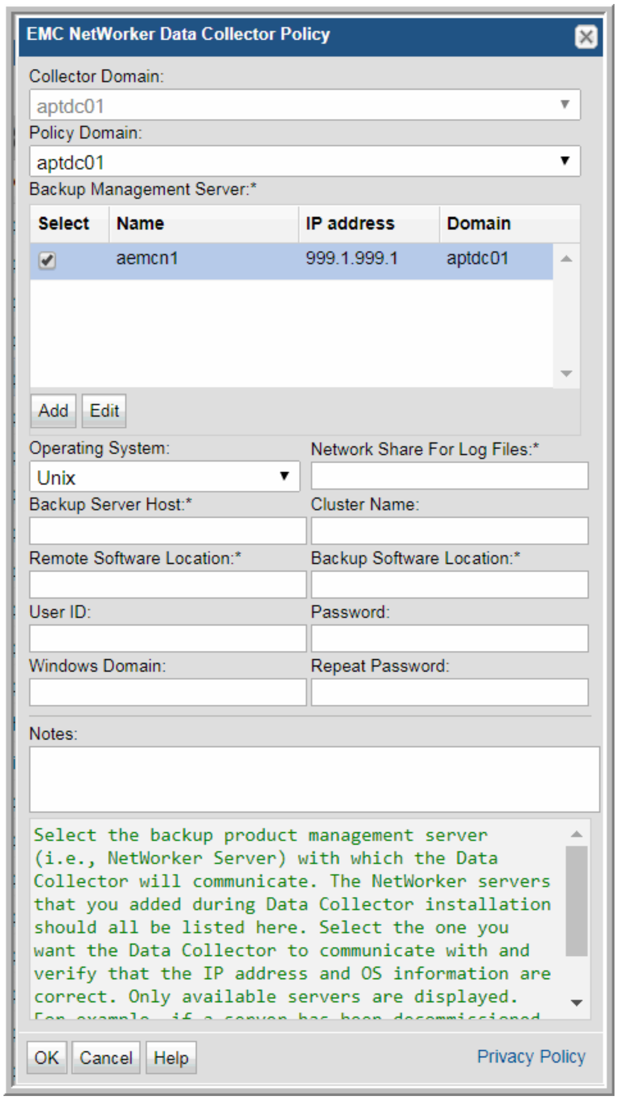
   Specifically, this account needs to have read-only access to have SSH/SMB access to read files in the following directories:

   ```
   <NetWorker install directory>/logs/
   ```

   Also, for NetWorker 7.3 and 7.4:

   ```
   <NetWorker install directory>/res/jobsdb/ssinfo
   ```

5. Optionally add an EMC NetWorker Backup Server from the policy screen. This action can also be completed in the Inventory. See Adding/Editing a EMC NetWorker Server within the Data Collector Policy.



Collector Domain: aptdc01

Policy Domain: aptdc01

Backup Management Server:*

Select	Name	IP address	Domain
☑	aemcn1	999.1.999.1	aptdc01

Operating System: Unix

Network Share For Log Files:*

Backup Server Host:*

Cluster Name:

Remote Software Location:*

Backup Software Location:*

User ID:

Password:

Windows Domain:

Repeat Password:

Notes:

```
Select the backup product management server
(i.e., NetWorker Server) with which the Data
Collector will communicate. The NetWorker servers
that you added during Data Collector installation
should all be listed here. Select the one you
want the Data Collector to communicate with and
verify that the IP address and OS information are
correct. Only available servers are displayed.
For example, if a server has been decommissioned
```

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

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

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

Field	Description	Sample Value
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Backup Management Server*	Select the backup product management server (i.e., NetWorker Server) with which the Data Collector will communicate. The NetWorker servers that you added during Data Collector installation should all be listed here. Select the one you want the Data Collector to communicate with and verify that the IP address and OS information are correct. Only available servers are displayed. For example, if a server has been decommissioned or it has been selected for use by another policy, it will not be displayed.	
Add	Click **Add** to add a NetWorker server. Once added, servers are also displayed in the Inventory. See also Adding/Editing a EMC NetWorker Server within the Data Collector Policy.	
Edit	Select a server and click **Edit** to update the server values.	
Operating System	The operating system on which NetWorker is running.	

Field	Description	Sample Value
Network Share for Log Files*	Starting with NetWorker 7.5, a writable and network accessible share must be created on the NetWorker server to enable the Data Collector to transfer log files from this share to the Data Collector server. The Data Collector needs write permissions to the share to be able to copy files from the Networker directories and save them. It needs read permissions to be able to read from the share across the network via SMB (Server Message Block protocol). The Data Collector needs a network-accessible directory defined somewhere on the NetWorker host into which it can copy the log files before copying them over to the Data Collector host. This setup is needed even when the Data Collector and Networker are on the same machine. --- **Example:** User creates the directory: `C:\Temp` User defines the network share `\\host\Temp` pointed at `C:\Temp` User enters **Temp** in this Data Collector policy field. --- Note that though the example is for Windows, the same situation exists on *nix.	
Backup Server Host*	The Internal name of the Backup Server Host. This is the host name known to the backup product.	server1
Cluster Name	The name of the cluster, if applicable, to which the backup server host belongs.	
Remote Software Location*	The home directory on the NetWorker Server where NetWorker is installed. Typically, C:\Program Files\Legato\nsr for Windows, or /nsr for Linux.	
Backup Software Location*	The home directory of the NetWorker Admin Client software (location of the nsradmin command) **- on the Data Collector Server**. Typically, C:\Program Files\Legato\nsr\ for Windows, or /usr/sbin for Linux.	
Windows Domain	The Windows domain, if applicable.	

Field	Description	Sample Value

User ID	A Linux or Windows user id that provides access to the NetWorker log files in the directory specified in “Remote Software Location” above. Specifically, this account needs to have SSH access (Linux) or SMB access (Windows) to read log files in the following directories:
	`<NetWorker install directory>/logs/`
	Also, for NetWorker 7.3 and 7.4:
	`<NetWorker install directory>/res/`
	Note: The User ID and password are optional if the NetWorker server is installed on the same server as the Data Collector.
		Administrator

Password	The password associated with the User ID.	Pwd1
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.	

8. Click **OK** to save the policy.
9. On the Data Collector server, install/update the Data Collector software.
10. For long-running backups, it may be necessary to configure the MMINFO_MOVE_BACKWARD_MIN Advanced Parameter to ensure that all savesets are collected successfully. See Backup Manager Advanced Parameters.
11. Continue to the next step: Configure a Notification Action in EMC NetWorker.

Adding/Editing a EMC NetWorker Server within the Data Collector Policy

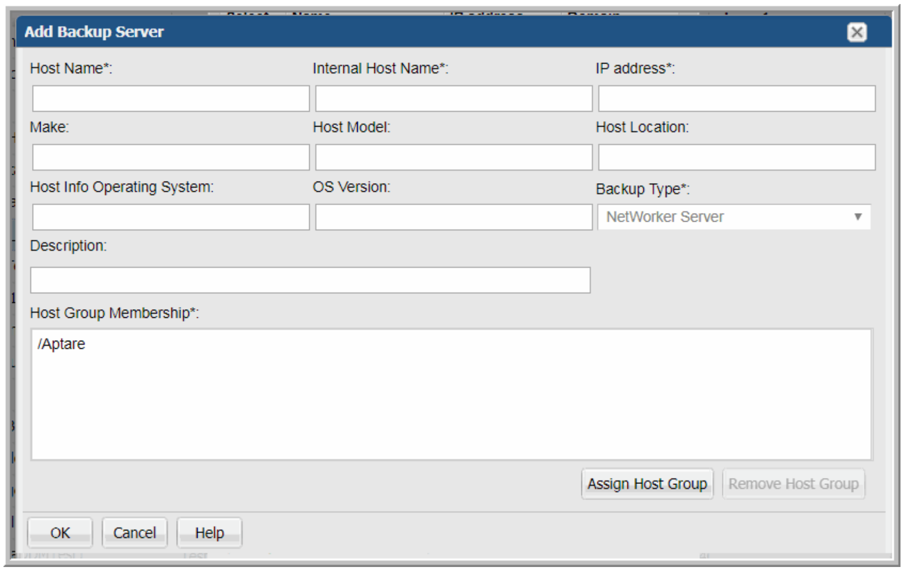
Add and edit EMC NetWorker servers directly from the data collector policy. This functionality is also available in the **Inventory**. See Adding and Editing Hosts and Backup Servers for details.

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

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

1. Click **Add** on the EMC NetWorker Data Collector Policy screen.
   - Select a Backup Management Server and click **Edit**.

2. The **Add Backup Server** screen displays.



Backup Type*: NetWorker Server

Host Group Membership*: /Aptare

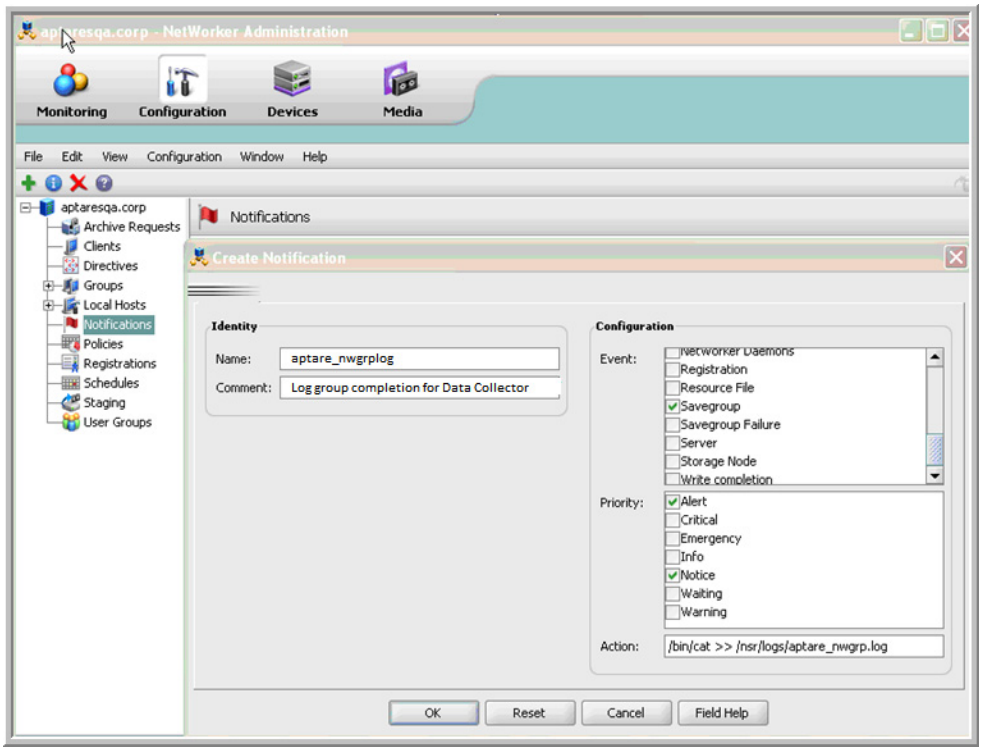
3. Enter or update values. Required fields are denoted by *. See Adding and Editing Hosts and Backup Servers for details.

4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups. See Managing Host Groups for details.

Configure a Notification Action in EMC NetWorker

The Data Collector parses a custom NetWorker message log file to collect information on failed jobs and group instances that have been running. The NetWorker Administrator must set up a Notification Action via the NetWorker Management Console.

Note: A Notification Action must be set up *on each NetWorker Host Server* that you specified in the pre-installation worksheet.



Identity

Name: aptare_nwgrplog

Comment: Log group completion for Data Collector

Configuration

Event:
- □ NetWorker Daemons
- □ Registration
- □ Resource File
- ☑ Savegroup
- □ Savegroup Failure
- □ Server
- □ Storage Node
- □ Write completion

Priority:
- ☑ Alert
- □ Critical
- □ Emergency
- □ Info
- ☑ Notice
- □ Waiting
- □ Warning

Action: /bin/cat >> /nsr/logs/aptare_nwgrp.log

Ensure that the notification has the following checkboxes checked:

- Savegroup
- Alert
- Notice

Select the appropriate text for the Action field, based on the operating system of the EMC NetWorker server:

Linux (shown above):	`/bin/cat>>/nsr/logs/aptare_nwgrp.log`

Windows:	`nsrlog -f "C:\Program Files\Legato\nsr\logs\`
	`aptare_nwgrp.log"`

Note: Adjust the path accordingly if NetWorker has been installed in a directory structure that is different from the above example and be sure to use the exact file name: **aptare_nwgrp.log**.

7

Pre-Installation Setup for Generic Backup

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

- Generic Backup Data Collection
- Prerequisites for Adding Data Collectors (Generic Backup)
- Installation Overview (Generic Backup)
- Adding a Generic Backup Data Collector Policy
- CSV Format Specification
- Manually Loading the CSV File (Generic Backup)

Generic Backup Data Collection

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

Note: In addition to the regularly scheduled data collection, the CSV file also can be imported manually. See Manually Loading the CSV File (Generic Backup).

Considerations

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

Prerequisites for Adding Data Collectors (Generic Backup)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Create a comma-separated file of the backup/restore data—typically, export the data using the backup software utilities. See CSV Format Specification.

Installation Overview (Generic Backup)

1. Updating the Local Hosts File for Data Collection.
2. Add Generic Backup Servers.
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. In the Portal, add the Generic Backup data collector policy. Adding a Generic Backup Data Collector Policy
5. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
6. Validate the Data Collector Installation. See Validating Data Collection.

Add Generic Backup Servers

Add or edit Generic Backup servers to APTARE IT Analytics using the data collector policy screen or through the Inventory. See Managing Hosts and Backup Servers.

Adding a Generic Backup Data Collector Policy

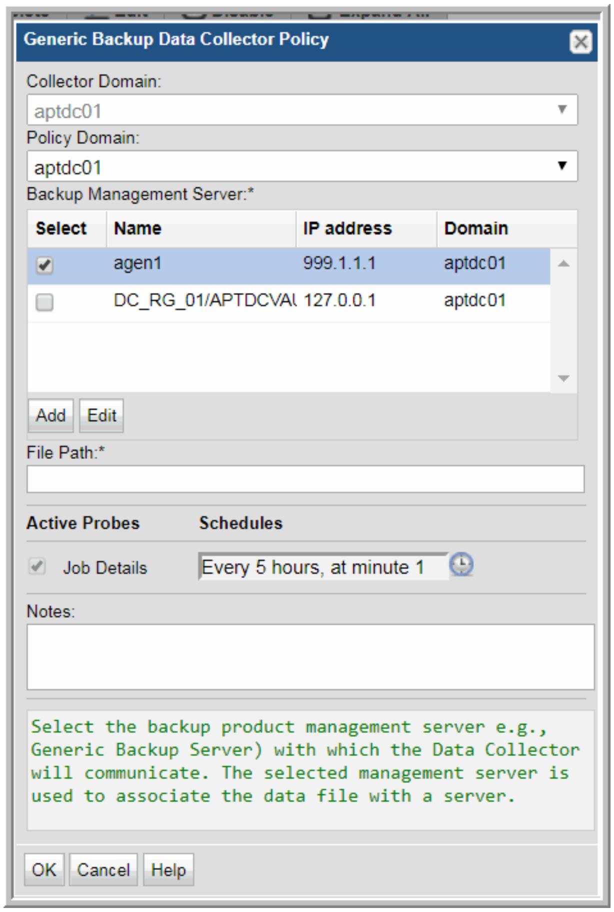
- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE Certified Configurations Guide*.
- **After adding 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

Note: In this instance, select Generic Backup.



Collector Domain: aptdc01

Policy Domain: aptdc01

Backup Management Server:*

Select	Name	IP address	Domain
☑	agen1	999.1.1.1	aptdc01
☐	DC_RG_01/APTDCVAI	127.0.0.1	aptdc01

File Path:*

Active Probes	Schedules
☑ Job Details	Every 5 hours, at minute 1

Notes:

```
Select the backup product management server e.g.,
Generic Backup Server) with which the Data Collector
will communicate. The selected management server is
used to associate the data file with a server.
```

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

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

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

Field	Description	Sample Value
Job Details	Check the box to activate details collection. Click the clock icon to create a schedule frequency. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

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

Adding/Editing a Generic Backup Server within the Data Collector Policy

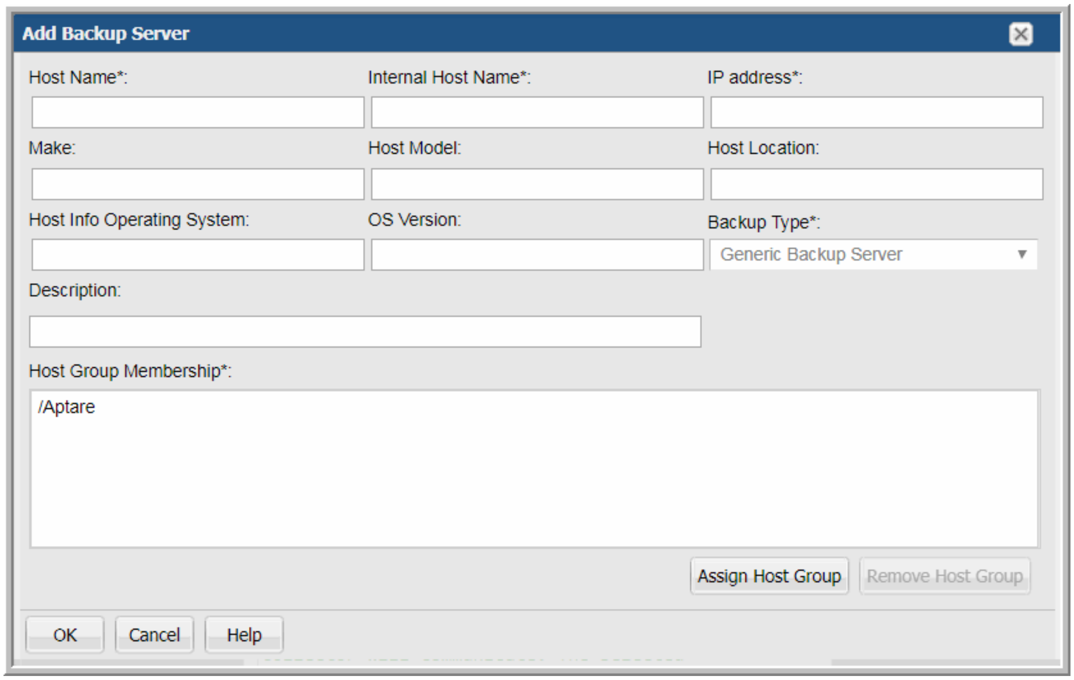
Add and edit Generic Backup servers directly from the data collector policy. This functionality is also available in the **Inventory**. See Adding and Editing Hosts and Backup Servers for details.

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

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

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

2. The **Add Backup Server** screen displays.



Backup Type*: Generic Backup Server

Host Group Membership*: /Aptare

3. Enter or update values. Required fields are denoted by *. See Adding and Editing Hosts and Backup Servers for details.
4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups. See Managing Host Groups for details.

CSV Format Specification

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

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

Name	Type	Value
VendorName	STRING	The name of the backup application used to perform the backup, enclosed in single straight quotes.
ClientName	STRING	The host name of the machine being backed up, enclosed in single straight quotes.
ClientIPAddress	NUMBER	The IP address of the machine being backed up. If an IP address is not available, simply use two single straight quotes ('') or 'null' to indicate a blank/missing value.
VendorJobType	STRING	Valid values include: BACKUP or RESTORE—enclosed in single straight quotes.

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

EXAMPLE: genericBackupJobs.csv

```
'Mainframe Backup','mainframe_name','10.10.10.10','BACKUP','2008-03-24 10:25:00', '2008-
03-24 11:50:00',3713,45221,'D',0,'413824','Retail_s01002030','Incremental','/I:/Shared/
','Daily'

'UNIX tar backup','host_xyz.anyco.com','null','BACKUP','2008-03-24 10:22:00',
'2008-03-24 12:50:00',1713,45221,'T',1,'5201','HQ_Finance','Full','/D:/Backups/','Daily'

'ArcServe','host_123.anyco.com','null','RESTORE','2008-03-24 8:22:00',
'2008-03-24 9:12:00',0,0,'T',0,'2300','Retail_s03442012','Incremental','/I:/Shared/
','EOM'
```

Manually Loading the CSV File (Generic Backup)

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

Pre-requisites:

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

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

   Windows:

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

Linux:

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

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

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

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

   Windows:

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

   Linux:

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

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

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

8

Pre-Installation Setup for HP Data Protector

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

Architecture Overview (HP Data Protector)

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

Cell Manager

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

Disk Agent (Backup Agent)

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

Media Agent

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

Client Systems

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

User Interface (UI)

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

Prerequisites for Adding Data Collectors (HP Data Protector)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 5555, WMI range of ports, Linux ssh 22
- The HP Data Protector (HPDP) client software version must match the specific version (major and minor) of the HPDP server being probed.

Installation Overview (HP Data Protector)

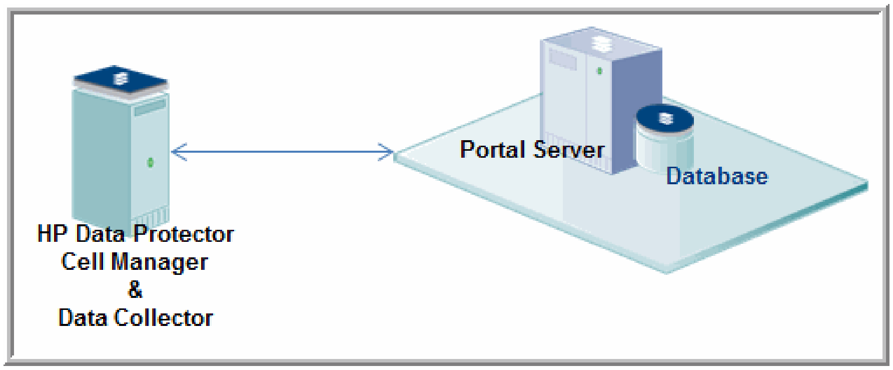
1. Updating the Local Hosts File for Data Collection
2. Identify the specific HP Data Protector elements required for the Data Collector configuration:
   - Identify HP Data Protector Collection Requirements
   - Configure the Data Collector Server in Cell Manager (HP Data Protector)
   - Configure an HP Data Protector Admin User
   - Validate HP Data Protector Setup
3. In the APTARE IT Analytics Portal, configure the HP Data Protector servers that are needed for data collection. See Add HP Cell Manager Servers to APTARE IT Analytics.
4. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
5. Configure an HP Data Protector data collection policy. See Adding/Editing Data Collectors.
6. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
7. Validate the Data Collector Installation. See Validating Data Collection.

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

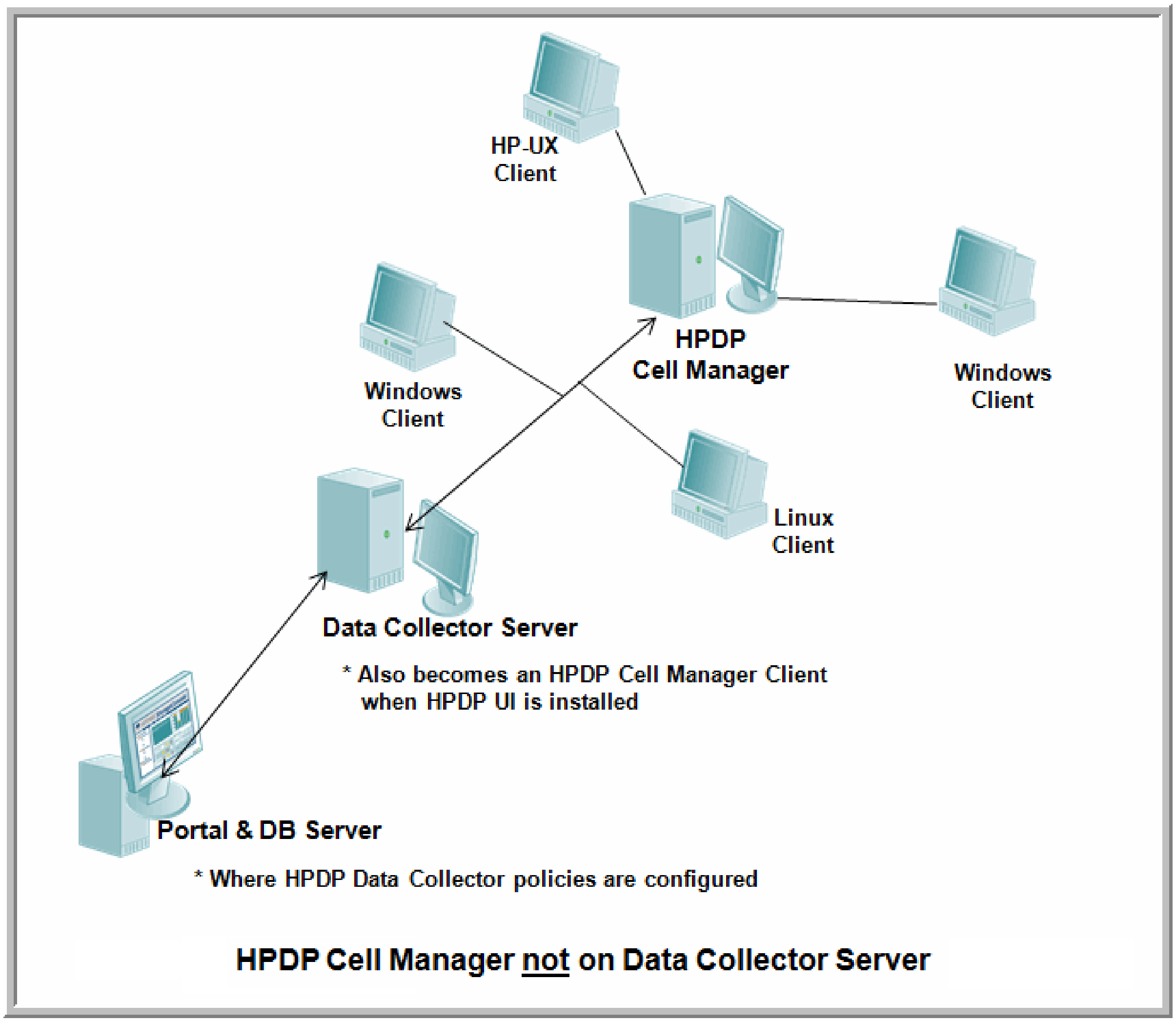
Identify HP Data Protector Collection Requirements

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

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



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


HP-UX Client
HPDP Cell Manager
Windows Client
Windows Client
Linux Client
Data Collector Server
* Also becomes an HPDP Cell Manager Client when HPDP UI is installed
Portal & DB Server
* Where HPDP Data Collector policies are configured
HPDP Cell Manager not on Data Collector Server

Cell Manager Commands for Data Collection

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

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

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

Preparing for Centralized Data Collection on a Remote Cell Manager

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

The following information will be used later when you configure a Data Collection Policy via the APTARE IT Analytics Portal (See Adding/Editing Data Collectors).

On the HP Data Protector Cell Manager Server:

1. Identify the Cell Manager Server's Name: ________________________________
2. Identify the OS of the Cell Manager Server: ________________________________
3. Identify the directory where the Cell Manager is installed. This path will be used later to fill in the *Remote Software Location* field when you configure the Data Collector policy in the APTARE IT Analytics Portal:

   ____

   Typically, this location will be:

   Windows: C:\Program Files\Omniback

   Linux: /opt/omni
4. If the Data Collector is installed on a Linux OS, a WMI Proxy Server must be installed on a Windows system in order to collect data from a Cell Manager that is installed on a Windows system.
5. Configure the Data Collector server to be an HPDP Client. See Configure the Data Collector Server in Cell Manager (HP Data Protector).
6. The `omnidbutil` command is executed on the Cell Manager server to obtain drive status. Therefore, the following configuration is required:

   The user defined in the Data Collector must be an *Admin user* that the Cell Manager Server recognizes—either as a local user account or a Windows domain user account—that has *execute* rights to the `omnidbutil` command. See also Configure an HP Data Protector Admin User and Adding/Editing Data Collectors.

On the APTARE IT Analytics Data Collector Server:

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

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

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

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

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

Requirements for the Data Collector (Windows)

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

Steps to Configure the Data Collector Server in Cell Manager

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

On the HP Data Protector Cell Manager Server:

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

     Start > Programs > HP Data Protector > Data Protector Manager
   - Data Protector Java UI (Windows):

     Start > Programs > HP Data Protector > Data Protector Java GUI Manager

     Then, in the *Connect to Cell Manager* dialog, select or type the name of the Cell Manager and click **Connect**.
   - Data Protector Java UI (Linux):

     `/opt/omni/java/client/bin/javadpgui.sh`
2. Make sure that you have a user that is a **Local System Administrator account from the Data Collector Server**. See Configure an HP Data Protector Admin User.
3. Validate the conditions. See Validate HP Data Protector Setup.

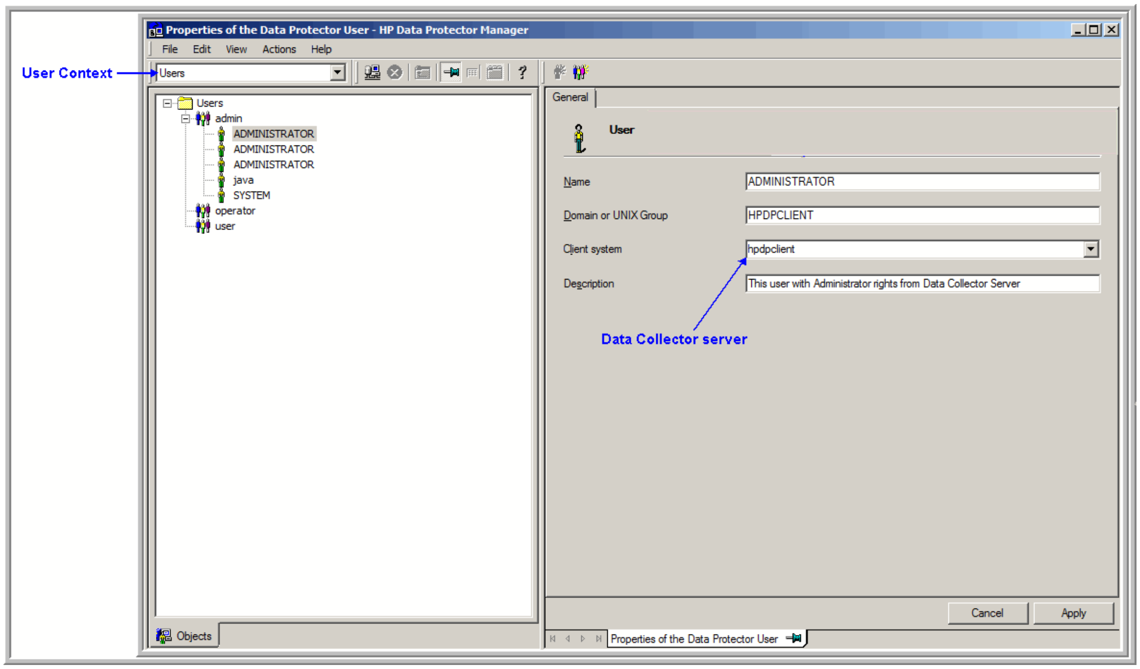
Configure an HP Data Protector Admin User

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

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

On the HP Data Protector Cell Manager Server:

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



Name: ADMINISTRATOR

Domain or UNIX Group: HPDPCLIENT

Client system: hpdpclient

Description: This user with Administrator rights from Data Collector Server

Validate HP Data Protector Setup

On the Data Collector Server:

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

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

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

Add HP Cell Manager Servers to APTARE IT Analytics

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

1. Open a browser window and point it to your instance of the Portal
   (for example: http://aptareportal.*yourdomain.com*).
2. Login as an admin user (e.g. admin@*yourdomain.com*).
3. Add a Backup Server. This can be done directly from the data collector policy or from the Inventory. See Adding and Editing Hosts and Backup Servers.

4. Enter values for all required fields (denoted by an *) and click **OK**. The field, *Internal Host Name*, needs to match the host name of the HP Cell Manager Server. Ensure you select **HP Cell Manager Server** as the Type. The fields *External Name*, *Make* and *Model* are not used by the application for anything other than display purposes.
5. Select the Host Group while you are adding the backup server. See Managing Host Groups for details.

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

Adding an HP Data Protector Data Collector Policy

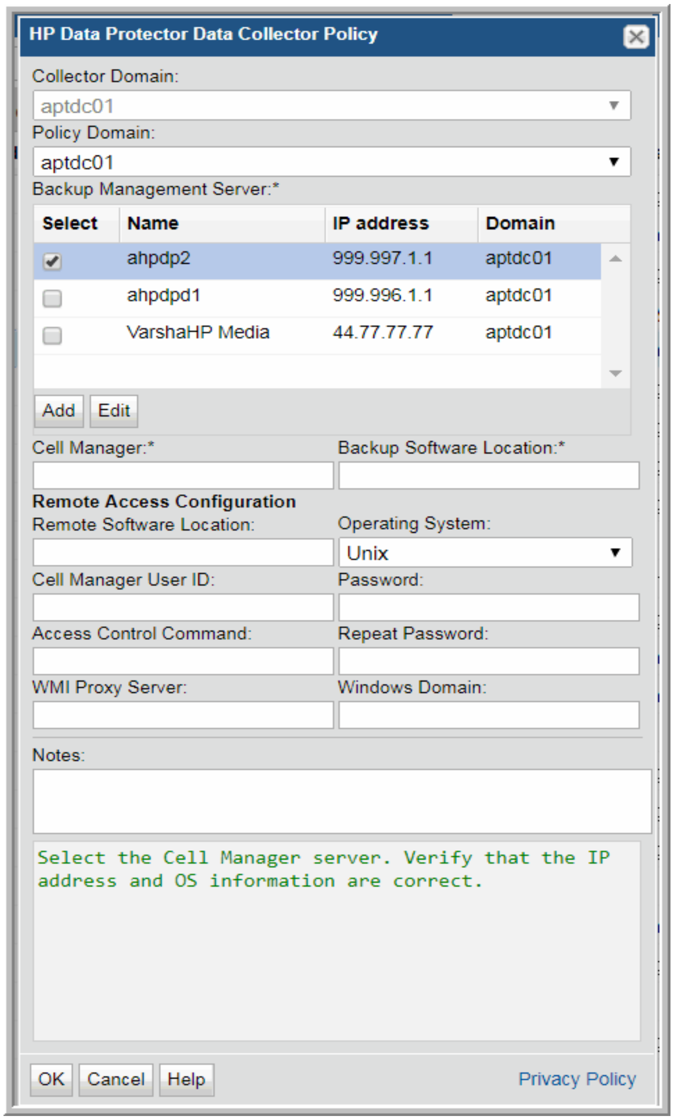
- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE Certified Configurations Guide*.
- **After adding 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.
5. Optionally add an HP Data Protector Backup Server from the policy screen. This action can also be completed in the Inventory. See Adding/Editing a HP Data Protector Server within the Data Collector Policy.

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



HP Data Protector Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Backup Management Server:*

Select	Name	IP address	Domain
☑	ahpdp2	999.997.1.1	aptdc01
□	ahpdpd1	999.996.1.1	aptdc01
□	VarshaHP Media	44.77.77.77	aptdc01

Cell Manager:*

Backup Software Location:*

Remote Access Configuration

Remote Software Location:

Operating System: Unix

Cell Manager User ID:

Password:

Access Control Command:

Repeat Password:

WMI Proxy Server:

Windows Domain:

Notes:

```
Select the Cell Manager server. Verify that the IP
address and OS information are correct.
```

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

Field	Description	Sample Value
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.	`yourdomain`
Backup Management Server*	Select the Cell Manager server. Verify that the IP address and OS information are correct.	
Add	Click **Add** to add a Cell Manager server. Added servers are also displayed in the **Inventory**.	
Edit	Select a Cell Manager server and click **Edit** to update the values.	
Cell Manager*	The Cell Manager is the server that runs session managers and core software to manage the backup details in the HP Data Protector database. Enter the name or IP address of the HPDP Cell Manager Server. In the majority of cases, this field should contain the *same server that you selected from the above Backup Management Server list*; however, for special-case situations, an alias may be entered.	HPSERVER
Backup Software Location*	On the Data Collector server, this is the home directory of the HP Data Protector Admin Client software—that is, the location of the *omni* commands, such as *omnicellinfo* and *omnireport*—to be used by the Data Collector server.	
Remote Access Configuration The following parameters are required *only* when the Data Collector server is different from the Cell Manager server.		
Remote Software Location	The home directory on the HP Data Protector server where Cell Manager is installed. Typically C:\Program Files\Omniback for Windows, or /opt/omni for Linux; only required for remote access to Cell Manager.	
Operating System	The operating system on which the HP Data Collector is running; only required for remote access to Cell Manager.	

Field	Description	Sample Value
Cell Manager User ID	An Admin User that the Cell Manager server recognizes—either a local user account or a Windows domain user account—that has execute rights to the omnidbutil command. This command is used to obtain drive status. Required only when the Data Collector is on a server that is different from the Cell Manager server.	
Password/Repeat Password	Password for the Cell Manager User ID on the remote system.	
Access Control Command	For Linux hosts: If the user ID is not root, provide the full path to access control; Example: /usr/bin/sudo	
WMI Proxy Server	Enter the server name or IP address where the WMI Proxy is installed. Only needed if collecting from Windows hosts and when the Data Collector is on a server that is different from the Cell Manager server. If the Data Collector is installed on a Linux OS, a WMI Proxy Server must be installed on a Windows system in order to collect data from a Cell Manager that is installed on a Windows system.	
Windows Domain	The Windows domain, if applicable.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	

Adding/Editing a HP Data Protector Server within the Data Collector Policy

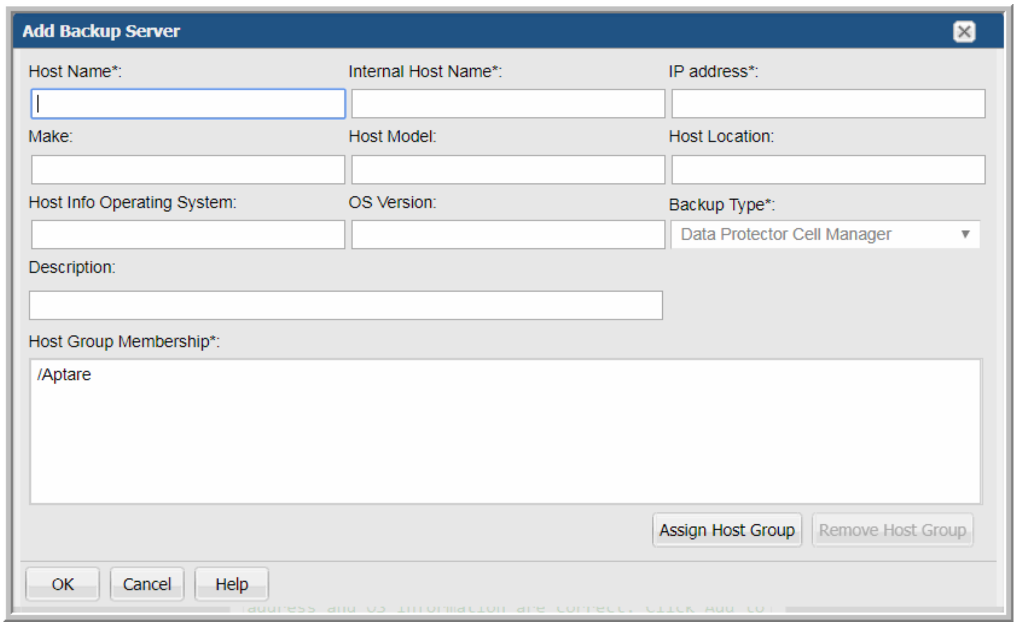
Add and edit HP Data Protector Cell Manager servers directly from the data collector policy. This functionality is also available using the **Inventory**. See Adding and Editing Hosts and Backup Servers for details.

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

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

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

2. The **Add Backup Server** screen displays.



Add Backup Server

Host Name*:

Internal Host Name*:

IP address*:

Make:

Host Model:

Host Location:

Host Info Operating System:

OS Version:

Backup Type*: Data Protector Cell Manager

Description:

Host Group Membership*: /Aptare

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

Tune the Configuration

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

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

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

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

9

Pre-Installation Setup for IBM Spectrum Protect (TSM)

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

- Architecture Overview (IBM Spectrum Protect -TSM)
- Prerequisites for Adding Data Collectors (IBM Spectrum Protect - TSM)
- Installation Overview (IBM Spectrum Protect - TSM)
- Adding/Configuring an IBM Spectrum Protect (TSM) Server within the Data Collector Policy

Architecture Overview (IBM Spectrum Protect -TSM)

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

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

IBM Spectrum Protect (TSM) - Servers and Instances Defined

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

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

Prerequisites for Adding Data Collectors (IBM Spectrum Protect - TSM)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- A IBM Spectrum Protect (TSM) client must be installed on the Data Collector server with the dsmadmc command available.
- Ports to IBM Spectrum Protect (TSM) instances must be open. Each instance will have a unique port. Make note of these instance/port combinations for data collection. Typically, TCP 1500 is the default port.
- The Data Collector server can be any server within your network that is Java 1.7 compatible and with **dsmadmc** installed. For Linux platforms, this server must be added to **dsm.sys** so the Data Collector can use the **dsmadmc** command.

Installation Overview (IBM Spectrum Protect - TSM)

1. Updating the Local Hosts File for Data Collection
2. Add IBM Spectrum Protect (TSM) Servers
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. In the Portal, add the IBM Spectrum Protect (TSM) data collector policy. Adding an IBM Spectrum Protect (TSM) Data Collector Policy.
5. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
6. Validate the Data Collector Installation. See Validating Data Collection.

Add IBM Spectrum Protect (TSM) Servers

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

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

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

Note: You can also add IBM Spectrum Protect (TSM) servers directly from the Data Collector policy screen. See Adding/Configuring an IBM Spectrum Protect (TSM) Server within the Data Collector Policy.

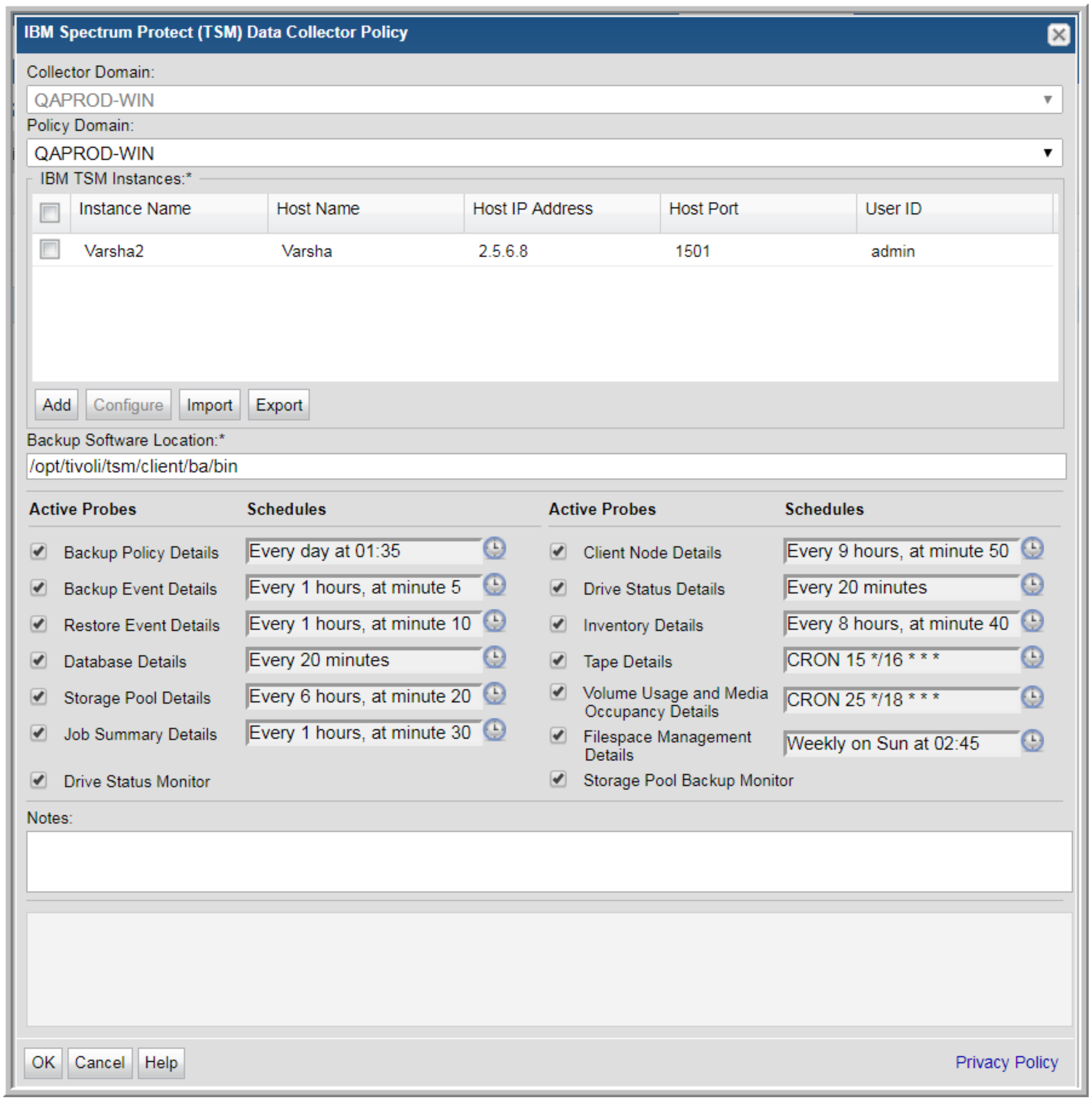
Adding an IBM Spectrum Protect (TSM) Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



IBM Spectrum Protect (TSM) Data Collector Policy

Collector Domain: QAPROD-WIN

Policy Domain: QAPROD-WIN

IBM TSM Instances:*

□	Instance Name	Host Name	Host IP Address	Host Port	User ID
□	Varsha2	Varsha	2.5.6.8	1501	admin

Backup Software Location:* /opt/tivoli/tsm/client/ba/bin

Active Probes	Schedules	Active Probes	Schedules
☑ Backup Policy Details	Every day at 01:35	☑ Client Node Details	Every 9 hours, at minute 50
☑ Backup Event Details	Every 1 hours, at minute 5	☑ Drive Status Details	Every 20 minutes
☑ Restore Event Details	Every 1 hours, at minute 10	☑ Inventory Details	Every 8 hours, at minute 40
☑ Database Details	Every 20 minutes	☑ Tape Details	CRON 15 */16 * * *
☑ Storage Pool Details	Every 6 hours, at minute 20	☑ Volume Usage and Media Occupancy Details	CRON 25 */18 * * *
☑ Job Summary Details	Every 1 hours, at minute 30	☑ Filespace Management Details	Weekly on Sun at 02:45
☑ Drive Status Monitor		☑ Storage Pool Backup Monitor	

Notes:

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

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

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. (The Collector Domain is the domain that was supplied during the Data Collector installation process.) The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
IBM Spectrum Protect (TSM) Instances	
Active	Click **Active** to indicate the IBM Spectrum Protect (TSM) server/instances to use in the data collection policy. Multi-select is supported. If additional fields must be configured, the **Configure Server** dialog is automatically displayed when you make your selection.
Add	Click **Add** to add an IBM Spectrum Protect (TSM) server/instance. The IBM Spectrum Protect (TSM) servers added to this table using **IBM Spectrum Protect (TSM) Data Collector Policy** screen are also displayed in the Inventory **Note**: Data Collector policies can be in place for multiple instances, but an instance cannot exist in multiple policies. See also Adding/Configuring an IBM Spectrum Protect (TSM) Server within the Data Collector Policy.
Configure	Select a row in the **IBM Spectrum Protect (TSM) Instances** table. Double-click or click **Configure** to revise or add information to the TSM server/instance you selected. See also Adding/Configuring an IBM Spectrum Protect (TSM) Server within the Data Collector Policy.
Import	Click **Import** to browse for the CSV file in which you entered the IBM Spectrum Protect (TSM) server/instance configuration details. This enables you quickly add a list of IBM Spectrum Protect (TSM) instances or servers. See also Importing IBM Spectrum Protect (TSM) Information.
Export	Click **Export** to create and download a comma-separated values (CSV) file containing all the host/instance information listed in the **IBM Spectrum Protect (TSM) Instances** table. This enables you to extract your IBM Spectrum Protect (TSM) server information and transfer it easily into a spreadsheet or some other media. See also Exporting IBM Spectrum Protect (TSM) Server Information.
Backup Software Location*	The home directory of the TSM Admin Client software—that is, the dsmadmc command on the Data Collector server. Typically C:\Program Files\Tivoli\TSM\baclient for Windows, or /opt/tivoli/tsm/client/ba/bin for Linux
Active Probes and Schedules	

Field	Description
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Backup Policy Details	Collects backup policy details including policy name, policy identifier, date and time as it relates to the specified IBM Spectrum Protect (TSM) instances/ servers.
Backup Event Details	Collects backup event details including backup type, client names, duration, dates, size, files, directories and so on.
Restore Event Details	Collects restore event details such as job duration, number of files backed up and also skipped, amount of data restored, and restore job status.
Database Details	Collects IBM Spectrum Protect (TSM) backup database details, such as total capacity, available space, cache hit percentages, and buffer requests.
Storage Pool Details	Collects IBM Spectrum Protect (TSM) storage pool information, such as migration and reclamation details.
Job Summary Details	Collects IBM Spectrum Protect (TSM) job summary details including client name, node name, backup type, dates, duration and so on, as it relates to the specified IBM Spectrum Protect (TSM) instances/servers.
Client Node Details	Collects client node details covered by the selected policy domain as they relate to the specified IBM Spectrum Protect (TSM) instances/servers.
Drive Status Monitor	Continuously monitors the IBM Spectrum Protect (TSM) console for drive status messages, there is no schedule.
Drive Status Details	Collects drive status details including, drive name, library name, status, start and end times as it relates to the specified IBM Spectrum Protect (TSM) instances/ servers.
Inventory Details	Collects IBM Spectrum Protect (TSM) host details including host name, IP Address, Host ID, and port number. Also collects from drives and paths such as device type, device name, library name, and ACS drive ID.
Tape Details	Collects the tape details including media type name, media status, storage pool name, and estimated capacity.
Volume Usage and Media Occupancy Details	Collects client and node information, and then for each node it retrieves the volume usage details from the IBM Spectrum Protect (TSM) instance or server. For each volume, collects details of media occupying the storage pool. Details include the type and size of the media.
Filespace Management Details	Collects filespace details such as capacity, backup start/finish dates, and the percentage of the filespace that is occupied.
Storage Pool Backup Monitor	Continuously monitors the IBM Spectrum Protect (TSM) console for storage pool migration messages, there is no schedule.
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.

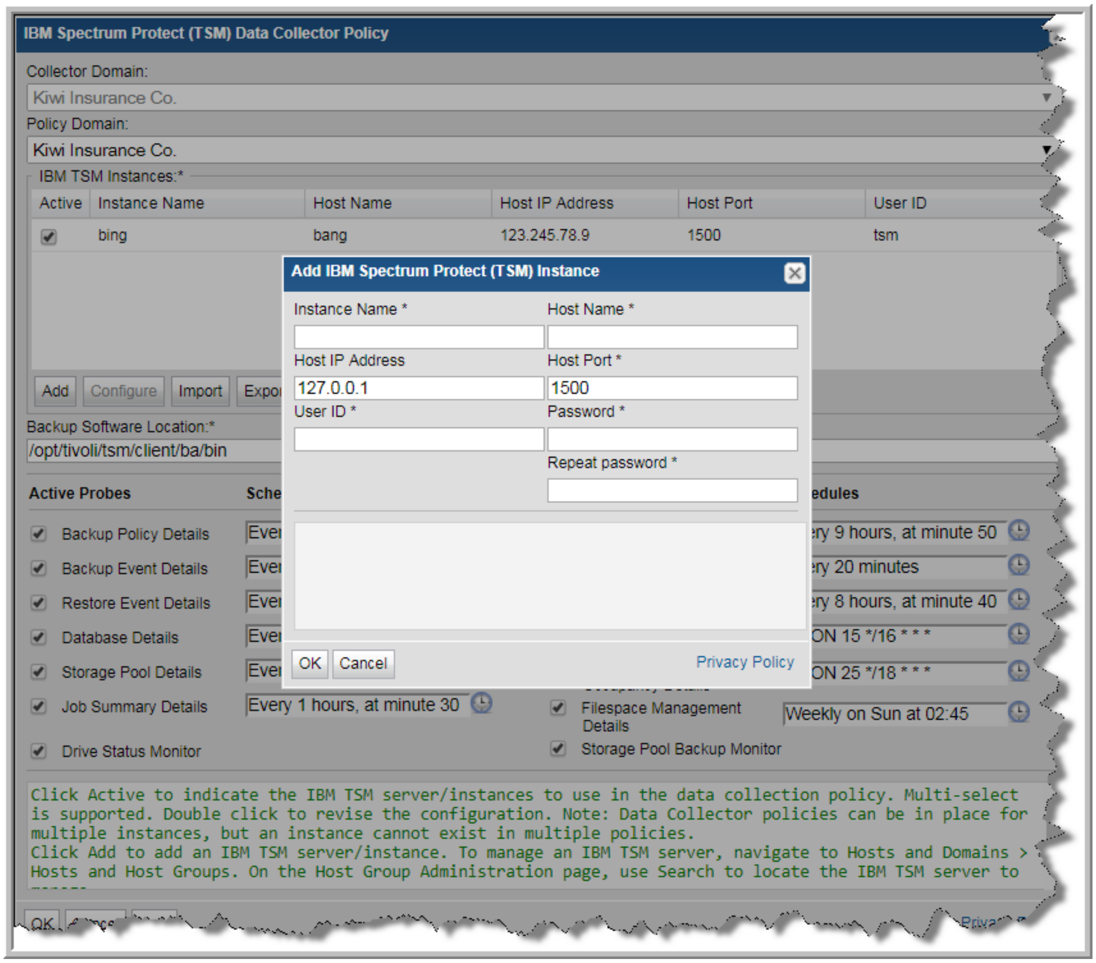
6. Click **OK** to save the policy.
7. On the Data Collector server, install/update the Data Collector software.

Adding/Configuring an IBM Spectrum Protect (TSM) Server within the Data Collector Policy

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

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

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



IBM Spectrum Protect (TSM) Data Collector Policy

Collector Domain: Kiwi Insurance Co.

Policy Domain: Kiwi Insurance Co.

IBM TSM Instances:*

Active	Instance Name	Host Name	Host IP Address	Host Port	User ID
☑	bing	bang	123.245.78.9	1500	tsm

Backup Software Location:* /opt/tivoli/tsm/client/ba/bin

Add IBM Spectrum Protect (TSM) Instance

Instance Name *

Host Name *

Host IP Address: 127.0.0.1

Host Port *: 1500

User ID *

Password *

Repeat password *

Active Probes	Schedules
☑ Backup Policy Details	Ever
☑ Backup Event Details	Ever
☑ Restore Event Details	Ever
☑ Database Details	Ever
☑ Storage Pool Details	Ever
☑ Job Summary Details	Every 1 hours, at minute 30
☑ Drive Status Monitor	
	ry 9 hours, at minute 50
	ry 20 minutes
	ry 8 hours, at minute 40
	ON 15 */16 * * *
	ON 25 */18 * * *
☑ Filespace Management Details	Weekly on Sun at 02:45
☑ Storage Pool Backup Monitor	

Click Active to indicate the IBM TSM server/instances to use in the data collection policy. Multi-select is supported. Double click to revise the configuration. Note: Data Collector policies can be in place for multiple instances, but an instance cannot exist in multiple policies.
Click Add to add an IBM TSM server/instance. To manage an IBM TSM server, navigate to Hosts and Domains > Hosts and Host Groups. On the Host Group Administration page, use Search to locate the IBM TSM server to

2. Enter the values:

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

Importing IBM Spectrum Protect (TSM) Information

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

CSV Format Specifications

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

1. **Instance Name**
2. **Host Name**
3. **Host Port**
4. **Host IP Address**
5. **Admin Account**
6. **Software Location**

To Import IBM Spectrum Protect (TSM) Hosts

1. Prepare the CSV according to CSV Format Specifications.
2. Select **Admin > Data Collection > Collector Administration**.
3. Search for a Collector if required. See To Add a Data Collector.

4. Select a collector.
5. Click **Add Policy** and select **IBM Spectrum Protect (TSM)**. The **IBM Spectrum Protect (TSM) Data Collector Policy** screen is displayed.
6. Click **Import**. The **Import IBM Spectrum Protect (TSM) Instances** dialog is displayed. You can browse for the CSV file you created.

Exporting IBM Spectrum Protect (TSM) Server Information

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

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

10

Pre-Installation Setup for Veritas Backup Exec

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.

- Installation Overview (Veritas Backup Exec)
- Prerequisites for Adding Data Collectors (Veritas Backup Exec)
- Installation Overview (Veritas Backup Exec)
- Enable TCP/IP for the SQL Server
- Configure a Windows User
- Add Veritas Backup Exec Servers
- Adding a Veritas Backup Exec Data Collector Policy

Architecture Overview (Veritas Backup Exec)

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

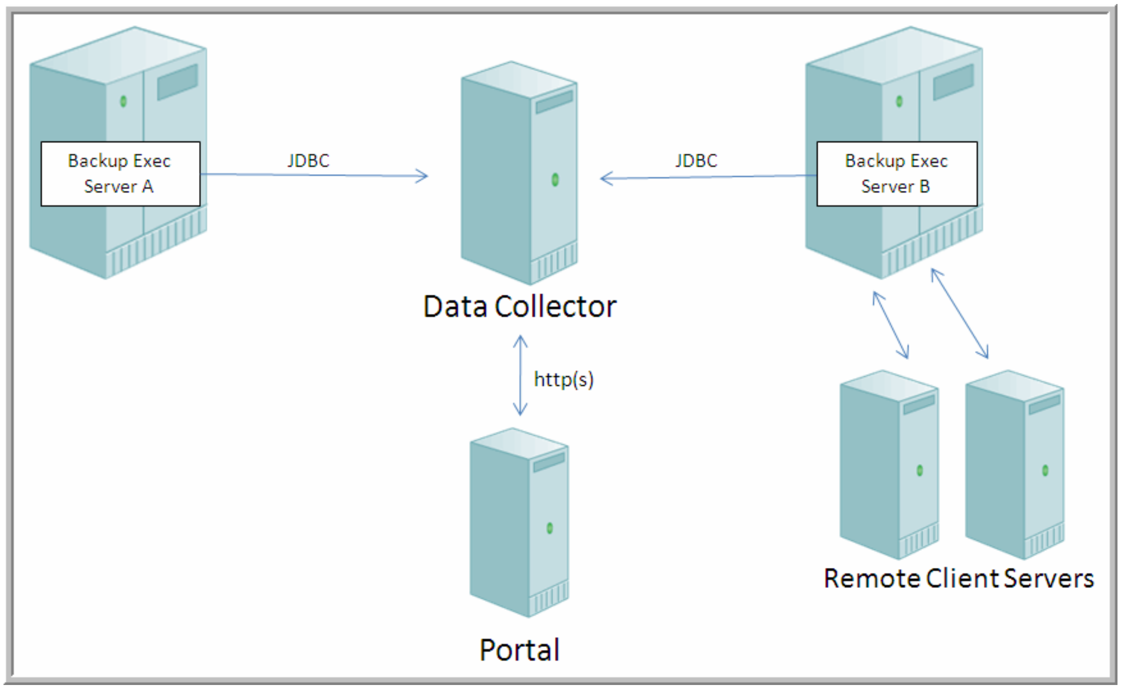


Figure 3 Data Collector in a Veritas Backup Exec Environment

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

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

Backup Exec Terminology

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

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

Prerequisites for Adding Data Collectors (Veritas Backup Exec)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 1433. The BUE collector first connects via UDP on port 1434 to get information about available SQL Server instances, then connects via TCP to the port number that is returned for the specified instance. By default this is 1433.
- If your environment requires NTML v2 authentication (Windows authentication) for the data collection connection, create an Advanced Parameter named USE_NTML_V2 and set the value to Y. Note that the IT Analytics default is NTML v1 (database authentication). Windows authentication is used when the Backup Exec server credentials configured in the Data Collector Policy contain a Windows domain name, user name, and password. If Windows credentials are *not* in the policy, the connection defaults to using database authentication.
- The Backup Exec Administrator account used by the Data Collection policy must have the database role membership of **db_datareader** for the BEDB (Backup Exec Database).
- Note that the version of Backup Exec that is reported by the Backup Exec 15 installation is version 14.2.

Upgrade Troubleshooting: Microsoft SQL Server and Java 10

With release version 10.3 introducing support for Java 10, 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 version 10.3 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 10.

```
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)
```

APTARE recommends to upgrade MS SQL Server to the latest version to enable secure collection. Your MS SQL Server version may not be supported for APTARE IT Analytics version 10.3. 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 allow communication with the data collector:

1. Edit <collector install dir>/jre/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=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
#    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

4. Remove `3DES_EDE_CBC`.

```
#jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
#    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, DES40_CBC, RC4_40
```

5. Save the file.
6. Run **checkinstall** and verify collection succeeds.

If **checkinstall** does not succeed, each of the following algorithms can be individually re-enabled in an attempt to restore compatibility.

7. If **checkinstall** does not succeed, restore, remove `RC4_40`, save, re-run **checkinstall**.

```
#jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
#    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, DES40_CBC, 3DES_EDE_CBC
```

8. If **checkinstall** does not succeed, restore, remove `DES40_CBC`, save, re-run **checkinstall**.

```
#jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
#    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, RC4_40, 3DES_EDE_CBC
```

9. If **checkinstall** does not succeed, restore, change the `DH keySize` as follows, save, re-run **checkinstall**.

```
#jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 1024, \
#    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
jdk.tls.disabledAlgorithms=TLSv3, RC4, MD5withRSA, DH keySize < 768, \
    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

10. After a working configuration is found, restart the collector service.

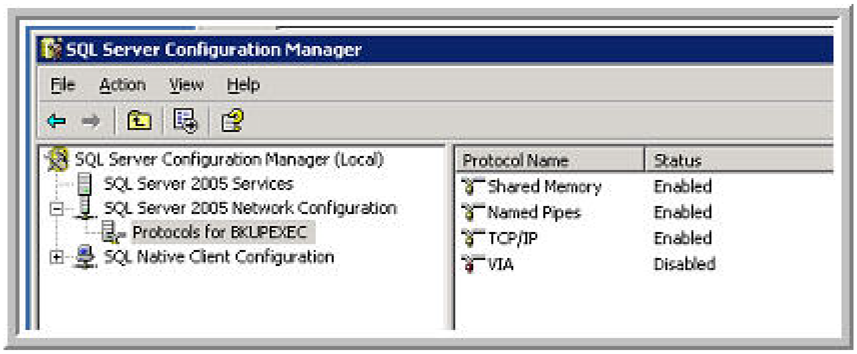
Installation Overview (Veritas Backup Exec)

1. Updating the Local Hosts File for Data Collection
2. Enable TCP/IP for the SQL Server
3. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
4. Enable TCP/IP for the SQL Server.
5. Configure a Windows User.
6. Add Veritas Backup Exec Servers.
7. In the Portal, add the Veritas Backup Exec data collector policy. Adding a Veritas Backup Exec Data Collector Policy.
8. On the Data Collector Server, install the Data Collector software. See Installing Data Collectors.
9. Validate the Data Collector Installation. See Validating Data Collection

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

Enable TCP/IP for the SQL Server

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


SQL Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
Protocols for BKUPEXEC
SQL Native Client Configuration

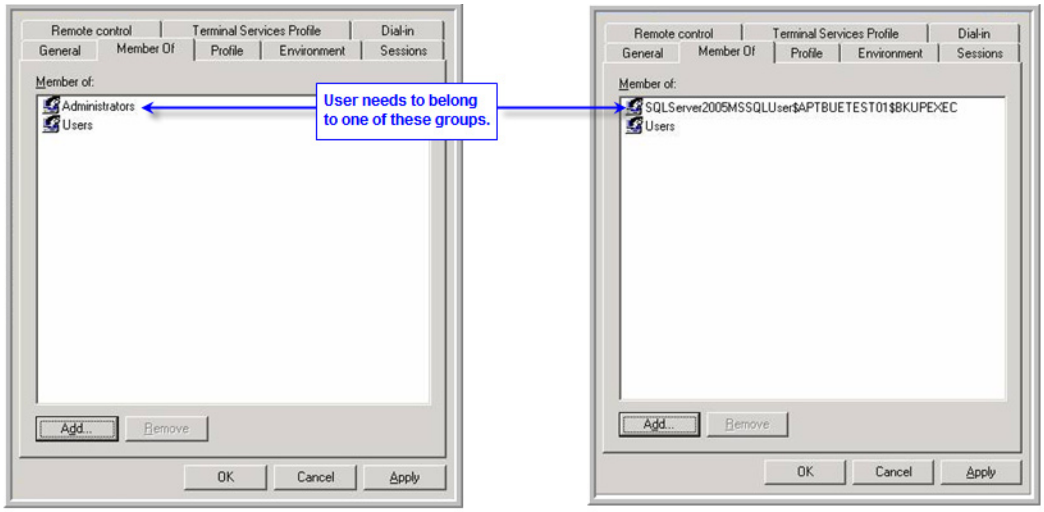
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

Configure a Windows User

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

1. Complete the worksheet found in the Appendix of this guide, providing configuration details for each backup server that will be polled by a Data Collector.
2. Ensure that you have a **Windows User** that is a member of *one of the following groups,* either locally or as part of the Windows Domain:
   - the local **Administrators** group
   - a group named: **SQLServer2005MSSQLUser$*ServerName*$BKUPEXEC**

   where *ServerName* is the name of the server on which the SQL Server and Backup Exec reside, as shown in the following example.

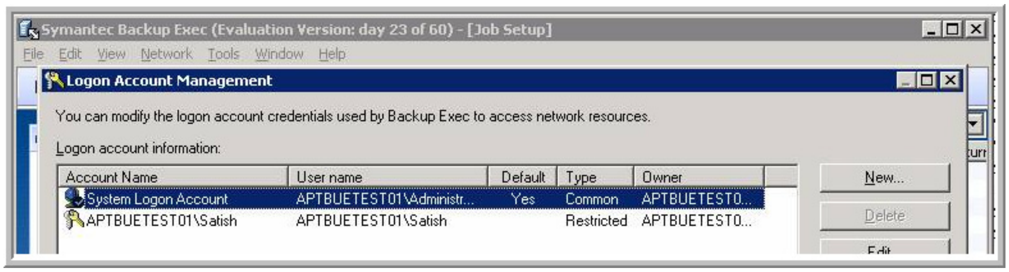


Member of:
- Administrators
- Users

User needs to belong to one of these groups.

Member of:
- SQLServer2005MSSQLUser$APTBUETEST01$BKUPEXEC
- Users

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



You can modify the logon account credentials used by Backup Exec to access network resources.

Logon account information:

Account Name	User name	Default	Type	Owner
System Logon Account	APTBUETEST01\Administr...	Yes	Common	APTBUETEST0...
APTBUETEST01\Satish	APTBUETEST01\Satish		Restricted	APTBUETEST0...

Add Veritas Backup Exec Servers

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

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

Importing Backup Exec Server Information

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

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

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

   Each line in the CSV file should follow this format:

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

   Example CSV File:

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

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

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

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

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

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

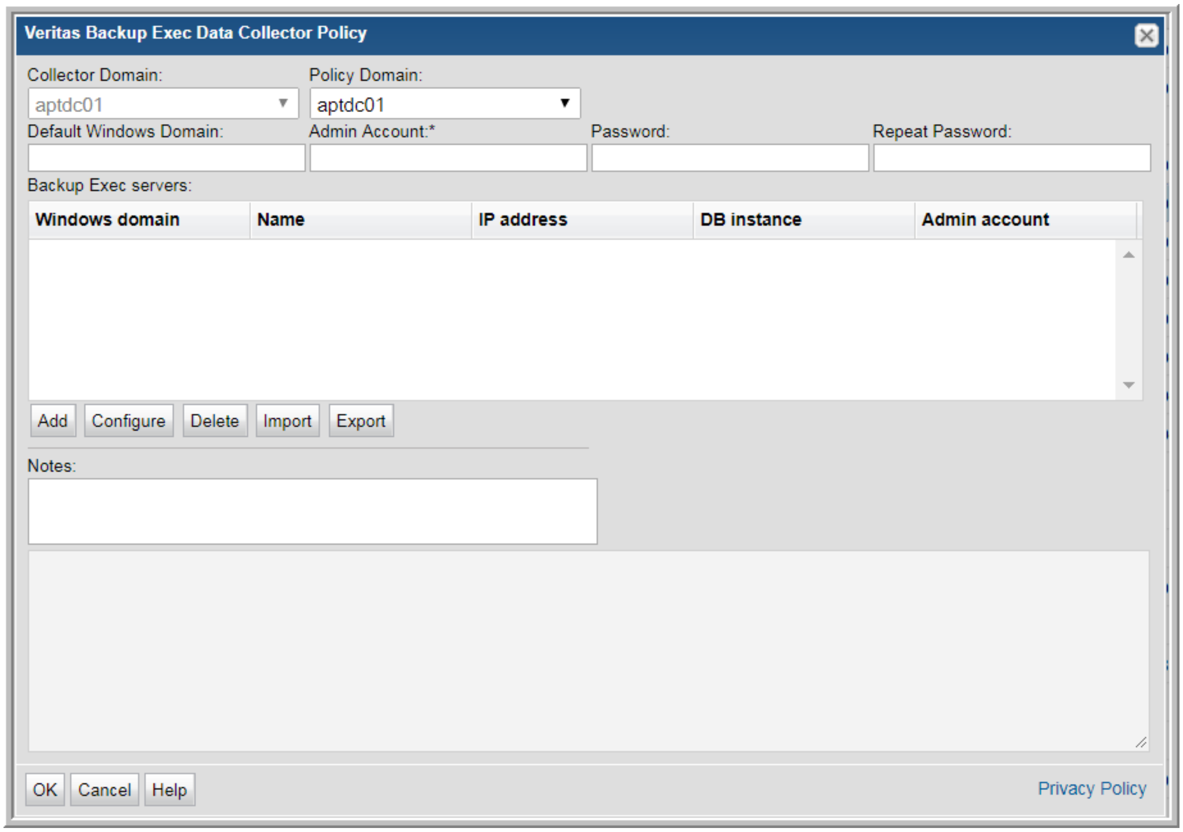
Adding a Veritas Backup Exec Data Collector Policy

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

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

To add the policy

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



Veritas Backup Exec Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Default Windows Domain:

Admin Account:*

Password:

Repeat Password:

Backup Exec servers:

Windows domain	Name	IP address	DB instance	Admin account

Notes:

5. Enter or select the parameters.

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

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

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

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

11

Pre-Installation Setup for Veritas NetBackup

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)

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses ports 1556 and 13724, WMI range of ports, Linux ssh 22
- For specific NetBackup Data Collector requirements, see Centralized or Distributed Deployment (Veritas NetBackup).
- **Solaris Deployment** - The `nohup` command must be substituted in the `startup.sh` script for the APTARE agent services to run. Edit the `startup.sh` script under /opt/aptare/mbs/bin and replace `exec` with `nohup`.

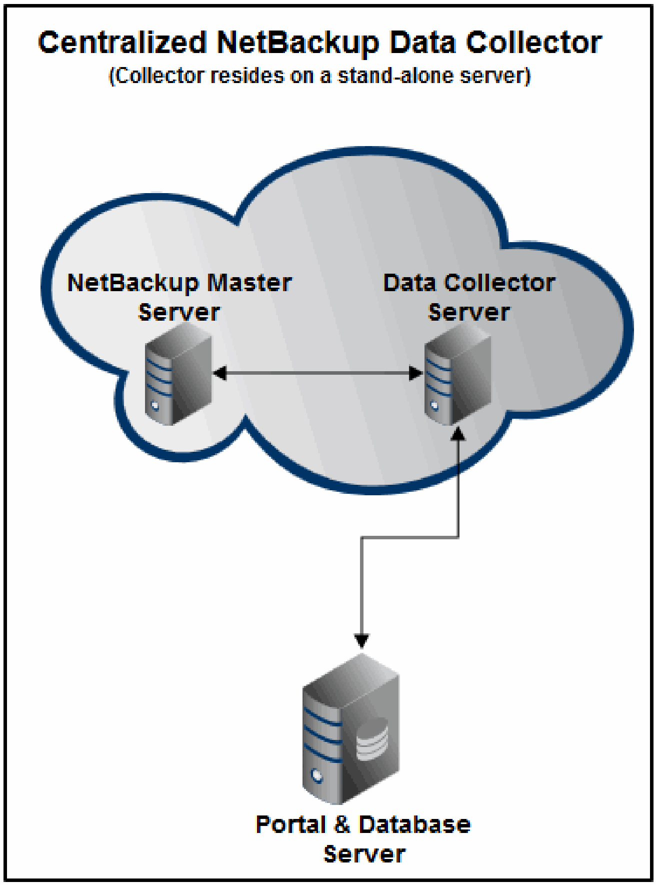
Centralized or Distributed Deployment (Veritas NetBackup)

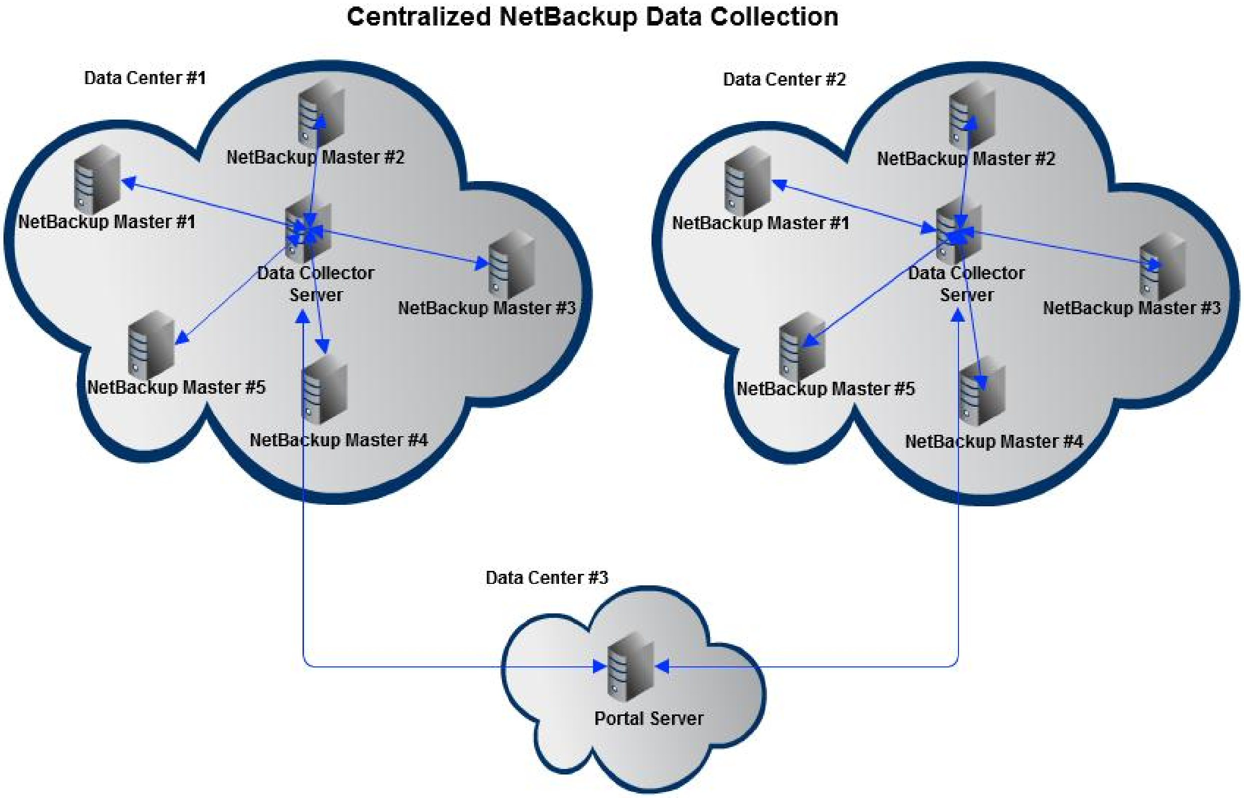
Two upgrade/installation options are available. Choose the one that best meets your needs.

- Centralized NetBackup Data Collection (Recommended)
- Distributed NetBackup Data Collection

Centralized NetBackup Data Collection (Recommended)

Use a centralized Data Collector to collect data from multiple NetBackup Master Servers, *without* any APTARE software installed on the Master Servers, as illustrated below.


Centralized NetBackup Data Collector
(Collector resides on a stand-alone server)
NetBackup Master Server
Data Collector Server
Portal & Database Server



Requirements for Centralized Data Collection

- **Minimum Requirements**: 64-bit OS, 2 CPUs or vCPUs and 32 GiB RAM.
- If there is a firewall between the NetBackup Master Servers and the Data Collector Server, ensure that bi-directional port communication is open on ports 1556 and 13724.
- For a NetBackup Centralized Data Collector (Linux or Windows OS), the Data Collector needs access to the Admin commands (CLI). This typically requires the NetBackup Master Server or Media Server binaries to be installed on the Data Collector server. The CLI is available only with the Master or Media Server binaries. Note that the installation of these binaries may require you to acquire a NetBackup Master or Media Server license from Veritas.
- For Veritas NetBackup 8.1, see Veritas NetBackup 8.1 Requirements for Centralized Collection.
- The NetBackup software version on the Data Collector must match the major and minor version of the NetBackup software that is installed on the Master or Media Server that is being probed. When the Data Collector starts, it checks versions and halts collection for the Master Server where the mismatch is found. Refer to the Veritas documentation for more information about major and minor version requirements.
- If you are currently running version 9.0 with centralized NetBackup data collection, and if the NetBackup software versions don't match, when you upgrade to APTARE Release Version 10 (or higher) data collection will cease for the Master Servers with the incompatible versions.
- For SLP collection, a WMI Proxy Server is required. See Required Software. 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.

Note: If all NetBackup Masters configured in the collection policy are using the Linux operating system, then a WMI Proxy is not required.

Veritas NetBackup 8.1 Requirements for Centralized Collection

Veritas NetBackup 8.1 introduces a series of changes to the way a NetBackup host (such as the APTARE Data Collector) communicates with NetBackup Masters. These changes incorporate an enhanced secured channel for communication and more sophisticated host identity verification.

These changes require installation steps on the centralized Data Collector system that are not required for collection from NetBackup Master Servers prior to version 8.1.

Requirements for successful collection from a NetBackup 8.1 system:

- As with all centralized NetBackup Data Collectors post NetBackup v7.7.3, the NetBackup software version on the Data Collector must match the major and minor version of the NetBackup software that is installed on the Master or Media Server that is being probed.
- After installing the correct Veritas software, the Data Collector server needs to be added as a **trusted server** to all NetBackup Master Servers from which you want to collect data. This is typically accomplished using the netbackup command `nbcertcmd`. If the Data Collector is NOT registered as a trusted server, collection will not work.
- A CA root certificate and a host ID-based security certificate must be installed on the Data Collector Server for each Master Server that will be accessed for data collection. Refer to the *Veritas NetBackup Security and Encryption Guide, Version 8.1* for information on how to deploy CA and host ID-based certificates.
- The Data Collector Server must be added as a NetBackup Media Server in both NBDB and registry/bp.conf files, on each NetBackup Master that will be accessed for data collection. Refer to the Managing Media Servers section of the *Veritas NetBackup Administrators Guide, Volume 1*.
- The NetBackup media server software daemons on the Data Collector Server must be active.

Required Software

NetBackup 7.6 or earlier Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Master	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Master or Media Server software installed on the Data Collector server. If SLP collection is required, a WMI Proxy Server must be set up on a Windows server.
Linux NetBackup Master	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Master or Media Server software installed on the Data Collector server.

NetBackup 7.7 or later Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Master	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Master or Media Server software installed on the Data Collector server.	NetBackup Master or Media Server software installed on the Data Collector server. If SLP collection is required, a WMI Proxy Server must be set up on a Windows server.
Linux NetBackup Master	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Master or Media Server software installed on the Data Collector server.	NetBackup Master or Media Server software installed on the Data Collector server.

Overview of Centralized Data Collector Steps

The following list provides an overview of the steps to be taken. Details are provided later in this guide.

1. Identify a Data Collector server for the installation of the collection software, based on Requirements for Centralized Data Collection.
2. For a NetBackup Centralized Data Collector (Linux or Windows OS), that is collecting from NetBackup Masters running v7.7 or later, the NetBackup Master Server or Media Server binaries must be installed on the Data Collector. The Data Collector needs access to the CLI, which is only available with the Master or Media Server binaries. Note that the installation of these binaries may require you to acquire a NetBackup Master or Media Server license from Veritas.
3. Verify connectivity and correct configuration. See Verify Remote Commands for Centralized NetBackup Data Collection.
4. The Data Collector server needs to be added to the list of servers allowed to access the NetBackup Master Server from which you want to collect data. See Enable Access to the Veritas NetBackup Master Server.
5. In the Portal, add a host entry for the NetBackup Master Server and select the type as Veritas NetBackup Master Server.
6. In the Portal, add a NetBackup Data Collector Policy to an existing Data Collector or create a New Data Collector and then add a NetBackup Data Collector Policy. See Pre-Installation Setup for Veritas NetBackup.
7. (If changing from Distributed to Centralized NetBackup collection)

   Un-install the APTARE NetBackup Data Collectors from all NetBackup Master Servers.
8. On the Data Collector server, run checkinstall. See Validation Methods.
9. Start the Data Collector.

Verify Remote Commands for Centralized NetBackup Data Collection

The NetBackup centralized Data Collector executes a number of NetBackup commands remotely using the NetBackup Remote Administrator Console software. Many commands query NetBackup Master Servers that are listed in the collection policy and so the NetBackup Master needs to be configured to accept these requests from the Data Collector. Some collection probes query NetBackup Media Servers and some probe NetBackup clients; therefore, network connectivity and NetBackup permissions need to be configured to allow these commands to return the correct output.

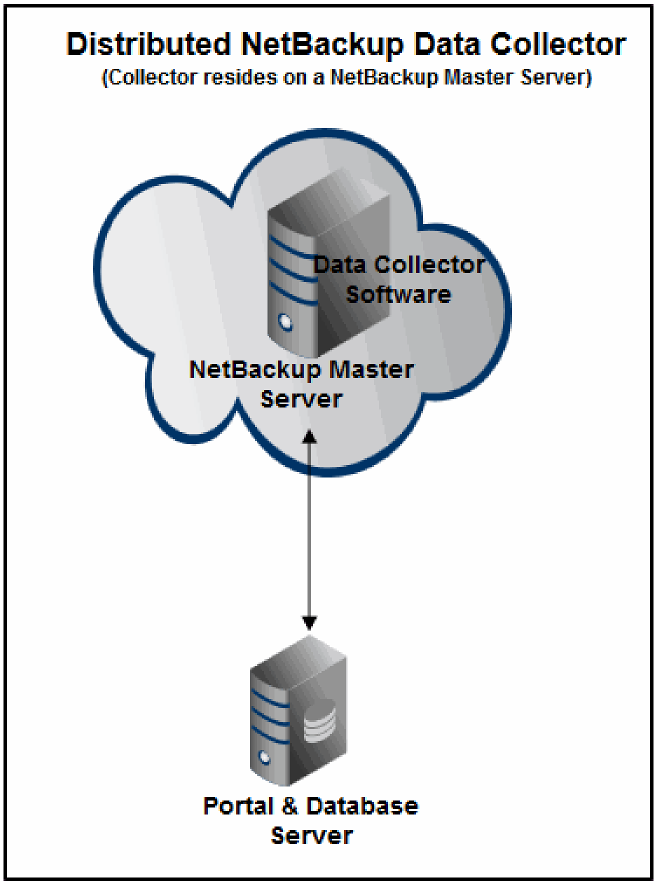
The following commands should execute without error and with data returned before the Data Collector can probe the systems.

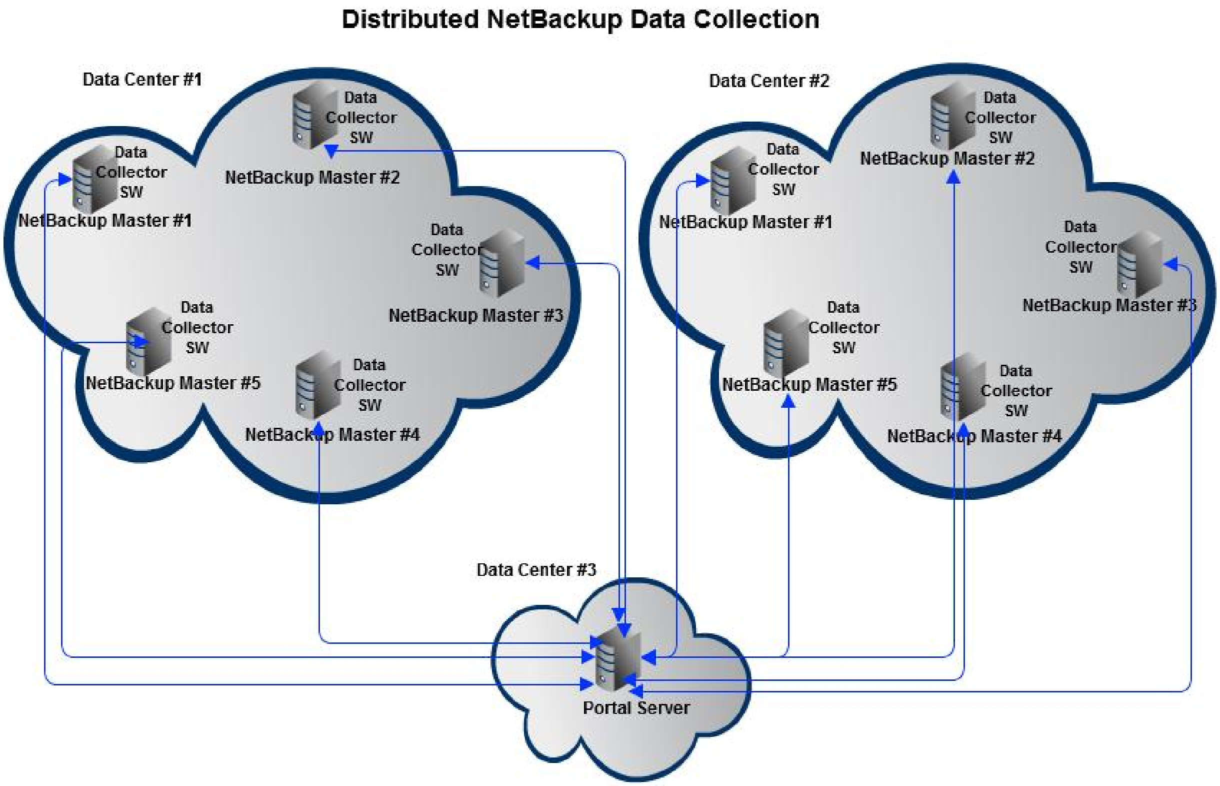
Master Servers	`bpgetconfig -L -s [server name]`
	`bppllist -M [server name]`
	`nbdevquery -liststs -U -EMM [server name]`

Every Master and Media Server	`/usr/openv/volmgr/bin/vmoprcmd -h [server name] -devconfig`
Every Client	`bpgetconfig -L -s [client name]`

Distributed NetBackup Data Collection

APTARE Data Collector software is installed on *each* NetBackup Master Server.


Distributed NetBackup Data Collector
(Collector resides on a NetBackup Master Server)
Data Collector Software
NetBackup Master Server
Portal & Database Server



The following list provides an overview of the steps to be taken. Details are provided later in this guide.

1. Verify the Data Collector server minimum requirements.
   - **Minimum Requirements**: 64-bit OS, 2 CPUs or vCPUs and 16 GB RAM.
2. For upgrades, a distributed Data Collector (Release Version 9.x+) installed on a NetBackup Master Server will be automatically updated to APTARE Release Version 10.x. You do not need to re-install the Data Collector.
3. For new installations, in the Portal, add a host entry for each NetBackup Master Server and select the type as **Veritas Master Server**.
4. In the Portal, for each NetBackup Master Server, create one of each of the following:
   - **New Data Collector -** For distributed collection there must be one Data Collector entry on the Portal for each NetBackup Master Server.
   - **NetBackup Data Collector Policy** for the New Data Collector. See Pre-Installation Setup for Veritas NetBackup.
5. For both upgrades and new installations, install the Data Collector software on each NetBackup Master Server. See Installing Data Collectors.
6. On each NetBackup Master Server, run checkinstall. See Validation Methods.
7. Start the Data Collector.

Enable Access to the Veritas NetBackup Master Server

Centralized NetBackup Data Collection must be able to access the NetBackup Master Server to retrieve metadata. If this access is not authorized, Data Collection will encounter this error: *(46) Server not allowed access*.

- Using the NetBackup Remote Administration Console, add the Data Collector servers to the list of servers allowed to access the NetBackup Master Server.

Linux Master Servers

If the NetBackup Master Server is *not* an appliance, access can be granted by editing `/usr/openv/netbackup/bp.conf` and adding SERVER lines with the relevant Data Collector host names, as shown in the following example.

Example:

```
SERVER = sc90legoportalit
SERVER = nbu-master
SERVER = aptarenbu-win
CONNECT_OPTIONS = localhost 1 0 2
USE_VXSS = PROHIBITED
VXSS_SERVICE_TYPE = INTEGRITYANDCONFIDENTIALITY
EMMSERVER = nbu-master
HOST_CACHE_TTL = 3600
VXDBMS_NB_DATA = /usr/openv/db/data
LIST_FS_IMAGE_HEADERS = NO
TELEMETRY_UPLOAD = NO
```

Before You Install the Data Collector (Veritas NetBackup)

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.

In preparation for Data Collector installation, take the steps.

- Review the requirements listed in Centralized or Distributed Deployment (Veritas NetBackup) and Enable Access to the Veritas NetBackup Master Server.
- Ensure that Ports 1556 and 13724 are open.

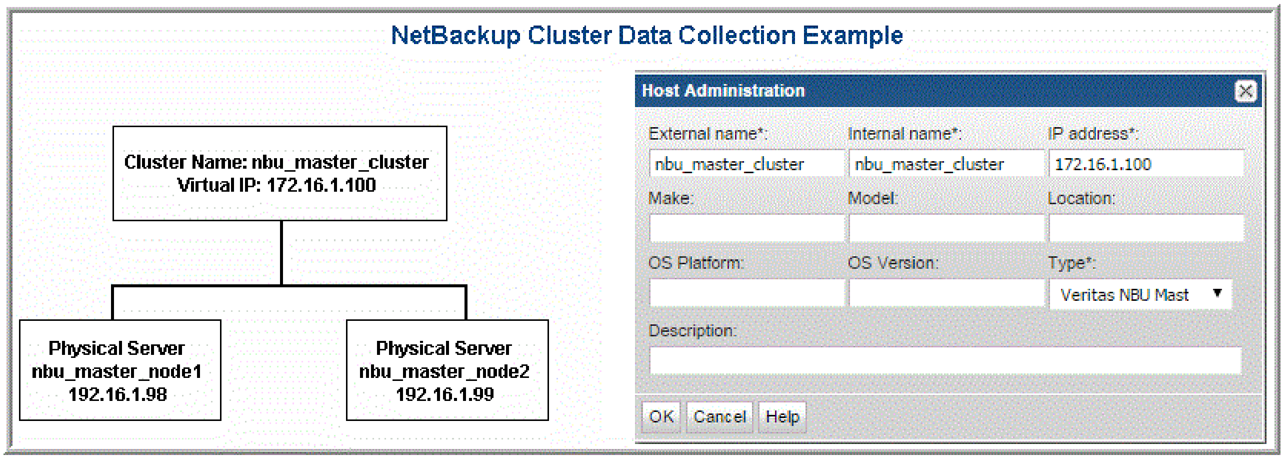
Collecting from NetBackup Clusters

Regardless of your NetBackup data collection architecture—either Centralized or Distributed collection—if your Master Servers belong to a cluster, the Data Collector will communicate with the cluster to gather data from the active Master Server.

Best Practices for Collecting from NetBackup Clusters

- Install the Data Collector on *both* Master Servers in the cluster, but only run the collector on one of them. This enables one server to be the active node while the other server is the failover node.

- Enable the Data Collector only on the active node of the cluster.
- If a Master Server belongs to a cluster, when you add the Data Collector server via the IT Analytics Portal, enter the *NetBackup Cluster Name* for the Internal Name along with the cluster's Virtual IP address.
- See also, Clustered NetBackup Upgrade Procedure.



NetBackup Cluster Data Collection Example

External name*: nbu_master_cluster

Internal name*: nbu_master_cluster

IP address*: 172.16.1.100

Make:

Model:

Location:

OS Platform:

OS Version:

Type*: Veritas NBU Mast ▼

Description:

Clustered NetBackup Upgrade Procedure

For Distributed NetBackup deployments only (Data Collector software is installed on each NetBackup Master Server)

Clustered NetBackup Nodes require a unique upgrade strategy in order to keep their Data Collector versions in synch:

- The active node automatically updates during the Portal upgrade process.
- The passive node requires a manual update.

To ensure that both the active and passive nodes in a clustered pair are operating with the same version of the Data Collector, take the following steps:

1. After a Portal upgrade, the Data Collector automatically updates the NetBackup Master active node to the latest `aptare.jar` version. This process then pushes the update to all the collectors in the policy.
2. Fail over to the passive node in order to make it the active node.
3. At the command line of the newly active node, use the `downloadlib` utility to manually download and update `aptare.jar`.

```
Windows: <Home>\mbs\bin\downloadlib.bat
Linux: <Home>/mbs/bin/downloadlib.sh
```

Note: Check with your Veritas representative to determine if anything needs to be disabled prior to taking this step on the newly active node so that the upgrade does not trigger an event.

Adding a Veritas NetBackup Data Collector Policy

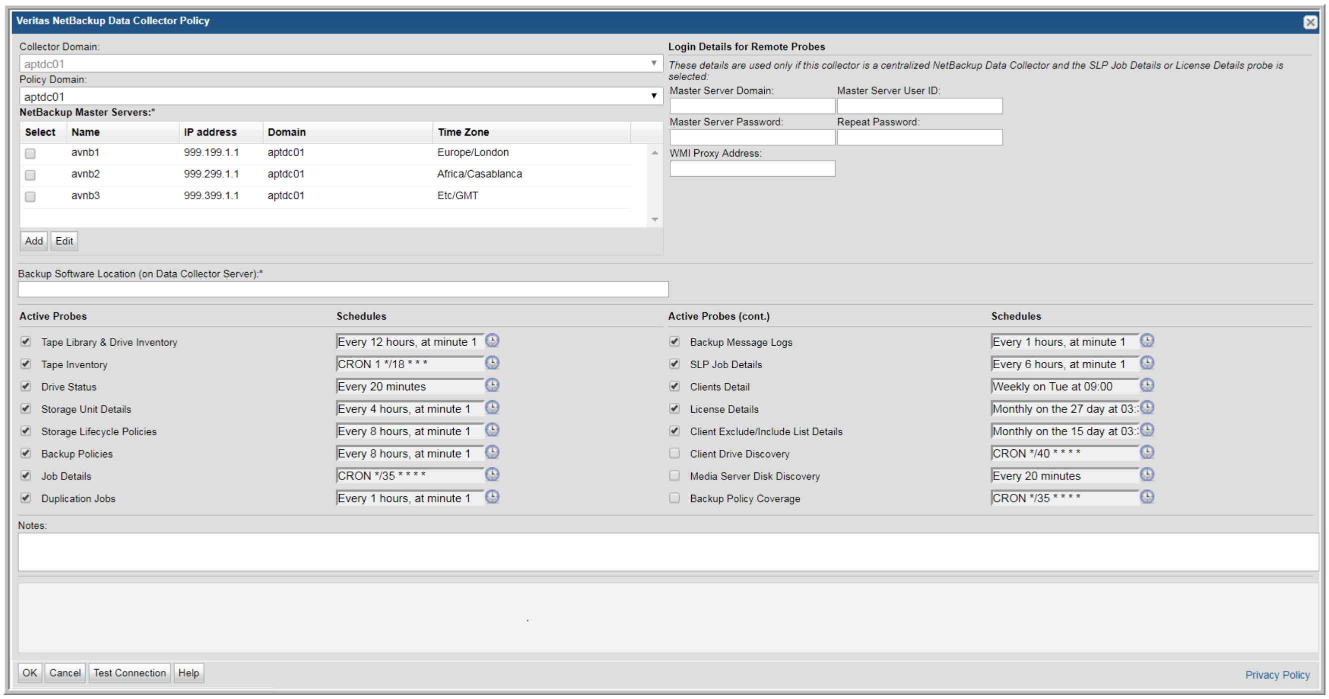
The User ID and Passcode configured in this step will be used later when you install the Data Collector software on the Data Collector server. This configuration enables communication between the Portal and the Data Collector server.

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
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.



Veritas NetBackup Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

NetBackup Master Servers:*

Select	Name	IP address	Domain	Time Zone
□	avnb1	999.199.1.1	aptdc01	Europe/London
□	avnb2	999.299.1.1	aptdc01	Africa/Casablanca
□	avnb3	999.399.1.1	aptdc01	Etc/GMT

Login Details for Remote Probes

These details are used only if this collector is a centralized NetBackup Data Collector and the SLP Job Details or License Details probe is selected:

Master Server Domain:

Master Server User ID:

Master Server Password:

Repeat Password:

WMI Proxy Address:

Backup Software Location (on Data Collector Server):*

Active Probes	Schedules	Active Probes (cont.)	Schedules
☑ Tape Library & Drive Inventory	Every 12 hours, at minute 1	☑ Backup Message Logs	Every 1 hours, at minute 1
☑ Tape Inventory	CRON 1 */18 * * *	☑ SLP Job Details	Every 6 hours, at minute 1
☑ Drive Status	Every 20 minutes	☑ Clients Detail	Weekly on Tue at 09:00
☑ Storage Unit Details	Every 4 hours, at minute 1	☑ License Details	Monthly on the 27 day at 03::
☑ Storage Lifecycle Policies	Every 8 hours, at minute 1	☑ Client Exclude/Include List Details	Monthly on the 15 day at 03::
☑ Backup Policies	Every 8 hours, at minute 1	□ Client Drive Discovery	CRON */40 * * * *
☑ Job Details	CRON */35 * * * *	□ Media Server Disk Discovery	Every 20 minutes
☑ Duplication Jobs	Every 1 hours, at minute 1	□ Backup Policy Coverage	CRON */35 * * * *

Notes:

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

7. Optionally, add/edit a NetBackup Master server from the policy screen. These operations can also be completed in the Inventory.

Field	Description	Sample Value
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.	
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy.	`yourdomain`
NetBackup Master Servers	Select the NetBackup Master Server(s) from which data will be collected. Multi-select is supported. Only available NetBackup Master Servers are displayed. For example, if a server has been decommissioned or it has been selected for use by another policy, it will not be displayed.	
Add	Click **Add** to add a NetBackup server. Added servers are also displayed in the Inventory. See also Adding/Editing NetBackup Master Servers within the Data Collector Policy.	
Edit	Select a server and click **Edit** to update the server values.	
Backup Software Location (on Data Collector Server)	Backup Software Location should be either the root folder or directory where the NetBackup Remote Administration Console for Windows 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 NetBackup: For Windows: C:\Program Files\Veritas. For Linux: /usr/openv.	
Login Details for Remote Probes **These details are only used if this collector is a centralized NetBackup Data Collector and the SLP Job Details probe is selected.**		

Field	Description	Sample Value
Master Server Domain	Specify the domain associated with the NetBackup Master Server User ID. For Windows Master Servers, this domain is used, in conjunction with the User ID, for the execution of the remote lifecycle policies utility (nbstlutil) by the SLP Job Details probe, when the Data Collector is not installed on the NetBackup Master Server; unused for remote Linux Master Servers. In addition, for NetBackup 7.7.3 only, this domain is used by the License Details probe to collect plugin information (bpstsinfo).	
Master Server User ID	Specify the user name with login rights on the selected NetBackup Master Server. The user name and password are used for the execution of the remote lifecycle policies utility (nbstlutil) by the SLP Job Details probe, when the Data Collector is not installed on the NetBackup Master Server. In addition, for NetBackup 7.7.3 only, the credentials are used by the License Details probe to collect plugin information (bpstsinfo). A Windows user name requires administrative privileges.	
Master Server Password	The password associated with the NetBackup Master Server User ID. The user name and password are used for the execution of the remote lifecycle policies utility (nbstlutil) by the SLP Job Details probe, when the Data Collector is not installed on the NetBackup Master Server. In addition, for NetBackup 7.7.3 only, the credentials are used by the License Details probe to collect plugin information (bpstsinfo).	
WMI Proxy Address	Specify the IP address or hostname of the WMI Proxy. If this field is blank, 127.0.0.1 will be used. This is used for remote nbstlutil execution of the SLP Job Details probe, when the Data Collector is not installed on the NetBackup Master Server. In addition, for NetBackup 7.7.3 only, this is used by the License Details probe to collect plugin information (bpstsinfo).	
Active Probes		
Tape Library & Drive Inventory	Select the check box to activate Tape Library data collection from your NetBackup environment. The default polling frequency is every 12 hours. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. Optimize performance by scheduling less frequent collection. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Tape Inventory	Select the check box to activate Tape data collection from your NetBackup environment. The default polling frequency is every 18 hours. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. Optimize performance by scheduling less frequent collection. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Drive Status	Select the check box to activate Tape Drive status collection from your NetBackup environment. The default polling frequency is every 20 minutes. This probe is selected by default.Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Storage Unit Details	Select the check box to activate Storage Unit data collection from your NetBackup environment. The default polling frequency is every 4 hours. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Storage Lifecycle Policies	When selecting this option, you must also configure settings in the **Login Details for Remote Probes s**ection of this Data Collector policy. Select the check box to activate Storage Lifecycle Policy (SLP) collection from your NetBackup environment. The default polling frequency is every 8 hours. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Backup Policies	Select the check box to activate Backup Policy data collection from your NetBackup environment. The default polling frequency is every 8 hours. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Job Details	Select the check box to activate Job data collection from your NetBackup environment. The default polling frequency is every 35 minutes. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Duplication Jobs	Select the check box to activate Duplication Job data collection from your NetBackup environment. The default polling frequency is every 60 minutes. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Backup Message Logs	Select the check box to activate Message Log (bperror) data collection from your NetBackup environment. The default polling frequency is every 60 minutes. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
SLP Job Details	Select the check box to activate SLP Job Details collection from your NetBackup environment. The default polling frequency is every 6 hours. IMPORTANT: When selecting this SLP Job Details option, if you are using centralized NetBackup data collection, you must also configure the settings in the Login Details for Remote Probes section of this Data Collector policy.	
Clients Details	Select the check box to activate Client Details data collection from your NetBackup environment. This probe connects directly to each NetBackup client to collect and persist environmental details. The default polling frequency is once a week. This probe is selected by default. Click the clock icon to modify the schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. The default collection is scheduled to start on Tuesday at 9:00 a.m. **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.	
License Details	Select the check box to activate License Details data collection from your NetBackup environment. This probes collects and persists license key information for NetBackup. The default polling frequency is monthly. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. **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.	
Client Exclude/Include List Details	Select the check box to activate Client Exclude/Include List Details data collection from your NetBackup environment. This probe collects from Linux/Unix and Windows NetBackup clients. This probe connects directly to each NetBackup client to collect and persist the NetBackup client exclude/include list of files and directories. The default polling frequency is monthly. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Client Drive Discovery	**This feature requires a Discovery license**. Therefore, do not check this check box unless you have activated this license. This discovery process seeks out hosts and devices in your environment. The process identifies all hosts in your environment, in particular those that are not currently stored in the reporting database and are therefore potentially not being backed up. This probe uses SNMP to probe for drive utilization; therefore, SNMP must be enabled. The default polling frequency is every 40 minutes. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Media Server Disk Discovery	This discovery process probes all the media servers associated with the management server to gather disk-based information such as capacity and free space on the media server file systems. This information is then displayed in the "*Disk Usage and Performance"* report. If the Media Server Disk Discovery process is not enabled, the disk information will show as **Unknown** in the report. The default polling frequency is every 20 minutes. This probe is selected by default. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	

Field	Description	Sample Value
Backup Policy Coverage	**This feature requires a Discovery license**. Therefore, do not check this check box unless you have activated this license. This discovery process probes all the NetBackup clients known to the database that are associated with the management server. A client is determined to be associated with the management server if it belongs to a policy associated with the management server. This probe uses SNMP to probe for drive utilization; therefore, SNMP must be enabled. View the "Client Protection Summary" report to identify how well your data is being protected. If this report is not in your list of available reports, you do not have a Discovery license. The default polling frequency is every 35 minutes. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.	
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.	
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.	

8. Click **OK** to save the Policy.
9. On the Data Collector server, install/update the Data Collector software.

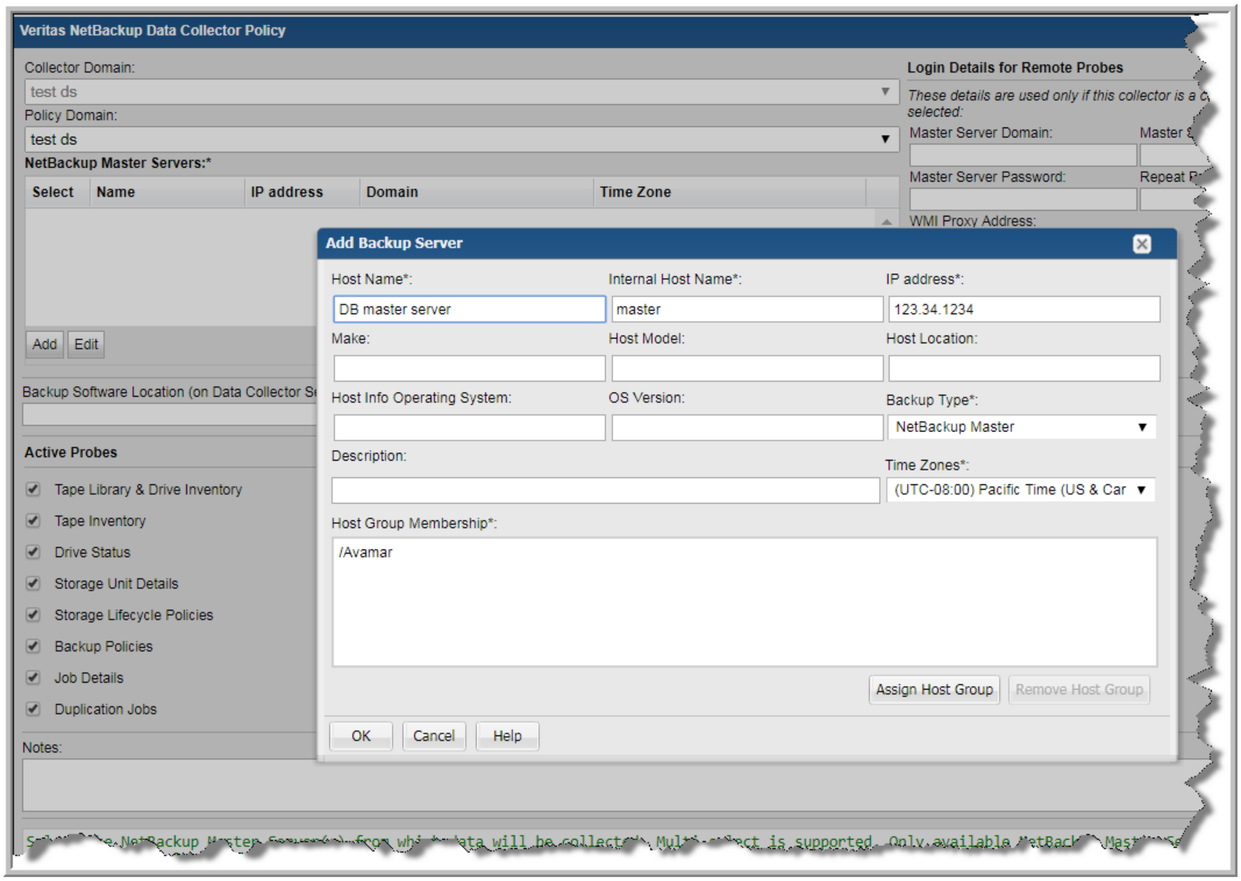
Adding/Editing NetBackup Master Servers within the Data Collector Policy

Add and edit Veritas NetBackup servers directly from the data collector policy screen. These functions are also available from the **Inventory**. See Adding and Editing Hosts and Backup Servers.

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

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

1. Click **Add**.
    - Select a Master Server and click **Edit**.
2. The **Add Backup Server** window is displayed.



Veritas NetBackup Data Collector Policy

Collector Domain: test ds

Policy Domain: test ds

NetBackup Master Servers:*

Select	Name	IP address	Domain	Time Zone

Add Backup Server

Host Name*: DB master server

Internal Host Name*: master

IP address*: 123.34.1234

Backup Type*: NetBackup Master

Time Zones*: (UTC-08:00) Pacific Time (US & Car

Host Group Membership*: /Avamar

Active Probes

- ☑ Tape Library & Drive Inventory
- ☑ Tape Inventory
- ☑ Drive Status
- ☑ Storage Unit Details
- ☑ Storage Lifecycle Policies
- ☑ Backup Policies
- ☑ Job Details
- ☑ Duplication Jobs

3. Enter or update values. Required fields are denoted by *.
    - **Host Name** - Name displayed in the portal. This is a required field.
    - **Internal Host Name** - Must match the host name of the Master Server. If a Master Server belongs to a cluster, enter the *NetBackup Cluster Name* for the Internal Name. See Collecting from NetBackup Clusters. This is a required field.
    - **IP Address** - IP address of the host/backup server. This is a required field.

- **Make, Host Model, Host Location, Host Info Operating System**, and **OS Version**, are optional.
- **Backup Type -** Select Veritas NetBackup Master. The **Time Zones** field is displayed when the server is designated as a Master Server. The Time Zone setting is only available only for a host that is configured as a NetBackup Master.
- **Time Zone -** Select a Time Zone to associate with the NetBackup Master. Whenever the Time Zone is modified, the system marks the Data Collector as *dirty* so that the updates will be pushed to the Data Collector server. If the time zone is not explicitly configured for a NetBackup Master, IT Analytics defaults to the time zone of the Data Collector server. Note that in IT Analytics reports, the date and time displayed for a backup transaction represents the date and time when the event actually happened.

4. Click **Assign Host Group** to select a host group membership. Host group membership is mandatory when creating a backup server. A server can belong to multiple groups. See Managing Host Groups for details.

12

Pre-Installation Setup for Oracle Recovery Manager (RMAN)

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

Prerequisites for Adding Data Collectors (Oracle Recovery Manager - RMAN)

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

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Database Host and Port: Identify the hostname of the server where the database in which the RMAN data resides as well as the port this database is listening on. The default port is 1521.
- The configured user must exist in all configured instances with the same password. The user should the CREATE SESSION privilege and have the following permissions in the schemas to be collected from:
    - User must have the SELECT_CATALOG_ROLE to retrieve RMAN data from the Dynamic Performance (V$) views:

      ```
      GRANT SELECT_CATALOG_ROLE TO <user>;
      ```

    - User requires the RECOVERY_CATALOG_OWNER (or RECOVERY_CATALOG_USER role in Oracle 12c or later) for example:

      ```
      GRANT RECOVERY_CATALOG_OWNER TO <user>;
      ```

      or

      ```
      GRANT RECOVERY_CATALOG_USER TO <user>;
      ```

      or have a virtual private catalog set up for the user (see Oracle documentation).

    - User must have SELECT permission to V$INSTANCE and V$DATABASE (which is included in SELECT_CATALOG_ROLE).

Installation Overview (Oracle Recovery Manager - RMAN)

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

1. Update the Local Hosts file. This enables Portal access. See Updating the Local Hosts File for Data Collection.
2. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
3. In the Portal, add the Oracle Recovery Manager (RMAN) data collector policy. See Add an Oracle Recovery Manager (RMAN) Data Collector Policy
4. On the Data Collector Server, install the Data Collector software. See Data Collector Installation.
5. Validate the Data Collector Installation. See Validating Data Collection.

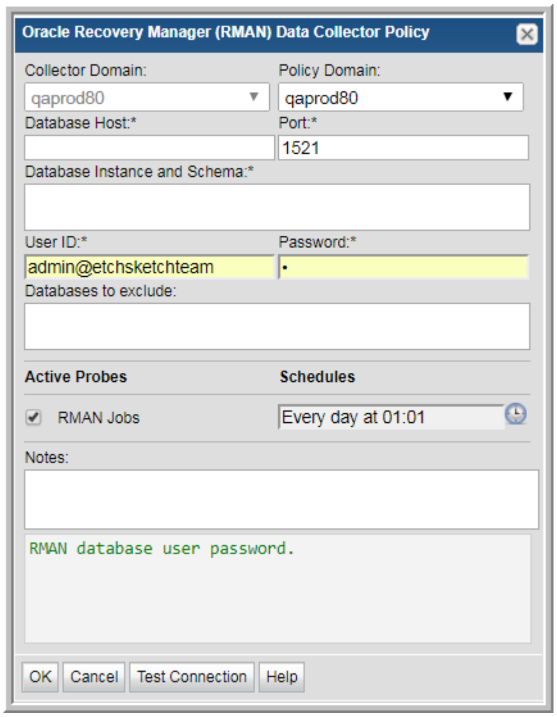
Add an Oracle Recovery Manager (RMAN) Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



Oracle Recovery Manager (RMAN) Data Collector Policy

Collector Domain: qaprod80

Policy Domain: qaprod80

Database Host:*

Port:* 1521

Database Instance and Schema:*

User ID:* admin@etchsketchteam

Password:* •

Databases to exclude:

Active Probes	Schedules
☑ RMAN Jobs	Every day at 01:01

Notes:

RMAN database user password.

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

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

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Database Host	RMAN database server.
Port	Database listener port. By default the port is 1521.
Database Instance and Schema	RMAN database instance names and optional schemas, each formatted as INSTANCE.SCHEMA and separated by commas or spaces. If a schema is not specified then all Recovery Catalog schemas in the instance accessible to the user ID will be collected. If there are no accessible Recovery Catalog schemas then the Dynamic Performance (V$) views will be collected. Use the PUBLIC schema to force collection from the V$ views, or a Recovery Catalog schema name to only collect from that schema. Example (to collect both from a Recovery Catalog schema and the V$ views in the DB1 instance): DB1.RMAN, DB1.PUBLIC
User ID*	This field is required. RMAN database user name. This must be a user with SELECT permission for the Dynamic Performance (V$) views and any Recovery Catalog schema views being collected from.
Password*	This field is required. RMAN database user password.
Databases to exclude	RMAN numeric database IDs to exclude from collection, separated by commas or spaces.
Active Probes	
RMAN Jobs	Probe for Oracle Recovery Manager (RMAN) jobs.
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

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

13

Pre-Installation Setup for Rubrik Cloud Data Management

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

Prerequisites for Adding Data Collectors (Rubrik Cloud Data Management)

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

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Read-only Rubrik user account

Installation Overview (Rubrik Cloud Data Management)

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

1. Update the Local Hosts file. This enables Portal access. See Updating the Local Hosts File for Data Collection.
2. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
3. In the Portal, add the Rubrik Cloud Data Management data collector policy. See Add a Rubrik Cloud Data Management Data Collector Policy
4. On the Data Collector Server, install the Data Collector software. See Installing the Data Collector.
5. Validate the Data Collector Installation. See Validating Data Collection.

Add a Rubrik Cloud Data Management Data Collector Policy

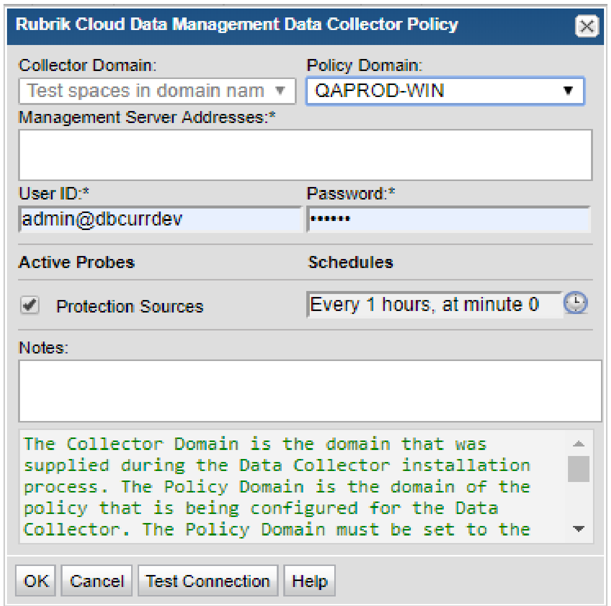
- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE Certified Configurations Guide*.
- **After adding 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.

•



Rubrik Cloud Data Management Data Collector Policy

Collector Domain: Test spaces in domain nam

Policy Domain: QAPROD-WIN

Management Server Addresses:*

User ID:* admin@dbcurrdev

Password:* ••••••

Active Probes | Schedules

☑ Protection Sources | Every 1 hours, at minute 0

Notes:

```
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
```

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

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

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more Cloud Data Management's server IP addresses or host names to probe. Comma-separated addresses are supported, e.g. 192.168.1.10, myhost NOTE: To collect from a Cluster, enter the IP address of only one of the management servers.
User ID*	Read-only userID for the Rubrik Cloud Data Management system.
Password*	Password for the Rubrik Cloud Data Management system. The password associated with the User ID.
Protection Sources	Probe for Rubrik Cloud Data Management Protection Details.
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

14

Pre-Installation Setup for Veeam Backup & Replication

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

Prerequisites for Adding Data Collectors (Veeam Backup & Replication)

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

- 64-bit OS. See the *APTARE Certified Configurations Guide* for supported operating systems.
- Support Java Runtime Environment (JRE) 10.0.2.
- For performance reasons, APTARE recommends that you do not install Data Collectors on the same server as the IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Requires a Microsoft Windows Data Collector server
- Requires Microsoft PowerShell 4.0 or above. Veeam Backup & Replication comes with a PowerShell extension - a snap-in to Microsoft Windows PowerShell. The Veeam Backup PowerShell snap-in enables most operations that are available in the user interface.
- **Veeam Requirement**: User credentials with a Veeam Backup Administrator role are required to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in.
- Veeam Backup & Replication Console (version 9.5.x) must be installed on the system where the Data Collector service is running.
- Default port is 9392.

Verifying Data Collector Servers can Connect to Veeam Servers

Basic PowerShell Commands for Veeam

- **Add Veeam Snapin**

```
Add-PSSnapin -PassThru VeeamPSSnapIn
```

- **Connect to Veeam Backup Server**

```
Connect-VBRServer -User <user> -Password <password> -Server <server>
```

- **Disconnect from Previous Connection**

```
Disconnect-VBRServer
```

Verification Steps

In this section, we'll use a scenario to illustrate the verification steps. The task is to connect to Veeam Servers *Server-A* and *Server-B* from the same Veeam Data Collector Server, where the Veeam Backup & Replication Console is installed.

1. From Microsoft PowerShell Console (in Administrator mode), add Veeam SnapIn.

   ```
   Add-PSSnapin -PassThru VeeamPSSnapIn
   ```

2. Log into the Veeam Backup & Replication Console using *Server-A* credentials.

3. Open a PowerShell Console and connect to *Server-A*.

   ```
   Connect-VBRServer -User ServerAUserId -Password ServerAPassword -Server Server-A
   ```

   The *Server -A* connection should be successful.

4. Open a PowerShell Console and disconnect from *Server-A*.

   ```
   Disconnect-VBRServer
   ```

5. Open a PowerShell Console and connect to *Server-B*.

   ```
   Connect-VBRServer -User ServerBUserId -Password ServerBPassword -Server Server-B
   ```

If the *Server-B* connection is successful, it means: both Servers are on the same software version (including minor patch releases/ updates).

If the *Server-B* connection fails with the following error:

```
Connect-VBRServer: Cannot connect to backup server because some of its components are out
of date.
```

it means: *Server-A* and *Server-B* are on different software versions. The Veeam Backup & Replication Console is only in sync with *Server-A*.

Known Issues and Limitations (Veeam Backup & Replication)

- **Backup File Names**

  Veeam allows a backup job to have different backup and retention policies. For certain configuration types such as, *Synthetic Full Backup* or *Forever Forward Incremental Backup Retention Policy,* one of the *.vib files is renamed as *.vbk at regular intervals by Veeam. In APTARE IT Analytics, the Veeam Data Collector retrieves backup information for a specified period of time at regular intervals. This set of backup information may contain file names with a *.vib extension (instead of *.vbk) and display in the Job Details report.

  For details about the various use cases, see https://helpcenter.veeam.com/docs/backup/vsphere/backup_files.html?ver=95.

  As you compare APTARE IT Analytics reports to native Veeam reports, if there are discrepancies in the files, you can force a historic data collection to examine the details. Additionally, when validating IT Analytics reports against Veeam reports, focus on the file names and not the file extensions.

- **Successful Endpoint Backup Jobs Displaying Size = 0.00 Bytes**

  Occasionally, Veeam will create additional maintenance jobs such as *Full backup file merge completed successfully* and there is not a data size associated with the job. These jobs will be displayed with a status of *Successful* but without an associated data size.

- **Veeam Collection does not support collection of jobs or backup data which are based on VMware Tags**.

Installation Overview (Veeam Backup & Replication)

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

1. Update the Local Hosts file. This enables Portal access. See Updating the Local Hosts File for Data Collection.
2. In the Portal, add a Data Collector, if one has not already been created. See Adding/Editing Data Collectors.
3. In the Portal, add the Veeam Backup & Replication data collector policy. See Add a Veeam Backup & Replication Data Collector Policy
4. On the Data Collector Server, install the Data Collector software. See Data Collector Installation.
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).
6. Validate the Data Collector Installation. See Validating Data Collection.

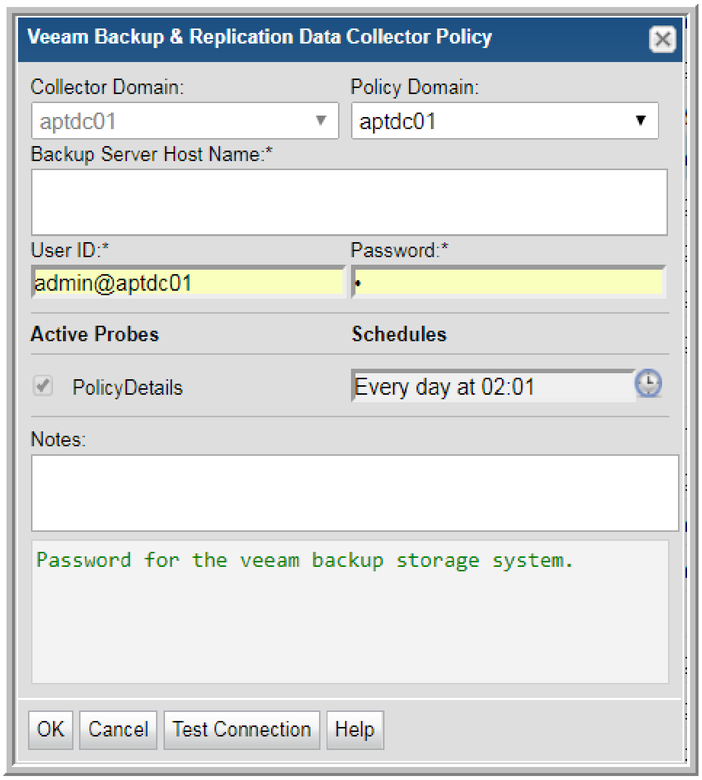
Add a Veeam Backup & Replication Data Collector Policy

- **Before adding the policy**: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the *APTARE 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. See Navigating with Search.
3. Select a Data Collector from the list.
4. Click **Add Policy**, and then select the vendor-specific entry in the menu.



Veeam Backup & Replication Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Backup Server Host Name:*

User ID:* admin@aptdc01

Password:* •

Active Probes | Schedules

☑ PolicyDetails | Every day at 02:01

Notes:

```
Password for the veeam backup storage system.
```

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

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Backup Server Host Name*	One or more Veeam Backup Server Host Names to probe. IP Address is not supported. Comma-separated host names are supported. Example, VeeamServer1, VeeamServer2.
Time Zone	Select the time zone of Veeam Backup Server. By default, the data collector server time zone is used.
User ID*	View only User ID for Veeam Backup Server. To include a domain name use the format DOMAIN\USERNAME.
Password*	Password for Veeam Backup Server associated with the User ID.
Active Probes	
Client Details	Probe for collecting clients to be backed up using Veeam Backup & Replication.
Job Details	Probe for collecting jobs scheduled for Veeam Backup & Replication.
Session and Backup Details	Probe for collecting session details and backups created by Veeam Backup & Replication.
Schedule	Click the clock icon to create a schedule. By default, it is collected at 4:04 am daily. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

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

15

Discovery Policies for Veritas NetBackup

Task Overview: Configuring and Monitoring Discovery Policies

To configure Discovery, perform the following sequence of steps:

	Task	For Instructions
1.	Learn about how Discovery policies can help you protect your data.	Discovery Policies Overview
2.	Purchase and activate your Discovery license. Two of the three Discovery processes require a license: • Client Drive Discovery • Backup Policy Coverage	Activate a Discovery License
3.	Enable SNMP, if you are enabling these Discovery types: • Client Drive Discovery • Backup Policy Coverage	Enable SNMP for Discovery
4.	Determine the master server that requires the policy that you are about to create, and identify the Discovery type(s) that you want to enable on this master server.	About Discovery Types
5.	Create Discovery policies via Discovery Administration. **Admin > Reports > NetBackup Discovery**	Create and Edit Discovery Policies
6.	If necessary, exclude specific network devices from your policies.	Exclude Devices from Discovery Policies
7.	Turn on Discovery probes in the NetBackup Data Collector policy.	Activate Discovery Probes in the NetBackup Data Collector Policy
8.	Regularly monitor the status of Discovery processes.	Monitor Discovery Processes
9.	View the *Client Protection Summary* report to see how well your data is being protected.	View Client Protection Status
10.	If significant changes in your environment warrant a fresh view, rebuild the Discovery database.	Reset Discovery Data
11.	Tune Discovery by modifying time out settings for probes.	See the *APTARE System Administrator's Guide* for details.

Discovery Policies Overview

The Discovery module, specific to Veritas NetBackup, uses Discovery policies to illuminate risk and exposure within the corporate IT backup and recovery environment. The Discovery module is a separately licensed feature. See About Discovery Types and Activate a Discovery License.

Discovery policies provide answers to the following questions:

- Where is my data protected? (for example, disk-to-disk, disk-to-tape, or disk-to-disk-to-tape)
- What is the extent and coverage of my data protection?
- Are *all* my clients and applications protected?
- Is every data set on every client and every application protected?

Discovery finds hosts on a corporate network and compares those hosts with the policies of the underlying backup and recovery software. Discovery performs the following steps:

1. Identifies orphan clients that are not being protected.
2. Probes and determines the file systems or drives of the hosts.
3. Compares and contrasts the file systems to the equivalent policies within the underlying backup and recovery software.

Use Discovery policies if:

- Your IT infrastructure, applications, and servers are rapidly changing.
- Your backup solution cannot detect your backup servers and cannot provide information about successful or unsuccessful backups.

About Discovery Types

Three different Discovery types can be configured to collect additional NetBackup data. To configure and manage Discovery, see *Create and Edit Discovery Policies*.

Client Drive Discovery

- *This feature requires a Discovery license and SNMP*. This Discovery process seeks out hosts and devices in your environment. The process identifies all hosts in your environment, in particular those that are not currently stored in the reporting database and are therefore potentially not being backed up. This probe uses SNMP to probe the IP address range for drive utilization; therefore, SNMP must be enabled.

Media Server Disk Discovery

- This Discovery process probes all the media servers associated with the management server to gather disk-based information such as capacity and free space on the media server file systems. This information is then displayed in the *Disk Usage and Performance* report. If the Media Server Disk Discovery process is not enabled, disk-based information will show as `Unknown` in reports. If you have several master servers in your environment, and they have media servers and disk storage units attached to them, you must enable the Media Server Disk Discovery module on each of the master servers.

Backup Policy Coverage

- *This feature requires a Discovery license and SNMP*. This Discovery process, probes all the NetBackup clients known to the NetBackup database that are associated with the management server. It queries NetBackup to discover if there are backup policies that cover the client. A client is determined to be associated with the NetBackup management server if it belongs to a policy associated with the management server. This probe uses SNMP to probe for drive utilization; therefore, SNMP must be enabled.

Activate a Discovery License

You need to activate your Discovery license so that you can access the additional discovery features beyond the Media Server Disk Discovery component.

A Discovery license is required for the following Discovery types:

- Client Drive Discovery
- Backup Policy Coverage

To activate the Discovery license:

1. Go to the utilities directory.

   Linux: `/opt/aptare/utils`

   Windows: `C:\opt\aptare\utils`

2. Run the following license utilities to view the status of your current license or to install your updated license.

   Linux:

   ```
   ./printLicense.sh
   ./installLicense.sh
   ```

   Windows:

   printlicense.bat

   installlicense.bat

Create and Edit Discovery Policies

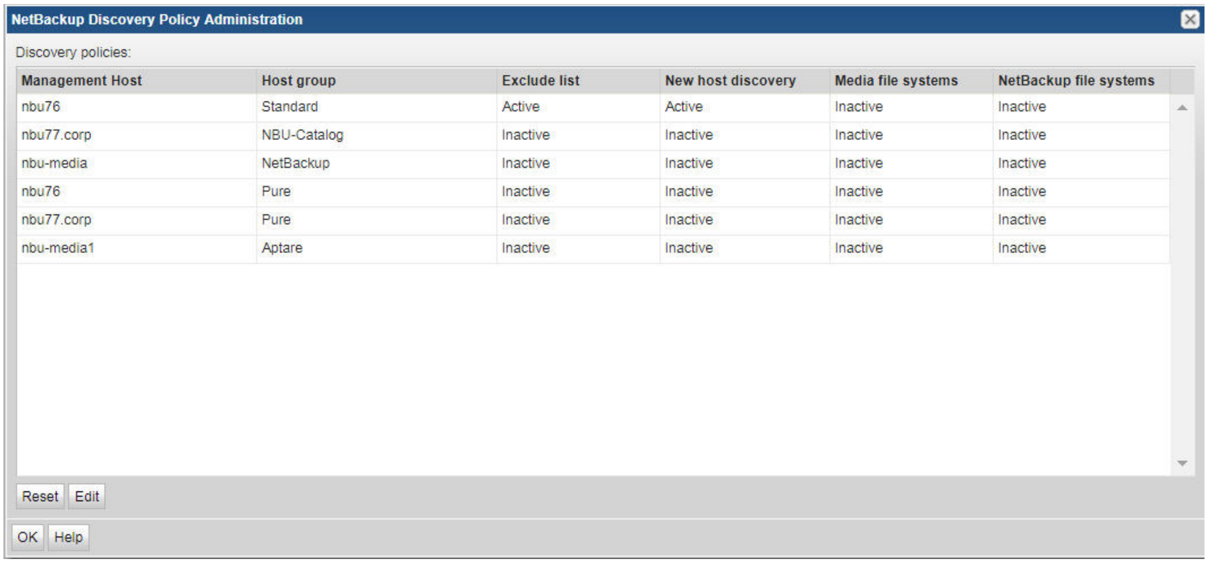
Discovery is a policy-based module that enables you to tune and configure parameters for the Discovery engine. You must create a Discovery policy for each Veritas NetBackup master server and for each Discovery type that you want to enable on them.

Discovery policies are executed on the master servers at intervals that you can set. Although the values that you specify for these "wake-up" intervals reside in a configuration file, APTARE recommends that you update these intervals via the Portal, not the configuration file.

For additional information, see *Discovery Policies Overview* and *About Discovery Types*.

To create Discovery policies

1. Determine the master server that requires the policy that you are about to create.
2. Select **Admin** > **Reports** > **NetBackup Discovery** to display the list of master servers in the Discovery Administration window.



NetBackup Discovery Policy Administration

Discovery policies:

Management Host	Host group	Exclude list	New host discovery	Media file systems	NetBackup file systems
nbu76	Standard	Active	Active	Inactive	Inactive
nbu77.corp	NBU-Catalog	Inactive	Inactive	Inactive	Inactive
nbu-media	NetBackup	Inactive	Inactive	Inactive	Inactive
nbu76	Pure	Inactive	Inactive	Inactive	Inactive
nbu77.corp	Pure	Inactive	Inactive	Inactive	Inactive
nbu-media1	Aptare	Inactive	Inactive	Inactive	Inactive

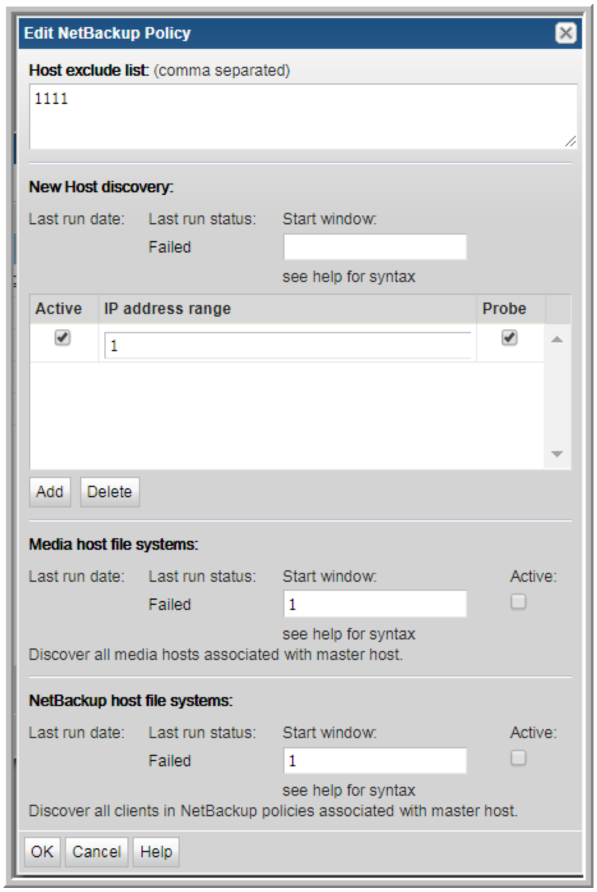
3. Select a Management Server and click **Edit**. You also can double-click the server.

   Three Discovery processes can be scheduled via this Discovery Administration window:

   New server discovery: See Client Drive Discovery.

   Media server file systems: See Media Server Disk Discovery.

   NetBackup server file systems: See Backup Policy Coverage.



Host exclude list: (comma separated)

1111

New Host discovery:

Last run date: Last run status: Start window:

Failed

see help for syntax

Active	IP address range	Probe
☑	1	☑

Media host file systems:

Last run date: Last run status: Start window: Active:

Failed 1 □

see help for syntax

Discover all media hosts associated with master host.

NetBackup host file systems:

Last run date: Last run status: Start window: Active:

Failed 1 □

see help for syntax

Discover all clients in NetBackup policies associated with master host.

4. Set the times that specify when the Discovery process will be executed.

The format for the time:

* **minutes**	* **hours**	* **day of month**	* **month**	* **day of week**

Table 1 lists the allowed values and Table 2 lists the default values.

Field	Values
minutes	0-59
hours	0-23
day of month	1-31
month	1-12
day of week	1-7 (1 is Sunday)
A field may also be an asterisk (*), which means the full range - i.e. “first” to “last”.	

Table 1 Allowed Values for Discovery Types

When configuring the start window, you need to consider the wake-up period of the Discovery processes. If you configure a window of “* 2-3 1 * *” (that is, between 2 and 3 am on the first day of each month) for the

New Server Discovery process, the process might run twice if it wakes up at 2am, takes 15 minutes to execute, sleeps for 40 minutes, then wakes up again at 2:55am. Since the start window is still active at 2:55am, it will run again.

Discovery Type	Wake-up Time	Start Window
New Server Discovery	40 minutes	* 14-15 * * 1 (Every Monday, between 2 and 3pm)
Media Server Discovery	20 minutes	* * * * * (Anytime - i.e. runs every 20 minutes)
NetBackup Client File Systems	35 minutes	* 16-17 * * 1 (Every Monday, between 4 and 5pm)

Table 2 Default Values for Discovery Types

5. For each device that Discovery should probe:

   a In the Discovery Administration window, click **Add** to add a device or select device and click **Edit**.

   b In the IP address range field, enter either a single IP address or an IP address range.

   An IP range is in the format nnn-nnn (For example: 172.16.100-110.1-255 covers 11*255 = 2805 IP addresses). Multiple ranges can be added and each range can be independently activated or deactivated via the **active** check box.

   The Media Server Discovery Policy automatically generates the list of devices to probe— essentially all media servers associated with the management server. Similarly, the NetBackup Server File System Discovery Policy automatically generates the list of servers to probe by finding all servers contained in policies on that management server.

6. Click **OK** to save your settings.

Exclude Devices from Discovery Policies

An exclude list is a list of names or IP addresses that will not be probed by any of the Discovery policies configured for a given management server. Each management server maintains its own exclude list.

To exclude devices from Discovery policies

1. In the **Discovery Administration** window, enter a comma-separated list of the IP addresses that you want to exclude.

2. Click **OK**.

Activate Discovery Probes in the NetBackup Data Collector Policy

The NetBackup Data Collector Policy lists probes that can be turned on to collect different types of data. Three of these probes are specific to Discovery.

- Client Drive Discovery
- Media Server Disk Discovery
- Backup Policy Coverage

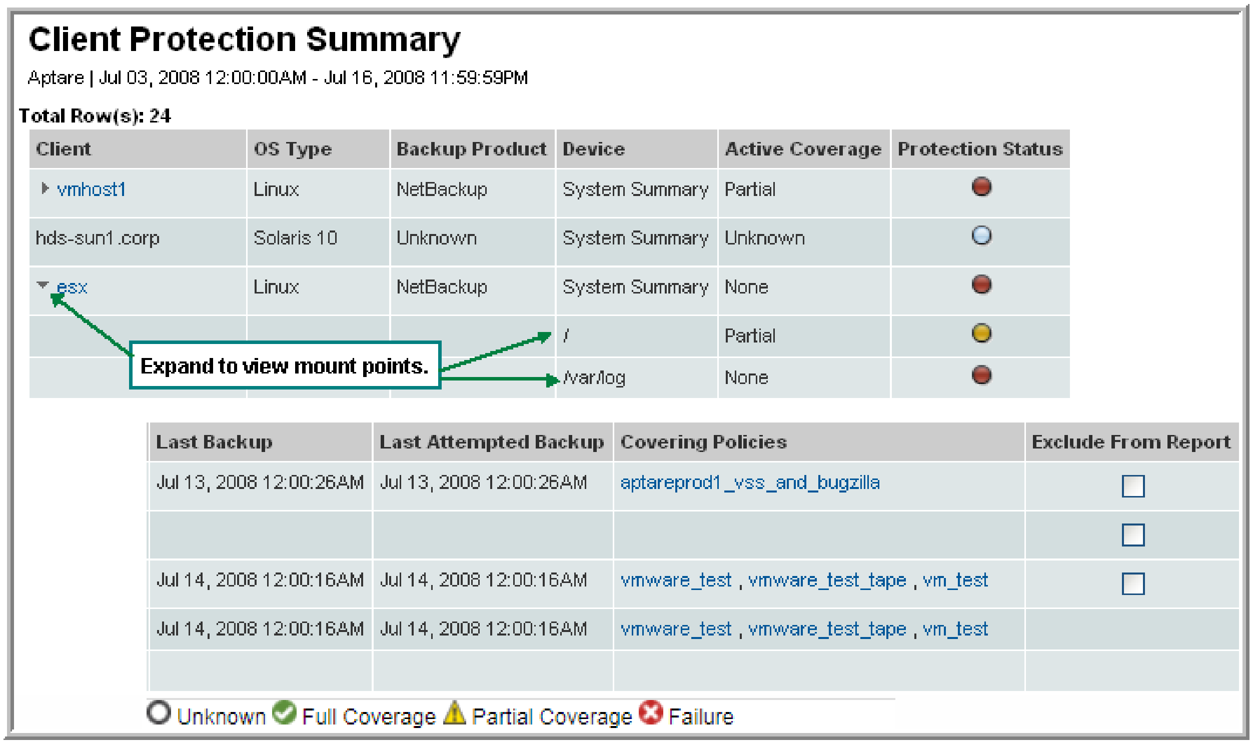
Monitor Discovery Processes

To monitor a Discovery process

1. From the Portal toolbar, view the Discovery Administration window by selecting **Admin > Reports > Discovery Policies**.
   - **Inactive**. Indicates that there are currently no active policies for the particular Discovery process.
   - **Active**. Indicates that there is at least one active policy for the particular Discovery process. To access the individual Discovery processes, click on the management server row.
2. For each active policy, double-click on the management server that is responsible for running a particular policy.
3. Using the `last run status` field, determine the status of the Discovery process that last ran:
   - **Failed**. Indicates a problem during the execution of the policy or a problem with saving the data to the Reporting Database. Check the `mbs/logs/crontab.log` file for detailed information about the failure.
   - **Partial**. Indicates one or more probes time out and a response was not received.

View Client Protection Status

The *Client Protection Summary* report provides a view of the protection status of clients that you think are being backed up by NetBackup.



Client Protection Summary

Aptare | Jul 03, 2008 12:00:00AM - Jul 16, 2008 11:59:59PM

Total Row(s): 24

Client	OS Type	Backup Product	Device	Active Coverage	Protection Status
▸ vmhost1	Linux	NetBackup	System Summary	Partial	🔴
hds-sun1.corp	Solaris 10	Unknown	System Summary	Unknown	○
▾ esx	Linux	NetBackup	System Summary	None	🔴
			/	Partial	🟡
			/var/log	None	🔴

Expand to view mount points.

Last Backup	Last Attempted Backup	Covering Policies	Exclude From Report
Jul 13, 2008 12:00:26AM	Jul 13, 2008 12:00:26AM	aptareprod1_vss_and_bugzilla	□
			□
Jul 14, 2008 12:00:16AM	Jul 14, 2008 12:00:16AM	vmware_test , vmware_test_tape , vm_test	□
Jul 14, 2008 12:00:16AM	Jul 14, 2008 12:00:16AM	vmware_test , vmware_test_tape , vm_test	

○ Unknown ✓ Full Coverage ⚠ Partial Coverage ✖ Failure

See the *APTARE Report Reference Guide* for details about this report.

Reset Discovery Data

When Discovery processes execute, they collect information on discovered devices and store this information in the Reporting Database. When you reset the Discovery data, you purge all this information from the Reporting Database and reset the *Client Protection Summary* report. The data re-populates the next time the Discovery processes run.

Consider resetting your Discovery data if any of the following conditions are true:

- If your initial Discovery policy was too broad, and included devices that were in a DHCP range. This policy configuration could result in potentially large numbers of IP addresses showing up in the *Client Protection Summary* report thereby diminishing the effectiveness of the report.
- If previously discovered clients no longer exist in your environment, but are still showing in the *Client Protection Summary* report.
- If a file system on a previously discovered client had subsequently been removed, and is still showing up in the *Client Protection Summary* report.

By resetting the Discovery data, you can start over and rebuild a fresh list of discovered devices and file systems. A reset only impacts the *Client Protection Summary* report. A reset does not affect any of the other collected backup data that is used in all other reports.

Why Enable SNMP?

Note: The information contained in this section is intended for the administration of Discovery functionality. APTARE provides this SNMP configuration guidance for informational purposes only. APTARE Global Support Services will not provide assistance with the installation, configuration, and troubleshooting of SNMP subsystems on your Master Servers.

The Simple Network Management Protocol (SNMP) is an Internet standard that provides a common way to query, monitor, and manage devices connected to IP networks. The protocol is defined in RFC 2571. For additional information, see http://www.ietf.org/rfc/rfc2571.txt.

To capture filesystem level information on your media servers and any other servers in your environment, you must enable SNMP.

Using SNMP v2c messaging, Discovery queries all media servers and other servers or devices and retrieves information about the physical attributes of their configured storage units and file systems. The SNMP probe uses UDP and the standard SNMP Port 161 by default.

There are different SNMP probes for different operating systems. The way that you enable and configure SNMP services on your servers to take advantage of these probes depends on your operating system.

- Windows
- Red Hat Linux
- HP-UX
- Solaris 8/9
- Solaris 10

About SNMP Probes

To take full advantage of the Discovery functionality, the SNMP subsystem must be configured to respond to the following probes:

First Probe (sysObjectOID)

This probe is sysObjectOID (.1.3.6.1.2.1.1.2). This probe returns an OID that conforms to the enterprise OIDs allocated by the Internet Assigned Numbers Authority. Be aware that the SNMP agent resident on the device returns this number, and this number might not be the same number as the hardware manufacturer. For example an HP N-class server may return the enterprise OID of 1.3.6.1.4.1.11 or 1.3.6.1.4.1.2021.250.14 depending on whether the SNMP agent is provided by HP or is the open source NET-SNMP package. The number returned is matched against a lookup table to try and determine the company value of the OID. (For example, IBM or Sun).

Second Probe (sysDescr OID)

This probe is made for the sysDescr OID (.1.3.6.1.2.1.1.1). This probe returns a description of the device or agent. This string is matched against a lookup table to try and determine the system description value. (For example, Windows 2000 or Solaris).

Lastly, if configured, a query is made against the Device and Storage section of the Host Resources Management Information Block (MIB). Specific information retrieved is the file system mount point, storage type, storage description, allocation units, size in storage units, and storage units used. Before this information is returned, calculations are made to convert the values into kilobytes. Only fixed disk storage units are returned.

Enabling SNMP for Windows (NT/2000/XP)

This procedure assumes that you have Windows 2000/XP. However, the process is very similar on Windows NT. For more information about setting up SNMP on Windows, go to the following Microsoft articles:

- *How To Configure Security for a Simple Network Management Protocol Service in Windows 2000 (*http://support.microsoft.com/default.aspx?scid=KB;EN-US;q315154*)*
- *SNMP Storage Information Is Not Updated Dynamically (*http://support.microsoft.com/kb/q295587/*)*
- *Management information base support in Windows 2000, Windows XP, Windows Server 2003, and Windows Vista (*http://support.microsoft.com/kb/q237295/*)*

To install the SNMP on Windows 2000/XP:

You might need to install the CD for your operating system, so have the recovery CD available.

1. Click **Start** > **Settings** > **Control Panel.**
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Click **Management and Monitoring Tools** and click **Details**.

   The Management and Monitoring Tools window appears.
5. Select **Simple Network Management Protoco**l check box and click **OK**.
6. Click **Next** to initiate the installation.
7. After the installation completes and from the Control Panel, double-click on **Administrative Tools**.
8. Double-click on **Computer Management**.
9. In the navigation tree on the left, expand Services and Applications, then click on **Services**.
10. In the Services contextual frame, scroll down to SNMP Service, then double-click **SNMP Service**.
11. In the General tab, select **Automatic** for Startup Type.

12. In the Security tab, do one of the following:
    - Leave the default community name public.
    - To improve security, choose your own name. Click on Add... for accepted community names, leave Community Rights as Read-Only, pick a secure Community Name, and click on OK. Remove the public entry. Modify the default Discovery properties configuration file to match this value.
13. In the Security tab, choose which IP addresses can access the SNMP service. You must choose at least the IP address of the Master Server that runs APTARE IT Analytics.
14. In the Agent tab, specify the values for all fields, and select the Internet check box to make all SNMP values available.

Enabling SNMP for Red Hat Linux

Red Hat Linux has an SNMP agent, ucd-snmp, preinstalled. Ucd-snmp is the pre-cursor to net-snmp. You need to configure the ucd-snmp agent to return the host resource information and to ensure that it executes at system startup. This procedure provides the steps for enabling SNMP in a Red Hat Linux environment.

To enable SNMP for Red Hat Linux:

1. Locate the SNMPD configuration file in /etc/snmp/snmpd.conf and the executable at /usr/sbin/snmpd.
2. Configure the SNMP agent as shown in the following example, which shows read-only access to the system and host resource storage portions of the MIB.

```
####
# First, map the community name "public" into a "security name"
# sec.name source community
com2sec notConfigUser default public
####
# Second, map the security name into a group name:
# groupName securityModel securityName
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser
####
# Third, create a view for us to let the group have rights to:
# name incl/excl subtree mask(optional)
#view systemview included .1
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.system fe
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.host.hrStorage ff
view APTARE IT Analytics included
.iso.org.dod.internet.mgmt.mib-2.host.hrDevice ff
# .iso.org.dod.internet.mgmt.mib-2.system = .1.3.6.1.2.1.1
# .iso.org.dod.internet.mgmt.mib-2.host.hrStorage = .1.3.6.1.2.1.25.2
####
# Finally, grant read-only access to the system and storage portions of
```

```
the MIB2 tree
# group context sec.model sec.level prefix read write
notif
#access notConfigGroup "" any noauth exact systemview none
none
access notConfigGroup "" any noauth exact APTARE IT Analytics
none none
```

Enabling SNMP for HP-UX

Although HP-UX 11.00 has an SNMP agent installed, it does not provide access to the Host Resource MIB, so Discovery cannot use this agent to find storage units. However, net-snmp is supported on HP-UX 10.20, 11.00 and 11.11.

To install and configure SNMP for HP-UX 11.00:

1. Read the Net-SNMP HP-UX README.
2. Download and the net-snmp binaries
3. Install the net-snmp binaries. For an example, go to Example—Installing Net-SNMP.

Enabling SNMP for Solaris 8/9

The Solstice Enterprise Agent does not support the Host Resource MIB, so Discovery cannot use this agent to find storage units. However, net-snmp is supported on Solaris 5.6, 5.7, 5.8, and 5.9.

To install and configure SNMP for Solaris:

1. Read the Net-SNMP Solaris README.
2. Download and the net-snmp binaries. For an example, go to Example—Installing Net-SNMP.
3. Install the net-snmp binaries. For an example, go to Example—Installing Net-SNMP.

Enabling SNMP for Solaris 10

The Solaris System Management Agent (SMA) is an SNMP agent that Sun Microsystems offers, and it is based on the Net-SNMP open source implementation version 5.0.9.

To install and configure SNMP for Solaris 10:

1. Install the SMA packages just as you would install bundled products as outlined in the *Solaris 10 Installation Guide: Basic Installations and in the Solaris 10 Installation Guide: Custom JumpStart and Advanced Installations*.
2. Configure the SMA agent as outlined in the *Solaris System Management Agent Administration Guide*.

Troubleshooting

If you have problems installing and configuring SMA, go to SunSolve.

Example—Installing Net-SNMP

Net-SNMP is an open source implementation of the Simple Network Management Protocol.

Net-SNMP provides an extensible agent for responding to SNMP queries for management information, and this functionality is important to the Media Discovery module Net-SNMP includes built-in support for a wide range of MIB information modules, specifically the Host Resource MIB. Net-SNMP is available for many Linux and Linux-like operating systems and also for Microsoft Windows, though functionality can vary depending on the operating system.

To install net-snmp:

1. Download and install Perl 5.6 or above, if the package is not already installed.
2. Install net-snmp as outlined in the following example:

```
# /usr/local/bin/snmpconf -g basic_setup
*** Beginning basic system information setup ***
Do you want to configure the information returned in the system MIB group
(contact info, etc)? (default = y): no
Do you want to properly set the value of the sysServices.0 OID (if you don't know, just
say no)? (default = y): no
*** BEGINNING ACCESS CONTROL SETUP ***
Do you want to configure the agent's access control? (default = y):
Do you want to allow SNMPv3 read-write user based access (default = y): no
Do you want to allow SNMPv3 read-only user based access (default = y): no
Do you want to allow SNMPv1/v2c read-write community access (default = y): no
Do you want to allow SNMPv1/v2c read-only community access (default = y): yes
Configuring: rocommunity
Description:
a SNMPv1/SNMPv2c read-only access community name arguments: community [default|hostname|
network/bits] [oid]
The community name to add read-only access for: public
The hostname or network address to accept this community name from [RETURN for all]:
The OID that this community should be restricted to [RETURN for norestriction]:
Finished Output: rocommunity public
Do another rocommunity line? (default = y): no
*** Beginning trap destination setup ***
Do you want to configure where and if the agent will send traps? (default= y): no
*** Beginning monitoring setup ***
Do you want to configure the agent's ability to monitor various aspects of your system?
(default = y): no
The following files were created:
snmpd.conf
```

3. Move the **snpd.conf** file to one of the following locations:
   - If you want this file used by everyone on the system, moved the file to **/usr/local/share/snmp**. Next time, use the **-i** option if you want the command to copy the files to that location automatically.

- If you want the file for your personal use only, copy the file to your HOME directory. Next time, use the **-p** option if you want the command to copy the file to that location automatically.

4. Ensure that user **root** starts the snmpd executable that is located in **/usr/local/sbin/snmpd**.

Troubleshooting Net-SNMP Installations

The /usr/local/bin/snmpconf file requires Perl v5.6 and above.

Replace the line:

```
#!/usr/local/bin/perl
```

in /usr/local/bin/snmpconf to reference your Perl installation:

If your version of Perl is 5.0 or before then you might receive a runtime error when the snmpconf file executes. To correct this problem, edit the snmpconf file and make the following changes:

```
#!/usr/local/bin/perl
- if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}"))) {
+ if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}", 0755))) {
print "\nCould not create $opts{'I'} directory: $!\n";
print ("File $didfile{$i} left in current directory\n");
}
@@ -198,7 +198,7 @@
}
}
} elsif ($opts{'p'}) {
- if (! (-d "$home") && ! (mkdir ("$home"))) {
+ if (! (-d "$home") && ! (mkdir ("$home", 0755))) {
print "\nCould not create $home directory: $!\n";
print ("File $didfile{$i} left in current directory\n");
```

16

Installing Data Collectors

Installing the Data Collector

Follow the steps in the following sections to install the Data Collector on the Data Collector Server. The particular sequence of instructions depends on your environment. The data collector installations can be downloaded via the Internet.

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.

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

- Installing Using the Internet
- UI Deployment of the Data Collector

Installing Using the Internet

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

Note: If your Data Collector Server does not have Internet access or web browser access—for example, X-Windows not available, proceed to the next section, Internet Access Not Available from the Data Collector Server, for the relevant installation steps.

1. Start the web browser on the **Data Collector Server**.
2. Go to the Downloads site in the Customer Portal at www.aptare.com and click on the relevant download link.
3. Select the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.

OS	Data Collector Installer File Name
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 UI Deployment of the Data Collector.

Internet Access *Not* 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. Go to the Downloads site in the Customer Portal at www.aptare.com and click on the relevant download link.
4. Download the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.

OS	Data Collector Installer File Name
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 UI Deployment of the Data Collector.
   - **On Linux**:

     If the **Data Collector Server** *has* X-Windows, take these steps, substituting the relevant Data Collector Installer name for `<installer_file>`, as listed in Step 4.

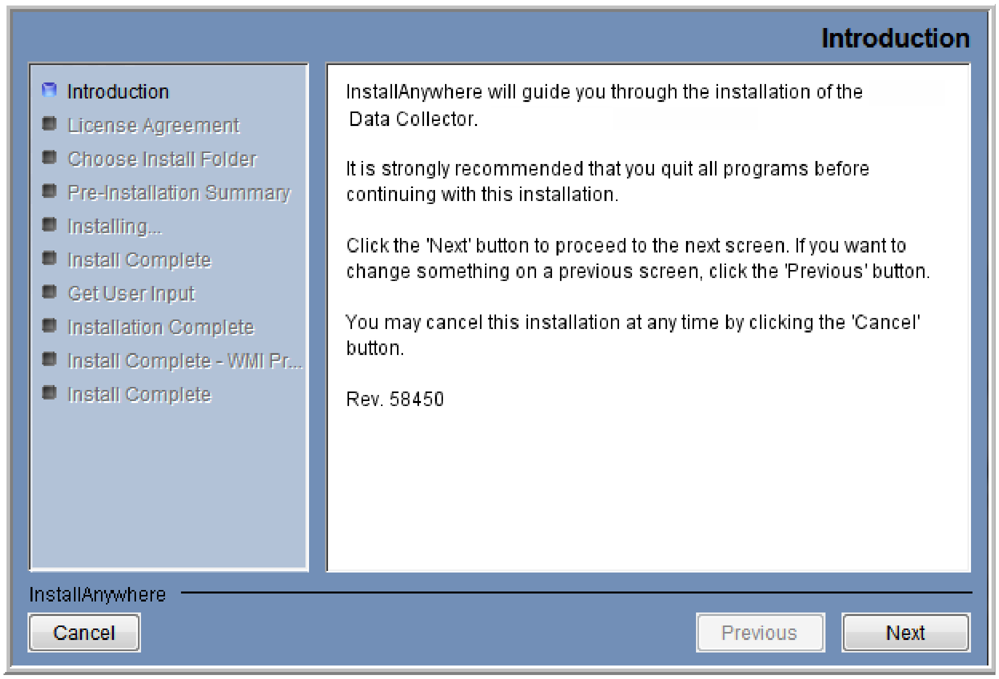
     chmod +x <*installer_file*>

     sh ./<*installer_file*> –i swing
   - Proceed to UI Deployment of the Data Collector.

     If the **Data Collector Server** *does not have* X-Windows:
   - Proceed to the Console Installation instructions.

UI Deployment of the Data Collector

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.



InstallAnywhere will guide you through the installation of the Data Collector.

It is strongly recommended that you quit all programs before continuing with this installation.

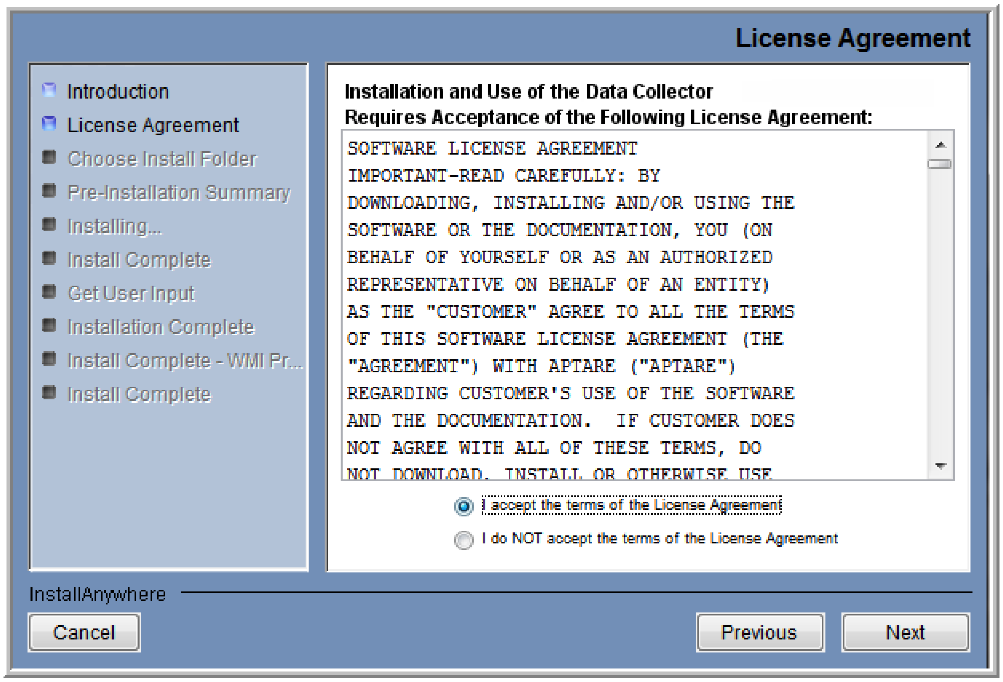
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Rev. 58450

1. Review the installation process and click **Next**.

   The License Agreement displays for your acknowledgement.



Installation and Use of the Data Collector
Requires Acceptance of the Following License Agreement:

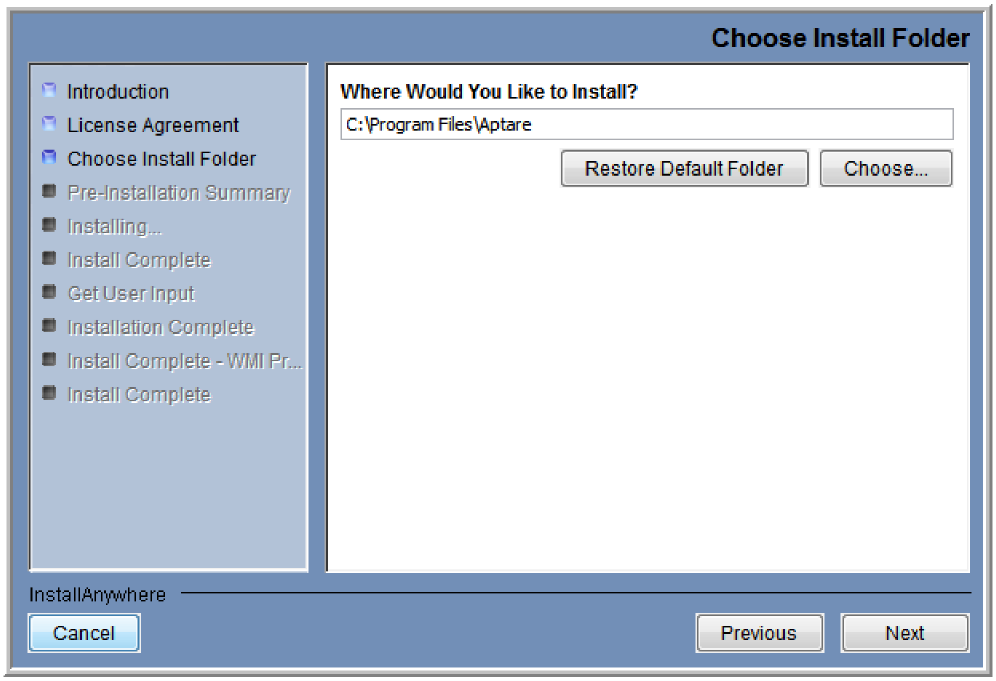
```
SOFTWARE LICENSE AGREEMENT
IMPORTANT-READ CAREFULLY: BY
DOWNLOADING, INSTALLING AND/OR USING THE
SOFTWARE OR THE DOCUMENTATION, YOU (ON
BEHALF OF YOURSELF OR AS AN AUTHORIZED
REPRESENTATIVE ON BEHALF OF AN ENTITY)
AS THE "CUSTOMER" AGREE TO ALL THE TERMS
OF THIS SOFTWARE LICENSE AGREEMENT (THE
"AGREEMENT") WITH APTARE ("APTARE")
REGARDING CUSTOMER'S USE OF THE SOFTWARE
AND THE DOCUMENTATION.  IF CUSTOMER DOES
NOT AGREE WITH ALL OF THESE TERMS, DO
NOT DOWNLOAD, INSTALL OR OTHERWISE USE
```

● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

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.



Where Would You Like to Install?

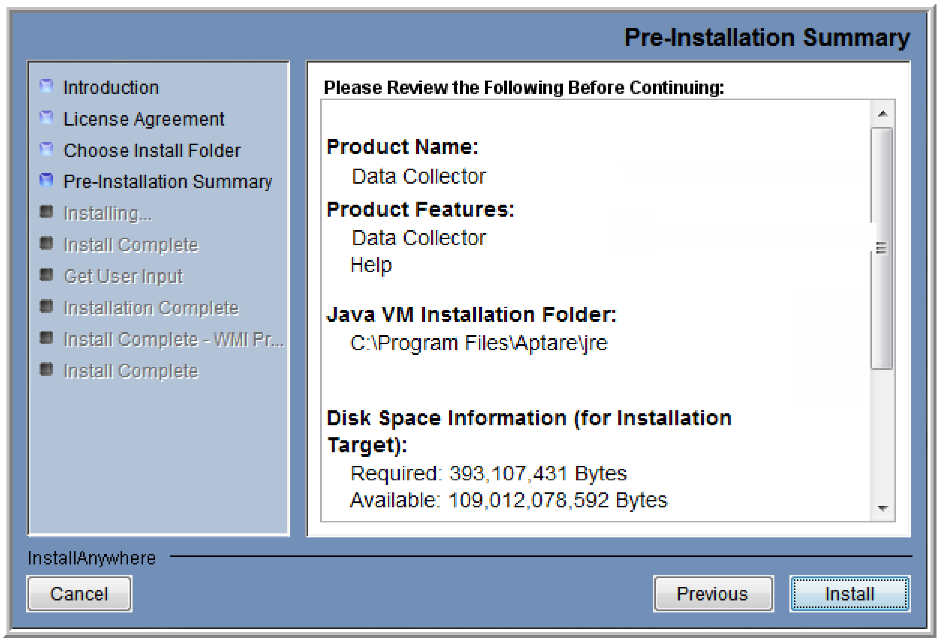
C:\Program Files\Aptare

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.



Please Review the Following Before Continuing:

Product Name:
Data Collector

Product Features:
Data Collector
Help

Java VM Installation Folder:
C:\Program Files\Aptare\jre

Disk Space Information (for Installation Target):
Required: 393,107,431 Bytes
Available: 109,012,078,592 Bytes

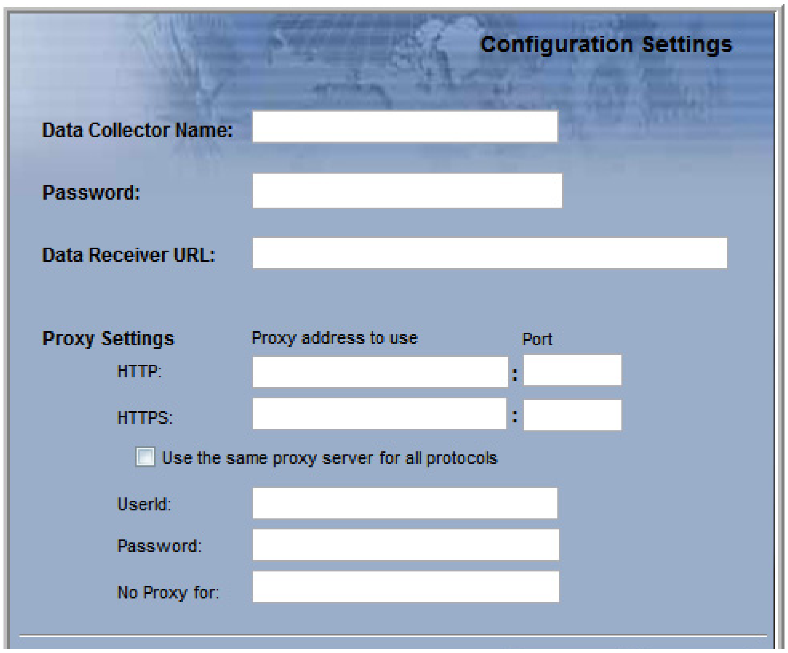
5. Review the summary and click **Install**. The dialog tracks the installation as it progresses.

6. A Configuration Settings window will prompt you to select a Data Collection Task. The configuration choices are: Data Collector (includes WMI Proxy) or APTARE 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. Click **Next**.

8. Enter the configuration settings for your particular environment.



Configuration Settings

Data Collector Name:

Password:

Data Receiver URL:

Proxy Settings

Proxy address to use

Port

HTTP: :

HTTPS: :

□ Use the same proxy server for all protocols

UserId:

Password:

No Proxy for:

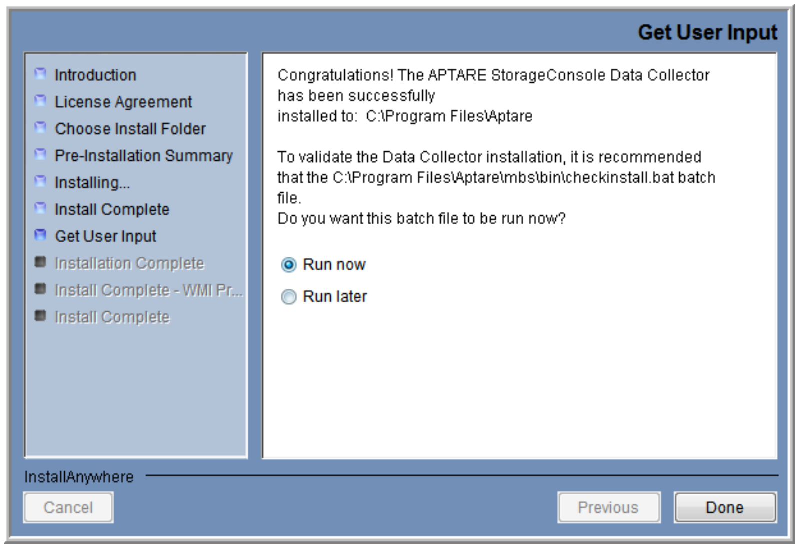
Field	Description
Data Collector Name *	A unique name assigned to this Data Collector. This is the name that you used during the Pre-Installation setup. The Data Collector will use this value for authentication purposes.
Password *	The password assigned to this Data Collector. The password is encrypted 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).* **IMPORTANT NOTE:** Be sure to enter the URL with the prefix *aptareagent* and NOT *aptareportal.*

Field	Description
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

* Denotes a mandatory configuration.

9. 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.



Get User Input

Congratulations! The APTARE StorageConsole Data Collector has been successfully installed to: C:\Program Files\Aptare

To validate the Data Collector installation, it is recommended that the C:\Program Files\Aptare\mbs\bin\checkinstall.bat batch file.
Do you want this batch file to be run now?

● Run now

○ Run later

10. 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.

11. Continue using the instructions in Validating Data Collection.

Console Installation Instructions

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.

   ```
   =====================================================
   (created with InstallAnywhere by Macrovision)
   -----------------------------------------------------
   Introduction
   ------------


   InstallAnywhere will guide you through the installation of the APTARE IT Analytics Data
   Collector.


   It is strongly recommended that you quit all programs before continuing with this
   installation.


   Respond to each prompt to proceed to the next step in the installation.  If you want to
   change something on a previous step, type 'back'.


   You may cancel this installation at any time by typing 'quit'.


   PRESS <ENTER> TO CONTINUE:
   ```

4. The License Agreement will be displayed.

   ```
   License Agreement
   -----------------


   Installation and use of APTARE IT Analytics requires acceptance of the following License
   Agreement:
   PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING, INSTALLING OR
   USING THE SOFTWARE YOU INDICATE ACCEPTANCE OF AND AGREE TO THETERMS AND CONDITIONS OF
   THIS AGREEMENT….<etc.>
   ```

5. Read the agreement and type **Y** to accept it.

6. The installer will prompt for the installation location:

   ```
   Choose Install Folder
   ---------------------


   Where would you like to install?


     Default Install Folder: /opt/aptare
   ```

```
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      : /opt/aptare

INSTALL FOLDER IS: /opt/aptare
   IS THIS CORRECT? (Y/N): y
```

7. A Pre-Installation Summary will be displayed.

```
==================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    APTARE IT Analytics

Install Folder:
    /opt/aptareagent

Link Folder:
    /tmp/install.dir.30662/Do_Not_Install

Product Components:
    APTARE IT Analytics Agent,
    Help

Java VM Installation Folder:
    /opt/aptareagent/jre

Disk Space Information (for Installation Target):
    Required:  136,083,162 bytes
    Available: 3,786,149,888 bytes


PRESS <ENTER> TO CONTINUE:
```

8. The installation process will track the progress:

```
==================================================
Installing...
-------------

 [==================|==================|=============]
 [------------------|------------------|-------------]
```

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.

```
Enter Data Collector Name
(Required Field)

Data Collector Name (DEFAULT: ):
```

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 “passcode” during the Pre-Installation step.

```
Configuration Settings - 2
--------------------------

Enter Data Collector Password:
(Please enter the Password, which will be used to authenticate the Data
Collector with the Data Receiver)
(Required)

Data Collector Password: password1
```

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.
```

13. Continue with Validating Data Collection.

17

Validating Data Collection

You can quickly validate the data collection process once you've set up a policy. Validation methods differ based on the subsystem vendor associated with the policy. Validation methods enable you to:

- Test connections, using IP addresses and credentials
- Test the collection run end to end by collecting real data from your subsystem vendors while selecting specific servers and probes

You can initiate Data Collection validation through the Portal or from the Checkinstall utility.

- 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. See Monitoring APTARE IT Analytics for details about starting and stopping components.
- **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. Refer to Data Collectors: Vendor-Specific Validation Methods to determine which data collector policies support On-Demand collection.
- **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.

Note: APTARE 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

Data Collector Policy	Validation Methods		
	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	
Commvault Simpana			x
Dell Compellent			x
EMC Avamar		x	
EMC Data Domain Backup	x	x	
EMC Data Domain Storage	x	x	
EMC Isilon		x	
EMC NetWorker			x
EMC Symmetrix	x	x	
EMC VNX Celerra			x
EMC VNX CLARiiON	x	x	
EMC VPLEX			x
EMC XtremIO	x	x	
HDS HCP	x	x	
HDS HNAS		x	
Hitachi Block			x
HP 3PAR			x
HP Data Protector			x
HP EVA			x
Huawei OceanStor	x	x	
IBM Enterprise			x
IBM SVC			x

Data Collector Policy	Validation Methods		
	Test Connection	On-Demand	CLI Checkinstall Utility
IBM Spectrum Protect (TSM)		x	
IBM XIV			x
INFINIDAT Infinibox	x	x	
Microsoft Azure	x	x	
Netapp		x	
Netapp Cluster Mode		x	
NetApp E Series			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	
Veeam Backup & Replication	x	x	
Veritas Backup Exec			x
Veritas NetBackup		x	
VMWare			x

Working with On-Demand Data Collection

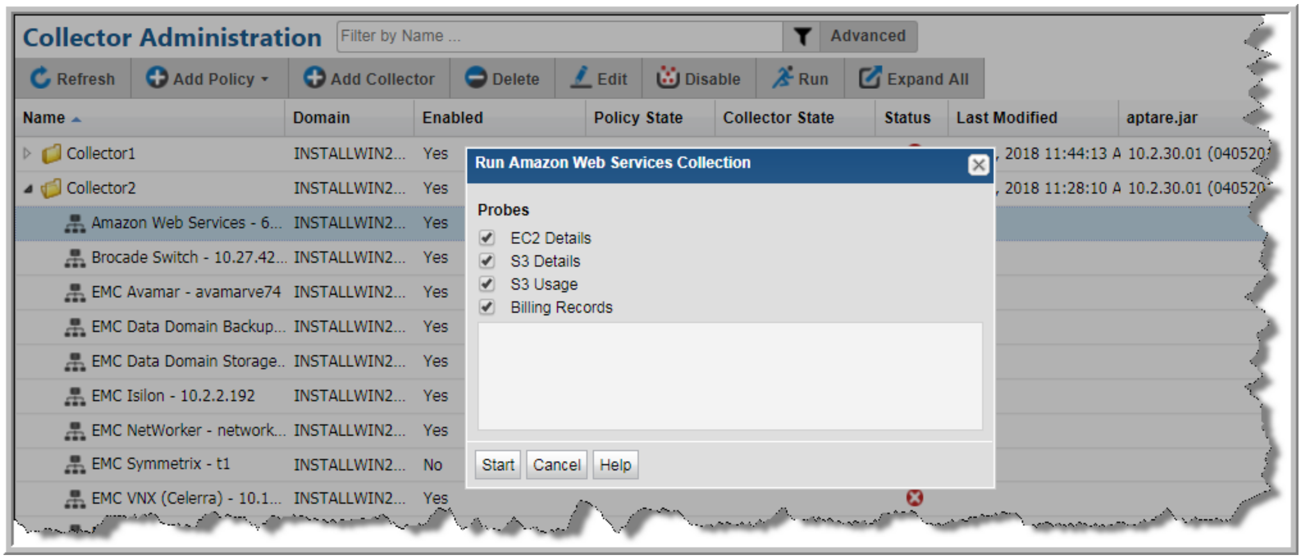
Note: On-Demand data collection is not available for all policies. Refer to Data Collectors: Vendor-Specific Validation Methods to determine which policies support On-Demand collection.

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**. See Navigating with Search for details.
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.



Name	Domain	Enabled	Policy State	Collector State	Status	Last Modified	aptare.jar
Collector1	INSTALLWIN2...	Yes				, 2018 11:44:13 A	10.2.30.01 (040520
Collector2	INSTALLWIN2...	Yes				, 2018 11:28:10 A	10.2.30.01 (040520
Amazon Web Services - 6...	INSTALLWIN2...	Yes					
Brocade Switch - 10.27.42...	INSTALLWIN2...	Yes					
EMC Avamar - avamarve74	INSTALLWIN2...	Yes					
EMC Data Domain Backup...	INSTALLWIN2...	Yes					
EMC Data Domain Storage..	INSTALLWIN2...	Yes					
EMC Isilon - 10.2.2.192	INSTALLWIN2...	Yes					
EMC NetWorker - network...	INSTALLWIN2...	Yes					
EMC Symmetrix - t1	INSTALLWIN2...	No					
EMC VNX (Celerra) - 10.1...	INSTALLWIN2...	Yes			⊗		

Run Amazon Web Services Collection

Probes

☑ EC2 Details
☑ S3 Details
☑ S3 Usage
☑ Billing Records

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. See Monitoring Data Collection Status.

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 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, as described in Host Resources: Collection in Stand-Alone Mode.

   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 the Global Support Center 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`**

18

Manually Starting the Data Collector

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
```

19

Uninstalling the Data Collector

Use the procedures in this section to uninstall a Data Collector.

- 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 APTARE IT Analytics 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.

20

Load Historic Events

After installing the backup Data Collectors, you may want to capture historical backup events for inclusion in the APTARE IT Analytics database.

- Load Commvault Simpana Events
- Load EMC Avamar Events
- Load EMC NetWorker Events
- Load HP Data Protector Events
- Load IBM Spectrum Protect (TSM) Events
- Load Oracle Recovery Manager (RMAN) Events
- Load Veritas NetBackup Events
- Load Veritas Backup Exec Events

Load Commvault Simpana Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Commvault Simpana Data Collector software.

Note: You can only collect historic Commvault Simpana data if you have *not* already done a Simpana data collection.

Windows:

```
C:\Program Files\Aptare\mbs\bin\commvault\cvsimpanadetails.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/commvault/cvsimpanadetails.sh
```

To capture data from a specific period, use the following utility:

```
    cvsimpanadetails.{sh|bat} <output_dir> <cvdb_username> <cvdb_password>
    <cvdb_hostname>[:port] [max_hours [cv_username cv_password [cv_hostname]]]
```

Where:

- This utility will write data to a set of files in the output directory specified in output_dir.
- The cvdb_username, cvdb_password and cvdb_hostname refer to the CommServ database system (this is usually the same as the CommServ server) from which you are collecting data.
- An optional port number can be appended to the cvdb_hostname, separated by a colon. If a port number is not specified, it will default to port 1433.
- An optional maximum number of hours from which to start the collection can be specified. This value is used to calculate the current time minus the number of hours that was entered. If you do not enter a maximum number of hours, then *all* details retained by the Commvault Simpana database will be retrieved.
- The last set of cv_username, cv_password and cv_hostname are required *only* if you are collecting Skipped File Details from a Windows-based CommServ Server.

Load EMC Avamar Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Avamar Data Collector software.

Windows:

```
C:\Program Files\Aptare\mbs\bin\avamar\avamarhistoricdetails.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/avamar/avamarhistoricdetails.sh
```

To capture data from a specific period, use the following utility:

```
avamarhistoricdetails.{sh|bat} <MetadataCollectorID> <SubSystemID> ["<Start Date>" "<End Date>"] [verbose]
```

Where:

- The MetadataCollectorID and the SubSystemID can be found by executing the utility:

  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Avamar commands called to the metadata.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last two weeks.

Load EMC NetWorker Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the NetWorker Data Collector software.

Windows:

```
C:\Program Files\Aptare\mbs\bin\networker\nwhistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/networker/nwhistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
nwhistoricevents.{sh|bat} <EventCollectorID> <ServerID> ["<Start Date>" "<End Date>"]
[verbose]
```

Where:

- The EventCollectorID and the ServerID can be found by executing the utility:

  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the NetWorker commands called to the eventcollector.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours.

Load HP Data Protector Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the HP Data Protector Data Collector software.

Windows:

```
C:\Program Files\Aptare\mbs\bin\dataprotector\hpdphistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/dataprotector/hpdphistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
hpdphistoricevents.{sh|bat} <EventCollectorID> <ServerID> ["<Start Date>" "<End Date>"]
[verbose]
```

Where:

- The EventCollectorID and the ServerID can be found by executing the utility:

  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Data Protector commands called to the eventcollector.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours. HP Data Protector commands ignore the time segment of the start and end date values. In addition, the end date value is used as an “until” value. For example, a value of "2015-05-11 23:59:59" will only collect historic values up to 2015-05-11 00:00:00. To collect values for the date of 2015-05-11 you should enter a end date of "2015-05-12 00:00:00".

Load IBM Spectrum Protect (TSM) Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the IBM Spectrum Protect (TSM) Data Collector software.

Windows:

```
C:\Program Files\Aptare\mbs\bin\tsm\tsmhistoricevents.bat
```

Linux:

```
<APTARE HOME>/mbs/bin/tsm/tsmhistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
tsmhistoricevents.{sh/bat} <MetadataCollectorID> <ServerID> ["<Start Date>" "<End Date>"
[verbose]]
```

Where:

- The MetadataCollectorID and the ServerID can be found by executing the utility:

  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the IBM Spectrum Protect (TSM) commands called to the metadata.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours.

Load Oracle Recovery Manager (RMAN) Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Oracle Recovery Manager (RMAN) Data Collector software.

1. Set Advanced Parameter RMAN_BACKUP_LOOKBACK_DAYS=# days to load (from current day).
2. Set Advanced Parameter RMAN_BACKUP_LOOKBACK_OVERRIDE=Y.

   See RMAN_BACKUP_LOOKBACK_DAYS and RMAN_BACKUP_LOOKBACK_OVERRIDE for details.
3. Navigate to **Admin>Data Collection>Collector Administration**.
4. Select the Oracle RMAN Data Collection policy and click **Run**.

   See Working with On-Demand Data Collection for details.

   You can also wait for the scheduled collection to complete.
5. Reset RMAN_BACKUP_LOOKBACK_DAYS and RMAN_BACKUP_LOOKBACK_OVERRIDE to their original values (or the default values) once the Collection Run is complete. Do not delete the advanced parameters.

Load Veeam Backup & Replication Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Veeam Backup & Replication Data Collector software.

1. Set Advanced Parameter VEEAM_BACKUP_LOOKBACK_DAYS to the number of days. Also specify the Data Collector and the Host Name(s) for which the historical data must be collected.

1. Set Advanced Parameter VEEAM_BACKUP_LOOKBACK_OVERRIDE=Y. Also specify the Data Collector and the Host Name(s) for which the historical data must be collected.

   See VEEAM_BACKUP_LOOKBACK_DAYS and VEEAM_BACKUP_LOOKBACK_DAYS_OVERRIDE for details.
2. Navigate to **Admin>Data Collection>Collector Administration**.
3. Select the Veeam Backup & Replication Data Collection policy and click **Run**.

   See Working with On-Demand Data Collection for details.
4. Reset VEEAM_BACKUP_LOOKBACK_OVERRIDE to N (or the default values) once the Collection Run is complete to avoid historic data collection on future scheduled or On Demand runs,

Load Veritas NetBackup Events

APTARE IT Analytics gathers backup events from both the NetBackup catalog and the NetBackup activity log. You specify the date range for the backup jobs that occurred during a given time period. To minimize the impact on performance, it is best to load backup events for each individual client. However, in many cases, this is not practical. Therefore, several methods are provided to accommodate various needs. Only successful jobs are retrieved from the NetBackup environment.

Load Events for Individual NetBackup Clients

To retrieve historic data from a NetBackup client, execute the following command-line scripts.

Windows:

```
C:\Program Files\Aptare\mbs\bin\symantec\load_nbu_backups.bat <metaDataCollectorId>
<masterServerName> <client_name> "<Start_Date>" "<End_Date>"
```

Linux:

```
<APTARE HOME>/mbs/bin/symantec/load_nbu_backups.sh <metaDataCollectorId> <masterServerName>
<client_name> "<Start_Date>" "<End_Date>"
```

Note: Start_Date and End_Date must be in the format: `YYYY-MM-DD HH:MM:SS`

Where:

- The MetadataCollectorID can be found by executing the utility:

  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

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

Load Events for a Group of NetBackup Clients

To load historic events for a group of NetBackup clients, execute the following command-line scripts.

Note: This process will only load data for clients that are listed in standard policies. It will not retrieve data for clients not explicitly listed in policies. For example, VMware VMs that are part of a VMware Intelligent Policy will not be included.

Linux

1. Create a NetBackup client list:

   ```
   /usr/openv/netbackup/bin/admincmd/bpplclients -noheader -allunique > /<APTARE HOME>/mbs/
   bin/client_list.txt
   ```

2. Load the list into a *for* loop:

   ```
   for i in 'awk '{print $3}' /<APTARE HOME>/mbs/bin/client_list.txt'
   do
   /<APTARE HOME>/mbs/bin/load_nbu_backups.sh <metaDataCollectorId> <masterServerName> $i
   "<Start_Date>" "<End_Date>"
   Done
   ```

Note: Start_Date and End_Date must be in the format: `YYYY-MM-DD HH:MM:SS`

Where:

- The MetadataCollectorID can be found by executing the utility:

Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

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

Windows

1. Create a NetBackup client list:

```
C:\program files\Veritas\netbackup\bin\admin\cmd\bpplclients -noheader -allunique > "c:\
program files\aptare\mbs\bin\client_list.txt"
```

2. Load the list into a *for* loop:

```
for /F "tokens=3" %A in ("c:\program files\aptare\mbs\bin\client_list.txt") do "c:\program
files\aptare\mbs\bin\load_nbu_backups.bat" <metaDataCollectorId> <masterServerName> %A
"<Start_Date>" "<End_Date>"
```

Note: Start_Date and End_Date must be in the format: `YYYY-MM-DD HH:MM:SS`

Note: If the path C:\Program Files fails, try it as C:\Progra~1 or C:\Progra~2

Load Veritas Backup Exec Events

Collecting Missed Events

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Backup Exec Data Collector software.

Windows:

C:`\Program Files\Aptare\mbs\bin\backupexec\buehistoricevents.bat`

Linux:

```
<APTARE HOME>/mbs/bin/backupexec/buehistoricevents.sh
```

To capture data from a specific period, use the following utility:

```
buehistoricevents.{sh|bat} <AdministratorDomain> <AdministratorUser>
<AdministratorPassword> ["<Start Date>" "<End Date>"] [verbose]
```

Where:

- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Backup Exec commands called to the metadata.log file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the last 24 hours.

A

Troubleshooting

This section lists some of the common issues. If the issue cannot be resolved by following the steps in this section, contact the APTARE Global Support Services. Be sure to include the log files that were generated during the installation process. The topics covered in this section apply to all supported backup vendors.

- Verify the Data Collector Configuration
- Verify Connectivity
- Configuring Web Proxy Updates
- Adding New Data Domain Models to the Reporting Database
- Collecting Missed Events for Veritas Backup Exec
- Substituting ODBC for JDBC to Connect to SQL Server for Veritas Backup Exec

Verify the Data Collector Configuration

The Data Collector configuration file contains key information captured during the installation process. If the information was entered incorrectly, this may be the cause of the failure.

Check the Configuration File

1. Edit the configuration file.

   Windows:

   ```
   edit "C:\Program Files\Aptare\mbs\conf\wrapper.conf"
   ```

   Linux:

   ```
   edit "/opt/aptare/mbs/bin/startup.sh" and "/opt/aptare/mbs/bin/updateconfig.sh"
   ```

2. Verify the values of the following parameters and update them, if necessary.

wrapper.app.parameter.2	Should match the Collector Name you specified in Adding/Editing Data Collectors.

wrapper.app.parameter.3	Should match the Passcode you specified in Adding/Editing Data Collectors.
wrapper.app.parameter.4	For IN-HOUSE installations: http://aptareagent.*yourdomain.com* where: *yourdomain.com* has the appropriate value. For APTARE HOSTED installations: http://agent.storageconsole.com For third-party HOSTED installations: http://aptareagent.*domain.com* where: *domain.com* has the appropriate value.

3. If you changed any of the configuration file parameters, you'll need to:
   - Restart the Data Collector service, as described in Manually Starting the Data Collector.
   - Re-run the installation validation utility, as described in Validating Data Collection.

Verify Connectivity

To verify that the Data Collector Server can access the Portal Server:

1. Ping the Data Collector URL:

```
ping http://aptareagent.yourdomain.com
```

2. Verify that the URL has been set up correctly in DNS or in the local hosts file, to resolve to the Portal Server.

Configuring Web Proxy Updates

If you are using a proxy server to connect to the Portal, the Data Collector was configured during installation to use the proxy to connect to the Portal. If the web proxy configuration changes in your environment, the Data Collector must be aware of those changes in order to maintain connectivity. These settings can be found in:

```
/opt/aptare/mbs/conf/collectorsystem.properties
```

Adding New Data Domain Models to the Reporting Database

There may be times when new Data Domain models have been released by EMC and your current APTARE IT Analytics version does not yet have the models in the database. When these new models are not in the database, certain values, such as raw capacity, may not be accurately represented in reports.

To update the IT Analytics database with new Data Domain models, take the following steps.

1. Log on to the Portal Server as user **aptare**.
2. At the command prompt, type: **sqlplus <pwd>/<pwd>**
3. At the SQL prompt, use the following example to insert the model and its raw capacity into the database table.

```
SQL> INSERT INTO apt_ddm_system_model(ddm_system_model_number, raw_capacity_kb)
VALUES('DD880', 206158430208.00);

SQL> Commit;
```

Note: Any updates that you make to this table will be retained when you upgrade to a new IT Analytics version.

Collecting Missed Events for Veritas Backup Exec

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Backup Exec Data Collector software.

To capture data from a specific period, use the following utility:

```
buehistoricevents.{sh/bat} {AdministratorDomain} {AdministratorUser}
{AdministratorPassword} [{Start Date} {End Date}] [verbose]
```

Where:

- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Backup Exec commands called to the eventcollector.log file.

Note: If the Start and End Dates are not specified, the utility will capture Events that occurred in the last 24 hours.

Substituting ODBC for JDBC to Connect to SQL Server for Veritas Backup Exec

The Backup Exec data collector, by default, uses JDBC (Java Database Connectivity) to connect to the SQL Server database. In most cases, this is the preferred mechanism for communicating with the SQL Server. However, in some instances—for example, TCP/IP is disabled for the SQL Server—JDBC will not be feasible.

In these rare situations, you can configure ODBC (Open Database Connectivity) to connect. The main limitation of this option is that it requires that a DSN (Data Source Name) be set up for *each* Backup Exec server for which the data collector needs access.

Note: The data collector can be configured to use a mixture of JDBC and ODBC for specific servers.

Use the following steps to turn on ODBC for specific servers.

1. Obtain a copy the **servers.csv** file from the Portal Server (the one that you created to load the Backup Exec servers into the database).
2. Edit **servers.csv** and delete those servers that you do not want to use ODBC. The format of the entry in the CSV file is:

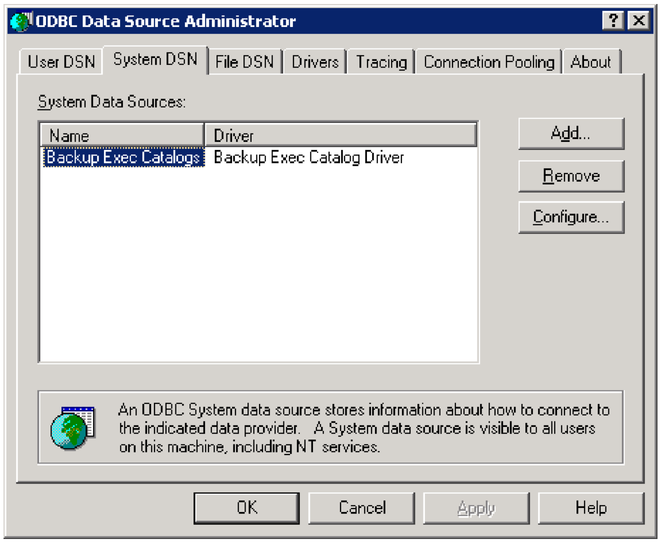
   ```
   <windows_domain>, <host or ipaddress>, <ipaddress>, , , BKUPEXEC
   ```
3. Save the file to **$APTARE_HOME/mbs/conf** as **odbcservers.conf** on the Data Collector server.
4. Launch the ODBC Data Source Administrator window:

   ```
   Control Panel > Administrative Tools > Data Sources (ODBC)
   ```
5. Set up the ODBC DSN for each of the Backup Exec servers in **odbcservers.conf**, as depicted in the following sequence of windows.

   The DSN needs to be of the form `hostname_BKUPEXEC`, where hostname is the second token in **odbcservers.conf**.

   Note: If the `hostname_BKUPEXEC` form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

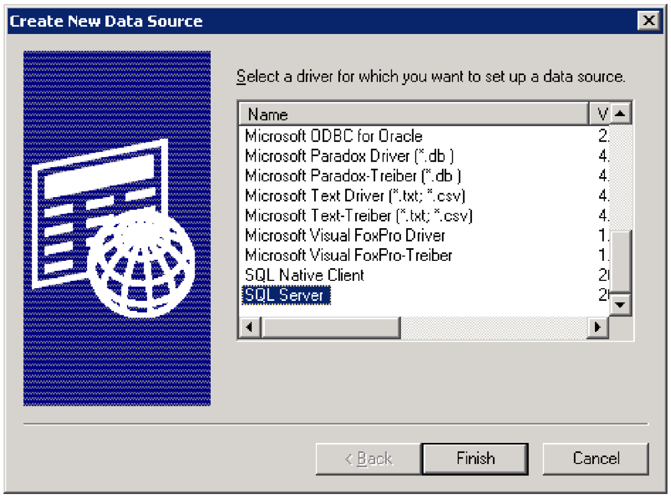
```
<windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
```



System Data Sources:

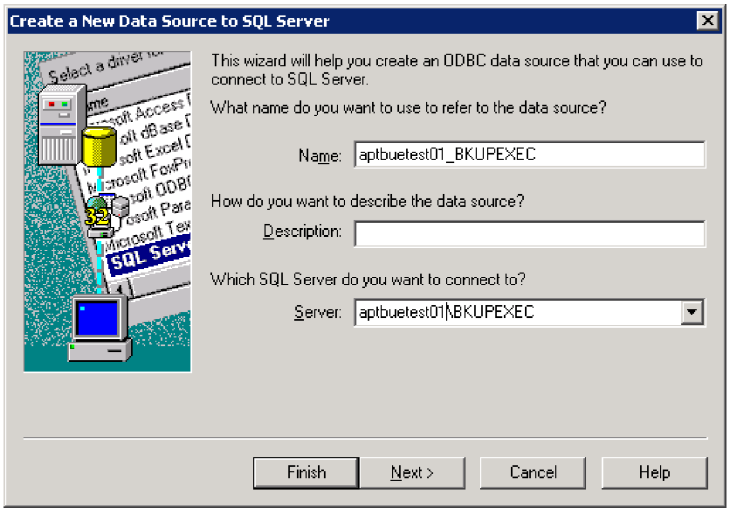
Name	Driver
Backup Exec Catalogs	Backup Exec Catalog Driver

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



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

Name	V
Microsoft ODBC for Oracle	2.
Microsoft Paradox Driver (*.db)	4.
Microsoft Paradox-Treiber (*.db)	4.
Microsoft Text Driver (*.txt; *.csv)	4.
Microsoft Text-Treiber (*.txt; *.csv)	4.
Microsoft Visual FoxPro Driver	1.
Microsoft Visual FoxPro-Treiber	1.
SQL Native Client	2(
SQL Server	2(



This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: aptbuetest01_BKUPEXEC

How do you want to describe the data source?

Description:

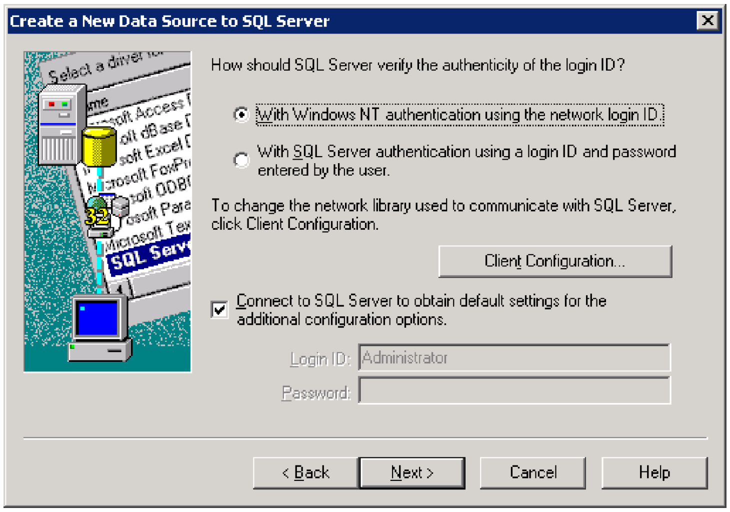
Which SQL Server do you want to connect to?

Server: aptbuetest01\BKUPEXEC

The DSN needs to be of the form hostname_BKUPEXEC, where hostname is the second token in **odbcservers.conf**.

Note: If the `hostname_BKUPEXEC` form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

```
<windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
```



Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

● With Windows NT authentication using the network login ID.

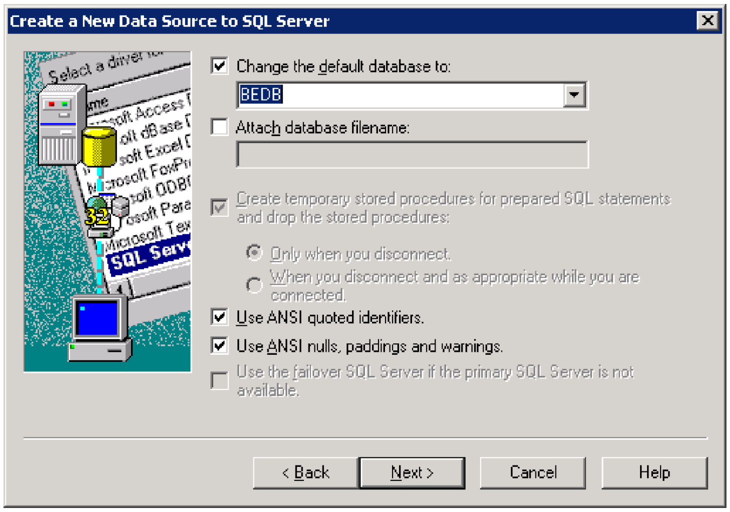
○ With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

☑ Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: Administrator

Password:



Create a New Data Source to SQL Server

☑ Change the default database to:

BEDB

☐ Attach database filename:

☑ Create temporary stored procedures for prepared SQL statements and drop the stored procedures:

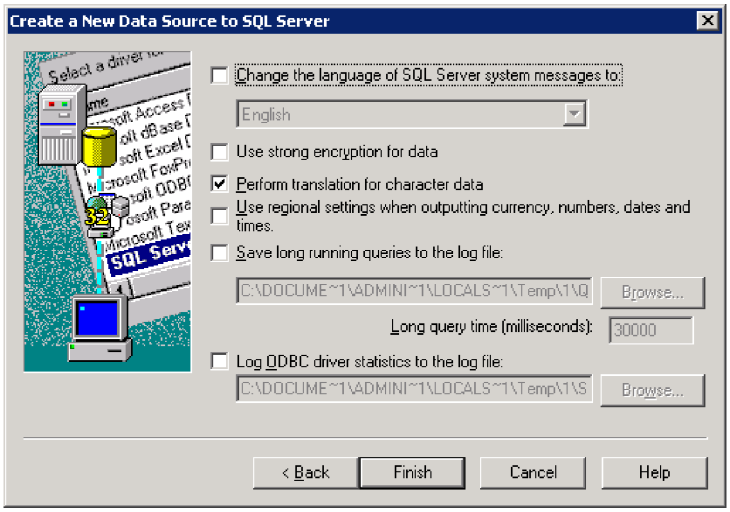
● Only when you disconnect.

○ When you disconnect and as appropriate while you are connected.

☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

☐ Use the failover SQL Server if the primary SQL Server is not available.


Create a New Data Source to SQL Server

☐ Change the language of SQL Server system messages to:

English

☐ Use strong encryption for data

☑ Perform translation for character data

☐ Use regional settings when outputting currency, numbers, dates and times.

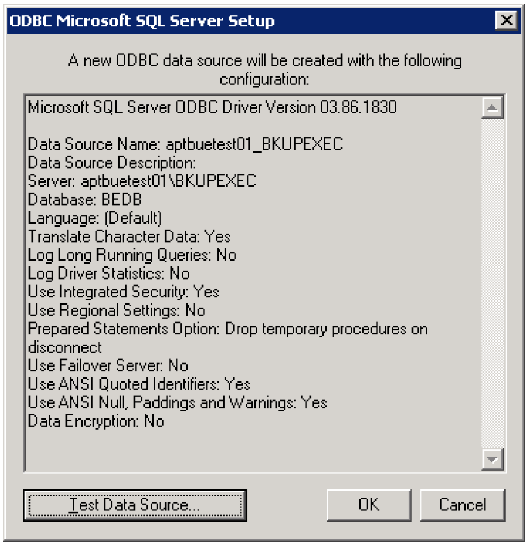
☐ Save long running queries to the log file:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\Q

Long query time (milliseconds): 30000

☐ Log ODBC driver statistics to the log file:

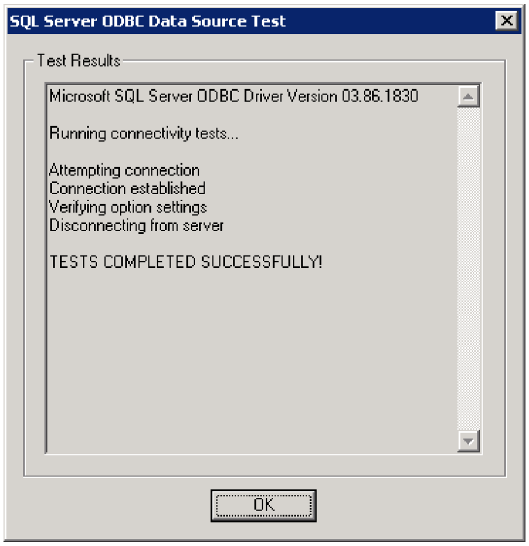
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1\S


ODBC Microsoft SQL Server Setup

A new ODBC data source will be created with the following configuration:

```
Microsoft SQL Server ODBC Driver Version 03.86.1830

Data Source Name: aptbuetest01_BKUPEXEC
Data Source Description:
Server: aptbuetest01\BKUPEXEC
Database: BEDB
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Integrated Security: Yes
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on
disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
Data Encryption: No
```


SQL Server ODBC Data Source Test

Test Results

```
Microsoft SQL Server ODBC Driver Version 03.86.1830

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```

A

CRON Expressions and Probe Schedules

Many Data Collector policy configurations require a schedule. Native CRON expressions are supported for fine-tuning a schedule. The format for the schedule follows the CRON standard:

*	*	*	*	*
minutes	**hours**	**day of month**	**month**	**day of week**

Probe Schedule Allowed Values:

Field	Allowed Values
minutes	0-59 (0 is “on the hour”)
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)

- IT Analytics supports a maximum of 80 characters in a CRON expression.

Special Characters:

- A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the minutes position is *not* permitted, as this would excessively trigger the probe—every minute.
- A forward slash (/) can be used to specify intervals.
- Use a dash (-) to specify a range.
- The CRON expression for the last day of the month, denoted by the letter L, is not supported.

Probe Schedule Examples	Scheduled Run Time
0 14-15 * * 1	On the hour, every Monday, between 2 and 3pm **Note**: A zero in the minutes position denotes the beginning of the hour.
30 9-13 * * 1-5	9:30, 10:30, 11:30, 12:30, and 13:30, Monday through Friday.
0 */2 * * *	To run the probe every 2 hours, put */2 in the hour position. This schedules the probe at 2am, 4am, 6am, 8am, 10am, 12pm, 2pm, and so on.
*/30 * * * *	Every 30 minutes

Probe Schedule Examples	Scheduled Run Time
*/20 9-18 * * *	Every 20 minutes between 9 am and 6 pm
*/30 * * * 1-5	Every 30 minutes, Monday through Friday
1 2 * * *	2:01 every day
30 9,11 * * *	9:30 and 11:30 every day

B

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.

Component	Default Ports	Description
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	
OpenLDAP	external LDAP 3268 LDAPS 638 LDAP 389	
Oracle	1521	Oracle TNS listener port
Tomcat - Data Receiver	8011, 8017	Apache connector port and shutdown port for Data Receiver instance of tomcat
Tomcat - Portal	8009, 8015	Apache connector port and shutdown port for Portal instance of tomcat
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445	

Default Ports for Firewall Configurations

Data Collector Vendors by Product	Default Ports and Notes
Storage	
Dell Compellent	1433 SMI-S http (5988) SMI-S https (5989)
Dell EMC Data Domain Storage	SSH 22
Dell EMC Elastic Cloud Storage (ECS)	REST API 80/443
Dell EMC Isilon	SSH 22
Dell EMC Symmetrix	SymCLI over Fibre Channel 2707
Dell EMC Unity	REST API version 4.3.0 on 443 or 8443
Dell EMC VNX (Celerra)	XML API 443, 2163, 6389, 6390, 6391, 6392
Dell EMC VNX (CLARiiON)	NaviCLI 443, 2163, 6389, 6390, 6391, 6392
Dell EMC VPLEX	https TCP 443
Dell EMC XtremIO	REST API https 443
Hitachi Block Storage	TCP 2001
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
HP 3PAR	22 for CLI
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0
Huawei OceanStor Enterprise Storage	8080
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMMOM 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
Data Protection	
Cohesity DataProtect	REST API on Port 80 or 443

Data Collector Vendors by Product	Default Ports and Notes
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023
Dell EMC Avamar	5555 SSH 22
Dell EMC Data Domain Backup	SSH 22
Dell EMC NetWorker	• 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
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)
Network & Fabrics	
Brocade Switch	SMI-S 5988/5989
Cisco Switch	SMI-S 5988/5989
Virtualization	
IBM VIO	SSH 22, Telnet 23
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESXi,vCenter,vSphere	vSphere VI SDK https TCP 443
Replication	
NetApp ONTAP 7-Mode	ONTAP API 80/443
Cloud	
Amazon Web Services	https 443
Microsoft Azure	https 443

Data Collector Vendors by Product	Default Ports and Notes
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22