NetBackup IT Analytics Data Collector Installation Guide for Backup Manager

Release 11.2

NetBackup IT Analytics Data Collector Installation Guide for Backup Manager

Last updated: 2023-08-01

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.

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 13

Chapter 14

Chapter 1

Introduction

This chapter includes the following topics:

- Overview
- Backup Manager Collection of Backup and Restore Data

Overview

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

The 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.

Chapter 2

Pre-Installation setup for Commvault Simpana

This chapter includes the following topics:

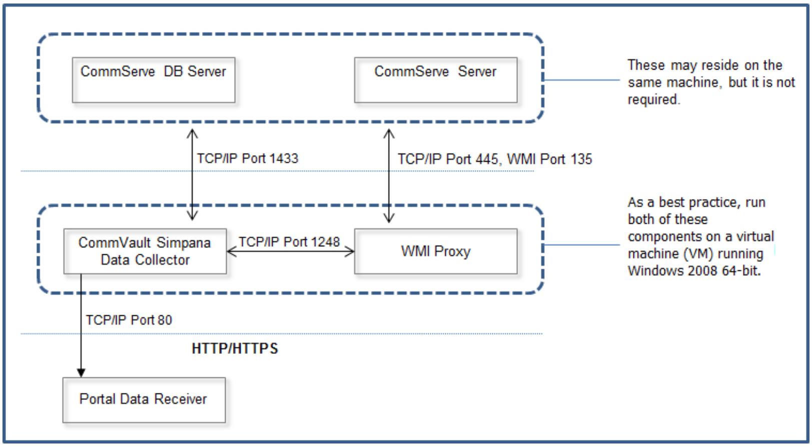
Introduction

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

Architecture overview (Commvault Simpana)

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

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


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
As a best practice, run both of these components on a virtual machine (VM) running Windows 2008 64-bit.
CommVault Simpana Data Collector
TCP/IP Port 1248
WMI Proxy
TCP/IP Port 80
HTTP/HTTPS
Portal Data Receiver

Prerequisites for adding Data Collectors (Commvault Simpana)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the 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" on page 18.
- MS SQL Server needs to be accessible to the collector on a static TCP Port (1433 recommended), requiring a restart of the SQL database service, if not already configured.
- MS SQL Server must be set to Mixed-mode authentication, and the login to be used for collection must be using SQL authentication.
  https://msdn.microsoft.com/en-us/library/ms188670.aspx.
- WMI Proxy access requires the following: Port 135 is required for skipped files collection and 445 for CIFS over TCP. A fixed port can be configured for WMI as specified at:
  http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx
- The Data Collector should be installed on the same server as the WMI proxy server.
- Read-only user configured on the CommServe server.
  See "Set up a read-only user in the CommServe server" on page 20.
- If you want to load historical data from a CommServe database, use the utility described in the following section.
  See "Load historical data prior to initial data collection" on page 24.
- 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 11

With the introduction of support for Java 11, older versions of MS SQL Server may encounter compatibility issues. The following section covers potential workarounds. Collection occurs from the Microsoft SQL Server database used by the system the data collector is collecting from. The version of Java used by NetBackup IT Analytics disables some insecure TLS algorithms by default. If collection fails with the following error in the collector logs, the version of MS SQL Server may be incompatible and not allow collection using the TLS algorithms enabled by default with Java 11.

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

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

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

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

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

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

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

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

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

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

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

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

Installation overview (Commvault Simpana)

1. See “Open TCP/IP access to the Commvault database” on page 18.
2. See “Set up a read-only user in the CommServe server” on page 20.
3. See “Add Commvault Simpana servers” on page 24.
4. See “Load historical data prior to initial data collection” on page 24.
5. Open TCP/IP access to the Commvault database.
6. Set up a read-only user in the CommServe server.
7. Load historical data (prior to the initial data collection).
8. In the Portal, add a Data Collector, if one has not already been created.
9. In the Portal, add the Commvault Simpana data collector policy.
10. On the Data Collector Server, install the Data Collector software.
11. Validate the Data Collector Installation.

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

Open TCP/IP access to the Commvault database

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

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

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

   See “Additional Static Port Configuration Steps” on page 19.
7. Click **OK.**
8. Click **SQL Server Services.**
9. Right-click **SQL Server <COMMVAULT>** and select **Restart.**

Additional Static Port Configuration Steps

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

On the Commvault CommCell Server:

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

- Click **OK**.

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

Set up a read-only user in the CommServe server

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

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

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

1. Create a new read-only user with a non-expiring password and assign the **db_datareader** role in the CommServe database. After completing the following steps, verify the connectivity with the read-only user ID.

2. Grant EXECUTE permission for the following stored procedures to the new read-only user:

   dbo.GetDateTime

   dbo.GetUnixTime

   dbo.GetJobFailureReason

   dbo.JMGetLocalizedMessageFunc

There are two methods for assigning EXECUTE permission.

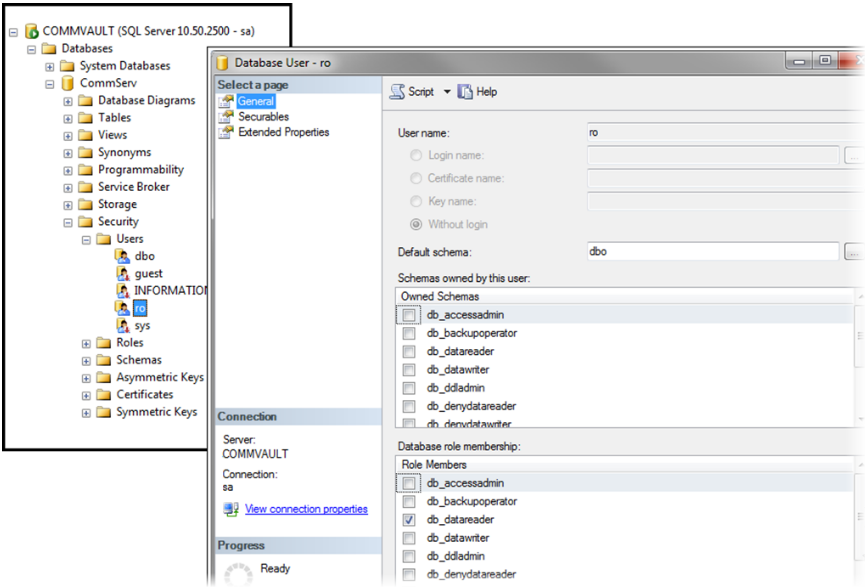
Option 1: Execute SQL commands in the CommServe database

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

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

Option 2: Use MSSQL Management Studio

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



User name: ro
○ Login name:
○ Certificate name:
○ Key name:
● Without login
Default schema: dbo

Schemas owned by this user:

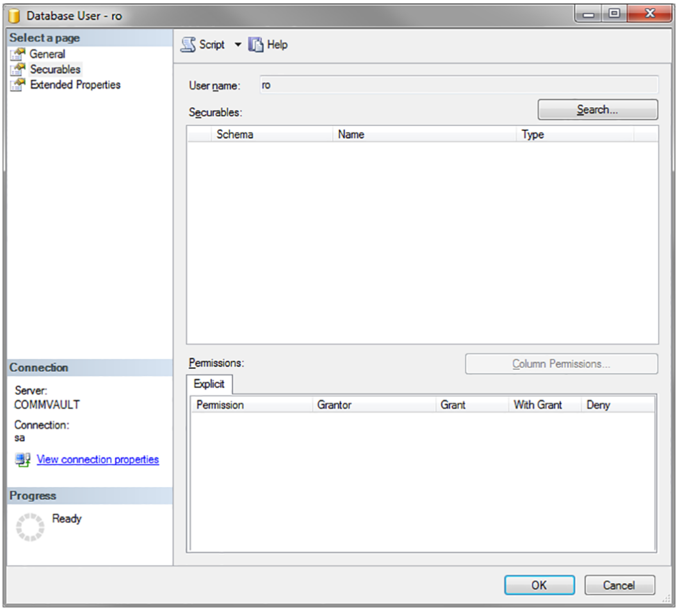
Owned Schemas
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter

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.



Database User - ro

User name: ro

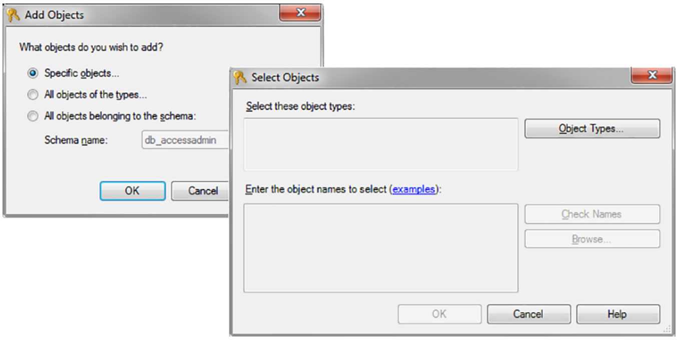
Server: COMMVAULT

Connection: sa

Progress: Ready

4. Click Search.

5. Add specific objects.



Add Objects

What objects do you wish to add?

● Specific objects...

○ All objects of the types...

○ All objects belonging to the schema:

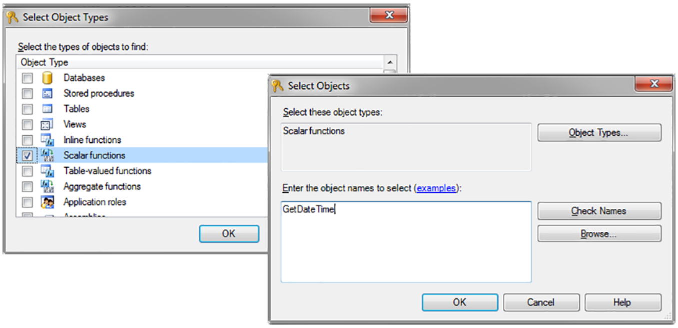
Schema name: db_accessadmin

Select Objects

Select these object types:

Enter the object names to select (examples):

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



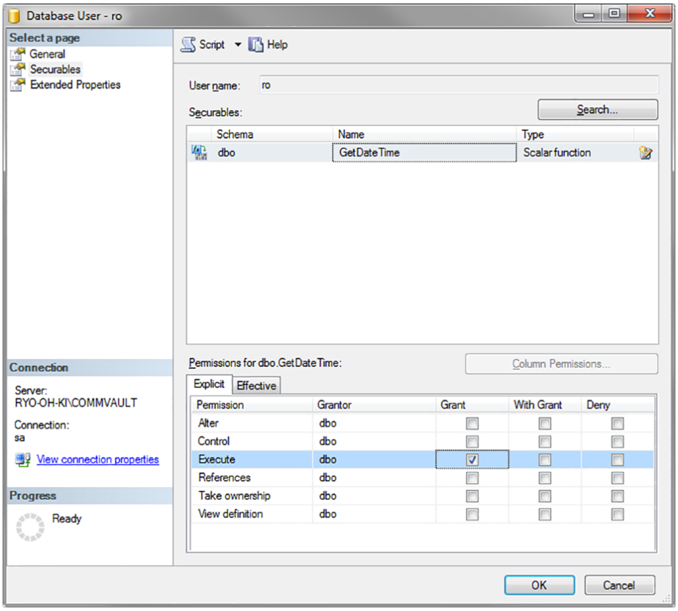
Select the types of objects to find:

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	□	□	□

Connection

Server:
RYO-OH-KI\COMMVAULT

Connection:
sa

Progress

Ready

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

9. Repeat steps 4-8 for each function:

   - GetUnixTime
   - GetJobFailureReason
   - JMGetLocalizedMessageFunc

10. Verify connectivity with the read-only user ID.

Load historical data prior to initial data collection

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

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

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

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

2. Login to SQL Plus.

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

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

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

4. Exit SQL Plus.

   SQL> exit

Add Commvault Simpana servers

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

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

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

Add a Commvault Simpana Data Collector policy

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

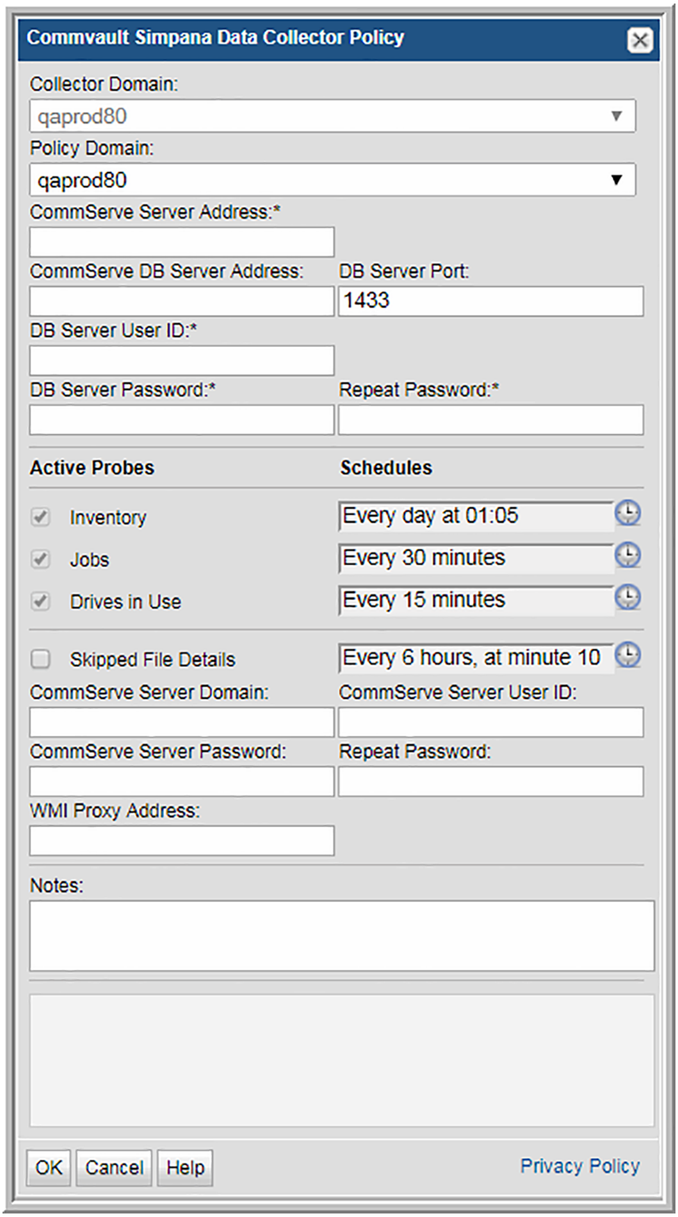
  For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only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

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

To add the policy

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

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



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

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

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

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

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

Chapter 3

Pre-Installation setup for Cohesity DataProtect

This chapter includes the following topics:

Introduction

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

Prerequisites for adding Data Collectors (Cohesity DataProtect)

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

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

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

- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- User must be assigned the Cohesity Operator role

Installation overview (Cohesity DataProtect)

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

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

Add a Cohesity DataProtect Data Collector policy

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

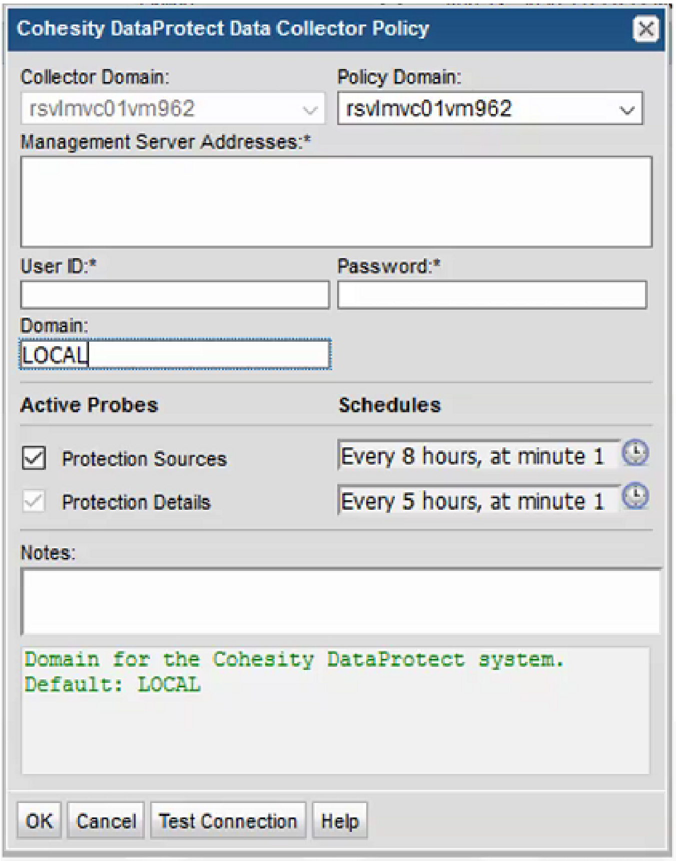
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only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

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

To add the policy

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

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



Cohesity DataProtect Data Collector Policy

Collector Domain: rsvlmvc01vm962

Policy Domain: rsvlmvc01vm962

Management Server Addresses:*

User ID:*

Password:*

Domain: LOCAL

Active Probes | Schedules

☑ Protection Sources | Every 8 hours, at minute 1

✓ Protection Details | Every 5 hours, at minute 1

Notes:

```
Domain for the Cohesity DataProtect system.
Default: LOCAL
```

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

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

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

Pre-Installation setup for EMC Avamar

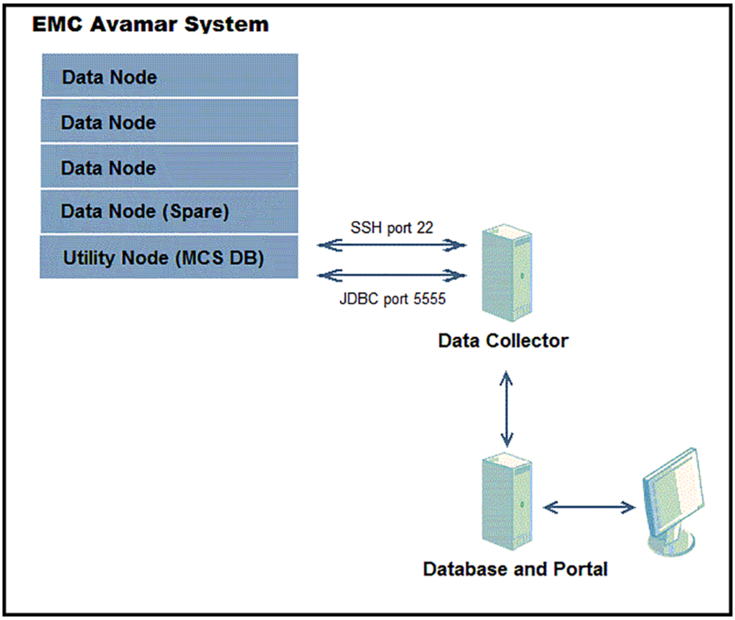
This chapter includes the following topics:

Introduction

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

Architecture overview (EMC Avamar)

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



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

Prerequisites for adding Data Collectors (EMC Avamar)

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

- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- 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. Update the Local Hosts file. This enables Portal access.
2. Add EMC Avamar Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the EMC Avamar data collector policy.
5. On the Data Collector Server, install the Data Collector software.
6. Validate the Data Collector Installation.

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

Add EMC Avamar servers

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

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

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

See "Add/Configure an Avamar Server within the Data Collector policy window" on page 43.

Adding an EMC Avamar Data Collector policy

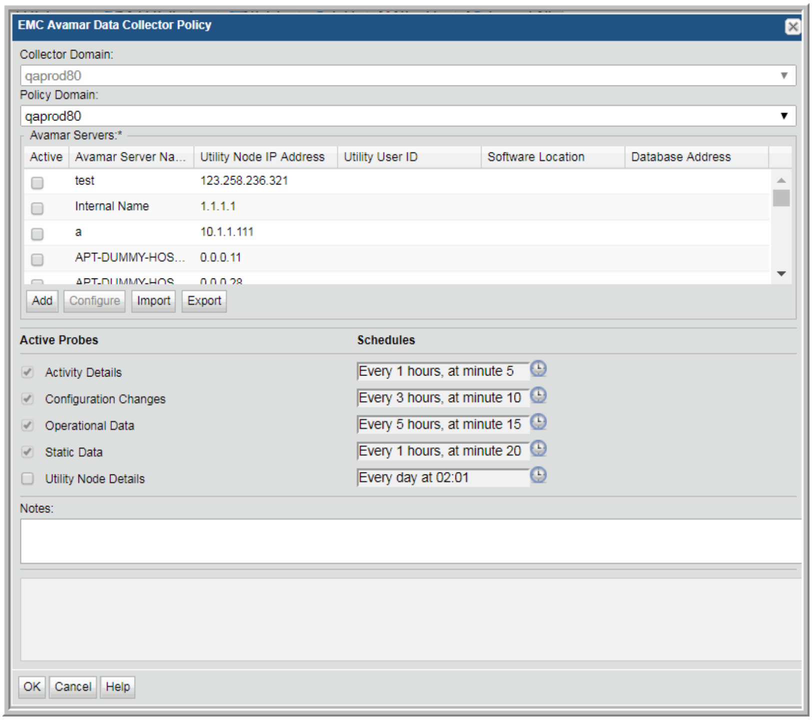
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

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

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

To add the policy

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



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.

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Avamar Servers*	You can add Avamar servers by clicking **Add**. You can also import multiple servers using a .CSV file. You can also do this using the Inventory. The **Avamar Servers** table is populated using any of these methods. The servers added to this table using **EMC Avamar Data Collector Policy** screen are also displayed under **Inventory**. You must indicate which servers are active.
Active	Click **Active** to indicate the Avamar server(s) to use in the data collection policy. For Avamar, this is the Utility Node. If additional fields must be configured, the **Configure Server** dialog is automatically displayed when you make your selection.
Add	Click **Add** to add an Avamar server type. The added servers are also displayed under **Inventory**. **Note:** Data Collector policies can be in place for multiple servers, but a server cannot have multiple policies. See “Add/Configure an Avamar Server within the Data Collector policy window” on page 43.
Configure	Click **Configure** to revise or add information to the Avamar server you selected. See “Add/Configure an Avamar Server within the Data Collector policy window” on page 43.
Import	Click **Import** to browse for the CSV file in which you entered the Avamar server configuration details. See “Import EMC Avamar server information” on page 45.

Field	Description
Export	Click **Export** to create and download a comma-separated values (CSV) file containing all the server information listed in the **Avamar Servers** table. See "Export EMC Avamar server information" on page 46.
Active Probes	Click the clock icon to set a schedule frequency. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. You can set a schedule to collect on: ■ Activity Details ■ Configuration Changes ■ Operational Data ■ Static Data **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Activity Details	Collects backup events/activities from the Avamar server.
Configuration Changes	Collects datasets, retention policies, schedules, Avamar clients, groups and group members from the Avamar server.
Operational Data	Collects node utilization, node space, events, DPN statistics, Garbage Collection (GC) status, current Global Storage Area Network (GSAN) status from the Avamar.
Static Data	Collects the Axion systems, event catalog and plugin catalog entries from the Avamar server.
Utility Node Details	Collects chassis information for the Avamar Utility Node.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

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

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

Testing the collection

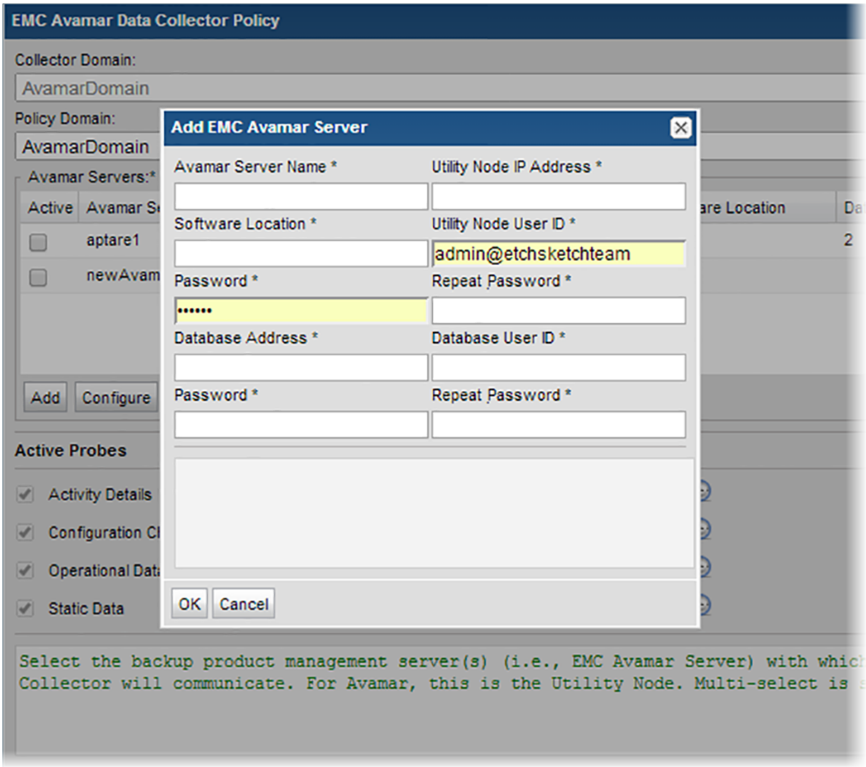
You can test the collection of data using the **Run** functionality available in **Admin**>**Data Collection**>**Collector Administration**. This test run performs a high-level check of the installation, including a check for the domain, host group and URL, plus Data Collector policy and database connectivity.

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

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

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

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



Collector Domain: AvamarDomain

Policy Domain: AvamarDomain

Active	Avamar S	are Location	Da
□	aptare1		2
□	newAvam		

Avamar Server Name *:

Utility Node IP Address *:

Software Location *:

Utility Node User ID *: admin@etchsketchteam

Password *: ••••••

Repeat Password *:

Database Address *:

Database User ID *:

Password *:

Repeat Password *:

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

2. Enter the values:

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

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

Import EMC Avamar server information

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

CSV Format Specifications

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

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

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

Import Notes

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

To Import EMC Avamar Servers

1. Prepare the CSV according to CSV Format Specifications.

   See “CSV Format Specifications” on page 45.
2. Select **Admin** > **Data Collection** > **Collector Administration**.
3. Click **Add Policy**.
4. Select **EMC Avamar**. The **EMC Avamar Data Collector Policy** screen is displayed.
5. Click **Import**. The **Import EMC Avamar Servers** window is displayed. You can browse for the CSV file you created.

Export EMC Avamar server information

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

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

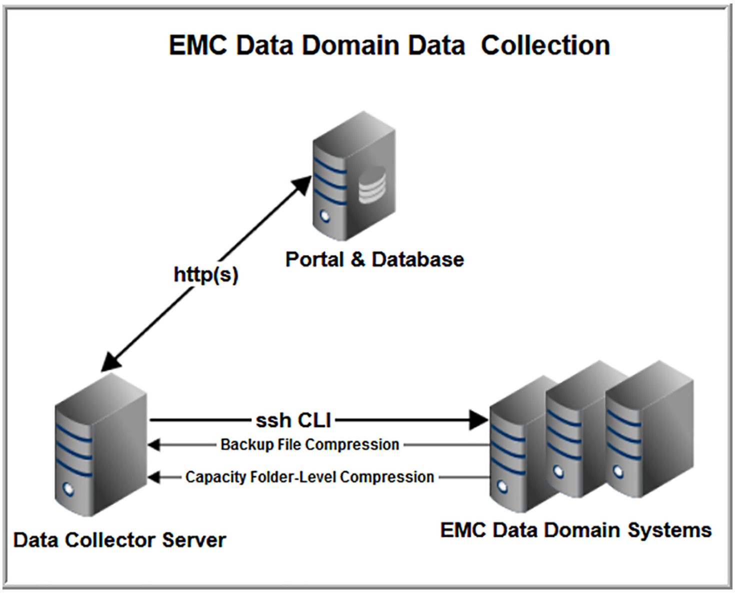
Chapter 5

Pre-Installation setup for EMC Data Domain backup

This chapter includes the following topics:

Architecture overview (EMC Data Domain Backup)

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



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

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

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

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

Prerequisites for adding Data Collectors (EMC Data Domain Backup)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- 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 Primary Servers. These Primary Servers must have an active Data Collector that has successfully completed an initial data collection. Initiate compression rate collection by selecting File-Level Compression in the Data Domain Data Collector Policy.

Installation overview (EMC data domain Backup)

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

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

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

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

Add EMC data domain servers

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

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

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

   See " Add an EMC data domain backup Data Collector policy" on page 50.

Add an EMC data domain backup Data Collector policy

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

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

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

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

To add an EMC data domain backup Data Collector policy

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

   See “Adding/Configuring an EMC data domain server within the Data Collector policy window” on page 54.

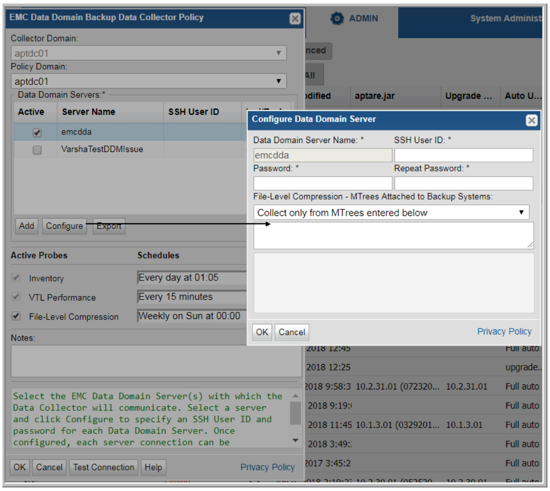
6 When selecting the File-Level Compression probe, additional configuration is required, as follows:

Select a Data Domain Server.

Select the File-Level Compression probe.

Click **Configure**.

See "Configure a data domain server for file-level compression collection" on page 55.



EMC Data Domain Backup Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Data Domain Servers:*

Active	Server Name	SSH User ID
☑	emcdda	
☐	VarshaTestDDMIssue	

Add | Configure | Export

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
```

OK | Cancel | Test Connection | Help | Privacy Policy

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

OK | Cancel | Privacy Policy

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

See See Table 5-1 on page 52.

Table 5-1 Policy Parameters

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

Table 5-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Data Domain Servers*	When you check **Active** for a server shown in the list, a dialog window prompts for the SSH credentials. Alternatively, select a server and click **Configure**. You must indicate which servers are active. You must configure each server with a **Backup Type** of **Data Domain Server**. See "Add EMC data domain servers" on page 50.
Add	Click **Add** to add a Data Domain servers. The added servers are also displayed under **Inventory**. See "Adding/Configuring an EMC data domain server within the Data Collector policy window" on page 54. **Note:** If the hosts already exists, APTARE IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.
Configure	Select a Data Domain server and click **Configure** to enter the SSH credentials that will be used to access the server. This allows provides access to setting up file-level compression. Refer to the following for additional setup information. See "Configure a data domain server for file-level compression collection" on page 55.
Export	Click **Export** to retrieve a list of all the Data Domain servers in a comma-separated values file.
Inventory Probe	Inventory details such as system, disk, tape, and VTL details are collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 5-1 Policy Parameters *(continued)*

Field	Description
VTL Performance	Data associated with the performance of the Data Domain system virtual tape libraries (VTL) is collected by default. Click the clock icon to create a schedule. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available.
File-Level Compression Probe	When this probe is selected, MTrees can be entered into the File-Level Compression list configured for a Data Domain Server. The Data Domain Servers will then display an Include/Exclude column, with negative numbers indicating MTrees are excluded and positive numbers indicating MTrees are included. Hover your mouse over the Incl/Excl column to view the MTrees.If the column displays +0, it indicates no Mtrees have been included in the collection, and -0 indicates no Mtrees have been excluded, so all Mtrees will be collected from. For additional setup information refer to the following section. This section also contains information about RMAN and NetBackup jobs. See “Configure a data domain server for file-level compression collection” on page 55.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. You can also test the collection of data using the **Run** functionality available in **Admin>Data Collection>Collector Administration**. This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

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

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

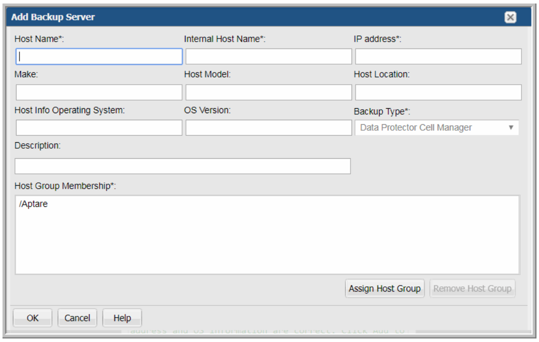
The **Data Domain Servers** table, shown in the policy, is populated using either of these methods. Servers added to this table are also displayed under **Inventory**. The Data Domain Servers table only displays available servers. These servers are not assigned to other policies within the domain.

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

---

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

   The **Add Backup Server** screen displays.



Backup Type*: Data Protector Cell Manager

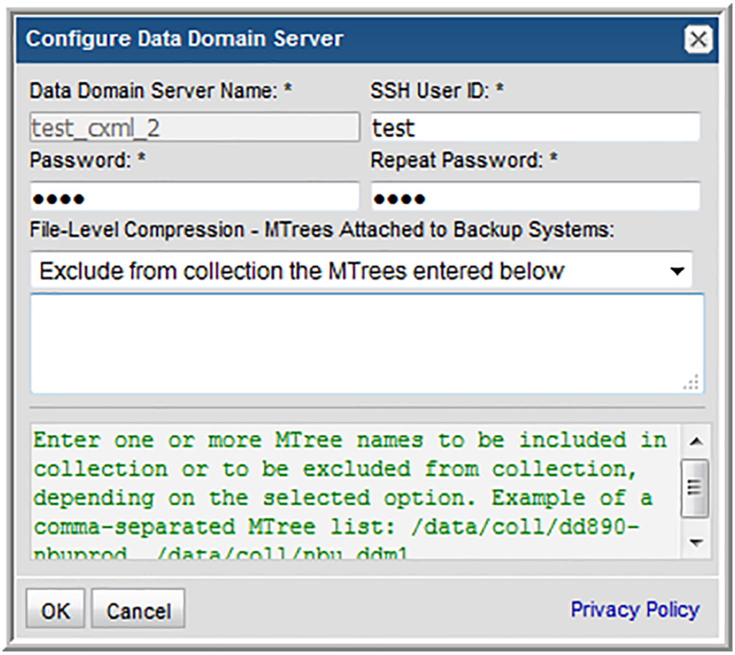
Host Group Membership*: /Aptare

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

Configure a data domain server for file-level compression collection

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

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



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
```

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

Field	Description
Data Domain Server Name*	In order for Data Domain Servers to be listed in the policy window, they must be configured with a **Backup Type** of **Data Domain Server**. See “Add EMC data domain servers” on page 50.
SSH User ID*	The command-line interface (CLI) via SSH is used to gather Data Domain system data. This requires the SSH Service to be enabled and a Data Domain user that has a management role of 'user'. This User ID must be the same for all addresses listed in the System Addresses entry field for the Data Domain systems.

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

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

Field **Description**

Enter one or more MTree names to be included in collection or to be excluded from collection, depending on the selected option. When compression information is collected from the MTree, an attempt is made to connect the file with a backup job that has previously been collected. A 'hint' must be specified to allow this to occur. Currently Oracle RMAN, Veritas NetBackup, and EMC Avamar are supported. For this probe to collect data, the RMAN / NetBackup / Avamar jobs must have been previously collected and all RMAN or NetBackup collection probes must have been run.

Note: The **Exclude from collection the MTrees entered below** field will not collect for Avamar.

To specify an MTree to which RMAN is sending backup files to, enter:

RMAN:[MTree Name].

For NetBackup, enter:

NBU:[MTree Name].

For Avamar, enter:

AVM:[MTree Name].

Example of a comma-separated MTree list: RMAN:/data/col1/rman_su1, NBU:/data/col1/nbu_ddm1

AVM:/data/col1/avamar-1629802442

If you do not specify a hint, it is assumed that the Data Domain MTree contains files created by Veritas NetBackup.

To run File-Level compression across all Mtrees on a Data Domain system, with a 'hint' to specify that the database attempt to link files with Backup jobs, enter:

RMAN:*

or

NBU:*

or

AVM:*

depending on the Backup system using the MTree. Mixed use of wildcards is not supported.

Aggregated global and local compression rates for all NetBackup backup images are collected for all MTrees that are connected to the Active Data Domain servers via DDBOOST and where the NetBackup Data Collector is active and has successfully completed an initial data collection.

Warning: Choosing to exclude collection with an empty MTree list may cause

Field	Description
	collection to take several hours to complete.

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

Chapter 6

Pre-Installation setup for EMC NetWorker

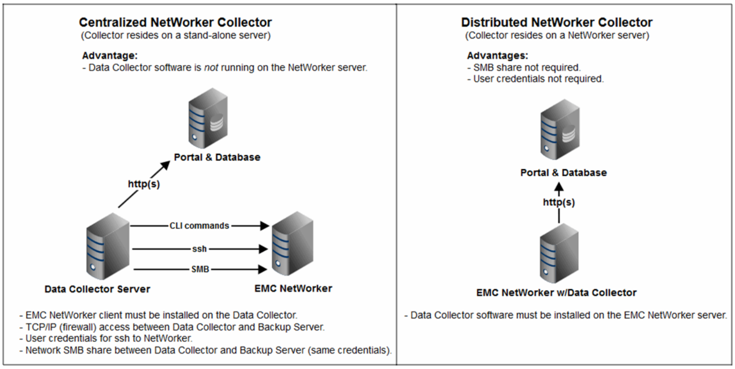
This chapter includes the following topics:

Introduction

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

Architecture overview (EMC 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.

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)

- EMC NetWorker data collection policies are implemented based on vendor version number. Legacy versions of EMC NetWorker (pre version 9.2.1.x) are collected using the policy titled: EMC NetWorker. For EMC NetWorker versions post 9.2.1.x, collection is done using the policy titled: DELL EMC NetWorker Backup & Recovery.
  See “Prerequisites for adding data collectors (Dell EMC NetWorker Backup & Recovery)” on page 72.

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside inBackup Manager the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most 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 a range of WMI 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.
- See "Configure a notification action in EMC NetWorker" on page 70.

Installation overview (EMC NetWorker)

1. Update the Local Hosts file. This enables Portal access.
2. Add EMC NetWorker Servers.
3. In the Portal, add a Data Collector, if one has not already been created.
4. In the Portal, add the EMC NetWorker data collector policy.
5. Configure a notification action in EMC NetWorker.
6. See "Configure a notification action in EMC NetWorker" on page 70.
7. On the Data Collector Server, install the Data Collector software.

8. Validate the Data Collector Installation.

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

Add EMC NetWorker servers

Add a host for each NetWorker server (Utility Node) to NetBackup IT Analytics using the data collector policy screen or through the Inventory.

- 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.

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

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

To add the policy

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

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

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:

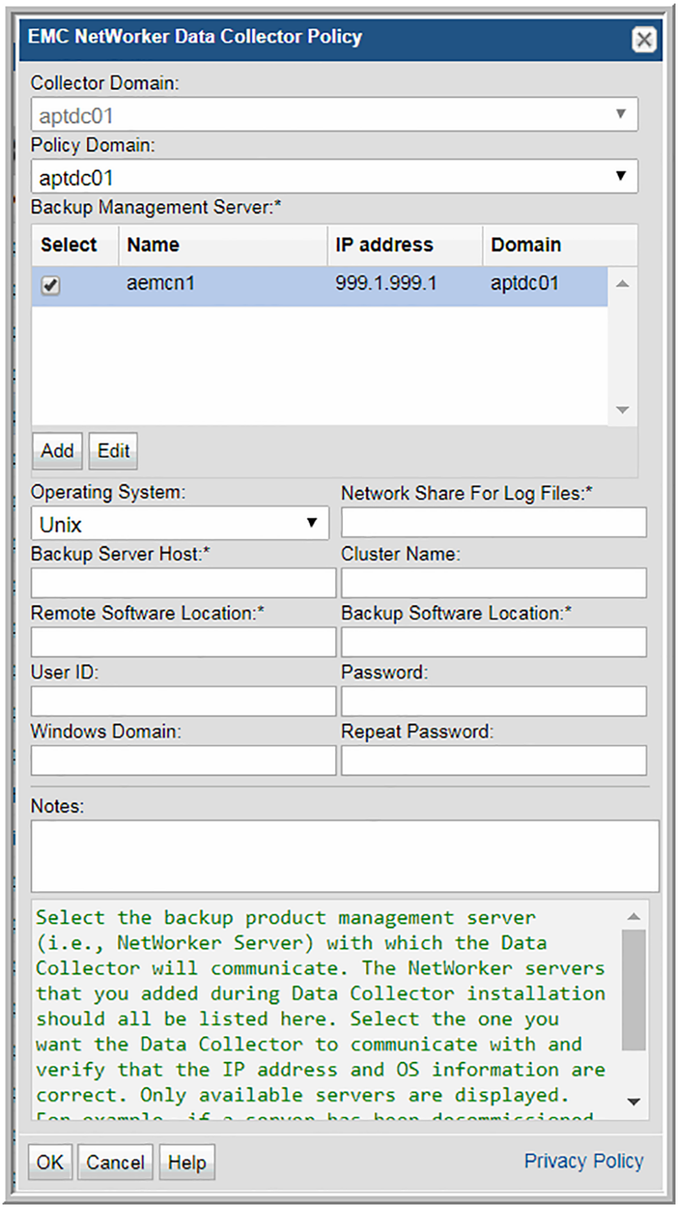
```
<NetWorker install directory>/logs/
```

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” on page 69.



EMC NetWorker 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.

See See Table 6-1 on page 67.

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.

11 Continue to the next step:

See "Configure a notification action in EMC NetWorker" on page 70.

Table 6-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Backup Management Server*	Select the backup product management server (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.

Table 6-1 Policy Parameters *(continued)*

Field	Description
Add	Click **Add** to add a NetWorker server. Once added, servers are also displayed in the Inventory. See "Adding/Editing a EMC NetWorker server within the Data Collector policy" on page 69. **Note:** If the hosts already exists, APTARE IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.
Edit	Select a server and click **Edit** to update the server values.
Operating System	The operating system on which NetWorker is running.
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. Example: 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.

Table 6-1 Policy Parameters *(continued)*

Field	Description
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.

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.
	Example: Administrator

Password	The password associated with the User ID. Example: 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.

Adding/Editing a EMC NetWorker server within the Data Collector policy

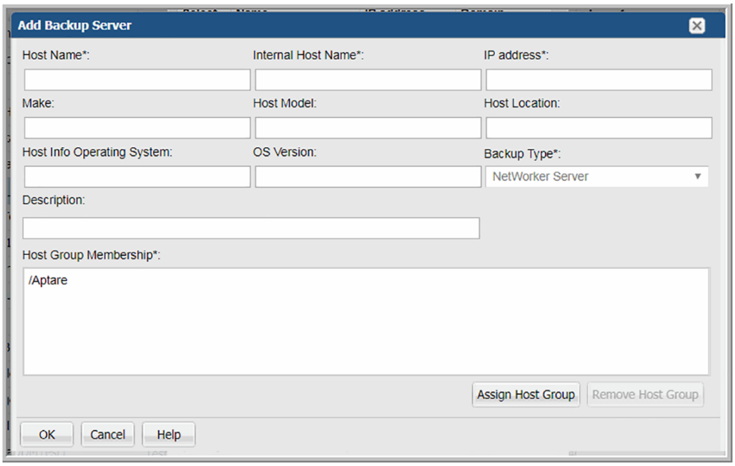
Add and edit EMC NetWorker servers directly from the data collector policy. This functionality is also available in the **Inventory**.

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

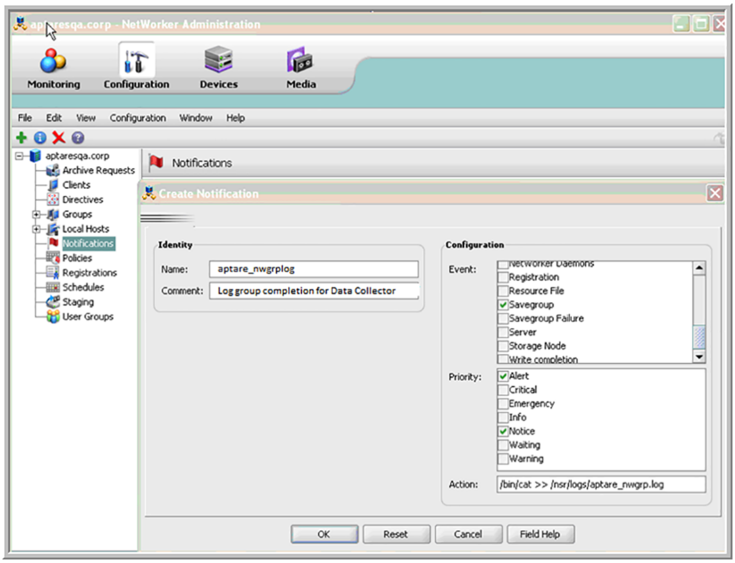
Host Group Membership*: /Aptare

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

Configure a 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.



Create Notification

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**.

Pre-Installation setup for Dell EMC NetWorker backup & Recovery

This chapter includes the following topics:

Introduction

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

Prerequisites for adding data collectors (Dell EMC NetWorker Backup & Recovery)

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

See " Adding an EMC NetWorker Data Collector policy" on page 64.

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- The NetWorker REST API is installed with the NetWorker installation. As part of the installation process, an Apache Tomcat instance is installed and a nonroot -user, nsrtomcat, is created. If your system has special user security requirements, ensure that proper operational permissions are granted to the nsrtomcat users.
- With the NetWorker REST API, all endpoints other than initial landing endpoint (https://your-server-name:9090/nwrestapi/) require authentication. Once a user has been authenticated by the API, permissions to NetWorker resources will be based on the NetWorker permissions for that user.
- Default port number to connect to NetWorker REST API is 9090. This value is configurable in the policy.

Installation overview (Dell EMC Networker Backup & Recovery)

1. Update the Local Hosts file. This enables portal access.
2. In the Portal, add a Data Collector, if one has not already been created.

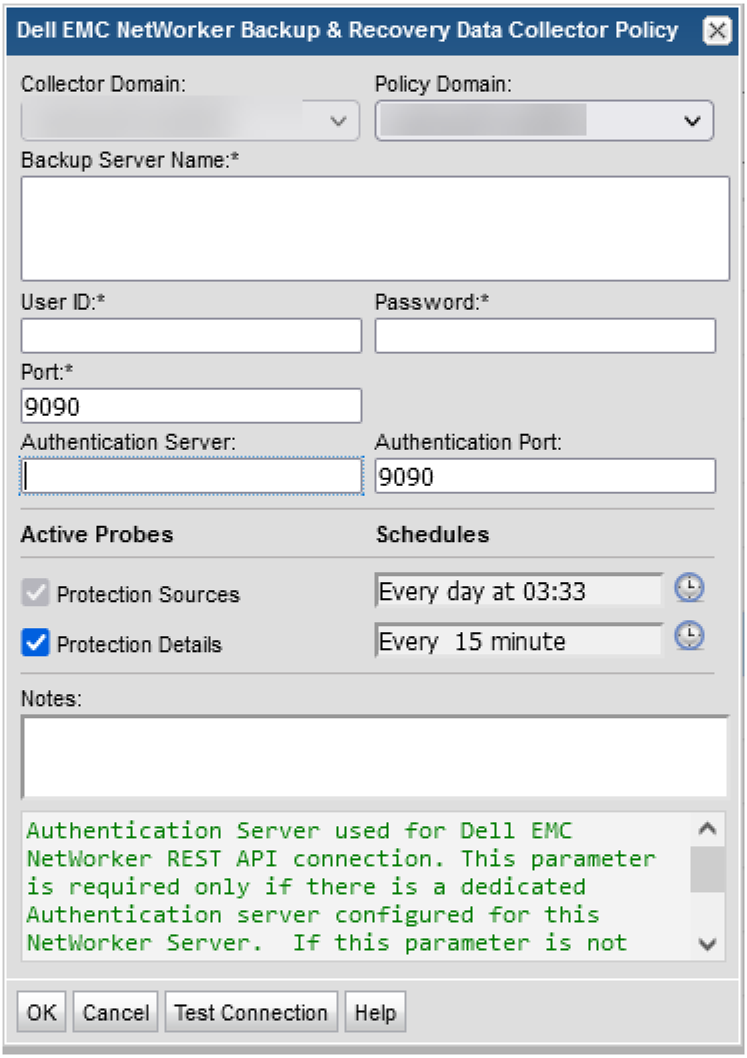
3. In the Portal, add the Dell EMC Networker Backup & Recovery data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the data collector installation.

Adding a Dell EMC Networker Backup & Recovery Data Collector policy

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

To add the policy

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



Dell EMC NetWorker Backup & Recovery Data Collector Policy

Collector Domain:

Policy Domain:

Backup Server Name:*

User ID:*

Password:*

Port:* 9090

Authentication Server:

Authentication Port: 9090

Active Probes | **Schedules**

☑ Protection Sources — Every day at 03:33

☑ Protection Details — Every 15 minute

Notes:

```
Authentication Server used for Dell EMC
NetWorker REST API connection. This parameter
is required only if there is a dedicated
Authentication server configured for this
NetWorker Server.  If this parameter is not
```

Table 7-1 Dell EMC Networker Backup and Recovery Data Collector policy

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

Table 7-1 Dell EMC Networker Backup and Recovery Data Collector policy *(continued)*

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

Table 7-1 Dell EMC Networker Backup and Recovery Data Collector policy *(continued)*

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

Chapter 8

Pre-Installation setup for generic backup

This chapter includes the following topics:

Introduction

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

Generic backup data collection

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

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

See “Manually load the CSV file (generic backup)” on page 84.

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

Prerequisites for adding Data Collectors (Generic Backup)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.

- Create a comma-separated file of the backup/restore data--typically, export the data using the backup software utilities.
  See “CSV format specification” on page 86.

Installation overview (generic backup)

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

Add generic backup servers

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

Add a generic backup Data Collector policy

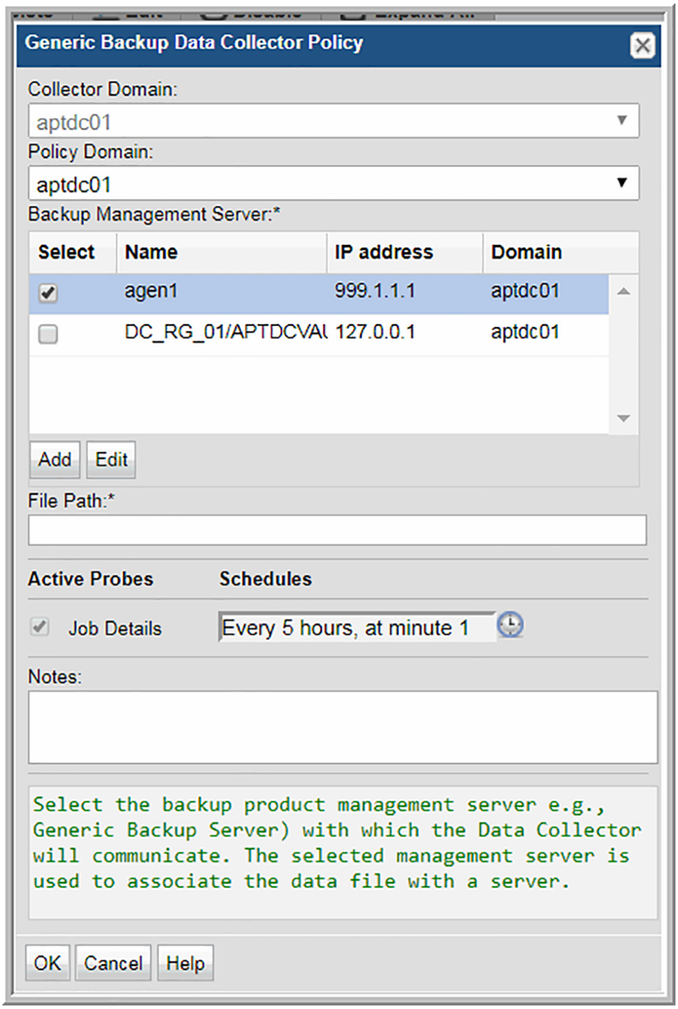
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.
- After adding the policy: For some policies, collections can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

To add the policy

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

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

Note: In this instance, select Generic Backup.



Generic Backup Data Collector Policy

Collector Domain: aptdc01

Policy Domain: aptdc01

Backup Management Server:*

Select	Name	IP address	Domain
☑	agen1	999.1.1.1	aptdc01
□	DC_RG_01/APTDCVAl	127.0.0.1	aptdc01

Add Edit

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 (*).

See See Table 8-1 on page 82.

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

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

Table 8-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings. Example: **yourdomain**
Backup Management Server*	Select the backup product management server, e.g., Generic Backup Server with which the Data Collector will communicate. The selected management server is used to associate the data file with a server.
Add	Click **Add** to add a Generic Backup server. Added servers are also displayed in the Inventory. See “Adding/Editing a generic backup server within the Data Collector policy” on page 83.
Edit	Select a server and click **Edit** to update the server values.

Table 8-1 Policy Parameters *(continued)*

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

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

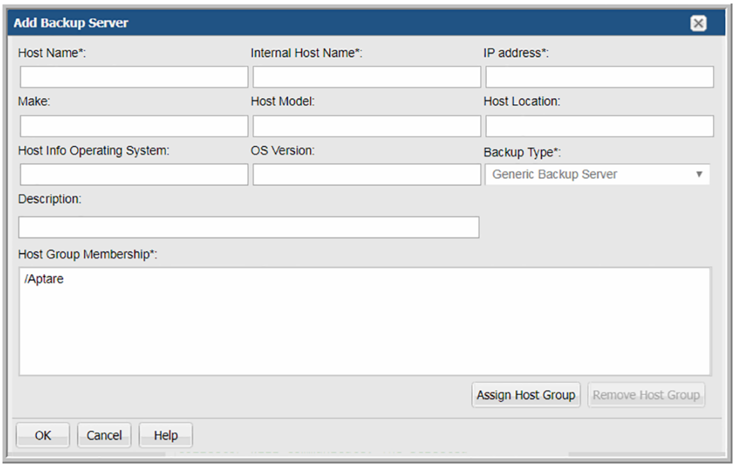
Add and edit Generic Backup servers directly from the data collector policy. This functionality is also available in the **Inventory**.

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

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

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

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



Add Backup Server

Host Name*:

Internal Host Name*:

IP address*:

Make:

Host Model:

Host Location:

Host Info Operating System:

OS Version:

Backup Type*: Generic Backup Server

Description:

Host Group Membership*: /Aptare

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

Manually load the CSV file (generic backup)

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

Pre-requisites:

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

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

   Windows:

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

Linux:

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

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

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

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

   Windows:

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

   Linux:

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

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

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

CSV format specification

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

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

Table 8-2 CSV format specification

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

Table 8-2 CSV format specification *(continued)*

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

Table 8-2 CSV format specification *(continued)*

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

EXAMPLE: genericBackupJobs.csv

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

Chapter 9

Pre-Installation setup for HP Data Protector

This chapter includes the following topics:

Introduction

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

Architecture overview (HP Data Protector)

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

Cell Manager

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

Disk agent (backup agent)

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

Media agent

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

Client systems

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

User interface (UI)

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

Prerequisites for adding Data Collectors (HP Data Protector)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 5555, WMI range of ports, Linux ssh 22
- The HP Data Protector (HPDP) client software version must match the specific version (major and minor) of the HPDP server being probed.

Installation overview (HP Data Protector)

1. Update the Local Hosts file. This enables Portal access.
2. Identify the specific HP Data Protector elements required for the Data Collector configuration:
   - See “Identify HP Data Protector collection requirements” on page 92.

- See “Configure the Data Collector server in Cell Manager (HP Data Protector)” on page 95.
- See “Configure an HP Data Protector admin user” on page 96.
- See “Validate HP Data Protector setup” on page 97.

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

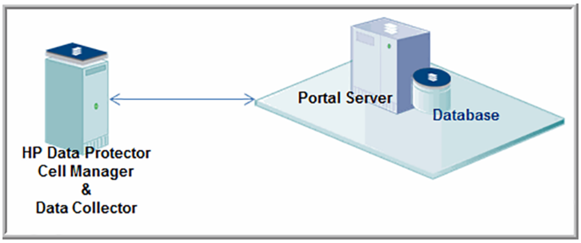
   See “Add HP Cell Manager servers to NetBackup IT Analytics” on page 97.
4. In the Portal, add a Data Collector, if one has not already been created.
5. Configure an HP Data Protector data collection policy.
6. On the Data Collector Server, install the Data Collector software.
7. Validate the Data Collector Installation.

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

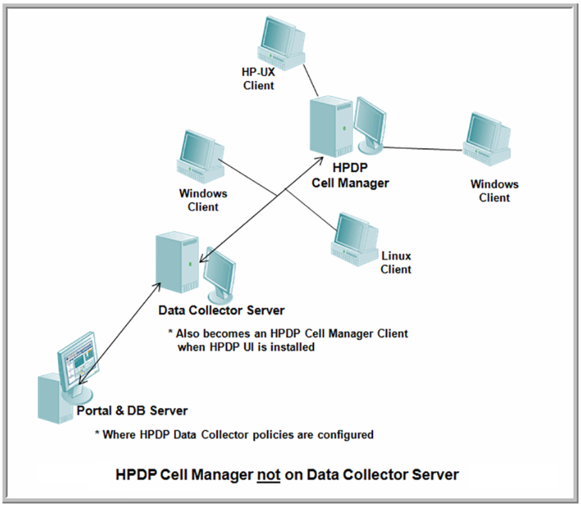
Identify HP Data Protector collection requirements

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

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



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


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 NetBackup IT Analytics Data Collector server.

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

On the HP Data Protector Cell Manager server:

1. Identify the Cell Manager Server's Name:

   ____

2. Identify the OS of the Cell Manager Server:

   ____

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

   ____

   Typically, this location will be:

   Windows: C:\Program Files\Omniback

   Linux: /opt/omni

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

   See "Configure the Data Collector server in Cell Manager (HP Data Protector)" on page 95.

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

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

   See "Configure an HP Data Protector admin user" on page 96.

On the NetBackup IT Analytics Data Collector Server:

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

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

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

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

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

Requirements for the Data Collector (Windows)

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

Steps to Configure the Data Collector Server in Cell Manager

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

On the HP Data Protector Cell Manager Server:

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

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

- Data Protector Java UI (Linux):

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

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

   See “Configure an HP Data Protector admin user” on page 96.

3. Validate the conditions.

   See “Validate HP Data Protector setup” on page 97.

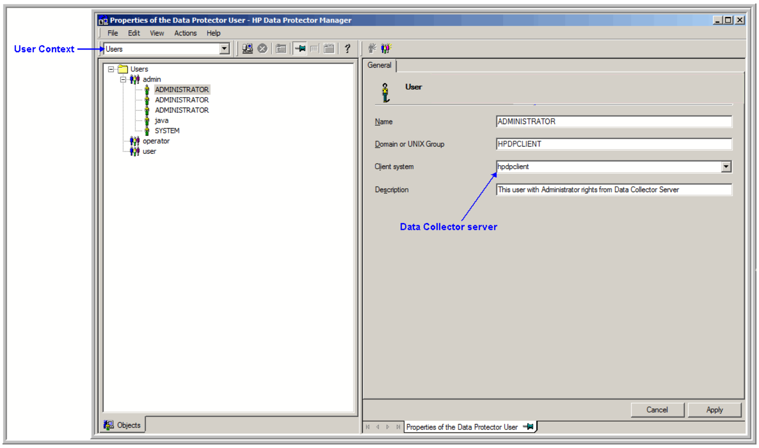
Configure an HP Data Protector admin user

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 NetBackup IT Analytics

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

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

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

Add an HP Data Protector Data Collector policy

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

  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.

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

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

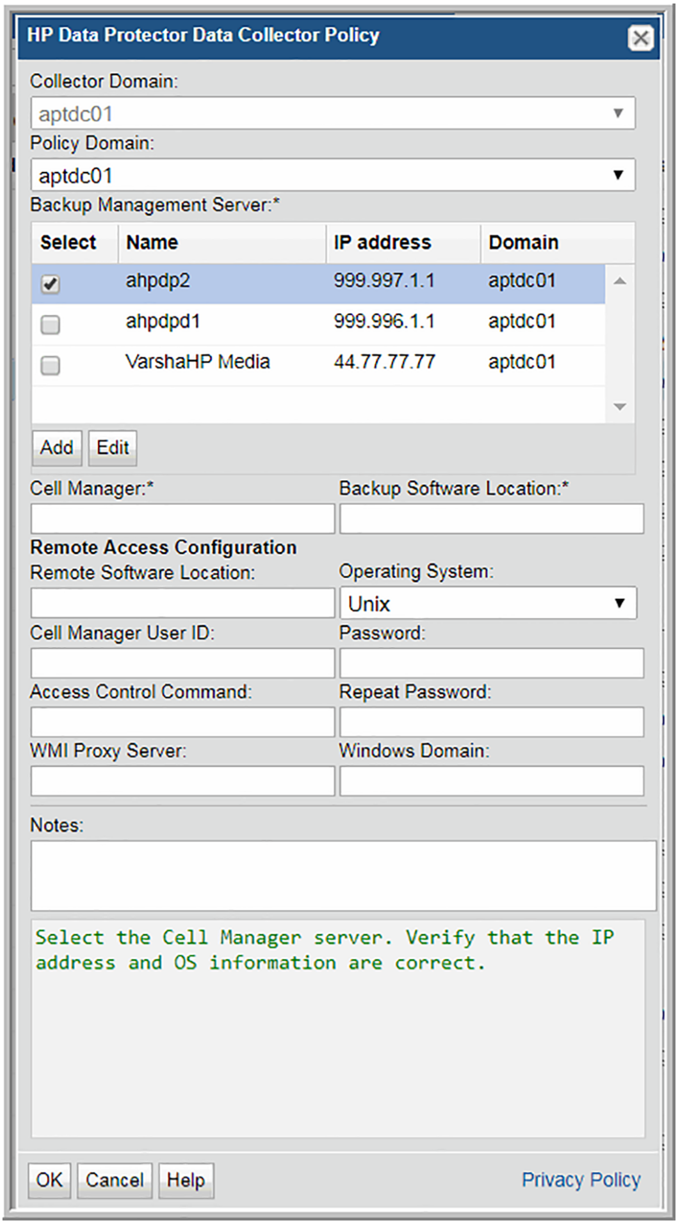
To add the policy

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

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

See "Add/Edit a HP Data Protector server within the Data Collector policy" on page 103.

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



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.

Table 9-1

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

Table 9-1 *(continued)*

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

Table 9-1 *(continued)*

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

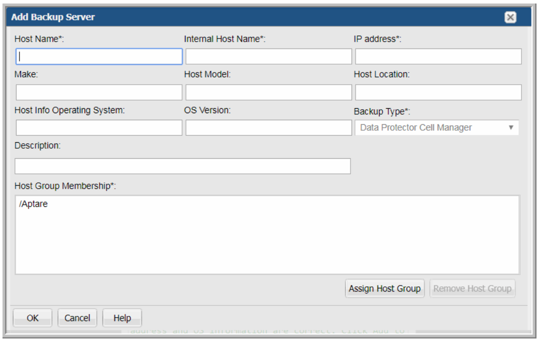
Add/Edit a HP Data Protector server within the Data Collector policy

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

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

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

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



Backup Type*: Data Protector Cell Manager

Host Group Membership*: /Aptare

3. Enter or update values. Required fields are denoted by *.

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

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

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

Tune the configuration

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

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

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

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

Chapter 10

Pre-Installation setup for IBM Spectrum Protect (TSM)

This chapter includes the following topics:

Introduction

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

Architecture overview (IBM Spectrum Protect -TSM)

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

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

IBM Spectrum Protect (TSM) - servers and instances defined

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

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

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

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server’s language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same

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

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

Installation overview (IBM Spectrum Protect - TSM)

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

Add IBM Spectrum Protect (TSM) servers

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

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

- Backup Type = IBM Spectrum Protect (TSM) Server

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

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

See “Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy” on page 113.

Adding an IBM Spectrum Protect (TSM) Data Collector policy

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

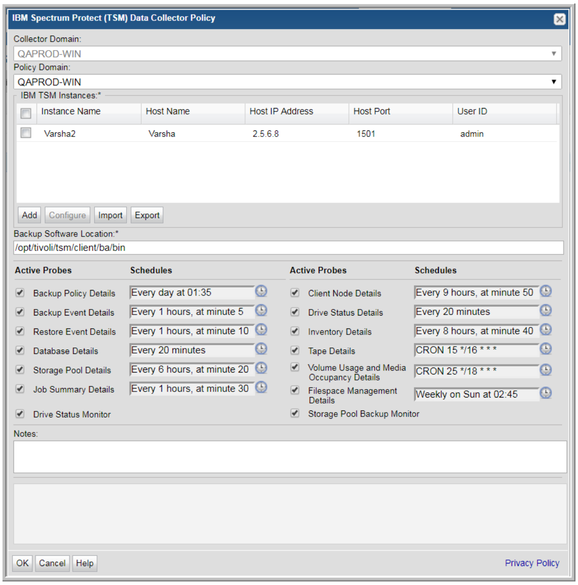
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only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

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

To add the policy

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

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



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 (*):

See See Table 10-1 on page 109.

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

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

Table 10-1 Policy Parameters

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

Table 10-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. (The Collector Domain is the domain that was supplied during the Data Collector installation process.) The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
IBM Spectrum Protect (TSM) Instances	
Active	Click **Active** to indicate the IBM Spectrum Protect (TSM) server/instances to use in the data collection policy. Multi-select is supported. If additional fields must be configured, the **Configure Server** dialog is automatically displayed when you make your selection.
Add	Click **Add** to add an IBM Spectrum Protect (TSM) server/instance. The IBM Spectrum Protect (TSM) servers added to this table using **IBM Spectrum Protect (TSM) Data Collector Policy** screen are also displayed in the Inventory **Note:** Data Collector policies can be in place for multiple instances, but an instance cannot exist in multiple policies. See “Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy” on page 113.
Configure	Select a row in the **IBM Spectrum Protect (TSM) Instances** table. Double-click or click **Configure** to revise or add information to the TSM server/instance you selected. See “Add/Configure an IBM Spectrum Protect (TSM) server within the Data Collector policy” on page 113.

Table 10-1 Policy Parameters *(continued)*

Field	Description
Import	Click **Import** to browse for the CSV file in which you entered the IBM Spectrum Protect (TSM) server/instance configuration details. This enables you quickly add a list of IBM Spectrum Protect (TSM) instances or servers. See "Import IBM Spectrum Protect (TSM) information" on page 115.
Export	Click **Export** to create and download a comma-separated values (CSV) file containing all the host/instance information listed in the **IBM Spectrum Protect (TSM) Instances** table. This enables you to extract your IBM Spectrum Protect (TSM) server information and transfer it easily into a spreadsheet or some other media. See "Export IBM Spectrum Protect (TSM) server information" on page 116.
Backup Software Location*	The home directory of the TSM Admin Client software--that is, the dsmadmc command on the Data Collector server. Typically `C:\Program Files\Tivoli\TSM\baclient` for Windows, or /opt/tivoli/tsm/client/ba/bin for Linux
Active Probes and Schedules	
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Backup Policy Details	Collects backup policy details including policy name, policy identifier, date and time as it relates to the specified IBM Spectrum Protect (TSM) instances/servers.
Backup Event Details	Collects backup event details including backup type, client names, duration, dates, size, files, directories and so on.
Restore Event Details	Collects restore event details such as job duration, number of files backed up and also skipped, amount of data restored, and restore job status.

Table 10-1 Policy Parameters *(continued)*

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

Table 10-1 Policy Parameters *(continued)*

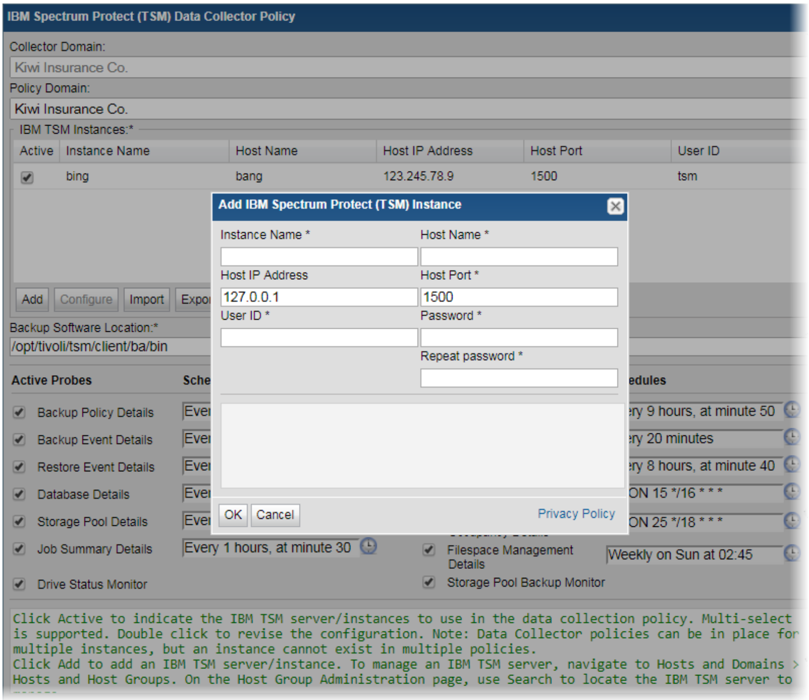
Field	Description
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

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

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

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

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



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	Sche…		…edules
☑ Backup Policy Details	Ever…		…ry 9 hours, at minute 50
☑ Backup Event Details	Ever…		…ry 20 minutes
☑ Restore Event Details	Ever…		…ry 8 hours, at minute 40
☑ Database Details	Ever…		ON 15 */16 * * *
☑ Storage Pool Details	Ever…		ON 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	

```
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.

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

Import IBM Spectrum Protect (TSM) information

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

CSV format specifications

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

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

To import IBM Spectrum Protect (TSM) hosts

1. Prepare the CSV according to CSV format specifications.

   See “CSV format specifications” on page 115.

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

Export IBM Spectrum Protect (TSM) server information

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

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

Pre-Installation setup for NAKIVO Backup & Replication

This chapter includes the following topics:

Introduction

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

Prerequisites for adding data collectors (NAKIVO Backup & Replication)

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

- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- NAKIVO Backup & Replication Server must have the license that allows access to NetBackup IT Analytics reporting REST APIs. User credentials to access NetBackup IT Analyticsreporting REST APIs are also required.
- Install only one Data Collector on a server (or OS instance).
- Default port 4443 - Director Web UI port (used during NAKIVO Backup & Replication installation.

Installation overview (NAKIVO Backup & Replication)

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

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

Add a NAKIVO Backup & Replication Data Collector policy

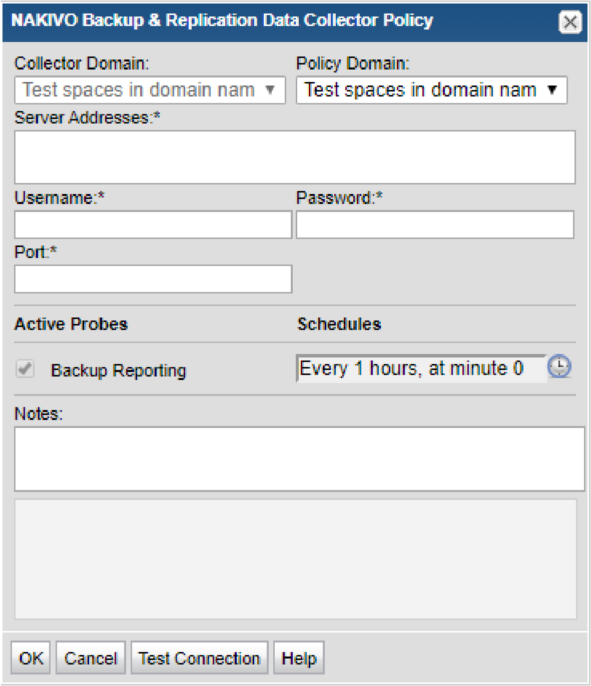
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. See Adding/Editing Data Collectors. For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide.

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

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

To add the policy

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



NAKIVO Backup & Replication Data Collector Policy

Collector Domain: Test spaces in domain nam ▾
Policy Domain: Test spaces in domain nam ▾
Server Addresses:*
Username:*
Password:*
Port:*

Active Probes	Schedules
☑ Backup Reporting	Every 1 hours, at minute 0

Notes:

Table 11-1 NAKIVO Backup & Replication Data Collector Policy

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

Table 11-1 NAKIVO Backup & Replication Data Collector Policy *(continued)*

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

Chapter 12

Pre-Installation setup for Veritas Backup Exec

This chapter includes the following topics:

Introduction

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

Architecture overview (Veritas Backup Exec)

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

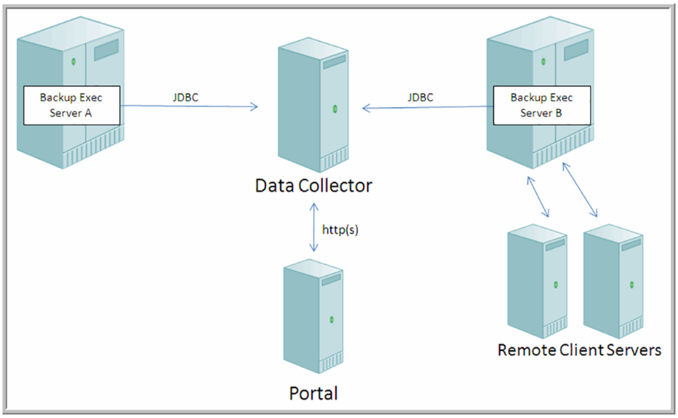


Figure 1 Data Collector in a Veritas Backup Exec Environment

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

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

Backup Exec terminology

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

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

Prerequisites for adding data collectors (Veritas Backup Exec)

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Veritas NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses TCP port 1433. The BUE collector first connects via UDP on port 1434 to get information about available SQL Server instances, then connects via TCP to the port number that is returned for the specified instance. By default this is 1433.
- If your environment requires NTML v2 authentication (Windows authentication) for the data collection connection, create an Advanced Parameter named USE_NTML_V2 and set the value to Y. Note that the NetBackup IT Analytics default is NTML v1 (database authentication). Windows authentication is used when the Backup Exec server credentials configured in the Data Collector Policy contain a Windows domain name, user name, and password. If Windows credentials are not in the policy, the connection defaults to using database authentication.
- The Backup Exec Administrator account used by the Data Collection policy must have the database role membership of **db_datareader** for the BEDB (Backup Exec Database).
- Note that the version of Backup Exec that is reported by the Backup Exec 15 installation is version 14.2.

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 NetBackup 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)
```

Upgrade MS SQL Server to the latest version to enable secure collection. Your MS SQL Server version may not be supported for NetBackup 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.

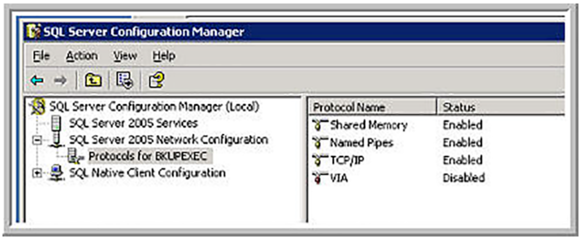
Installation overview (Veritas Backup Exec)

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

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

Enable TCP/IP for the SQL server

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


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

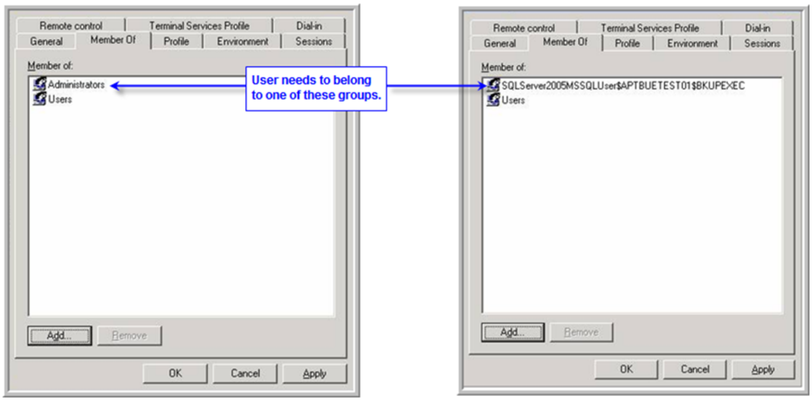
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

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.

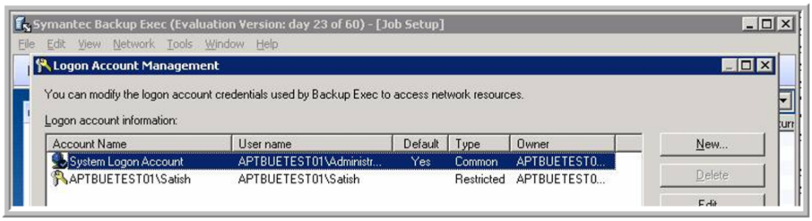
1. Complete the worksheet found in the Appendix of this guide, providing configuration details for each backup server that will be polled by a Data Collector.
2. Ensure that you have a **Windows User** that is a member of one of the following groups, either locally or as part of the Windows Domain:

- 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.



User needs to belong to one of these groups.

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 NetBackup IT Analytics.

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

Importing Backup Exec Server information

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

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

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

   Each line in the CSV file should follow this format:

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

   Example CSV File:

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

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

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

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

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

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

Add a Veritas Backup Exec Data Collector policy

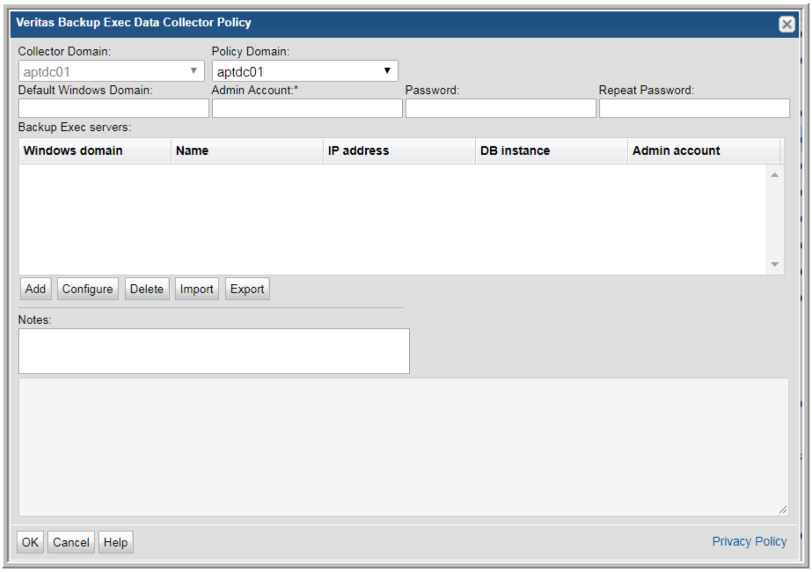
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies. For specific prerequisites and supported configurations for a specific vendor, see the Certified Configurations Guide .
- After adding the policy: For some policies, collections can be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

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

To add the policy

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

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



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.

See See Table 12-1 on page 131.

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

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

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

Table 12-1 Policy Parameters

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

Table 12-1 Policy Parameters *(continued)*

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

Chapter 13

Pre-Installation setup for Veritas NetBackup

This chapter includes the following topics:

Introduction

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

General prerequisites for adding Data Collectors (Veritas NetBackup)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- In support of near-real time collection for Veritas NetBackup, the following knowledge base article discusses additional information about nbu_monitor_util: https://www.veritas.com/support/en_US/article.100047232.
- Windows Only Requirement -
  If a Data Collector is required to collect data from Veritas NetBackup Primary Server running on Windows System to non-English (United States) locale:
  - A Windows user must be created with the Administrative group of Windows system that will run the data Collector with culture set to English-US, and Region and Language set to English -US.
  - The current system locale must be set to the same language as the NetBackup Primary Server.
- For performance reasons, do not install Data Collectors on the same server as the Portal. 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 443, 1556, and 13724 WMI range of ports, Linux ssh 22
- The NetBackup Event Monitor probe, enabled on the data collector policy screen, uses the nb_monitor_util executable. This executable is installed by default for

all NetBackup 8.2 installations. It can be found in the /usr/openv/netbackup/bin/goodies directory on Linux and \Program Files\Veritas\Netbackup\bin\goodies on Windows. The Event Monitor probe collects events generated by the nb_monitor_util and handles create/update/delete events for Backup Policy, Storage Unit, Storage Unit Group and Storage Lifecycle Policy.

- The data collection, while executing the NetBackup probes, is supported even if the root/admin users does NOT have the CLI access permission in NetBackup.

Note: This scenario is applicable in the distributed environment.

See "Centralized or distributed deployment (Veritas NetBackup)" on page 135.

Centralized or distributed deployment (Veritas NetBackup)

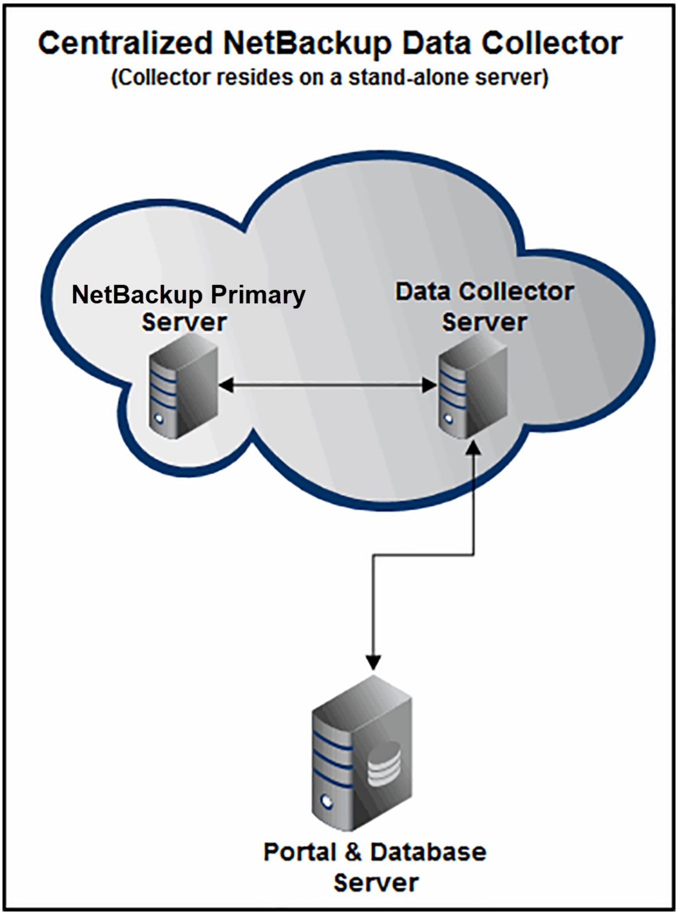
Two upgrade/installation options are available. Choose the one that best meets your needs.

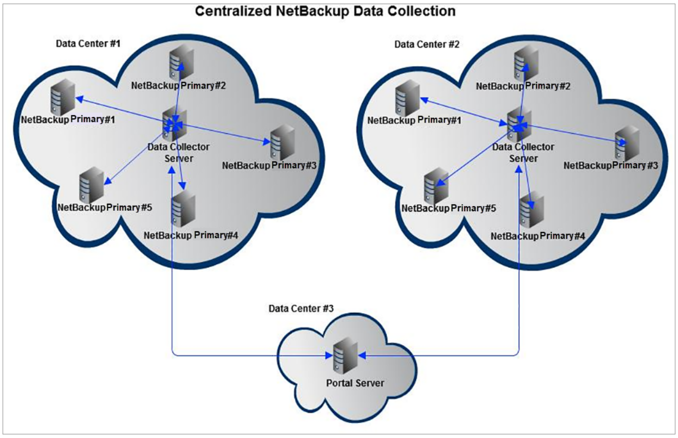
- See "Centralized NetBackup data collection (Recommended)" on page 135.
- See "Distributed NetBackup data collection" on page 149.

Note: Irrespective of the number client primary servers configured for data collection, NetBackup IT Analytics can collect from a maximum of two primary servers at a time in parallel. Other collections will be queued during the process.

Centralized NetBackup data collection (Recommended)

Use a centralized Data Collector to collect data from multiple NetBackup Primary Servers, without any NetBackup IT Analytics software installed on the Primary Servers, as illustrated below.


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


Centralized NetBackup Data Collection
Data Center #1
NetBackup Primary#2
NetBackup Primary#1
Data Collector Server
NetBackup Primary#3
NetBackup Primary#5
NetBackup Primary#4
Data Center #2
NetBackup Primary#2
NetBackup Primary#1
Data Collector Server
NetBackup Primary#3
NetBackup Primary#5
NetBackup Primary#4
Data Center #3
Portal Server

Prerequisites to use SSH and WMI (Veritas NetBackup)

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.

Click here to know how to set up a fixed port for WMI,.

- While performing remote collection, each policy must have either Linux or Windows Primary Servers, but not both. The credentials entered on the policy screen will be used for all selected Primary Servers.
- When collecting data using remote SSH or WMI, the NetBackup software does not need to be installed on the collector.
- Using the SSH Collection method to a NetBackup Primary Server requires a user with superuser privileges to run NetBackup commands. You may configure additional security requirements using NetBackup Access Control (NBAC) or sudo.
- You may use a non-privileged user and enable the additional security requirements to run these commands using NetBackup Access Control (NBAC) or sudo.
- The SSH Collection method creates temporary files for command output. For SSH collection the temporary directory location is controlled by the TMPDIR environment variable (defaulting to /tmp). For WMI the temporary directory location is controlled by the TEMP environment variable.
- Veritas NetBackup Appliances require additional setup and permissions to use SSH for collection.

Configure NetBackup Access Control (NBAC) for NetBackup Data Collection

NetBackup data collection using the SSH Collection method to a NetBackup Primary Server requires root privileges to run NetBackup commands. If your security requirements require NBAC to provide elevated privileges, follow the instructions in your *Veritas NetBackup Security and Encryption Guide* for using the nbac_cron utility. Note that the credentials are valid for one year and will need to be refreshed prior to expiration.

Configure NetBackup sudo access for NetBackup data collection

Collection of NetBackup data using the SSH Collection method to a NetBackup Primary Server requires root privileges to run NetBackup commands.

If your security requirements require sudo access to provide temporary, elevated privileges, use the following instructions. NetBackup IT Analytics requires the use of passwordless sudo.

- Create a Linux user to grant sudo access.
- Modify the sudo Configuration. Depending on the version of Linux, either run the `visudo` command, or create a drop-in sudoers file in the correct directory to restrict the commands that this user can execute.

To modify the sudoers file

1. Configure `visudo` to modify the sudoers file. `visudo` will use the editor specified in the $EDITOR variable, or vi, by default. Specify a preferred editor. For example, to use nano as your editor, execute the following:

   ```
   export EDITOR=nano
   ```

2. Once the preferred editor is configured, execute the following commands. Use `visudo` if available.

   ```
   visudo -f /etc/sudoers.d/<username>
   ```

3 Add the following lines to the sudoers file, substituting the name of the user you created for <username>:

```
Defaults:<username> !requiretty
<username> ALL=(ALL) NOPASSWD: \
/usr/openv/netbackup/bin/admincmd/* ,\
/usr/openv/volmgr/bin/* ,\
/usr/openv/netbackup/bin/*
```

Or to further restrict access to NetBackup administrative commands, use the following:

```
Defaults:<username> !requiretty
<username> ALL=(ALL) NOPASSWD: \
/usr/openv/netbackup/bin/admincmd/bpgetconfig ,\
/usr/openv/netbackup/bin/admincmd/bpcoverage ,\
/usr/openv/netbackup/bin/admincmd/bpdbjobs ,\
/usr/openv/netbackup/bin/admincmd/bpimagelist ,\
/usr/openv/netbackup/bin/admincmd/bperror ,\
/usr/openv/netbackup/bin/admincmd/bppllist ,\
/usr/openv/netbackup/bin/admincmd/bpretlevel ,\
/usr/openv/netbackup/bin/admincmd/bpplclients ,\
/usr/openv/netbackup/bin/admincmd/bpmedialist ,\
/usr/openv/netbackup/bin/admincmd/bpstulist ,\
/usr/openv/netbackup/bin/admincmd/nbdevquery ,\
/usr/openv/netbackup/bin/admincmd/nbauditreport ,\
/usr/openv/netbackup/bin/admincmd/nbstl ,\
/usr/openv/netbackup/bin/admincmd/nbstlutil ,\
/usr/openv/netbackup/bin/admincmd/bpstsinfo ,\
/usr/openv/netbackup/bin/admincmd/bpminlicense ,\
/usr/openv/volmgr/bin/vmquery ,\
/usr/openv/volmgr/bin/vmpool ,\
/usr/openv/volmgr/bin/vmglob ,\
/usr/openv/volmgr/bin/vmcheckxxx ,\
/usr/openv/volmgr/bin/vmoprcmd ,\
/usr/openv/volmgr/bin/tpconfig ,\
/usr/openv/netbackup/bin/bplist ,\
/usr/openv/netbackup/bin/nbsqladm ,\
/usr/openv/netbackup/bin/nboraadm
```

4 Save the sudoers file.

Configure NetBackup Appliances for Data Collection

1. Create a new NetBackup administrator CLI user account, for example "aptare". Refer to *Creating NetBackup administrator user accounts* in the *Veritas NetBackup™ Appliance Administrator's Guide*.

2. Create a location for temporary files (e.g. /log/aptare/tmp).

   ```
   maintenance-!> sudo bash
   root-!> mkdir -p /log/aptare/tmp
   ```

3. Assign read and write permissions to the folder for the CLI user account and nbusers group.

   Refer to *Overriding the NetBackup appliance intrusion prevention system policy* in the *Veritas NetBackup™ Appliance Security Guide.*

   ```
   maintenance-!> sudo bash
   root-!> chown -R aptare:nbusers /log/aptare
   ```

4. Create a .profile file in the `/home/nbusers` directory.

   It is recommended to use a .profile that only sets TMPDIR for the CLI user created for collection.

   For example:

   ```
   if [ "${USER}" = "aptare" ] ; then

       TMPDIR=/log/aptare/tmp

       export TMPDIR

   fi
   ```

   OR

   Use the advanced parameter NBU_SSH_TMPDIR. For available methods of configuring the TMPDIR environment variable.

   See “Veritas NetBackup SSH: Changing the Linux Temporary Directory for Collection” on page 144.

Configure NetBackup Flex Appliances for Data Collection

To configure NetBackup Flex Appliances for data collection, you must first create a new user account on the Flex primary server and grant `sudo` access to the user account in `/etc/sudoers.d` and `/mnt/nbdata/vxos/etc/sudoers.d`, as described in the procedure below. You must also obtain the REST API key from the NetBackup UI.

1 Open a SSH session to the NetBackup instance as an admin or root user to create an **appadmin** user.

2 Create a local user account:

```
sudo useradd <username>
sudo passwd <username>
```

3 Grant `sudo` access to the local user account created above in `/etc/sudoers.d`:

- Create `sudoers` file in `/etc/sudoers.d`, substituting the name of the user you created for <username>.

  ```
  sudo visudo -f /etc/sudoers.d/<username>
  ```

- Add these permissions in the interactive editor.
  To allows unrestricted access to all the permissions:

  ```
  Defaults:<username> !requiretty
  <username> ALL=(ALL) NOPASSWD: \
  /usr/openv/netbackup/bin/admincmd/* ,\
  /usr/openv/volmgr/bin/* ,\
  /usr/openv/netbackup/bin/*
  ```

  Or to further restrict access to NetBackup administrative commands, use the following:

  ```
  Defaults:<username> !requiretty
  <username> ALL=(ALL) NOPASSWD:
  /usr/openv/netbackup/bin/admincmd/bpgetconfig ,\
  /usr/openv/netbackup/bin/admincmd/bpcoverage ,\
  /usr/openv/netbackup/bin/admincmd/bpdbjobs ,\
  /usr/openv/netbackup/bin/admincmd/bpimagelist ,\
  /usr/openv/netbackup/bin/admincmd/bperror ,\
  /usr/openv/netbackup/bin/admincmd/bpminlicense ,\
  /usr/openv/netbackup/bin/admincmd/bppllist ,\
  /usr/openv/netbackup/bin/admincmd/bpretlevel ,\
  /usr/openv/netbackup/bin/admincmd/bpplclients ,\
  /usr/openv/netbackup/bin/admincmd/bpmedialist ,\
  /usr/openv/netbackup/bin/admincmd/bpstulist ,\
  /usr/openv/netbackup/bin/admincmd/nbdevquery ,\
  /usr/openv/netbackup/bin/admincmd/nbauditreport ,\
  /usr/openv/netbackup/bin/admincmd/nbstl ,\
  ```

```
/usr/openv/netbackup/bin/admincmd/nbstlutil ,\
/usr/openv/netbackup/bin/admincmd/bpstsinfo ,\
/usr/openv/volmgr/bin/vmquery ,\
/usr/openv/volmgr/bin/vmpool ,\
/usr/openv/volmgr/bin/vmglob ,\
/usr/openv/volmgr/bin/vmcheckxxx ,\
/usr/openv/volmgr/bin/vmoprcmd ,\
/usr/openv/volmgr/bin/tpconfig ,\
/usr/openv/netbackup/bin/bplist ,\
/usr/openv/netbackup/bin/nbsqladm ,\
/usr/openv/netbackup/bin/nboraadm
```

- Save and exit the interactive editor.

4 Grant sudo access to the local user account created above in /mnt/nbdata/vxos/etc/sudoers.d:

- Create sudoers file in /mnt/nbdata/vxos/etc/sudoers.d.

```
sudo visudo -f  /mnt/nbdata/vxos/etc/sudoers.d/<username>
```

- Add these permissions in the interactive editor.
  To allows unrestricted access to all the permissions:

```
Defaults:<username> !requiretty
<username> ALL=(ALL) NOPASSWD: \
/usr/openv/netbackup/bin/admincmd/* ,\
/usr/openv/volmgr/bin/* ,\
/usr/openv/netbackup/bin/*
```

Or to further restrict access to NetBackup administrative commands, use the following:

```
Defaults:<username> !requiretty
<username> ALL=(ALL) NOPASSWD:
/usr/openv/netbackup/bin/admincmd/bpgetconfig ,\
/usr/openv/netbackup/bin/admincmd/bpcoverage ,\
/usr/openv/netbackup/bin/admincmd/bpdbjobs ,\
/usr/openv/netbackup/bin/admincmd/bpimagelist ,\
/usr/openv/netbackup/bin/admincmd/bperror ,\
/usr/openv/netbackup/bin/admincmd/bpminlicense ,\
/usr/openv/netbackup/bin/admincmd/bppllist ,\
/usr/openv/netbackup/bin/admincmd/bpretlevel ,\
/usr/openv/netbackup/bin/admincmd/bpplclients ,\
/usr/openv/netbackup/bin/admincmd/bpmedialist ,\
/usr/openv/netbackup/bin/admincmd/bpstulist ,\
/usr/openv/netbackup/bin/admincmd/nbdevquery ,\
/usr/openv/netbackup/bin/admincmd/nbauditreport ,\
/usr/openv/netbackup/bin/admincmd/nbstl ,\
/usr/openv/netbackup/bin/admincmd/nbstlutil ,\
/usr/openv/netbackup/bin/admincmd/bpstsinfo ,\
/usr/openv/volmgr/bin/vmquery ,\
/usr/openv/volmgr/bin/vmpool ,\
/usr/openv/volmgr/bin/vmglob ,\
/usr/openv/volmgr/bin/vmcheckxxx ,\
/usr/openv/volmgr/bin/vmoprcmd ,\
/usr/openv/volmgr/bin/tpconfig ,\
/usr/openv/netbackup/bin/bplist ,\
/usr/openv/netbackup/bin/nbsqladm ,\
/usr/openv/netbackup/bin/nboraadm
```

- Save and exit the interactive editor.

5 Obtain the REST API key from the NetBackup UI and copy it in the **API key** field. The **API key** field appears on **Add Backup Server** or **Edit Backup Server** popup that is displayed when you click **Add** or **Edit** on the **Veritas NetBackup Data Collector Policy** window.

Configure custom RBAC for FETB collection

To execute NetBackup IT Analytics data collector properly, a non-root user requires access to the NetBackup using API/CLI method. The FETB section of the NetBackup policy collection will fail if the non-root user is NOT configured.

Configuring a customs RBAC user in NetBackup is required.

Note: To know more about configuring a RBAC role in NetBackup, see *NetBackup Web UI Administrator's Guide* > *Managing Security* > *Managing role-based access control* > *Add a customs RBAC role* section.

Note: You need to select **Customs** option when configuring the user.

A NetBackup administrator needs to provide the following permission to the respective user by creating a custom role and associating the role with that non-root user using Netbackup WebUI.

Namespace	Required operation
IMAGES	VIEW
LICENSING	VIEW
CLI sessions	CLI execute
MALWARE|SCAN-TOOL	VIEW
MALWARE|SCAN-HOST	VIEW
MALWARE|SCAN-HOST-POOL	VIEW
MALWARE:VIEW-SCAN-RESULT	VIEW

Note: The user needs to have customs role access with global access permissions in NetBackup to execute data collection successfully.

Veritas NetBackup SSH: Changing the Linux Temporary Directory for Collection

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

Option 1: User Profile

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

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

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

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

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

```
    export TMPDIR
fi
```

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

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

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

Option 2: Advanced Parameter

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

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

Prerequisites for NetBackup collection over SSH (Kerberos option)

These prerequisites and parameter configurations enable the NetBackup policy to perform data collection through Kerberos authentication.

Prerequisites

Ensure the following prerequisites:

- Data collector and NetBackup systems are under Kerberised domain.
- Password-less SSH using Kerberos authentication from Data Collector system to NetBackup server works without errors.
- The data collector system must have the `keytab/ticket cache` file ready, which contains the Kerberos user service keys for authentication.
- The `krb5.conf` file must be present at the below location. It contains information related to the default realm and kdc server address
  - Linux: `/etc/krb5.conf`
  - Solaris: `/etc/krb5/krb5.conf`

- Verify the SSH configurations for Kerberos on the data collector and NetBackup server as follows:
  - Ensure that the following lines are present in the `/etc/ssh/ssh_config` file. If required, add them within the **Hosts** section. Make sure these lines are uncommented.
    GSSAPIAuthentication
    GSSAPIDelegateCredentials
  - Set the values of the following configuration to **yes** in the `/etc/ssh/sshd_config` file. Make sure these lines are uncommented.
    KerberosAuthentication
    KerberosOrLocalPasswd
    KerberosTicketCleanup
    GSSAPIAuthentication
    GSSAPICleanupCredentials

Enable Kerberos authentication for NetBackup SSH collection

These steps describe the advanced parameter configuration required for the data collection by the NetBackup policy

1 On the NetBackup IT Analytics Portal, go to **Admin** > **Advanced** > **Parameters**.

2 Add the advanced parameters and their respective default values as specified in the table below:

Parameter	Default Parameter Value	Server
SUPPRESS_KERBEROS_PROMPT (Mandatory)	N	Enter the NetBackup server IP.
KERBEROS_USE_TICKET_CACHE (Mandatory)	Y	None
KERBEROS_TICKET_CACHE	Enter the path to the ticket cache on the data collector server, only if KERBEROS_USE_TICKET_CACHE value is set to **Y**. Default location of the ticket cache: `/tmp/krb5cc_`*`<uid>`* Ensure the root user does not have access to this file.	None
KERBEROS_KEYTAB_LOCATION	Enter the `keytab` file location on data collector server, only if KERBEROS_USE_TICKET_CACHE value is set to **N**.	None
NBU_VXSS_CREDENTIALS (Mandatory)	Enter the custom VXSS credentials file location on the NetBackup Primary Server.	None

3 Proceed to set up the NetBackup policy as suggested below:

- Provide all the required details for creating the policy.
- Enter the Kerberos non-human ID as the **Primary Server User ID** and non-empty **Primary Server Password** for Kerberos user authentication.
- Set **Collection Method** as **SSH or WMI protocol to NetBackup Primary Server**.

See “ Add a Veritas NetBackup Data Collector policy” on page 154.

4 Validate the connection using **Test Connection**.

The test takes some time to complete at first so test again if required. Verify the status from the logs to ensure a successful connection.

Prerequisites for collection from Veritas NetBackup deployed as a Docker image

This section describes the portal configurations required, before adding a Veritas NetBackup policy, when Veritas NetBackup is deployed as a Docker image in the cloud and it is using the cloud resources to perform backups.

SSH key-based authentication

Since Veritas NetBackup is deployed as a Docker image, it must communicate with the Data Collector using SSH key-based authentication.

1 Generate an SSH public/private key pair. This key will be required later during configuration. To generate this key pair, run the `ssh-keygen` command on a Linux system or an equivalent command on Windows.

Save the public and private key pair along with the passphrase used while generating the key, as you will need to provide the private key path and the passphrase while creating the NetBackup Collection policy in NetBackup IT Analytics Portal.

2 Copy the public key to the **itAnalyticsPublicKey** spec of the Environment Custom Resource `environment.yaml`. You can find this file on the jumpserver that was used to create the initial NetBackup setup on Kubernetes cluster.

3 Apply the update to **itAnalyticsPublicKey** spec using `kubectl apply -f environment.yaml`. The `environment.yaml` file is available on the jumpserver used to create the NetBackup primary server setup on Kubernetes cluster.

Alternatively, if the jumpserver is not accessible, use `kubectl edit environment <environment_name> -n <namespace>` command to edit the environment to add the public key to the itAnalyticsPublicKey sec

4 On a successful deployment, describe the Environment Custom Resource using `kubectl describe PrimaryServer <primary-server-name> -n <namespace>`.

Get Veritas NetBackup API key

This API key is required when you add or edit a Veritas NetBackup primary server for the Veritas NetBackup policy configuration. This API key is essential especially when NetBackup IT Analytics has to collect metrics from NetBackup deployed as a Docker image in the cloud.

See the *Manage API keys* section from the *NetBackup Web UI Security Administrator's Guide* for steps to get the API key.

Firewall consideration

If the Firewall of the NetBackup primary server is turn on, follow these steps to communicate through the Firewall port:

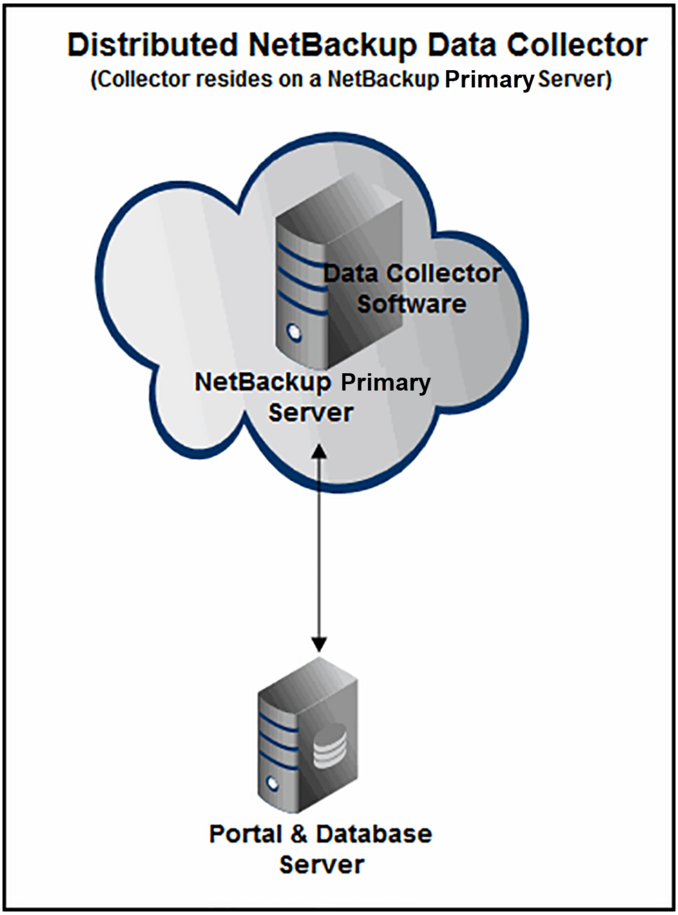
1. Open and edit the file `/etc/firewalld/zones/public.xml`.
2. Add the following lines in the file:

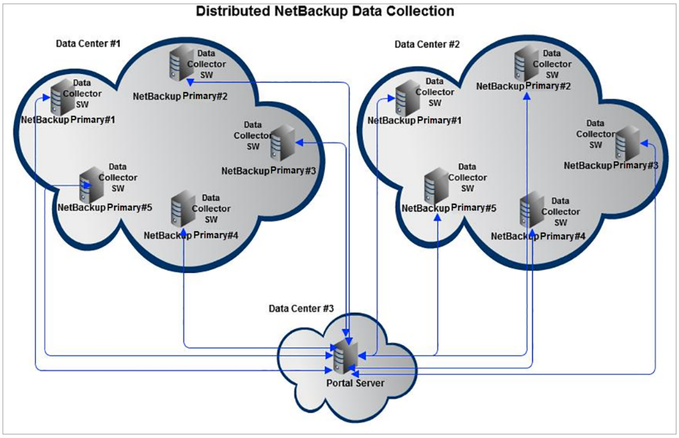
   ```
   <service-name="https"/>

   <port protocol = "tcp" port="1556">
   ```

3. Save the file.

Distributed NetBackup data collection

NetBackup IT Analytics Data Collector software is installed on each NetBackup Primary Server.


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


Distributed NetBackup Data Collection
Data Center #1
Data Collector SW
NetBackup Primary#1
Data Collector SW
NetBackup Primary#2
Data Collector SW
NetBackup Primary#3
Data Collector SW
NetBackup Primary#5
Data Collector SW
NetBackup Primary#4
Data Center #2
Data Collector SW
NetBackup Primary#1
Data Collector SW
NetBackup Primary#2
Data Collector SW
NetBackup Primary#3
Data Collector SW
NetBackup Primary#5
Data Collector SW
NetBackup Primary#4
Data Center #3
Portal Server

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

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 Primary Server will be automatically updated to 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 Primary Server and select the type as **Veritas Primary Server**.
4. In the Portal, for each NetBackup Primary 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 Primary Server.
   - NetBackup Data Collector Policy for the New Data Collector.
5. For both upgrades and new installations, install the Data Collector software on each NetBackup Primary Server.
6. On each NetBackup Primary Server, run checkinstall.

   See “Validation methods” on page 234.
7. Start the Data Collector.

Enable access to the Veritas NetBackup Primary Server

Centralized NetBackup Data Collector must be able to access the NetBackup Primary Server to retrieve metadata. If this access is not authorized, Data Collector 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 Primary Server.

Linux Primary Servers

If the NetBackup Primary 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)

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 following steps.

- Review the requirements.
  See "Centralized or distributed deployment (Veritas NetBackup)" on page 135.
  See "Enable access to the Veritas NetBackup Primary Server" on page 151.
- Ensure that Ports 1556 and 13724 are open.

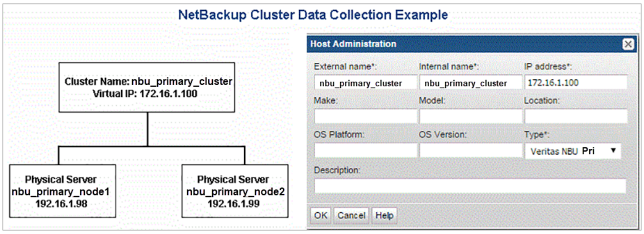
Collecting from NetBackup clusters

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

Best practices for collecting from NetBackup clusters

- Install the Data Collector on both Primary 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 Primary Server belongs to a cluster, when you add the Data Collector server via the NetBackup IT Analytics Portal, enter the `NetBackup Cluster Name` for the Internal Name along with the cluster's Virtual IP address.
- See "Clustered NetBackup upgrade procedure" on page 153.



External name*: nbu_primary_cluster
Internal name*: nbu_primary_cluster
IP address*: 172.16.1.100
Make:
Model:
Location:
OS Platform:
OS Version:
Type*: Veritas NBU Pri
Description:

Clustered NetBackup upgrade procedure

For Distributed NetBackup deployments only (Data Collector software is installed on each NetBackup Primary 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 Primary 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.

Add a Veritas NetBackup Data Collector policy

Prerequisites

To add a Veritas NetBackup Data Collector policy, you must have:

- Data Collector added on the NetBackup IT Analytics Portal. See *Add/Edit Data Collectors* section in the *NetBackup IT Analytics User Guide* for more information. Preserve the user ID and passcode used while adding a Data Collector on the portal and use the same credentials to install and configure the Data Collector software on the Data Collector server.
- Data Collector server installed with the collector software.

  For specific prerequisites and supported configurations for a specific vendor, see the *NetBackup IT Analytics Certified Configurations Guide*.

  See "Install Data Collector Software on Windows" on page 209.

  See "Install Data Collector software on Linux" on page 220.
- NetBackup Primary Server (RBAC or NBAC) user credentials with the required access permissions. The steps to enable the access permissions for NetBackup users are described below.

User permissions for RBAC-enabled NetBackup

This option of applying permissions to a custom role is applicable for NetBackup 9.0 and later. If you enter a non-root user, you must create a custom role in NetBackup web UI RBAC screen with the following permissions and attach the role to this user ID. See *Add a custom RBAC role* section in *NetBackup Web UI Administrator's Guide* for steps to create a custom role.

1. Select all the **View** permission for all the objects under **NetBackup Management**, **Protection**, and **Storage** sections of the NetBackup web UI.
2. From the **NetBackup Management** > **CLI Sessions** section under, enable **CLI Execute**.
3. From the **NetBackup Management** > **NetBackup Management**, enable **View scan results**.

User permissions for NBAC-enabled NetBackup

If you are configuring the policy in an environment with NetBackup Access Control (NBAC), provide the credential of a NetBackup user created using the following steps:

1. Login as an Administrator to the NBAC-enabled NetBackup and go to **Security Management** > **Access management** > **User group**.
2. Create a new user group for the NetBackup IT Analytics collection.

3. Within the new user group, select **Authenticated principles** as assigned users.

4. From the **Permissions** tab, assign these permissions from the respective section for the NetBackup IT Analytics collection.

   - **Job**: **Browse**, **Read** permissions.
   - **Policy**: **Browse**, **Read** , **Operate**, **Configure** permissions.
   - **Drive**: **Browse**, **Read** permissions.
   - **Media**: **Browse**, **Read** permissions.
   - **Robot**: **Browse**, **Read** , **Operate**, **Configure** permissions.
   - **Device Host**: **Browse**, **Read** permissions.
   - **Storage Unit**: **Browse**, **Read** permissions.
   - **NetBackup Catalog**: **Browse**, **Read** permissions.
   - **Audit**: **Browse**, **Read**, **Run Report** permissions.
   - **Volume Pool**: **Browse**, **Read** permissions.
   - **Report**: **Browse**, **Read** permissions.

To add Veritas NetBackup Data Collector policy:

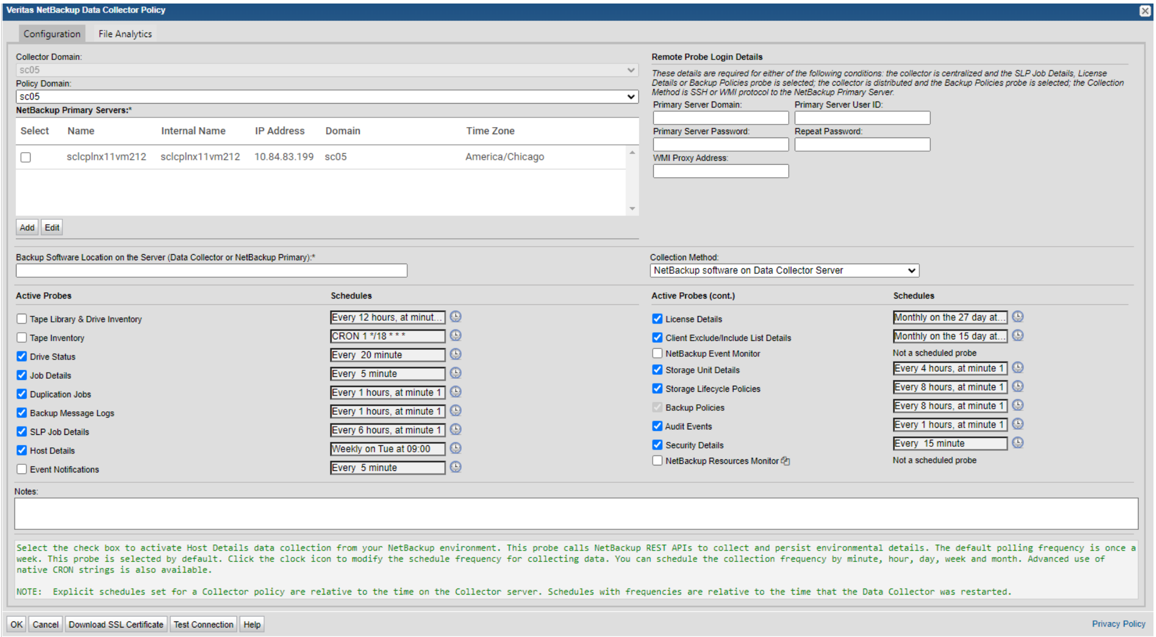
1. Select **Admin** > **Data Collection** > **Collector Administration**. Currently configured Data Collectors are displayed.

2. Select the Data Collector from the list to which you want to add the policy. Use the filter to find the collector if required.

3 Click **Add Policy**, and then select **Veritas NetBackup** from the policy list.

4 Configure the Veritas NetBackup Data Collector policy based on the filed descriptions under policy parameters below and then click **OK** to save the policy. Mandatory parameters are denoted by an asterisk (*).

See the section called “Policy Parameters” on page 156.



Collector Domain: sc05

Policy Domain: sc05

NetBackup Primary Servers:*

Select	Name	Internal Name	IP Address	Domain	Time Zone
☐	sclcplnx11vm212	sclcplnx11vm212	10.84.83.199	sc05	America/Chicago

Remote Probe Login Details

These details are required for either of the following conditions: the collector is centralized and the SLP Job Details, License Details or Backup Policies probe is selected; the collector is distributed and the Backup Policies probe is selected; the Collection Method is SSH or WMI protocol to the NetBackup Primary Server.

Primary Server Domain:
Primary Server User ID:
Primary Server Password:
Repeat Password:
WMI Proxy Address:

Backup Software Location on the Server (Data Collector or NetBackup Primary):*

Collection Method: NetBackup software on Data Collector Server

Active Probes	Schedules
☐ Tape Library & Drive Inventory	Every 12 hours, at minut...
☐ Tape Inventory	CRON 1 */18 * * *
☑ Drive Status	Every 20 minute
☑ Job Details	Every 5 minute
☑ Duplication Jobs	Every 1 hours, at minute 1
☑ Backup Message Logs	Every 1 hours, at minute 1
☑ SLP Job Details	Every 6 hours, at minute 1
☑ Host Details	Weekly on Tue at 09:00
☐ Event Notifications	Every 5 minute

Active Probes (cont.)	Schedules
☑ License Details	Monthly on the 27 day at...
☑ Client Exclude/Include List Details	Monthly on the 15 day at...
☐ NetBackup Event Monitor	Not a scheduled probe
☑ Storage Unit Details	Every 4 hours, at minute 1
☑ Storage Lifecycle Policies	Every 8 hours, at minute 1
☑ Backup Policies	Every 8 hours, at minute 1
☑ Audit Events	Every 1 hours, at minute 1
☑ Security Details	Every 15 minute
☐ NetBackup Resources Monitor	Not a scheduled probe

Notes:

```
Select the check box to activate Host Details data collection from your NetBackup environment. This probe calls NetBackup REST APIs 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.

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.
```

Policy Parameters

The following are the fields and its description:

- **Collector Domain**: The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
- **Policy Domain**: The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain.

  The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain.

Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy.

- **NetBackup Primary Servers**: Select the NetBackup Primary Server(s) from which data will be collected. Multi-select is supported. Only available NetBackup Primary 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. Optionally, add/edit a NetBackup Primary server. These operations can also be completed in the **Inventory** tab.
- **Add**: Click **Add** to add a NetBackup server. Added servers are also displayed in the Inventory. See "Add/Edit NetBackup Primary Servers within the Data Collector policy" on page 164.

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

- **Edit**: Select a server and click **Edit** to update the server values.
- **Backup Software Location on the Server (Data Collector or NetBackup Primary Server)**: Backup Software Location should point to a location on either the Data Collector server or the NetBackup Primary Server. The location should either be the root folder or directory to the netbackup/volmgr folder(s) where the NetBackup software is installed.

Note: If you are using the SSH/WMI remote collection method, this location is where the NetBackup software is installed on all the remote NetBackup Primary Servers that are configured.

Default Backup Software Home location for NetBackup:

For Windows: `C:\Program Files\Veritas`.

For Linux: `/usr/openv`.

- **Collection Method**: Select from **NetBackup Software on a Data Collector Server** (default) or **SSH or WMI protocol to NetBackup Primary Server**. When **NetBackup Software on Data Collector Server** is selected, then the probe **NetBackup Event Monitor** is unselected, and following probes are selected: Storage Unit Details, Storage Lifecycle Policies, and Backup Policies.

  When **SSH or WMI protocol to NetBackup Primary Server** is selected, the probe **NetBackup Event Monitor** is unselected and disabled.

- **Remote Probe Login Details**: These details are required for either of the following conditions.
  - The collector is centralized and the SLP Job Details, License Details, or Backup Policies probe is selected.
  - The collector is distributed and the Backup Policies probe is selected.
  - The Collection Method is SSH or WMI protocol to the NetBackup Primary Server.
- **Primary Server Domain**: Specify the domain associated with the NetBackup Primary Server User ID. For Windows Primary 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 Primary Server; unused for remote Linux Primary Servers. In addition, for NetBackup 7.7.3 only, this domain is used by the License Details probe to collect plugin information (bpstsinfo).

  For NetBackup 8.3 and above, this domain is used by Backup Policies probe (FETB and Protection Plan collection) for REST API based authentication.

  This field is required when the Collection Method is SSH or WMI protocol to the NetBackup Primary Server and that Primary Server is a Windows Server.
- **Primary Server User ID**: This field is required when the Collection Method is SSH or WMI protocol to the NetBackup Primary Server. Depending on NBAC or RBAC-enabled NetBackup, enter the appropriate credentials of the user created using the steps described in the prerequisites above.

  Specify the user name with login rights on the selected NetBackup Primary 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 Primary 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.

  In case of NetBackup 8.3 and above, these credentials are also used by the Backup Policies probe for REST API based authentication. These credentials will be used for all Primary Servers.

  If SSH/WMI collection is specified, the username must have superuser privileges to run most NetBackup commands.
- **Primary Server Password**: This field is required when the Collection Method is SSH or WMI protocol to the NetBackup Primary Server.

  The password associated with the NetBackup Primary 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 Primary Server. In addition, for NetBackup 7.7.3

only, the credentials are used by the License Details probe to collect plugin information (bpstsinfo).

In case of NetBackup 8.3 and above these credentials are also used by the Backup Policies probe for REST API based authentication. These credentials will be used for all Primary Servers.

If password-based login to NetBackup primary server is not allowed, for example in cloud deployment of NetBackup, then SSH private key can be specified here in the following format:

privateKey=<path-of-private-key>|password=<passphrase> where

- <path-of-private-key>| is the file path of the SSH private key.
- <passphrase> is the password used while creating the SSH private key.

See "Prerequisites for collection from Veritas NetBackup deployed as a Docker image" on page 148.

- **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 Primary Server. In addition, for NetBackup 7.7.3 only, this is used by the License Details probe to collect plugin information (bpstsinfo).

  For NetBackup 8.3 and above, this domain is used by Backup Policies probe (FETB and Protection Plan collection) for REST API based authentication.

  This field is required when the Collection Method is SSH or WMI protocol to the NetBackup Primary Server and that Primary Server is a Windows Server.

Active Probes

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.
- **Job Details**: Select the check box to activate Job data collection from your NetBackup environment. The polling frequency would depend on the value of **ENABLE_MINUS_T_OPTION** advanced parameter.

  Refer to **Backup Manager advanced parameters** section for more details on **ENABLE_MINUS_T_OPTION** parameter.

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.

- **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.
- **Backup Message Logs**:

  This probe is active by default and cannot be deactivated. It performs the Message Log (bperror) data collection from your NetBackup environment. Its default polling frequency is every 5 minutes.

  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.
- **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.

  Note: 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.
- **Host Details**: Select the check box to activate Host Details data collection from your NetBackup environment. This probe calls NetBackup REST APIs to collect and persist environmental details. The default polling frequency is once a week.

  This probe is selected by default.

  Also, ensure this probe is selected to enable access to NetBackup web interface from the IT Analytics Portal. The steps to enable access to the web interface are documented under *Access NetBackup web interface from the IT Analytics Portal* section of the *User Guide*.

  Click clock icon to modify the scheduled 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.

- **Event Notifications**: Select the check box to activate Event Notifications data collection from your NetBackup environment. This probe calls NetBackup REST APIs to collect and persist critical event notifications.

  This probe supports NetBackup version 9.1 and above. For version lower than 9.1, the data collection fails and an error status is displayed on the collection status page.

  The default polling frequency is every minute. 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.

- **Audit Events**: The Audit Events probe collects the audit events such as user login success or failure, policy modification etc. from Netbackup Primary server.

  Select the check box to activate Audit Events data collection from your NetBackup environment. This probes connects directly to NetBackup Primary server to collect and persist the audit details.

  The default schedule is every 1 hour.

  You can configure the Advanced parameter NBU_AUDIT_LOOKBACK_DAYS for the first time collection of the NetBackpup Audit events. By default, it collects events from last 3 days for the first time.

  Change the value of this advanced parameter to collect events that are anything other than 3 days.

  Note: When selecting this Audit Events 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.

- **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.

- **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.

- **NetBackup Event Monitor**: Collects events generated by the nb_monitor_util executable present in the NBU installation. Events include create/update/ delete for Backup Policies, Storage Unit Details, Storage Unit Groups and Storage Lifecycle Policies. This probe is selected by default for new installations.

  NetBackup Event Monitor is disabled if WMI/SSH collection is enabled.
- **Storage Unit Details**: Select the checkbox 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.
- **Storage Lifecycle Policies**: When selecting this option, you must also configure settings in the **Login Details for Remote Probes** section 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.
- **Backup Policies**: Performs Backup Policy data collection from your NetBackup environment. This probe also collects the FETB and protection plan data using REST APIs, provided the NetBackup version is 8.3 or later. You need to provide the REST API credentials under **Remote Probe Login Details** to allow the APIs to collect data. This probe is enabled by default and is not editable. The FETB data collected is also validated against the license entitlement of the subscription.

  The default polling frequency is every 8 hours. 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.

  NetBackup IT Analytics supports VMware, Hyper-V, Oracle, MSSQL intelligent policies in NetBackup. As a part of Oracle and MSSQL intelligent policies, the instance details backed up by policy is displayed in NetBackup Policies Details report.

  Security Details: Select the checkbox to activate Security Details data collection from your NetBackup environment. The default polling frequency is every hour at minute 15. This probe is not selected by default. It collects data using NetBackup commands and REST APIs, provided the NetBackup version is 10.0 or later. You need to provide the REST API credentials under Remote Probe Login Details to allow the APIs to collect data. If API key is provided during configuration of NetBackup Primary servers, it is used to execute the REST API.

See *Add/Edit Netbackup Primary Servers within the Data Collector policy* for details about the API key.

Click 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 string is also available.

- **NetBackup Resources Monitor**: Select the checkbox to activate NetBackup Resources data collection from your NetBackup environment. The probe does not have a default schedule. Once enabled, it collects data received from the NetBackup IT Analytics Exporter installed on the NetBackup Primary Server. When you enable this probe, the NetBackup Primary Server (Internal Name) is added to Compute Resources Data Collection Policy. If there is no existing policy, a new policy for Compute Resources is added.

  Note that the Internal Name of the NetBackup Primary server must match the instance (Hostname) of the NetBackup Primary Server.

  See the *NetBackup IT Analytics Exporter Installation and Configuration Guide* for details on exporter installation.

- **NetBackup Actions**:

  Note: The following Three actions for NetBackup probe are ALTA-specific

  - **Veritas.NetBackup.VTNB.AltaConnectorTaskProbeAPIKeyRenewal**
    In Alta Connector deployment there is a API Key shared between Alta View and NBU. This key needs to be renewed periodically. This action is implemented to trigger key renewal logic.

  - **Veritas.NetBackup.VTNB.AltaConnectorTaskProbeNotificationMessageKey**
    In Alta Connector deployment notification keys need to be add to NBU so that NBU can correctly interpret I18N text send to it by Alta Connector. This action is implemented to add notification keys on NBU Primary Server.

  - **Veritas.NetBackup.VTNB.AltaConnectorTaskProbeUpgrade**
    In Alta Connector deployment , NBU specific scripts need to be invoked when NBU upgrades to 10.1.1 or above. This Action triggers execution of the script once it detects NBU is upgraded to 10.1.1 or above.

- **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.

- **Download SSL Certificate**: Downloads the SSL certificate required to set up NetBackup IT Analytics Exporter on the NetBackup Primary Server.

See the *NetBackup IT Analytics Data Exporter Installation and Configuration Guide* for details on exporter installation.

- **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.

  Test Connection checks if the utility nb_monitor_util is installed. This is required to use the probe NetBackup Event Monitor.

  It also checks if the REST APIs were successfully executed against the NetBackup Primary Server. For REST APIs to succeed, you must provide the user credentials of the NetBackup Primary that has REST API access. The FETB and Protection Plan collection fails in absence of the user credentials.

  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.

After adding the policy, 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 for some policies. 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.

See “Veritas NetBackup SSH: Changing the Linux Temporary Directory for Collection” on page 144.

Add/Edit NetBackup Primary 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**.

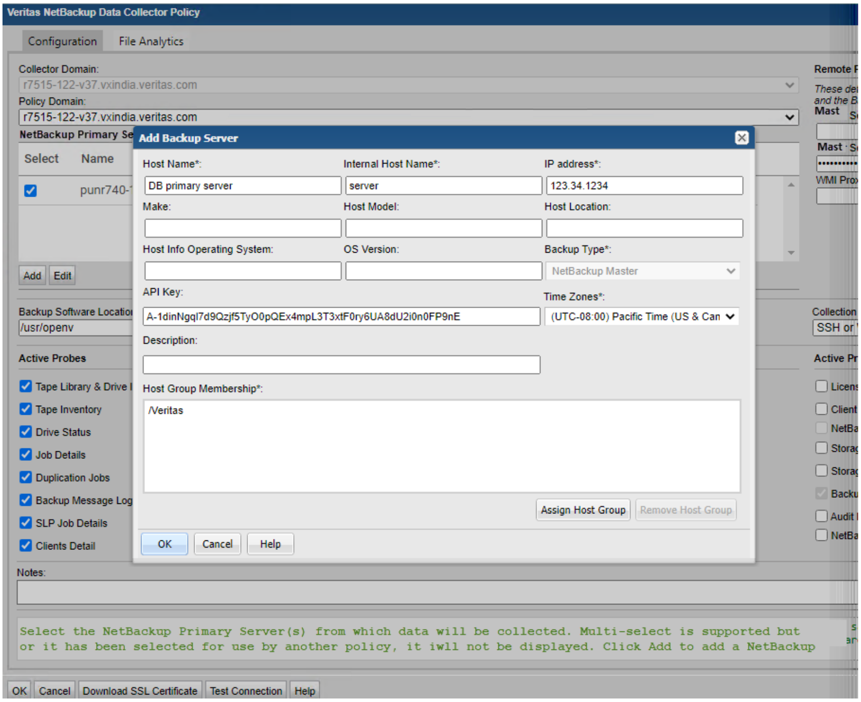
The **NetBackup Primary Servers** table, shown in the policy, is populated using either of these methods. Servers added from the policy are also displayed under

Inventory. The **NetBackup Primary Servers** table only displa ys 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**.
2. Select a Primary Server and click **Edit**.
3. The **Add Backup Server** window is displayed.



Veritas NetBackup Data Collector Policy

Collector Domain: r7515-122-v37.vxindia.veritas.com

Policy Domain: r7515-122-v37.vxindia.veritas.com

Backup Software Locatio /usr/openv

Active Probes:

☑ Tape Library & Drive I
☑ Tape Inventory
☑ Drive Status
☑ Job Details
☑ Duplication Jobs
☑ Backup Message Log
☑ SLP Job Details
☑ Clients Detail

Add Backup Server

Host Name*: DB primary server

Internal Host Name*: server

IP address*: 123.34.1234

Make:

Host Model:

Host Location:

Host Info Operating System:

OS Version:

Backup Type*: NetBackup Master

API Key: A-1dinNgql7d9Qzjf5TyO0pQEx4mpL3T3xtF0ry6UA8dU2i0n0FP9nE

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

Description:

Host Group Membership*: /Veritas

Notes:

```
Select the NetBackup Primary Server(s) from which data will be collected. Multi-select is supported but
or it has been selected for use by another policy, it iwll not be displayed. Click Add to add a NetBackup
```

4. 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 Primary Server. If a Primary Server belongs to a cluster, enter the `NetBackup Cluster Name` for the Internal Name.

     See “Collecting from NetBackup clusters” on page 152.

     This is a required field.

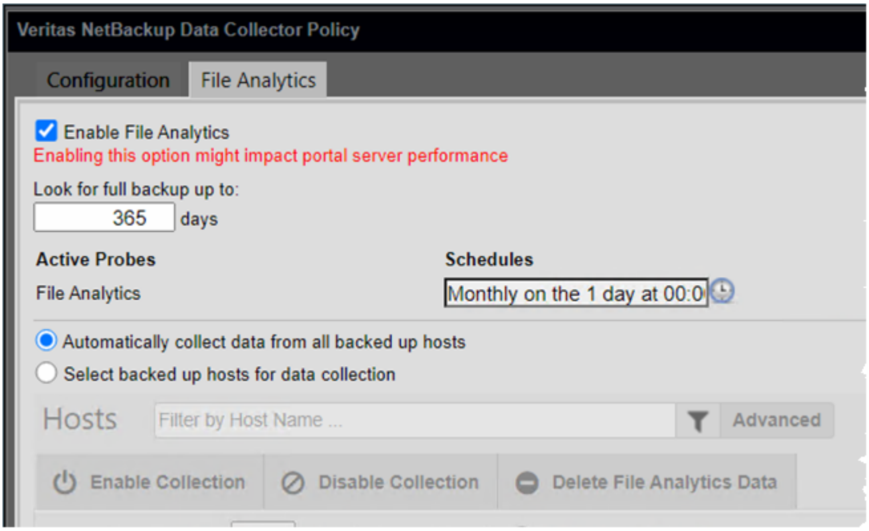
- **IP Address**: IP address of the host/backup server. This is a required field.
- **Make**, **Host Model**, **Host Location**, **Host Info Operating System**, and **OS Version**, are optional.
- **Backup Type**: Select Veritas NetBackup Primary. The **Time Zones** field is displayed when the server is designated as a Primary Server. The Time Zone setting is only available only for a host that is configured as a NetBackup Primary.
- **API Key**: Enter the API key obtained from the Veritas NetBackup Web UI to successfully execute the REST APIs. This API key must be specified in cases where password-based authentication is not allowed on the Veritas NetBackup Primary Servers. For policies with Collection Method as NetBackup Software on a Data Collector Server, self-configured JWT tokens using certificates on the NetBackup Primary are used to execute the REST APIs. In this case, API Key is optional and will be used only when Data Collector is unable to get JWT token. Refer *NetBackup Security and Encryption Guide* for setting up certificates in NetBackup. See the *Manage API keys* section from the *NetBackup Web UI Security Administrator's Guide* for steps to get the API key.

  See “Prerequisites for collection from Veritas NetBackup deployed as a Docker image” on page 148.
- **Time Zones**: Select a Time Zone to associate with the NetBackup Primary. 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 Primary, NetBackup IT Analytics defaults to the time zone of the Data Collector server. Note that in NetBackup IT Analytics reports, the date and time displayed for a backup transaction represents the date and time when the event actually happened.
- **Host Group Membership**: 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.

Configuring file analytics in NetBackup Data Collector policy

File Analytics leverages the data collection capabilities of the NetBackup Data Collector Policy, and in turn, provides insights into the organizational files. The data backups enable file-level visibility and the data thus collected is used to populate various reports and dashboards for further analyses. File Analytics can prove crucial in detecting ransomware attacks or detecting restricted content and policy breach.

However, enabling File Analytics can impact your portal server performance, as it imposes additional load of retrieving the file metadata. Ensure you adhere to the sizing guidelines and the prerequisites for File Analytics to function seamlessly.



Veritas NetBackup Data Collector Policy

☑ Enable File Analytics
Enabling this option might impact portal server performance

Look for full backup up to: 365 days

Active Probes	Schedules
File Analytics	Monthly on the 1 day at 00:0

● Automatically collect data from all backed up hosts
○ Select backed up hosts for data collection

Prerequisites to configure File Analytics for NetBackup

You can configure File Analytics within the NetBackup policy provided you adhere to these prerequisites:

- File Analytics supports NetBackup v7.6 and later, NetBackup Appliance v2.6 and later.
- Complete License Suite subscription: You must subscribe to the Complete License Suite of to enable File Analytics for your account.
- Enabled Backup Policies probe: Ensure the **Backup Policies** probe is active or enabled within the NetBackup Policy.

Supported NetBackup policy types

Even though NetBackup has several policy types and reports to display their collected data. However, File Analytics captures data from these file policies for reporting and analytics:

- MS-Windows
- Standard

- NDMP
- Hyper V
- VMware

Data Collector and Portal sizing guidelines for File Analytics

The following guidelines help you to calculate the resource allocation in your environment based on the data collection load. The suggested values below are recommended for a collection of 1.5 TB NetBackup catalog size. You can use this reference calculate the RAM, CPU, and disk space requirements in your respective environment.

The sizing guidelines for Data Collector and Portal are as follows:

Table 13-1 Data Collector sizing for File Analytics

Data Collector	
Minimum RAM	32 GB
CPU	Minimum 4 CPU core
Minimum usable hard disk space	200 GiB

Table 13-2 Portal sizing for File Analytics

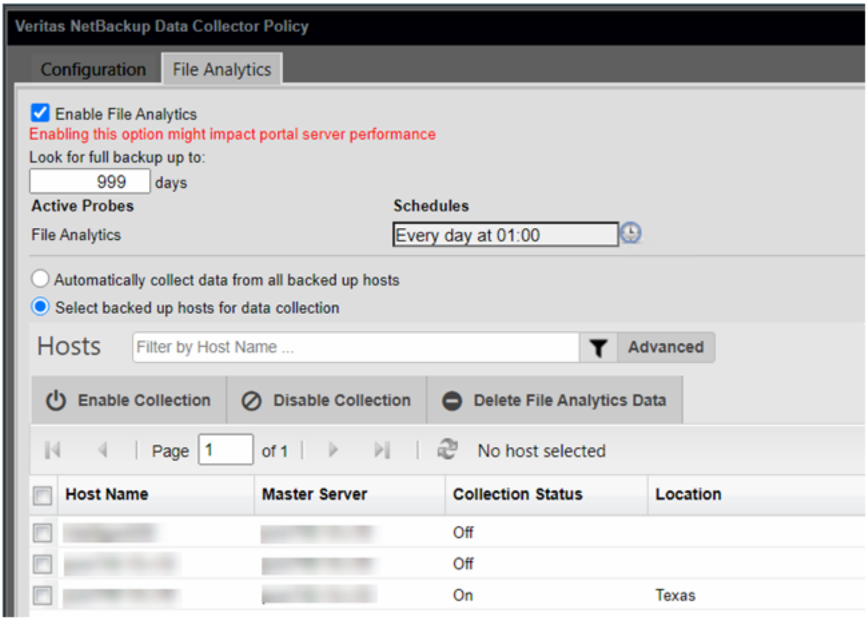
Portal	
Minimum RAM	32 GB
CPU	Minimum 4 CPU core, but 8 CPU core is recommended
Minimum usable hard disk space	200 GiB **Note:** It is observed that for every 100 million files, approximately 5 GB disk space is consumed on the portal.

The above guidelines and recommended values are inline with the *Recommend Portal Configurations* in *File Analytics Certified Configurations Guide*. However, you may have to manage your resource allocation based on the data collection side in your environment.

Configure File Analytics

Since the File Analytics is a component of the NetBackup Policy, it can provide analytics on the data captured from the hosts probed by the NetBackup policy. As a result, the hosts that you can configure to collect data for File Analytics become available only after the first probe cycle of the **Backup Policies** probe is complete. Until then, the tab displays **No Host Available**.

Remember to adhere to the prerequisites before you proceed with the configuration.



Veritas NetBackup Data Collector Policy

☑ Enable File Analytics

Enabling this option might impact portal server performance

Look for full backup up to: 999 days

Active Probes	Schedules
File Analytics	Every day at 01:00

○ Automatically collect data from all backed up hosts

● Select backed up hosts for data collection

Hosts: Filter by Host Name ...

No host selected

□	Host Name	Master Server	Collection Status	Location
□	[redacted]	[redacted]	Off	
□	[redacted]	[redacted]	Off	
□	[redacted]	[redacted]	On	Texas

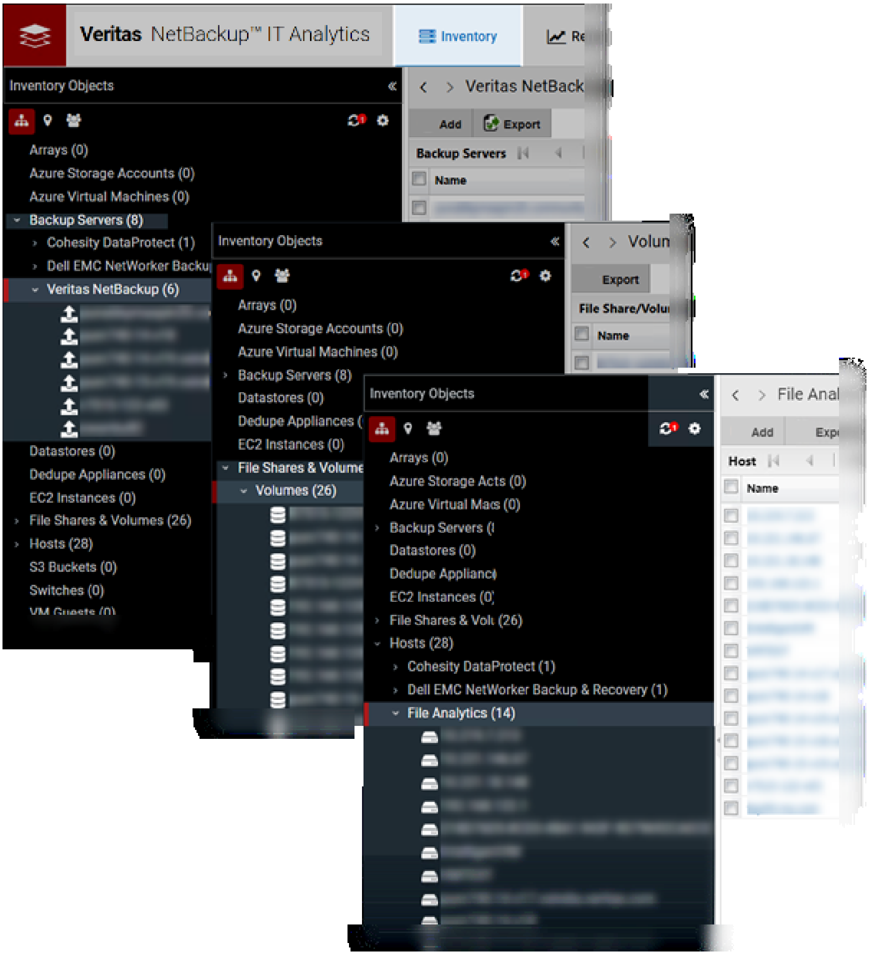
You can configure the following for File Analytics:

- **Enable File Analytics**: Enables the File Analytics configuration.
- **Look for full backup up to**: Determines the time span in number of days to look back for the last successful full backup.
- **Schedules**: Allows you to configure a cron job or a time interval at which data collection can be triggered.
- **Automatically collect data from all backed up hosts**: Enables collecting data from all the hosts probed by the NetBackup Policy but with respect to the policies relevant to File Analytics.
- **Select backed up hosts for data collection**: Enables data collection from selective hosts probed by the NetBackup Policy.

- **Enable Collection**: Marks the host for data collection. You must select a host from the **Host Name** column before clicking this option. Once marked for data collection, the **Collection Status** for the host is indicated as **On**.
- **Disable Collection**: Removes the host from data collection. You must select a host from the **Host Name** column before clicking this option. After removal, the Collection status for host is indicated as **Off**.
- **Delete File Analytics Data**: Deletes the data collected from the selected hosts and stored on the portal server. The data once deleted is not recoverable.

Once File Analytics is configured within the NetBackup policy, the respective data collection hosts are displayed in the Inventory as follows:

- Primary Servers: Under **Inventory** > **Backup Servers** > **Veritas NetBackup**
- Shares and volumes: Under **Inventory** > **File Shares & Volumes** > **Volumes**
- Hosts: Under **Inventory** > **Hosts** > **File Analytics**



Export File Analytics data

The data collected for File Analytics is stored on the portal server in the `/opt/aptare/fa/db` or `C:\opt\aptare\fa\db` folder, depending on the operating system. Separate folders titled by timestamp are created and the exported data contains the following details:

- DomainId
- HostName
- Filepath
- Size

- Owner
- CreateTime
- ModifiedTime
- AccessTime
- BackupPolicies
- BackupTime

Note: BackupPolicies and BackupTime headers are seen on when you export the File Analytics data collected by the NetBackup policy.

See the *Data Export* section of the *NetBackup IT Analytics Data Collector Installation Guide for File Analytics* guide for the export procedure.

Pre-Installation setup for Oracle Recovery Manager (RMAN)

This chapter includes the following topics:

Introduction

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

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

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

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Database Host and Port: Identify the hostname of the server where the database in which the RMAN data resides as well as the port this database is listening on. The default port is 1521.
- The configured user must exist in all configured instances with the same password. The user should the CREATE SESSION privilege and have the following permissions in the schemas to be collected from:
  - User must have the SELECT_CATALOG_ROLE to retrieve RMAN data from the Dynamic Performance (V$) views:

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

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

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

    or

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

    or have a virtual private catalog set up for the user (see Oracle documentation).
  - User must have SELECT permission to V$INSTANCE and V$DATABASE (which is included in SELECT_CATALOG_ROLE).

Installation overview (Oracle Recovery Manager - RMAN)

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

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

Add an Oracle Recovery Manager (RMAN) Data Collector policy

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

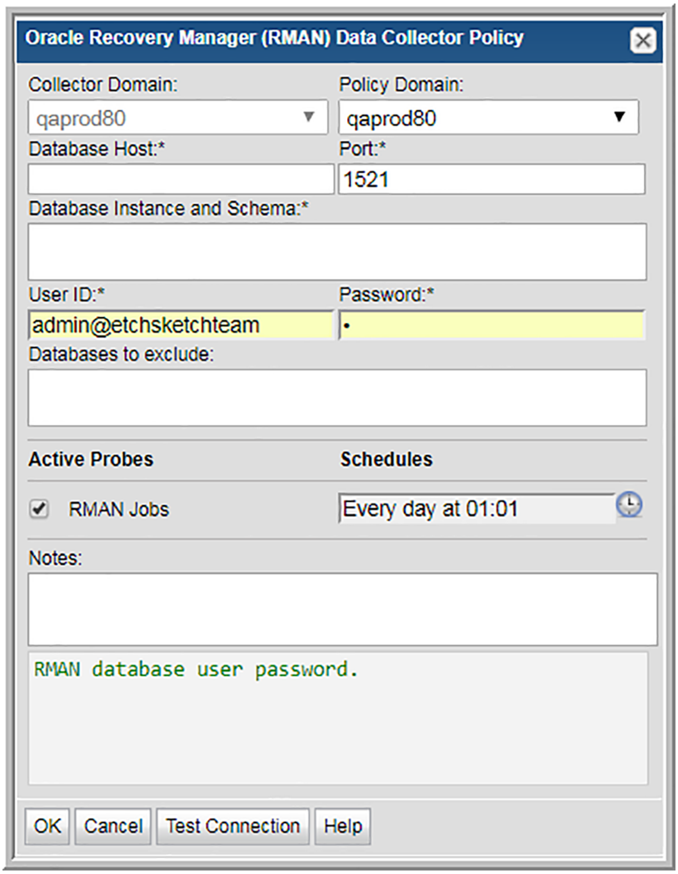
  For specific prerequisites and supported configurations for a specific vendor, see the*Certified Configurations Guide*.
- After adding the policy: For some policies, collections can be run on-demand using the **Run** button on the **Collector Administration** page action bar. The **Run** button is only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

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

To add the policy

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

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


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 (*).

See See Table 14-1 on page 176.

Table 14-1 Policy Parameters

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

Table 14-1 Policy Parameters *(continued)*

Field	Description
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select My Profile from the menu. Your Domain name is displayed in your profile settings.
Database Host	RMAN database server.
Port	Database listener port. By default the port is 1521.
Database Instance and Schema	RMAN database instance names and optional schemas, each formatted as INSTANCE.SCHEMA and separated by commas or spaces. If a schema is not specified then all Recovery Catalog schemas in the instance accessible to the user ID will be collected. If there are no accessible Recovery Catalog schemas then the Dynamic Performance (V$) views will be collected. Use the PUBLIC schema to force collection from the V$ views, or a Recovery Catalog schema name to only collect from that schema. Example (to collect both from a Recovery Catalog schema and the V$ views in the DB1 instance): DB1.RMAN, DB1.PUBLIC
User ID*	This field is required. RMAN database user name. This must be a user with SELECT permission for the Dynamic Performance (V$) views and any Recovery Catalog schema views being collected from.
Password*	This field is required. RMAN database user password.
Databases to exclude	RMAN numeric database IDs to exclude from collection, separated by commas or spaces.
Active Probes	
RMAN Jobs	Probe for Oracle Recovery Manager (RMAN) jobs.

Table 14-1 Policy Parameters *(continued)*

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

Chapter 15

Pre-Installation setup for Rubrik Cloud Data Management

This chapter includes the following topics:

Introduction

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

Prerequisites for adding Data Collectors (Rubrik Cloud Data Management)

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

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Read-only Rubrik user account

Installation overview (Rubrik Cloud Data Management)

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

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

Add a Rubrik Cloud Data Management Data Collector policy

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

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

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

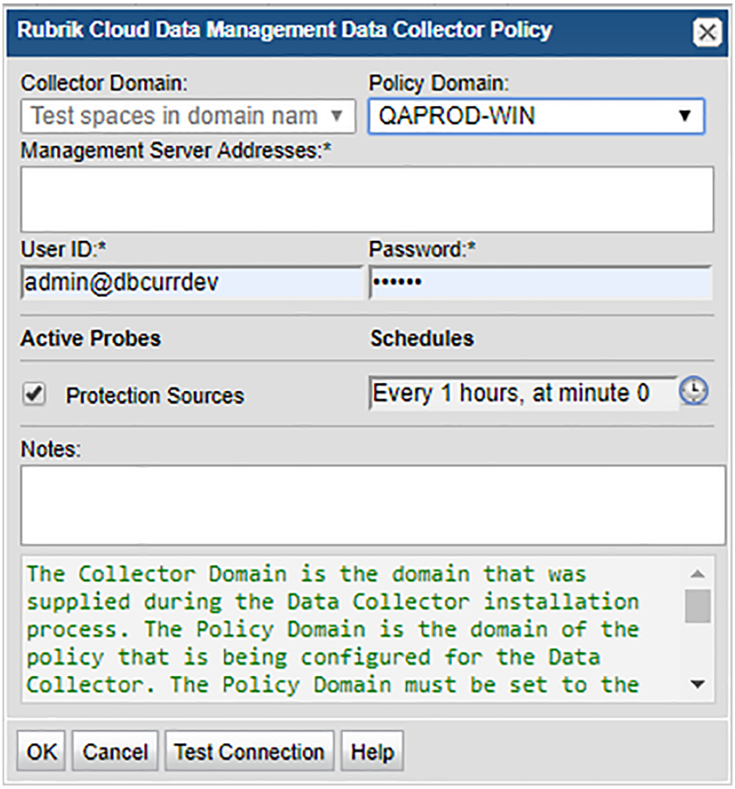
To add the policy

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

2 Search for a Collector if required.

3 Select a Data Collector from the list.

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



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 (*).

See

Table 15-1 Policy Parameters

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Management Server Addresses	One or more Cloud Data Management's server IP addresses or host names to probe. Comma-separated addresses are supported, e.g. 192.168.1.10, myhost NOTE: To collect from a Cluster, enter the IP address of only one of the management servers.
User ID*	Read-only userID for the Rubrik Cloud Data Management system.
Password*	Password for the Rubrik Cloud Data Management system. The password associated with the User ID.
Protection Sources	Probe for Rubrik Cloud Data Management Protection Details.
Schedule	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.

Table 15-1 Policy Parameters *(continued)*

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

Chapter 16

Pre-Installation setup for Veeam Backup & Replication

This chapter includes the following topics:

Introduction

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

Prerequisites for adding data collectors (Veeam Backup & Replication)

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

- 64-bit OS. See the Certified Configurations Guide for supported operating systems.
- When the NetBackup IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the NetBackup IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- Requires a Microsoft Windows Data Collector server
- Requires Microsoft PowerShell 4.0 or above. Veeam Backup & Replication comes with a PowerShell extension - a snap-in to Microsoft Windows PowerShell. The Veeam Backup PowerShell snap-in enables most operations that are available in the user interface. For version 11.0, Veeam Backup & Replication comes with a PowerShell module which can be used on any machine with the backup console installed.
- Veeam Requirement: User credentials with a Veeam Backup Administrator role are required to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in or PowerShell module (version 11.0).
- Veeam Backup & Replication Console must be installed on the system where the Data Collector service is running.
- Default port is 9392.

Verifying Data Collector servers can connect to Veeam servers

Basic PowerShell commands for Veeam

- Add Veeam Snapin

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

  Note: Skip this command for Veeam version 11.0, as it supports the PowerShell module.

- Connect to Veeam Backup Server

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

- Disconnect from Previous Connection

  ```
  Disconnect-VBRServer
  ```

Verification steps

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

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

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

   Note: Skip this step for Veeam version 11.0, as it supports the PowerShell module.

2. Log into the Veeam Backup & Replication Console using Server-A credentials.
3. Open a PowerShell Console and connect to Server-A.

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

   The Server -A connection should be successful.

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

```
Disconnect-VBRServer
```

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

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

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

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

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

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

Known issues and limitations (Veeam Backup & Replication)

- Backup File Names
  Veeam allows a backup job to have different backup and retention policies. For certain configuration types such as, Synthetic Full Backup or Forever Forward Incremental Backup Retention Policy, one of the *.vib files is renamed as *.vbk at regular intervals by Veeam. In NetBackup IT Analytics, the Veeam Data Collector retrieves backup information for a specified period of time at regular intervals. This set of backup information may contain file names with a *.vib extension (instead of *.vbk) and display in the Job Details report.
  For details about the various use cases,
  https://helpcenter.veeam.com/docs/backup/vsphere/backup_files.html?ver=95.
  As you compare NetBackup IT Analytics reports to native Veeam reports, if there are discrepancies in the files, you can force a historic data collection to examine the details. Additionally, when validating NetBackup IT Analytics reports against Veeam reports, focus on the file names and not the file extensions.
- Successful Endpoint Backup Jobs Displaying Size = 0.00 Bytes
  Occasionally, Veeam will create additional maintenance jobs such as Full backup file merge completed successfully and there is not a data size associated with the job. These jobs will be displayed with a status of Successful but without an associated data size.

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

Installation overview (Veeam Backup & Replication)

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

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

   See “Installing the WMI Proxy service (Windows host resources only)” on page 204.
6. Validate the Data Collector installation.

Add a Veeam Backup & Replication Data Collector policy

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

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

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

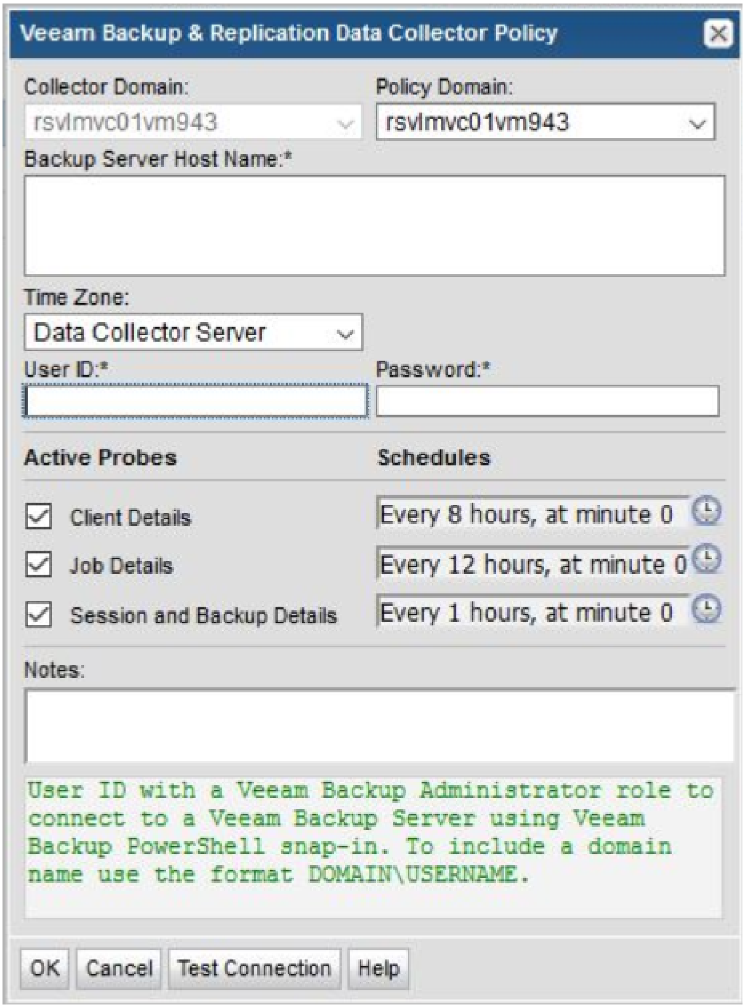
To add the policy

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

2 Search for a Collector if required.

3 Select a Data Collector from the list.

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



Veeam Backup & Replication Data Collector Policy

Collector Domain: rsvlmvc01vm943

Policy Domain: rsvlmvc01vm943

Backup Server Host Name:*

Time Zone: Data Collector Server

User ID:*

Password:*

Active Probes	Schedules
☑ Client Details	Every 8 hours, at minute 0
☑ Job Details	Every 12 hours, at minute 0
☑ Session and Backup Details	Every 1 hours, at minute 0

Notes:

User ID with a Veeam Backup Administrator role to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in. To include a domain name use the format DOMAIN\USERNAME.

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

Table 16-1

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Backup Server Host Name*	One or more Veeam Backup Server Host Names to probe. IP Address is not supported. Comma-separated host names are supported. Example, VeeamServer1, VeeamServer2.
Time Zone	Select the time zone of Veeam Backup Server. By default, the data collector server time zone is used.
User ID*	User ID with a Veeam Backup Administrator role to connect to a Veeam Backup Server using Veeam Backup PowerShell snap-in or PowerShell module (version 11.0). To include a domain name, use the format **DOMAIN\USERNAME**.
Password*	Password for Veeam Backup Server associated with the User ID.
Active Probes	
Client Details	Probe for collecting clients to be backed up using Veeam Backup & Replication.
Job Details	Probe for collecting jobs scheduled for Veeam Backup & Replication.
Session and Backup Details	Probe for collecting session details and backups created by Veeam Backup & Replication.

Table 16-1 *(continued)*

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

Chapter 17

Discovery policies for Veritas NetBackup

This chapter includes the following topics:

Task overview: Configure and monitor discovery policies

To configure Discovery, perform the following sequence of steps:

Table 17-1 Configure and monitor discovery policies

	Task	For Instructions
1.	Learn about how Discovery policies can help you protect your data.	See " Discovery policies overview " on page 194.
2.	Purchase and activate your Discovery license. Two of the three Discovery processes require a license: ■ See "Client drive discovery" on page 195. ■ See "Backup policy coverage" on page 195.	See "Activate a Discovery license" on page 195.
3.	Enable SNMP, if you are enabling these Discovery types: ■ See "Client drive discovery" on page 195. ■ See "Backup policy coverage" on page 195.	
4.	Determine the primary server that requires the policy that you are about to create, and identify the Discovery type(s) that you want to enable le on this primary server.	See "About Discovery types" on page 195.
5.	If necessary, exclude specific network devices from your policies.	See "Exclude devices from Discovery policies" on page 196.
6.	Turn on Discovery probes in the NetBackup Data Collector policy.	See "Activate Discovery probes in the NetBackup Data Collector policy" on page 196.
7.	Regularly monitor the status of Discovery processes.	See " Monitor Discovery processes" on page 197.
8.	View the Client Protection Summary report to see how well your data is being protected.	See "View client protection status" on page 197.

Table 17-1 Configure and monitor discovery policies *(continued)*

	Task	For Instructions
9.	If significant changes in your environment warrant a fresh view, rebuild the Discovery database.	See " Reset Discovery data " on page 198.
10.	Tune Discovery by modifying time out settings for probes.	See the *System Administrator 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" on page 195.

See "Activate a Discovery license" on page 195.

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.

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 primary 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 primary 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
   ```

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.

- See “Client drive discovery” on page 195.
- See “Media server disk discovery” on page 195.
- See “Backup policy coverage” on page 195.

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.

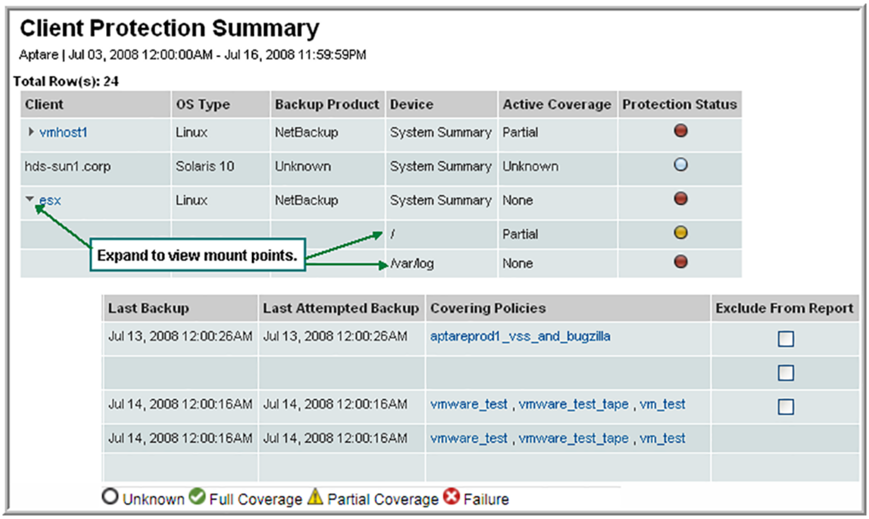
2. For each active policy, double-click on the management server that is responsible for running a particular policy.

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

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?

The information contained in this section is intended for the administration of Discovery functionality. This SNMP configuration guidance for informational purposes only. Veritas Support will not provide assistance with the installation, configuration, and troubleshooting of SNMP subsystems on your Primary 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.

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.

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`.

Troubleshoot 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");
```

Installing the Data Collector software

This chapter includes the following topics:

Introduction

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

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

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

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

Installing the WMI Proxy service (Windows host resources only)

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

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

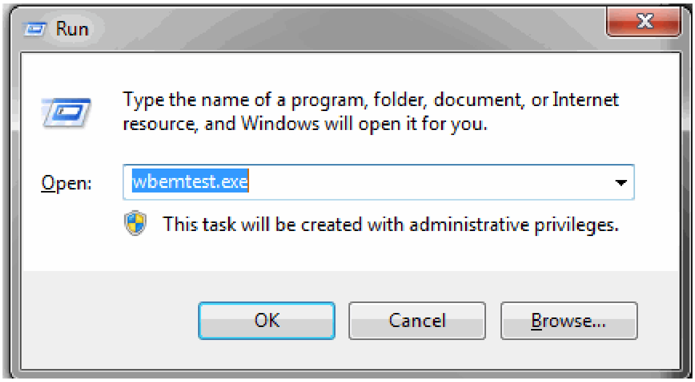
See "Install Data Collector Software on Windows" on page 209.

Testing WMI connectivity

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

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

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

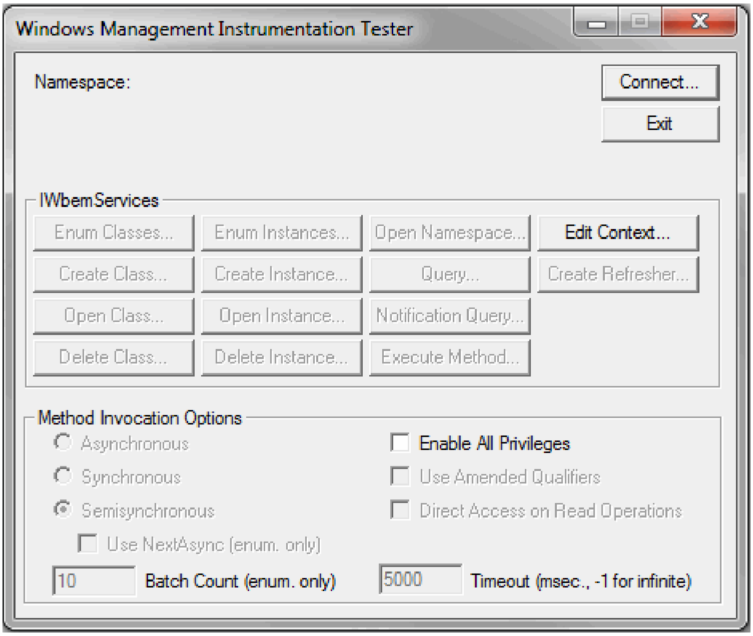


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wbemtest.exe

This task will be created with administrative privileges.

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



Namespace:

○ Asynchronous

○ Synchronous

● Semisynchronous

□ Use NextAsync (enum. only)

□ Enable All Privileges

□ Use Amended Qualifiers

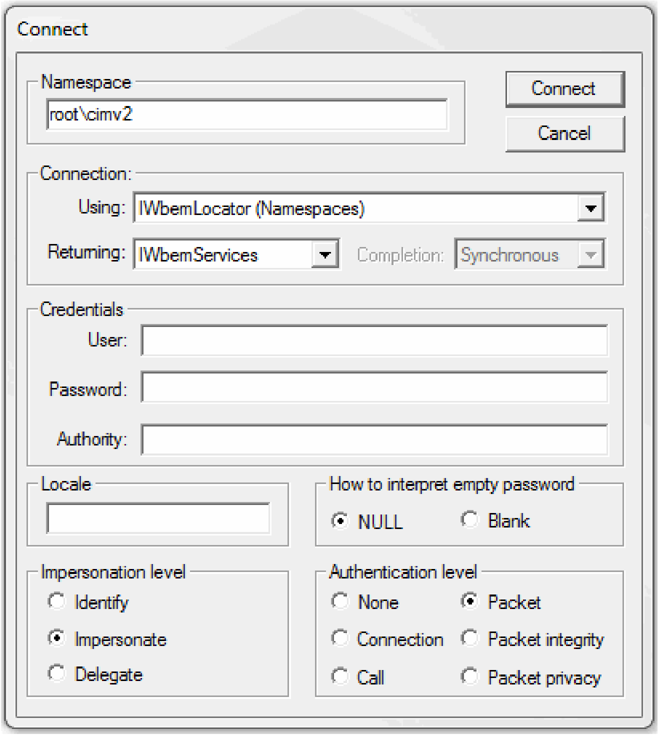
□ Direct Access on Read Operations

10 Batch Count (enum. only)

5000 Timeout (msec., -1 for infinite)

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

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



Namespace: root\cimv2

Connection:

Using: IWbemLocator (Namespaces)

Returning: IWbemServices   Completion: Synchronous

Credentials

User:

Password:

Authority:

Locale

How to interpret empty password: ● NULL ○ Blank

Impersonation level: ○ Identify ● Impersonate ○ Delegate

Authentication level: ○ None ● Packet ○ Connection ○ Packet integrity ○ Call ○ Packet privacy

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

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

Considerations to install Data Collector on non-English systems

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

- Simplified Chinese
- French
- Korean
- Japanese

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

The OS-specific requirements mentioned below.

Non-English Linux OS

On a non-English Linux host:

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

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

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

1. Check the current language.

   ```
   #locale
   ```

2. Check whether your system has multiple languages:

   ```
   #locale -a
   ```

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

   - To add Simplified Chinese:

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

   - To add French:

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

   - To add Korean

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

   - To add Japanese

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

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

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

See “Install Data Collector software on Linux” on page 220.

Non-English Windows OS

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

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

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

See "Install Data Collector Software on Windows" on page 209.

Install Data Collector Software on Windows

To install your Data Collector software:

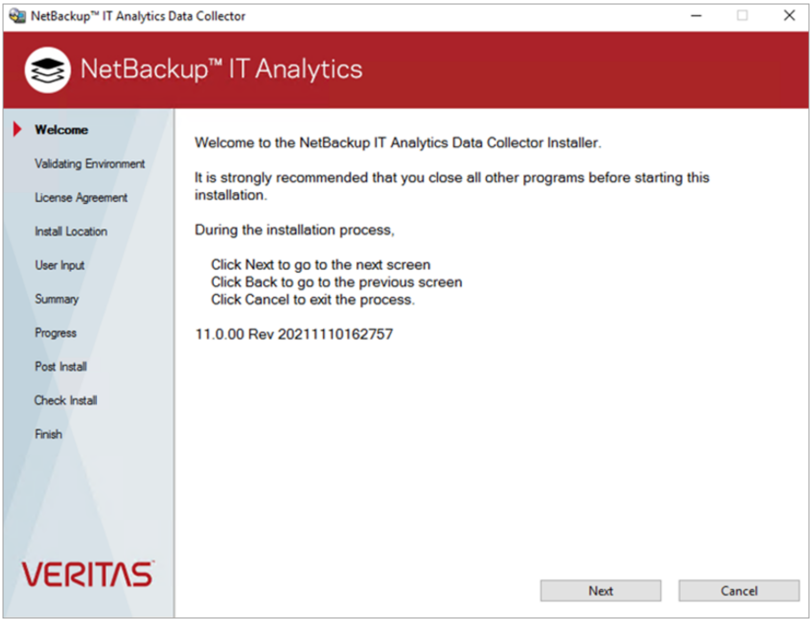
1 Login to the Data Collector server as a local administrator.

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

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

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

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



Welcome to the NetBackup IT Analytics Data Collector Installer.

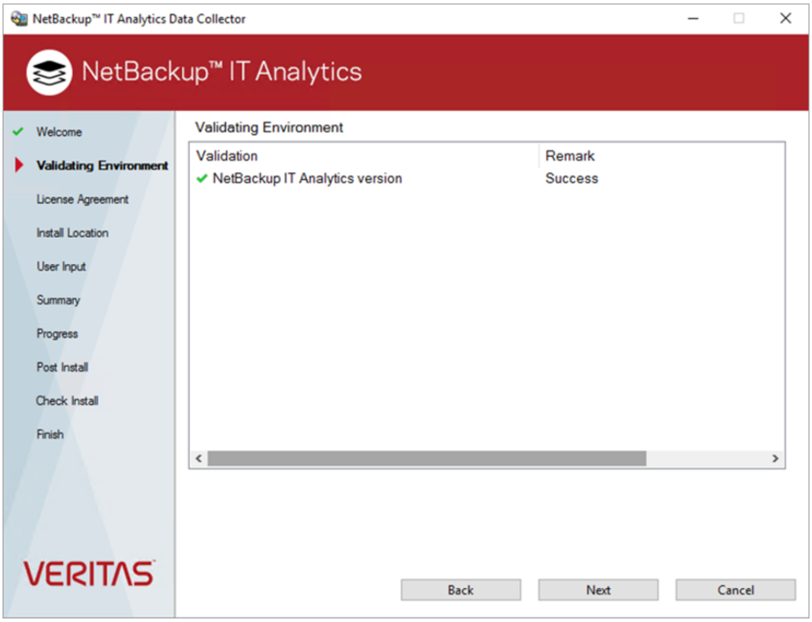
It is strongly recommended that you close all other programs before starting this installation.

During the installation process,

Click Next to go to the next screen
Click Back to go to the previous screen
Click Cancel to exit the process.

11.0.00 Rev 20211110162757

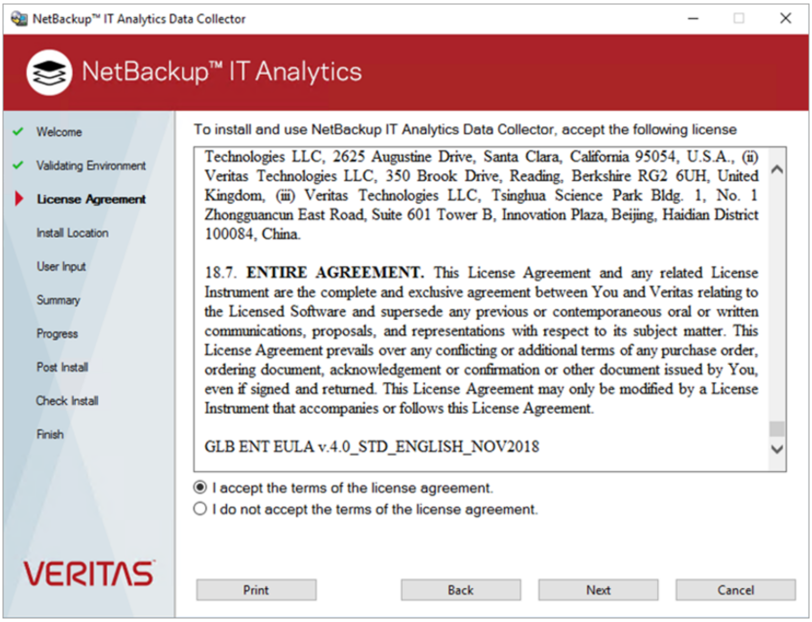
4 The installation wizard validates the system environment. On successful validation, click **Next**.



Validating Environment

Validation	Remark
✓ NetBackup IT Analytics version	Success

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



To install and use NetBackup IT Analytics Data Collector, accept the following license

Technologies LLC, 2625 Augustine Drive, Santa Clara, California 95054, U.S.A., (ii) Veritas Technologies LLC, 350 Brook Drive, Reading, Berkshire RG2 6UH, United Kingdom, (iii) Veritas Technologies LLC, Tsinghua Science Park Bldg. 1, No. 1 Zhongguancun East Road, Suite 601 Tower B, Innovation Plaza, Beijing, Haidian District 100084, China.

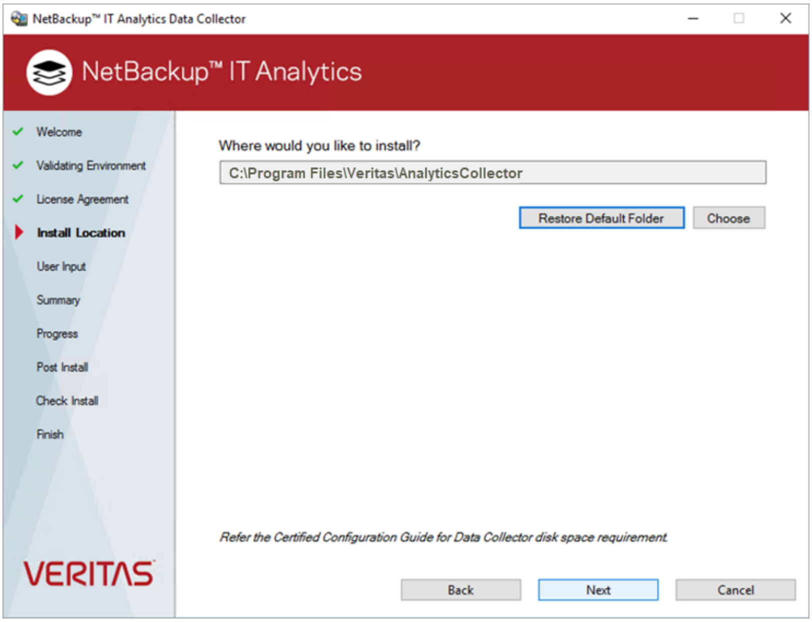
18.7. **ENTIRE AGREEMENT.** This License Agreement and any related License Instrument are the complete and exclusive agreement between You and Veritas relating to the Licensed Software and supersede any previous or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter. This License Agreement prevails over any conflicting or additional terms of any purchase order, ordering document, acknowledgement or confirmation or other document issued by You, even if signed and returned. This License Agreement may only be modified by a License Instrument that accompanies or follows this License Agreement.

GLB ENT EULA v.4.0_STD_ENGLISH_NOV2018

● I accept the terms of the license agreement.
○ I do not accept the terms of the license agreement.

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

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



Where would you like to install?

C:\Program Files\Veritas\AnalyticsCollector

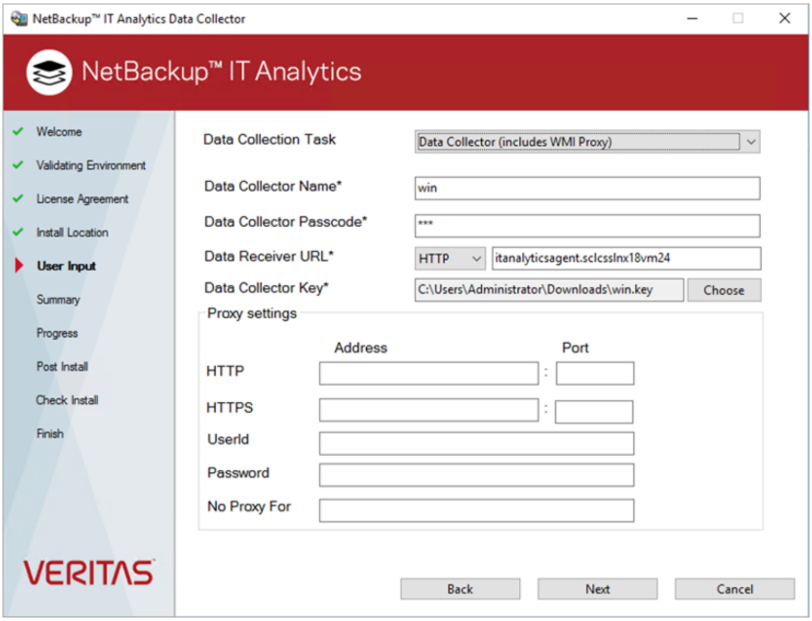
Refer the Certified Configuration Guide for Data Collector disk space requirement.

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

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

Data Collector Name	Specify the Data Collector name that you used during its configuration on the NetBackup IT Analytics Portal. Data Collector uses this for authentication. If you are installing on a non-English OS, the Data Collector name must be in English.
Data Collector Passcode	Specify the Data Collector passcode that you used for the Data Collector name during its configuration on the NetBackup IT Analytics Portal. This passcode is encrypted prior to saving it to the portal database and is never visible in any part of the application. If the password contains a special character, make sure it is one of the following OS-specific supported character: ■ Linux: !@#%^* ■ Windows: !@#$%^&*() If the special character in the passcode is not supported on the OS, you must update the Data Collector passcode on the portal.
Data Receiver URL	Enter the URL that the Data Collector will use to communicate with the portal server. The format must be *http://itanalyticsagent.yourdomain.com*. Make sure you enter the URL with the prefix **itanalyticsagent** and not itanalyticsportal.
Data Collector Key	Enter the key that was downloaded from the portal during the Data Collector configuration. Obtain it from the download location of the collector key file for encryption. If the existing key file is not available, regenesrate it and download a new key file from the portal and use its file path.

Proxy Settings	1 **HTTP/HTTPS**: Enter the hostname or IP address and a port number. 2 **UserId**: User ID of the proxy server. 3 **Password**: Password of the proxy server. 4 **No Proxy For**: Enter the host names or IP addresses separated by commas that will not be routed through the proxy.



Data Collection Task: Data Collector (includes WMI Proxy)

Data Collector Name*: win

Data Collector Passcode*: ***

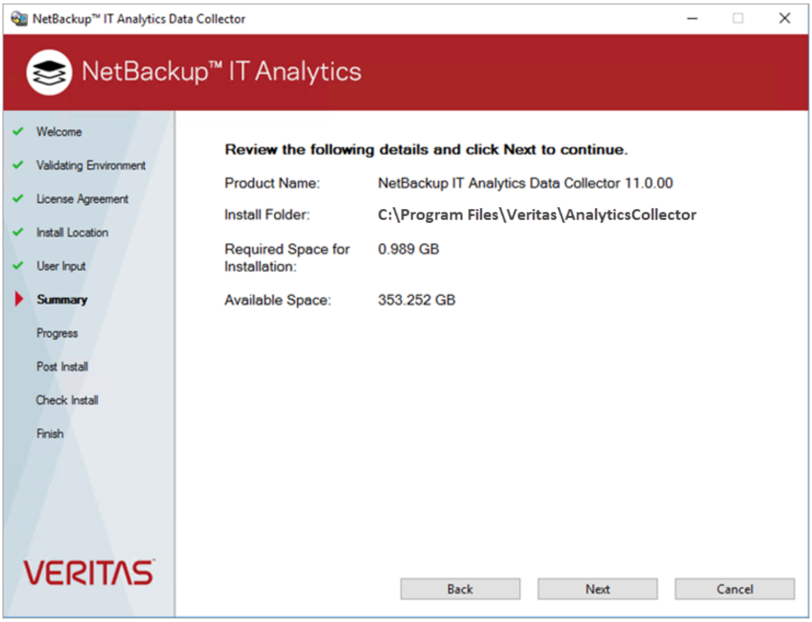
Data Receiver URL*: HTTP itanalyticsagent.sclcsslnx18vm24

Data Collector Key*: C:\Users\Administrator\Downloads\win.key

Proxy settings

	Address	Port
HTTP		
HTTPS		
UserId		
Password		
No Proxy For		

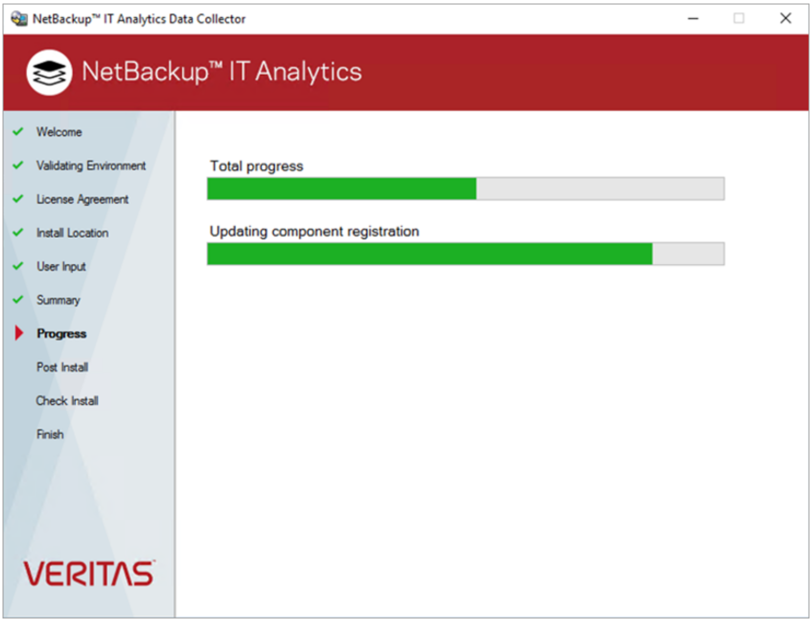
8 Review the installation summary and the available disk space before you proceed with the installation.



Review the following details and click Next to continue.

Product Name:	NetBackup IT Analytics Data Collector 11.0.00
Install Folder:	C:\Program Files\Veritas\AnalyticsCollector
Required Space for Installation:	0.989 GB
Available Space:	353.252 GB

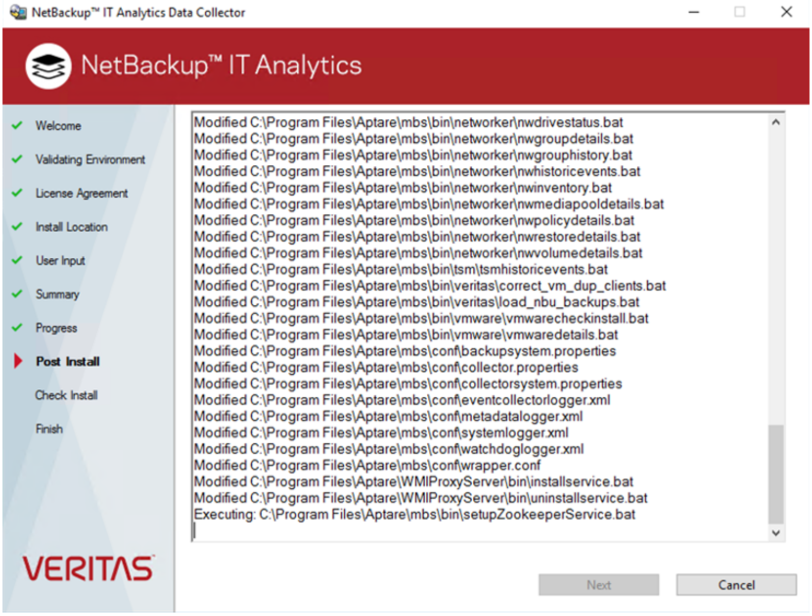
9 Click **Next** to initiate the installation.



Total progress

Updating component registration

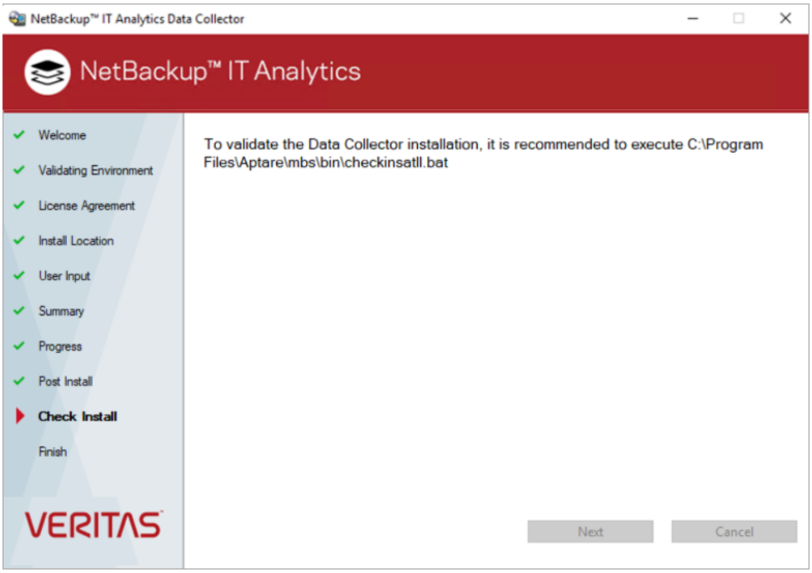
10 Review the post install details and click **Next**.



```
Modified C:\Program Files\Aptare\mbs\bin\networker\nwdrivestatus.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwgroupdetails.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwgrouphistory.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwhistoricevents.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwinventory.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwmediapooldetails.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwpolicydetails.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwrestoredetails.bat
Modified C:\Program Files\Aptare\mbs\bin\networker\nwvolumedetails.bat
Modified C:\Program Files\Aptare\mbs\bin\tsm\tsmhistoricevents.bat
Modified C:\Program Files\Aptare\mbs\bin\veritas\correct_vm_dup_clients.bat
Modified C:\Program Files\Aptare\mbs\bin\veritas\load_nbu_backups.bat
Modified C:\Program Files\Aptare\mbs\bin\vmware\vmwarecheckinstall.bat
Modified C:\Program Files\Aptare\mbs\bin\vmware\vmwaredetails.bat
Modified C:\Program Files\Aptare\mbs\conf\backupsystem.properties
Modified C:\Program Files\Aptare\mbs\conf\collector.properties
Modified C:\Program Files\Aptare\mbs\conf\collectorsystem.properties
Modified C:\Program Files\Aptare\mbs\conf\eventcollectorlogger.xml
Modified C:\Program Files\Aptare\mbs\conf\metadatalogger.xml
Modified C:\Program Files\Aptare\mbs\conf\systemlogger.xml
Modified C:\Program Files\Aptare\mbs\conf\watchdoglogger.xml
Modified C:\Program Files\Aptare\mbs\conf\wrapper.conf
Modified C:\Program Files\Aptare\WMIProxyServer\bin\installservice.bat
Modified C:\Program Files\Aptare\WMIProxyServer\bin\uninstallservice.bat
Executing: C:\Program Files\Aptare\mbs\bin\setupZookeeperService.bat
```

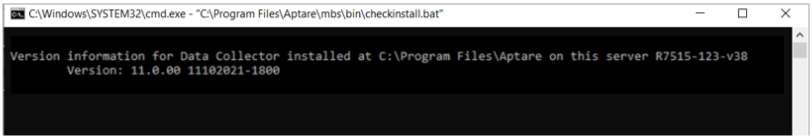
11 To validate the Data Collector installation, run the `C:\Program Files\Veritas\AnalyticsCollector\mbs\bin\checkinstall.bat` batch file.

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



To validate the Data Collector installation, it is recommended to execute C:\Program Files\Aptare\mbs\bin\checkinsatll.bat

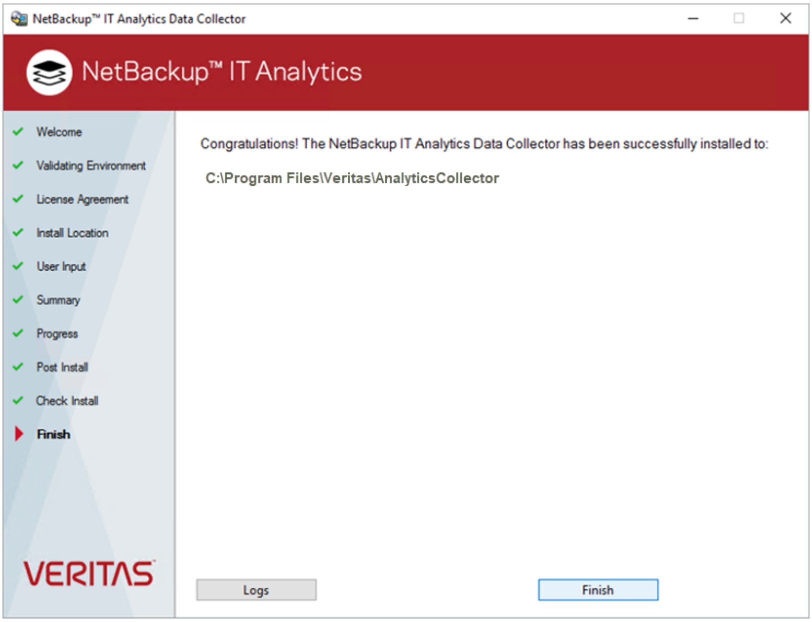
If you wish to run `checkinstall.bat` later, you can run the script from the command prompt.


C:\Windows\SYSTEM32\cmd.exe - "C:\Program Files\Aptare\mbs\bin\checkinstall.bat"

```
Version information for Data Collector installed at C:\Program Files\Aptare on this server R7515-123-v38
        Version: 11.0.00 11102021-1800
```

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

Your Data Collector installation is complete.



Congratulations! The NetBackup IT Analytics Data Collector has been successfully installed to:

C:\Program Files\Veritas\AnalyticsCollector

Install Data Collector software on Linux

To install Data Collector software on Linux:

1. Login as root on the server where NetBackup IT Analytics Data Collector has to be installed.
2. Ensure the following rpms are present on the system:

   On SuSe: libXrender1 and libXtst6 insserv-compat

   On other Linux systems: libXtst and libXrender chkconfig

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

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

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

   The output of the above commands will print the rpms that are present on the system.
3. Go to the downloads section under **Support** on *www.veritas.com* and click the relevant download link.
4. Mount the ISO image that you downloaded.

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

   Substitute the name of the ISO image downloaded have downloaded.
5. Start the installer:

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

6. Review the End User License Agreement (EULA) and enter **accept** to agree.
7. Provide the install location. The default location is `/usr/openv/analyticscollector`. Accepting the default paths is recommended.

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

8 The installer will prompt for the Data Collector Name. This is the name that you used during the configuration of Data collector in Portal UI. The Data Collector will use this value for authentication purposes.

9 The installer requests for the following details.

- **Data Collector Name**: Specify the Data Collector name that you used during its configuration on the NetBackup IT Analytics Portal. Data Collector uses this for authentication. If you are installing on a non-English OS, the Data Collector name must be in English.
- **Data Collector Passcode**: Specify the Data Collector passcode that you used for the Data Collector name during its configuration on the NetBackup IT Analytics Portal. This passcode is encrypted prior to saving it to the portal database and is never visible in any part of the application. If the password contains a special character, make sure it is one of the following OS-specific supported character:
  - Linux: !@#%^*
  - Windows: !@#$%^&*()

  If the special character in the passcode is not supported on the OS, you must update the Data Collector passcode on the portal.
- **Data Receiver URL**: Enter the URL that the Data Collector will use to communicate with the portal server. The format must be *http://itanalyticsagent.yourdomain.com*.

  Make sure you enter the URL with the prefix **itanalyticsagent** and not itanalyticsportal.
- **Data Collector Key File Path**: Enter the location of the downloaded collector key file for encryption.

  If the existing key file is not available, regenerate it and download a new key file from the portal and enter its file path.
- Web Proxy (HTTP) settings can be configured. Enter **y** to configure proxy. The installer prompts for:
  - **HTTP Proxy IP Address**: Enter the hostname or IP address and a port number.
  - **HTTP Proxy Port**: Enter the proxy port number for HTTP proxy.
  - **Proxy UserId and password**: Enter the credentials for the proxy server.
  - **No Proxy For**: Enter the host names or IP addresses separated by commas that will not be routed through the proxy.

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

Deploy Data Collector in native Kubernetes environment

This procedure provides the steps to deploy Data Collector Docker image on a Kubernetes cluster through an operator with the required configuration on Linux hosts. This method enables efficient Data Collector installation and reduces the human errors caused during manual or ISO-based installations.

Prerequisites and dependencies

System requirements and installation dependencies for the system on which Data Collector will be installed are listed below:

- Obtain the Docker image generated from the CI/CD build.
- Kubernetes must be pre-installed on the system.
- Assume root role on the host system.
- Kubernetes cluster must be accessible on the system.
- Ensure that the file system supporting the `/data` directory has enough free space as recommended in the *NetBackup IT Analytics Certified Configurations Guide* for Data Collector.

  The `/data` directory in the host system will be mounted inside the container as `/usr/openv/analyticscollector`.
- Obtain the following Data Collector details. You are required to supply these details to the installer during the installation process.
  - Registry: The name of the registry to which you want to push the installer images.
  - Data Collector Name: Name of the Data Collector as defined in the portal.
  - Data Collector Passcode: The passcode assigned to the Data Collector during its creation.
  - Data Receiver URL: Either http:// or https:// URL of the data receiver.
  - Absolute path of Data Receiver Certificate file: Absolute path of the data receiver certificate file downloaded from NetBackup IT Analytics Portal.
  - Absolute path of the Data Collector key file: Absolute path of the data collector key file downloaded from NetBackup IT Analytics Portal.

  - Proxy settings:
  - Portal IP address: IP address of the system hosting the NetBackup IT Analytics Portal.
  - Portal HostName: aptareportal.<DOMAIN> or itanalyticsportal.<DOMAIN>
  - Agent HostName: aptareagent.<DOMAIN> or itanalyticsagent.<DOMAIN>
  - StorageClass Name: Name of the Kubernetes storage class to be used.

- Obtain the `itanalytics_k8s_artificats.tar` from the *Veritas Download Center*. The tarball has the container image, operater image, set of `.yaml` files, and the scripts.

Deploy the Data Collector in Kubernetes environment

To deploy the Data Collector in Kubernetes environment:

1. Login to the Kubernetes cluster.
2. Run this command on the primary node and label the node on which you want to deploy the Data Collector.

   ```
   kubectl label node <worker_node_name>
   itaDcNodeKey=itaDcDeploymentNode
   ```

3. From the `itanalytics_k8s_artifacts.tar` location, run this command to initiate the Data Collector installation.

   ```
   tar -xvf itanalytics_k8s_artifacts.tar scripts
   ```

   This saves a `scripts` folder at the `itanalytics_k8s_artifacts.tar` file location,.

4. From the `scripts` folder, run this script.

   ```
   cd scripts/
   sh itanalytics_dc_installer.sh
   ```

   Note: The installation logs are saved to `itanalytics_dc_installer_<time_stamp>.log`.

5. Provide the Data Collector configuration details when asked by the installer in the following order.

   - Registry

     The installer asks for a confirmation after providing the registry name to proceed with pushing the images. You need to enter **y** for a fresh installation.

If for any reason, you are required to re-run the installation and this step was successfully completed anytime before for the same cluster node, you can enter **n** to avoid a rewrite and bypass this step.

- Data Collector Name
- Data Collector Passcode
- Data Receiver URL
- Absolute path of Data Receiver Certificate file (if you have set an https:// URL for the data receiver)
- Absolute path of the Data Collector key file
- Proxy settings
- Portal IP address
- Portal HostName
- Agent HostName
- StorageClass Name

6 The installer asks to confirm the configuration details before proceeding with the installation. Enter **y** to proceed with the data collector installation

After a successful installation, verify whether the Data Collector status appears **Online** on the NetBackup IT Analytics Portal.

Connect to the pod instance

Run this command to connect to the pod instance and also to facilitate debugging when required.

```
# kubectl exec -it<pod ID> -- bash
```

Configure Data Collector manually for Veritas NetBackup

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

This procedure provides the manual steps to configure the Data Collector for Veritas NetBackup when Veritas NetBackup primary is not managed under Veritas Alta.

Note that NetBackup IT Analytics Portal must be already installed in your data center and a Data Collector entry must be added via the **Collector Administration** screen of the portal for each NetBackup primary server before you perform this configuration.

Keep the following details handy when you configure the Data Collector:

1. Name of the Data Collector (as it appears on the portal)
2. Passcode of the Data Collector (as configured on the portal)
3. Data receiver URL (generated while creating the data collector on the portal)
4. Key file path (generated while creating the data collector on the portal and copied to the NetBackup primary server)

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

To configure the Data Collector manually on Windows:

1 Create a responsefile as a batch script `responsefile.cmd` with the following contents. These are the responses to the user input required to configure the Data Collector

```
SET DATACOLLECTOR_NAME=<name of the data collector>
SET DATACOLLECTOR_PASSWORD=<passcode for the data collector>
SET DATARECEIVER_URL=< data receiver URL >
SET DATACOLLECTOR_KEY_FILE_PATH=<path to the key file>
SET HTTP_PROXY_CONF=N
SET PROXY_HTTP_URL=
SET PROXY_HTTP_PORT=
SET PROXY_HTTPS_URL=
SET PROXY_HTTPS_PORT=
SET PROXY_USERID=
SET PROXY_PASSWORD=
SET PROXY_NOT_FOR=
```

Note: A sample response file responsefile.cmd is also available in the installer media.

2 Run the command:

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

To configure the Data Collector manually on Linux:

1 Create a response file with the following contents:

```
COLLECTOR_NAME=<name-of-collector>
COLLECTOR_PASSWORD=<passcode>
DR_URL=<data
receiver-url-example:-http://aptareagent.punr740-16-vm14>
COLLECTOR_KEY_PATH=<keyfile path>
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

2 Update the value for each field with appropriate data.

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

3 Run any one of the following command:

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

Or

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

Install Data Collector on Windows host independent of portal

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

Install the Data Collector

To install a Data Collector:

1. Download and mount the Data Collector installer ISO file.
2. Install the Data Collector using `silentinstall.cmd` and follow the installation prompt.

   You can install the Data Collector in the following options:

   - Install at default location:

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

   - Install at custom location:

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

   The independent Data Collector installation is complete.

Configure the Data Collector using responsefile

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

To configure the Data Collector:

1. Obtain the following details from the NetBackup IT Analytics Portal:
   - Data Collector name
   - Data Collector passcode
   - Key file downloaded from the portal
   - Data receiver URL

- Proxy server configuration details

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

```
@ECHO OFF

REM -------------------------------------------------
SET DATACOLLECTOR_NAME=
REM -------------------------------------------------
REM  Description: Enter Data Collector Name. This Data Collector
 name will be used to authenticate the Data Collector with the
Data Receiver.
REM  Required: True

REM -------------------------------------------------
SET DATACOLLECTOR_PASSCODE=
REM -------------------------------------------------
REM  Description: Enter Data Collector Passcode. This Data
Collector passcode will be used to authenticate the Data Collector
 with the Data Receiver.
REM  Required: True

REM -------------------------------------------------
SET DATARECEIVER_URL=
REM -------------------------------------------------
REM  Description: Enter Data Receiver URL. Enter the URL to the
Data Receiver. Ex: http(s)://itanalyticsagent.mycompany.com.
REM  Required: True
REM  Example: http://itanalyticsagent.mycompany.com ,
https://itanalyticsagent.mycompany.com

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

REM -------------------------------------------------
SET HTTP_PROXY_CONF=N
REM -------------------------------------------------
REM  Description: It indicate whether proxy should be configured
 or not
```

```
REM  Valid input values: Y,N
REM  Default value: N

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

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

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

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

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

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

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

```
for proxy
REM  Default value:
```

3 For config installation, run below command from command prompt:

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

or

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

Uninstall Data Collector

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

Install Data Collector on Linux host independent of portal

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

To install a Data Collector:

1 Download and mount the Data Collector installer `itanalytics_datacollector_linux_11100.iso`.

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

2 Install the Data Collector installer at its default path.

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

To install at custom location:

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

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

Configure the Data Collector using responsefile

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

To configure the Data Collector:

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

- Data Collector name
- Data Collector passcode
- Key file downloaded from the portal
- Data receiver URL
- Proxy server configuration details

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

```
COLLECTOR_NAME=<name-of-collector>
COLLECTOR_PASSCODE=<passcode>
DR_URL=<data receiver-url>
COLLECTOR_KEY_PATH=<keyfile path>
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

3 Configure the data collector using the above response file.

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

or

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

4 Start the data collector service

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

Uninstall Data Collector

Run this command to uninstall the Data Collector.

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

Validate data collection

This chapter includes the following topics:

Validation methods

Validation methods are initiated differently based on subsystem vendor associated with the Data Collector policy, but perform essentially the same functions. Refer to the following table for vendor-specific validation methods.

- Test Connection - Initiates a connection attempt directly from a data collector policy screen that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors.
- On-Demand data collection run - Initiates an immediate end-to-end run of the collection process from the Portal without waiting for the scheduled launch. This on-demand run also serves to validate the policy and its values (the same as Test Connection), providing a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. This is initiated at the policy-level from **Admin>Data Collection>Collector Administration.**
  See "Working with on-demand Data Collection" on page 237.

- CLI Checkinstall Utility- This legacy command line utility performs both the Test Connection function and On-Demand data collection run from the Data Collector server.
  See "Using the CLI check install utility" on page 245.

Note: NetBackup IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

Data Collectors: Vendor-Specific validation methods

Table 19-1 Vendor-specific validation requirements.

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Amazon Web Services (AWS)	x	x	
Brocade Switch		x	
Brocade Zone Alias	x	x	
Cisco Switch		x	
Cisco Zone Alias	x	x	
Cohesity DataProtect	x	x	
Commvault Simpana			x
Compute Resources	x		
Dell Compellent			x
Dell EMC Elastic Cloud Storage (ECS)	x	x	
Dell EMC NetWorker Backup & Recovery	x		
Dell EMC Unity	x	x	
EMC Avamar		x	
EMC Data Domain Backup	x	x	
EMC Data Domain Storage	x	x	

Table 19-1 Vendor-specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
EMC Isilon		x	
EMC NetWorker			x
EMC Symmetrix	x	x	
EMC VNX	x	x	
EMC VNX Celerra			x
EMC VPLEX			x
EMC XtremIO	x	x	
HDS HCP	x	x	
HDS HNAS		x	
HP 3PAR			x
HP Data Protector			x
HP EVA			x
HPE Nimble Storage	x	x	
Hitachi Block			x
Hitachi Content Platform (HCP)	x	x	
Hitachi NAS	x	x	
Huawei OceanStor	x	x	
IBM Enterprise			x
IBM SVC			x
IBM Spectrum Protect (TSM)		x	
IBM VIO	x	x	
IBM XIV			x
INFINIDAT Infinibox	x	x	
Microsoft Azure	x	x	

Table 19-1 Vendor-specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Microsoft Hyper-V	x	x	
Microsoft Windows Server	x	x	
NAKIVO Backup & Replication	x	x	
NetApp E Series			x
Netapp		x	
Netapp Cluster Mode		x	
OpenStack Ceilometer	x	x	
OpenStack Swift	x Test Connection is included with the Get Nodes function.	x	
Oracle Recovery Manager (RMAN)	x	x	
Pure FlashArray	x	x	
Rubrik Cloud Data Management	x	x	
VMWare			x
Veeam Backup & Replication	x	x	
Veritas Backup Exec			x
Veritas NetBackup	x	x	
Veritas NetBackup Appliance	X	x	

Working with on-demand Data Collection

Collections can run on a schedule or on-demand using the **Run** button on the action bar. On-demand allows you to select which probes and devices to run. The on-demand run collects data just like a scheduled run plus additional logging information for troubleshooting. A stopped Policy still allows an on-demand collection run, provided the policy is assigned to one of the specified vendors and the collector is online.

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

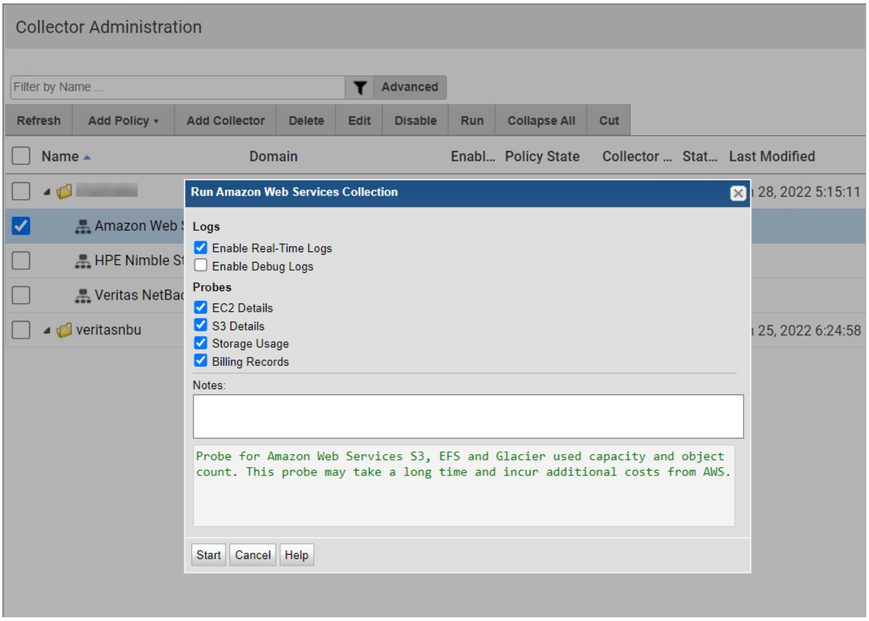
On-Demand data collection serves multiple purposes. You can use it to:

- Validate the collection process is working end-to-end when you create a data collector policy
- Launch an immediate run of the collection process without waiting for the scheduled run
- Populate your database with new/fresh data
- Choose to view the collection logs on the portal while performing an on-demand run.

To initiate an on-demand data collection

1. Select **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Click **Expand All** to browse for a policy or use **Search**.
3. Select a data collector policy from the list. If the vendor is supported, the **Run** button is displayed on the action bar.

4. Click **Run**. A dialog allowing you to select servers and individual probes to test the collection run is displayed. The following example shows the Amazon Web Services dialog. See the vendor specific content for details on probes and servers.



☐	Name ▴	Domain	Enabl...	Policy State	Collector ...	Stat...	Last Modified
☐	[redacted]						28, 2022 5:15:11
☑	Amazon Web S						
☐	HPE Nimble St						
☐	Veritas NetBac						
☐	veritasnbu						25, 2022 6:24:58

Run Amazon Web Services Collection

Logs

☑ Enable Real-Time Logs
☐ Enable Debug Logs

Probes

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

Notes:

```
Probe for Amazon Web Services S3, EFS and Glacier used capacity and object
count. This probe may take a long time and incur additional costs from AWS.
```

5. Select the servers and probes for data collection.

6. The portal enables the user to log the messages at various level during the collection process. Following are the available options:

   - **Enable Real-Time Logs**: This option enables the user to log generally useful information in real-time when the collection is in progress, select **Enable Real-Time Logs**.

   - **Enable Debug Logs**: This option enables the user to log information at a granular level, select **Enable Debug Logs**

7. Click **Start**. Data is collected just like a scheduled run plus additional logging information for troubleshooting. Once started, you can monitor the status of the run through to completion.

Note: If there is another data collection run currently in progress when you click **Start**, the On-Demand run will wait to start until the in-progress run is completed.

See "View real-time logging during an on-demand collection" on page 240.

See "Generating debug level logs during an on-demand collection" on page 241.

View real-time logging during an on-demand collection

By default, real-time logging is enabled when you initiate an on-demand collection for a data collector. **Admin** > **Data Collection** > **Collector Administration** provides a window to view the logs in real-time as the collection progresses.

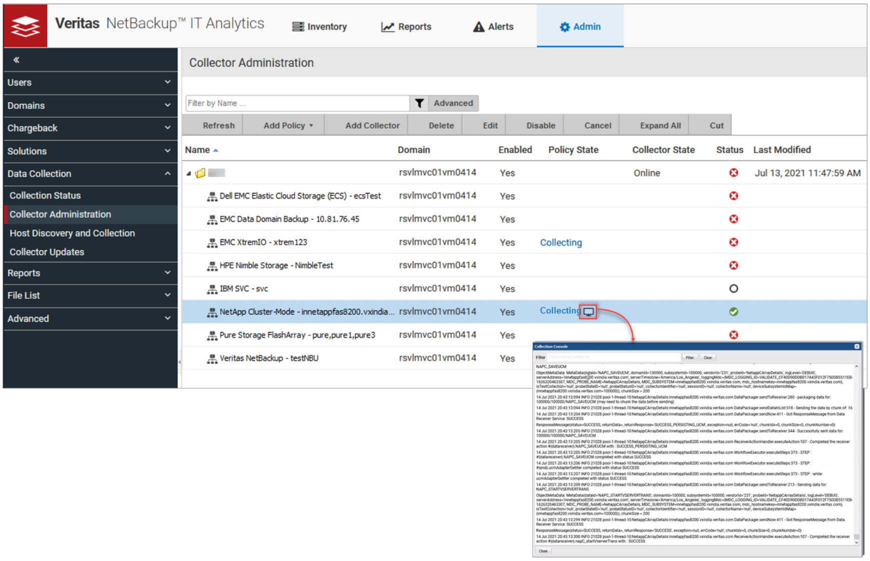
The following steps help you to view the real-time logging:

1. Go to **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.

2. Initiate an on-demand data collection as described under Working with on-demand Data Collection with **Enable Real-Time Logs** selected.

   The **Policy State** column displays status as **Collecting** and an icon to open the **Collection Console** pop-up.

3. Click the icon next to the **Collecting** link to view the real-time logs in the **Collection Console**. Real-time logs are visible as long as the data collection is in progress and the **Collection Console** is open.



Collector Administration

Name ▲	Domain	Enabled	Policy State	Collector State	Status	Last Modified
[redacted]	rsvlmvc01vm0414	Yes		Online	☒	Jul 13, 2021 11:47:59 AM
Dell EMC Elastic Cloud Storage (ECS) - ecsTest	rsvlmvc01vm0414	Yes			☒	
EMC Data Domain Backup - 10.81.76.45	rsvlmvc01vm0414	Yes			☒	
EMC XtremIO - xtrem123	rsvlmvc01vm0414	Yes	Collecting		☒	
HPE Nimble Storage - NimbleTest	rsvlmvc01vm0414	Yes			☒	
IBM SVC - svc	rsvlmvc01vm0414	Yes			○	
NetApp Cluster-Mode - innetappfas8200.vxindia...	rsvlmvc01vm0414	Yes	Collecting		✓	
Pure Storage FlashArray - pure,pure1,pure3	rsvlmvc01vm0414	Yes			☒	
Veritas NetBackup - testNBU	rsvlmvc01vm0414	Yes				

```
NAPC_SAVEUCM
ObjectMetaData: MetaData(dataId='NAPC_SAVEUCM', domainId=100000, subsystemId=100000, vendorId='231', probeId='NetappCArrayDetails', logLevel='DEBUG', serverAddress='innetappfas8200.vxindia.veritas.com', serverTimezone='America/Los_Angeles', loggingMdc={MDC_LOGGING_ID=VALIDATE_CF40D90DDB017A43F012F750DB5511EB-1626320463307, MDC_PROBE_NAME=NetappCArrayDetails, MDC_SUBSYSTEM=innetappfas8200.vxindia.veritas.com, mdc_hostnamekey=innetappfas8200.vxindia.veritas.com}, isTestCollection='null', probeStateID='null', probeStatusID='null', collectorIdentifier='null', sessionID='null', collectorName='null', deviceSubsystemIdMap={innetappfas8200.vxindia.veritas.com=100000}), chunkSize = 200
14 Jul 2021 20:43:13:094 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendToReceiver:280 - packaging data for: 100000/100000/NAPC_SAVEUCM (may need to chunk the data before sending)
14 Jul 2021 20:43:13:094 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendDataInList:518 - Sending the data by chunk of: 16
14 Jul 2021 20:43:13:204 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendNow:411 - Got ResponseMessage from Data Receiver Service: SUCCESS
ResponseMessage(status=SUCCESS, returnData=, returnResponse='SUCCESS_PERSISTING_UCM', exception=null, errCode='null', chunkIdx=0, chunkSize=0, chunkNumber=0)
14 Jul 2021 20:43:13:205 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendToReceiver:344 - Successfully sent data for: 100000/100000/NAPC_SAVEUCM
14 Jul 2021 20:43:13:205 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com ReceiverActionHandler.executeAction:107 - Completed the receiver action #(datareceiver).NAPC_SAVEUCM with : SUCCESS_PERSISTING_UCM
14 Jul 2021 20:43:13:205 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com WorkflowExecutor.executeSteps:373 - STEP : #(datareceiver).NAPC_SAVEUCM completed with status SUCCESS
14 Jul 2021 20:43:13:206 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com WorkflowExecutor.executeSteps:373 - STEP : #(end).ucmAdapterGetIter completed with status SUCCESS
14 Jul 2021 20:43:13:207 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com WorkflowExecutor.executeSteps:373 - STEP : while-ucmAdapterGetIter completed with status SUCCESS
14 Jul 2021 20:43:13:209 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendToReceiver:213 - Sending data for: NAPC_STARTVSERVERTRANS
ObjectMetaData: MetaData(dataId='NAPC_STARTVSERVERTRANS', domainId=100000, subsystemId=100000, vendorId='231', probeId='NetappCArrayDetails', logLevel='DEBUG', serverAddress='innetappfas8200.vxindia.veritas.com', serverTimezone='America/Los_Angeles', loggingMdc={MDC_LOGGING_ID=VALIDATE_CF40D90DDB017A43F012F750DB5511EB-1626320463307, MDC_PROBE_NAME=NetappCArrayDetails, MDC_SUBSYSTEM=innetappfas8200.vxindia.veritas.com, mdc_hostnamekey=innetappfas8200.vxindia.veritas.com}, isTestCollection='null', probeStateID='null', probeStatusID='null', collectorIdentifier='null', sessionID='null', collectorName='null', deviceSubsystemIdMap={innetappfas8200.vxindia.veritas.com=100000}), chunkSize = 200
14 Jul 2021 20:43:13:299 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com DataPackager.sendNow:411 - Got ResponseMessage from Data Receiver Service: SUCCESS
ResponseMessage(status=SUCCESS, returnData=, returnResponse='SUCCESS', exception=null, errCode='null', chunkIdx=0, chunkSize=0, chunkNumber=0)
14 Jul 2021 20:43:13:300 INFO 21028 pool-1-thread-10:NetappCArrayDetails:innetappfas8200.vxindia.veritas.com ReceiverActionHandler.executeAction:107 - Completed the receiver action #(datareceiver).napC_startVserverTrans with : SUCCESS
```

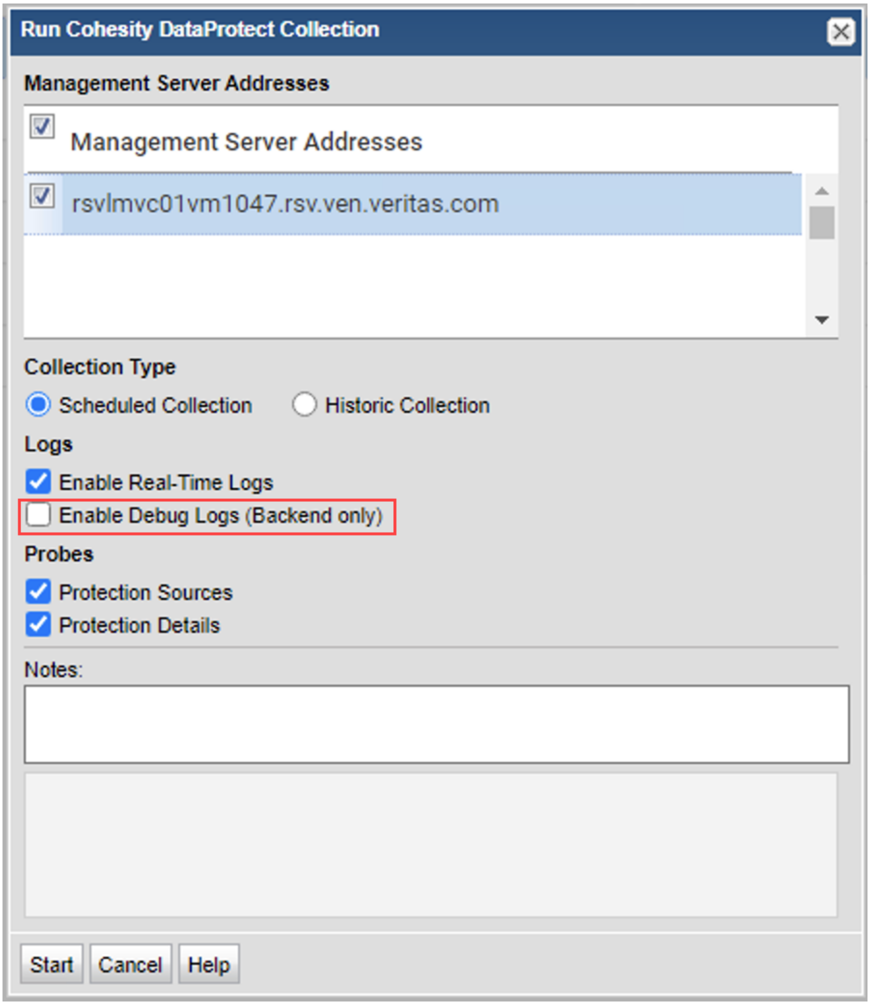
You can use the filter on the console to selectively view the logs of your choice. The **Collection Console** icon is not visible if the data collection is not in progress.

Generating debug level logs during an on-demand collection

By default, **Enable Debug Logs (Backend only)** option is not selected when you initiate an on-demand collection for a data collector. The **Collector Administration** provides a window to generate debug level information as the collection progresses.

The following steps to enable debug level log file generation:

1. Go to **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Initiate an on-demand data collection as described under Working with on-demand Data Collection with **Enable Debug logs (Backend only)** option selected.



Run Cohesity DataProtect Collection

Management Server Addresses

☑ Management Server Addresses

☑ rsvlmvc01vm1047.rsv.ven.veritas.com

Collection Type

● Scheduled Collection ○ Historic Collection

Logs

☑ Enable Real-Time Logs

☐ Enable Debug Logs (Backend only)

Probes

☑ Protection Sources

☑ Protection Details

Notes:

Note: The path for generated log file on data collector server:
`<APTARE_HOME>/mbs/logs/validation/`

Collect historic data on-demand

You can follow this procedure to run an on-demand historic data collection of the supported vendor policies and load historic events on the NetBackup IT Analytics Portal.

Ensure you have an existing supported vendor policy configured with a Data Collector and the Data Collector must be online before you initiate a on-demand historic data collection.

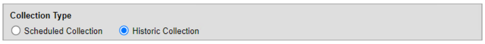
Table 19-2 Supported vendors for historic data collection

Vendor name	Supported collection
Veritas NetBackup	Date range
Cohesity	Time period (in hours) and date range

To initiate a on-demand historic data collection:

1. Select **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Click **Expand All** to browse for a supported vendor policy or use **Search**.
3. Select the supported data collector policy from the list.
4. From the action bar, click **Run**. A dialog allowing you to select individual probes and servers to run the collection is displayed. See the vendor specific content for details on probes and servers.

   A dialog allowing you to specify the collection type is displayed.

   Collection Type
   ○ Scheduled Collection ● Historic Collection

5 Select **Historic Collection** and specify other details based on the field descriptions below:

NetBackup Servers (for NetBackup policies) Management Server Addresses (for Cohesity policies)	Select the servers from which the policy must collect the historic data.
Probes	Applicable probes are enabled by default. If you disable any probes, ensure you keep at least one probe in enabled state.
Time Period	The on-demand function retrieves historic data collected within the duration specified under this.
Lookback Hours (for Cohesity policies)	Enter the duration in hours. The moment you initiate the on-demand collection, historic data from the collection performed within the Lookback Hours is retrieved, based on the policy and the probe.
Start Date and Time	Specify the start date and time of the historic data collection.
End Date and Time	Specify the end date and time of the historic data collection.
Client Names (for NetBackup policies)	Specify one or more client names for NetBackup historic collection. Separate the names by commas. This field appears if only one server is selected in **NetBackup Servers**.
Notes	Enter your comments about the on-demand historic data collection.

Note: The Start Date/Time and End Date/Time are calculated based on the time zone of the server specified while adding the server on the policy screen. Also, the Scheduled Collection interface remains disabled until the on-demand collection is in progress.

6 Click **Start**. Data is collected just like a scheduled run plus additional logging information for troubleshooting. You can monitor the collection progress of the run through **Collection Status** page. The collection is queued if another data collection run is in progress.

Using the CLI check install utility

This legacy utility performs both the Test Connection function and On-Demand data collection run from a command line interface launched from the Data Collector server.

Note: NetBackup IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

The following directions assume that the Data Collector files have been installed in their default location:

Windows (`C:\Program Files\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 terminal/SSH session logged in as root to the **Data Collector Server**.

2 Change to the directory where you’ll run the validation script.

Windows: At the command prompt, type:

```
cd C:\Program Files\Aptare\mbs\bin <enter>
```

Linux: In the SSH 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 SSH session. type: `./checkinstall.sh` <enter>

The **checkinstall** utility performs a high-level check of the installation, including a check for the domain, host group and URL, Data Collector policy and database connectivity. This utility will fail if a Data Collector policy has not been configured in the Portal. For a component check, specifically for Host Resources, run the **hostresourcedetail.sh|bat**utility.

Checkinstall includes an option to run a probe for one or more specific devices. Note that certain Data Collectors will not allow individual selection of devices. Typically these are collectors that allow the entry of multiple server addresses or ranges of addresses in a single text box.

These collectors include: Cisco Switch, EMC Data Domain, EMC VNX arrays, HP 3PAR, IBM mid-range arrays, IBM XIV arrays and VMware.

Data Collectors that probe all devices that are attached to a management server also do not allow individual selection of devices: EMC Symmetric, File Analytics, Hitachi arrays and IBM VIO.

4 If the output in the previous steps contains the word **FAILED**, then contact Support and have the following files ready for review:

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

```
C:\Program Files\Aptare\mbs\logs\validation\
```

List Data Collector configurations

Use this utility to list the various child threads and their configurations encapsulated within a data collector configuration. This utility can be used in conjunction with other scripts, such as **checkinstall.[sh|bat]**.

On Linux: **./listcollectors.sh**

On Windows: **listcollectors.bat**

Chapter 20

Manually start the Data Collector

This chapter includes the following topics:

Introduction

The installer configures the Data Collector to start automatically, however, it does not actually start it upon completion of the installation because you must first validate the installation. Follow these steps, for the relevant operating system, to manually start the Data Collector service.

This also starts the Aptare Agent process, Zookeeper, and Kafka services on the respective systems.

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 **Services** dialog is displayed.
4. Start the **Aptare Agent** service.

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:

```
/opt/aptare/mbs/bin/aptareagent start
```

Uninstall the Data Collector

This chapter includes the following topics:

Uninstall the Data Collector on Linux

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

To uninstall the Data Collector software from a Linux host:

1 Login to the Data Collector server as root.

2 For NetBackup IT Analytics Data Collector version 10.6 or lower, execute the `Uninstall APTARE IT Analytics Data Collector Agent` script located at `*<Data Collector home folder>*/UninstallerData`

For example:

```
/opt/aptare/UninstallerData/Uninstall APTARE IT Analytics Data
Collector Agent
```

3 For NetBackup IT Analytics Data Collector version 11.0 or later, execute `uninstall_dc.sh script` located at `*<Data Collector home folder>*/UninstallerData/uninstall_dc.sh`

For example:

```
/opt/aptare/UninstallerData/uninstall_dc.sh
```

Uninstall the Data Collector on Windows

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

To uninstall the Data Collector software from a Windows host:

1 Login to the Data Collector server as an administrator.

2 Go to **Control Panel** > **Add and Remove Program** > **Programs and Features** and uninstall **NetBackup IT Analytics Data Collector**.

The uninstaller may not delete the entire Data Collector directory structure. Sometimes new files that were created after the installation are retained along with their parent directories. If the Data Collector was upgraded from version 10.6 or older, you may find entries of Kafka and Zookeeper services on the services panel (default `C:\Program Files\Aptare`), even after the uninstallation of the Data Collector. You must manually delete the services and reboot the system.

Appendix A

Load historic events

This appendix includes the following topics:

Introduction

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

Note: If the scheduled data collection process oversights the data, the Historic Event Collection should be used.

Note: For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Data Collector software.

Load Commvault Simpana events

Commvault Simpana Historic Collection uses a JDBC connection to collect jobs data from the Commvault Simpana database for a given look back hours.

Configure **COMMVAULT_OLDEST_JOB_HOURS** parameter for historic data collection.

Note: The allowed maximum number of hours to look back for historic data collection is 168 hours. Historic collection is normally used on first time collection. It retrieves the details of the backup jobs, restore jobs, and job failures from the database using the SQL queries.

Windows:

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

Linux:

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

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

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

Where:

- This utility will write data to a set of files in the output directory specified in `output_dir`.
- The cvdb_username, cvdb_password and cvdb_hostname refer to the CommServ database system (this is usually the same as the CommServ server) from which you are collecting data.
- [Optional]Port Number can be appended to the cvdb_hostname, separated by a colon.

Note: If a port number is not specified, default 1433 port is assigned.

- [Optional]Maximum number of hours from which to start the collection can be specified. This value is used to calculate the current time minus the number of hours that was entered.

  If you do not enter a maximum number of hours, then all details retained by the Commvault Simpana database will be retrieved.
- The last set of cv_username, cv_password and cv_hostname are required only if you are collecting Skipped File Details from a Windows-based CommServ Server.

Load EMC Avamar events

EMC Avamar Historic Data Collection uses JDBC as a read-only user to collect point-in-time data of backup events / activities from the Avamar Management Console Server (MCS) database within a given time frame.

It retrieves backup information from Avamar MCS database using the following views:

- `v_repl_activities` - extracts record for each replication activity.
- `v_plugin_catalog` - extracts record for each known plug-in.
- `v_activities_2` - extracts record for each backup, restore, or validation activity.
- `v_datasets` - extracts record for each data set known to the MCS.
- `v_retention_policies` - extracts record for each retention policy known to the MCS.

Windows:

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

Linux:

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

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

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

Where:

- The MetadataCollectorID and the SubSystemID can be found by executing the utility:
  Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Avamar commands called to the metadata.log file.

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

Load EMC NetWorker events

NetWorker Historic Collection uses `mminfo` command to extract backup information and save sets for a given time frame.

By default, the `mminfo` command gets information about the Backup media and save sets that were completed during the last 24 hours. This includes: the volume name, client name, creation date, amount of data saved to the volume, level of backup performed, and the name of the save set.

Windows:

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

Linux:

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

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

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

Where:

- The EventCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the NetWorker commands called to the `eventcollector.log` file.

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

Load HP Data Protector events

The HP Data Protector (HPDP) Historic event collection captures backup details for all the sessions within a given time frame which is present in HPDP System. It uses the HPDP omnidb and omnirpt CLIs to query the data protector internal database for detailed backup information.

- `omnidb` - Queries the data protector internal database. This command is available on systems with the data protector user interface component installed.
- `omnirpt` - Generate various reports of the data protector environment, for example, about backup, object copy, object consolidation and object verification sessions in a specific time phase, session specification, media, data protector configuration, and single sessions. This command is available on systems with the data protector user interface component installed.

Windows:

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

Linux:

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

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

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

Where:

- The EventCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`

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

- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the Data Protector commands called to the `eventcollector.log` file.

Note: If the Start and End Dates are not specified, the utility will capture events that occurred in the previous 24 hours. HP Data Protector commands ignore the time segment of the start and end date values. In addition, the end date value is used as an “until” value.

Note: For example, a value of "2015-05-11 23:59:59" will only collect historic values up to 2015-05-11 00:00:00. To collect values for the date of 2015-05-11 you should enter a end date of "2015-05-12 00:00:00".

Load IBM Spectrum Protect (TSM) events

TSM Historic collection uses `dsmadmc` command with SQL query as one of the parameters to collect all historic data.

Windows:

```
C:\Program Files\Tivoli\TSM\baclient\dsmadmc  -id= <userId>
-password= <password> -tcpserveraddress= <server> -tcpport= <serverPort>
-DISPLaymode=LIst -noconfirm  <query>
```

Linux:

```
C:\Program Files\Tivoli\TSM\baclient\dsmadmc  -id= <userId>
-password= <password> -se= <configInstanceName> -DISPLaymode=LIst
-noconfirm  <query>
```

SQL queries utilizes the following database tables:

- sessions
- EVENT
- actlog
- summary
- summary_extended

Windows:

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

Linux:

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

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

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

Where:

- The MetadataCollectorID and the ServerID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`
- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the IBM Spectrum Protect (TSM) commands called to the `metadata.log` file.

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

Load Oracle Recovery Manager (RMAN) events

RMAN Historic collection fetches Jobs data over JDBC connection from RMAN database. It uses Dynamic Performance (V$) views for fetching backups in individual instances, or Recovery Catalog views for fetching backups from a central Recovery Catalog.

1. Set Advanced Parameter `RMAN_BACKUP_LOOKBACK_DAYS=#`, where # must be a positive numeric value that indicates the days to load (from current day).
2. Set Advanced Parameter `RMAN_BACKUP_LOOKBACK_OVERRIDE=Y`.

   Note: For more information on RMAN_BACKUP_LOOKBACK_OVERRIDE and RMAN_BACKUP_LOOKBACK_DAYS, see *NetBackup IT Analytics User Guide > Customize with advanced parameters >> Adding an advance parameter* section.

3. Navigate to *Admin* >> *Data Collection* >> *Collector Administration*.

4. Select **Oracle RMAN Data Collection** policy and click **Run**.

   You can also wait for the scheduled collection to complete.

5. Reset RMAN_BACKUP_LOOKBACK_DAYS and RMAN_BACKUP_LOOKBACK_OVERRIDE to their original values (or the default values) once the Collection Run is complete. Do not delete the advanced parameters.

Load Veeam Backup & Replication events

Veeam Historic collection uses PowerShell commands to get client, job, session and backup data for a given time span defined by advanced parameters.

The following are the advanced parameters used in the process.

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

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

   Note: For more information on RMAN_BACKUP_LOOKBACK_OVERRIDE and RMAN_BACKUP_LOOKBACK_DAYS, see *NetBackup IT Analytics User Guide* >> *Customizing with Advance Parameter* >> *Adding an advance parameter* section.

   Configuring these parameters, the normal collection (scheduled or on-demand) works as a historic collection. With these parameters, collection probes such as Client Details, Job Details, Session, and Backup Details can be executed to get the historic data.

3. Navigate to **Admin** >> **Data Collection** >> **Collector Administration**.

4. Select Veeam Backup & Replication Data Collection policy and then click **Run**.

   See “Working with on-demand Data Collection” on page 237.

5. Reset `VEEAM_BACKUP_LOOKBACK_OVERRIDE=N` (or the default values) once the Collection Run is complete to avoid historic data collection on future scheduled or On Demand runs,

Load Veritas NetBackup events

The Veritas NetBackup Historic collection is limited to capturing details on successful backup images that are still present in the NetBackup catalog (i.e. unexpired backup images). This historic information is captured using the NetBackup `bpimagelist` command.

The failed jobs are not:

- the part of the historic collection as they are not present in the catalog
- point-in-time metrics such as job throughput.

The following are the steps to execute historic collection from the portal:

1. Log in to the portal.
2. Navigate to *Admin* >> *Data Collection* >> *Collector Administration*.
3. Expand the collector and then select the **NetBackup Policy**.
4. Click **Run**. The **Run Veritas NetBackup Collection** dialog box is displayed.
5. Click **Historic Collection**.
6. Clear the **Enable Real-Time Logs** check box.
7. Clear the **Enable Debug Logs** check box.
8. Select the appropriate **Start Date** and **End Date**.
9. Specify one or more **Client Name(s)**, separated by commas, to limit historic collection to only these specified clients. For example, Client_a, Client_b
10. Click **Start**.

NetBackup IT Analytics gathers backup events from both the NetBackup catalog and the NetBackup activity log. Specify the date range for the backup jobs that occurred during a given time period.

To minimize the impact on performance, upload the backup events for each individual client. However, in many cases, this is not practical. Therefore, several methods are provided to accommodate various needs. Only successful jobs are retrieved from the NetBackup environment.

Load events for individual NetBackup clients

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

Windows:

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

Linux:

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

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

Where:

- The MetadataCollectorID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Load events for a group of NetBackup clients

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

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

Linux

1. Create a NetBackup client list:

   ```
   /usr/openv/netbackup/bin/admincmd/bpplclients -noheader -allunique
    > /tmp/client_list.txt
   ```

2. Load the list into a for loop:

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

```
"<End_Date>"
            done
```

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

Where:

- The MetadataCollectorID can be found by executing the following utility:
  For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
  For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Windows

1. Create a NetBackup client list:

```
C:\program files\Veritas\netbackup\bin\admincmd\bpplclients
-noheader -allunique > c:\client_list.txt
```

2. Load the list into a for loop:

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

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

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

Load Veritas Backup Exec events

Veritas Backup Exec Historic collection uses JDBC connection to query Backup Exec database for capturing all Backup Events data for a specific given time period.

SQL queries utilizes the following Backup Exec Database tables:

- JobHistorySummary
- JobHistoryDetail, Resource
- ResourceContainer

- Jobs
- TaskDefinition
- Policy
- Device
- Schedule
- ComplexTask

Windows:

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

Linux:

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

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

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

Where:

- yyyy-mm-dd hh:mm:ss date format.
- Specifying verbose will log the Backup Exec commands called to the `metadata.log` file.

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

Corrections in duplication of clients

This section applies to those clients that are being reported by Veritas NetBackup's VMware policy.

A VMware backup policy in NetBackup can be configured in several ways with Virtual Machine (VM) Primary identifier set to one of

- Hostname
- Display Name

- DNS Name
- Instance UUID
- BIOS UUID

Due to which the name of the same VM reported by NetBackup may differ depending on how the policy is created, which may result in the same VM getting persisted in Aptare database with different name resulting in duplicates.

To fix the historic data having duplicate clients, execute the following command-line scripts on Data Collector.

Warning: The command should be executed only after upgrading to version 10.6 P14 or 11.0.02.

Windows:

```
C:\Program Files\Aptare\mbs\bin\veritas\correct_vm_dup_clients.bat
<metaDataCollectorId> <primaryServerName>
```

Linux:

```
<APTARE HOME>/mbs/bin/symantec/correct_vm_dup_clients.sh
<metaDataCollectorId> <primaryServerName>
```

Where: The MetadataCollectorID can be found by executing the following utility:

- For Windows: `C:\opt\Aptare\mbs\bin\listcollectors.bat`
- For Linux: `/opt/aptare/mbs/bin/listcollectors.sh`

Cohesity

Cohesity Historic collection uses REST APIs to collect the session and backup information.

To execute the Cohesity Historic data collection from the portal, configure the following advanced parameters within the specific time frame.

- COHESITY_BACKUP_LOOKBACK_HOURS
- COHESITY_BACKUP_START_TIMESTAMP (Unix epoch time in microseconds) Example: 1590488100000000 for (May 26, 2020 10:15:00 AM GMT)
- COHESITY_BACKUP_END_TIMESTAMP (Unix epoch time in microseconds) Example: 1590922800000000 (May 31, 2020 11:00:00 AM GMT)

Note: If the above parameters are not set, then the default look-back time is 36 hours

REST APIs

- `GET /irisservices/api/v1/public/protectionRuns`
  All the parent and child data
- `GET /irisservices/api/v1/public/restore/tasks`
  All the recovery-related data
- `GET /irisservices/api/v1/public/protectionSources/objects/`
  Returns the Protection Source objects corresponding to the specified IDs.
- `GET /irisservices/api/v1/public/protectionJobs/`
  All Protection Jobs currently on the Cohesity Cluster are returned
- `GET /irisservices/api/v1/public/protectionPolicies/`
  Returns the created Protection Policy

Dell EMC NetWorker Backup & Recovery

To enable Historic Collection for Dell EMC Networker, Advanced parameters need to be added.

Note: To add an advance parameter, see *NetBackup IT Analytics User Guide* >> *Customize with advanced parameters* >> *Adding an advance parameter* section.

- DELLEMC_NETWORKER_START_TIME
- DELLEMC_NETWORKER_END_TIME
- Date
  Format - 'yyyy-MM-ddTHH:mm:ss'.
  Example: 2018-05-10T16:00:03. This will be Dell EMC NetWorker server time.
- Host
  Add Dell EMC NetWorker servers, for which this advanced parameter should be applied.

REST API

global/jobs - This call is used in REST API to collect job details.

Firewall configuration: Default ports

This appendix includes the following topics:

- Firewall configuration: Default ports

Firewall configuration: Default ports

The following table describes the standard ports used by the Portal servers, the Data Collector servers, and any embedded third-party software products as part of a standard "out-of-the-box" installation.

Table B-1 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139

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

Component	Default Ports
Oracle Oracle TNS listener port	1521
Tomcat - Data Receiver Apache connector port and shutdown port for Data Receiver instance of tomcat	8011, 8017
Tomcat - Portal Apache connector port and shutdown port for Portal instance of tomcat	8009, 8015
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445
ZooKeeper	2181 **Note:** NetBackup IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the local host where NetBackup IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table B-2 Storage Vendors: Default Ports

Storage Vendor	Default Ports and Notes
Dell Compellent	1433 SMI-S http (5988) SMI-S https (5989)
Dell EMC Elastic Cloud Storage (ECS)	REST API 4443

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

Storage Vendor	Default Ports and Notes
Dell EMC Unity	REST API version 4.3.0 on 443 or 8443
EMC Data Domain Storage	SSH 22
EMC Isilon	SSH 22
EMC Symmetrix	SymCLI over Fibre Channel 2707
EMC VNX	NaviCLI 443, 2163, 6389, 6390, 6391, 6392
EMC VNX (Celerra)	XML API 443, 2163, 6389, 6390, 6391, 6392
EMC VPLEX	https TCP 443
EMC XtremIO	REST API https 443
HP 3PAR	22 for CLI
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0
Hitachi Block Storage	TCP 2001 For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
Hitachi Vantara All-Flash and Hybrid Flash Storage	Hitachi Ops Center Configuration Manager REST API: 23450 for HTTP and 23451 for HTTPS. HIAA : 22015 for HTTP, and 22016 for HTTPS
Huawei OceanStor Enterprise Storage	8080
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989

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

Storage Vendor	Default Ports and Notes
IBM XIV	XCLI TCP 7778
INFINIDAT InfiniBox	REST API TCP 80, 443
Microsoft Windows Server	2012 R2, 2016 WMI 135 DCOM TCP/UDP > 1023
NetApp E-Series	SMCLI 2436
NetApp ONTAP 7-Mode and Cluster-Mode	ONTAP API 80/443
Pure Storage FlashArray	REST API https 443
Veritas NetBackup Appliance	1556

Table B-3 Data protection: Default ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023
Dell EMC Networker Backup & Recovery	Port used for Dell EMC NetWorker REST API connection. Default: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
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
NAKIVO Backup & Replication	Director Web UI port (Default: 4443)

Table B-3 Data protection: Default ports *(continued)*

Data Protection Vendor	Default Ports and Notes
Oracle Recovery Manager (RMAN)	1521
Rubrik Cloud Data Management	REST API 443
Veeam Backup & Replication	9392
Veritas Backup Exec	1433
Veritas NetBackup	443, 1556, and 13724 WMI ports SSH 22 (Linux)

Table B-4 Network & Fabrics: Default Ports

Network & Fabrics Vendor	Default Ports and Notes
Brocade Switch	SMI-S 5988/5989
Cisco Switch	SMI-S 5988/5989

Table B-5 Virtualization Vendors: Default Ports

Virtualization Vendor	Default Ports and Notes
IBM VIO	SSH 22
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESX or ESXi,vCenter,vSphere	vSphere VI SDK https TCP 443

Table B-6 Replication Vendors: Default Ports

Replication Vendor	Default Ports and Notes
NetApp ONTAP 7-Mode	ONTAP API 80/443

Table B-7 Cloud Vendors: Default Ports

Cloud Vendor	Default Ports and Notes
Amazon Web Services	https 443
Microsoft Azure	https 443
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22
Google Cloud Platform	https 443