IT Analytics Data Collector Installation and Configuration Guide for Cohesity NetBackup

Release 11.8

VERITAS
now part of Cohesity

IT Analytics Data Collector Installation and Configuration Guide for Cohesity NetBackup

Last updated: 2026-08-12

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

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

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

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

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

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

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Introduction 10

Overview 10
Distributed Data Collector (recommended for NetBackup) 12
Centralized Data Collector 13
Collection of backup and restore data 15
Data Collection Policies 15

Chapter 2 Configure a IT Analytics Distributed Data Collector on a NetBackup Primary Server 16

Overview 16
Configure Data Collector on non-clustered NetBackup 10.4 and later primary server 18
Manage Data Collector installation on NetBackup primary server 24
Configuration workflow for NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 on a non-clustered NetBackup primary server 25
Configure Data Collector on non-clustered NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 primary server 26
Manage Data Collector installation on NetBackup (install/remove) 38
Configuration workflow for NetBackup versions lower than 10.1.1 39
Configure Data Collector on NetBackup primary with version lower than 10.1.1 41

Chapter 3 Configure a Veritas NetBackup Data Collector Policy 51

Veritas NetBackup Data Collector policy configuration prerequisites 51
Prerequisites for collection from Cohesity NetBackup deployed on Kubernetes clusters 52
Create NetBackup Data Collector Role, Service Account, and API Key 53
Add a Veritas NetBackup Data Collector policy 55

Add/Edit NetBackup Primary Servers within the Data Collector policy 64
Configuring file analytics in NetBackup Data Collector policy 66
Prerequisites to configure File Analytics for NetBackup 67
Data Collector and Portal sizing guidelines for File Analytics 68
Configure File Analytics 68
Export File Analytics data 71

Chapter 4 Installing the Data Collector software 72

Introduction 72
Considerations to install Data Collector on non-English systems 73
Install Data Collector Software on Windows 75
Install Data Collector software on Linux 84
Configure Data Collector manually for Cohesity NetBackup 86
Install Data Collector binaries on Windows (without configuration) 88
Install Data Collector binaries on Linux host (without configuration) 93
Override default Java Heap memory (XMX) value for Data Collector utilities 217

Chapter 5 Configure SSL 96

SSL/TLS certificate configuration 96
SSL implementation overview 97
Obtain an SSL certificate 98
Update the web server configuration to enable SSL on the Portal server 99
Enable / Disable SSL for a Data Collector 104
Enable / Disable SSL for emailed reports 104
Test and troubleshoot SSL configurations 105
Keystore file locations on the Data Collector server 106
Import a certificate into the Data Collector Java keystore 106
Keystore on the portal server 108
Add a virtual interface to a Linux server 108
Add a virtual / secondary IP address on Windows 110

Chapter 6 Centralized Data Collector for NetBackup - Prerequisites, Installation, and Configuration 113

Overview 114
Step-1: Choose operating system and complete prerequisites 115

Factors impacting Data Collector performance and memory requirements 115
Data Collector Supported Operating Systems 116
Data Collector server memory and CPU guidelines 116
Additional prerequisites 116
Linux Data Collector Prerequisites: Changing the Linux Temporary Directory for Collection 117
Step-2: HTTPS requirement 118
Step-3: Add Data Collector on IT Analytics Portal 118
Step-4: Create NetBackup Data Collector Role, Service Account, and API Key 123
Step-5: SSH/WMI 124
Linux Centralized Data Collector: SSH 125
Windows Data Collector: WMI Connectivity 130
Step-6: Install the Data Collector 134
Step-7: Configure Data Collector 135
Step-8: Verify the Data Collector is online from the Portal 141
Step-9: Confirm that the Data Collector is updated 141
Step-10: Configure the data collection policy 141
Step-11: Confirm that the NetBackup data collection policy is collecting data 141

Chapter 7 Upgrading Data Collector Locally 142

Overview 142
Verification of upgrade bundle available on Data Collector server 143
Upgrade the Upgrade Manager component 145
Upgrade the Data Collector component which is the aptare.jar file 146
Upgrade the Upgrade Manager and Data Collector components together 147
Upgrade logs and upgrade related database views 148
Resolve file lock issue on Windows host during Data Collector upgrade 149

Chapter 8 Clustering Data Collectors with VCS and Veritas NetBackup (RHEL) 151

Clustering Data Collectors with VCS and Veritas NetBackup (RHEL) 151
Prerequisites 151
Getting started with Data Collector clustering 152
Configuring the Data Collector 153

Upgrading a clustered Data Collector 153
Considerations when Data Collector is pointing to Alta Domain Management 154

Chapter 9 Clustering Data Collectors with VCS and Veritas NetBackup (Windows) 155

Clustering Data Collectors with VCS and Veritas NetBackup (Windows) 155
Prerequisites 155
Getting Started with Data Collector Clustering 156
Main.cf 159
Upgrading a Clustered Data Collector 163
Manage cluster configuration during NetBackup upgrade (Windows) 163
Uninstall cluster Data Collector 163

Chapter 10 Install and configure IT Analytics Data Collector on MSCS environment 165

Cluster Data Collectors with MSCS on Windows 165
Perform cluster configurations 170
Upgrade IT Analytics Data Collector in MSCS 174
Uninstall IT Analytics Data Collector 176
Steps to perform before and after NetBackup upgrade 177

Chapter 11 Data Collector Policy Migration 181

Migrate NetBackup data collection policy from centralized to distributed Data Collector 181

Chapter 12 Pre-Installation setup for Veritas NetBackup appliance 185

Overview 185
Prerequisites for adding Data Collectors (Veritas NetBackup appliance) 185
Installation Overview (Veritas NetBackup Appliance) 186
Adding a Veritas NetBackup Appliance Data Collector policy 187

Chapter 13 Pre-installation setup for Veritas Flex Appliance 191

Pre-Installation setup for Cohesity Flex Appliance 191
Prerequisites for adding Data Collectors (Veritas Flex Appliance) 192
Installation overview (Cohesity Flex Appliance) 192
Add a Veritas Flex Appliance policy 193
Troubleshoot Veritas Flex Appliance policy configuration 198

Chapter 14 Data Collector Troubleshooting 200

Resolving Data Collectors connections issues - Linux specific 201
Resolving Data Collectors connections issues - Windows specific 202
Portal upgrade performance issues 202
Configuring web proxy updates 203
Host resources troubleshooting 203
Host resources: Check the status of the WMI proxy server 204
Host resources: Post-Installation verification 207
Host resources: Check host connectivity using standard SSH 207
Checking Paths for SSH 208
Environment setting for bash users 208
Host resources: Check host connectivity 208
Host resources: Check host connectivity using Host Resource Configuration file 210
Host resources: Generating host resource configuration files 211
Sample lines in an input file 211
Host resources: Check the execution of a command on a remote server 212
Host resources Data Collection 213
Host resources: Collection in stand-alone mode 213
Configuring parameters for SSH 214
Configure channelWaitTime 214
Configure singleChannelSession 214
Configure sudoWithPassword 214
Identifying Windows file system access errors (File Analytics) 215
Collect from remote shares (File Analytics) 215
Adding a certificate to the Java keystore 216
Override default Java Heap memory (XMX) value for Data Collector utilities 217

Appendix A Configure Appliances 219

Configure NetBackup Appliances for Data Collection 219
Configure NetBackup Flex Appliances for Data Collection 220

Appendix B Load historic events 223

Introduction 223
Load Veritas NetBackup events 223
Load events for individual NetBackup clients 224
Load events for a group of NetBackup clients 225
Update Cohesity NetBackup SLP Job Details 226

Appendix C Firewall configuration: Default ports 228

Firewall configuration: Default ports 228

Appendix D CRON Expressions for Policy and Report Schedules 230

CRON expressions for policy probe schedules 230
CRON expressions for scheduling reports 232

Chapter 1

Introduction

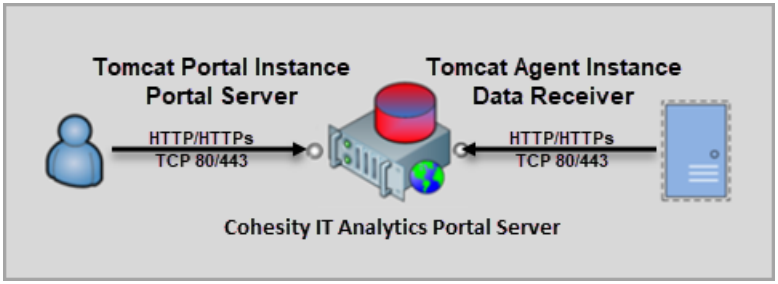
This chapter includes the following topics:

- Overview
- Distributed Data Collector (recommended for NetBackup)
- Centralized Data Collector
- Collection of backup and restore data
- Data Collection Policies

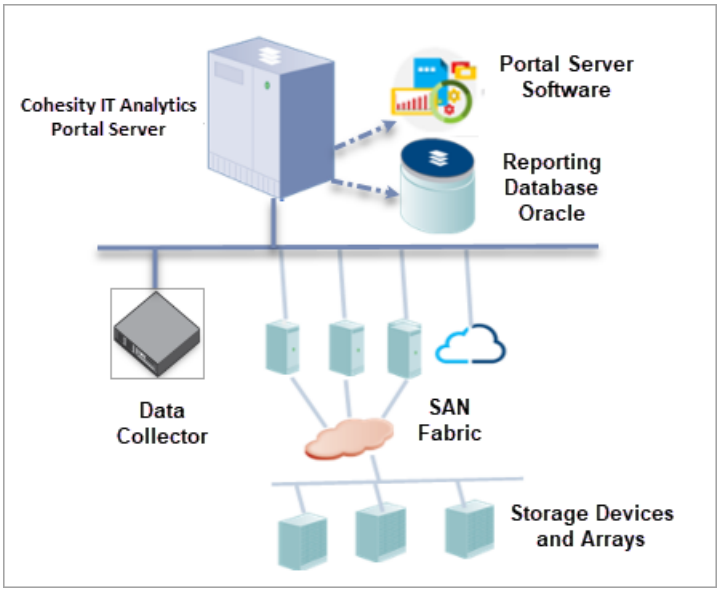
Overview

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

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



When you use the Portal to generate a report, the Portal requests this information from the Reporting Database, then returns the results in one of the many available reports. In addition to NetBackup, IT Analytics can collect data from Veritas Backup Exec, NetBackup Appliances and Flex, third-party Data Protection vendors, Storage Arrays, SAN Fabric, and Cloud assets.



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

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

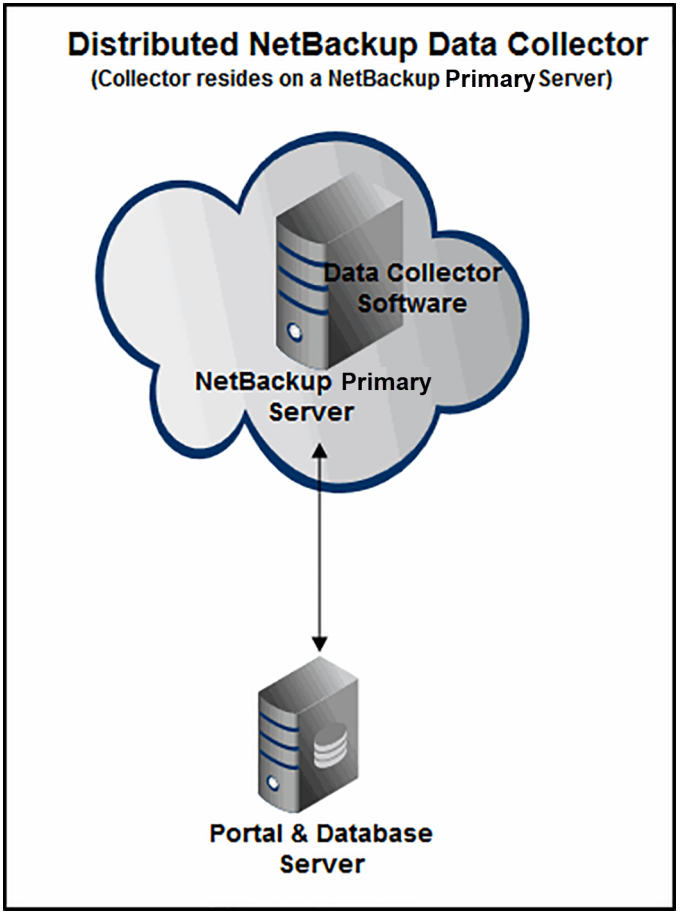
A centralized Data Collector can be used to collect data from all backup products. You can also include other enterprise objects, such as storage arrays, SAN switches, Compute and Cloud assets for a centralized Data Collector.

If you collect data from Veritas Backup Exec, third-party data protection vendors, storage arrays, SAN switches, and cloud assets, then choose a centralized Data Collector that is installed on a remote Linux or Windows Server. Please note that there can be situations where you would also use a centralized Data Collector to collect from NetBackup.

Distributed Data Collector (recommended for NetBackup)

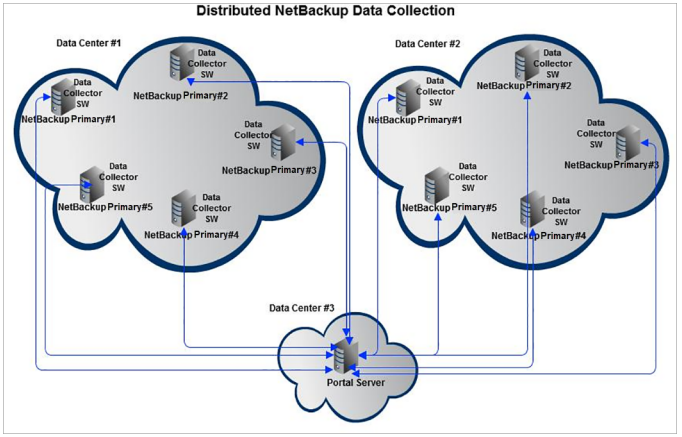
If collecting data from NetBackup, you can use a Distributed Data Collector, which is installed by default on a non-clustered NetBackup Primary Server. A Distributed Data Collector should ONLY be used to collect data from the NetBackup Primary Server and/or the appliance/Flex instance it resides on.

Figure 1-1 Example of a single primary server collection



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

Figure 1-2 Example of a multiple primary server collection



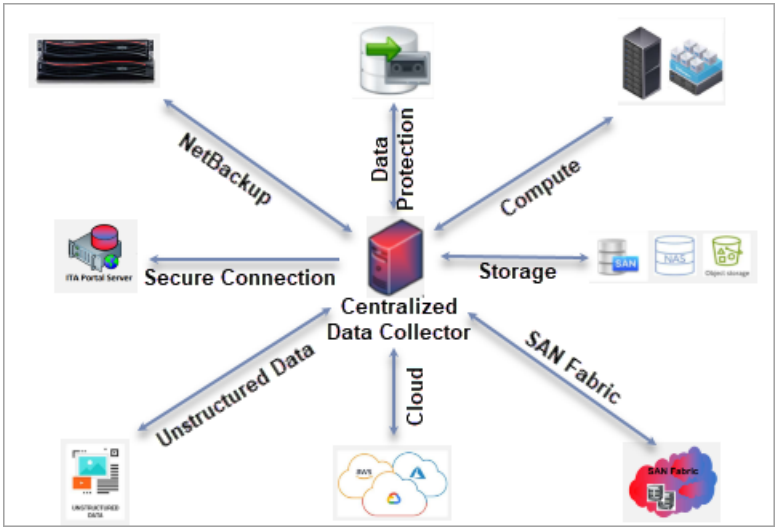
Centralized Data Collector

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

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

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

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



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

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

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

Collection of backup and restore data

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

Where you install the Data Collector also depends on the backup solution. For NetBackup 10.1.1 and later, a Data Collector is already pre-installed and embedded on the NetBackup Primary Server. Since the Data Collector is pre-installed, you simply need to configure and register the Data Collector, as its binaries are preinstalled.

Data Collection Policies

Data Collectors are configured with data collection policies. Which data collection policy to choose depends on what data you need to collect. Within IT Analytics, there are data collection policies for Storage, Data Protection, Network & Fabrics, Virtualization, File Analytics and Cloud. The types of data collection policies available to you also depends on the IT Analytics license that you have purchased.

The Cohesity NetBackup Data Collection Policy collects NetBackup-specific data regarding NetBackup backup policies, jobs, job successes, failures, etc., from NetBackup or Cohesity Alta Data Protection, whether the NetBackup Primary resides on a dedicated NetBackup server, a Flex Appliance, or a NetBackup Appliance.

To collect storage and capacity information specific to NetBackup Appliances or Flex, you can configure the Cohesity Flex Appliance or Cohesity NetBackup Appliance Data Collection Policy. A Distributed Data Collector is required for the Cohesity NetBackup Appliance data collection policy.

Chapter 2

Configure a IT Analytics Distributed Data Collector on a NetBackup Primary Server

This chapter includes the following topics:

- Overview
- Configure Data Collector on non-clustered NetBackup 10.4 and later primary server
- Configuration workflow for NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 on a non-clustered NetBackup primary server
- Configure Data Collector on non-clustered NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 primary server
- Configuration workflow for NetBackup versions lower than 10.1.1
- Configure Data Collector on NetBackup primary with version lower than 10.1.1

Overview

Starting with NetBackup 10.1.1 or later, IT Analytics Data Collector software comes preinstalled on non-clustered NetBackup primary servers. The Data Collector is installed during the installation or upgrade of the NetBackup primary server. Only the Data Collector binaries are deployed with NetBackup. The collector is not

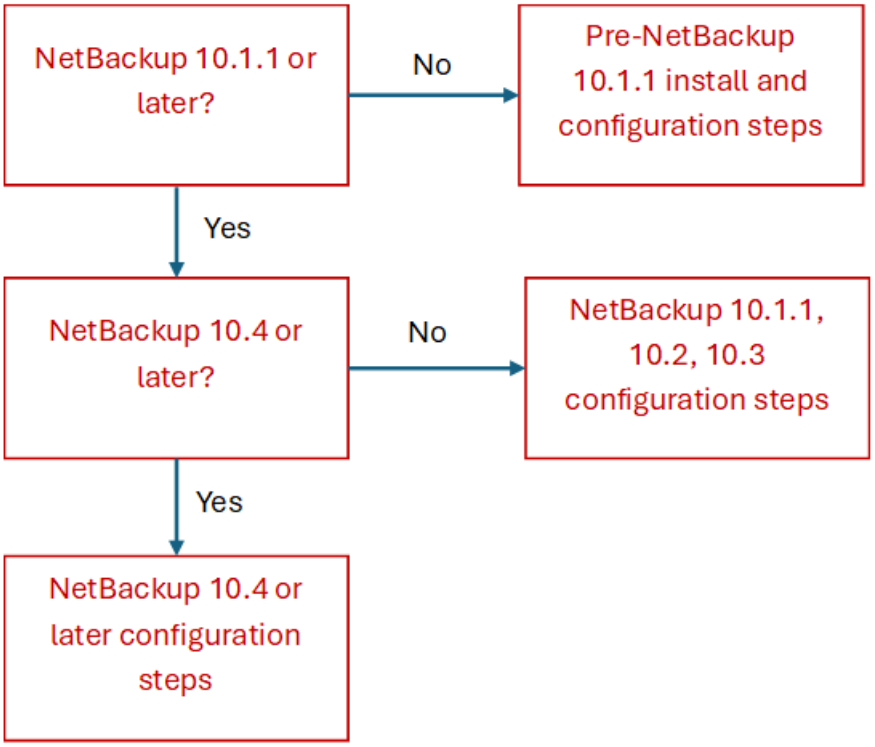
configured to communicate with the IT Analytics Portal as part of the NetBackup install. You must configure the Data Collector separately.

Clustered NetBackup Primaries do not have the Data Collector software installed by default, nor do NetBackup primaries with software versions prior to NetBackup 10.1.1. In these scenarios, you must install the Data Collector binaries.

If you have Veritas InfoScale Availability (VCS) or Microsoft Cluster Server (MSCS), you must review the later chapters of this guide as additional instructions and details about how to set up Data Collector software on a cluster, in addition to the steps below.

If you are running NetBackup 10.1.1 or later but have not yet upgraded to 10.4, the Data Collector binaries are preinstalled on the non-clustered NetBackup Primary, but you must manually register the Data Collector by configuring a response file. If you are on NetBackup 10.4 or later, then you can register the Data Collector directly within the NetBackup Web UI. Note that from NetBackup 10.4 onwards, Data Collector is optional to install. If you are planning to use IT Analytics or Alta View, you must opt to install Data Collector while installing/upgrading NetBackup.

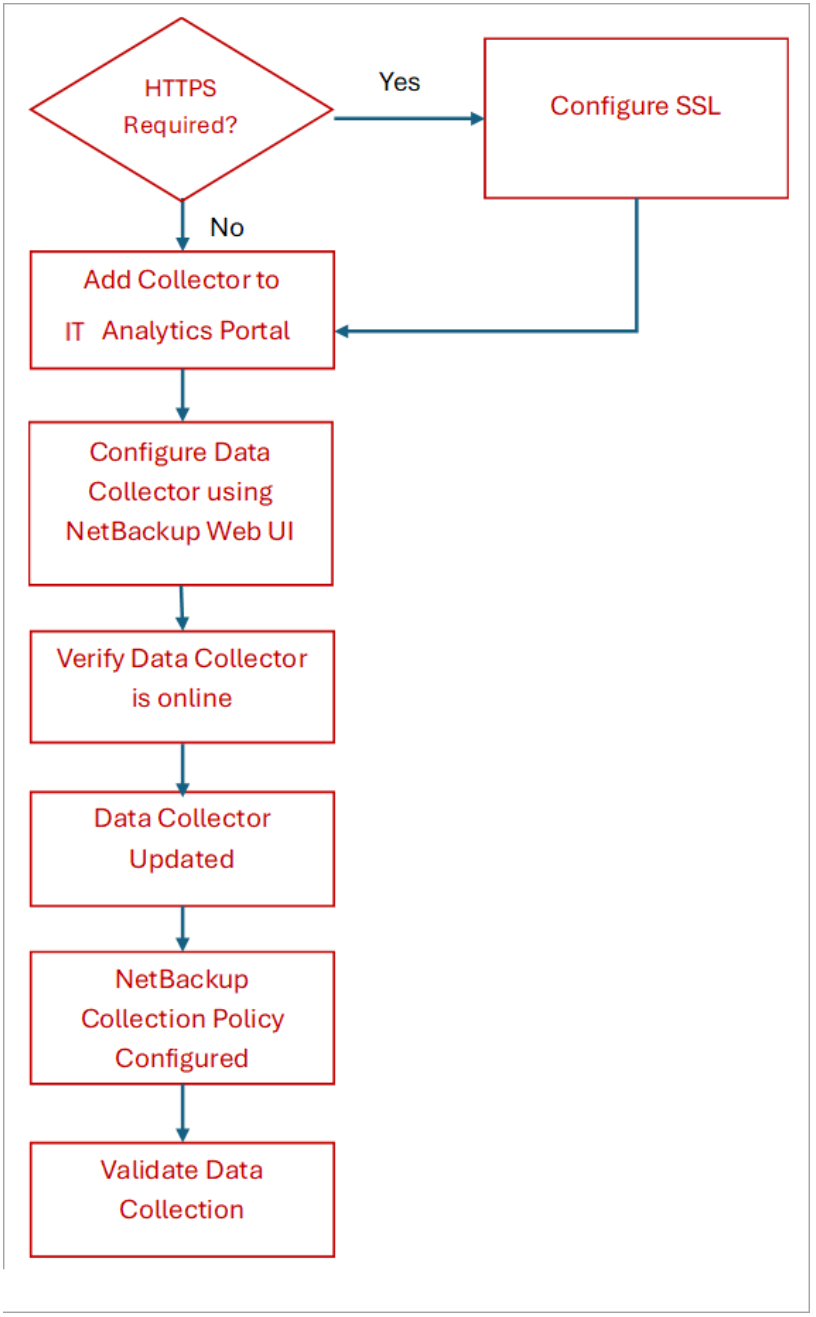
Follow the decision tree below to determine which section to follow and click on the associated hyperlinks below the flowchart to take you to that section.



- See "Configure Data Collector on NetBackup primary with version lower than 10.1.1" on page 41.
- See "Configure Data Collector on non-clustered NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 primary server" on page 26.
- See "Configure Data Collector on non-clustered NetBackup 10.4 and later primary server" on page 18.

Configure Data Collector on non-clustered NetBackup 10.4 and later primary server

This section assumes you are running NetBackup 10.4 or later, on a non-clustered NetBackup primary.


HTTPS Required?
Yes
Configure SSL
No
Add Collector to IT Analytics Portal
Configure Data Collector using NetBackup Web UI
Verify Data Collector is online
Data Collector Updated
NetBackup Collection Policy Configured
Validate Data Collection

Step-1: HTTPS requirement

The default IT Analytics configuration is HTTP Port 80 between the Data Collector and the Web Portal, and between the User's Web Browser to the IT Analytics Portal. If HTTP is not acceptable in your environment, you must configure HTTPS before proceeding. Once the Data Collection Policy configuration is complete, continue to Step-2: Add Data Collector in the IT Analytics Portal. If HTTP is acceptable, continue with Step-2: Add Data Collector in the IT Analytics Portal.

Step-2: Add Data Collector in the IT Analytics Portal

To add a Data Collector

1. Select **Admin** > **Data Collection** > **Collector Administration**. The list of currently configured Portal Data Collectors is displayed. If a Data Collector has already been created, rather than creating a new Data Collector, you may want to add your collection policies to an existing Data Collector.
2. Click **Add Collector**.

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

Although you can have any name for the Data Collector, it is recommended that the Data Collector name be the hostname of the NetBackup Primary Server. In the example below, the NetBackup Primary Server Name is used followed by "_DC" as an abbreviation for Data Collector. The **Enable SSL** checkbox is visible only if the IT Analytics Portal is configured for SSL.

Note: Copy the Data Receiver URL at the bottom of the **Add Collector** screen. The host name in this URL, executed on the NetBackup Primary, must resolve to the IT Analytics Portal Server's IP Address.

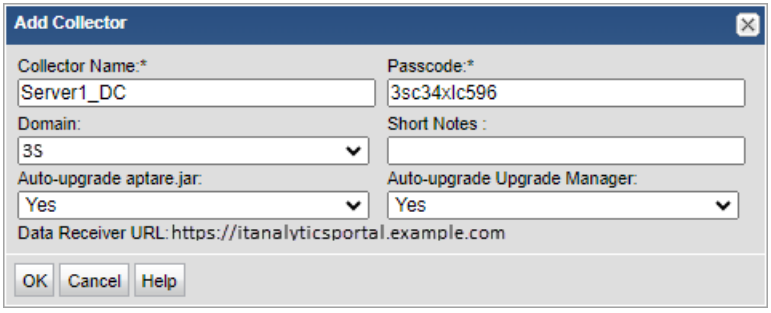


Table 2-1 Field description

Field	Description
Collector Name*	The collector name cannot include a space and is case sensitive. The names must match exactly as entered in the Data Collector configuration screen and the Data Collector Installer screen. Edit the unique name assigned to this Data Collector. The Data Collector will use this value for authentication purposes. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made.
Passcode*	Edit the passcode assigned to this Data Collector. It can be any character sequence. Unlike other system passwords (which are encrypted and then saved) this Data Collector passcode is not encrypted prior to saving in the database and may appear as clear case in certain files. It simply is intended as a “handshake” identification between the Data Collector and the policy. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made. You can use the following OS-specific special characters in the passcode. Make sure the special characters you include are supported on the OS where the Data Collector is installed. You can specify from one to 128 characters in your passcode. ■ Linux: !@#%^* ■ Windows: !@#$%^&*()
Short Notes	Descriptive notes associated with this Data Collector.

Table 2-1 Field description *(continued)*

Field	Description
Enable SSL	Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use. This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com
Auto-upgrade aptare.jar	Indicate if you want this configuration file upgraded automatically. This part of the Data Collector is responsible for event and metadata processing threads. The .jar file contains the processing and parsing logic for data collection. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.
Auto-upgrade Upgrade Manager	Indicate if you want this configuration bundle upgraded automatically. This Data Collector component is responsible for managing Data Collector upgrades. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

Click **OK**. You will now be presented with the following message, indicating that a .json file has been created. This file is required when you configure and register your data collector.

Click **OK**. Copy the .json file to the NetBackup Primary Server.

Step-3: Configure the Data Collector from the NetBackup Web UI

The Data Collector reports NetBackup information to IT Analytics or to Cohesity Alta View. The Data Collector is installed along with a NetBackup installation or upgrade.

For NetBackup 10.4 or higher, you can register their Data Collector directly from the NetBackup Web UI by adding a `.json` file.

To register the Data Collector from the NetBackup Web UI:

1. On the top right corner within the NetBackup Web UI, click the Cog icon and select **Data Collector Registration**.
2. Click **Register with Cohesity IT Analytics**.
3. Click **Choose file** to select the registration file (JSON) that you have created earlier.
4. If required, click the **Proxy server** option to specify Proxy server settings.
5. Click **Register**.

To validate the Data Collector communication with the Portal, go to `/usr/openv/analyticscollector/mbs/bin/` and run `./checkinstall.sh`. If the Data Collector is able to communicate with the IT Analytics Portal, the response is displayed as **SUCCESS**.

Note: The host name in data receiver URL, executed from the NetBackup Primary, must resolve to the Portal server's IP Address.

If the agent URL is is enabled with SSL and is created with self-signed certificate, ensure that you follow the steps in the *Test and troubleshoot SSL configurations*.

See "Test and troubleshoot SSL configurations" on page 105.

Step-4: Verify the Data Collector is online from the portal

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

Step-5: Confirm the Data collector is updated

On the IT Analytics Portal, go to **Admin** > **Data Collection** > **Collector Updates** and select the Data Collector for which the component needs to be upgraded. Version must match the required versions and there should be no version displayed in red text.

Step-6: Configure the data collection policy

Please refer to *Chapter 3: Configuring NetBackup Collection Policies*. Once the Data Collection Policy configuration is complete, continue to *Step-7*.

See "*Installing the Data Collector software*" on page 72.

Step-7: Confirm that the NetBackup data collection policy is collecting data

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

Manage Data Collector installation on NetBackup primary server

You may need to manually install the Data Collector if it fails to install during the NetBackup install or upgrade. A failure to install the Data Collector does not cause the entire NetBackup primary server installation or upgrade to fail. The steps shown do not configure the Data Collector to connect with any portal. These steps only install the Data Collector.

Install the Data Collector on NetBackup primary server

To manually install the Data Collector on a Linux primary server:

1. Extract the installer from `/usr/openv/ita_dc.tar.gz` to a temporary location.

   The default Data Collector installer archive path is `/usr/openv/ita_dc.tar.gz` if you have opted not to install Data Collector while installing NetBackup.

2. Run:

   ```
   <temporary_location>/dc_installer -i /usr/openv -n
   ```

To manually install the Data Collector on a Windows primary server:

1. Locate the installation media kit and navigate to the `x64/ITA_DC` folder.
2. Run:

   ```
   silentinstall.cmd /INSTALL_PATH:NetBackup_install_path
   /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y
   ```

Uninstall Data Collector from NetBackup primary

To manually uninstall the Data Collector from a Linux primary server, run:

```
/usr/openv/analyticscollector/UninstallerData/uninstall_dc.sh -r
```

On Windows

To manually uninstall the Data Collector from a Windows primary server:

1. In Windows Programs and Features, locate IT Analytics Data Collector.
2. Select and right-click on IT Analytics Data Collector and select **Uninstall**.

You can also use a uninstall script:

```
C:\ProgramData\Cohesity\IT Analytics\DC\silentuninstall.cmd
```

Configuration workflow for NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 on a non-clustered NetBackup primary server

This configuration assumes you are running NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 on a non-clustered NetBackup primary.

Configure Data Collector on non-clustered NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 primary server

Step-1: HTTPS requirement

The default IT Analytics configuration is HTTP Port 80 between the Data Collector and the Portal and between the User's Web Browser to the IT Analytics Web Portal. If HTTPS is required, then follow the steps detailed in *Chapter 5: Configure SSL*. Once SSL is set up, continue with Step-2: Add Data Collector in the IT Analytics Portal. Alternatively, if you are just configuring with HTTP, continue with Step-2: Add Data Collector in the IT Analytics Portal.

See "*Configure SSL*" on page 96.

Step-2: Add Data Collector in the IT Analytics Portal

Once logged in to the Portal:

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

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

Although you can have any name for the Data Collector, it is recommended that the Data Collector name be the hostname of the NetBackup primary server. In the example below, the NetBackup primary server name is used followed by "_DC" as an abbreviation for Data Collector.

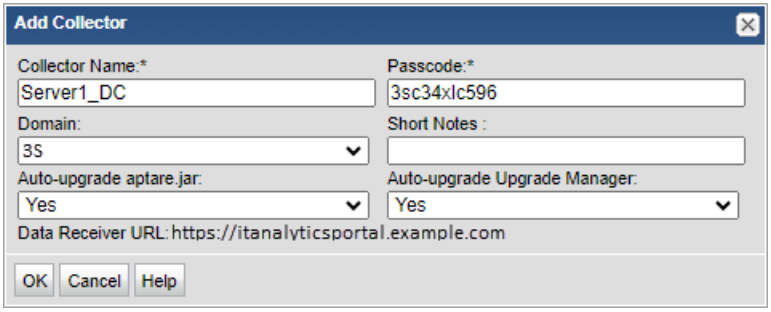


Table 2-2 Field description

Field	Description
Collector Name*	The collector name cannot include a space and is case sensitive. The names should match exactly as entered in the Data Collector configuration screen and the Data Collector Installer screen. Edit the unique name assigned to this Data Collector. The Data Collector will use this value for authentication purposes. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made.
Passcode*	Edit the passcode assigned to this Data Collector. It can be any character sequence. Unlike other system passwords (which are encrypted and then saved) this Data Collector passcode is not encrypted prior to saving in the database and may appear as clear case in certain files. It simply is intended as a “handshake” identification between the Data Collector and the policy. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made. You can use the following OS-specific special characters in the passcode. Make sure the special characters you include are supported on the OS where the Data Collector is installed. You can specify from one to 128 characters in your passcode. ■ Linux: !@#%^* ■ Windows: !@#$%^&*()
Short Notes	Descriptive notes associated with this Data Collector.

Table 2-2 Field description *(continued)*

Field	Description
Enable SSL	Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use. This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com
Auto-upgrade aptare.jar	Indicate if you want this configuration file upgraded automatically. This part of the Data Collector is responsible for event and metadata processing threads. The .jar file contains the processing and parsing logic for data collection. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.
Auto-upgrade Upgrade Manager	Indicate if you want this configuration bundle upgraded automatically. This Data Collector component is responsible for managing Data Collector upgrades. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

Click **OK**. You will now be presented with the following message, indicating that a .json file has been created. This file is required when you configure and register your data collector.

Click **OK**.

Some older NetBackup releases came bundled with IT Analytics Data Collector software that leveraged a `.key` file rather than a `.json` file. The configuration steps are slightly different depending on the file type required to configure the Data Collector. Listed below is a table that shows what versions of the IT Analytics Data Collector binaries are installed on which versions of NetBackup. This table is also applicable to NetBackup Appliances and Flex Appliances. By checking the NetBackup version installed on the appliance, you can determine whether to use a `.key` or a `.json` file, when configuring the Data Collector.

Table 2-3 Reference for `.key` and `.json` usage

NetBackup version	IT Analytics Data Collector version installed on NetBackup	.key or .json file to be used
10.1.1	11.1.50	.key
10.2	11.2.00	.key
10.2.0.1	11.2.00	.key
10.3	11.2.05	.key
10.3.0.1	11.2.05	.key
10.4	11.3.02	.json
10.4.0.1 (or later)	11.3.04 (or later)	.json
10.5	11.4.03	.json
11.0	11.5.04 (or later)	.json

To download the `.key` file:

1. Login to the Portal and go to **Admin** > **Collector Administration**.
2. Select the Data Collector you just created, as described in Step-2: Add Data Collector in the IT Analytics Portal.
3. Click **Edit**.
4. Select **Key File**.
5. Note the following information:
   - Name of the Data Collector (as it appears on the Portal)
   - Passcode of the Data Collector (as configured on the Portal)
   - Data receiver URL (generated while creating the Data Collector on the Portal)

Note: The host name in data receiver URL, executed from the NetBackup primary, must resolve to the Portal server's IP address.

6 Click **Generate**.

Following message, which indicates that a `.key` file has been created is displayed. This file is required when you configure and register all Data Collector versions of 11.2 and earlier.

7 Note the `.key` file path.

If your Data Collector version is 11.3 or higher, you must download the `.json` file from the Portal.

The `.key` or the `.json` file needs to be downloaded and copied to the NetBackup primary server, when you manually configure the Data Collector.

- For a NetBackup Server, proceed to Step 2A: Configure the IT Analytics Data Collector manually for NetBackup .
- For a NetBackup Appliance or NetBackup Flex Appliance proceed to Step-2B: Configure Data Collector for NetBackup Appliances (including Flex appliance).

Step 2A: Configure the IT Analytics Data Collector manually for NetBackup

This section details the steps required to manually configure the Data Collector using a `.key` file. This configuration requires editing a response file to configure the distributed Data Collector, installed by default on the non-clustered NetBackup primary. The Cohesity NetBackup primary server installation will deploy IT Analytics Data Collector binaries automatically on Windows (`C:\Program Files\Veritas\AnalyticsCollector`) and Linux (`/usr/openv/analyticscollector`).

The 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.

See the section called “Step-2: Add Data Collector in the IT Analytics Portal” on page 26.

To configure the Data Collector manually on Windows using `.key` file:

1. Create a response file as a batch script `responsefile.cmd` with the contents shown. These are the responses to the user input required to configure the Data Collector. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.

```
SET DATACOLLECTOR_NAME=name_of_the_data_collector
SET DATACOLLECTOR_PASSCODE=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=
```

   To configure the Data Collector manually on Windows using `.json` file, create the below batch script. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.

```
SET DATACOLLECTOR_REGISTRATION_FILE_PATH=path of .json
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=
```

2. Update the value for each field with appropriate data.
3. Run the command shown:

```
"C:\ProgramData\Veritas\NetBackup IT Analytics\DC\configure.cmd"


\RESPFILE:response_file_path \INSTALL_TYPE:CONFIG
```

4 Validate the Data Collector integration with IT Analytics by going to `C:\Program Files\Veritas\analyticscollector\mbs\bin\` and running this command: `checkinstall.bat`.

If the Data Collector is configured with the Portal, the response is displayed as **SUCCESS**.

Note: The host name in Data receiver URL, executed from the NetBackup Primary, must resolve to the Portal server's IP address.

To configure the Data Collector manually on Linux using `.key` file:

1. Create a response file with the contents shown. A sample response file is available on the install media and from `/usr/openv/analyticscollector/installer/responsefile.sample` on the primary server. These are the responses to the user input required to configure the Data Collector:

```
COLLECTOR_NAME=name_of_the_data_collector
COLLECTOR_PASSCODE=passcode_for_the_data_collector
DR_URL=data_receiver_URL
COLLECTOR_KEY_PATH=path_to_the_key_file
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

   To configure the Data Collector manually on Linux using `.json` file, create a responsefile as below. A sample response file is available on the install media and from `/usr/openv/analyticscollector/installer/responsefile.sample` on the primary server.

```
COLLECTOR_REGISTRATION_PATH=<path-to-registration-file-downloaded-from-portal-including-filename>
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.
3. Run the command:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
responsefile_path
```

4 Validate the Data Collector integration with IT Analytics by navigating to `/usr/openv/analyticscollector/mbs/bin/ and running ./checkinstall.sh`. If the Data Collector is able to communicate with the IT Analytics Portal, the response is displayed as **SUCCESS**.

Note: The host name in data receiver URL, executed from the NetBackup Primary, must resolve to the Portal server's IP address.

Step-2B: Configure Data Collector for NetBackup Appliances (including Flex appliance)

You can configure a Data Collector on the primary server pod using the following steps. From NetBackup version 10.3 Cloud Scale release, Data Collector on primary server pod is supported. The below steps to configure the Data Collector on a primary server must be performed as a root user. On a Flex appliance, connect to the primary server pod first and then switch to the root user using `sudo`. On a NetBackup Appliance, access shell by creating NetBackup CLI user.

To configure IT Analytics for NetBackup deployment:

1 Create a DNS server entry in such a way that IP of the Portal must be resolvable to a single FQDN. IP of the IT Analytics Portal must be resolved to:

`itanalyticsagent.<yourdomain>`

Note the following:

- If the Portal URL is `itanalyticsportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `itanalyticsagent.<yourdomain>`
- If the Portal URL is `aptareportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `aptareagent.<yourdomain>`

The above default values are based on the initial IT Analytics Portal version installed.

2 Depending upon the Data Collector version, collect the `<your-collector-name>.key` or `<your-collector-name>.json` file for the new Data Collector by accessing the Portal link and creating a collector. Copy it to the host machine from where NetBackup primary is deployed.

For more information, refer to *Data Collector Encryption* section in *IT Analytics User Guide*.

3. Create a new folder `analyticscollector` at persisted location (for example, `/mnt/nbdata/`) using the following commands:

   ```
   cd "/mnt/nbdata/"
   mkdir analyticscollector
   ```

4. Copy `<your-collector-name>.key` or `<your-collector-name>.json` file to `/mnt/nbdata/analyticscollector` inside the NetBackup primary host or container.
5. In case the data-receiver is configured with self-signed certificate (https), user must add the certificate in the Data Collector.

   See *Configure the Data Collector to trust the certificate* section in the *IT Analytics Administrator Guide*.
6. Connect to the NetBackup primary host or the container.
7. Navigate to `/usr/openv/analyticscollector/installer/` location and perform the following.

   - Open the `responsefile.sample` and add the following parameters:
     If the Data Collector is lower than 11.3, create the response file with the following contents.

     ```
     COLLECTOR_NAME=<your-collector-name>
     COLLECTOR_PASSCODE=<your-password>
     DR_URL=<http>/<https>://itanalyticsagent.<yourdomain>
     COLLECTOR_KEY_PATH=<path to your-collector-name.key>
     HTTP_PROXY_CONF=N
     HTTP_PROXY_ADDRESS=
     HTTP_PROXY_PORT=
     HTTPS_PROXY_ADDRESS=
     HTTPS_PROXY_PORT=
     PROXY_USERNAME=
     PROXY_PASSWORD=
     PROXY_EXCLUDE=
     ```

     If the Data Collector version is 11.3 or later, create the response file with the following contents.

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

```
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

8 Configure the Data Collector with the IT Analytics Portal as follows.

Note: If the Data Collector installed is of a lower version than the Portal, wait for the Data Collector auto-upgrade to finish before you proceed.

For NetBackup Appliance version 5.3 or later:

- Run the following command as a NetBackup CLI user:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
/usr/openv/analyticscollector/installer/responsefile.sample
```

- To verify the Data Collector integration with IT Analytics Portal, run:

```
/usr/openv/analyticscollector/mbs/bin/checkinstall.sh
```

For NetBackup Appliance version 5.1.1:

- Run the following command as a NetBackup CLI user:

```
sudo /usr/openv/analyticscollector/installer/dc_installer.sh
-c /usr/openv/analyticscollector/installer/responsefile.sample
```

- To verify the Data Collector integration with IT Analytics Portal, run:

```
sudo /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
```

If you are on Flex Appliance:

- Connect to the primary server container and then switch to root user using `sudo` and run:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
/usr/openv/analyticscollector/installer/responsefile.sample
```

- To verify the Data Collector integration with IT Analytics Portal, run:

```
/usr/openv/analyticscollector/mbs/bin/checkinstall.sh
```

If the Data Collector is configured with the Portal, it will display **SUCCESS**.

Note: If there is a version mismatch of `aptare.jar` between Data Collector and Portal, execution of `checkinstall.sh` command will trigger an auto-update of the Data Collector. If the Data Collector can communicate with the IT Analytics Portal, the response is shown as **SUCCESS**.

9 Check the Data Collector services status by running the following command and ensure that the following Data Collector services are up and running:

```
/usr/openv/analyticscollector/mbs/bin/aptare_agent status
```

Output of the above command:

```
IT Analytics Zookeeper Server is running (pid: 16137).
IT Analytics Kafka Server is running (pid: 16145).
IT Analytics WatchDog is running (pid: 7225).
IT Analytics MetaDataCollector is stopped.
IT Analytics EventDataCollector is stopped.
IT Analytics DataCollector process is running (pid: 7365).
IT Analytics On-demand process is running (pid: 7361).
IT Analytics Message Relay Server process is running (pid: 7366).
```

For more information about the Data Collector policy, see *IT Analytics User Guide*.

Step-3: Verify the collector is online from the portal

1 Login to the IT Analytics Portal.

2 Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector is **Online**.

Step-4: Confirm the Data collector is updated

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

Step-5: Configure the data collection policy

Please refer to *Chapter 3: Configure a Veritas NetBackup Data Collector Policy* . Once the Data Collection Policy configuration is complete, continue to *Step-8*.

See "*Configure a Veritas NetBackup Data Collector Policy*" on page 51.

Step-6: Confirm that the NetBackup data collection policy is collecting data

Select **Collector Administration** and confirm that the **Policy State** column is showing **Collecting**, for the Veritas NetBackup collection policy, or has a green

check mark under the **Status** column, indicating a successful collection. Note that you may need to Refresh the screen for several minutes.

Manage Data Collector installation on NetBackup (install/remove)

You may need to manually install the Data Collector if it fails to install during the NetBackup install or upgrade. A failure to install the Data Collector does not cause the entire NetBackup primary server installation or upgrade to fail. The steps shown do not configure the Data Collector to connect with any portal. These steps only install the Data Collector.

Install

To manually install the Data Collector on a Linux primary server:

1. Extract the installer from `/usr/openv/ita_dc.tar.gz` to a temporary location.

   The default Data Collector installer archive path is `/usr/openv/ita_dc.tar.gz` if you have opted not to install Data Collector while installing NetBackup.

2. Run:

   ```
   <temporary_location>/dc_installer -i /usr/openv -n
   ```

To manually install the Data Collector on a Windows primary server:

1. Locate the installation media kit and navigate to the `x64/ITA_DC` folder.
2. Run:

   ```
   silentinstall.cmd /INSTALL_PATH:NetBackup_install_path
   /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y
   ```

Uninstall

To manually uninstall the Data Collector from a Linux primary server, run:

```
/usr/openv/analyticscollector/UninstallerData/uninstall_dc.sh -r
```

To manually uninstall the Data Collector from a Windows primary server:

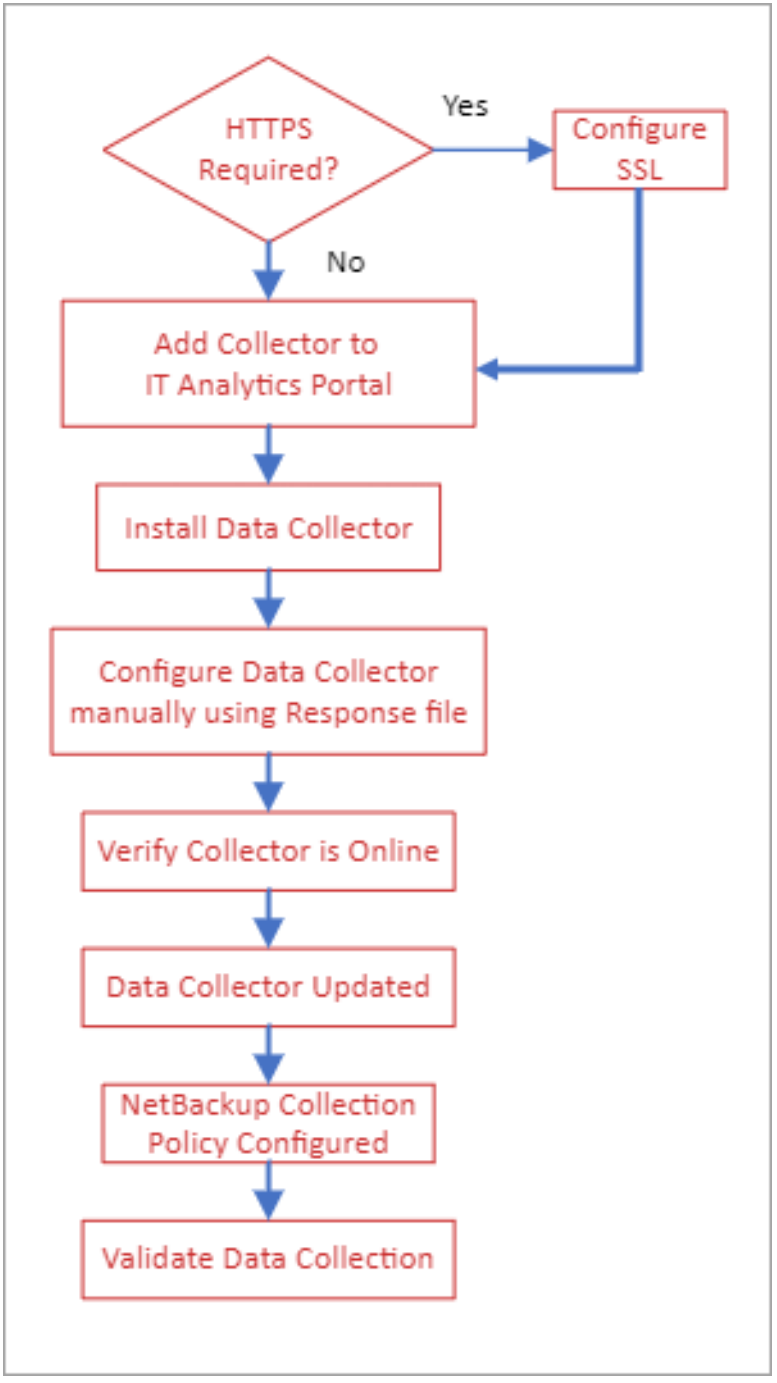
1. In Windows Programs and Features, locate IT Analytics Data Collector.
2. Select and right-click on IT Analytics Data Collector and select **Uninstall**.

You can also use a uninstall script:

```
C:\ProgramData\Cohesity\IT Analytics\DC\silentuninstall.cmd
```

Configuration workflow for NetBackup versions lower than 10.1.1

This configuration assumes that you are running a NetBackup version lower than 10.1.1.


HTTPS Required?
Yes
Configure SSL
No
Add Collector to IT Analytics Portal
Install Data Collector
Configure Data Collector manually using Response file
Verify Collector is Online
Data Collector Updated
NetBackup Collection Policy Configured
Validate Data Collection

Configure Data Collector on NetBackup primary with version lower than 10.1.1

Step-1: HTTPS requirement

The default IT Analytics configuration is HTTP Port 80 between the Data Collector and the Portal and between the User's Web Browser to the Portal. If HTTP is not acceptable in your environment, you will need to configure HTTPS before proceeding. Once the Data Collection policy configuration is complete, continue to Step-2: Add Data Collector on IT Analytics Portal.

If HTTP is acceptable, you can also configure SSL at the end of the configuration process once you have completed the remaining steps.

Step-2: Add Data Collector on IT Analytics Portal

Once logged in to the Portal:

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

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

Although you can have any name for the Data Collector, it is recommended that the Data Collector name be the hostname of the NetBackup primary server. In the example below, the NetBackup primary server name is used followed by "_DC" as an abbreviation for Data Collector.

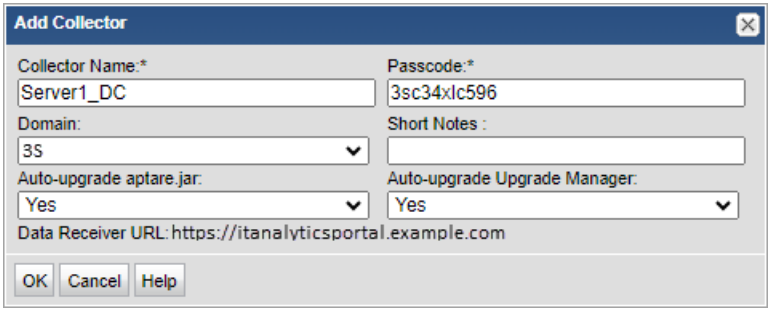


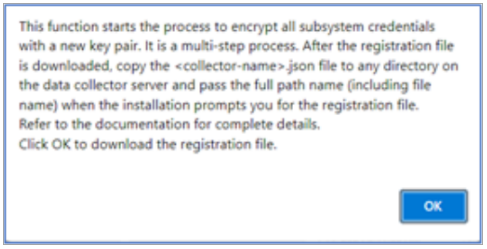
Table 2-4 Field description

Field	Description
Collector Name*	The collector name cannot include a space and is case sensitive. The names should match exactly as entered in the Data Collector configuration screen and the Data Collector Installer screen. Edit the unique name assigned to this Data Collector. The Data Collector will use this value for authentication purposes. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made.
Passcode*	Edit the passcode assigned to this Data Collector. It can be any character sequence. Unlike other system passwords (which are encrypted and then saved) this Data Collector passcode is not encrypted prior to saving in the database and may appear as clear case in certain files. It simply is intended as a “handshake” identification between the Data Collector and the policy. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made. You can use the following OS-specific special characters in the passcode. Make sure the special characters you include are supported on the OS where the Data Collector is installed. You can specify from one to 128 characters in your passcode. ■ Linux: !@#%^* ■ Windows: !@#$%^&*()
Short Notes	Descriptive notes associated with this Data Collector.

Table 2-4 Field description *(continued)*

Field	Description
Enable SSL	Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use. This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com
Auto-upgrade aptare.jar	Indicate if you want this configuration file upgraded automatically. This part of the Data Collector is responsible for event and metadata processing threads. The .jar file contains the processing and parsing logic for data collection. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.
Auto-upgrade Upgrade Manager	Indicate if you want this configuration bundle upgraded automatically. This Data Collector component is responsible for managing Data Collector upgrades. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

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



Click **OK**. Get the `.json` file path.

Download the `.json` file and copy it to the NetBackup primary server when you configure the Data Collector.

Step-3: Install the Data Collector

Refer *Chapter 4: Installing Data Collector Software*. This section assumes that you will install a IT Analytics Data Collector 11.4 or greater, which will allow you to register the data collector using a `.json` file. When complete, resume at *Step 4*.

Chapter 4

Step-4: Configure the Data Collector

If configuring the Data Collector for a non-clustered NetBackup primary running a NetBackup version earlier than 10.1.1, configure the Data Collector manually using a response file.

- For a NetBackup server, proceed to Step-4A: Configure the IT Analytics Data Collector manually for NetBackup.
- For NetBackup Appliances or NetBackup Flex Appliances proceed to Step-4B: Configure Data Collector for NetBackup Appliances (including Flex appliance).

Step-4A: Configure the IT Analytics Data Collector manually for NetBackup

This section details the steps required to manually configure the Data Collector using a `.key` file. This configuration requires editing a response file to configure the distributed Data Collector, installed by default on the non-clustered NetBackup primary. The Cohesity NetBackup primary server installation will deploy IT Analytics Data Collector binaries automatically on Windows (`C:\Program Files\Veritas\AnalyticsCollector`) and Linux (`/usr/openv/analyticscollector`).

The 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. See Step-2: Add Data Collector on IT Analytics Portal.

To configure the Data Collector manually on Windows:

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

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

2. Update the value for each field with appropriate data. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.

3. Run the command shown:

```
"C:\ProgramData\Veritas\NetBackup IT Analytics\DC\configure.cmd"

\RESPFILE:response_file_path \INSTALL_TYPE:CONFIG
```

4. Validate the Data Collector integration with IT Analytics by going to `C:\Program Files\Veritas\analyticscollector\mbs\bin\` and running this command: `checkinstall.bat`.

   If the Data Collector is configured with the Portal, the response is displayed as **SUCCESS**.

Note: The host name in Data receiver URL, executed from the NetBackup Primary, must resolve to the Portal server's IP address.

To configure the Data Collector manually on Linux using key file:

1. Create a response file with the contents shown. These are the responses to the user input required to configure the Data Collector.

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

   A sample response file is available on the install media and from `/usr/openv/analyticscollector/installer/responsefile.sample` on the primary server.

2. Update the value for each field with appropriate data.

3. Run the command:

   ```
   /usr/openv/analyticscollector/installer/dc_installer.sh -c
   responsefile_path
   ```

4. Validate the Data Collector integration with IT Analytics by navigating to `/usr/openv/analyticscollector/mbs/bin/ and running ./checkinstall.sh`. If the Data Collector is able to communicate with the IT Analytics Portal, the response is displayed as **SUCCESS**.

Note: The host name in data receiver URL, executed from the NetBackup Primary, must resolve to the Portal server's IP address.

Step-4B: Configure Data Collector for NetBackup Appliances (including Flex appliance)

You can configure a Data Collector on the primary server pod using the following steps: From NetBackup version 10.3 Cloud Scale release, Data Collector on primary server pod is supported. The below steps to configure the Data Collector on a primary server must be performed as a root user. On a Flex appliance, connect to the primary server pod first and then switch to the root user using sudo. On a NetBackup Appliance, access shell by creating NetBackup CLI user.

To configure IT Analytics for NetBackup deployment:

1. Create a DNS server entry in such a way that IP of the Portal must be resolvable to a single FQDN. IP of the IT Analytics Portal must be resolved to:

   `itanalyticsagent.<yourdomain>`

   Note the following:

   - If the Portal URL is `itanalyticsportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `itanalyticsagent.<yourdomain>`
   - If the Portal URL is `aptareportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `aptareagent.<yourdomain>`

2. Collect the `<your-collector-name>.key` for the new Data Collector by accessing the Portal link and creating a collector and copy it to the host machine from where NetBackup primary is deployed.

3. Collect the `<your-collector-name>.json` file for the new Data Collector by accessing the Portal link and creating a collector and copy it to the host machine from where NetBackup primary is deployed.

   For more information, refer to the *Data Collector Encryption* section in *IT Analytics User Guide*.

4. Create a new folder `analyticscollector` at persisted location (for example, `/mnt/nbdata/`) using the following commands:

   ```
   cd "/mnt/nbdata/"
   mkdir analyticscollector
   ```

5. Copy `<your-collector-name>.key` or `<your-collector-name>.json` file to `/mnt/nbdata/analyticscollector` inside the NetBackup primary host or container.

6. In case the data-receiver is configured with self-signed certificate (https). User must add the certificate in the data collector.

   See *Configure the Data Collector to trust the certificate* section in the *IT Analytics Administrator Guide*.

7. Connect to the NetBackup primary host or the container.

8. Navigate to `/usr/openv/analyticscollector/installer/` location and perform the following.

   - Open the `responsefile.sample` and add the following parameters:

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

9 Configure the Data Collector with the IT Analytics Portal as follows.

Note: If the Data Collector installed is of a lower version than the Portal, wait for the Data Collector auto-upgrade to finish before you proceed.

For NetBackup Appliance version 5.3 or later:

- Run the following command as a NetBackup CLI user:

  ```
  /usr/openv/analyticscollector/installer/dc_installer.sh -c
  /usr/openv/analyticscollector/installer/responsefile.sample
  ```

- To verify the Data Collector integration with IT Analytics Portal, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
  ```

For NetBackup Appliance version 5.1.1:

- Run the following command as a NetBackup CLI user:

  ```
  sudo /usr/openv/analyticscollector/installer/dc_installer.sh
  -c /usr/openv/analyticscollector/installer/responsefile.sample
  ```

- To verify the Data Collector integration with IT Analytics Portal, run:

  ```
  sudo /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
  ```

If you are on Flex Appliance:

- Connect to the primary server container and then switch to root user using `sudo` and run:

  ```
  /usr/openv/analyticscollector/installer/dc_installer.sh -c
  /usr/openv/analyticscollector/installer/responsefile.sample
  ```

- To verify the Data Collector integration with IT Analytics Portal, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
  ```

If the Data Collector is configured with the Portal, it will display **SUCCESS**.

Note: If there is a version mismatch of `aptare.jar` between Data Collector and Portal, execution of `checkinstall.sh` command will trigger an auto-update of the Data Collector.

---

10 Check the Data Collector services status by running the following command and ensure that the following Data Collector services are up and running:

```
/usr/openv/analyticscollector/mbs/bin/aptare_agent status
```

Output of the above command:

```
IT Analytics Zookeeper Server is running (pid: 16137).
IT Analytics Kafka Server is running (pid: 16145).
IT Analytics WatchDog is running (pid: 7225).
IT Analytics MetaDataCollector is stopped.
IT Analytics EventDataCollector is stopped.
IT Analytics DataCollector process is running (pid: 7365).
IT Analytics On-demand process is running (pid: 7361).
IT Analytics Message Relay Server process is running (pid: 7366)
```

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

1 Login to the IT Analytics Portal.

2 Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector is **Online**.

Step-6: Confirm that the Data Collector is updated

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

Step-7: Configure the data collection policy

Refer to *Chapter 3: Configuring NetBackup Collection Policies* . Once the Data Collection Policy configuration is complete, continue to *Step 8*.

Chapter 3

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

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

Chapter 3

Configure a Veritas NetBackup Data Collector Policy

This chapter includes the following topics:

- Veritas NetBackup Data Collector policy configuration prerequisites
- Prerequisites for collection from Cohesity NetBackup deployed on Kubernetes clusters
- Create NetBackup Data Collector Role, Service Account, and API Key
- Add a Veritas NetBackup Data Collector policy
- Add/Edit NetBackup Primary Servers within the Data Collector policy
- Configuring file analytics in NetBackup Data Collector policy

Veritas NetBackup Data Collector policy configuration prerequisites

Prerequisites

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

- Data Collector added on the IT Analytics Portal. 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, see the *Chapter 6: Centralized Data Collector for NetBackup Prerequisites, Installation and Configuration*.
Chapter 6

- 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.

Note: After modifications of the access rights, RBAC user must run `bpnbat -login -loginType WEB` command as non-root user.

See "Create NetBackup Data Collector Role, Service Account, and API Key " on page 53.

See "Add a Veritas NetBackup Data Collector policy" on page 55.

Prerequisites for collection from Cohesity NetBackup deployed on Kubernetes clusters

This section describes the portal configurations required, before adding a Cohesity NetBackup policy, when Cohesity NetBackup is deployed on Kubernetes clusters in the cloud and it is using the cloud resources to perform backups.

SSH key-based authentication

Since Cohesity NetBackup is deployed on Kubernetes clusters, 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 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 Cohesity NetBackup API key

This API key is required when you add or edit a Cohesity NetBackup primary server for the Cohesity NetBackup policy configuration. This API key is essential especially when IT Analytics has to collect metrics from NetBackup deployed on Kubernetes clusters 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.

Create NetBackup Data Collector Role, Service Account, and API Key

A Data Collector Service Account and API key is used while configuring the Cohesity NetBackup Data Collector policy. This must be configured to enable complete collection from NetBackup. Create a Data Collector Service Account and add an RBAC custom role in the NetBackup Web UI. 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 the NetBackup Web UI RBAC screen with the following permissions and attach the role to a service account.

Custom role

To create the custom role within the NetBackup Web UI:

1. On the left, click **Security** > **RBAC**.
2. Under the **Roles** tab, click **Add**.
3. Select **Custom role** and click **Next**.
4. Enter the **Role Name** and **Role Description**.
5. Under **Permissions**, click **Assign**.
   - Select all the **View** permissions for all the objects under **NetBackup Management**, **Protection**, and **Storage** sections of the NetBackup web UI.
   - From the **NetBackup Management** > **CLI Sessions** section, enable **CLI Execute**.
   - From the **NetBackup Management** > **Malware** section, enable **View scan results**.
   - From the **RBAC** > (**Edit RBAC customs role**) > **Global Permission** tab > **Security** > enable **View** permission for **Global Security Settings**.
   - From the **RBAC** > (**Edit RBAC customs role**) > **Global Permission** tab > **Security** > enable **View** permission for **Security Events**.
6. Select **Users** tab and **Add to List** service account to be associated with this role.

API key

Copy the API key generated with these steps for future use. It will be required while configuring the NetBackup Collection Policy.

To add an API key:

1. Select **Security** > **Access keys** on the NetBackup Web UI.
2. Enter the **Username** and **Description**.

   The service account associated with the API key and the Role, must be the same service account that is associated with the Veritas NetBackup Collection Policy in IT Analytics.
3. Click **ADD**.

If you are configuring a Centralized Data Collector with SSH access to the NetBackup primary, then you must create a second user in addition to the account

created in the steps above. This second user must be an OS user with an identical username, same as the account you just created. See the section *Linux Centralized Data Collector: SSH* for instructions on how to create the second account.

See "Linux Centralized Data Collector: SSH" on page 125.

Add a Veritas NetBackup Data Collector policy

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 field descriptions under policy parameters below and then click **OK** to save the policy. Mandatory parameters are denoted by an asterisk (*).

   When configuring the Veritas NetBackup Data Collection policy, select the appropriate **Collection Method**, depending on whether your Data Collector is Distributed or Centralized.

   - Distributed Data Collector – select **Data Collector installed on NetBackup Primary Server(s)**.
   - Centralized Data Collector – select either **SSH Protocol to NetBackup Primary Server(s) (Linux, Windows)** or **WMI protocol to NetBackup Primary Server(s) (Windows only)**

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. If the hosts already exists, IT Analytics displays a confirmation dialog box to update the Host Details (including the Host Type). Click **Ok** to update Host details / Host Type.
    See "Add/Edit NetBackup Primary Servers within the Data Collector policy" on page 64.

  Edit: Select a server and click **Edit** to update the server values.

Note: You can add multiple servers while creating the NetBackup policy, provided the NetBackup servers have the same credentials and **Backup Software Location** is also same for the servers.

- **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 one of the following collection methods.
  - **Data Collector installed on NetBackup Primary Server**
  - **SSH Protocol to NetBackup Primary Server(s) (Linux, Windows)**
  - **WMI Protocol to NetBackup Primary Server(s) (Windows Only)**

- **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.
  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. 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 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.

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 Cohesity NetBackup deployed on Kubernetes clusters" on page 52.

- **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.

  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.

- **Tape Library & Drive Inventory**: Select the check box to activate Tape Library data collection from your NetBackup environment.

  The default polling frequency is every 12 hours. Click the clock icon to create a schedule frequency for collecting data. You can schedule the collection frequency by minute, hour, day, week and month. Advanced use of native CRON strings is also available. Optimize performance by scheduling less frequent collection.

- **Telemetry**: This probe collects Telemetry data from NetBackup primary and sends to SORT/Usage Insights in Alta View. This probe is active by default for Alta View users only.
  - Probe will be active by default and not editable for a new **Veritas NetBackup Data Collector Policy** when the **Collection Method** is **NetBackup software on Data Collector server**.
  - Probe will be de-activated and disabled when the protocol **SSH** / **WMI** is selected for the **Collection Method** to **NetBackup Primary Server**.

  - The default scheduled for the execution is: **Runs Every day at 12:00:00**
  - This probe is *NOT* visible or active for non-Alta View customers

- **Tape Inventory**: Select the check box to activate Tape data collection from your NetBackup environment.
  The default polling frequency is every 18 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. Optimize performance by scheduling less frequent collection.
- **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.
  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 probe 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 NetBackup 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.
  This probe skips exclude/include data collection from VMware, HyperV, RHEV, Nutanix, AWS, Azure, and GCP workloads. Configure the **NBU_CLNT_EXC_INC_SKIP_POLICY_TYPE_IDS** advanced parameter to add comma separated policy id(s) of any additional workload(s) to skip exclude/include data collection.
  USE_ALT_NBU_INCL_EXCL - This advanced parameter can be configured for collection of NetBackup include/exclude lists from Unix clients. By default, the collector uses the NetBackup-recommended command syntax to retrieve the lists. If the lists are not collected successfully, set the advanced parameter to Y, which instructs the collector to use an alternative command syntax for list data retrieval from Unix clients. Valid values for this parameter are Y or N (Default= N). This parameter can be set at the Data Collector level.

Note: For information on NetBackup policy types, refer to *NetBackup Self Service Configuration Guide* > *Appendix A NetBackup policy types* > *List of NetBackup policy types* section.

- **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, Storage Lifecycle Policies, and update for Media Servers and Services. 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, and day. Advanced use of native CRON strings is also available. 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 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 IT Analytics Exporter on the NetBackup Primary Server.
  See the *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.

Add/Edit NetBackup Primary Servers within the Data Collector policy

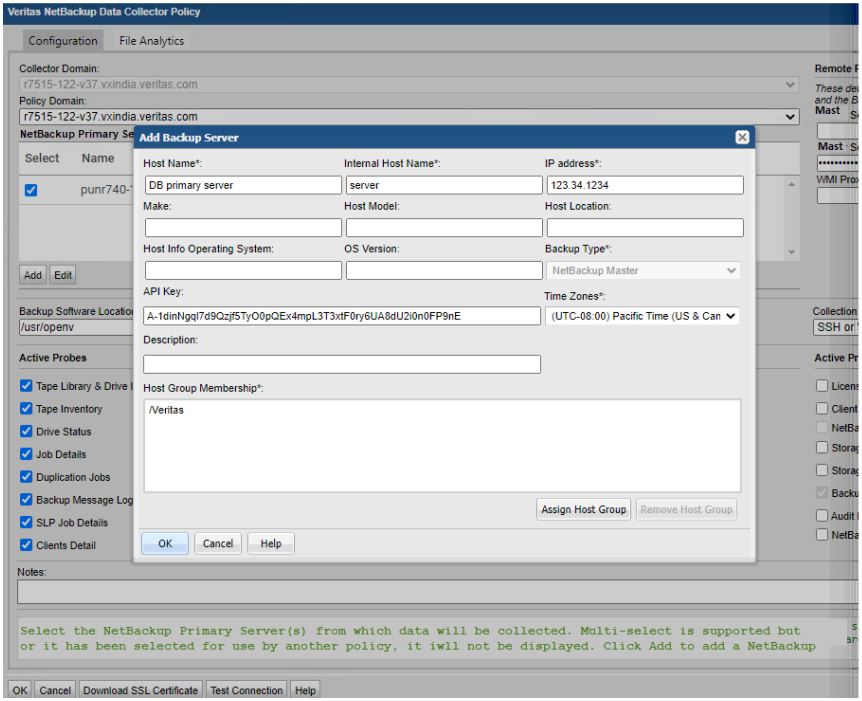
Add and edit Veritas NetBackup servers directly from the data collector policy screen. These functions are also available from the **Inventory**.

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.



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.
     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 for a host that is configured as a NetBackup Primary.
   - **API Key**: Enter the API key obtained from the Cohesity 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 Cohesity 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.

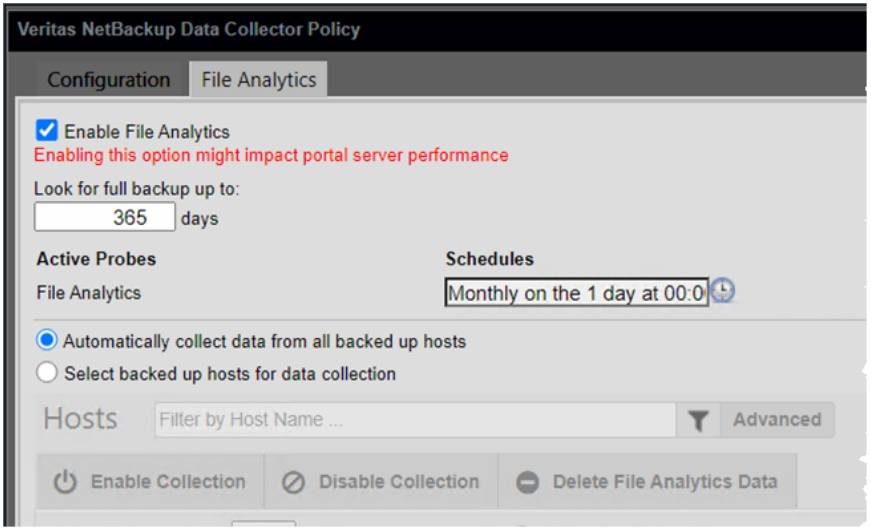
See "Prerequisites for collection from Cohesity NetBackup deployed on Kubernetes clusters" on page 52.

- **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, IT Analytics defaults to the time zone of the Data Collector server. Note that in IT Analytics reports, the date and time displayed for a backup transaction represents the date and time when the event actually happened.
- **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.



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 or Protection License Suite subscription: You must subscribe to the Complete or Protection License Suite of IT Analytics to enable File Analytics, as a policy, 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 3-1 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 3-2 Portal sizing for File Analytics

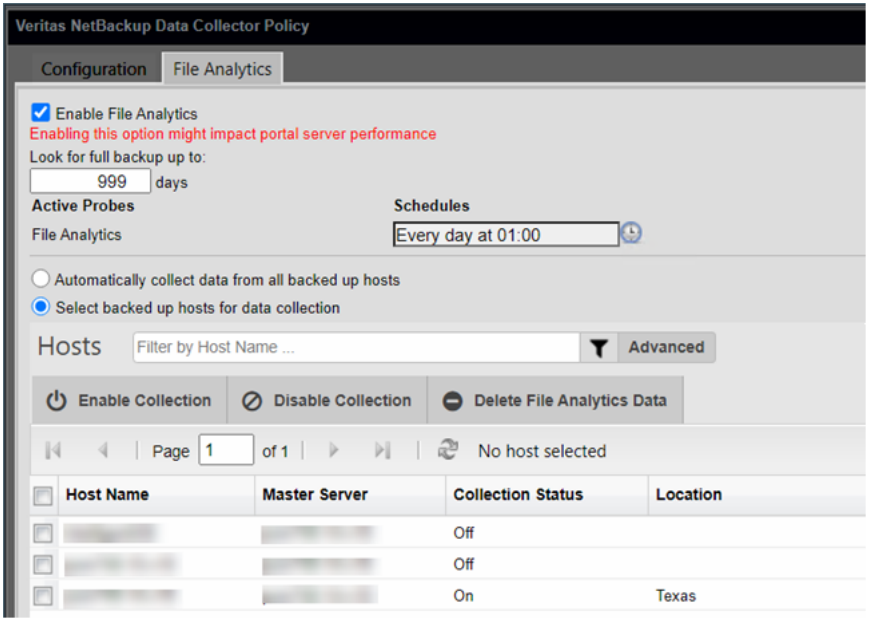
Portal	
Minimum RAM	32 GB
CPU	Minimum 4 CPU core, but 8 CPU core is recommended
Minimum usable hard disk space	200 GiB **Note:** It is observed that for every 100 million files, approximately 5 GB disk space is consumed on the portal.

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.



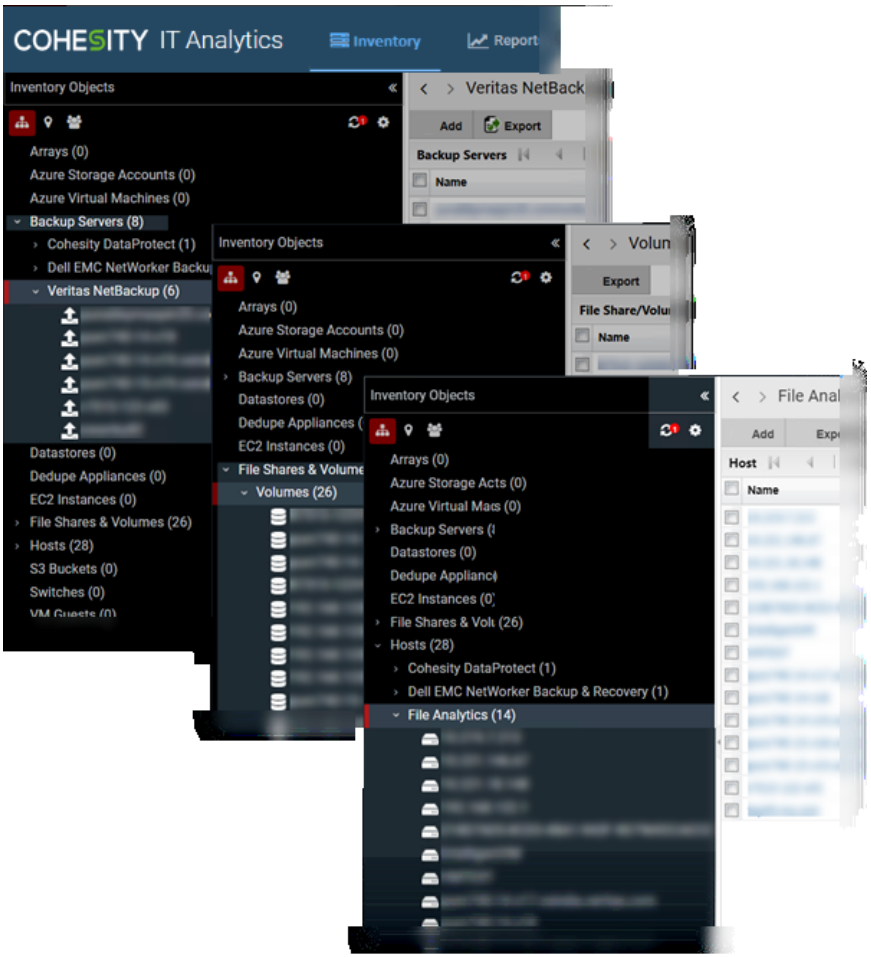
You can configure the following for File Analytics:

- **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 *IT Analytics Data Collector Installation Guide for File Analytics* guide for the export procedure.

Chapter 4

Installing the Data Collector software

This chapter includes the following topics:

- Introduction
- Considerations to install Data Collector on non-English systems
- Install Data Collector Software on Windows
- Install Data Collector software on Linux
- Configure Data Collector manually for Cohesity NetBackup
- Install Data Collector binaries on Windows (without configuration)
- Install Data Collector binaries on Linux host (without configuration)
- Override default Java Heap memory (XMX) value for Data Collector utilities

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 IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English, and requires the

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

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

Considerations to install Data Collector on non-English systems

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

- Simplified Chinese
- French
- Korean
- Japanese

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

The OS-specific requirements mentioned below.

Non-English Linux OS

On a non-English Linux host:

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

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

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

1. Check the current language.

   ```
   #locale
   ```

2. Check whether your system has multiple languages:

   ```
   #locale -a
   ```

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

   - To add Simplified Chinese:

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

   - To add French:

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

   - To add Korean

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

   - To add Japanese

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

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

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

See “Install Data Collector software on Linux” on page 84.

Non-English Windows OS

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

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

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

See "Install Data Collector Software on Windows" on page 75.

Install Data Collector Software on Windows

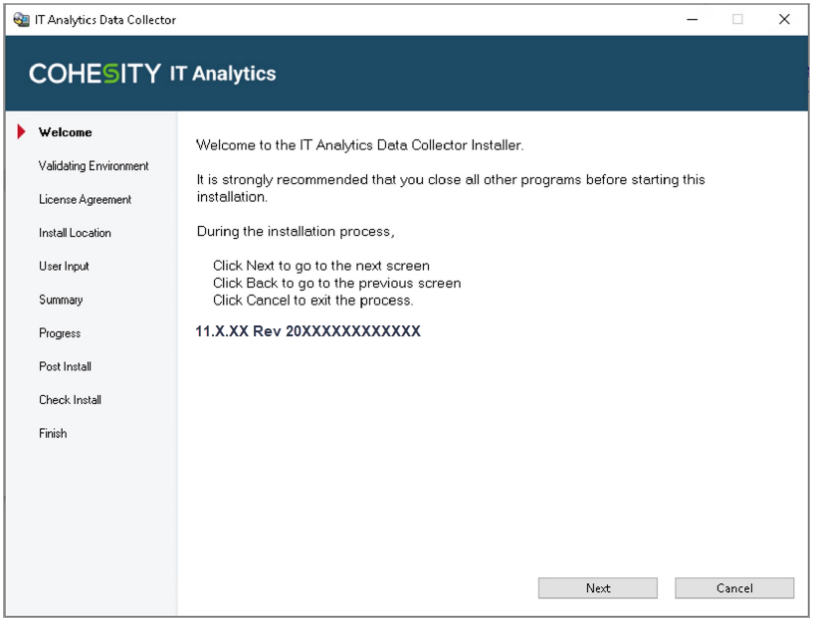
To install your Data Collector software:

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

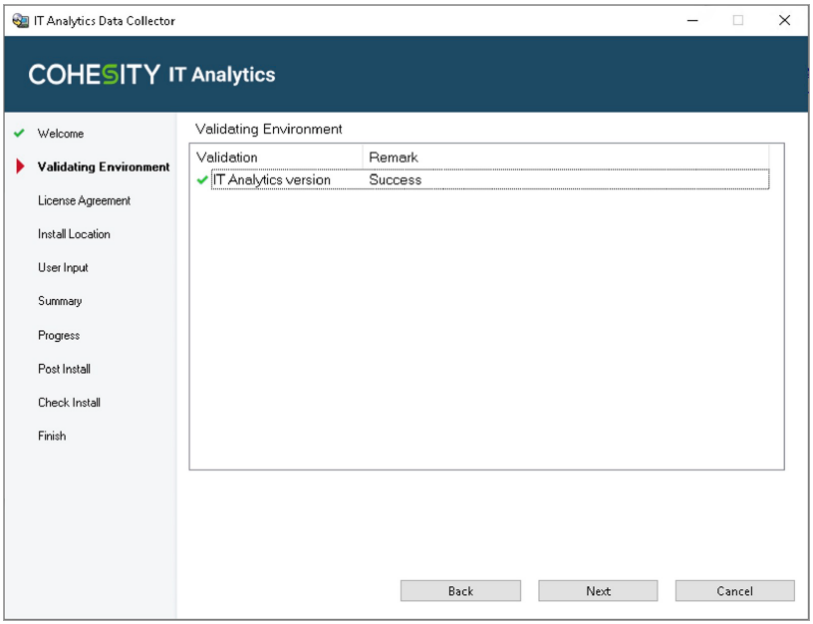
   Once, downloaded, the Data Collector Installation Wizard launches automatically. If it does not, navigate to its directory and double-click the executable file `Setup.exe`.

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

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



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



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

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

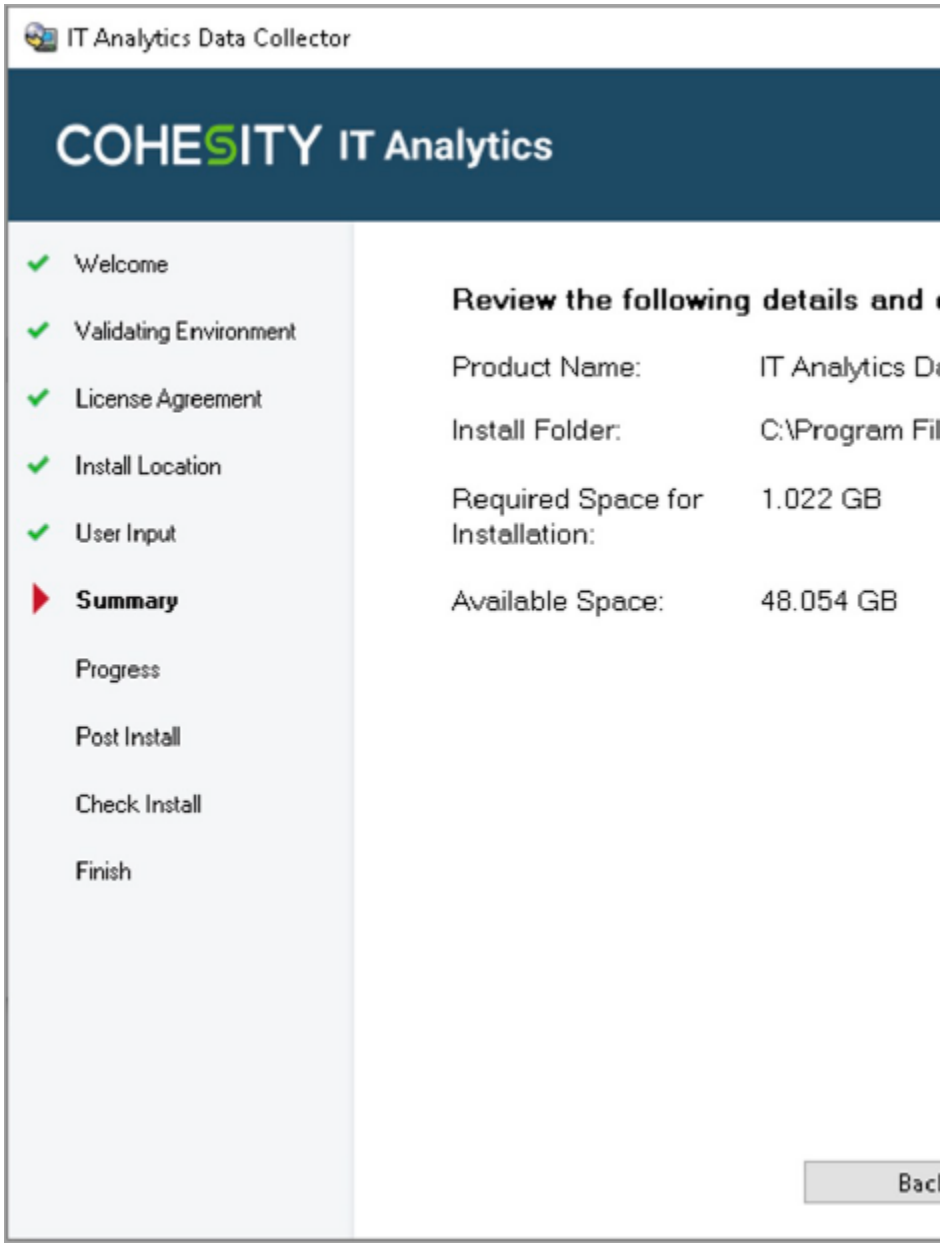
If you specify a custom directory, the install creates the `AnalyticsCollector` folder within the specified directory.

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

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

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

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



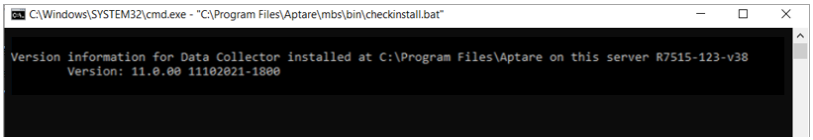
9 Click **Next** to initiate the installation.

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

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

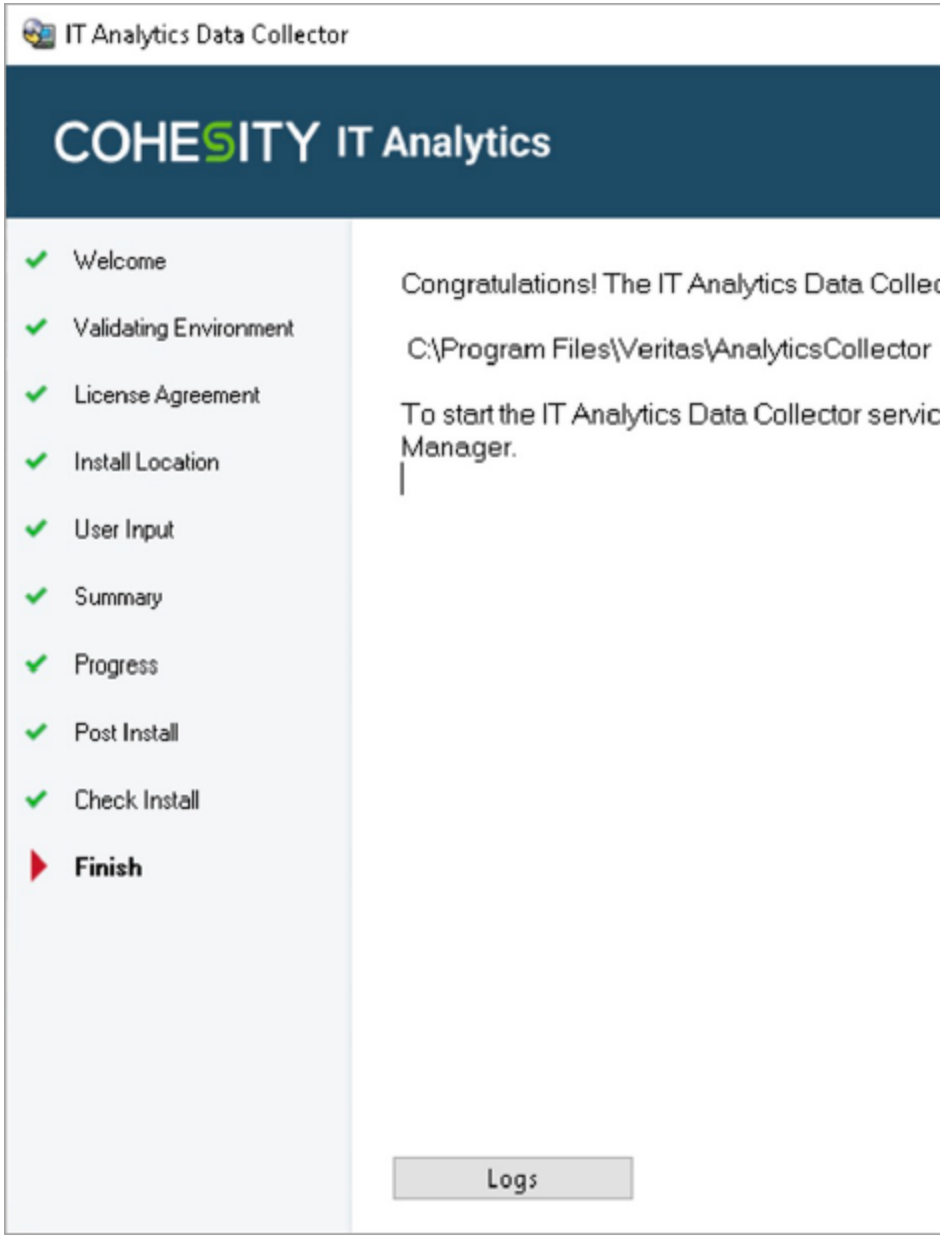
Close the terminal window once the validation is complete and then click **Next**.

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



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

Your Data Collector installation is complete.



Install Data Collector software on Linux

To install Data Collector software on Linux:

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

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

   For RHEL or OEL:

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

     ```
     yum install rng-tools
     ```

   - Start the services.

     ```
     systemctl start rngd
     ```

   - Enable the services.

     ```
     systemctl start rngd
     ```

   For SUSE:

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

     ```
     zypper install rng-tools
     ```

   - Start the services.

     ```
     systemctl start rng-tools
     ```

   - Enable the services.

     ```
     systemctl enable rng-tools
     ```

3. Ensure the following rpms are present on the system:

   On SUSE: libXrender1 and libXtst6 insserv-compat

   On other Linux systems: libXtst and libXrender chkconfig

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

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

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

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

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

5. Mount the ISO image that you downloaded.

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

   Substitute the name of the ISO image downloaded have downloaded.

6. Start the installer:

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

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

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

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

9. The installer requests for the following details.

   - **Data Collector Registration File Path**: Enter the absolute file path of the registration file generated and downloaded from the IT Analytics Portal.
   - Web Proxy (HTTP) settings can be configured. Enter **y** to configure proxy. The installer prompts for:
     - **HTTP Proxy IP Address**: Enter the hostname or IP address and a port number.

- **HTTP Proxy Port**: Enter the proxy port number for HTTP proxy.
- **Proxy UserId and password**: Enter the credentials for the proxy server.
- **No Proxy For**: Enter the host names or IP addresses separated by commas that will not be routed through the proxy.

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

Configure Data Collector manually for Cohesity NetBackup

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

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

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

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

To configure the Data Collector manually on Windows:

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

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

3. Run the command:

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

To configure the Data Collector manually on Linux:

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

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

3 Update the value for each field with appropriate data.

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

4 Run any one of the following command:

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

Or

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

Install Data Collector binaries on Windows (without configuration)

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

- Registration file downloaded from the Portal.

- Proxy server configuration details

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

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

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

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

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

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

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

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

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

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

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

Configure the Data Collector using responsefile from command prompt

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

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

or

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

Uninstall Data Collector

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

Install Data Collector binaries on Linux host (without configuration)

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

To install a Data Collector:

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

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

2. Install the Data Collector at a custom location.

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

   Example:

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

Configure the Data Collector using response file

A sample response file is saved when you install the Data Collector. To connect the Data Collector with the 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 IT Analytics Portal:
   - Registration file downloaded from the Portal.

- Proxy server configuration details

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

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

3 Configure the data collector using the above response file.

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

or

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

4 Start the data collector service

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

Uninstall Data Collector

Run this command to uninstall the Data Collector.

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

Override default Java Heap memory (XMX) value for Data Collector utilities

You may require to override the default Java Heap Memory (XMX) value to avoid performance degradation or potential "OutOfMemoryError" exceptions. The following procedure provides the override steps for Windows and Linux hosts.

Override default Java Heap memory (XMX) value for Windows Data collector utilities

To override the default XMX value for Data Collector Windows batch scripts, uncomment the XMX variable in `dc_override_config.bat` present in the `mbs\conf` directory and provide the updated XMX value. The comment in the batch file will guide you to identify the variable to be overridden for the script you are interested.

Example: Override XMX value for `checkinstall.bat` script

Update XMX value in `dc_override_config.bat`

```
:: checkinstall.bat
              XMX_CHECK_INSTALL=-Xmx17g
```

The backup of the `dc_override_config.bat` is saved to the `mbs\conf` directory with the name `dc_override_config.bat_bkp`.

Note: Use **::** only for comment and at the beginning of the line.

Override default Java Heap memory (XMX) value for Linux Data collector utilities

To override the default XMX value for Data collector Linux batch scripts, uncomment the XMX variable in `dc_override_config.sh` present in the `mbs/conf` directory and provide the updated XMX value. The comment in the shell script file will guide you to identify the variable to be overridden for the script you are interested.

Example: Override XMX value for `checkinstall.sh` script

Update XMX value in `dc_override_config.sh`

```
#checkinstall.sh
            XMX_CHECK_INSTALL=-Xmx17g
```

The backup of the `dc_override_config.sh` is saved to the `mbs\conf` directory with the name `dc_override_config.sh_bkp`.

Note: Use **#** only for comment and at the beginning of the line.

Chapter 5

Configure SSL

This chapter includes the following topics:

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

SSL/TLS certificate configuration

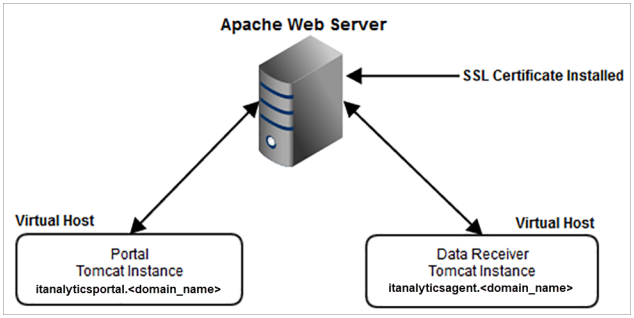
The following sections use the legacy and familiar reference to the Secure Socket Layer (SSL) protocol within IT Analytics. In reality, the IT Analytics communications are configured to utilize the newer and much more secure TLS (Transport Layer Security) protocols. This document retains the familiar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

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

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

SSL implementation overview

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



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

Implementing SSL involves these main tasks:

- See “Obtain an SSL certificate” on page 98.
- See “Update the web server configuration to enable SSL on the Portal server” on page 99.
- See “Enable / Disable SSL for a Data Collector” on page 104.

- See "Enable / Disable SSL for emailed reports" on page 104.

Obtain an SSL certificate

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

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

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

```
cd /tmp

vi san.cnf
```

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

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

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

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

```
[ v3_req ]
subjectAltName = @alternate_names

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Linux:

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

   Windows:

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

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

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

   Linux

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

   Windows

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

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

Linux:

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

Windows:

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

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

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

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

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

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

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

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

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

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

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

   Linux:

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

   Windows:

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

8. Update the Apache SSL configuration file.

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

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

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

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

   Example:

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

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

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

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

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

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

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

    If this message occurs:

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

Resolve Syntax Error by linking libraries:

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

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

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

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

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

    Linux

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

    Windows

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

Configure virtual hosts for Portal and / or Data Collector SSL

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

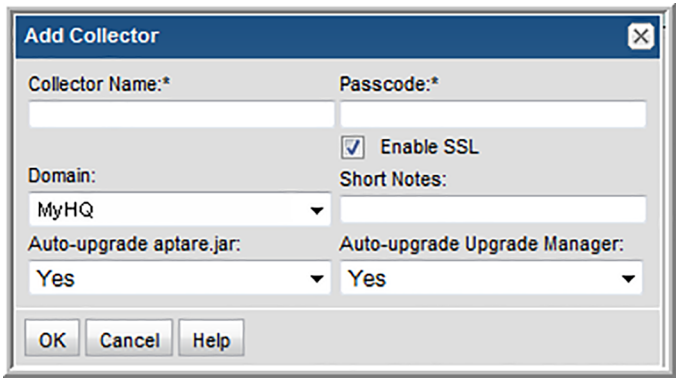
- *SSL Implementation for the Portal only*
- *SSL Implementation for data collection only*
- *SSL Implementation for both portal and data collection*

Enable / Disable SSL for a Data Collector

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

To enable and disable SSL for a specific Data Collector:

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



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

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

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

Enable / Disable SSL for emailed reports

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

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

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

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

   Example:

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

2. Restart the Portal service.

Test and troubleshoot SSL configurations

The following sections cover common configuration for testing and troubleshooting.

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

Test if SSL is set up for the Portal

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

   The Portal login page should display.

Test if SSL is set up for Data Collection

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

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

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

Keystore file locations on the Data Collector server

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

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

See "Import a certificate into the Data Collector Java keystore" on page 106.

Import a certificate into the Data Collector Java keystore

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

See "Keystore file locations on the Data Collector server" on page 106.

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

   Linux:

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

Windows:

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

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

   ```
   changeit
   ```

   The results will be similar to the following example:

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

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

   Linux:

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

   Windows:

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

   Sample Linux Output

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

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

Keystore on the portal server

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

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

The utility is located here:

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

The keystore is located here:

/opt/aptare/portalconf/itanalytics.jks

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

Add a virtual interface to a Linux server

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

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

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

   ```
   ifconfig -a
   ```

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

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

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

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

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

   ```
   ifconfig eth0:0 111.222.333.444
   ```

   where

   111.222.333.444 is the new IP address for the virtual interface.

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

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

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

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

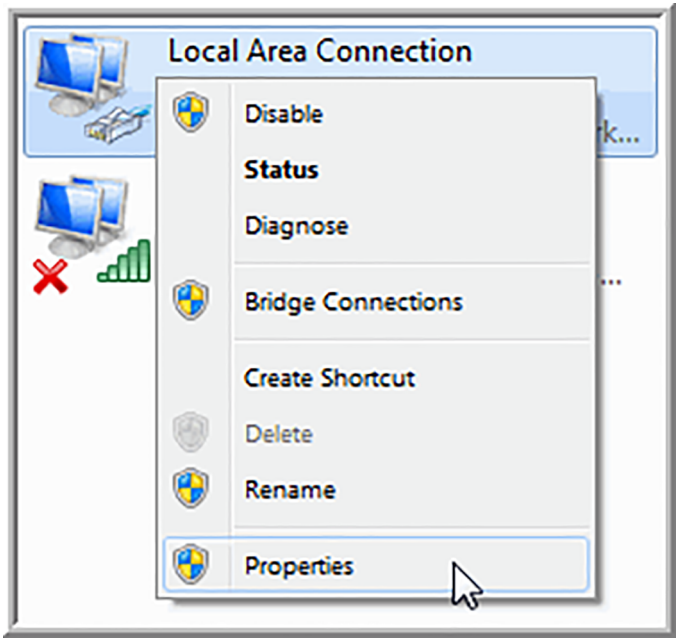
6. Finally, update your DNS server so that the new IP address is mapped to the data collection URL (for example, **itanalyticsportal.<domainname>**).

Add a virtual / secondary IP address on Windows

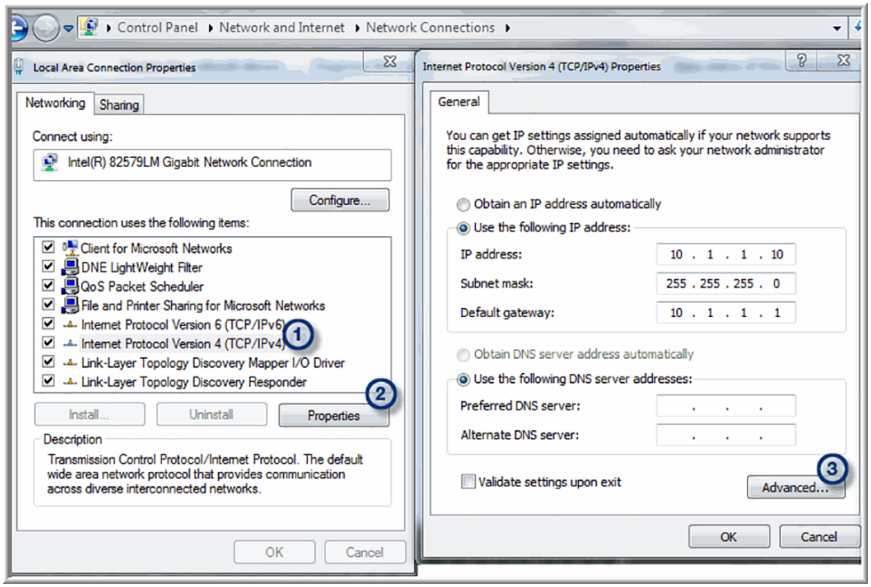
To add a Virtual IP Address on Windows, go to:

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

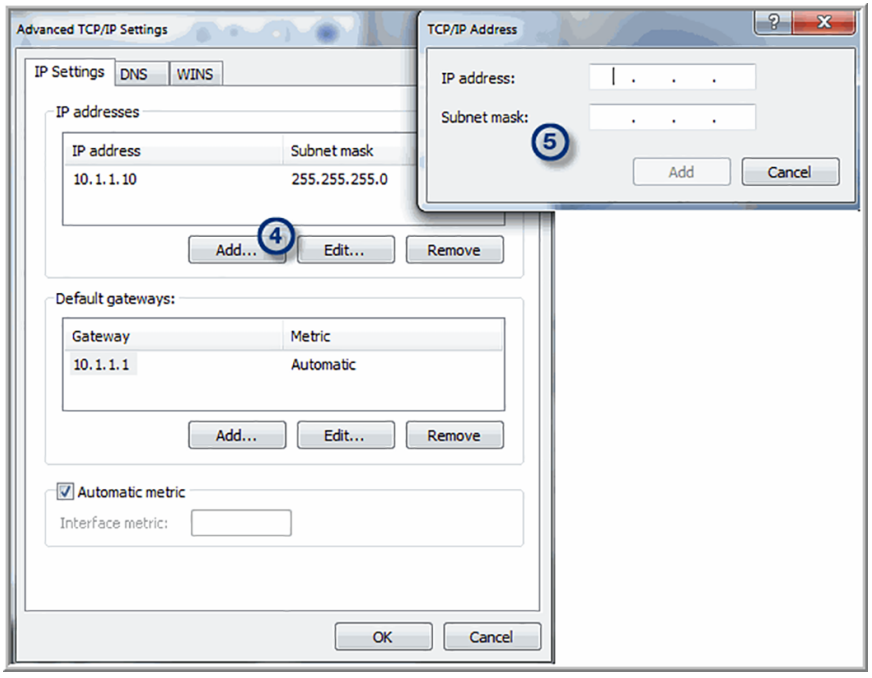
Right-click on a Network connection and select **Properties**.



Take the following steps to configure a secondary IP address.



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



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

Chapter 6

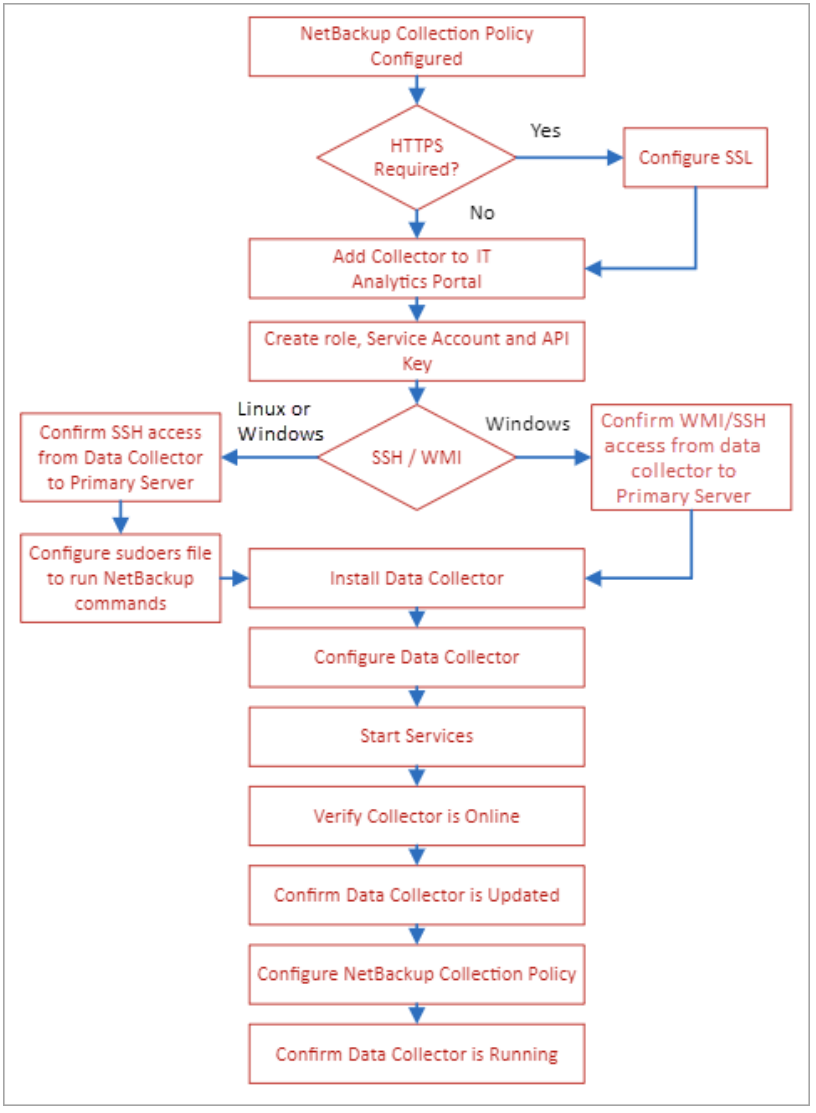
Centralized Data Collector for NetBackup - Prerequisites, Installation, and Configuration

This chapter includes the following topics:

- Overview
- Step-1: Choose operating system and complete prerequisites
- Step-2: HTTPS requirement
- Step-3: Add Data Collector on IT Analytics Portal
- Step-4: Create NetBackup Data Collector Role, Service Account, and API Key
- Step-5: SSH/WMI
- Step-6: Install the Data Collector
- Step-7: Configure Data Collector
- Step-8: Verify the Data Collector is online from the Portal
- Step-9: Confirm that the Data Collector is updated
- Step-10: Configure the data collection policy
- Step-11: Confirm that the NetBackup data collection policy is collecting data

Overview

This section includes preinstallation, installation, and configuration instructions for a Centralized Data Collector for NetBackup. The flowchart below details the steps to install and configure a Centralized Data Collector for NetBackup, Flex, and Flex Scale.



Step-1: Choose operating system and complete prerequisites

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

Things to consider include:

- The data protection vendors and subsystems from which you plan to collect data using the Centralized Data Collector. If you use the Data Collector to collect from other subsystems and applications, the operating system you select might need to be considered.
- Have you restricted remote access to NetBackup for just non-privileged users? (The Windows Data Collector requires root access for WMI.) If you are using the latest versions of NetBackup and Flex appliances that can be configured for Multifactor Authentication and restrict remote access to non-privileged users, it is preferable to choose the Linux OS for your Centralized Data Collector, or opt for a Distributed Data Collector, as detailed in *Chapter 2: Distributed Data Collector on a NetBackup Primary Server* .
  Chapter 2

Factors impacting Data Collector performance and memory requirements

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

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

Data Collector Supported Operating Systems

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

Table 6-1 Data Collector supported operating systems

Operating System	Version
Red Hat Enterprise Linux	7, 8.6 (update 10), and 9
SUSE Linux Enterprise	■ SLES 12 SP3, SP4, SP5 ■ SLES15 SP4
OEL	7, 8, and 9
Windows Server	2016, 2019, and 2022

Data Collector server memory and CPU guidelines

Use the following guidelines for Data Collector Servers.

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

Additional prerequisites

- Windows Only Requirement - If a Data Collector is required to collect data from Cohesity NetBackup Primary Server running on Windows System to non-English (United States) locale:
  - A Windows user must be created with the Administrators group of Windows system that will run the data Collector with culture set to English-US, and Region and Language set to English -US.
  - The current system locale must be set to the same language as the NetBackup Primary Server.
- For performance reasons, do not install Data Collectors on the same server as the Portal.

- Install only one Data Collector on a server (or OS instance).
- For Cohesity NetBackup collection, the Data Collector server and backup server can be in different time zones.
- Uses ports 443, 1556, and 13724 WMI range of ports, Linux ssh 22
- The NetBackup Event Monitor probe, enabled on the Data Collector policy screen, uses the `nb_monitor_util` executable. This executable is installed by default for all installations. It can be found in the `/usr/openv/netbackup/bin/goodies` directory on Linux and `\Program Files\Veritas\Netbackup\bin\goodies` on Windows. The Event Monitor probe collects events generated by the `nb_monitor_util` and handles create/update/delete events for Backup Policy, Storage Unit, Storage Unit Group and Storage Lifecycle Policy.

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

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

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

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

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

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

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

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

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

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

Option 2: Advanced Parameter

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

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

Step-2: HTTPS requirement

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

If HTTP is acceptable, continue with step 3.

See "*Configure SSL*" on page 96.

Step-3: Add Data Collector on IT Analytics Portal

Once logged in to the Portal:

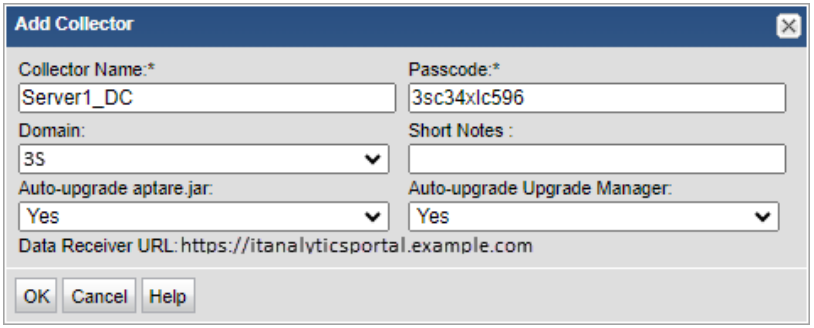
1 Select **Admin** > **Data Collection** > **Collector Administration**.

2 Click **Add Collector**.

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

Although the Data Collector name can be anything, Cohesity recommends that the Data Collector name be the hostname of the server the Data Collector

software is installed on. In the example below, we use the Data Collector Server Name followed by "_DC".



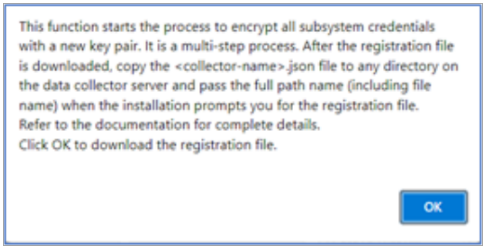
Field	Description
Collector Name*	The collector name cannot include a space and is case sensitive. The names should match exactly as entered in the Data Collector configuration screen and the Data Collector Installer screen. Edit the unique name assigned to this Data Collector. The Data Collector will use this value for authentication purposes. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made.

Field	Description
Passcode*	Edit the passcode assigned to this Data Collector. It can be any character sequence. Unlike other system passwords (which are encrypted and then saved) this Data Collector passcode is not encrypted prior to saving in the database and may appear as clear case in certain files. It simply is intended as a “handshake” identification between the Data Collector and the policy. Changing the Collector ID or passcode requires manual changes to the corresponding Data Collector server. Collection will break if these corresponding changes are not made. You can use the following OS-specific special characters in the passcode. Make sure the special characters you include are supported on the OS where the Data Collector is installed. ■ Linux: !@#%^* ■ Windows: !@#$%^&*()
Short Notes	Descriptive notes associated with this Data Collector.
Enable SSL	Both secure (SSL) and non-secure Data Collectors can send data to the same Portal. Check this box to select the secure communication protocol (https) that the Data Collector will use. This check box will not appear in the dialog box if SSL is not enabled in your environment. The Portal data receiver must be listening for https traffic; for example: https://agent.mycollector.com
Auto-upgrade aptare.jar	Indicate if you want this configuration file upgraded automatically. This part of the Data Collector is responsible for event and metadata processing threads. The .jar file contains the processing and parsing logic for data collection. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

Field	Description
Auto-upgrade Upgrade Manager	Indicate if you want this configuration bundle upgraded automatically. This Data Collector component is responsible for managing Data Collector upgrades. The latest versions can be downloaded automatically and applied to the collector during upgrades. It is recommended that this setting be set to Yes.

3 Click **OK**.

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



4 Click **OK**.

Many NetBackup releases came bundled with IT Analytics Data Collector software that leveraged a `.key` file rather than a `.json` file. The configuration steps are slightly different depending on the file type required to configure the Data Collector. Listed below is a table that shows what versions of the IT Analytics Data Collector binaries are installed on which versions of NetBackup. This table is also applicable to NetBackup Appliances and Flex Appliances. By checking the NetBackup version installed on the appliance, you can determine whether to use a `.key` or a `.json` file, when configuring the Data Collector.

Table 6-2 Reference for `.key` and `.json` usage

NetBackup version	IT Analytics Data Collector version installed on NetBackup	.key or .json file to be used
10.1.1	11.1.50	.key
10.2	11.2.00	.key

Table 6-2 Reference for `.key` and `.json` usage *(continued)*

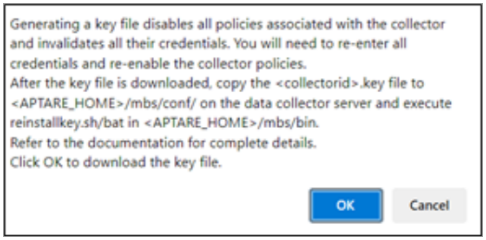
NetBackup version	IT Analytics Data Collector version installed on NetBackup	.key or .json file to be used
10.2.0.1	11.2.00	.key
10.3	11.2.05	.key
10.3.0.1	11.2.05	.key
10.4	11.3.02	.json
10.4.0.1 (or later)	11.3.04 (or later)	.json

To download the `.key` file:

1. Login to the Portal and go to **Admin** > **Collector Administration**.
2. Select the Data Collector you just created, as described in the procedure above..
3. Click **Edit**.
4. Select **Key File**.
5. Note the following information:
   - Name of the Data Collector (as it appears on the Portal)
   - Passcode of the Data Collector (as configured on the Portal)
   - Data receiver URL (generated while creating the Data Collector on the Portal)

Note: The host name in data receiver URL, executed from the NetBackup primary, must resolve to the Portal server's IP address.

6 Click **Generate**.



Following message, which indicates that a `.key` file has been created is displayed. This file is required when you configure and register all Data Collector versions of 11.2 and earlier.

A message indicating that a `.key` or a `.json` file has been created is displayed. The `.key` is required when you configure and register your IT Analytics 11.2 or earlier Data Collector. The `.json` file is required when you configure and register your IT Analytics 11.3 or later

7 Get the `.key` or `.json` file path.

Download and copy the `.key` or `.json` file to the NetBackup primary server when you configure the Data Collector.

Step-4: Create NetBackup Data Collector Role, Service Account, and API Key

A Data Collector Service Account and API key is used while configuring the Cohesity NetBackup Data Collector policy. This must be configured to enable complete collection from NetBackup. Create a Data Collector Service Account and add an RBAC custom role in the NetBackup Web UI.

Custom role

To create the custom role within the NetBackup Web UI:

1 On the left, click **Security** > **RBAC**.

2 Under the **Roles** tab, click **Add**.

3 Select **Custom role** and click **Next**.

4 Enter the **Role Name** and **Role Description**.

5 Under **Permissions**, click **Assign**.

- Select all the **View** permissions for all the objects under **NetBackup Management**, **Protection**, and **Storage** sections of the NetBackup web UI.
- From the **NetBackup Management** > **CLI Sessions** section, enable **CLI Execute**.
- From the **NetBackup Management** > **Malware** section, enable **View scan results**.
- From the **RBAC** > (**Edit RBAC customs role**) > **Global Permission** tab > **Security** > enable **View** permission for **Global Security Settings**.
- From the **RBAC** > (**Edit RBAC customs role**) > **Global Permission** tab > **Security** > enable **View** permission for **Security Events**.

6 Select **Users** tab and **Add to List** service account to be associated with this role.

API key

Copy the API key generated with these steps for future use. It will be required while configuring the NetBackup Collection Policy.

To add an API key:

1 Select **Security** > **Access keys** on the NetBackup Web UI.

2 Enter the **Username** and **Description**.

The service account associated with the API key and the Role, must be the same service account that is associated with the Veritas NetBackup Collection Policy in IT Analytics.

3 Click **ADD**.

If you are configuring a Centralized Data Collector with SSH access to the NetBackup primary, then you must create a second user in addition to the account created in the steps above. This second user must be an OS user with an identical username, same as the account you just created. See the section *Linux Centralized Data Collector: SSH* for instructions on how to create the second account.

See "Linux Centralized Data Collector: SSH" on page 125.

Step-5: SSH/WMI

SSH requires a configuring a Sudoers file to execute NetBackup commands. A WMI Proxy Service is required, and installed by default, as part of the Data Collector installation on a Windows server. For configuring a Linux Data Collector, proceed

to Linux Centralized Data Collector: SSH. For a Windows Data Collector, proceed to Windows Data Collector: WMI Connectivity .

Linux Centralized Data Collector: SSH

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. 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.

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.

Windows Data Collector: WMI Connectivity

WMI is only used for connecting to a remote Windows Primary Server from a Centralized Data Collector or another subsystem that requires WMI. 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. The WMI Proxy Service is installed by default, as part of the Data Collector installation on a Windows server. Customers must work with their Windows Hosting Team and Domain Admins for setting up WMI for their specific version of Windows and in alignment with their domain policies.

See “Testing WMI connectivity” on page 130.

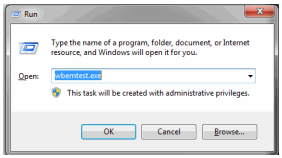
See “Installing the WMI Proxy Service (Windows Host Resources only)” on page 132.

Testing WMI connectivity

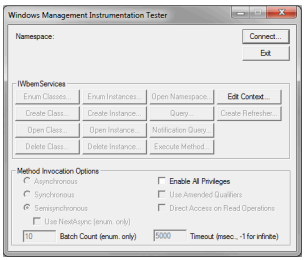
The Windows Management Instrumentation (WMI) Proxy is used by IT Analytics to collect data from Windows hosts. Should you have connectivity issues, these steps can be taken to test and troubleshoot connectivity.

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

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

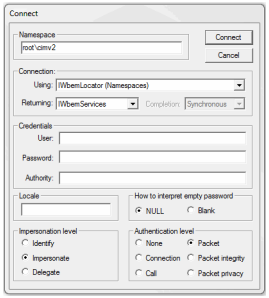


3. In the Windows Management Instrumentation Tester window, click **Connect**.



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

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



5. Complete the following fields in the Connect window and then click **Connect**.
   - User - Enter the credentials for accessing the remote computer. This may require you to enable RPC (the remote procedure call protocol) on the remote computer.
   - Password
   - Authority: Enter **NTLMDOMAIN:<NameOfDomain>**

where NameOfDomain is the domain of the user account specified in the User field.

6. Click **Enum Classes**.
7. In the Superclass Info window, select the **Recursive** radio button, but do not enter a superclass name. Then, click **OK**.
8. The WMI Tester will generate a list of classes. If this list does not appear, go to the Microsoft Developer Network web site for troubleshooting help.

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

Installing the WMI Proxy Service (Windows Host Resources only)

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

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

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

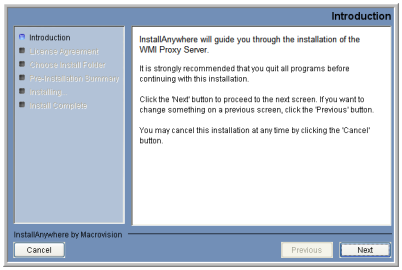
   On Windows:

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

   On Linux:

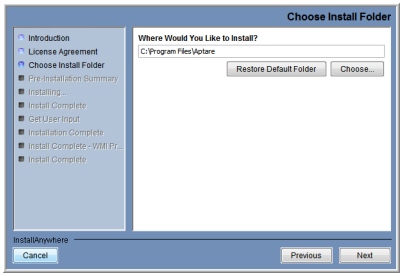
   ```
   /opt/aptare/utils/aptarewmiproxyserver.exe
   ```

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



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

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

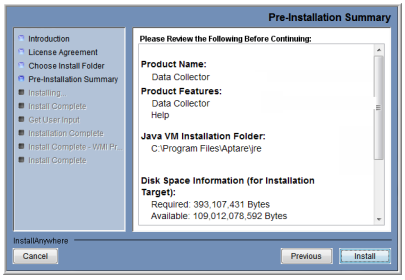


7. Specify the directory where you would like to install the Data Collector software.
   - Default for Windows: **C:\Program Files\Aptare**
   - Default for Linux: **/opt/aptare**

Note: Accepting the default path is recommended.

---

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

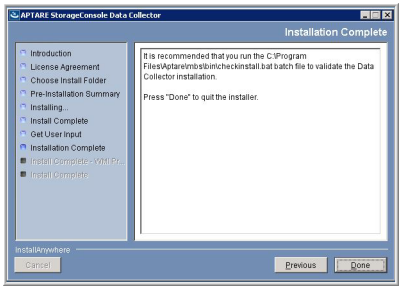


10. Click **Install** to proceed with the installation.
11. If the installer detects that you do not have Microsoft .NET already installed on the server, it will notify you of this required dependency. Microsoft .NET contains several necessary libraries. Refer to the *Certified Configurations Guide*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

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

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

    Startup > Control Panel > Administrative Tools > Services
14. The following window will appear when the installation is complete.



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

Step-6: Install the Data Collector

Proceed to *Chapter 4: Installing the Data Collector*. This section assumes that you will install a IT Analytics Data Collector 11.4 or greater, which will allow you to register the data collector using a `.json` file. When complete, resume to *Step-7: Configure Data Collector* .

See "*Installing the Data Collector software*" on page 72.

See "Step-7: Configure Data Collector" on page 135.

Step-7: Configure Data Collector

- For a NetBackup Server 10.4 or greater, proceed to Step-7A: Configure Data Collector for NetBackup 10.4 or later from its Web UI.
- For earlier versions of NetBackup, proceed to Step-7B: Configure IT Analytics Data Collector manually for earlier versions of NetBackup.
- For a NetBackup Appliance or NetBackup Flex Appliance proceed to Step-7C: Configure Data Collector for NetBackup Appliances (including Flex appliance) .

Step-7A: Configure Data Collector for NetBackup 10.4 or later from its Web UI

The Data Collector reports NetBackup information to IT Analytics or to Cohesity Alta View. The Data Collector is installed along with a NetBackup installation or upgrade.

For NetBackup 10.4 or higher, you can register their Data Collector directly from the NetBackup Web UI by adding a .json file.

To register the Data Collector from the NetBackup Web UI:

1. On the top right corner within the NetBackup Web UI, click the Cog icon and select **Data Collector Registration**.
2. Click **Register with Cohesity IT Analytics**.
3. Click **Choose file** to select the registration file (JSON) that you have created earlier.
4. If required, click the **Proxy server** option to specify Proxy server settings.
5. Click **Register**.

Step-7B: Configure IT Analytics Data Collector manually for earlier versions of NetBackup

This section details the steps required to manually configure the Data Collector using a `.key` file. This configuration requires editing a response file to configure the distributed Data Collector, installed by default on the non-clustered NetBackup primary. The Cohesity NetBackup primary server installation will deploy IT Analytics Data Collector binaries automatically on Windows (`C:\Program Files\Veritas\AnalyticsCollector`) and Linux (`/usr/openv/analyticscollector`).

The 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.

See "Step-3: Add Data Collector on IT Analytics Portal" on page 118.

To configure the Data Collector manually on Windows using key file:

1. Create a response file as a batch script `responsefile.cmd` with the contents shown. These are the responses to the user input required to configure the Data Collector. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.

```
SET DATACOLLECTOR_NAME=name_of_the_data_collector
SET DATACOLLECTOR_PASSCODE=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=
```

2. Update the value for each field with appropriate data. A sample response file is also available in the installer media in `x64\ITA_DC\responsefile.cmd`.
3. Run the command shown:

```
"C:\ProgramData\Veritas\NetBackup IT Analytics\DC\configure.cmd"


\RESPFILE:response_file_path \INSTALL_TYPE:CONFIG
```

4. Validate the Data Collector integration with IT Analytics by going to `C:\Program Files\Veritas\analyticscollector\mbs\bin\` and running this command: `checkinstall.bat`.

   If the Data Collector is configured with the Portal, the response is displayed as **SUCCESSFUL**.

Note: If there is a version mismatch of `aptare.jar` between the Data Collector and the Portal, execution of the `checkinstall.bat` command starts an auto-update of the Data Collector.

To configure the Data Collector manually on Linux using key file:

1. Create a response file with the contents shown. These are the responses to the user input required to configure the Data Collector:

```
COLLECTOR_NAME=name_of_the_data_collector
COLLECTOR_PASSCODE=passcode_for_the_data_collector
DR_URL=data_receiver_URL
COLLECTOR_KEY_PATH=path_to_the_key_file
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 response file is available on the install media and from `/usr/openv/analyticscollector/installer/responsefile.sample` on the primary server.
3. Run the command:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
responsefile_path
```

4. Validate the Data Collector integration with IT Analytics by navigating to `/usr/openv/analyticscollector/mbs/bin/` and running `./checkinstall.sh`. If the Data Collector is able to communicate with the IT Analytics Portal, the response is displayed as **SUCCESSFUL**.

Note: If there is a version mismatch of `aptare.jar` between the Data Collector and the Portal, execution of the `checkinstall.bat` command starts an auto-update of the Data Collector.

Step-7C: Configure Data Collector for NetBackup Appliances (including Flex appliance)

You can configure a Data Collector on the primary server pod using the following steps. From NetBackup version 10.3 Cloud Scale release, Data Collector on primary server pod is supported. The below steps to configure the Data Collector on a

primary server must be performed as a root user. On a Flex appliance, connect to the primary server pod first and then switch to the root user using `sudo`. On a NetBackup Appliance, access shell by creating NetBackup CLI user.

To configure IT Analytics for NetBackup deployment:

1. Create a DNS server entry in such a way that IP of the Portal must be resolvable to a single FQDN. IP of the IT Analytics Portal must be resolved to:

   `itanalyticsagent.<yourdomain>`

   Note the following:

   - If the Portal URL is `itanalyticsportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `itanalyticsagent.<yourdomain>`
   - If the Portal URL is `aptareportal.<yourdomain>`, then ensure to add the DNS entries for the following hostnames: `aptareagent.<yourdomain>`

2. Depending upon the Data Collector version, collect the `<your-collector-name>.key` or `<your-collector-name>.json` file for the new Data Collector by accessing the Portal link and creating a collector. Copy it to the host machine from where NetBackup primary is deployed.

   For more information, refer to the *Data Collector Encryption* section in *IT Analytics User Guide*.

3. Create a new folder `analyticscollector` at persisted location (for example, `/mnt/nbdata/`) using the following commands:

   ```
   cd "/mnt/nbdata/"
   mkdir analyticscollector
   ```

4. Copy the `<your-collector-name>.key` file to `/mnt/nbdata/analyticscollector` inside the NetBackup primary host or container.

5. Exit from the container and copy the `<your-collector-name>.json` inside the NetBackup primary host or container.

6. In case if the data-receiver is configured with self-signed certificate (https), user must add the certificate in the Data Collector.

7. Connect to the NetBackup primary host or the container.

8. Navigate to `/usr/openv/analyticscollector/installer/` location and perform the following.

   - Open the `responsefile.sample` and add the following parameters:

If the Data Collector is lower than 11.3, create the response file with the following contents.

```
COLLECTOR_NAME=<your-collector-name>
COLLECTOR_PASSCODE=<your-password>
DR_URL=<http>/<https>://itanalyticsagent.<yourdomain>
COLLECTOR_KEY_PATH=<path to your-collector-name.key>
HTTP_PROXY_CONF=N
HTTP_PROXY_ADDRESS=
HTTP_PROXY_PORT=
HTTPS_PROXY_ADDRESS=
HTTPS_PROXY_PORT=
PROXY_USERNAME=
PROXY_PASSWORD=
PROXY_EXCLUDE=
```

If the Data Collector version is 11.3 or later, create the response file with the following contents.

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

9 Configure the Data Collector with the IT Analytics Portal as follows.

Note: If the Data Collector installed is of a lower version than the Portal, wait for the Data Collector auto-upgrade to finish before you proceed.

For NetBackup Appliance version 5.3 or later:

- Run the following command as a NetBackup CLI user:

  ```
  /usr/openv/analyticscollector/installer/dc_installer.sh -c
  /usr/openv/analyticscollector/installer/responsefile.sample
  ```

- To verify the Data Collector integration with IT Analytics Portal, run:

  ```
  /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
  ```

For NetBackup Appliance version 5.1.1:

- Run the following command as a NetBackup CLI user:

```
sudo /usr/openv/analyticscollector/installer/dc_installer.sh
-c /usr/openv/analyticscollector/installer/responsefile.sample
```

- To verify the Data Collector integration with IT Analytics Portal, run:

```
sudo /usr/openv/analyticscollector/mbs/bin/checkinstall.sh
```

If you are on Flex Appliance:

- Connect to the primary server container and then switch to root user using `sudo` and run:

```
/usr/openv/analyticscollector/installer/dc_installer.sh -c
/usr/openv/analyticscollector/installer/responsefile.sample
```

- To verify the Data Collector integration with IT Analytics Portal, run:

```
/usr/openv/analyticscollector/mbs/bin/checkinstall.sh
```

If the Data Collector is configured with the Portal, it will display **SUCCESSFUL**.

Note: If there is a version mismatch of `aptare.jar` between Data Collector and Portal, execution of `checkinstall.sh` command will trigger an auto-update of the Data Collector.

---

10 Check the Data Collector services status by running the following command and ensure that the following Data Collector services are up and running:

```
/usr/openv/analyticscollector/mbs/bin/aptare_agent status
```

Output of the above command:

```
IT Analytics WatchDog is running (pid: 13312).
IT Analytics MetaDataCollector is stopped.
IT Analytics EventDataCollector is stopped.
IT Analytics DataCollector process is running (pid: 13461).
IT Analytics On-demand process is running (pid: 13463).
```

For more information about the Data Collector policy, see *IT Analytics User Guide*.

For more information about the Data Collector policy, see *IT Analytics User Guide*.

Step-8: Verify the Data Collector is online from the Portal

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

Step-9: Confirm that the Data Collector is updated

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

Step-10: Configure the data collection policy

Refer to *Chapter 3: Configuring NetBackup Collection Policies* . Once the Data Collection Policy configuration is complete, continue to *Step 11*.

Chapter 3

Step-11: Confirm that the NetBackup data collection policy is collecting data

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

Chapter 7

Upgrading Data Collector Locally

This chapter includes the following topics:

- Overview
- Verification of upgrade bundle available on Data Collector server
- Upgrade the Upgrade Manager component
- Upgrade the Data Collector component which is the aptare.jar file
- Upgrade the Upgrade Manager and Data Collector components together
- Upgrade logs and upgrade related database views
- Resolve file lock issue on Windows host during Data Collector upgrade

Overview

IT Analytics Data Collector software includes two components:

- Data Collector
- Upgrade Manager

Both these components have their own upgrade bundles that are downloaded from the IT Analytics Data Receiver service running on the Portal server.

Data Collector component:

- It is responsible for monitoring the policies associated with the collector, scheduling probes as per policy configurations, thereby enabling the probes to collect data from various subsystems and sending it to the Data Receiver service running on the Portal server.

- t spawns different Java processes,
  like Watchdog, DataCollector, ValidationDataCollector, MessageRelayServer, EventDataCollector, and so on to perform these operations.

Upgrade Manager component:

- It is responsible for upgrading the Data Collector component, which is the `aptare.jar` file.

Functionality

- The WatchDog Java process initializes a thread (SmartUpdaterThread) that polls the Data Receiver every 11 minutes for any potential upgrade requests.
- If an Upgrade Manager upgrade is due:
  - SmartUpdaterThread checks if the Upgrade Manager upgrade bundle is available in a specified location on the Data Collector server, and proceeds to upgrade the Upgrade Manager component after verifying the credibility of the bundle.
  - If not available in the specified location, SmartUpdaterThread thread tries to download the Upgrade Manager upgrade bundle.
  - After successful download of the upgrade bundle, Upgrade Manager is upgraded.
- If a Data Collector upgrade is due:
  - SmartUpdaterThread thread checks if the Data Collector upgrade bundle is available in a specified location on the Data Collector server, and proceeds to initialize the Upgrade Manager component to upgrade the Data Collector component.
  - If the upgrade bundle is not available in the specified location, SmartUpdaterThread downloads the Data Collector upgrade bundle.
  - After successful download of the Data Collector upgrade bundle, the Upgrade Manager component is initialized (a new java process is started) to upgrade the Data Collector component.

Verification of upgrade bundle available on Data Collector server

SmartUpdaterThread validates both bundles in the following order.

- Version comparison: Bundle's version is compared against the expected upgrade version received from IT Analytics Data Receiver.

- Checksum verification: Checksum is retrieved from a Data Receiver, and compared against the one generated using the bundle available locally on the Data Collector server.
- Signed Jar verification: Java utility `jarsigner` is used to verify whether the bundle is signed or not.
- At any point, if the verification fails, the upgrade fails and bundles are deleted from the Data Collector server.

When to verify upgrade bundle?

When the IT Analytics Portal is upgraded successfully to a newer version, and subsequently, the Data Collector upgrade fails due to errors like:

- Collector bundle download failed for 11.2.1.03 Premature EOF
- Upgrade Manager upgrade failed. Exception is : Premature EOF

These errors indicate that the upgrade bundle could not be downloaded successfully on to the Data Collector server due to slow network/low bandwidth.

How to use the upgrade bundle?

Prerequisites:

- These errors indicate that the upgrade bundle could not be downloaded successfully on to the Data Collector server due to slow network/low bandwidth.
- Requires access permissions to copy files to/from Data Collector Server and Portal Server.

Notations:

- <PORTAL_APTARE_HOME> is where Portal is installed. Default value:
  Linux Portal: `/opt/aptare`
  Windows Portal: <drive>:\opt\aptare
- <DC_APTARE_HOME> is where the Data Collector is installed. Default values:
  Data Collector on Linux: /user/openv/analyticscollector
  Data Collectors on Windows: C:\Program Files\Veritas\AnalyticsCollector
- <OS> is the Operating System where Data Collector software is installed.
- <version> is the IT Analytics version (Portal is on this version)

Upgrade the Upgrade Manager component

To upgrade the Upgrade Manager component:

1. Log on to the Portal server.
2. Go to `<PORTAL_APTARE_HOME>/updates` location and copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgrader-linux.zip` to a temporary location on any other server or Data Collector server directly.
   - For Data Collector on Windows, copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgrader-windows.zip`.
   - For Data Collector on Linux, copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgrader-linux.zip`.
3. Log on to Data Collector server and copy `aptare_dc_upgrader-<OS>.zip` from temporary location to `<DC_APTARE_HOME>/upgrade/bundles`.
4. Remove all `*.properties` files from the `<DC_APTARE_HOME>/upgrade` directory
5. Remove `restore.txt` file from `<DC_APTARE_HOME>/upgrade` directory
6. Upgrade either from the Portal (recommended) or from the Data Collector server as described in the procedures below.
7. Option-1 (recommended): Upgrade the IT Analytics Portal.
   - Login to the Portal.
   - Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector appears online.
   - Go to **Admin** > **Data Collection** > **Collector Updates**
   - Select the Data Collector for which the Upgrade Manager component needs to be upgraded.
   - Click **Update Upgrade Manager**.
     The upgrade takes up to 15 minutes to complete.
8. Option-2: Upgrade the Data Collector server:
   - Log on to the Data Collector server.
   - For Data Collector in Windows, open the command prompt as an administrator user and run:

     ```
     <DC_APTARE_HOME>/mbs/bin/downloadlib.bat
     ```

   - For Data Collector in Linux, as a root user run:

     ```
     <DC_APTARE_HOME>/mbs/bin/downloadlib.sh
     ```

The upgrade takes up to 15 minutes to complete.

Upgrade the Data Collector component which is the aptare.jar file

To upgrade the Data Collector component:

1. Log on to the Portal server and go to `<PORTAL_APTARE_HOME>/dc_upgraders/<version>/<OS>`.
2. Copy `aptare.jar` to a temporary location on any other server or Data Collector server directly.
3. Log on to the Data Collector server.
4. Copy `aptare.jar` from the temporary location to `<DC_APTARE_HOME>/upgrade/bundles`.
5. Rename `aptare.jar` to `dc_upgrader.<version>.zip`.

   For example, if <version> is 11.3.1.02, then file name will be `dc_upgrader.11.3.1.02.zip`
6. Remove all `*.properties` files from the `<DC_APTARE_HOME>/upgrade` directory
7. Remove `restore.txt` file from `<DC_APTARE_HOME>/upgrade` directory
8. Upgrade the Data Collector component either from the Portal (recommended) or from the Data Collector server as described in the procedures below.

To upgrade from IT Analytics Portal:

1. Login to the Portal.
2. Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector appears online.
3. Go to **Admin** > **Data Collection** > **Collector Updates** and select the Data Collector for which the component needs to be upgraded.
4. Select **Upgrade aptare.jar**.

   The upgrade takes up to 15 minutes to complete.

To upgrade from the Data Collector server:

1. Log on to the Data Collector server.
2. For Data Collector in Windows, open the command prompt as an administrator user and run:

   ```
   <DC_APTARE_HOME>/mbs/bin/downloadlib.bat
   ```

3. For Data Collector in Linux, as a root user run:

   ```
   <DC_APTARE_HOME>/mbs/bin/downloadlib.sh
   ```

   The upgrade takes up to 15 minutes to complete.

Upgrade the Upgrade Manager and Data Collector components together

To upgrade both Upgrade Manager and Data Collector components together:

1. Log on to the Portal server.
2. Go to `<PORTAL_APTARE_HOME>/updates` location and copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgrader-<OS>.zip` to a temporary location on any other server or Data Collector server directly.
3. For Data Collector on Windows, copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgraders-windows.zip` to a temporary location on any other server or Data Collector server directly.
4. For Data Collector on Linux, copy `<PORTAL_APTARE_HOME>/updates/aptare_dc_upgrader-linux.zip` to a temporary location on any other server or Data Collector server directly.
5. Go to `<PORTAL_APTARE_HOME>/dc_upgrades/<version>/<os>` location, and copy `aptare.jar` to a temporary location on any other server or to the Data Collector server directly.
6. Log on to Data Collector server and copy `aptare_dc_upgrader-<OS>.zip` from the temporary location to `<DC_APTARE_HOME>/upgrade/bundles`.
7. Copy `aptare.jar` from the temporary location to `<DC_APTARE_HOME>/upgrade/bundles`.

8. Rename `aptare.jar` to `dc_upgrader.<version>.zip`. This <version> is the IT Analytics version from which `aptare.jar` was copied from the Portal server.

   For example, if <version> is 11.3.1.02, then file name will be `dc_upgrader.11.3.1.02.zip`.

9. Remove all `*.properties` files from the `<DC_APTARE_HOME>/upgrade` directory
10. Remove `restore.txt` file from `<DC_APTARE_HOME>/upgrade` directory
11. Upgrade the Data Collector component either from the Portal (Option-1 and recommended) or from the Data Collector server (Option-2) as described in the procedures below.

Option-1: To upgrade from IT Analytics Portal (recommended):

1. Login to the Portal.
2. Go to **Admin** > **Data Collection** > **Collector Administration** and verify whether the Data Collector appears online.
3. Go to **Admin** > **Data Collection** > **Collector Updates** and select the Data Collector for which the component needs to be upgraded.
4. Select **Upgrade Both**.

   The upgrade takes up to 15 minutes to complete.

Option-2: To upgrade from the Data Collector server:

1. Log on to the Data Collector server.
2. For Data Collector in Windows, open the command prompt as an administrator user and run:

   ```
   <DC_APTARE_HOME>/mbs/bin/downloadlib.bat
   ```

3. For Data Collector in Linux, as a root user run:

   ```
   <DC_APTARE_HOME>/mbs/bin/downloadlib.sh
   ```

   The upgrade takes up to 15 minutes to complete.

Upgrade logs and upgrade related database views

Logs:

- Upgrade Manager upgrade logs:

  ```
  <DC_APTARE_HOME>/mbs/logs/watchdog.log
  ```

- Data Collector upgrade logs:
  - Download of Data Collector upgrade bundle and verification related:

    `<DC_APTARE_HOME>/mbs/logs/watchdog.log`

  - For IT Analytics version 11.3.02 and later:

    `<DC_APTARE_HOME>/upgrade/logs`

    Note: For older releases of IT Analytics - <DC_APTARE_HOME>/upgrade/upgradeManager/logs.

Database views

- **apt_v_system_upgrade**: High level upgrade status
  - The **Component_Name** column indicates the Data Collector server.
  - The **Message From** column indicates if it is a Data Collector component or Upgrade Manager component upgrade.
    - If **Message From** is `Super_Upgrader` - The status is related to "Upgrade Manager" component upgrade.
    - If **Message From** is `Upgrade_Manager` - The status is related to "Data Collector" component upgrade.
- **apt_v_system_upgrade_detail**: Detailed upgrade messages for a particular upgrade session.

Resolve file lock issue on Windows host during Data Collector upgrade

Data Collector can detect files in use during upgrade on a Windows host and can kill processes holding these files before proceeding with the upgrade.

To make use of this feature:

1. Download a third-party Handle utility from Microsoft site: https://learn.microsoft.com/en-us/sysinternals/downloads/handle.
2. Unzip the file and copy its contents to the default location `C:\Program Files\Handle`.
3. If you want to copy at a custom location:
   - Make sure the custom location appears as `C:\<CustomFolder>\Handle`.

- On the IT Analytics Portal, navigate to **Admin** > **Advanced** > **Parameters** and add the parameter **DC_UPGRADE_HANDLE_UTILITY_PATH**. Set its value as the custom location.

4 If the Handle utility is located correctly, then the detected file locking process is killed automatically during the Data Collector upgrade by default.

To prevent the file locking process from being killed automatically during the Data Collector upgrade, go to **Admin** > **Advanced** > **Parameters** on the IT Analytics Portal and set the parameter **DC_UPGRADE_UPGRADE_KILL_FILE_LOCKING_PROCESSES** value as **N**.

5 Initiate the Data Collector upgrade.

Note: The default values of **DC_UPGRADE_HANDLE_UTILITY_PATH**: C:\Program Files\Handle and **DC_UPGRADE_KILL_FILE_LOCKING_PROCESSES**: Y.

Chapter 8

Clustering Data Collectors with VCS and Veritas NetBackup (RHEL)

This chapter includes the following topics:

- Clustering Data Collectors with VCS and Veritas NetBackup (RHEL)
- Prerequisites
- Getting started with Data Collector clustering
- Configuring the Data Collector
- Upgrading a clustered Data Collector
- Considerations when Data Collector is pointing to Alta Domain Management

Clustering Data Collectors with VCS and Veritas NetBackup (RHEL)

These instructions cover configuring IT Analytics data collectors with Veritas Infoscale Availability (VCS) with NetBackup running on Red Hat Enterprise Linux.

Prerequisites

- Veritas Cluster Server is installed and configured.
- Veritas NetBackup is installed and configured on the Veritas Infoscale Availability (VCS) in a clustered mode.

- Veritas NetBackup data volume resides on a volume shared across cluster nodes.
- A shared storage of sufficient capacity is configured across the cluster nodes. The size of the shared storage depends on the data to be collected. Refer to *IT Analytics Certified Configuration Guide* for recommended storage size.
- The shared storage can be either a Veritas Infoscale Volume Manager (VxVM) or a disk. If the storage is under VxVM, ensure that Disk group and Volumes are already created.
- Ensure that file system is created on the shared storage.
- Ensure that the file system is mounted on a mount point. The Data Collector will be installed on this file system.
- Passwordless SSH for root user must be configured among the cluster nodes for installation and upgrade to work properly.

Getting started with Data Collector clustering

1. Install the Veritas NetBackup Data Collector on shared volume attached to the active node.

   Refer to the *Cohesity IT Analytics Data Collector Installation Guide on Linux* for the general prerequisites for the deployment.

2. To install the Data Collector on VCS cluster environment, execute the below command on the node where the shared storage is mounted. Mount the ISO image that you downloaded.

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

3. Substitute the name of the downloaded ISO image.

   ```
   cd /
   ```

   If you are planning to use only the NetBackup, NetBackup Appliance or the Backup Exec policies with the Data Collector, then start the installer as below:

   ```
   /mnt/diska/dc_installer.sh -i <mountpoint of shared storage> -n
   -C vcs
   ```

   In case you wanted to use all the policies that Data Collector supports, then start the installer as below:

```
/mnt/diska/dc_installer.sh -i <mountpoint of shared storage> -C vcs
```

The installer also places the required files on the remote cluster nodes using the passwordless SSH setup.

The installer will deploy the Data Collector binaries on the shared storage and create the required cluster configuration. Installer detects the block device configured with the mount point and use this information while creating cluster configuration. The Data Collector creates an online local firm group dependency with NetBackup service group. The installer also places the required files on the remote cluster nodes using the passwordless SSH setup.

The Data Collector refers the cluster configuration file `<Mount point>/analyticscollector/mbs/conf/cluster_config.properties` while creating the configuration.

The script `<Mount point>/analyticscollector/mbs/bin/create_cluster_config.sh` can be used to create a cluster configuration in case user needs to re-create a cluster configuration for the Data Collector. Similarly, `<Mount point>/analyticscollector/mbs/bin/clean_cluster_config.sh` can be used to clean up the cluster configuration in case the user needs to delete the cluster configuration for the Data Collector.

Configuring the Data Collector

The Data Collector can be configured using:

- NetBackup Web UI if the NetBackup version is 10.4 or later.
- Installer with `-c` option and the `responsefile`.
  See the *Configure Data Collector manually for Cohesity NetBackup* in any of the Data Collector installation guides.

Upgrading a clustered Data Collector

Upgrading a Data Collector using `downloadlib` or auto-upgrade mechanism does not need any specific action other than ensuring passwordless SSH configuration among cluster nodes.

Manage Data Collector cluster configuration during NetBackup Upgrade (RHEL)

Upgrade of NetBackup does not need any special action of the Data Collector.

Considerations when Data Collector is pointing to Alta Domain Management

If the Netbackup domain is removed from Alta Domain Management, as a part of un-configuration, aptare_agent services will be stopped. This causes the Data Collector service group to fault.

Therefore, you must freeze the Data Collector service group before removing a NetBackup domain from Alta Domain Management.

Chapter 9

Clustering Data Collectors with VCS and Veritas NetBackup (Windows)

This chapter includes the following topics:

- Clustering Data Collectors with VCS and Veritas NetBackup (Windows)
- Prerequisites
- Getting Started with Data Collector Clustering
- Main.cf
- Upgrading a Clustered Data Collector
- Manage cluster configuration during NetBackup upgrade (Windows)
- Uninstall cluster Data Collector

Clustering Data Collectors with VCS and Veritas NetBackup (Windows)

These instructions cover configuring IT Analytics data collectors on a Veritas Infoscale Availability (VCS) with NetBackup running on Microsoft Windows.

Prerequisites

- Veritas NetBackup is installed and configured on the Veritas Infoscale Availability (VCS) with clustered nodes in a clustered mode.

- Veritas NetBackup data volume resides on a volume shared across cluster nodes.
- Data Collector is installed on a volume shared across cluster nodes.
- Disk groups created are dynamic clustered disk groups.

Getting Started with Data Collector Clustering

Data Collector clustering:

1. Install the Veritas NetBackup Data Collector on shared volume attached to the active node using below options:
   - Flag option: Run the command:

     ```
     silentinstall.cmd /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y
      /INSTALL_PATH:<shared_disk_dc_installation_path>
     /CLUSTER_TYPE:VCS
     ```

   - Cluster configuration file option: The installer has `vcsclusterconfig.cmd` file present. Update the configuration properties and run the installer using command:

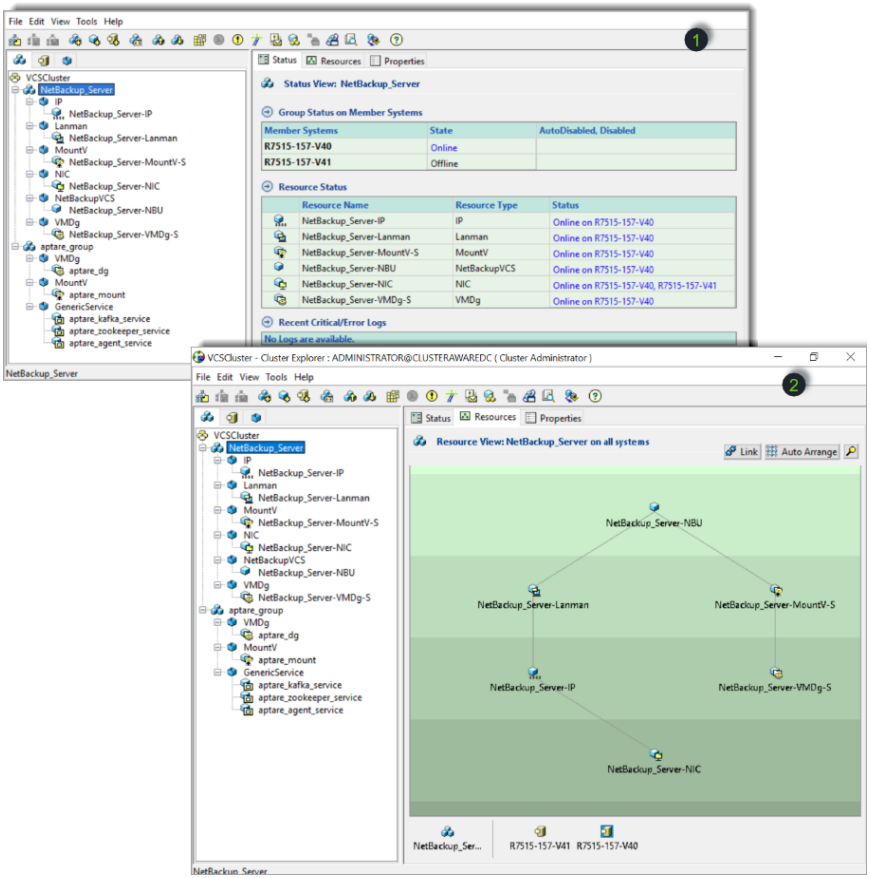
     ```
     silentinstall.cmd /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y
      /CLUSTER_CONFIG_PATH:<vcsclusterconfig.cmd-file-path>
     ```

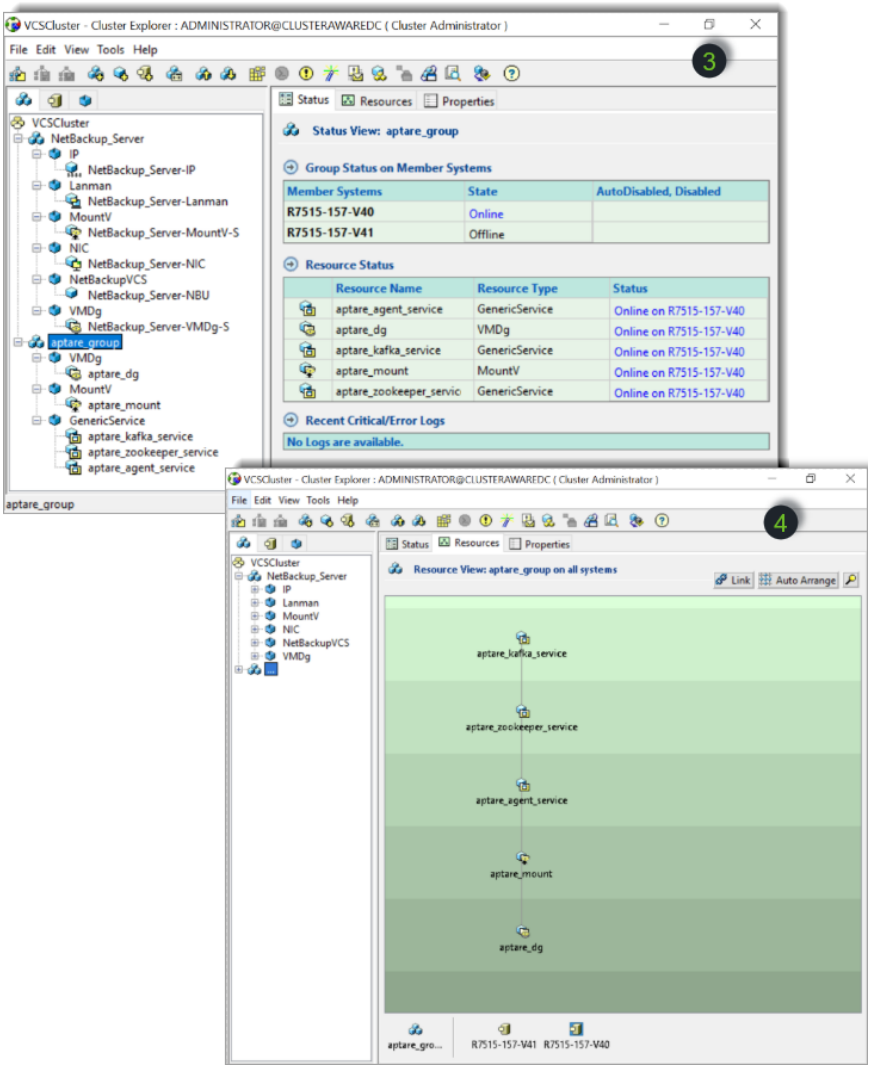
Note: Both the above commands install Data Collector on both active and passive nodes.

2 Configure the Data Collector either using NetBackup Web UI or using the silent configuration option:

```
silentinstall.cmd /INSTALL_TYPE:CONFIG
/RESPFILE:<response_file_path>
```

3 The cluster configuration for NetBackup and Data Collector after installation and configuration of Data Collector:





Main.cf

The main.cf for the previous configuration is as follows. Please note, the following configuration uses example values as required:

```
include "types.cf"

include "C:\Program Files\Veritas\Cluster
```

```
Server\conf\config\NetBackupVCSTypes.cf"
cluster VCSCluster (
ProtocolNumber = 11000
SecureClus = 1
)

system R7515-157-V40 (
)

system R7515-157-V41 (
)

group aptare_group (
SystemList = { R7515-157-V40 = 1, R7515-157-V41 = 2 }
AutoStartList = { R7515-157-V40, R7515-157-V41 }
)

GenericService aptare_kafka_service (
ServiceName = AptareDCKafka
)

GenericService aptare_zookeeper_service (
ServiceName = AptareDCZooKeeper
)

GenericService aptare_agent_service (
ServiceName = aptareagent
)

MountV aptare_mount (
MountPath = "T:"
VolumeName = DCVol
VMDGResName = aptare_dg
)

VMDg aptare_dg (
DiskGroupName = DCDG
DGGuid = fbc46fd3-2ab3-48cc-8274-3342b85271e8
)

requires group NetBackup_Server online local firm
aptare_mount requires aptare_dg
aptare_kafka_service requires aptare_zookeeper_service
```

```
aptare_zookeeper_service requires aptare_agent_service
aptare_agent_service requires aptare_mount

// resource dependency tree
//
// group aptare_group
// {
// GenericService aptare_kafka_service
//     {

//     GenericService aptare_zookeeper_service
//         {
//         GenericService aptare_agent_service
//             {
//             MountV aptare_mount
//                 {
//                 VMDg aptare_dg
//                 }
//             }
//         }
//     }
// }


group NetBackup_Server (
SystemList = { R7515-157-V40 = 1, R7515-157-V41 = 2 }
AutoStartList = { R7515-157-V40, R7515-157-V41 }
)


IP NetBackup_Server-IP (
Address = "10.221.148.250"
SubNetMask = "255.255.240.0"
MACAddress @R7515-157-V40 = 00-50-56-BB-D3-77
MACAddress @R7515-157-V41 = 00-50-56-BB-7D-D0
)

Lanman NetBackup_Server-Lanman (
VirtualName = r7515-157-v42
IPResName = NetBackup_Server-IP
)
```

```
MountV NetBackup_Server-MountV-S (
MountPath = "S:\\"
VolumeName = NBUVol
VMDGResName = NetBackup_Server-VMDg-S
)

NIC NetBackup_Server-NIC (
MACAddress @R7515-157-V40 = 00-50-56-BB-D3-77
MACAddress @R7515-157-V41 = 00-50-56-BB-7D-D0
)

NetBackupVCS NetBackup_Server-NBU (
ResourceOwner = unknown
ServerName = r7515-157-v42
ServerType = NBU
)

VMDg NetBackup_Server-VMDg-S (
DiskGroupName = NBUDG
DGGuid = f2f47ff0-9f95-41fa-b9f5-df97a5b0788c
)

NetBackup_Server-IP requires NetBackup_Server-NIC
NetBackup_Server-Lanman requires NetBackup_Server-IP
NetBackup_Server-MountV-S requires NetBackup_Server-VMDg-S
NetBackup_Server-NBU requires NetBackup_Server-MountV-S
NetBackup_Server-NBU requires NetBackup_Server-Lanman

// resource dependency tree
//
// group NetBackup_Server
// {
// NetBackupVCS NetBackup_Server-NBU
//     {
//     MountV NetBackup_Server-MountV-S
//         {
//         VMDg NetBackup_Server-VMDg-S
//         }
//     Lanman NetBackup_Server-Lanman
//         {
//         IP NetBackup_Server-IP
//             {
//             NIC NetBackup_Server-NIC
```

```
//                }
//           }
//      }
// }
```

Upgrading a Clustered Data Collector

Irrespective of whether the Data Collector upgrade is done manually or through auto-upgrade, manual intervention is not required. The cluster Data Collector upgrade is taken care for both the paths.

Manage cluster configuration during NetBackup upgrade (Windows)

During NetBackup upgrade, the VCS cluster configurations are removed and recreated. Follow these steps before you upgrade NetBackup:

1. Invoke the script to clean Data Collector cluster configuration:

   ```
   <APTARE_HOME>\mbs\bin\vcscleanclusterconfig.bat
   ```

2. Upgrade NetBackup.
3. Invoke the script to recreate Data Collector cluster configuration:

   ```
   <APTARE_HOME>\mbs\bin\vcscreateclusterconfig.bat
   ```

Uninstall cluster Data Collector

Cluster Data Collector can uninstalled from the node where it was installed. Before you uninstall, ensure the shared drive where the Data Collector was installed is imported on the node from where it was installed. If you uninstall the Data Collector without importing the shared drive, the uninstallation will complete without a complete cleanup. Follow the manual steps provided below to perform the cleanup.

Use any one option to uninstall cluster Data Collector:

- Invoke `C:\ProgramData\Veritas\NetBackup IT Analytics\DC\silenuninstall.cmd .`
- Uninstall from **Add/Remove programs** by clicking on **IT Analytics Data Collector** program.

To perform a manual cleanup:

1. Delete aptare service group cluster configuration.
2. Import Data Collector disk and delete data collector files.
3. Delete symbolic link `C:\Program Files\Veritas\AnalyticsCollector` from both nodes.
4. Stop and Delete **aptareagent**, **AptareDCKafka**, and **AptareDCZookeeper** services using commands: `sc stop <service_name>` and `sc delete <service_name>`.

Chapter 10

Install and configure IT Analytics Data Collector on MSCS environment

This chapter includes the following topics:

- Cluster Data Collectors with MSCS on Windows
- Perform cluster configurations
- Upgrade IT Analytics Data Collector in MSCS
- Uninstall IT Analytics Data Collector
- Steps to perform before and after NetBackup upgrade

Cluster Data Collectors with MSCS on Windows

Prerequisites

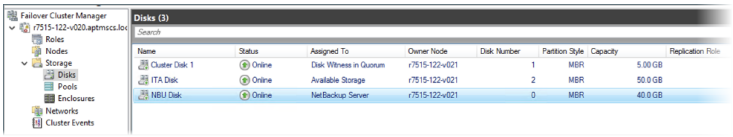
- Microsoft Cluster Server (MSCS) is already provisioned.
- NetBackup primary server is already clustered under MSCS and online on Node1.
- A disk of at-least 100 GB size is attached to all nodes in the cluster - to be used to install IT Analytics Data Collector.

Installing and configuring IT Analytics Data Collector in MSCS

Steps to be performed on Node1:

1. Verify whether a shared disk of minimum size of 100 GB is attached to Node1.
2. Create storage resource for the disk in the cluster. (**Storage** > **Disks** > **Actions** > <Disk name>)

   In the image below **ITA Disk** represents the shared disk for the Data Collector.



3. Get the shared disk (**ITA Disk**) online on Node1 and identify the drive letter.

   Note: Ensure the disk has the same drive letter across all cluster nodes.

4. Optional: Add Agent URL to `C:\Windows\System32\drivers\etc\hosts` file. This step is required if the agent URL is not updated on the DNS.

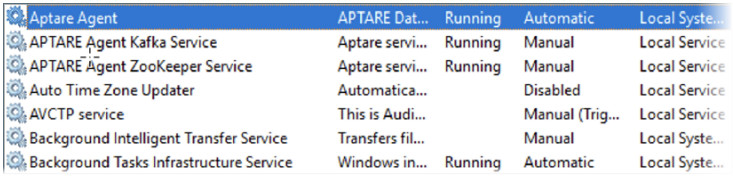
   Example:

   ```
   10.xx.yy.zz   itanalyticsportal.vxindia.veritas.com
   itanalyticsportal
   10.xx.yy.zz itanalyticsagent.vxindia.veritas.com itanalyticsagent
   ```

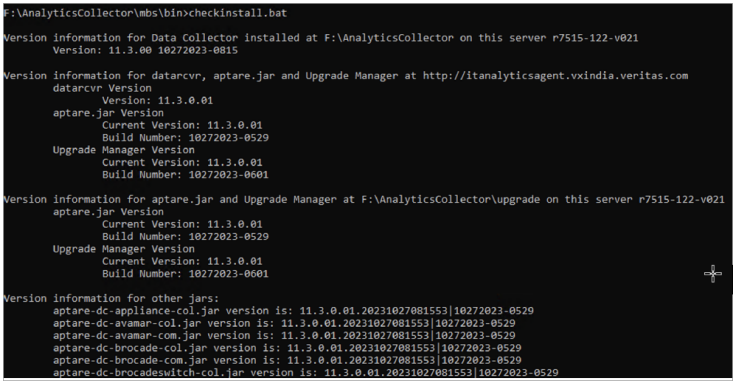
5. Install and Configure IT Analytics Data Collector on new shared drive (**ITA Disk**).

   See “Install Data Collector Software on Windows” on page 75.

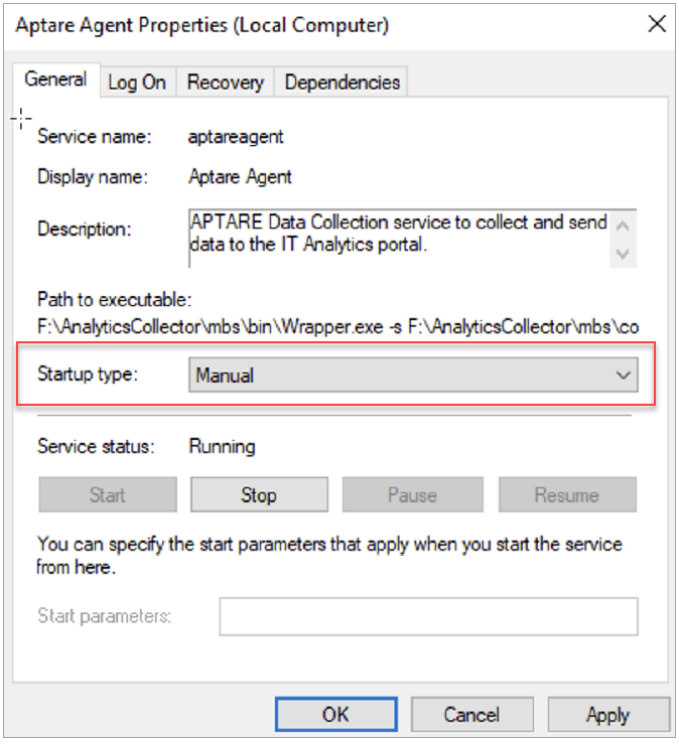
6. Verify that services Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper are created on services panel and are online.



7 Execute `checkinstall.bat` utility and ensure it is returning SUCCESS. The `checkinstall.bat` utility will be available at `<Shared disk drive>\veritas\AnalyticsCollector\mbs\bin`.



8 Change the service type for Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper services from **Automatic** to **Manual** from services panel.



9 Stop the services for Aptare Agent, Aptare Agent Kafka, and Aptare Agent Zookeeper on Node1.

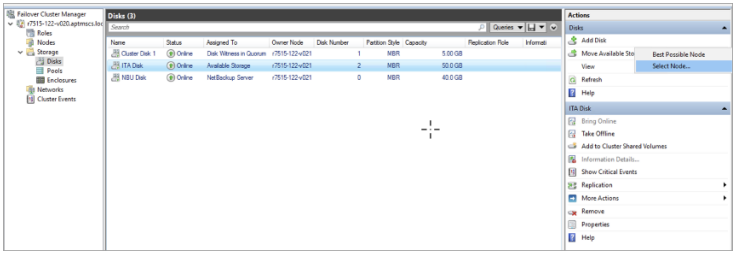
10 Move the storage resource to Node 2 on the cluster. Go to **Failover Cluster Manager** > **Storage** > **Disks** > select the shared disk (**ITA disk**) > on the right side below **Actions** > **Move Available Storage** > **Select Node**> select **Node 2**.

Steps to perform on Node 2:

1 Ensure to move the IT Analytics shared disk (**ITA disk**) from Node 1 to Node 2. Go to **FailOver cluster manager** > **Storage** > **Disks** > select the shared disk (**ITA Disk**).

2 Verify that the shared disk (**ITA disk**) is online and available on the Node 2.

3 On the right side below **Actions**, select **Move Available Storage** > **Select Node** > **Select Node 2**.



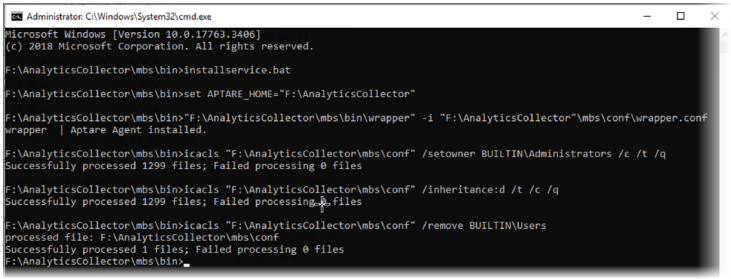
4 Optional: Add Agent URL to `C:\Windows\System32\drivers\etc\hosts` file. This step is required if the agent URL is not updated on the DNS.

Example:

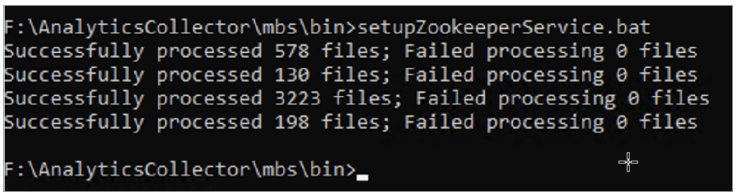
```
10.xx.yy.zz  itanalyticsportal.vxindia.veritas.com
itanalyticsportal
10.xx.yy.zz  itanalyticsagent.vxindia.veritas.com itanalyticsagent
```

5 Create services for Aptare Agent, Aptare Kafka, and Aptare ZooKeeper by executing:

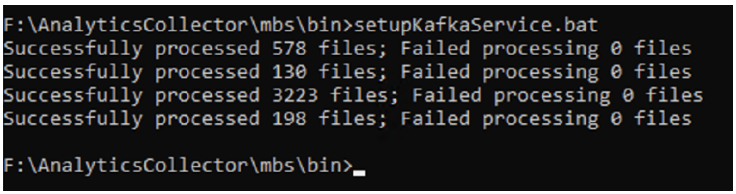
- For Aptare Agent: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\installservice.bat`.



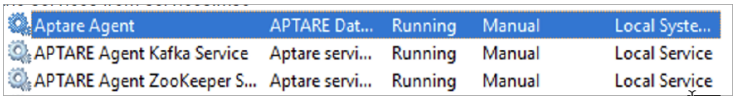
- For APTARE Agent ZooKeeper Service: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\setupZookeeperService.bat`.



- For APTARE Agent Kafka Service: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\setupKafkaService.bat`.



- Change the service type from Automatic to manual from services panel.
- Start the services from `services.msc`.

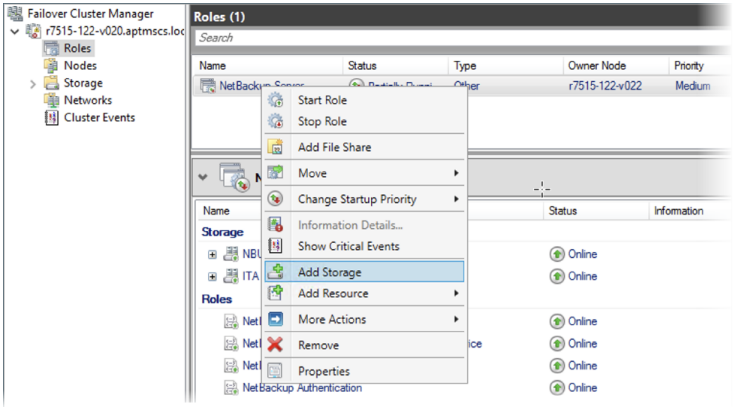


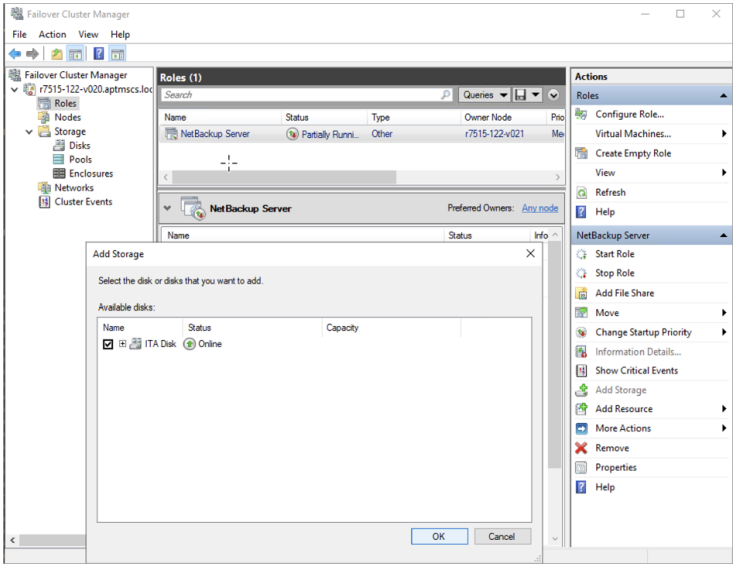
6 Execute `checkinstall` utility and ensure it returns SUCCESS. The `checkinstall.bat` utility will be available at `<Shared disk drive>:/veritas/AnalyticsCollector/mbs/bin`.

7 Stop the services for Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper on Node 2.

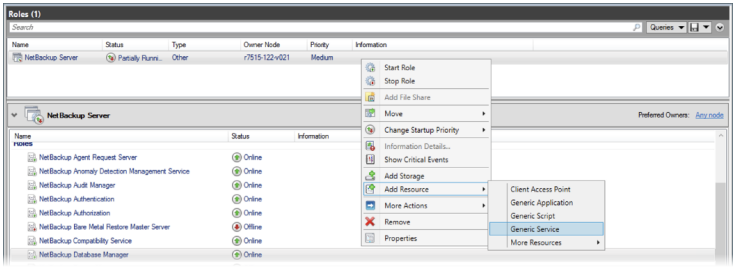
Perform cluster configurations

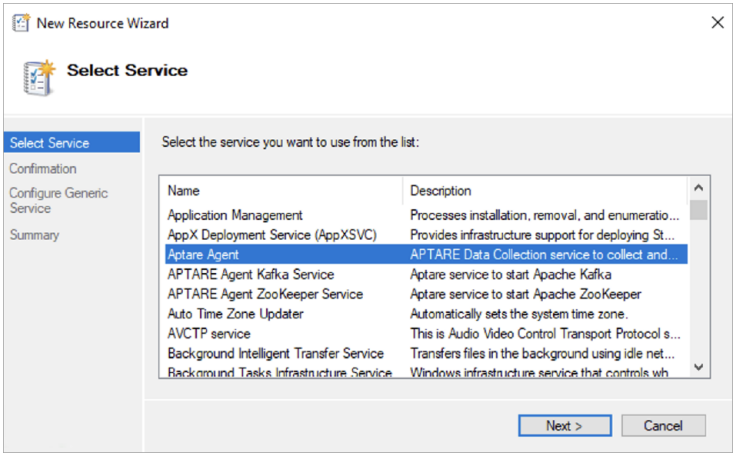
1. Ensure NetBackup Server Role is online on Node 1.
2. Update NetBackup Role:
   - Add IT Analytics shared disk (**ITA Disk**) into NetBackup Server Role from **Failover Cluster Manager**. Open **Failover Cluster Manager** > **Roles** > right-click on **NetBackup Server Role** > **Add Storage** > **ITA Disk** > **OK**.

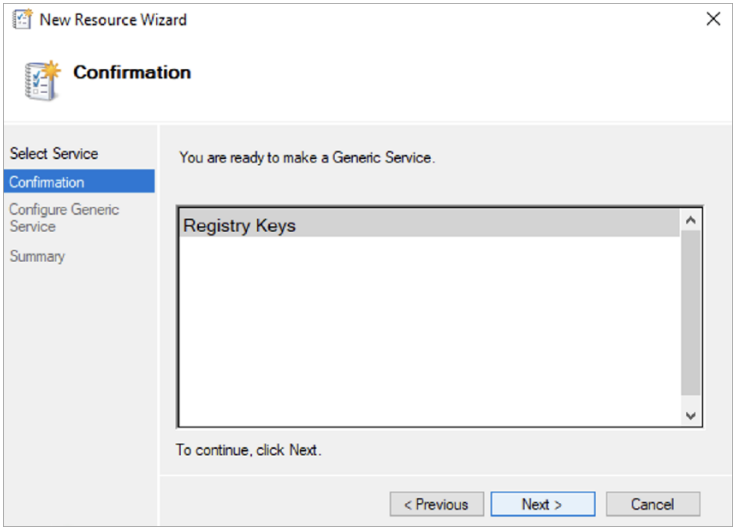


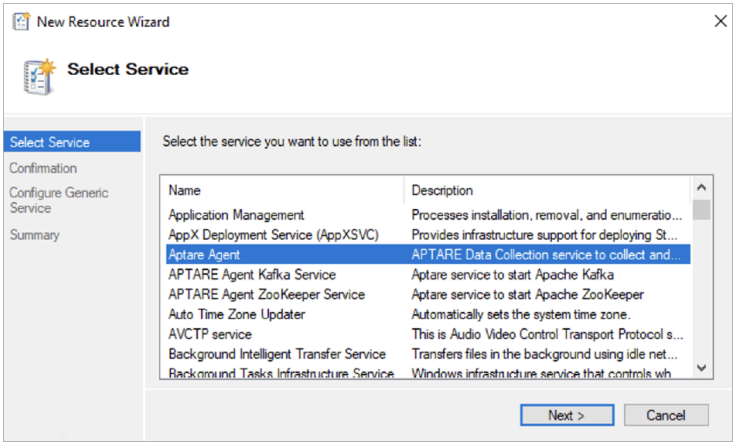


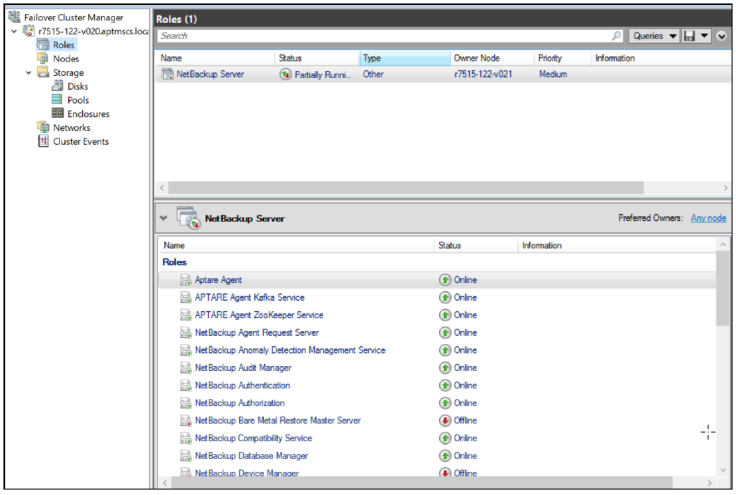
   - Add Roles for each IT Analytics service Aptare Agent, Kafka, and ZooKeeper to it. **Roles** > right-click on **NetBackup Server Role** > **Add Resource** > **Generic services**.


Roles (1)
Search
Queries
Name
Status
Type
Owner Node
Priority
Information
NetBackup Server
Partially Runni...
Other
r7515-122-v021
Medium
Start Role
Stop Role
Add File Share
Move
Change Startup Priority
Information Details...
Show Critical Events
Add Storage
Add Resource
More Actions
Remove
Properties
Client Access Point
Generic Application
Generic Script
Generic Service
More Resources
NetBackup Server
Preferred Owners:
Any node
Name
Status
Information
Roles
NetBackup Agent Request Server
NetBackup Anomaly Detection Management Service
NetBackup Audit Manager
NetBackup Authentication
NetBackup Authorization
NetBackup Bare Metal Restore Master Server
NetBackup Compatibility Service
NetBackup Database Manager
Online
Offline

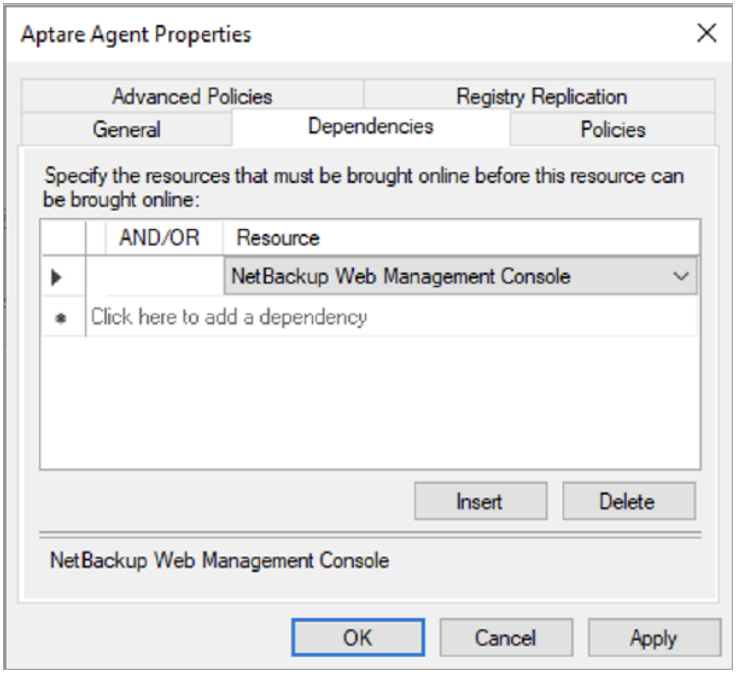

New Resource Wizard
Select Service
Select Service
Confirmation
Configure Generic Service
Summary
Select the service you want to use from the list:
Name
Description
Application Management
Processes installation, removal, and enumeratio...
AppX Deployment Service (AppXSVC)
Provides infrastructure support for deploying St...
Aptare Agent
APTARE Data Collection service to collect and...
APTARE Agent Kafka Service
Aptare service to start Apache Kafka
APTARE Agent ZooKeeper Service
Aptare service to start Apache ZooKeeper
Auto Time Zone Updater
Automatically sets the system time zone.
AVCTP service
This is Audio Video Control Transport Protocol s...
Background Intelligent Transfer Service
Transfers files in the background using idle net...
Background Tasks Infrastructure Service
Windows infrastructure service that controls wh
Next >
Cancel


New Resource Wizard
Confirmation
Select Service
Confirmation
Configure Generic Service
Summary
You are ready to make a Generic Service.
Registry Keys
To continue, click Next.
< Previous
Next >
Cancel

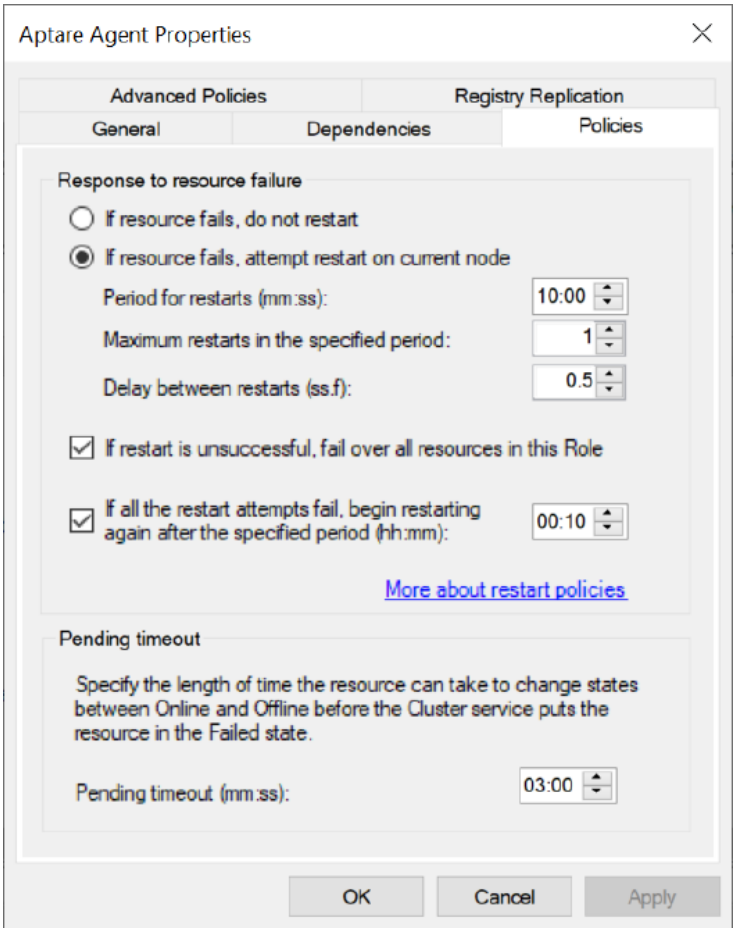




- Create dependency between services Netbackup Web Management Console and Aptare Agent.



- Ensure that the following failure policies are configured as below for Aptare Agent, Kafka, and Zookeeper Roles on NetBackup Role in MSCS cluster. Right-click on **Aptare service** > **Properties** > **Policies**.

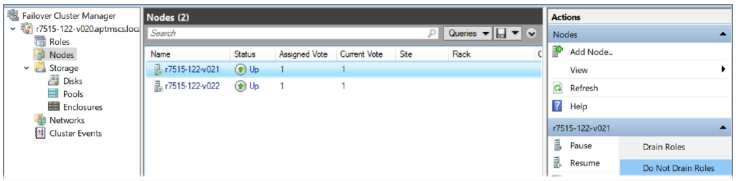


Upgrade IT Analytics Data Collector in MSCS

IT Analytics Data Collector performs auto-upgrade once the Portal is upgraded. As part of auto-upgrade, Data Collector services are stopped, binaries are updated, and then services are started. In order to avoid unwanted service restart/fail-over by MSCS cluster, it is advised to have the following manual interventions.

Before IT Analytics Portal is upgraded, ensure that the following steps are performed on each MSCS clusters where Data Collector is installed.

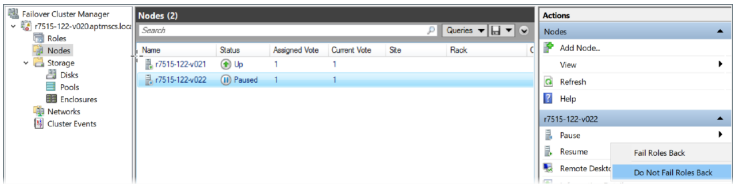
1 Pause the node on which Roles are online with **Do not drain Roles** option in MSCS cluster as given below. This will ensure cluster manager does not initiate failover of Roles when Data Collector upgrade is in progress.



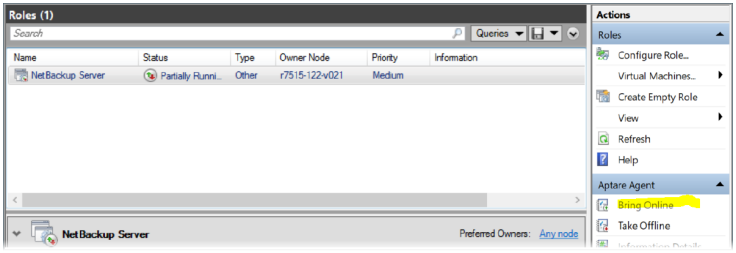
2 Perform Portal upgrade.

3 Once Data Collector contacts the Portal, it will perform auto-upgrade. During the auto-upgrade process, Data Collector services Aptare Agent, Kafka, and Zookeeper will be stopped and cluster detects this and marks the Roles as **Failed**. Once the auto upgrade is successfully completed, services Aptare Agent, Kafka, and ZooKeeper will be started, but the Roles on MSCS for Data Collector will be still marked as **Failed**.

4 Resume the Node that was paused earlier with option "Do not Fail Roles back".



5 For each Aptare Agent, Kafka, and Zookeeper Roles, perform **Bring Online**.



Uninstall IT Analytics Data Collector

1. Delete the Roles for IT Analytics services Aptare Agent, Kafka, and ZooKeeper from MSCS.
2. Identify the node on which "IT Analytics Data Collector" entry is present on the Add/Remove Programs (ARP) on control panel.
3. Fail over the NetBackup Role to other nodes and delete the services from command prompt.

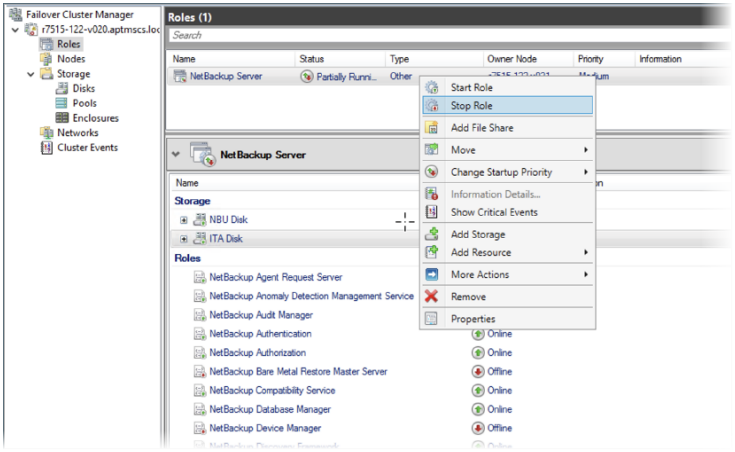
```
#SC DELETE AptareDCKafka
#SC DELETE AptareDCZooKeeper
#SC DELETE AptareAgent
```

4. Failback to the node where ARP entry is present.
5. Perform Uninstall of Data Collector from ARP.

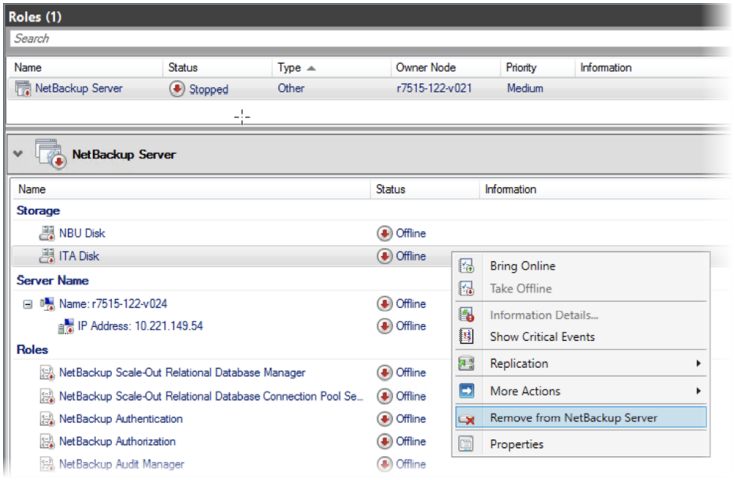
Steps to perform before and after NetBackup upgrade

Steps before upgrading NetBackup:

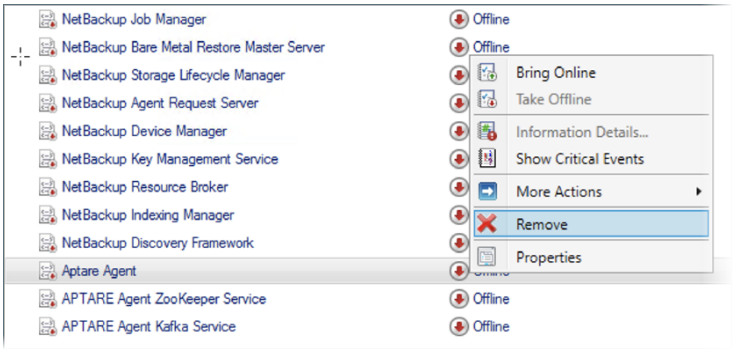
1 Stop the 'NetBackup Server' Role. This will bring down storage disk (both ITA and NetBackup disks) and both NetBackup and Aptare services.



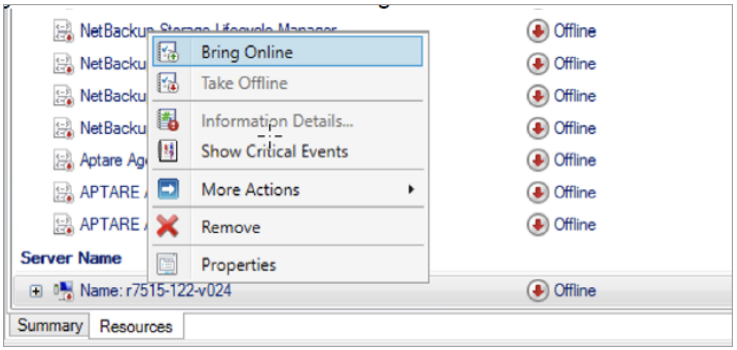
2 Remove IT Analytics disk from NetBackup Server Role.



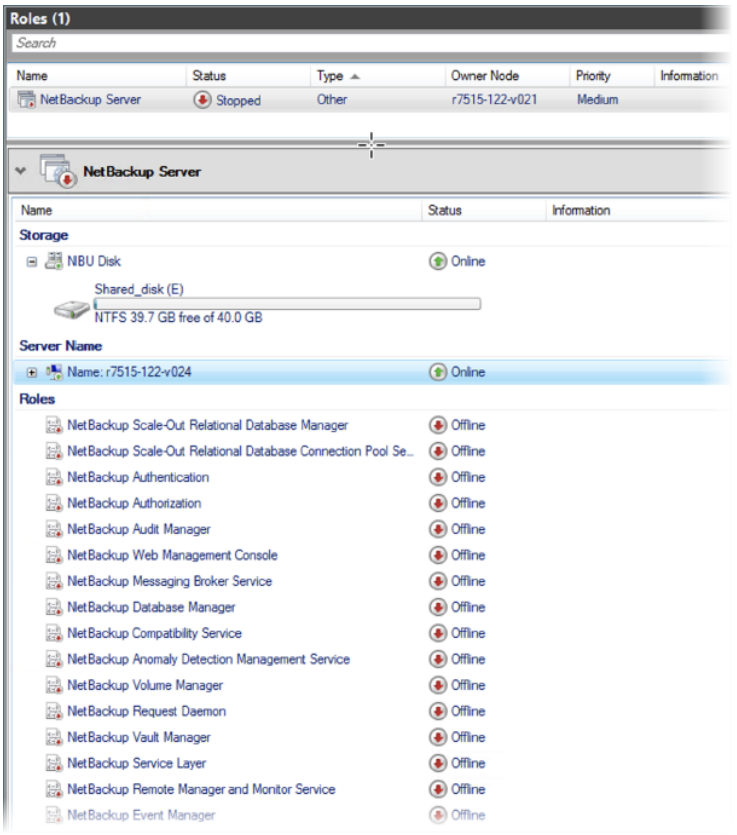
3 Remove Aptare Agent, ZooKeeper and Kafka services from NetBackup Server Role.



4 Bring Server Name online. This will bring NetBackup shared Disk online as well.



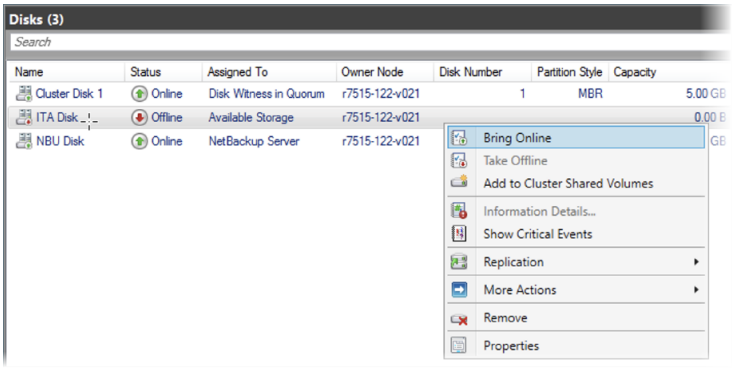
Final look of NetBackup Server Role.



5 Start with NetBackup Upgrade.

Steps after upgrading NetBackup

1 Bring the IT Analytics Disk online. Go to **Disks** > right-click on `ITA Disk` > **Bring online** (on the same node as NetBackup).



2 Now perform the steps from step#2 from section *Perform cluster configurations* .

See “Perform cluster configurations” on page 170.

Chapter 11

Data Collector Policy Migration

This chapter includes the following topics:

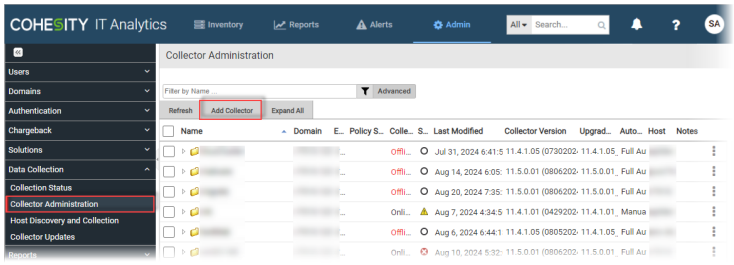
- Migrate NetBackup data collection policy from centralized to distributed Data Collector

Migrate NetBackup data collection policy from centralized to distributed Data Collector

This section details the process for migrating the NetBackup data collection policy performing collection on a centralized Data Collector to implementing Distributed Data collection.

To perform the migration:

1. Login to the IT Analytics Portal.
2. Go to **Admin** > **Data Collection** > **Collector Administration** and add a new Data Collector.



3 Verify whether the Data Collector software is installed on the NetBackup primary server. If the software is installed, the Watchdog process is found running state and in WAIT_INIT mode in the logs. Verify the Watchdog status and Data Collector software installation as follows:

Verify the Watchdog process is running from `<ITA_HOME>/mbs/logs/watchdog.log` and confirm that it is in WAIT_INIT mode.

```
16 Aug 2024 19:33:50:313 INFO  2125701
InstalledCollectorProperties.getCollectorNameProperties - Fetched
 passcode from collect or properties.
16 Aug 2024 19:33:50:314 INFO  2125701
DCRegistrationForNetbakupUtils.executeServices - Executing
services STOP_KAFKA other than aptare agent.
16 Aug 2024 19:33:50:315 INFO  2125701
DCRegistrationForNetbakupUtils.getNBUHome - NBU Home location -
/usr/openv
16 Aug 2024 19:33:50:315 INFO  2125701
ServicesCommandGenerator.getWorkingDirectory - Directory is:
/usr/openv/netbackup/bin
16 Aug 2024 19:33:50:316 INFO  2125701
DCRegistrationForNetbakupUtils.getNBUHome - NBU Home location -
/usr/openv
16 Aug 2024 19:33:50:316 INFO  2125701
ServicesCommandGenerator.getWorkingDirectory - Directory is:
/usr/openv/netbackup/bin
16 Aug 2024 19:33:50:316 INFO  2125701
ServicesCommandGenerator.addParameters - Adding parameters...
16 Aug 2024 19:33:50:317 INFO  2125701
ServicesCommandGenerator.addParameters - Adding stopkafka
parameter to nbcmdrun
16 Aug 2024 19:33:50:317 INFO  2125701
ServicesCommandGenerator.printCommand - Command to execute is:
/usr/openv/netbackup/bin/nbcmdrun stopkafka
16 Aug 2024 19:33:51:578 INFO  2125701
DCRegistrationForNetbakupUtils.executeServices - Process id =
2125772 []
16 Aug 2024 19:33:51:579 INFO  2125701
DCRegistrationForNetbakupUtils.executeServices - Exit status of
STOP_KAFKA is : 0
16 Aug 2024 19:33:51:579 INFO  2125701 WatchDog.main  - ITA Data
 Collector in WAIT-INIT mode
```

If the Data Collector is not installed, then install the Data Collector on NetBackup host without configuration.

To install the Data Collector:

- Download and mount the Data Collector ISO file.
- On Windows:

  Install the Data collector using `silentinstall.cmd` and follow the installation prompt. You can install the Data Collector in the following options:

  - Install at the default location:

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

  - Install at a custom location:

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

- On Linux:
  - Install at the default location:

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

  - Install at a custom location:

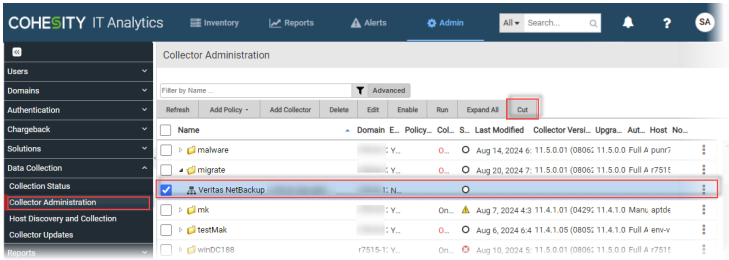
    ```
    # <path to mount>/dc_installer.sh -i <user selected path>
    -n
    Example:
    # <path to mount>/dc_installer.sh -i /usr/openv -n
    ```

4 Configure the IT Analytics Data Collector (created at Step 2) with NetBackup. Depending on your NetBackup version follow the procedures in the respective topics:

- Refer to *Step-3: Configure the Data Collector from the NetBackup Web UI* in See "Configure Data Collector on non-clustered NetBackup 10.4 and later primary server" on page 18.

- Refer to *Step 2A: Configure the IT Analytics Data Collector manually for NetBackup* in See "Configure Data Collector on non-clustered NetBackup 10.1.1, 10.2, 10.2.01, 10.3 or 10.3.0.1 primary server" on page 26.

5 Migrate the NetBackup collection policy to the new Data Collector.

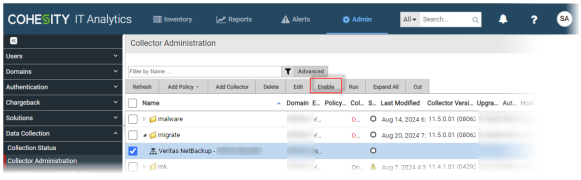


- Go to **Admin** > **Data Collection** > **Collector Administration**.
- Select the NetBackup collection policy and click **Cut**.
- Select the target Data Collector and click **Paste**.

6 Edit the NetBackup collection policy:

- Go to **Admin** > **Data Collection** > **Collector Administration** .
- Select the NetBackup collection policy and click **Edit**.
- Clear the **Primary Server Login Details** field and change the **Collection Method** to **Data Collector installed on NetBackup Primary Server**.
- Click **OK** to save the changes.

7 Enable the NetBackup policy: Go to **Admin** > **Data Collection** > **Collector Administration**, select the NetBackup collection policy, and click **Enable**.



Chapter 12

Pre-Installation setup for Veritas NetBackup appliance

This chapter includes the following topics:

- Overview
- Prerequisites for adding Data Collectors (Veritas NetBackup appliance)
- Installation Overview (Veritas NetBackup Appliance)
- Adding a Veritas NetBackup Appliance Data Collector policy

Overview

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

Prerequisites for adding Data Collectors (Veritas NetBackup appliance)

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

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

Installation Overview (Veritas NetBackup Appliance)

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

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

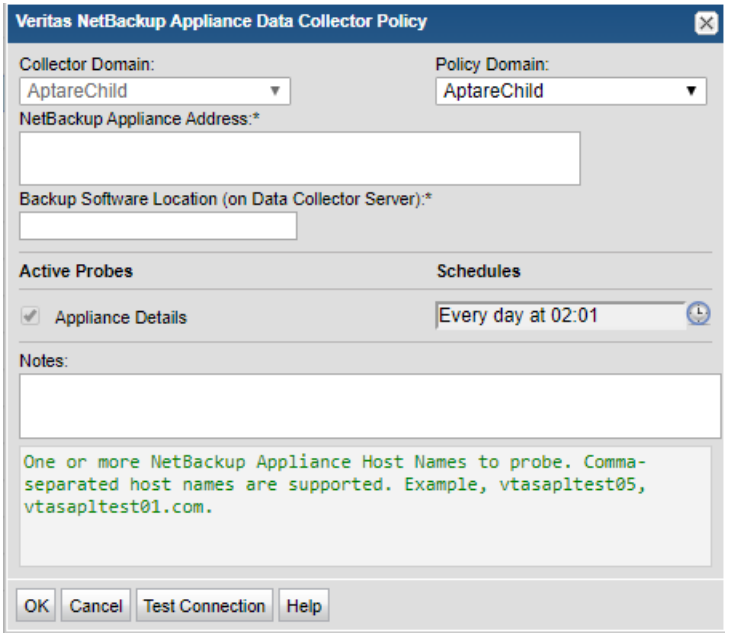
Note: Veritas NetBackup Appliance version 5.3 and above supports MFA enabled data collection.

Adding a Veritas NetBackup Appliance Data Collector policy

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

To add the policy

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



Field	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.

Field	Description
NetBackup Appliance Address**	One or more NetBackup Appliance Servers to probe. Comma-separated host names are supported. For example, nbuapltest05, nbuapltest01.com.
Backup Software Location (on Data Collector Server)*	Backup Software Home Location should either be the root folder or directory where the NetBackup Remote Administration Console software is installed, or the root folder to the netbackup/volmgr folder(s) where the NetBackup software is installed. Default Backup Software Home location for Veritas NetBackup: For Windows: C:\Program Files\Veritas. For Linux: /usr/openv
Appliance Details	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the **Collector Administration** page as a column making them searchable as well.

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. Test Connection also checks that the utility nb_monitor is installed. You can also test the collection of data using the Run functionality available in **Admin > Data Collection > Collector Administration.** This On-Demand data collection run initiates a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. You can also select individual probes and servers to test the collection run.

Chapter 13

Pre-installation setup for Veritas Flex Appliance

This chapter includes the following topics:

- Pre-Installation setup for Cohesity Flex Appliance
- Prerequisites for adding Data Collectors (Veritas Flex Appliance)
- Installation overview (Cohesity Flex Appliance)
- Add a Veritas Flex Appliance policy
- Troubleshoot Veritas Flex Appliance policy configuration

Pre-Installation setup for Cohesity Flex Appliance

With IT Analytics version 11.5 or higher, the Veritas Flex Appliance policy can also be configured with the Distributed Data Collector.

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.

Cohesity Flex Appliance policy consists of three probes - **Appliance Details**, **Performance Statistics**, and **Storage Statistics**. All the probes are independent of each other and can run in different schedules. All the probes collect data from NetBackup Flex Appliance using REST APIs exposed by the appliance. Data is collected for each container and is segregated on basis of appliance and host node on which container is running. The policy collects resource and storage utilization data and hardware details from all the configured appliances and differentiates the collection by appliances and its nodes and containers.

NetBackup Flex Appliance v4.0 supports multi-factor authentication (MFA). A secret key is generated while providing user access to such MFA-enabled appliances and it remains associated with the user credentials. IT Analytics NetBackup Flex Appliance policy requires this secret key for authentication every time it accesses the appliance for data collection.

Supported NetBackup Flex Appliance models

Following NetBackup Flex Appliance models are supported for data collection with Flex Appliance versions 2.0, 2.1, 3.1, 3.2, and 4.0:

- 5150
- 5250
- 5340
- 5350

Prerequisites for adding Data Collectors (Veritas Flex Appliance)

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

Installation overview (Cohesity Flex Appliance)

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

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

3. In the Portal, add the Cohesity Flex Appliance 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 132.
6. Validate the Data Collector installation.

Add a Veritas Flex Appliance 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 *IT Analytics 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.

The data collection form the appliances depends on the availability of the components that expose the appliance stats to the policy probes. The data collection supported for each Flex Appliance version is as indicated below. You need to create an RTD report to view the data. Collection is performed via REST APIs exposed by the Flex Appliance.

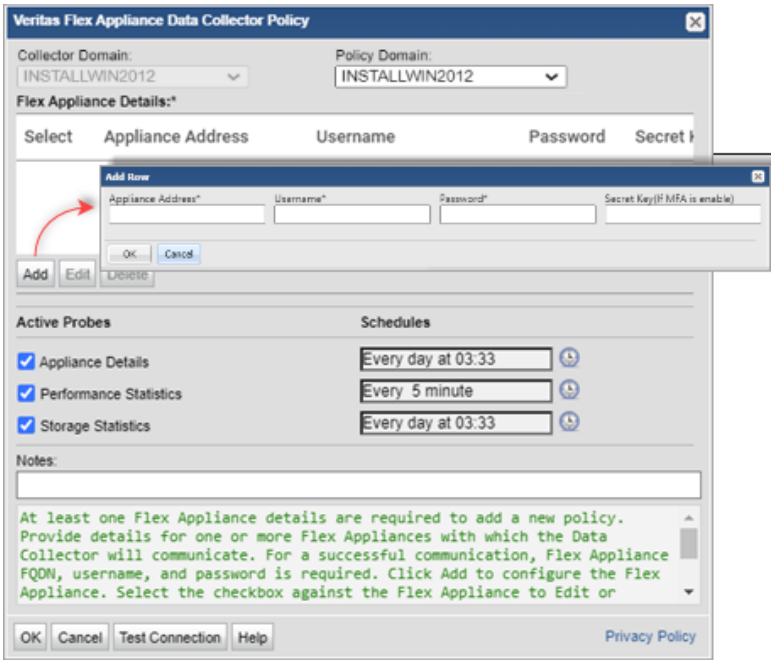
Table 13-1 Data collection based on appliance version

Policy probe	Collection type	Supported NetBackup Flex Appliance version
Appliance Details	Hardware details of appliance and its nodes	2.0, 2.1, 3.0 , 3.2, 4.0
Performance Statistics	Node and container details	2.0, 2.1, 3.0, 3.2, 4.0
Storage Statistics	Storage consumption details	2.0.1, 2.1, 3.0, 3.2, 4.0

Note: The Data Collector installed with the on-premise installation of NetBackup supports data collection from NetBackup Flex Appliance. You can configure the Veritas Flex Appliance 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 or select a Data Collector from the list.
3. Click **Add Policy**, and then select **Veritas Flex Appliance** entry in the menu.
4. 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 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.
Add	Click to add a Flex Appliance to the policy. Provide valid Appliance Address, User ID, and Password for a successful connection.
Appliance Address*	Fully qualified domain name (FQDN) of the Flex Appliance. This FQDN enables the policy to collect from all the appliance nodes that are up-and-running. The data persisted is distinguished by the node ID as registered on the appliance. **Note:** Flex Appliance connector supports only FQDN in Appliance Address.
Username*	Username required to access the Flex Appliance. Provide the user credentials of the admin user of the Flex Appliance. This user is the default user for the Flex Appliance Console. Use this user to sign in to the console for the first time and for operations that require elevated privileges.
Password*	Password required to access the Flex Appliance.
Secret Key (If MFA is enabled)	Secret key associated with the credentials entered in the **Username** and **Password** fields. Secret key is required only of the target Flex Appliance is MFA-enabled and it is crucial for the policy to get an authorized access to the appliance. **Note:** In a MFA-enabled Cohesity Flex Appliance, a new secret key is generated every time its user profile is edited. Ensure the IT Analytics Veritas Flex Appliance policy is configured with the latest secret key associated with the user configured in the policy.

Field	Description
Appliance Details	Collects hardware and software details of Flex Appliance added in the policy. The collected details include: ■ For appliance: appliance name, UUID, appliance type, and more. ■ For node: Node name, serial number, firmware version, Flex version and so on. The probe is selected by default and has a default schedule and its data collection is independent of other probes, irrespective of the data and the execution order.
Performance Statistics	Collects resource utilization and performance statistics from each appliance node and the containers running on the Flex Appliance. The data is collected for each container and is segregated on the basis of appliance and host node on which the container is running. You must create custom reports to view the collection from the nodes and containers. **Note:** Flex v3.0 supports per user active session limited to 10 sessions. Veritas recommends to create a dedicated user for ITA Flex Appliances policy and utilize those credentials for data collection. **Note:** In Flex v3.0, container metrics are restricted due to vulnerabilities in cAdvisor exporter. For this reason, Performance Probe will only collect node metrics from flex appliance with flex version 3.0. No data will be available for container metrics
Storage statistics	Collects storage utilization specific to the entire Flex Appliance, irrespective of its nodes. Collection is performed via REST APIs exposed by the Flex Appliance.

Field	Description
Schedules	By default, collection for Performance Statistics is run performed every 5 minutes and for Storage Statistics, collection is performed daily at 03:33 hours. Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. **Note:** Explicit schedules set for a Collector policy are relative to the time on the Collector server. Schedules with frequencies are relative to the time that the Data Collector was restarted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to all the appliances added to the policy using the FQDN and credentials supplied in the policy. Agent Services must be running for the Test Connection to succeed. 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 to test the collection run.

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

Note: Do not delete the swap directory (`<APTARE_HOME>\mbs\swap\veritas\flexappliance`) from the data collector server as it is used by the Veritas Flex Appliance policy.

The data collected from Flex Appliances is visible in the Host CPU Utilization, Host Memory Utilization, and Host Network Packets Sent/Received reports. See *IT Analytics Report Reference Guide* for more information on the reports.

Troubleshoot Veritas Flex Appliance policy configuration

Logs are generated when a connection is established with the virtual system server and details are collected from the server. Use the following references to access raw data and logs to troubleshoot any policy configuration issues:

- Location of raw data:
  Windows:`<APTARE_HOME>\mbs\rawdata\veritas\flexappliance\`
  Linux: `<APTARE_HOME>/mbs/rawdata/veritas/flexappliance\`
- For errors during collection, check the `Performancestatistics.log` and `StorageStatistics.log` log files in validation/scheduled logs.

  Validation log locations on Windows:

  - `<APTARE_HOME> \mbs\logs\validation\ veritas.flexappliance\<virtual-system-server >#META_< Collector Identifier number>\<probe-name>.log`
  - `<APTARE_HOME> \mbs\logs\validation\ veritas.flexappliance\<virtual-system-server >#VALIDATE_< Collector Identifier number>\<probe-name>.log`

  Validation log locations on Linux:

  - `<APTARE_HOME> /mbs/logs/validation/ veritas.flexappliance/<virtual-system-server >#META_< Collector Identifier number>/<probe-name>.log`
  - `<APTARE_HOME> /mbs/logs/validation/ veritas.flexappliance/<virtual-system-server >#VALIDATE_< Collector Identifier number>/<probe-name>.log`

  Scheduled log locations:

- Windows: `<APTARE_HOME> \mbs\logs\scheduled\ veritas.flexappliance\<virtual-system-server >#META_< Collector Identifier number>\<probe-name>.log`
- Linux:`<APTARE_HOME> /mbs/logs/scheduled/ veritas.flexappliance/<virtual-system-server >#META_< Collector Identifier number>/<probe-name>.log`

Note: Collector Identifier is the ID that matches with the ID in `collectorConig.xml` file for the policy.

- To collect rawdata and logs, create a request for logs and raw data from **Admin** tab > **Advanced** > **Support Tools** on the portal.

Chapter 14

Data Collector Troubleshooting

This chapter includes the following topics:

- Resolving Data Collectors connections issues - Linux specific
- Resolving Data Collectors connections issues - Windows specific
- Portal upgrade performance issues
- Configuring web proxy updates
- Host resources troubleshooting
- Host resources: Check the status of the WMI proxy server
- Host resources: Post-Installation verification
- Host resources: Check host connectivity using standard SSH
- Host resources: Check host connectivity
- Host resources: Check host connectivity using Host Resource Configuration file
- Host resources: Generating host resource configuration files
- Host resources: Check the execution of a command on a remote server
- Host resources Data Collection
- Host resources: Collection in stand-alone mode
- Configuring parameters for SSH
- Identifying Windows file system access errors (File Analytics)

- Collect from remote shares (File Analytics)
- Adding a certificate to the Java keystore
- Override default Java Heap memory (XMX) value for Data Collector utilities

Resolving Data Collectors connections issues - Linux specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal.
2. Verify that the key file is generated when the data collector was created.
3. On the portal, perform `wget` to the URL of the data receiver. The expected response is: `Index.html` file.

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify that the data receiver URL resolves via `NSLOOKUP`. If not then specify the data receiver IP address and name to the data collector's host file.

   Verify using `wget` from the data collector that a response back, index.html page, is received. If not then ,verify if the firewall is blocking the access to port 80/443, depending upon configurations.

5. Execute the command `/usr/openv/analyticscollector/mbs/bin/updateconfig`. The expected response is: quick return to the command prompt. If not then: verify that the /opt/aptare/datarcvrconf/collectorConfig.global.properties on the portal has the correct URL.
6. Execute the `checkinstall`. If there is initial communication but errors, confirm the data collector name, passcode, and URL are correct.
7. Examine the `<Data Collector home>/mbs/conf/collector.properties` file and verify that the collector name, collector password, and URL were specified appropriately during the installation.
8. Verify that the collector service is started, and **Watchdog** is running.

Resolving Data Collectors connections issues - Windows specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal
2. Verify that the key file generated when the data collector was created.
3. On the portal, access a web browser to the URL of the data receiver. Expected response: `Veritas NetBackup IT Analytics Data Receiver.`

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify the data receiver URL resolves via `NSLOOKUP`. If not, specify the data receiver IP address and name to the data collector's host file.
5. Verify the response by a browser session on the data collector to the URL. If not, verify if firewall is blocking access to port 80/443, based on the configuration.
6. Execute `<DC HOME>\mbs\bin\updateconfig`. The expected response is, quick return to the command prompt. If not, verify that the **<APTARE PORTAL HOME>datarcvrconf\collectorConfig.global.properties** on the portal has the correct URL.
7. Execute `checkinstall`. If there is initial communication with errors, verify the data collector name, passcode, and URL are correct.
8. Examine the `<Data Collector home>\mbs\conf\collector.properties` file and confirm the collector name, collector password, and URL were keyed in correctly at installation.
9. Verify that the collector service is started and running.

Portal upgrade performance issues

When the entropy of the system is very low, cryptographic functions takes considerable amount of time.

Following are the examples of low entropy:

- while adding new data collector on Portal, takes longer time to generate the key file.

- Upgrade of Portal hangs when upgrading internal objects.
- Aptare agent service takes longer time when started to get the `collectorconfig.xml` from data receiver side.
- `checkinstall.sh` file execution takes longer time than expecting.

These issues are observed on **Linux Platform**.

The following solution is recommended:

Note: Download and install **rng-tools rpm** on the Portal.

For **RHEL/OEL**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `yum install rng-tools` to install the rng-tools.
3. Type `systemctl start rngd` to start the services.
4. Type `systemctl enable rngd` to enable the services.

For **Suse**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `zypper install rng-tools` to install the rng-tools.
3. Type `systemctl start rng-tools` to start the services.
4. Type `systemctl enable rng-tools` to enable the services.

Configuring web proxy updates

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

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

Host resources troubleshooting

Use the following sequence of steps to determine the source of host resources data collection issues. All commands--except for the SSH commands and the WMI Proxy command--report errors to **metadata.log**. After executing a command, check the **metadata.log** file for error messages. If there is an error noted, correct the problem

and then re-issue the command. If the command succeeds, proceed to the next command in this sequence:

1. See “Host resources: Check the status of the WMI proxy server” on page 204.
2. See “Host resources: Post-Installation verification” on page 207.
3. See “Host resources: Check host connectivity using standard SSH” on page 207.
4. See “Host resources: Check host connectivity” on page 208.
5. See “Host resources: Check the execution of a command on a remote server” on page 212.
6. See “Host resources: Collection in stand-alone mode” on page 213.

Host resources: Check the status of the WMI proxy server

Use the following **checkwmiproxy**utility to verify that the WMI Proxy Server is up and running.

The WMI Proxy logs are written to:

```
C:\Program Files\Aptare\WMIProxyServer\logs\aptarewmiserver.log
```

Prerequisites

Either **checkinstall** or **updateconfig** must have been run before running **checkwmiproxy**. Otherwise, **checkwmiproxy** will not have access to the proxy server settings that are saved in the collector configuration file.

Usage

```
checkwmiproxy.[sh|bat] [wmiProxyServer wmiProxyPort remoteWinHost
DomainOfUserId UserId Password "Command"]
```

Where:

wmiProxyServer is the name of the WMI Proxy Server

wmiProxyPort is the proxy’s port (default is 1248)

Simple usage

```
checkwmiproxy.[sh|bat]
```

By default, this utility will look for the WMI Proxy Server details in the Host Resources Collector section of the collector configuration file. If it does not find a Host Resources Collector section, the **checkwmiproxy** will terminate with an error and

a recommendation to pass explicit parameters, as shown in the usage statement above.

Example 1:

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00
Connection to APTARE WMI Proxy server successfully validated.
```

Example 2: Remote WMI queries

This utility also can be used to execute remote WMI queries, as shown in the following example.

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh 172.16.1.152
Administrator password 172.16.1.152 "select * from
Win32_OperatingSystem"
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
   APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00

    Connection to APTARE WMI Proxy server successfully validated.

    APTAREWMIServer Response:
    instance of Win32_OperatingSystem
    {
         BootDevice = "\\Device\\HarddiskVolume1";
         BuildNumber = "3790";
         BuildType = "Multiprocessor Free";
         Caption = "Microsoft(R) Windows(R) Server 2003, Standard
Edition";
         CodeSet = "1252";
         CountryCode = "1";
         CreationClassName = "Win32_OperatingSystem";
         CSCreationClassName = "Win32_ComputerSystem";
         CSDVersion = "Service Pack 1";
         CSName = "APTARESTGRPT1";
         CurrentTimeZone = -420;
         DataExecutionPrevention_32BitApplications = TRUE;
         DataExecutionPrevention_Available = TRUE;
         DataExecutionPrevention_Drivers = TRUE;
         DataExecutionPrevention_SupportPolicy = 2;
         Debug = FALSE;
```

```
        Description = "aptarestgrpt1";
        Distributed = FALSE;
        EncryptionLevel = 168;
        ForegroundApplicationBoost = 2;
        FreePhysicalMemory = "160264";
        FreeSpaceInPagingFiles = "1967860";
        FreeVirtualMemory = "2084508";
        InstallDate = "20070212110938.000000-480";
        LargeSystemCache = 1;
        LastBootUpTime = "20080507115419.343750-420";
        LocalDateTime = "20080520142117.484000-420";
        Locale = "0409";
        Manufacturer = "Microsoft Corporation";
        MaxNumberOfProcesses = 4294967295;
        MaxProcessMemorySize = "2097024";
        Name = "Microsoft Windows Server 2003 R2 Standard
Edition|C:\\WINDOWS|\\Device\\Harddisk0\\Partition1";
        NumberOfLicensedUsers = 10;
        NumberOfProcesses = 90;
        NumberOfUsers = 8;
        Organization = "Aptare";
        OSLanguage = 1033;
        OSProductSuite = 272;
        OSType = 18;
        OtherTypeDescription = "R2";
        PAEEnabled = TRUE;
        Primary = TRUE;
        ProductType = 3;
        QuantumLength = 0;
        QuantumType = 0;
        RegisteredUser = "Aptare";
        SerialNumber = "69712-OEM-4418173-93136";
        ServicePackMajorVersion = 1;
        ServicePackMinorVersion = 0;
        SizeStoredInPagingFiles = "2039808";
        Status = "OK";
        SuiteMask = 272;
        SystemDevice = "\\Device\\HarddiskVolume1";
        SystemDirectory = "C:\\WINDOWS\\system32";
        SystemDrive = "C:";
        TotalVirtualMemorySize = "3256472";
        TotalVisibleMemorySize = "1363400";
        Version = "5.2.3790";
```

```
        WindowsDirectory = "C:\\WINDOWS";
};
```

Host resources: Post-Installation verification

Execute this utility to verify that the host resources installation was successful.

```
hostresourcecheckinstall.{sh|bat}
```

Host resources: Check host connectivity using standard SSH

IT Analytics uses SSH to communicate with devices to run SSH commands. Sometimes, a connectivity issue is simply an incorrect path to a host.

Note: Use the following SSH commands before attempting to collect data.

To check host connectivity using standard SSH:

1. Check that the connection to a Host is successful, using the credentials provided.

   ```
   [user@host ~] ssh <user>@<host> ls
   ```

   Similarly, if you are using Telnet, check your host access via Telnet and run **sudo** commands, as shown in the following step.

2. In access-controlled environments such as **sudo**, a sudo user must be set up. Ensure that the sudo user can run the commands required for the host operating system platform.

   To verify **sudo** access:

   ```
   [user@host ~] ssh <sudouser>@<host> "sudo <command>"
   ```

   If this command results in errors, such as command not found, set up the paths correctly and re-run this command.

   See "Checking Paths for SSH" on page 208.

   on page 11.

3. Paths should be set correctly for the commands to run.

Checking Paths for SSH

If you find messages in the metadata.log file that indicate that some of the commands are not found, then most likely the reason for it is the paths have not been set properly.

IT Analytics uses a non-interactive login shell to execute ssh commands on devices.

1. Check the environment setting for the shell by running the command.

   ```
   [user@host ~] ssh <user>@<host> "env"
   ```

   Check the PATH shown in the output and make sure that it contains the path to all the commands required for IT Analytics for the OS platform of the host.

   Sample PATH for each of the host operating system platforms:

   Linux: /bin:/sbin:/usr/bin:/usr/sbin

   Solaris: /usr/xpg4/bin:/usr/sbin:/usr/bin

   AIX: /usr/bin:/usr/sbin

   HPUX: /usr/bin:/usr/sbin:/opt/fcms/bin:/sbin

   Note: Since Veritas Volume Manager is supported, its path needs to be included in the PATH env variable.

   ---

2. In **sudo** environments, make sure that the sudo path is also in the PATH shown in the output of the above command.

Environment setting for bash users

1. Define all your settings in the file: **~/.bashrc**
2. Make sure that the file **~/.bash_profile** only contains the line: **source ~/.bashrc**

Host resources: Check host connectivity

This utility displays information on the connection status of a list of host names, IP addresses, or a range of IP addresses.

```
chkHostConnection.{sh|bat} HostAddresses userId password
[domain <domain>]
[exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

Table 14-1 Hosts resources and their values.

Host Addresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

As a result: for each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} HostAddresses userId password [domain
<domain>] [exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Host resources: Check host connectivity using Host Resource Configuration file

This utility provides information on the connection status of a list of Host Addresses that are provided in the Host Resource Configuration file.

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>]
[cto <connectTimeout>] [sto <socketTimeout>]
```

Table 14-2 Hosts resources and their values.

HostResourceFile	The file should be located under the home directory: /mbs/conf/hostresourceconf
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Result: For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>] [cto <connectTimeout>] [sto <socketTimeout>]
```

HostResourceFile	The file should be located under the home directory: **/mbs/conf/hostresourceconf**
wmiserver	Name of the WMI Proxy Server

cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Host resources: Generating host resource configuration files

This utility automatically generates the host resource configuration files and collector configuration file for each valid line provided in the input file.

```
genHostResourceConf.{sh|bat} {CollectorID} {fileName}
```

CollectorID	Identifier name used for the configuration files
filename	File containing the list of parameters--one per line--in the format: `HostAddresses:userId:password:domain:excludeHostAddress` Comments are allowed by using a # at the beginning of the line.
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Sample lines in an input file

```
# Sample configuration file to generate Host Resource Conf files
172.16.1.11-13,aptarelab3:root:adminpwd::172.16.1.12-13,apataredlab3
aptareaix1:root:superpwd::
apatrewin2k:samuel:adminpwd:aptarewin2kdomain:
```

Results

- For each valid line, a host resource configuration is created under the home directory: **/mbs/conf/hostresourceconf**. Lines that are not valid are sent to standard output.

- Creates a collector configuration xml file with Meta Data Collector child thread tags for each successfully created host resource configuration file. The file is saved in the home directory under **/mbs/conf**. The collector configuration xml is named in the following format:
  collectorconfig-<date>.xml where date is in DDMMMYYYHHMM format

Host resources: Check the execution of a command on a remote server

This utility provides the output of a command by running it on the specified remote server.

```
remoteExecCommand.{sh|bat} HostAddress [enc] userId password
[domain=<domain>]
[wmiserver=<wmiserver>] [cto=<connectTimeout>] [sto=socketTimeout>]
 [accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
userId password	Use the [enc] option to provide encrypted user ID and password arguments.
domain	The Domain for the Windows hosts (only for connecting to a Windows server)
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Example

```
remoteExecCommand.sh 172.16.1.21 myuser mypasswd /usr/bin/df -k
remoteExecCommand.sh 172.16.1.21 myuser mypasswd accessCmd=sudo
cto=10000 /usr/bin/df -k
```

Host resources Data Collection

IT Analytics can collect the following types of host resources:

- Capacity
- Oracle
- SQL Server
- Exchange
- Network
- Processor
- Memory
- Process
- System

Host resources: Collection in stand-alone mode

This utility executes the data collection process against the specific host resources files.

Usage (3 options)

```
hostresourceDetail.{sh|bat} all
hostresourceDetail.{sh|bat} <MetaCollectorID> <HostResourcePolicyName>
hostresourceDetail.{sh|bat} HostAddresses uid=userId pwd=password
[<domain>]
[<excludeHostAddresses>]
```

all	This option runs host resource policies against all Meta Collectors.
MetaCollectorID	The ID used to identify the MetaCollector within the collector configuration xml file.
HostResourcePolicyName	The Policy ID within the Meta Collector ID specified.
HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.

domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.

Configuring parameters for SSH

To add any configurable SSH parameters, modify the following scripts:

```
hostResourceDetail.{sh|bat} and aptarecron.{sh|bat}
```

For example, to add the **channelWaitTime**parameter, insert the following after java:

```
-DchannelWaitTime=5000
```

Configure channelWaitTime

If you are experiencing slow connectivity from the Data Collector Server to the Host, update the scripts with this Configurable Parameter. This parameter is specified in milliseconds.

```
-DchannelWaitTime=5000 // This will set the wait time for data from
 the server.
```

Configure singleChannelSession

This will run each command in a separate session.

```
-DsingleChannelSession=true // This will run the each command in a
separate session.
```

Configure sudoWithPassword

In sudo environments, this will send the password without waiting for a prompt.

```
-DsudoWithPassword=true // This will allow running sudo with -S option
 to send the password without waiting for a prompt.
```

Identifying Windows file system access errors (File Analytics)

While profiling the Windows primary file table and file systems, a number of error messages may appear in the **MFT.Aptare_File_Inventory.log** file

These errors actually may require no follow-up actions. Typically, the errors are legitimate, such as a file being locked for exclusive use. Therefore, some files in the C:\Windows\System32 directory will not be profiled.

Example of a Log Error Message:

```
Unable To Access File C:\Windows\System32\Boot. Error 2. Skipping!!!
```

The following table lists System Errors with descriptions.

Table 14-3 Windows file system errors and its description

System Error	Description
2	System cannot find the file specified; This error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.
3	System cannot find the path specified; This system error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.
5	Access Denied; The file is accessible only to SYSTEM; for example, C:\Windows\System32\LogFiles\WMI\RtBackup
32	Another process has the file opened in exclusive mode; for example, database files used by the SQL server

Collect from remote shares (File Analytics)

The functionality of the host File Analytics probe excludes remote shares that are mounted to the target host, thereby capturing only local files and folders.

To collect from remote shares, an advanced parameter must be configured.

1. In the Portal, navigate to **Admin > Advanced > Parameters**.
2. Click **Add** to add an advanced parameter with a value of **FA_HOST_CAPTURE_REMOTE_SHARES** with a default value of **Y**, along with the target server host name.

Adding a certificate to the Java keystore

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

Keystore file location

Note: For the following commands, if you are not running in the default collector location (/usr/openv/analyticscollector or \Program Files\Veritas\AnalyticsCollector), substitute the appropriate APTARE_HOME in the command path.

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Copy the certificate file (certfile.txt) to the Data Collector. Run the following command to add the certificate:

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -import
 -alias "somealias" -file certfile.txt -keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -import -alias
"somealias" -file certfile.txt -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

When prompted, enter the default password to the keystore:

```
changeit
```

The results will be similar to the following example:

```
Enter keystore password:
......
Certificate Shown here
......
......
```

```
.....
Trust this certificate? [no]: yes
```

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

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -list
-keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -list -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Sample Linux Output

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 79 entries
digicertassuredidrootca, Apr 16, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
trustcenterclass2caii, Apr 29, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
.....
```

Override default Java Heap memory (XMX) value for Data Collector utilities

You may require to override the default Java Heap Memory (XMX) value to avoid performance degradation or potential "OutOfMemoryError" exceptions. The following procedure provides the override steps for Windows and Linux hosts.

Override default Java Heap memory (XMX) value for Windows Data collector utilities

To override the default XMX value for Data Collector Windows batch scripts, uncomment the XMX variable in `dc_override_config.bat` present in the `mbs\conf`

directory and provide the updated XMX value. The comment in the batch file will guide you to identify the variable to be overridden for the script you are interested.

Example: Override XMX value for `checkinstall.bat` script

Update XMX value in `dc_override_config.bat`

```
:: checkinstall.bat
              XMX_CHECK_INSTALL=-Xmx17g
```

The backup of the `dc_override_config.bat` is saved to the `mbs\conf` directory with the name `dc_override_config.bat_bkp`.

Note: Use **::** only for comment and at the beginning of the line.

Override default Java Heap memory (XMX) value for Linux Data collector utilities

To override the default XMX value for Data collector Linux batch scripts, uncomment the XMX variable in `dc_override_config.sh` present in the `mbs/conf` directory and provide the updated XMX value. The comment in the shell script file will guide you to identify the variable to be overridden for the script you are interested.

Example: Override XMX value for `checkinstall.sh` script

Update XMX value in `dc_override_config.sh`

```
#checkinstall.sh
            XMX_CHECK_INSTALL=-Xmx17g
```

The backup of the `dc_override_config.sh` is saved to the `mbs\conf` directory with the name `dc_override_config.sh_bkp`.

Note: Use **#** only for comment and at the beginning of the line.

Appendix A

Configure Appliances

This appendix includes the following topics:

- Configure NetBackup Appliances for Data Collection
- Configure NetBackup Flex Appliances for Data Collection

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.

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.

Appendix B

Load historic events

This appendix includes the following topics:

- Introduction
- Load Veritas NetBackup events
- Update Cohesity NetBackup SLP Job Details

Introduction

After installing the backup Data Collectors, you may want to capture historical backup events for inclusion in the 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 Veritas NetBackup events

The Cohesity NetBackup Historic collection is limited to capturing details on successful backup images that are still present in the NetBackup catalog (i.e. unexpired backup images). This historic information is captured using the NetBackup `bpimagelist` command.

The failed jobs are not:

- the part of the historic collection as they are not present in the catalog

- point-in-time metrics such as job throughput.

The following are the steps to execute historic collection from the portal:

1. Log in to the portal.
2. Navigate to *Admin >> Data Collection >> Collector Administration*.
3. Expand the collector and then select the **NetBackup Policy**.
4. Click **Run**. The **Run Cohesity NetBackup Collection** dialog box is displayed.
5. Click **Historic Collection**.
6. Clear the **Enable Real-Time Logs** check box.
7. Clear the **Enable Debug Logs** check box.
8. Select the appropriate **Start Date** and **End Date**.
9. Specify one or more **Client Name(s)**, separated by commas, to limit historic collection to only these specified clients. For example, Client_a, Client_b
10. Click **Start**.

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

Update Cohesity NetBackup SLP Job Details

The Cohesity NetBackup Historic SLP collection captures details on incomplete backup images and copies whose associated jobs are already captured in IT Analytics. Over time, some images and copies can remain incomplete in IT Analytics but fall outside the normal SLP collection lookback window, so they are no longer refreshed by regular SLP job collection. This utility updates that historic data by collecting information still present in the NetBackup catalog (unexpired backup images and copies) using the NetBackup `nbstlutil list` command, and by marking images and copies not present in the catalog as complete in IT Analytics.

Note that:

- `<ANALYTICS_COLLECTOR_HOME>` is the Data Collector installation directory (example: `C:\Program Files\Cohesity NetBackup\AnalyticsCollector` or `/usr/openv/analyticscollector`)
- Specify a date range using `--start` and `--end` together. Dates must be in the format MM/DD/YYYY HH:MM:SS and enclosed in double quotes.
- Process the data in 6-month windows, rather than attempting a single run across all the history, as volume of historical incomplete SLP data can be very large.

To retrieve historic SLP data, run the following command-line scripts on the Data Collector:

1 On Windows:

```
<ANALYTICS_COLLECTOR_HOME>/mbs/bin/veritas/update_incomplete_slp_jobs.bat
 <primaryServerName> --start "01/01/2026 00:00:00" --end
"06/30/2026 23:59:59"
```

2 On Linux:

```
<ANALYTICS_COLLECTOR_HOME>/mbs/bin/veritas/update_incomplete_slp_jobs.sh
 <primaryServerName> --start "01/01/2026 00:00:00" --end
"06/30/2026 23:59:59"
```

Appendix C

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 C-1 Components: Default Ports

Component	Default Ports
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445 SSH 22

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

Component	Default Ports
ZooKeeper	2181 **Note:** 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 IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table C-2 Storage Vendors: Default Ports

Storage Vendor	Default Ports and Notes
Veritas NetBackup Appliance	1556
Veritas NetBackup Flex Appliance	SSH 22, REST API 443

Table C-3 Data protection: Default ports

Data Protection Vendor	Default Ports and Notes
Veritas NetBackup	443, 1556, and 13724 WMI ports SSH 22 (Linux)

Appendix D

CRON Expressions for Policy and Report Schedules

This appendix includes the following topics:

- CRON expressions for policy probe schedules
- CRON expressions for scheduling reports

CRON expressions for policy probe schedules

Many Data Collector policy configurations require a schedule. Native CRON expressions are supported for fine-tuning a schedule. The CRON expression format for the policy configurations follows strings with five single space-separated time and date fields:

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

The following are the general guidelines when using special characters during the CRON expressions.

Table D-1 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
minutes	0-59 (0 is “on the hour”)

Table D-1 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)

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

Special Characters:

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

Table D-2 Probe Schedule field examples of string with five single space-separated time and date fields

Probe Schedule Examples	Scheduled Run Time
0 14-15 * * 1	On the hour, every Monday, between 2 and 3pm **Note:** A zero in the minutes position denotes the beginning of the hour.
30 9-13 * * 1-5	9:30, 10:30, 11:30, 12:30, and 13:30, Monday through Friday.
0 */2 * * *	To run the probe every 2 hours, put */2 in the hour position. This schedules the probe at 2am, 4am, 6am, 8am, 10am, 12pm, 2pm, and so on.
*/30 * * * *	Every 30 minutes
*/20 9-18 * * *	Every 20 minutes between 9 am and 6 pm
*/30 * * * 1-5	Every 30 minutes, Monday through Friday

Table D-2 Probe Schedule field examples of string with five single space-separated time and date fields *(continued)*

Probe Schedule Examples	Scheduled Run Time
1 2 * * *	2:01 every day
30 9,11 * * *	9:30 and 11:30 every day

CRON expressions for scheduling reports

Many reports and dashboards may require a email or export schedule. Native CRON expressions are supported for fine-tuning a email or schedule. The format for scheduling reports and dashboard email and exports follows string with six single space-separated time and date fields:

*	*	*	*	*	*
second	minute	hour	day of the month	month	day of the week

The following are the general guidelines when using special characters during the CRON expressions.

Table D-3 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
second	0-59 in string with six single space-separated time and date fields
minutes	0-59 (0 is “on the hour”)
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)
■ IT Analytics supports a maximum of 80 characters in a CRON expression.	
Special Characters:	

Table D-3 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
■ A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the seconds and minutes position is not permitted, as this would excessively trigger the probe—every second or minute.	
■ A forward slash (/) can be used to specify intervals.	
■ Use a dash (-) to specify a range.	
■ Use ? (“no specific value”) when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, to schedule the trigger on a particular day of the month (the 10th), but irrespective of the day-of-the-week that happens to be, specify “10” in the day-of-month field, and “?” in the day-of-week fie	
■ You can use forward slash (/) can be used to specify increments. For example, “0/15” in the seconds field means “the seconds 0, 15, 30, and 45”. And “5/15” in the seconds field means “the seconds 5, 20, 35, and 50”. You can also specify ‘/’ after the ‘’ character - in this case ‘’ is equivalent to having ‘0’ before the ‘/’. ‘1/3’ in the day-of-month field means “fire every 3 days starting on the first day of the month”.	
■ The CRON expression for the last day of the month, denoted by the letter L, is not supported.	

Table D-4 Report Schedule field examples of string with six single space-separated time and date fields

Report Schedule Examples	Schedule Run Time
0 0 * * * *	the top of every hour of every day.
*/10 * * * * *	every ten seconds.
0 0 8-10 * * *	8, 9 and 10 o'clock of every day.
0 0 6,19 * * *	6:00 AM and 7:00 PM every day.
0 0/30 8-10 * * *	8:00, 8:30, 9:00, 9:30, 10:00 and 10:30 every day.
0 0 0 25 12 ?	every Christmas Day at midnight.
0 15 10 * * ? 2010	run at 10:15 AM every day during the year 2010.

Table D-4 Report Schedule field examples of string with six single space-separated time and date fields *(continued)*

Report Schedule Examples	Schedule Run Time
0 0 12 1/5 * ?	run at 12 PM (noon) every 5 days every month, starting on the first day of the month.
0 0 0 1W * *	first weekday of the month at midnight
0 11 11 11 11 ?	run every November 11th at 11:11 AM.
0 0-5 14 * * ?	run every minute starting at 2 PM and ending at 2:05 PM, every day.