

NetBackup IT Analytics Exporter Installation and Configuration Guide

Release: 11.6

NetBackup IT Analytics Exporter Installation and Configuration Guide

Last updated: 2026-03-02

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

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

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

Cohesity Support

21 September 2025

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

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

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

Cohesity Software Running on Partner Hardware

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

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

Documentation

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

Documentation

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

Cohesity Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	Introduction and Installation Overview	6
	About NetBackup IT Analytics Exporter	6
	Prerequisites for exporter installation	7
	Installation overview and ISO form factor	8
Chapter 2	Install and manage the NetBackup IT Analytics Exporter on a Linux Host	10
	Install the exporter on a Linux host using ISO	10
	Install the exporter on Linux host using response file	12
	Install the exporter on Linux host using RPM	13
	Exporter service management on Linux	15
	Upgrade or reinstall the exporter	15
Chapter 3	Install and Manage the NetBackup IT Analytics Exporter on a Windows Host	17
	Install the exporter on Windows host	17
	Install the exporter on Windows host using response file	21
	Exporter service management on Windows	22
	ISO-based upgrade on Windows host	22
Chapter 4	Configure the NetBackup IT Analytics Exporter	24
	Configure the NetBackup exporter	24
	Configure Node exporter	29
	Configure Process exporter	30
	Configure Windows exporter	30
	Configure Data Sender	30
Appendix A	Troubleshooting	36
	Resolve NetBackup exporter issues	36
	Resolve Node exporter issues	38
	Resolve Process exporter issues	38
	Resolve Windows exporter issues	39

Resolve Data Sender issues	39
Log locations	41
Resolves invalid sender ID related to security changes	42

Introduction and Installation Overview

This chapter includes the following topics:

- [About NetBackup IT Analytics Exporter](#)
- [Prerequisites for exporter installation](#)
- [Installation overview and ISO form factor](#)

About NetBackup IT Analytics Exporter

NetBackup IT Analytics Exporter provides an additional export mechanism for data collection from Windows or Linux hosts, including NetBackup primary servers.

NetBackup IT Analytics Exporter enables you to view and analyze the health of your Windows and Linux OS, including the NetBackup primary servers. After a successful installation, the exporter components probe the host for installed certificates and their validity, process running status, and active connections for some pre-specified processes, subsystem internals and metadata, third-party exporters for hardware related data collections, and OS-specific details.

NetBackup IT Analytics Exporter is developed using Prometheus exporter framework. Data Collection happens via a push model over HTTP connection with NetBackup IT Analytics Data Collector.

The following components are installed based on the host OS:

- NetBackup exporter: Exports details related to NetBackup file processing, host certificate, database file, network processes, pbx_exchange process, and block devices. Metrics are exposed on port 9099 and path /metrics.
- Node exporter: Exports details of system resources like RAM, disk, CPU, and network from Linux hosts. Metrics are exposed on port 9100 and path /metrics.

- Process exporter: Exports details of resources from `/proc` location on Linux hosts. Metrics are exposed on port 9256 and path `/metrics`.
- Windows exporter: Exports details of system resources like RAM, disk, CPU, and network from Windows hosts. Metrics are exposed on port 9182 path and `/metrics`.
- Data Sender: Collects metrics from exporters configured for metrics collection based on the host OS and pushes filtered metrics to the destination NetBackup IT Analytics Data Collector server.

Prerequisites for exporter installation

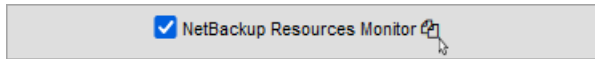
NetBackup IT Analytics exporter supports shell script based installer in ISO form factor, RPM form factor for installation on Linux, and .exe-based installer in ISO form factor for Windows. Ensure the following prerequisites are available before you install the exporter:

- NetBackup IT Analytics Data Collector must be installed and all services must be started. NetBackup IT Analytics Exporter must be able to communicate with the data collector.
- Compute Resources policy must be configured on the NetBackup IT Analytics Portal before this installation.
- If NetBackup Resources Monitor probe is enabled on the Cohesity NetBackup Data Collector policy on the NetBackup IT Analytics Portal, then this exporter installation must be performed on the NetBackup Primary Server.
- NetBackup IT Analytics Exporter installer must be downloaded from the Cohesity download center. This can be the RPM or Installer for a Linux host or .exe file for the Windows host.

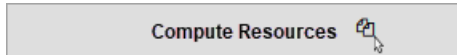
- Fully qualified domain name (FQDN) of the data collector must be available when you begin with the installation.

The Data Collector server listens to port 8883 by default. In case the Data Collector is configured to listen to a different port through advanced parameters, you must update the port post installation in the `datasender.yaml` configuration file.

- Depending on the probe you plan to enable, get the Sender ID as follows:
 - For NetBackup Resources Monitor probe, go to **Admin** tab > **Data Collection** > **Collector Administration** and double-click the Veritas NetBackup Data Collector Policy assigned to the NetBackup Master. On the policy screen, click the **Copy Sender ID** icon next to the **NetBackup Resources Monitor** probe label.



- For Compute Resource probe, go to **Admin** tab > **Data Collection** > **Collector Administration** and double-click the Compute Resources Data Collector Policy assigned to the Windows or Linux hosts (including NetBackup Primary Servers). On the policy screen, click the **Copy Sender ID** icon next to the **Compute Resources** probe label.



- Depending on the probe you enable, download the SSL certificate as follows. You will have to specify the absolute path to the SSL Certificate during the installation.
- For NetBackup Resources Monitor and Compute Resources probe, obtain the file using **Download SSL Certificate** button on the Cohesity NetBackup Data Collector policy screen of the NetBackup IT Analytics Portal and save it on the host.
- For Compute Resource probe, obtain the file using **Download SSL Certificate** button on the Compute Resources Data Collector policy screen of the NetBackup IT Analytics Portal and save it on the host.

Supported operating systems

NetBackup IT Analytics Exporter is supported on the following OSs.

Table 1-1 Supported OS for NetBackup IT Analytics Exporter

OS flavors	Versions
Red Hat Enterprise Linux Servers	7, 8
Windows server	2016, 2019

Installation overview and ISO form factor

The installer of the NetBackup IT Analytics Exporter comes with the following OS-specific form factors:

- For Linux: A script-based installer in ISO form factor and RPM.
- For Windows: An .exe-based installer in ISO form factor.

High-level installation steps:

- 1** Run the installer and review the terms and conditions before you agree to proceed.
- 2** Enter the fully qualified domain name of the data collector server. In case you are reinstalling the exporter, the installer asks permission to overwrite the previously installed files on your system.
- 3** Select the probes to install.
- 4** Provide the Sender ID.
- 5** Provide the Data Sender certificate location.

Install and manage the NetBackup IT Analytics Exporter on a Linux Host

This chapter includes the following topics:

- [Install the exporter on a Linux host using ISO](#)
- [Install the exporter on Linux host using response file](#)
- [Install the exporter on Linux host using RPM](#)
- [Exporter service management on Linux](#)
- [Upgrade or reinstall the exporter](#)

Install the exporter on a Linux host using ISO

Ensure you have addressed all the prerequisites before proceeding for the exporter installation.

See [“Prerequisites for exporter installation”](#) on page 7.

To install the NetBackup IT Analytics exporter on a Linux host:

- 1** Mount the installer on the Linux host.

```
# mount -o loop itanalytics_exporter_installer_linux_<version>.iso /mnt
```

Note: Replace the <version> with the appropriate portal versions.

- 2** Run the installer script.

```
# /mnt/exporter_installer.sh
```

The installer displays the End User License Agreement (EULA).

In case you are reinstalling the exporter, the installer asks permission to overwrite the previously installed files on your system.

- 3** Accept the EULA.
- 4** Enter the fully qualified domain name (FQDN) of the data collector server.
The hostname you provide must accurately resolve to the correct IP address of the data collector server.
- 5** Enable the appropriate probe based on your requirement. You can enter **1** for NetBackup Resources Monitor and Compute Resources probe or **2** for Compute Resources probe.

The subsequent steps for each probe are provided below.

If you enabled the NetBackup Resources Monitor and Compute Resources probe:

- 1** Enter the Sender ID of the NetBackup Resources Monitor obtained from the Veritas NetBackup Data Collector policy screen.
- 2** Enter the Sender ID of the Compute Resources probe obtained from the Compute Resources Data Collector policy screen.
- 3** Enter the absolute path of the Data Sender Certificate file.

This is the path of the file downloaded using **Download SSL Certificate** button on the Cohesity NetBackup Data Collector policy screen of the NetBackup IT Analytics Portal.

If you enabled the Compute Resources probe:

- 1 Enter the Sender ID of the Compute Resources probe obtained from the Compute Resources Data Collector policy screen.
- 2 Enter the absolute path of the Data Sender Certificate file.

This is the path of the file downloaded using **Download SSL Certificate** button on the Compute Resources Data Collector Policy screen of the NetBackup IT Analytics Portal.

After you have provided the required details mentioned in the steps above, the exporter is installed inside the `/opt/itanalytics` directory. The systemd service profiles are created in the `/etc/systemd/system` directory and the log files are generated under `/opt/itanalytics/logs`.

Install the exporter on Linux host using response file

You can also install the exporter on a Linux host using a response file. Ensure you have addressed all the prerequisites before proceeding for the exporter installation. You can obtain the response file template from the ISO downloaded from Cohesity Download Center on the Linux host. The values that you must configure in the response file are described in the table below.

See [“Prerequisites for exporter installation”](#) on page 7.

Table 2-1 Response file inputs

Response file parameters	Description
COLLECTOR_HOST	Fully qualified domain name (FQDN) of the data collector.
PROBE_ID	Accepts 1 or 2 as values for probe selection. If you enter 1 , NetBackup and Compute Resources probe is enabled. If your set value is 2 , Compute Resources probe is enabled.
DATASENDER_CERT	Absolute path of the data sender certificate file downloaded from NetBackup IT Analytics Portal.

Table 2-1 Response file inputs (*continued*)

Response file parameters	Description
COMPUTE_RES_SENDER_ID	Sender ID copied from NetBackup IT Analytics Portal. The ID is available from the Compute Resources probe of the Compute Resources Data Collector policy and is required if the PROBE_ID is set to 1 or 2 .
NBU_SENDER_ID	Sender ID copied from NetBackup IT Analytics Portal. The ID is available from the NetBackup Resource Monitor probe of the NetBackup policy and is required if the PROBE_ID is set to 1

Once your response file is ready, you can proceed with the installation.

To install the exporter using the response file:

- 1 Mount the installer on the Linux host.

```
# mount -o loop itanalytics_exporter_installer_linux_<version>.iso /mnt
```

Note: Replace the <version> with the appropriate portal versions.

- 2 Run the installer script with the path to the response file.

```
# /mnt/exporter_installer.sh -r <responsefile path>
```

The exporter is installed according to the configuration of the response file.

After you have provided the required details mentioned in the steps above, the exporter is installed inside the `/opt/itanalytics` directory. The systemd service profiles are created in the `/etc/systemd/system` directory and the log files are generated under `/opt/itanalytics/logs`.

Install the exporter on Linux host using RPM

Ensure you have addressed all the prerequisites before proceeding for the exporter installation.

See [“Prerequisites for exporter installation”](#) on page 7.

To install the exporter on Linux host using RPM:

1 Install the RPM:

```
# rpm -ivh VRTSexporter-<version>-0.x86_64.rpm
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
1:VRTSexporter-11.0.00-0 ##### [100%]
```

Note: For `# rpm -ivh VRTSexporter-<version>-0.x86_64.rpm`, replace `<version>` with the appropriate portal versions.

2 Run this installer script:

```
/opt/itanalytics/utils/exporter_installer.sh
```

The installer displays the End User License Agreement (EULA).

In case you are reinstalling the exporter, the installer asks permission to overwrite the previously installed files on your system.

3 Accept the EULA.

4 Enter the fully qualified domain name (FQDN) of the data collector server.

The hostname you provide must accurately resolve to the correct IP address of the data collector server.

5 Enable the appropriate probe based on your requirement. You can enter **1** for NetBackup Resources Monitor and Compute Resources probe or **2** for Compute Resources probe.

The subsequent steps for each probe are provided below.

If you enabled the NetBackup Resources Monitor and Compute Resources probe:

1 Enter the Sender ID of the NetBackup Resources Monitor obtained from the Veritas NetBackup Data Collector policy screen.

2 Enter the Sender ID of the Compute Resources probe obtained from the Compute Resources Data Collector policy screen.

3 Enter the absolute path of the Data Sender Certificate file.

This is the path of the file downloaded using **Download SSL Certificate** button on the Cohesity NetBackup Data Collector policy screen of the NetBackup IT Analytics Portal.

If you enabled the Compute Resources probe:

- 1 Enter the Sender ID of the Compute Resources probe obtained from the Compute Resources Data Collector policy screen.
- 2 Enter the absolute path of the Data Sender Certificate file.

This is the path of the file downloaded using **Download SSL Certificate** button on the Compute Resources Data Collector Policy screen of the NetBackup IT Analytics Portal.

After you have provided the required details mentioned in the steps above, the exporter is installed inside the `/opt/itanalytics` directory. The systemd service profiles are created in the `/etc/systemd/system` directory and the log files are generated under `/opt/itanalytics/logs`.

Exporter service management on Linux

The following systemd services are created in the `/etc/systemd/system` directory and started by installer:

```
itanalytics_datasender.service  
itanalytics_netbackup_exporter.service  
itanalytics_node_exporter.service  
itanalytics_process_exporter.service
```

You can manage all the the services of the NetBackup IT Analytics exporter with this command:

```
systemctl start|stop|status <exporter service name>
```

Note: Replace the `exporter service name` with appropriate service name, as mentioned above.

Upgrade or reinstall the exporter

Ensure you have addressed the prerequisites specified for the exporter installation before you proceed to upgrade or reinstall the exporter.

See [“Prerequisites for exporter installation”](#) on page 7.

ISO-based upgrade on Linux host

Run the `exporter_installer.sh` script from the ISO of the new version of the exporter. The script detects the existing exporter files and prompts to overwrite the files. You must overwrite the files and continue with the upgrade or reinstallation.

RPM based upgrade on Linux host

1. Install the RPM:

```
# rpm -Uvh VRTSexporter-<version>.x86_64.rpm
```

Note: Replace the `version` string with the required portal versions.

2. Run the script:

```
/opt/itanalytics/utils/exporter_installer.sh
```

Install and Manage the NetBackup IT Analytics Exporter on a Windows Host

This chapter includes the following topics:

- [Install the exporter on Windows host](#)
- [Install the exporter on Windows host using response file](#)
- [Exporter service management on Windows](#)
- [ISO-based upgrade on Windows host](#)

Install the exporter on Windows host

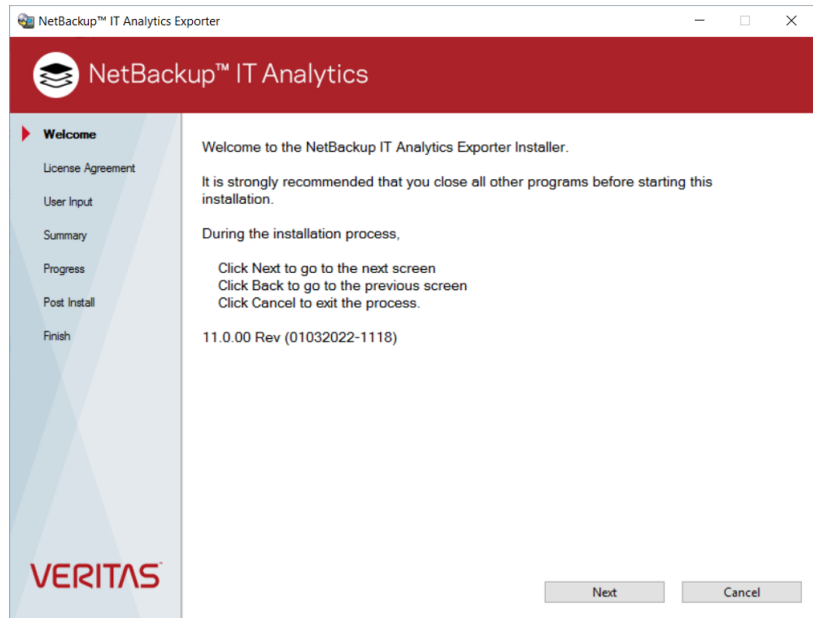
Download `itanalytics_exporter_installer_win_11000.iso` from the Cohesity Download Center before you proceed with the installation. Ensure you have addressed all the prerequisites before you install the exporter.

See [“Prerequisites for exporter installation”](#) on page 7.

To install the exporter on a Windows host:

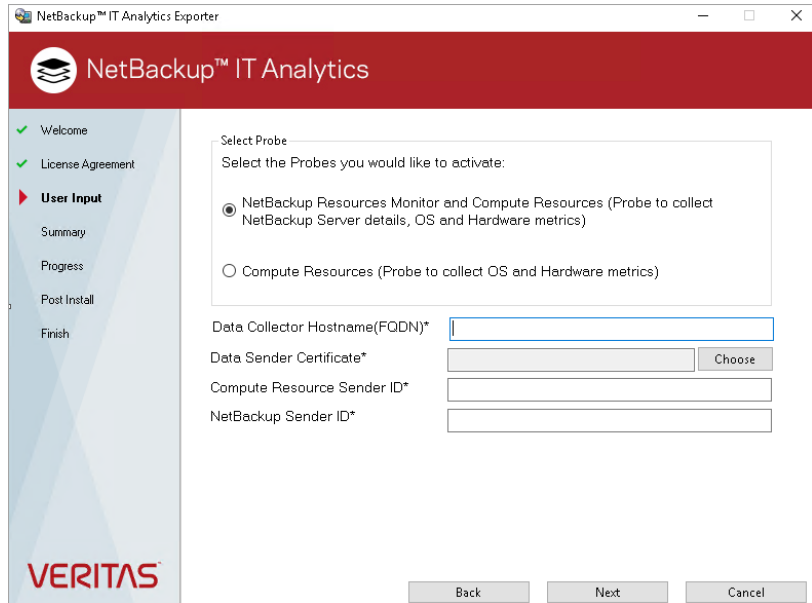
- 1 Double-click the `itanalytics_exporter_installer_win_11000.iso` file downloaded on the Windows host and run the `Setup.exe` inside the ISO.

The NetBackup IT Analytics Exporter installer wizard is launched.



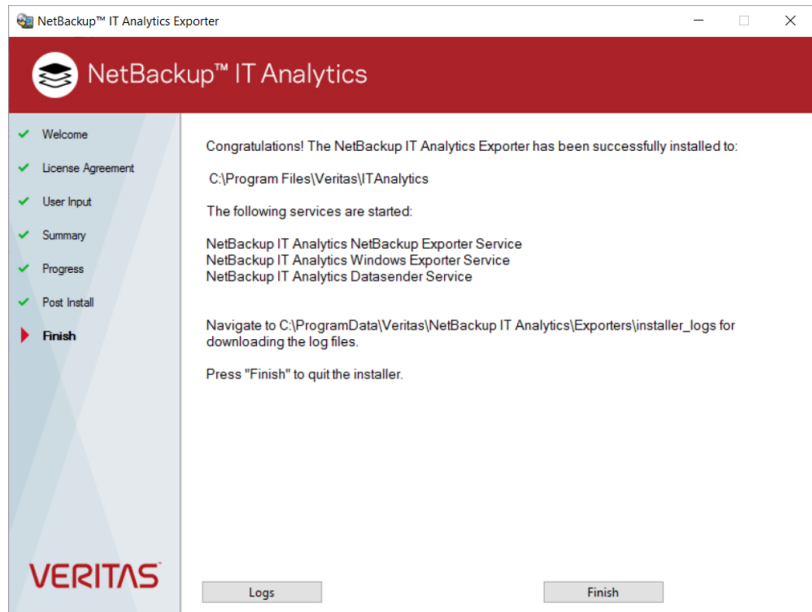
- 2 Review the high-level install instructions and click **Next**.
- 3 Review and accept the End User License Agreement (EULA) and click **Next**.
- 4 Select the probe you want to enable based on the below description.
 - **NetBackup Resources Monitor and Compute Resources:** Collects NetBackup Server details and OS as well as hardware metrics from the local system.
 - **Compute resources:** Collects OS and hardware metrics from the local system.
- 5 Enter the following details obtained while addressing the prerequisites.
 - **Data Collector HostName:** Fully qualified domain name (FQDN) of the data collector server.

- **Data Sender Certificate:** Click **Choose** to locate and assign the absolute path of the data sender certificate file downloaded from NetBackup IT Analytics Portal.
- **Compute Resources Sender ID:** Enter the Sender ID obtained from the Compute Resource Data Collector policy screen.
- **NetBackup Sender ID:** Enter the Sender ID obtained from the NetBackup Data Collector policy. This value is not required if you have selected the **Compute Resources** probe.



The screenshot shows the 'User Input' step of the NetBackup IT Analytics Exporter installation. The left sidebar lists the steps: Welcome, License Agreement, **User Input**, Summary, Progress, Post Install, and Finish. The main area is titled 'Select Probe' and asks the user to select the probes they want to activate. There are two radio button options: 'NetBackup Resources Monitor and Compute Resources (Probe to collect NetBackup Server details, OS and Hardware metrics)' which is selected, and 'Compute Resources (Probe to collect OS and Hardware metrics)'. Below the options are four input fields: 'Data Collector Hostname(FQDN)*', 'Data Sender Certificate*' (with a 'Choose' button), 'Compute Resource Sender ID*', and 'NetBackup Sender ID*'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons. The Veritas logo is in the bottom left.

- 6 Click **Next** to initiate the installation and click **Finish** once the installation is complete.



The screenshot shows the 'Finish' step of the NetBackup IT Analytics Exporter installation. The left sidebar lists the steps: Welcome, License Agreement, User Input, Summary, Progress, Post Install, and **Finish**. The main area displays a congratulatory message: 'Congratulations! The NetBackup IT Analytics Exporter has been successfully installed to: C:\Program Files\Veritas\ITAnalytics'. It also lists the services started: 'NetBackup IT Analytics NetBackup Exporter Service', 'NetBackup IT Analytics Windows Exporter Service', and 'NetBackup IT Analytics Datasender Service'. Below this, it provides the path to the log files: 'C:\ProgramData\Veritas\NetBackup IT Analytics\Exporters\installer_logs' and instructs the user to 'Press "Finish" to quit the installer.' At the bottom are 'Logs' and 'Finish' buttons. The Veritas logo is in the bottom left.

The NetBackup IT Analytics Exporter is always installed at `C:\Program Files\Veritas\ITAnalytics` and the logs are saved to `C:\ProgramData\Veritas\NetBackup IT Analytics\Exporters\installer_logs` directory.

Install the exporter on Windows host using response file

You can also install the exporter on a Windows host using a response file. Ensure you have addressed all the prerequisites before proceeding for the exporter installation. You can obtain the response file template from the ISO downloaded from Cohesity Download Center on the Windows host. The values that you must configure in the response file are described in the table below.

See [“Prerequisites for exporter installation”](#) on page 7.

Table 3-1 Response file inputs

Response file parameters	Description
SET COLLECTOR_HOST	Fully qualified domain name (FQDN) of the data collector server.
SET PROBE_ID	Accepts 1 or 2 as values for probe selection. If you enter 1 , NetBackup and Compute Resources probe is enabled. If your set value is 2 , Compute Resources probe is enabled.
SET DATASENDER_CERT_PATH	Absolute path of the data sender certificate file downloaded from NetBackup IT Analytics Portal.
SET COMPUTE_RES_SENDER_ID	Sender ID copied from NetBackup IT Analytics Portal. The ID is available from the Compute Resources probe of the Compute Resources policy and is required if the PROBE_ID is set to 1 or 2 .
SET NBU_SENDER_ID	Sender ID copied from NetBackup IT Analytics Portal. The ID is available from the NetBackup Resource Monitor probe of the NetBackup policy and is required if the PROBE_ID is set to 1 .

Once your response file is ready, you can proceed with the installation.

To install the exporter using the response file:

- 1 Run the `silentinstall.cmd` installer script with the response file as an argument.

```
Silentinstall.cmd <responsefile>
```

The installer displays the End User License Agreement (EULA).

In case you are reinstalling the exporter, the installer asks permission to overwrite the previously installed files on your system.

- 2 Accept the EULA and continue with the installation.

The exporter is installed according to the configuration of the response file.

The NetBackup IT Analytics Exporter is always installed at `C:\Program Files\Veritas\ITAnalytics` and the logs are saved to

`C:\ProgramData\Veritas\NetBackup IT Analytics\Exporters\installer_logs` directory.

Exporter service management on Windows

The following Windows services are created and started by installer:

```
NetBackup IT Analytics DataSender Service  
NetBackup IT Analytics NetBackup Exporter Service  
NetBackup IT Analytics Windows Exporter Service
```

You can stop all the services related to the NetBackup IT Analytics exporter with:

```
C:\Program Files\Veritas\ITAnalytics\bin\
```

```
stopallexporterservices.bat
```

You can start all the services related to the NetBackup IT Analytics exporter with:

```
C:\Program Files\Veritas\ITAnalytics\bin\
```

```
startallexporterservices.bat
```

ISO-based upgrade on Windows host

Ensure you have addressed the prerequisites specified for the exporter installation before you proceed to upgrade or reinstall the exporter.

See [“Prerequisites for exporter installation”](#) on page 7.

Run the `Setup.exe` from the new version of ISO.

Configure the NetBackup IT Analytics Exporter

This chapter includes the following topics:

- [Configure the NetBackup exporter](#)
- [Configure Node exporter](#)
- [Configure Process exporter](#)
- [Configure Windows exporter](#)
- [Configure Data Sender](#)

Configure the NetBackup exporter

To configure the NetBackup exporter, you must configure the `netbackup.yaml` file from the following location:

- **Linux:** `/opt/itanalytics/config/netbackup.yaml`
- **Windows:** `C:\Program Files\Veritas\ITAnalytics\config\netbackup.yaml`

Collectors within the exporter

The collectors embedded within the exporter are described in the table below. The scope of metrics collected by the NetBackup exporter is defined below. Other metrics are collected by the Node or Windows exporter.

Table 4-1 Collectors within the exporter

Collector	Collects
bp_configuration	NetBackup busy file processing details.

Table 4-1 Collectors within the exporter (*continued*)

Collector	Collects
host_certificates	Metrics for expiring host certificate.
jks_certificates	Collector checks key-store file for expiring non-host certificates.
nbdb_file_stats	NetBackup database file details.
net_stats	Connection details for pbx_exchange, vnetd, bpcd, inbound_proxy, outbound_proxy, nbdisco, nbsl, nbsvcmon, nbrmms, vmd, nbatd, NB_dbsrv, bpdbm, bpjobd, bprd, nbpem, nbjm, nbstserv, nbemm, nbrb, nbevtmgr, nbaudit, nbwmc, bpcompatd, nbvault, and nbars processes.
pbx_exchange_stats	Details for connections made to pbx_exchange process.
physical_devives_stats	Information about the available block devices. Collector is disabled for Windows host.
service_responsiveness	Status information of running processes, such as pbx_exchange, vnetd, bpcd, inbound_proxy, outbound_proxy, nbdisco, nbsl, nbsvcmon, nbrmms, vmd, nbatd, NB_dbsrv, bpdbm, bpjobd, bprd, nbpem, nbjm, nbstserv, nbemm, nbrb, nbevtmgr, nbaudit, nbwmc, bpcompatd, nbvault, and nbars.

The configuration parameters of the `netbackup.yaml` are described in the table below followed by a sample `netbackup.yaml` configuration file.

Table 4-2 Parameters of `netbackup.yaml` file

Parameter	Description
host	The host on which the the server runs. The default is localhost.
port	The port through which the exporter communicates: The default port is 9099.
install_path	If NetBackup is not installed at its default location, you need to specify its path here.
log_level	The default log level for the collectors. You can set it as error , warn , or debug . The default log level is info . You can configure different values for different collectors.

Table 4-2 Parameters of `netbackup.yaml` file (*continued*)

Parameter	Description
<code>collector_overrides</code>	A map keyed by the name of the collector which you can override the <code>poll_interval</code> and <code>log_level</code>. To disable an individual collector, set <code>enabled: false</code>. Collectors not mentioned in this map key are enabled by default. Exclude <code>physical_device_stats</code> collector if the exporter is configured to run on Windows.
<code>key_stores</code>	The list of key stores that you want the <code>jks_certificates</code> collector to check. For <code>jks_certificates</code> of a collector, you can added multiple keystore files to collect data in the same manner. The exporter can process collector keystore files of type <code>.jks</code> and <code>.bcfks</code> without the configuration of this property. For keystore files of other types, you must specify <code>store_type</code> and <code>provider_path</code> values..
Each key store entry has the following properties:	
<code>name</code>	The store label in the metrics.
<code>key_file</code>	The file that stores the keystore password.
<code>store_file</code>	Path to the keystore file.
<code>alias</code>	Alias name of the exported certificates.
<code>store_type</code>	Property that sets the <code>-storetype</code> switch while running the <code>keytool</code> command.
<code>provider_path</code>	Property that sets the <code>-providerpath</code> switch while running the <code>keytool</code> command.
<code>provider</code>	Property that sets the <code>-provider</code> switch while running the <code>keytool</code> command.

Example of `netbackup.yaml` file for Linux

```
host: localhost
port: 9099
install_path: /usr/openv
```

```
log_level: info
collector_overrides:
  bp_configuration:
    poll_interval: 10s
    log_level: info
    enabled: true
  host_certificates:
    poll_interval: 300s
    log_level: info
    enabled: true
  jks_certificates:
    poll_interval: 600s
    log_level: info
    enabled: true
  nbdb_file_stats:
    poll_interval: 86400s
    log_level: info
    enabled: true
  net_stats:
    poll_interval: 3600s
    log_level: info
    enabled: true
  pbx_exchange_stats:
    poll_interval: 300s
    log_level: info
    enabled: true
  physical_device_stats:
    poll_interval: 300s
    log_level: info
    enabled: true
  service_responsiveness:
    poll_interval: 10s
    log_level: info
    enabled: true
key_stores:
- name: vxss
  key_file: /usr/opensv/var/global/jkskey
  store_file:
    /usr/opensv/var/global/vxss/tomcatcreds/nbwebsevice.bcfks
  alias: nbwmc
  store_type: BCFKS
  provider_path: /usr/opensv/java/bcprov-jdk15on-168.jar
  provider: org.bouncycastle.jce.provider.BouncyCastleProvider
```

```
- name: wsl
  key_file: /usr/openssh/var/global/jkskey
  store_file:
/usr/openssh/var/global/wsl/credentials/nbwebsservice.bcfks
  alias: nbwmc
  store_type: BCFKS
  provider_path: /usr/openssh/java/bcprov-jdk15on-168.jar
  provider: org.bouncycastle.jce.provider.BouncyCastleProvider
```

Note: If `netbackup.yaml` file is missing or not configured correctly, the collectors collect metrics based on the default values.

Example of `netbackup.yaml` file for Windows

```
host: localhost
port: 9099
install_path: C:\Program Files\Veritas
log_level: info
collector_overrides:
  bp_configuration:
    poll_interval: 10s
    log_level: info
    enabled: true
  host_certificates:
    poll_interval: 300s
    log_level: info
    enabled: true
  jks_certificates:
    poll_interval: 600s
    log_level: info
    enabled: true
  nbdb_file_stats:
    poll_interval: 86400s
    log_level: info
    enabled: true
  net_stats:
    poll_interval: 3600s
    log_level: info
    enabled: true
  pbx_exchange_stats:
    poll_interval: 300s
    log_level: info
    enabled: true
```

```

    physical_device_stats:
      poll_interval: 300s
      log_level: info
      enabled: false
    service_responsiveness:
      poll_interval: 10s
      log_level: info
      enabled: true
  key_stores:
    - name: vxss
      key_file: C:\Program Files\Veritas\NetBackup\var\global\jkskey
      store_file: C:\Program
Files\Veritas\NetBackup\var\global\vxss\tomcatcreds\nbwebbservice.bcfks

      alias: nbwmc
      store_type: BCFKS
      provider: org.bouncycastle.jce.provider.BouncyCastleProvider
      provider_path: C:\Program
Files\Veritas\NetBackup\Java\bcprov-jdk15on-168.jar
    - name: wsl
      key_file: C:\Program Files\Veritas\NetBackup\var\global\jkskey
      store_file: C:\Program
Files\Veritas\NetBackup\var\global\wsl\credentials\nbwebbservice.bcfks

      alias: nbwmc
      store_type: BCFKS
      provider_path: C:\Program
Files\Veritas\NetBackup\Java\bcprov-jdk15on-168.jar
      provider: org.bouncycastle.jce.provider.BouncyCastleProvider

```

Configure Node exporter

Node exporter is an open-source Prometheus exporter to collect hardware and OS level metrics. It supports various collectors that can be configured to collect data from prime resources running on Linux operating system. It can export data from system resources such as RAM, disk, CPU, Network, and more. The exporter exposes the collected metrics on port 9100 and path /metrics.

Since running the Node exporter without any configuration enables all of its default collectors, no specific configuration is required for the exporter.

For additional information such as collectors and sample configuration templates, see https://github.com/prometheus/node_exporter.

Configure Process exporter

Process exporter is an open-source Prometheus exporter and it collects metrics from pre-specified processes of a Linux machine. It consists of a single collector and derives the metrics for specific processes from `/proc` location by default. The exporter is exposed on port 9256 with path `/metrics`. Since running the Process exporter without any configuration enables all of its default collectors, no specific configuration is required for the exporter.

For additional information such as collectors and sample configuration templates, see <https://github.com/ncabatoff/process-exporter>.

Configure Windows exporter

Windows exporter is an open-source Prometheus exporter designed to collect metrics from a Windows host. The collector exposes all the collected metrics on port 9182 on path `/metrics`. Since running the Windows exporter without any configuration enables all of its default collectors, no specific configuration is required for the exporter.

For additional information such as collectors and sample configuration templates, see https://github.com/prometheus-community/windows_exporter

Note: You can ignore the error `level=error msg="Failed to start service: The service process could not connect to the service controller." source="exporter.go:337"` if you see it when you start the exporter. The error may appear as the exporter is configured to run as a service on the a Windows server.

Configure Data Sender

Data Sender acts as a Prometheus server for all exporters, be it NetBackup IT Analytics Exporter or other third-party exporters. It pulls scraped data from exporters configured with it and pushes it to the Data Collector. Depending on the probe selection during the exporter installation, the default Data Sender will get configured for the applicable exporters. For Compute Resources probe, Data Sender for Node and Process exporter data is enabled for Linux OS and Data Sender for Windows exporter is enabled for Windows OS 1.

For NetBackup Resources Monitor probe, Data Sender for NetBackup IT Analytics Exporter will be enabled.

To configure the Data Sender, you must configure the `datasender.yaml` file from the following location:

- On Linux: `/opt/itanalytics/config/datasender.yaml`
- On Windows: `C:\Program Files\Veritas\ITAnalytics\config\datasender.yaml`

Since the probe selection during the NetBackup IT Analytics Exporter installation governs the Data Sender configuration, it does not require a separate configuration. However, to make changes to the poll interval or to the metrics collection, you must edit the `datasender.yaml` configuration file based on the property description below.

Table 4-3 `datasender.yaml` properties

Property	Description
<code>host_name</code>	System host name on which Data Sender will run. Default value will be system host name.
<code>destination_url</code>	URL of the NetBackup IT Analytics Data Collector where the scraped data will be pushed.
<code>destination_certificate_file</code>	Absolute path of the Data Sender's certificate file. The certificate file must be downloaded from the appropriate Data Collector policy screen based on the probe selection.
<code>data_directory</code>	Relative path of the directory for saving the collected data files. Default value is <code>/data</code> .
<code>log_level</code>	Logging level for Data Sender logs - trace, info, debug, warn, or error. Default will be info .
<code>gzip</code>	Flag for gzip post request content. Default value is set to true .
<code>exporters</code>	List of exporters with their scraping details:
<code><EXPORTER_NAME></code>	Exporter name.
<code>source_url</code>	URL on which the exporter is exposing its metrics.
<code>job_id</code>	The Sender ID provided during the NetBackup IT Analytics Exporter installation.
<code>job_type</code>	Set the value as host for all exporters.

Table 4-3 `datasender.yaml` properties (*continued*)

Property	Description
<code>jobs</code>	List of jobs running independently and collecting metrics.
	■ <code>job_name</code>: Name of the specified scraped data job. ■ <code>poll_interval</code>: Interval in seconds between two consecutive data collection jobs. ■ <code>gzip</code>: Flag for gzip post request content. ■ <code>target_metrics</code>: Defines the metrics to be sent to the Data Collector.

Sample Data Sender Configuration for Linux

```
# host_name: "nbl.example.com"
destination_url: "https://DC_HOSTNAME:8883/metrics"
destination_certificate_file: "/opt/itanalytics/config/DC_CERT_FILE"
# data_directory: "data/"
# log_level: "info"
# gzip: true

exporters:
  netbackup:
    source_url: "http://127.0.0.1:9099/metrics"
    job_id: "job_id_1"
    job_type: "host"
    jobs:
      - job_name: "nb_host_certificate"
        poll_interval: 86400 # daily
        gzip: true
        target_metrics: [ "netbackup_host_certificate_active",
                          "netbackup_host_certificate_issued_on_seconds",
                          "netbackup_host_certificate_updated_on_seconds",
                          "netbackup_host_certificate_valid_from_seconds",
                          "netbackup_host_certificate_valid_until_seconds" ]

      - job_name: "nb_keystore"
        poll_interval: 86400 # daily
        target_metrics: [ "netbackup_keystore_created_on_seconds",
                          "netbackup_keystore_valid_from_seconds",
                          "netbackup_keystore_valid_to_seconds" ]
```

```
- job_name: "nb_responsiveness"
poll_interval: 300 # 5 minutes
target_metrics: [ "netbackup_process_running",
                  "netbackup_process_responsive_seconds" ]

- job_name: "nb_configuration"
poll_interval: 86400 # daily
target_metrics: [ "netbackup_bp_config_state",
                  "netbackup_process_primary_server",
                  "netbackup_process_media_server" ]

- job_name: "nb_netstat"
poll_interval: 3600 # 1 hour
target_metrics: [ "netbackup_connection_active" ]

- job_name: "nb_dbfile"
poll_interval: 3600 # 1 hour
target_metrics: [ "netbackup_dbfile_bytes",
                  "netbackup_dbfile_mod_time_seconds" ]

- job_name: "nb_pbxexchange"
poll_interval: 300 # 5 minutes
target_metrics: [ "netbackup_pbx_exchange_number_of_connections" ]

- job_name: "nb_scrapeinfo"
poll_interval: 1800 # 30 minutes
target_metrics: [ "netbackup_scrape_success",
                  "netbackup_scrape_duration_seconds" ]

- job_name: "nb_buildinfo"
poll_interval: 86400 # daily
target_metrics: [ "netbackup_exporter_build_info" ]

node:
  source_url: "http://127.0.0.1:9100/metrics"
  job_id: "job_id_10"
  job_type: "host"
  jobs:
    - job_name: "node_all"
      poll_interval: 300 # 5 minutes

process:
  source_url: "http://127.0.0.1:9256/metrics"
```

```
job_id: "job_id_20"
job_type: "host"
jobs:
  - job_name: "process_all"
    poll_interval: 900 # 15 minutes
```

Sample Data Sender Configuration for Windows

```
# host_name: "nbl.example.com"
destination_url: "https://DC_HOSTNAME:8883/metrics"
destination_certificate_file: "C:\\Program Files\\Veritas\\IT
Analytics\\config\\DC_CERT_FILE"
# data_directory: "data/"
# log_level: "info"
# gzip: true

exporters:
  netbackup:
    source_url: "http://127.0.0.1:9099/metrics"
    job_id: "job_id_1"
    job_type: "host"
    jobs:
      - job_name: "nb_host_certificate"
        poll_interval: 86400 # daily
        gzip: true
        target_metrics: [ "netbackup_host_certificate_active",
                          "netbackup_host_certificate_issued_on_seconds",
                          "netbackup_host_certificate_updated_on_seconds",
                          "netbackup_host_certificate_valid_from_seconds",
                          "netbackup_host_certificate_valid_until_seconds" ]

      - job_name: "nb_keystore"
        poll_interval: 86400 # daily
        target_metrics: [ "netbackup_keystore_created_on_seconds",
                          "netbackup_keystore_valid_from_seconds",
                          "netbackup_keystore_valid_to_seconds" ]

      - job_name: "nb_responsiveness"
        poll_interval: 300 # 5 minutes
        target_metrics: [ "netbackup_process_running",
                          "netbackup_process_responsive_seconds" ]

      - job_name: "nb_configuration"
        poll_interval: 86400 # daily
```

```
target_metrics: [ "netbackup_bp_config_state",
                  "netbackup_process_primary_server",
                  "netbackup_process_media_server" ]

- job_name: "nb_netstat"
poll_interval: 3600 # 1 hour
target_metrics: [ "netbackup_connection_active" ]

- job_name: "nb_dbfile"
poll_interval: 3600 # 1 hour
target_metrics: [ "netbackup_dbfile_bytes",
                  "netbackup_dbfile_mod_time_seconds" ]

- job_name: "nb_pbxexchange"
poll_interval: 300 # 5 minutes
target_metrics: [ "netbackup_pbx_exchange_number_of_connections" ]

- job_name: "nb_scrapeinfo"
poll_interval: 1800 # 30 minutes
target_metrics: [ "netbackup_scrape_success",
                  "netbackup_scrape_duration_seconds" ]

- job_name: "nb_buildinfo"
poll_interval: 86400 # daily
target_metrics: [ "netbackup_exporter_build_info" ]

windows:
  source_url: "http://127.0.0.1:9182/metrics"
  job_id: "job_id_30"
  job_type: "host"
  jobs:
    - job_name: "windows_exporter_all"
      poll_interval: 300 # 5 minutes
```

Troubleshooting

This appendix includes the following topics:

- [Resolve NetBackup exporter issues](#)
- [Resolve Node exporter issues](#)
- [Resolve Process exporter issues](#)
- [Resolve Windows exporter issues](#)
- [Resolve Data Sender issues](#)
- [Log locations](#)
- [Resolves invalid sender ID related to security changes](#)

Resolve NetBackup exporter issues

Ideally, a simple restart of the exporter must resolve any issues observed during its operations. However, these generic steps help you troubleshoot any issues seen in the NetBackup exporter operations on the respective hosts.

On Linux host

- 1 Ensure the NetBackup Exporter service is running. The `itanalytics_netbackup_exporter.service` service is available in the `/etc/systemd/system` directory.
 - Check the service status using `systemctl status itanalytics_netbackup_exporter.service` on the terminal.

- If the service has stopped, start it using `systemctl start itanalytics_netbackup_exporter.service`.
- 2 Verify whether the exporter is exposing the metrics on 9099 port and path `/metrics`, using the `curl http://127.0.0.1:9099/metrics` command.
If it gives a Prometheus output as a response, then the NetBackup exporter is working fine. If not, restart the service and check again.
- 3 Check whether all collectors are enabled in the configuration file. If not then enable them and restart the NetBackup exporter service.
See [“Configure the NetBackup exporter”](#) on page 24.
- 4 Check for detailed logs at
`<INSTALLATION_PATH>/itanalytics/logs/netbackup_exporter.log`.

On Windows host

- 1 Ensure the NetBackup Exporter service is running from the Windows Services console. The service available by the name **NetBackup IT Analytics NetBackup Exporter Service**. Restart the service if required.
- 2 Ensure the metrics exposed by the NetBackup exporter on the specified path is reachable. All metrics are exposed on the running host at port 9099 and path `/metrics`.
To check:
 - Open any of the installed browsers on the same host.
 - Check the response for the URL `http://127.0.0.1:9099/metrics`.
If you get a Prometheus metrics output as a response, then the NetBackup exporter is running fine. Otherwise, restart the service and check again.
- 3 Check whether all collectors (excluding `physical_device_stats`) are enabled in the configuration file. If not then enable them and restart the NetBackup exporter service.
See [“Configure the NetBackup exporter”](#) on page 24.
- 4 Check whether following NetBackup exporter logs are available on the Windows host.
 - Detailed logs are available under
`<INSTALLATION_PATH>/ITAnalytics/logs/`
 - `ITAnalyticsNetBackupExporterService.<TIME_STAMP>.log` on Windows host.
 - `itanalyticsnetbackupexporterservice-stderr.<TIME_STAMP>.log` on Windows host.

- `itanalyticsnetbackupexporterservice-stdout.<TIME_STAMP>.log` on Windows host.

Resolve Node exporter issues

On Linux host

- 1 Ensure the Node exporter service is running. The service available at `itanalytics_node_exporter.service`.
 - Check the service status using `systemctl status itanalytics_node_exporter.service` on the terminal.
 - If the service has stopped, start it using `systemctl start itanalytics_node_exporter.service`.
- 2 Verify whether the exporter is exposing the metrics on 9100 port and path `/metrics`, using the `curl http://127.0.0.1:9100/metrics` command.

If you get an output, then the exporter is working well. If not, restart the service and check again.
- 3 Check for detailed logs at `<INSTALLATION_PATH>/itanalytics/logs/node_exporter.log`.

Resolve Process exporter issues

On Linux host

- 1 Ensure the Process exporter service is running. The service available at `itanalytics_process_exporter.service`.
 - Check the service status using `systemctl status itanalytics_process_exporter.service` on the terminal.
 - If the service has stopped, start it using `systemctl start itanalytics_process_exporter.service`.
- 2 Verify whether the exporter is exposing the metrics on 9256 port and path `/metrics`, using the `curl http://127.0.0.1:9256/metrics` command.

If you get an output, then the exporter is working well. If not, restart the service and check again.
- 3 Check for detailed logs at `<INSTALLATION_PATH>/itanalytics/logs/process_exporter.log`.

Resolve Windows exporter issues

- 1 Ensure the Windows exporter service is running from the Windows Services console. The service available by the name **NetBackup IT Analytics Windows Exporter Service**. Restart the service if required.
- 2 Ensure the metrics exposed by the Windows exporter on the specified path is reachable. All metrics are exposed on the running host at port 9182 and path `/metrics`.

To check:

- Open any of the installed browsers on the same host.
- Check the output given by the URL `http://127.0.0.1:9182/metrics`.

If you seen some output on the browser then it is working fine, else restart the service and check again.

- 3 Check whether following Windows exporter logs are available on the Windows host.
 - Detailed logs are available under `<INSTALLATION_PATH>/ITAnalytics/logs/`.
 - `ITAnalyticsWindowsExporterService.<TIME_STAMP>.log` on Windows host.
 - `itanalyticswindowsexporterservice-stderr.<TIME_STAMP>.log` on Windows host.
 - `itanalyticswindowsexporterservice-stdout.<TIME_STAMP>.log` on Windows host.

Resolve Data Sender issues

On Linux host

- 1 Ensure the Data Sender service is running. The service available at `itanalytics_datasender_exporter.service`.
 - Check the service status using `systemctl status itanalytics_datasender_exporter.service` on the terminal.
 - If the service has stopped, start it using `systemctl start itanalytics_datasender_exporter.service`.
- 2 Check for configuration as follows:

- Check whether the Data Sender is configured to pull scraped metrics from the configured exporters. Sample configuration files are available under `<INSTALLATION_PATH>/itanalytics/config/template`, from where it can be verified.
 - Check the validity of the sender IDs of Compute Resource probe and NetBackup Resources Monitor probe (if installed).
 - Check whether the destination URL provided to the Data Sender to push collected metrics is reachable.
 - If the Data Collector URL is not reachable using the default port 8883 and a custom port is configured on the Portal, the destination URL can look like `https://<hostname>:<port>/metrics`. You can open this URL in a browser for verification or can verify via a curl command (`curl https://<hostname>:<port>/metrics`) to check the response.
 - You can dump metrics to the local file system of the Data Sender to verify whether all collected metrics are getting pushed to the data collector server. You can uncomment the `data_directory` property in the configuration file and restart the Data Sender service to achieve this. However, since this can generate lot of data, you must comment it back when not required.
- 3 Ensure the SSL Certificate provided to the Data Sender to connect to the NetBackup IT Analytics Data Collector is valid.
 - 4 Check for detailed logs at
`<INSTALLATION_PATH>/itanalytics/logs/datasender.log`.

On Windows host

- 1 Ensure the Data Sender service is running from the Windows Services console. The service available by the name **NetBackup IT Analytics NetBackup Datasender Service**. Restart the service if required.
- 2 Check for the following configurations:
 - Check whether the Data Sender is configured to pull scraped metrics from the configured exporters. Template configuration files are available under `<INSTALLATION_PATH>/itanalytics/config/template`, from where it can be verified.
 - Check the validity of the sender IDs of Compute Resources probe and NetBackup Resources Monitor probe (if installed).
 - Check whether the destination URL provided to the Data Sender to push collected metrics is reachable.
 - If the Data Collector URL is not reachable using the default port 8883 and a custom port is configured on the Portal, the destination URL can look like

`https://<hostname>:<port>/metrics`. You can open this URL in a browser for verification or can verify via a curl command (`curl https://<hostname>:<port>/metrics`) to check the response.

- You can dump metrics to the local file system of the Data Sender to verify whether all collected metrics are getting pushed to the data collector server. You can achieve by uncommenting the `data_directory` property in the configuration file and restarting the Data Sender service. However, since this can generate lot of data, you must comment it back when not required.
- 3** Ensure the metrics exposed by the NetBackup exporter on the specified path is reachable. All metrics are exposed on the running host at port 9099 and path `/metrics`.

To check:

- Open any of the installed browsers on the same host.
- Check the output given by the URL `http://127.0.0.1:9099/metrics`

If you seen some output on the browser then it is working fine, else restart the service and check again.

- 4** Ensure the SSL Certificate provided to the Data Sender to connect to the NetBackup IT Analytics Data Collector is valid.
- 5** Check whether following Data Sender logs are available on the Windows host.
- Detailed logs are available under `<INSTALLATION_PATH>/ITAnalytics/logs/`.
 - `ITAnalyticsDatasenderService.<TIME_STAMP>.log` on Windows host.
 - `itanalyticsdatasenderservice-stderr.<TIME_STAMP>.log` on Windows host.
 - `itanalyticsdatasenderservice-stdout.<TIME_STAMP>.log` on Windows host.

Log locations

On Linux host

While you can find all logs under `/opt/itanalytics/logs`, component-specific log locations are provided below:

- Data Sender logs: `datasender.log`
- NetBackup Exporter logs: `netbackup_exporter.log`

- Process exporter logs: `process_exporter.log`
- Installation process logs: `exporter_installer_<TIMESTAMP>.log`

On Windows host

Logs are available under `C:\Program Files\Veritas\ITAnalytics\logs` directory.

Resolves invalid sender ID related to security changes

If the Data Collector version is 11.3 or above and NetBackup IT Analytics Exporter version installed on Windows or Linux hosts (including NetBackup Primary Servers) is below 11.3, then you must again copy the Compute Resource Sender ID and NetBackup Sender ID to the NetBackup IT Analytics Exporter configuration and restart the exporter services as described below.

Step-1: Depending on the Data Collector policy and probe that is configured, get the Sender ID as follows from the Portal:

- 1 For NetBackup Resources Monitor probe, go to **Admin** tab > **Data Collection** > **Collector Administration** and select the **Veritas NetBackup Data Collector Policy** assigned to the NetBackup Primary Server. On the policy screen, click the **Copy Sender ID** icon next to the **NetBackup Resources Monitor** probe label
- 2 For Compute Resource probe, go to **Admin** tab > **Data Collection** > **Collector Administration** and select the **Compute Resources Data Collector Policy** assigned to the Windows or Linux hosts (including NetBackup Primary Servers). On the policy screen, click the **Copy Sender ID** icon next to the **Compute Resources** probe label

Step-2: Configure NetBackup IT Analytics Exporter installed on Windows or Linux hosts (including NetBackup Primary Servers) with the new Sender ID:

- 1 Logon to the Windows or Linux hosts (including NetBackup Primaries) that has Exporter services installed.
- 2 Stop NetBackup IT Analytics Exporter services.
 - Linux: `/opt/itanalytics/bin/exporter_services stop`
 - Windows: `C:\Program Files\Veritas\ITAnalytics\bin\stopallexporterservices.bat`

3 Update configuration file to have the latest Compute Resource Sender ID or NetBackup Resource Monitor Sender ID.

Linux host: /opt/itanalytics/config/datasender.yaml

- Copy the NetBackup Resource Monitor Probe Sender ID to job_id attribute under "netbackup" exporters.
- Copy the Compute Resource Sender ID to job_id attribute under "node" and "process" exporters.
- Sample of datasender.yaml after modification:

```
netbackup:
  # URL of the metric exporter
  source_url: "http://127.0.0.1:9099/metrics"
  # 'id' header to be sent with the post
  job_id:
    "RsaAes.AAAADAAAQDj5trM6J9iRwjGZMoR0Unr3dF0p8f5yLIb0
    VxpIeTna+x6WDEzzupTncFqRaRJS/F9XrSgsHBTPwrr93RMQ+kFrpA6XW07h6qAJxYr
    K7S/VtC9ad3NjFYZXEog133l77R8zoGd+eLY6BZ5db50bzRC7YOkFlekwzt/zMEWgzj
    5WNNe7o6E4DKKsQ8vNaowzJyhQUww6+gpAfw0IydC/sHzyvY4/ZoWSQ8s3WEZXUa/e6Hi
    ROSyDAKp8asdqBiHXPzRlRj8zYm4iMaLoLMUfsobVD1kpQaJ8XQP6Ec2EY5o5r0xJbYzp0
    AbC+gv9KEFFCWj5cFACzd3v4JB2KL6bhWd0wCyufT8MlrxpHG/t7+fcCZgP2xTY186FNmj
    K5C1NjOapIWlukfli++cn249dIFIE1PK1+2N52wTRjcbLtl593TuzR85I+RV+ErnIQh
    F3g4moFBOhgtbPk7Ei67ScNppt34rUXPyfqJ3CKMO"
  # 'type' header to be sent with the post
  job_type: "host"
  ...
  ...
node:
  source_url: "http://127.0.0.1:9100/metrics"
  job_id:
    "RsaAes.AAAADAAAQCgUPONRZpYRqk2Q5N6ao4e7HVgl/3fvyhwrr59
    A8SQMqX4Vj1AkiT/j2QPXydIo+QiB8EXUK3CTflnR2MhY/qG8XOP1COUZhgm7XRJUi/1
    ZJT8B7bRKv87F70hOrancAVuF7lLcuz/dr7SZv7LVX46bZy9xbZwGFF5gS/yb8hHgLuH
    OZdTklmfoYNvulJqF9q+YkBWlcu0iDh2wKcQDmE8kRQhJhJhNalQX0TJTqR9fYvSFzn
    8oEKKU3jXIQSwF4+by6La3NvkPgdy/4zdkW8TpcpeMYIpYmX0hAUSVdmNBvhLjYgb0g
    uAL/D4lOvcIwOqRZmIhmFT3MeUktOetr4XQ4XdbYzQBsrYgkLYOUWq/YVc2MtDEOPYd
    mBq/dH1BUB6AWfcf+3Gx1hvM0WvEIxmZ6V7cDrRaAjtUUp80I+Z33bilnXipvAP6jbsY
    UDG77LdObsNFkMgcmFXyUixRPJTRAg=="
  job_type: "host"
jobs:
  - job_name: "node_all"
    poll_interval: 300 # 5 minutes
```

```
process:
  source_url: "http://127.0.0.1:9256/metrics"
  job_id:
    "RsaAes.AAAADAAAACgUPONRZpYRqk2Q5N6ao4e7HVgl/3fvyhwrr59
    A8SQMqX4Vj1AkiT/j2QPXydIo+QiB8EXUK3CTflnR2MhY/qG8XOPlCOUZhgm7XRJUi/1
    ZJT8B7bRKv87F70hOrancAVuF71Lcuz/dr7SZv7LVX46bZy9xbZwGFF5gS/yb8hHgLuH
    OZdTkcClmfOyNVu1JqF9q+YkBW1cu0iDh2wKcQDmE8kRQOhJhNalQX0TJTqR9fYvSFzn8o
    EKKU3jXIQSwF4+by6La3NvkPgdy/4zdkW8TpcpeMYIpYmX0hAUSVdmNBvhLjYgb0gu
    AL/D4lOvcIwOqRZmIhmFT3MeUktOetr4XQ4XdbYZQBsrSgkLYOUWq/YVc2MtDEOPYdm
    Bq/dH1Bub6AWfcf+3Gx1hvM0WvEIxmZ6V7cDrRaAjtuUp8OI+Z33biInXipvAP6jbSYU
    DG77LdObSNfKMgcmFXyUixRPJTRAg=="
  job_type: "host"
  jobs:
    - job_name: "process_all"
      poll_interval: 900 # 15 minutes
```

Windows host: C:\Program

Files\Veritas\ITAnalytics\config\datasender.yaml

- Copy the NetBackup Resource Monitor Probe Sender ID to job_id attribute under "netbackup" exporters
- Copy the Compute Resource Sender ID to job_id attribute under "windows" exporters
- Sample of datasender.yaml after modification:

```
netbackup:
  # URL of the metric exporter
  source_url: "http://127.0.0.1:9099/metrics"
  # 'id' header to be sent with the post
  job_id:
    "RsaAes.AAAADAAAQDj5trM6J9iRwjGZMoR0Unr3dF0p8f5yLib0Vxp
    IeTna+x6WDEzzupTncFqRaRJS/F9XrSgsHBTPwrr93RMQ+kFrpA6XW07h6qAJxYrK7
    S/VtC9ad3NjFYZXEogl33177R8zoGd+eLY6BZ5db50bzRC7YOkFlekwt/zMEWgzj5W
    Ne7o6E4DKKsQ8vNaowzJyhQUww6+gpAfw0IydC/sHzYvY4/ZoWSQ8s3WEZxuA/e6HiROSy
    DAKp8asdqBiHXPzR1Rj8zYm4iMaLoLMUfsobVD1kpQaJ8XQP6Ec2EY5o5r0xJbYzp0Ab
    C+gv9KEFFCWj5cFACzd3v4JB2KL6bhWd0wCyufT8M1rxpHG/t7+fcCZGp2xTY186F
    Nmjk5C1NjOapIWlufli++cn249dIFIE1PK1+2N52wTRjcbLt1s93TuzR85I+RV+Ern
    IQhF3g4moFBOhgtbPk7Ei67ScNppt34rUXPyfqJ3CKMO"
  # 'type' header to be sent with the post
  job_type: "host"
  jobs:
    ...
    ...
```

```

windows:
  source_url: "http://127.0.0.1:9182/metrics"
  job_id:
    "RsaAes.AABCDAAAAQDj5trM6J9iRwjGZMoR0Unr3dF0p8f5yLib0VxpIe
    Tna+x6WDEzzupTncFqRaRJS/F9XrSgsHBTPwrr93RMQ+kFrpA6XW07h6qAJxYrK7S/VtC9
    ad3NjFYZXEog133177R8zoGd+eLY6BZ5db50bzRC7YOkF1ekwzt/zMEWgzj5WNe7o6E4DK
    KsQ8vNaowzJyhQUww6+gpAfw0IydC/sHzYvY4/ZoWSQ8s3WEZXUa/e6HiROSyDAKp8asdq
    BiHXPzR1Rj8zYm4iMaLoLMUfsobVD1kpQaJ8XQP6Ec2EY5o5r0xJbYzp0AbC+gv9KEFFCW
    j5cFACzd3v4JB2KL6bhWd0wCyufT8M1rxpHG/s/t7+fcCZgP2xTY186FNmjK5C1NjOapIW1
    ukfli++cn249dIFIE1PK1+2N52wTRjcbLt1s93TuzR85I+RV+ErnIQhF3g4moFB0hgtbPk
    7Ei67ScNppt34rUXPyfqJ3CKMO"
  job_type: "host"
  jobs:
    - job_name: "windows_exporter_all"
      poll_interval: 300 # 5 minutes

```

4 Start the NetBackup IT Analytics Exporter services.

Linux: /opt/itanalytics/bin/exporter_services start

Windows: C:\Program

Files\Veritas\ITAnalytics\bin\startallexporterservices.bat