IT Analytics Foundation License Inclusions and Implementation Guide

Release: 11.8

COHESITY

IT Analytics Foundation License Inclusions and Implementation Guide

Last updated: 2026-10-01

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

Section 1 Foundation License - Inclusion and Installation 7

Chapter 1 Foundation license overview, inclusion, and installation 8

Overview 8
Third-party and Open Source Products Used 9
Install a license 10
Get the IT Analytics license key file 11
Install a license on Microsoft Windows Portal platform 13
Install a license on Linux Portal platform 14

Section 2 Install IT Analytics Portal for Foundation License 16

Chapter 2 Install IT Analytics on a Windows server 17

Introduction 17
Multi-language support and locale considerations (Windows) 18
Task 1: Portal and database deployment strategies (Windows) 18
Task 2: Pre-installation configuration (Windows) 18
Task 3: Installing Oracle application binaries (Windows) 21
Troubleshoot the Oracle installation 27
Task 4: Installing Portal application binaries (Windows) 29
Task 5: Request the license key file (Windows) 32
Task 6: Log into the Portal (Windows) 32
Task 7: Install the license key file (Windows) 33
Task 8: Performing a cold backup (Windows) 33
Uninstall the IT Analytics Portal 34

Chapter 3 Install IT Analytics on a Linux server 35

Introduction 35
Multi-language support and locale considerations (Linux) 36

Installer-based deployment 37
Task 1: Portal and database deployment strategies (Linux) 37
Task 2: Pre-installation configuration (Linux) 37
Task 3: Install Oracle database application binaries (Linux) 41
Task 4: Install the Portal application binaries (Linux) 46
Task 5: Installing the database schema (Linux) 49
Task 6: Start the Portal services (Linux) 52
Task 7: Request the license key file (Linux) 53
Task 8: Log into the Portal 53
Task 9: Install the license key file (Linux) 53
Task 10: Performing a cold backup of the database (Linux) 53
Recommended database backup process 53
Uninstall the IT Analytics Portal 54

Section 3 Data Collector Policy Configuration and Reports 55

Chapter 4 Configure NetBackup appliance 56

Overview 56
Prerequisites for adding Data Collectors (Veritas NetBackup appliance) 56
Installation Overview (Veritas NetBackup Appliance) 57
Adding a Veritas NetBackup Appliance Data Collector policy 57

Chapter 5 Configure NetBackup Flex Appliance 61

Pre-Installation setup for Cohesity Flex Appliance 61
Prerequisites for adding Data Collectors (Veritas Flex Appliance) 62
Installation overview (Cohesity Flex Appliance) 62
Add a Veritas Flex Appliance policy 63
Troubleshoot Veritas Flex Appliance policy configuration 68

Chapter 6 Configure NetBackup Data Collector policy 70

Introduction 70
General prerequisites for adding Data Collectors (Cohesity NetBackup) 70
Add a Veritas NetBackup Data Collector policy 72

Chapter 7 Configure Backup Exec 82

Introduction 82
Architecture overview (Veritas Backup Exec) 83

Backup Exec terminology 83
Prerequisites for adding data collectors (Veritas Backup Exec) 84
Upgrade troubleshooting: Microsoft SQL Server and Java 10 85
Installation overview (Veritas Backup Exec) 87
Enable TCP/IP for the SQL server 87
Configure a Windows user 87
Add Backup Exec servers 88
Importing Backup Exec Server information 89
Add a Veritas Backup Exec Data Collector policy 90

Appendix A Foundation License OOTB Reports 93

IT Analytics reports and alerts supported in Foundation license 93

Section 1

Foundation License - Inclusion and Installation

- Chapter 1. Foundation license overview, inclusion, and installation

Chapter 1

Foundation license overview, inclusion, and installation

This chapter includes the following topics:

- Overview
- Third-party and Open Source Products Used
- Install a license
- Get the IT Analytics license key file

Overview

The Foundation license enables only a limited set of features supporting only Veritas NetBackup and Veritas Backup Exec. This license being a Shared Services edition, it requires you to have your own Oracle license. The Foundation license uses Front End Terabyte (FETB) as the meter to consume a license. This license supports limited reports and alerts that are relevant to the Cohesity NetBackup, Cohesity Backup Exec, and Cohesity DataProtect policies.

Table 1-1 Features available under Foundation license

Category	Feature
Collection policy	Storage ■ Veritas NetBackup Appliance ■ Veritas Flex Appliance Data Protection ■ Veritas NetBackup ■ Veritas Backup Exec
Inventory	Backup Servers Hosts Arrays
Chargeback	Backup
Alert categories	System Administration Data Collection Data Protection except ServiceNow Performance

Third-party and Open Source Products Used

When you install the portal and reporting database, you install a compilation of software, which includes open source and third-party software.

For a list of open source components and licenses, see the license.txt file on the portal server.

Table 1-2 Open Source Products Used

Software Product	Linux	Windows
Apache HTTP Web Server	2.4.67	2.4.67
Apache Tomcat Java Servlet Engine	10.1.55	10.1.55
Java	Amazon Corretto 17.0.19.10.1	Amazon Corretto 17.0.19.10.1
Kafka	4.1.2.1	4.1.2.1
Oracle 19c	19c: 19.3.0.0.0	19c: 19.3.0.0.0

Note: If your environment has IT Analytics portal server and Data Collector installed on separate Linux servers and use Cohesity-provided Oracle, ensure the Oracle client RPM is installed or upgraded to 21.21.0.0.0-1.el8.x86_64.

If other versions of the above components are already running on the designated IT Analytics system, or other components are utilizing resources (such as specific ports) typically used by IT Analytics, the product usually can be reconfigured to work around these conflicts; however, this cannot be guaranteed.

*Refer to Support for updated binaries as they become available.

Install a license

Use the procedures listed in this section to install the Portal license. Your login credentials must be assigned the Super User role.

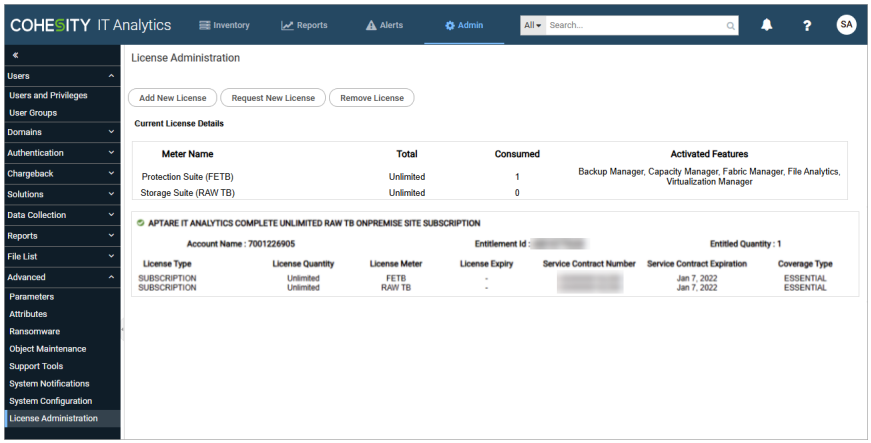
As a best practice, install your license directly through the Portal. Instructions for the command-line installation practices are also available.

See "Install a license on Linux Portal platform" on page 14.

See "Install a license on Microsoft Windows Portal platform" on page 13.

To install a license:

1. Receive the new license file and save the new license file on your Portal server and complete the subsequent steps.
2. Upload the New License
   - Navigate to **Admin > Advanced > License Administration**. The Portal displays your current license details.
   - Click **Add New License**.
   - Browse to locate the license file on your Portal server and click **OK**.



3 Verify the License Installation.

If you have issues with license installation, try uploading the license file again to overwrite the previous one.

Note: After you apply a new license or when you remove an existing license, restart the Portal to display the changes.

Get the IT Analytics license key file

A valid license file is required to run the Portal application. If you already have a license file, proceed to the Installation section.

To generate a license key:

1 Open the Veritas support portal. (https://support.cohesity.com/s//*en_US*/)

2 Click **Licensing** and login to the Veritas Entitlement Management System using your Administrator credentials.

3 Open the **Entitlements** tab and use the filters at the top to filter and locate the entitlements granted to your account.

4 Click the key icon located against the entitlement ID for which you wish to generate a license key. The **Generate License Key** page is displayed. Verify your account details for which you plan to generate the license key.

5 Select the product version for which you want to generate the key. By default, the latest product version is selected.

6 Specify the license quantity that you wish to deploy using the key. By default, the entire available quantity is displayed in the field. You can utilize a partial subset of your entitled licenses with this key and generate a separate key for the remainder.

Note: If you create a key for less than the entitled quantity and if you wish to increase the quantity of the systems later using the entitlement associated with the key, you must create a new key for the additional systems. On the contrary, to reduce the number of systems associated with a key, you need to assign a new key to the reduced systems and edit the older key.

---

7 Provide the host lock string of the system where IT Analytics will be installed using this key.

To get the correct host lock string, run one of these commands on the portal server:

- Linux: **`/opt/aptare/utils/VxLicGetHostLock.sh`**
  On Linux, `VxLicGetHostLock.sh` uses `hostname --fqdn` commands to get the hostname of the system and uses it to create the host string. Hence, ensure `hostname --fqdn` returns a fully qualified host name, instead of a short name. For example, the command output must have at least one dot (.) character.
- Windows:**`C:\opt\aptare\utils\VxLicGetHostLock.bat`**

If you have not installed the IT Analytics Portal, you can download the `VxLicGetHostLock.sh` or `VxLicGetHostLock.bat` from the Cohesity download center and run the appropriate script depending on the OS of the Portal server.

8. After running `VxLicGetHostLock.sh` or `VxLicGetHostLock.bat` file, you get the following output:

```
Veritas Get Host Lock utility v1.0.0.0
Copyright (c) 2022 Veritas Technologies LLC. All rights reserved.

FQDN: xyz.abc.com
Host Lock String: [sha512]4aba838e350d3c9471aa5334db5de8ad4a0ff
45e34a6cfaea064f4ca77812acd4c8abc7be6b2d756574b7d6e06ceb9581357
b824f4f70f84b39d938e85ee62b5
```

   While generating the license key on VEMS, use the same host lock string including `[sha512]`.

   For example:

```
[sha512]4aba838e350d3c9471aa5334db5de8ad4a0ff
45e34a6cfaea064f4ca77812acd4c8abc7be6b2d756574b7d6e06ceb9581357
b824f4f70f84b39d938e85ee62b5
```

9. Add comments about to the license key if required for the future reference.
10. Click **Generate**. The Generated Key page is displayed with the new key in the **License Key** column. You can click the key link and save it locally.

Install a license on Microsoft Windows Portal platform

Receive and save the license file on your portal server and then complete all of the following steps.

1. Ensure that the Oracle Processes are Running.

```
C:\opt\aptare\utils\startoracle.bat
```

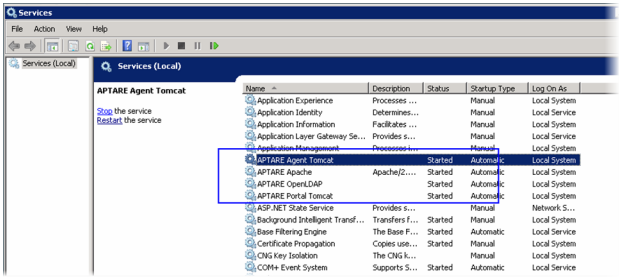
2. Open a DOS command prompt window using **Start** > **Run** > **cmd**
3. Run the license installer utility: `C:\opt\aptare\utils\installLicense.bat`
4. Enter the complete path to the license key file you saved on your server when prompted for the name of the license file. A sample dialog is shown below:

```
Enter the name of the license file you wish to install [*.slf] :

C:\Users\Administrator\Documents\Slic\
A3351334429_QTY200_APTARE_ITA_10_6_COMPLETE_STANDARD_DR_LIC_NNL_4756411672.slf
```

```
Verifying license...
License installed
```

Verify that the services are running by viewing the Services panel:



5. Verify the License Installation.

Note: After you apply a new license or when you remove an existing license, restart the Portal to display the changes.

Install a license on Linux Portal platform

Receive and save the license file on your portal server and then complete all of the following steps.

1. Ensure that the Oracle Processes are Running: Log in as **root** on your IT Analytics Database server (the Database and Portal servers are usually the same physical server).

   ```
   /opt/aptare/bin/oracle start
   ```

2. Run the Installation Script: Log in as **root** on your IT Analytics Portal server.

   ```
   /opt/aptare/utils/installlicenseUI.sh
   ```

3. When prompted for the name of the license file, enter the complete path to the license key file you saved on your server.

   For example:

   ```
   Enter the name of the license file
   you wish to install [*.slf]: /opt/aptare/license.slf
   Verifying license...
   License installed.
   ```

4. Verify the license installation.

Note: After you apply a new license or when you remove an existing license, restart the Portal to display the changes.

Section 2

Install IT Analytics Portal for Foundation License

- Chapter 2. Install IT Analytics on a Windows server
- Chapter 3. Install IT Analytics on a Linux server

Chapter 2

Install IT Analytics on a Windows server

This chapter includes the following topics:

- Introduction
- Multi-language support and locale considerations (Windows)
- Task 1: Portal and database deployment strategies (Windows)
- Task 2: Pre-installation configuration (Windows)
- Task 3: Installing Oracle application binaries (Windows)
- Task 4: Installing Portal application binaries (Windows)
- Task 5: Request the license key file (Windows)
- Task 6: Log into the Portal (Windows)
- Task 7: Install the license key file (Windows)
- Task 8: Performing a cold backup (Windows)
- Uninstall the IT Analytics Portal

Introduction

Local Administrator privileges are required for installing all Portal Server components. This document contains images, command-line prompts, and responses that provide a reasonable representation of the installation experience. However, the actual text and values seen may differ during the installation based on the installation environment and available resources.

Multi-language support and locale considerations (Windows)

Apart form English, you can perform the portal installation in Simplified Chinese, French, Korean, and Japanese. Once you have set the language preference, the installation progress and responses appear in your preferred language. Note that this language preference setting is only confined to the installation process and has no impact on the text of the portal UI.

To install the portal in your preferred language, Windows OS must be a native OS in either Simplified Chinese, French, Korean, or Japanese. Avoid having Windows OS in English installed with language pack and changing the locale later. The portal installer detects the locale from the Windows Language Settings and launches the installer in the respective locale.

If the Windows Language Setting is set to a language other than Simplified Chinese, French, Korean, or Japanese, the installer is launched in English. Having completed the language settings, you can proceed with the installation of the IT Analytics Portal.

See "Task 1: Portal and database deployment strategies (Windows)" on page 18.

Task 1: Portal and database deployment strategies (Windows)

Installing Oracle and portal binaries on the same server (Windows)

For the typical Portal installation, the installation process consists of these main tasks:

1. Verify that you have the latest binaries for the version you are installing.
2. Install Oracle application binaries.
3. Install the IT Analytics Portal software components and the database schema.

Task 2: Pre-installation configuration (Windows)

1. Choose a Portal Server. For performance reasons, the IT Analytics Portal software should not be installed on the same server as the Data Collectors. If, for some reason, you require both to be on the same server, be sure that both the Portal and Data Collector software do not reside in the same directory on the server. Root privileges are required for the Portal software installation tasks.

You will need to log in as a **Local Administrator** to perform the installation. Oracle requires that you are logged in as a **Local Administrator**. Logging in as a Domain Administrator is not sufficient for this installation. Refer to the Oracle web site for the requirement to install on Windows as a user who is a member of the server's local Administrator's group.

2. For new Portal installations, the minimum server memory requirement is 32 GB. Oracle database requires a minimum of 24 GB of memory. Portal installations will fail if sufficient memory resources are not available on the Portal server.
3. The Portal Installation software checks the following resources:
   - Total physical memory (physical + virtual) must be greater than 24 GB, otherwise Oracle will fail to start. Add more physical memory to the Portal server.
   - Windows Virtual Memory must be 24 GB or greater, otherwise Oracle will fail to start. Increase the size of the virtual memory if required (**Windows** > **System** > **Advanced System Settings** > **Advanced** tab > **Settings** > **Advanced** tab > click **Change**).
4. Verify the OS of the Portal Server. Check that the OS is one of the certified operating systems listed in the *Certified Configurations Guide*.
5. Verify the Third-Party Software list.

   See "Third-party and Open Source Products Used" on page 9.
6. Verify Microsoft Visual C++ Runtime libraries are installed.

   IT Analytics installs Apache HTTP Server which has a dependency on run-time components of Visual C++ libraries. These run-time components are included in the Microsoft Visual C++ 2015 Redistributable Update 3 RC. This Microsoft distribution is available for download from www.microsoft.com. If this redistributable update is not installed prior to running the IT Analytics installer, Apache HTTP Server will not be able to run.

   Note: If you installed Microsoft Visual C++ 2015 after IT Analytics 10.3.xx was installed, and services are failing, you must manually install the Apache service using the following command:

   ```
   C:\opt\apache\bin\httpd -k install -n "APTARE Apache"
   ```

7. Verify that sufficient disk space exists on the designated Portal Server. For the database file systems, the amount specified is the minimum to create the database. The database grows in size over the period of time. The growth of

database dependents on various factors such as subsystems from which data is collected, type of systems collecting data from, retention periods for data(which is configurable), and so on.

Directory	Minimum Disk Space	Recommended Disk Space	Max. Disk Space for DB Growth	Notes
C:\opt	20 GiB	30 GiB	30 GiB	
C:\tmp	10 GiB	10 GiB	10 GiB	
C:\oradata	305 GiB	565 GiB	3445 GiB	The Installer prompts for the target drive for the `oradata` directory, so alternate drives are supported.
Total	335 GiB	605 GiB	3485 GiB	

- Add **itanalyticsportal.yourdomain** and **itanalyticsagent.yourdomain.com**entries to your enterprise DNS Server. Both entries must resolve to the IP address of the Portal server. Also note that the last component of the domain must be one of the recognized root domains; for example, **.com**--not **.3com**.

8. Verify that there are no other web servers--for example, IIS--running on the system.
9. The installer will set up the following system-wide environment variables and update the PATH environment variable:

Variable Name	Variable Value
ORACLE_HOME	`C:\opt\oracle`
ORACLE_SID	**scdb**

The PATH environment variable will have the following path appended to the end of the current PATH:

```
C:\opt\oracle\bin
```

Task 3: Installing Oracle application binaries (Windows)

This section covers the installation of Oracle installer for both shared service edition and non-shared service edition on a Windows server.

Refer to the instructions provided with your purchase agreement confirmation email and consult the Cohesity Support, if you require additional assistance.

Prerequisites for Oracle application binaries on Windows

- If you are running IT Analytics on a version lower than Oracle 19c, you must first uninstall the older version before proceeding with this installation.
- Oracle 19c Windows support is limited to specific releases. Refer to the Certified Configurations Guide for supported versions.
- You must download the Oracle database for 19c zip file `WINDOWS.X64_1930000_db_home.zip` from the *Oracle Download Center*.
- The Oracle 19c binaries will be installed on a Windows server that will serve as the IT Analytics Portal server. This server cannot have any other Oracle database instances installed on it.
- Oracle requires that you are logged in using an account that has administrative privileges.
- An Oracle service user name is required for installation. The Oracle service user account can be an Active Directory account.
- The Oracle service user must be a standard user and must not be a part of Administrator group
- Windows User Account can be a Windows Local User, Windows Domain User or Managed Services Account (MSA). If you want to create a new user during installation, then it can only be a Windows Local User. It cannot be a Windows Domain User or an MSA.

  Note: If you use a Domain account, that user must login at least once to the Windows machine.

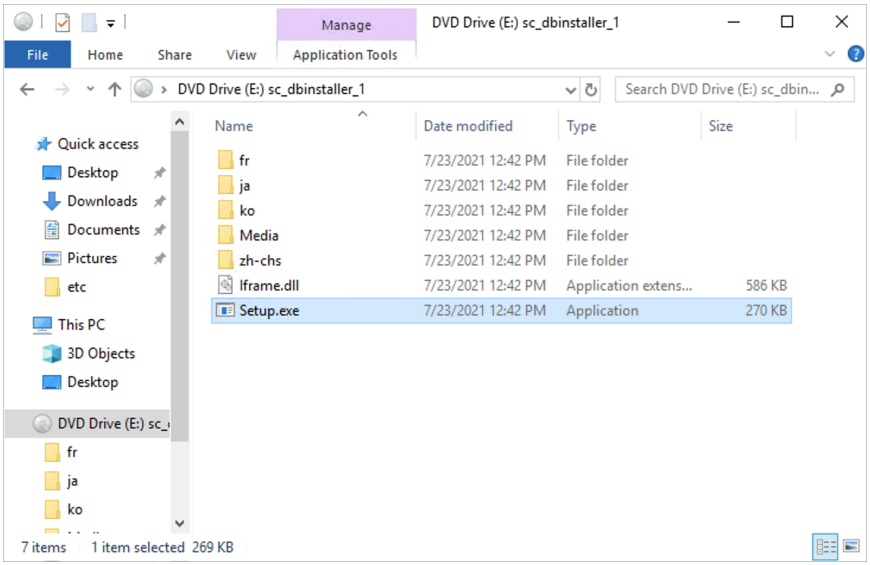
- Per Oracle requirements, passwords cannot exceed 30 characters.
- You cannot change the Oracle Home User once the installation is complete. To change the Oracle Home User, you must reinstall the Oracle Database software.

Install Oracle binaries for shared service edition

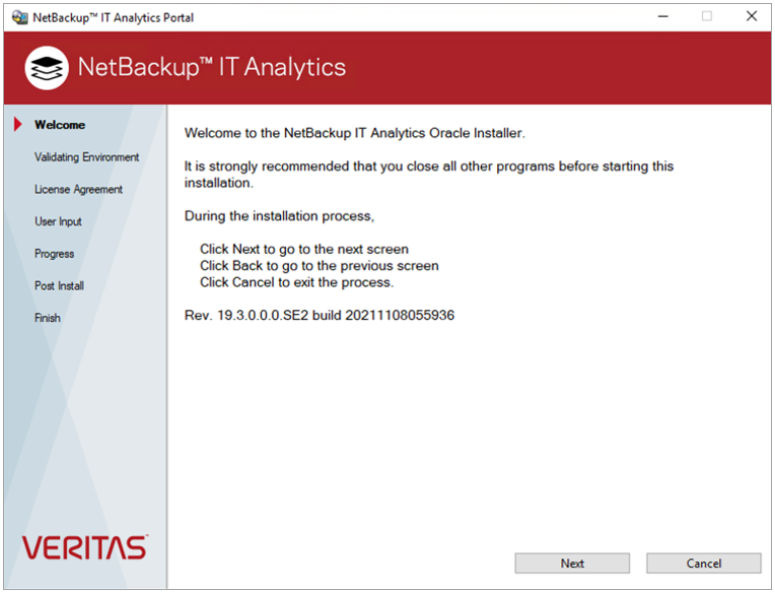
To install Oracle binaries for shared service edition, you must have a Standard or Enterprise Edition Oracle license. For the Enterprise Edition license, you must set the environment variable **ORACLE_LICENSE_OPTION** to **EE**. Also ensure that the Oracle database for 19c zip file `WINDOWS.X64_1930000_db_home.zip` that you have downloaded from Oracle Download center is copied to the Windows host.

To install Oracle binaries for shared service edition:

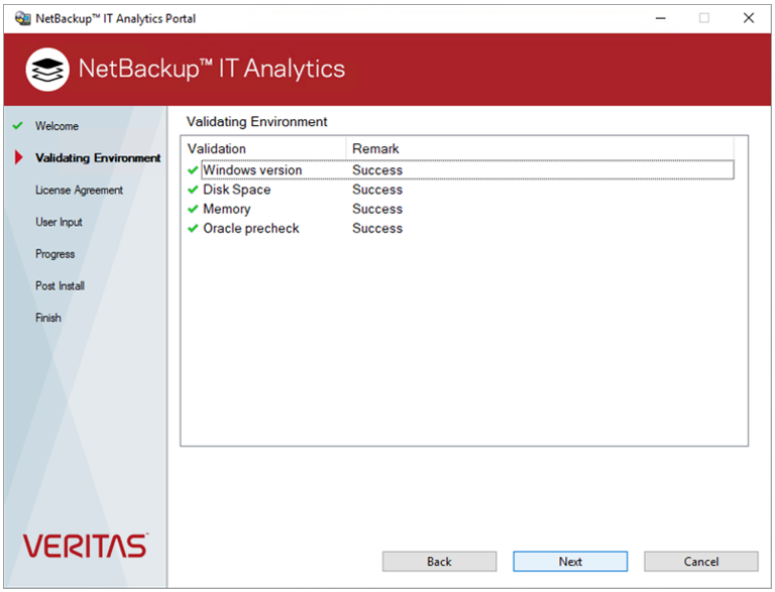
1. Login to the Windows host as and administrator. Oracle requires you to login with administrator privileges.
2. Download the `itanalytics_dbinstaller_shared-service_win.iso` to the Windows host.
3. Double-click the ISO file and run `Setup.exe`. The installation wizard is launched.



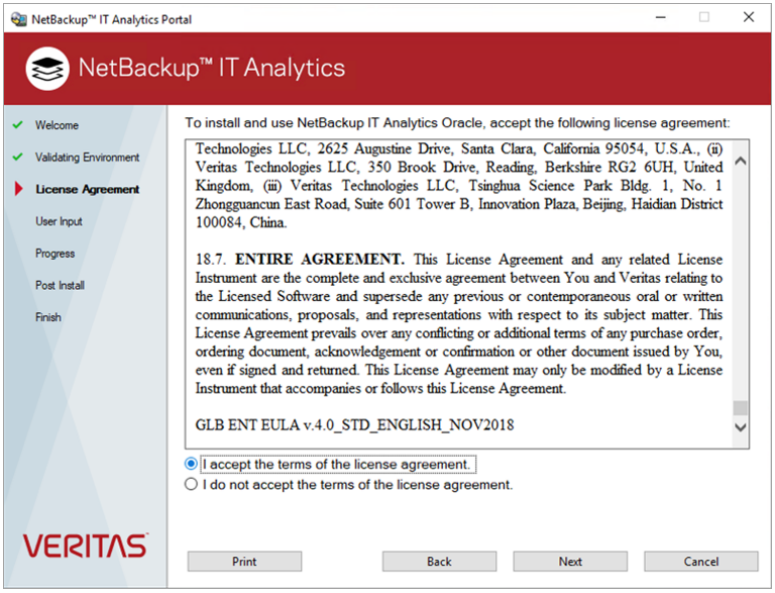
4 Review the instructions on the **Welcome** screen and click **Next**.



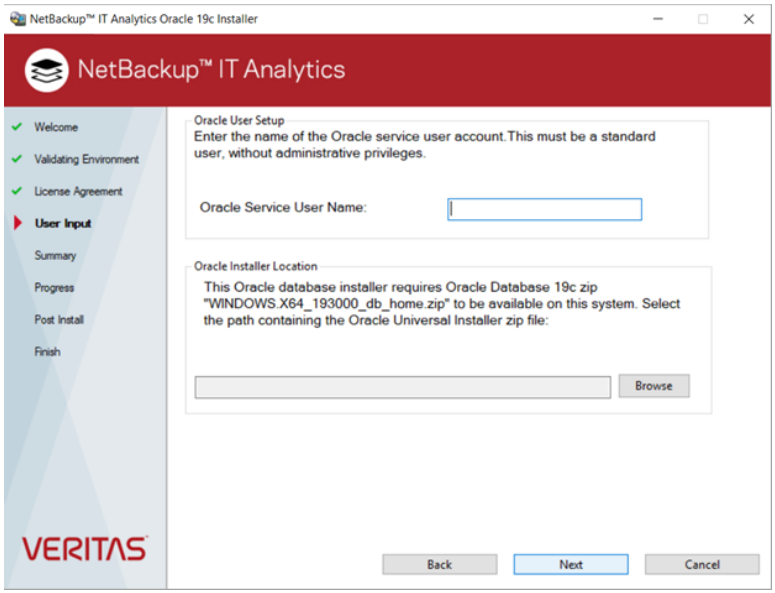
5 The wizard validates the environment for Windows version, Disk Space, Memory, and Oracle pre-checks. Click **Next** after the validation is successful.



6 Accept the End User License Agreement (EULA) and click **Next**.

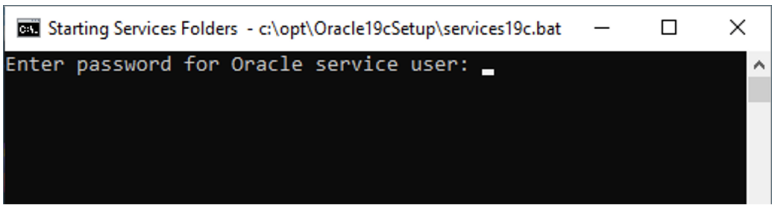


7 For Oracle User Setup and installer location, enter the valid **Oracle Service User Name** and click **Browse** to assign the absolute path to Oracle universal Installer archives.



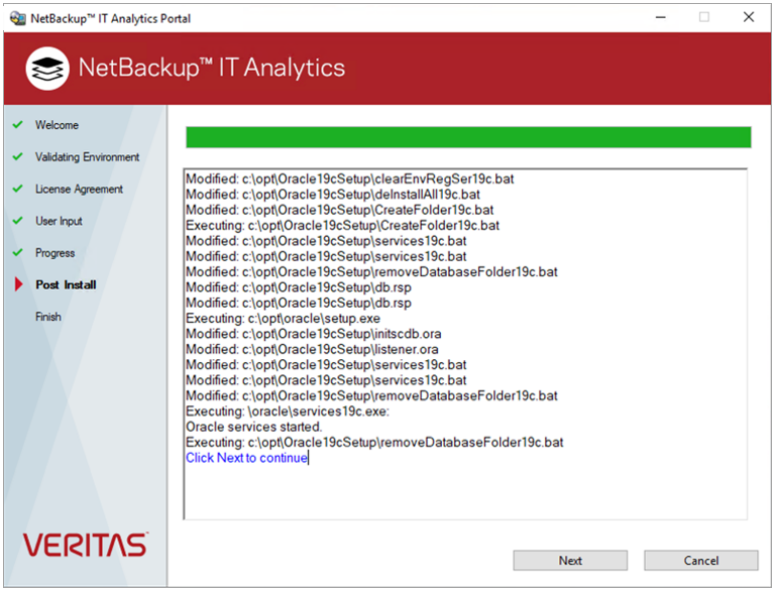
8 Enter the Oracle service user password on the command prompt.

Caution: If you exceed the maximum attempts for incorrect password on this prompt, your account can get locked.

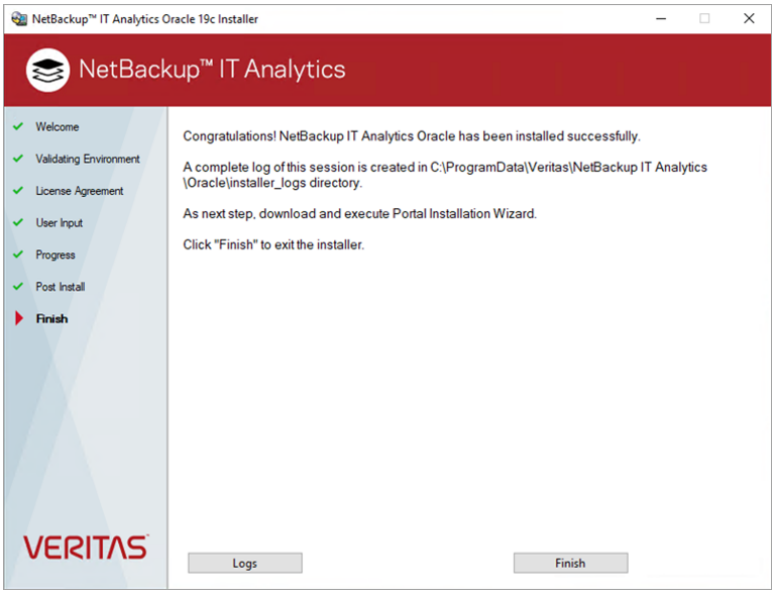


The **Progress** screen displays the installation and validation status.

9 On the **Post Install** screen, review the list of Oracle application binaries installed in the `C:\opt` folder and click **Next**.



10 On the **Finish** screen, a confirmatory message about the successful installation of IT Analytics Oracle is displayed. Click **Finish** to exit the installation wizard.



At this point, the Oracle Application binaries for shared service edition are installed on your server and Oracle services are created. This completes the installation of the IT Analytics Oracle Application component. The next step is to install the IT Analytics Portal software components.

Troubleshoot the Oracle installation

Because the Oracle installation relies on Oracle requirements and processes, you may encounter issues that require your intervention.

General troubleshooting

The Oracle installation process logs errors that can aid in troubleshooting. Locate the log file that coincides with the date and time of the error:

```
C:\Program
Files\Oracle\Inventory\logs\installActions<YYYY-MM-DD_HH-MM>
```

Account lockout

Too many incorrect password entry attempts will lock out the Oracle Service User account. To unlock the account, take the following steps.

1. Enter `lusrmgr.msc` in the Windows PowerShell command prompt window to launch the Local Users and Groups Manager.
2. Open the **Users** folder and double-click the user that needs to be unlocked.
3. In the User Properties window, uncheck the Account is locked out item to re-enable the user account.

Note: An alternative method for unlocking an account can be accessed via the Windows Server Manager: **Server Manager > Tools > Computer Management > Local Users and Groups > Users**

Invalid Oracle Service User Account

When an invalid Oracle Service User Name is entered, the Oracle Universal Installer displays the following messages:

```
The password field is empty.
CAUSE: The password should not be empty.
ACTION: Provide a non-empty password.
Please press Enter to exit...
```

These messages do not necessarily reflect the true issue. At this point, the password is not relevant. The process actually needs the Oracle Service User Name.

To recover from this error, take the following steps.

1. In the command prompt window, press **Enter**.
2. Return to the **Failed to Install Oracle** window and click **Previous**.
3. Enter a valid account name for the **Oracle Service User Name** and resume the installation.

Oracle universal installer fails

The most common reason for the Oracle Universal Installer to fail is due to an invalid Oracle Service User account.

See the section called “Invalid Oracle Service User Account” on page 28.

Other failures must be investigated by reviewing log messages, using the following steps.

1. In the **Failed to Install Oracle** installer window, click **Exit**.
2. Locate the error in the log file:

   ```
   C:\Program
   Files\Oracle\Inventory\logs\installActions<YYYY-MM_HH-MM>
   ```

Note: If you abort the Oracle Universal Installer process by closing the command window, close the installer window and re-run the installer from the beginning.

Oracle already exists on the portal server

If you are installing Oracle on a server that at some point had IT Analytics Oracle software installed, the installer will display an error dialog window.

Encountering previously installed software may occur under the following circumstances:

- You chose a server that has a version of the IT Analytics Portal already installed. Determine the version of Oracle that is already installed and reference the IT Analytics documentation for the steps to uninstall the database/Portal.
- You ran the Oracle installer more than once. In this case, it is likely that you do not want to proceed unless you have determined that it was not a successful installation. If you need to re-run this installer, refer to the following.

Unsupported Windows operating system

If you try to install Oracle on a version earlier than Windows Server 2016, you will get a warning message: **WARNING: The current OS is not supported.**

Exit the installation and choose a server with a supported Windows OS.

Task 4: Installing Portal application binaries (Windows)

In this procedure, you will install Portal Server software on your Windows Server.

System: Web/Application Server

To install your Portal Server software

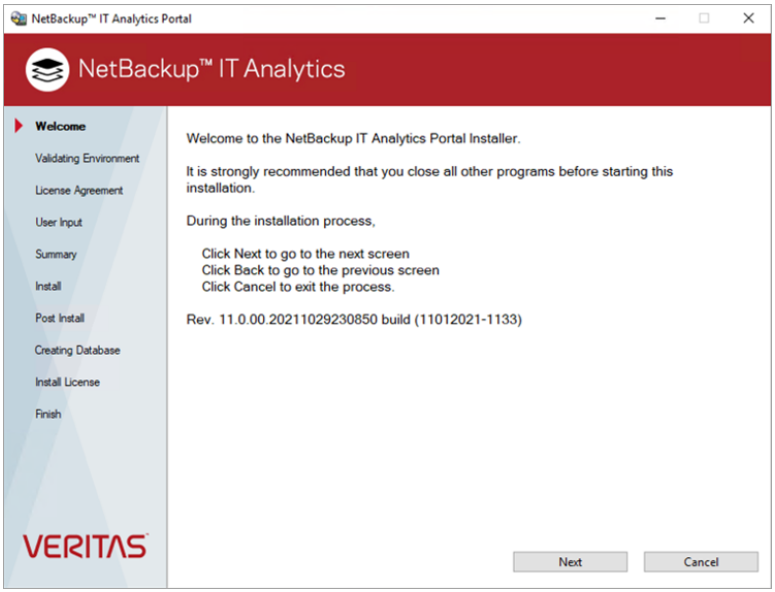
1. Log in to the Portal Server as a **Local Administrator**.

   Note: Oracle requires that you are logged in as a **Local Administrator**. Logging in as a Domain Administrator is not sufficient for this installation.

2. Go to the downloads section under Support at www.veritas.com and click the relevant download link.
   - Once downloaded, the Portal Installation Wizard launches automatically. If it does not, use Windows Explorer to navigate to the executable and double-click the file: **Setup.exe**

- The Portal Installation Wizard requires about a minute to start up. During this time, the following window is displayed:.

  Once the Portal Installation Wizard extracts the necessary startup files, the Portal Installation Wizard displays the launch screen.



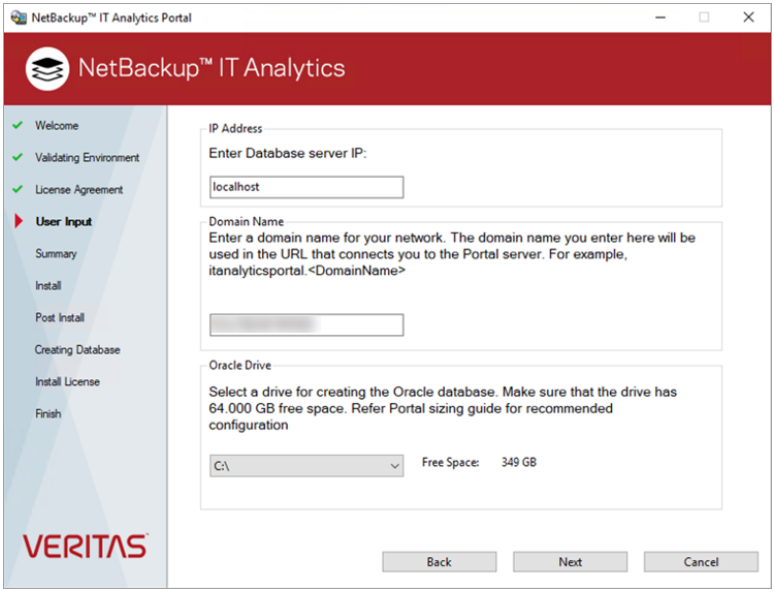
3 Click **Next** to start the installation process.

  The Portal Installation Wizard validates the system environment. Once the installer has validated successfully, click **Next**.

4 End User License Agreement (EULA) is displayed. If you agree to the terms of EULA, select **I accept the terms of the License Agreement** and click **Next**.

5 Provide the following details on the next form and click **Next**.

  - Enter the hostname or IP address of the server on which the Oracle Application binaries are installed. The installer prompts for the IP Address of your Oracle database server. If Oracle is running on the Portal server, you can enter **localhost**.
  - Enter the domain name for your environment (Example: *yourcompany.com*). The value entered here determines the URL you will use in your browser to access the portal. (For example: *itanalyticsportal.yourcompany.com*)
  - Select the drive letter on which you intend to create the Oracle database. The Portal Installation Wizard customizes the Database SQL Script based on the drive letter. Note the disk space requirement for this drive.



6 Review the installation summary.

The screen summarizes the product components that will be installed and describes the available and required disk space for the components before initiating the installation.

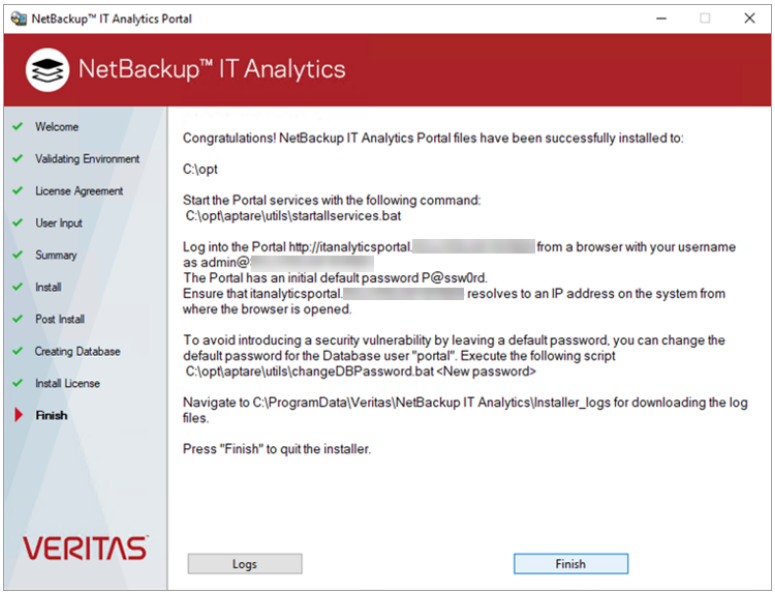
7 Click **Next** to begin the installation. The default location is `C:\opt`.

8 Review the **Post Install** details and click **Next**.

9 The installer creates the database. Click **Next** once the database creation is complete.

10 An evaluation license is installed. Click **Next** once the status displays **License has been installed successfully**.

11 On success installation of the IT Analytics Portal, click **Finish** to exit the installation wizard.



Task 5: Request the license key file (Windows)

Refer to the *IT Analytics Licensing Guide* for details.

See "Get the IT Analytics license key file" on page 11.

Task 6: Log into the Portal (Windows)

Log into the IT Analytics Portal (*http://itanalyticsportal.yourcompany.com*) with your username as <admin@yourcompany.com>. The Portal has an initial default password **P@ssw0rd**. You must change this password after your first login.

Note: The default password contains a zero, not an uppercase O.

Also verify whether the IT Analytics Portal services have started as follows:

1. Login to the portal system as an administrator.
2. Click **Start** > **Settings** > **Control Panel** and open **Administrative Tools**.
3. Click **Services**.
4. Verify whether the following services are running:
   - Oracleservicescdb
   - OraclescdbTNSListener
   - APTARE Kafka Service
   - APTARE Zookeeper Service
   - APTARE Portal Tomcat
   - APTARE Agent Tomcat
   - APTARE Anomaly Service
   - APTARE Apache

See "Install a license" on page 10.

Task 7: Install the license key file (Windows)

Refer to the *IT Analytics Licensing Guide* for details.

Task 8: Performing a cold backup (Windows)

Prior to deploying the Portal for operational use, it is recommended that you perform a cold backup of the Oracle database. This offline, cold backup simply means that you'll physically copy or backup the files to another location. This cold backup will simplify the restore process, in the event of unanticipated data loss. With a cold backup, you simply have to restore the files and then import the most recent database export. In addition to this initial cold backup, you may consider performing a cold backup periodically--for example, after a significant software upgrade--to re-capture the database schema. Refer to the System Administrator Guide.

Recommended database backup process

1. Cold Backup
2. Daily Exports of the database
3. In the event of data loss, restore the database and then import the most recent database export.

Uninstall the IT Analytics Portal

This procedure uninstalls the application and removes the Oracle database, including all the data that resides on that database. If required, you can back up the database at a different location before the uninstallation. Files that you created after the product was installed are not deleted. Perform this procedure on your Portal Server.

To uninstall Portal server software

1. Shut down the Distributed Transaction Coordinator service if it is running.

   ```
   > net stop msdtc
   ```

   This Microsoft service can sometimes lock one of the Oracle files and prevent the uninstall from completing successfully.

2. From the **Control Panel**, open **Add and Remove Program** > **Programs and Features** and uninstall IT Analytics.

   The IT Analytics uninstall wizard is invoked and it asks for confirmation to proceed with the uninstallation.

3. Click **Uninstall** and follow its subsequent prompts to complete the procedure.

4. From a Windows File Explorer window, remove the database and any other files created after the initial installation:

   Delete the `C:\oradata` folder.

   Delete the `C:\opt` folder.

5. Reboot the Windows Server.

   This step is important to ensure that the deletions are complete.

The uninstaller may not delete the entire Portal directory structure. Sometimes new files that were created after the installation are retained along with their parent directories. If the Portal was upgraded from version 10.5 or older, you may find entries of Kafka and Zookeeper services on the services panel (default `C:\Program Files\Aptare`), even after the uninstallation of the Data Collector. You must manually delete the services and reboot the system.

Chapter 3

Install IT Analytics on a Linux server

This chapter includes the following topics:

- Introduction
- Multi-language support and locale considerations (Linux)
- Installer-based deployment
- Uninstall the IT Analytics Portal

Introduction

You can install the Portal on a Linux server by two methods:

- OVA based deployment
- Installer-based deployment

Installing all Portal Server components requires **root** privileges.

Throughout this document, screen shots and command-line prompts and responses are used to provide a reasonable representation of the interaction you will be viewing. However, they may not display precisely the same text that you will see during the installation.

Caution: Regarding Oracle Linux based OVA deployment: This OVA is recommended to be used for the purposes of easing deployment of IT Analytics Portal. Support for the Oracle Linux Operating System distributed with this appliance is not provided by Cohesity.

Cohesity will be responsible for support and maintenance of only IT Analytics components on this appliance, depending on the license entitlement.

Multi-language support and locale considerations (Linux)

Apart form English, you can perform the portal installation in Simplified Chinese, French, Korean, and Japanese. To install the portal in one of the supported languages, you need to first check if the system has multiple languages and then add the preferred language for the installation. Once you have set the language preference, the installation progress and responses appear in the preferred language. Note that this language preference setting is only confined to the installation process and has no impact on the text of the portal UI.

1. To check the current system language:

   ```
   #locale
   ```

2. To check if your system has multiple languages:

   ```
   #locale -a
   ```

3. To add a language, run the command `# vi /etc/profile` and go to the end of the file and add the language as follows:

   - 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 system to set your language preference for the portal installation.

Having completed the language settings, you can proceed with the installation of the IT Analytics Portal.

See "Installer-based deployment" on page 37.

Installer-based deployment

To perform installer-based deployment of the IT Analytics Portal, you require root privileges.

Task 1: Portal and database deployment strategies (Linux)

If these components are to be installed on the same server, then Task 2 and Task 3 must be performed on the same machine.

Note: IT Analytics recommends that the Portal and Database components be installed on the same server.

Installing Oracle and Portal Binaries on the Same Server

For the typical Portal installation, the installation process consists of these main tasks:

1. Verify that you have the latest binaries for the version you are installing.
2. Install Oracle application binaries.
3. Install the IT Analytics Portal software components.
4. Create the IT Analytics Database and load the schema objects.

Task 2: Pre-installation configuration (Linux)

1. Choose a Portal Server.

   For performance reasons, avoid installing the IT Analytics Portal software on the same server as the IT Analytics Data Collectors. Precisely, avoid installing Data Collectors in `/opt/aptare`.

If for some reason, you require both to be on the same server, ensure that both the Portal and Data Collector software do not reside in the same directory on the server. Portal software installation tasks require root privileges.

2. For new Portal installations, the minimum server memory requirement is 32 GB. Oracle database requires a minimum of 24 GB of memory. Portal installations will fail if sufficient memory resources are not available on the Portal server.
3. The Portal Installation software checks the following resources:
   - Total physical memory (physical + virtual) must be greater than 24 GB, otherwise Oracle will fail to start. Add more physical memory to the Portal server.
   - Total temporary file system (tmpfs) memory must be 24 GB or greater, otherwise Oracle will fail to start. Increase the size of tmpfs, typically in /etc/fstab.
   - Shared memory (kernel.shmmax parameter) must be 12 GB or greater, otherwise Oracle will fail to start. Increase the value of the shmmax parameter, typically in /etc/sysctl.conf. After increasing the value for the shmmax parameter, execute: **sysctl -p**.
4. Verify the OS of the Portal Server. Check that the OS is one of the certified operating systems listed in the *Certified Configurations Guide*.

   Verify that sufficient disk space exists on the designated Portal Server. For the database file systems, the amount specified is the minimum to create the database. The database grows in size over the period of time. The growth of database dependents on various factors such as subsystems from which data is collected, type of systems collecting data from, retention periods for data(which is configurable), and so on.

File System/ Directory	Minimum Disk Space	Recommended Disk Space	Maximum Disk Space for DB Growth	Notes
/opt	20 GiB	30 GiB	30 GiB	
/tmp	10 GiB	10 GiB	10 GiB	Both /tmp and /var/tmp must be writable by the user aptare.

File System/ Directory	Minimum Disk Space	Recommended Disk Space	Maximum Disk Space for DB Growth	Notes
/data01	50 GiB	100 GiB	780 GiB	Required for data and index tablespaces.
/data02	50 GiB	100 GiB	750 GiB	Required for data and index tablespaces.
/data03	90 GiB	250 GiB	1800 GiB	Required for data and index tablespaces.
/data04	65 GiB	65 GiB	65 GiB	Temporary table space.
/data05	45 GiB	45 GiB	45 GiB	Temporary table space (undo log).
/data06	5 GiB	5 GiB	5 GiB	Temporary table space (redo log).
Total	335 GiB	615 GiB	3495 GiB	

5. Review the third-party software details.

   See "Third-party and Open Source Products Used" on page 9.

6. If you plan to export or email reports as PDF files, to ensure proper rendering of these output formats, a graphics manager such as X Virtual Frame Buffer (Xvfb) is required. Contact your IT organization to configure this capability.

7. Verify whether rng-tools, fontconfig, ss, and nest are installed. Either ss or netstat must be installed .

8. Verify that the necessary rpms exist on your system based on the OS.

   - For RHEL 8, use the following command:
     The command returns:
   -

- For RHEL 7 and CENTOS 7, use the following command:
  The command returns:
- For SUSE 12 Linux Enterprise, use the following command:
  The command returns:

9. Verify that the `bc` command is available, as it is required by the database installer.
10. Download the application binaries for both the Oracle Database Installer and the Portal Installer from www.veritas.com. Use the instructions provided in the confirmation of your purchase agreement.
11. **Troubleshooting User Account Creation**: The Portal installation process will create user accounts for aptare and tomcat. If you are using non-local user management (such as LDAP or NIS) to manage the Linux user accounts, the **useradd** command may fail to execute successfully. Take the following steps to manually pre-create the required users:
    - Using your normal process for creating user accounts in LDAP, pre-create the user accounts aptare and tomcat with home directories under **/home**.

User ID	Primary Group	Supplementary Groups
aptare	aptare	dba
tomcat	tomcat	aptare

    - Some environments, particularly virtualized ones using **automount**, will fail to create the home directories when the **useradd** command is used. In this situation, manually create the **/home/aptare** and **/home/tomcat** directories and **chown** them to aptare and tomcat respectively.
    - If you need additional clarification, contact the Cohesity Support for details.
12. Troubleshooting script issues: A known issue associated with Security Enhanced Linux (SELinux) may arise when executing scripts that require Java. This results in a permission denied error message. To resolve this issue, configure SELinux to allow the use of shared libraries with text relocation.

    The installer expects the SELinux configuration to be either disabled or permissive.
13. Ensure ports 80/tcp, 8011, and 8017 are open in the firewall for proper functioning of the portal.

Task 3: Install Oracle database application binaries (Linux)

This section covers the prerequisites and installation of Oracle database application binaries for both shared service edition and non-shared service edition. Typically, the Oracle Database application binaries are installed on the same server as the Portal binaries.

Prerequisites

Typically, the Oracle Database application binaries are installed on the same server as the Portal binaries. Some OS-specific basic requirements are listed below for quick reference. Detailed prerequisites are described under *Pre-installation configuration* section of the *IT Analytics Portal Install and Upgrade Guide* for Linux and Windows respectively.

1. Identify the portal server.
2. Ensure the OS on the portal server is certified according to the *IT Analytics Certified Configuration Guide* and has sufficient disk space.
3. Ensure the third-party software as specified under *Supported third-party and open-source products* are available on the server.
4. Ensure the `fontconfig` rpm and other OS-specific (RHEL 7,8; CENTOS 7; or SUSE Linux Enterprise) rpms are available on the server.
5. Ensure ports 80/tcp, 8011, and 8017 are open in the firewall for proper functioning of the portal.
6. Ensure that either `ss` or `netstat` command is available on the system.

Also, refer the instructions provided with your purchase agreement confirmation email and consult Veritas Support for additional assistance.

Install Oracle database binaries for shared service edition:

Prerequisites for the installation of Oracle database binaries for the shared service edition:

- For an installer-based deployment, download `LINUX.X64_193000_db_home.zip` from Oracle Download Center.
- Obtain a Standard or Enterprise edition license.
- For an Enterprise edition license, set the environment veriable ORACLE_LICENSE_OPTION to EE.

  ```
  # export ORACLE_LICENSE_OPTION=EE
  ```

Install Oracle database binaries for shared service edition:

To install the Oracle database binaries for shared service edition:

1. Verify that you have the current version of the Oracle 19c Installer binaries.
2. Login as **root** on the server where the IT Analytics Database will be installed. Typically, this is also the Portal server.
3. Place the ISO image into the `/mnt` directory.
4. Mount the ISO image that you downloaded.

   ```
   mkdir /mnt/diskd

   mount -o loop <itanalytics_dbinstaller_shared-service_linux.iso>

   /mnt/diskd
   ```

   where you substitute the relevant name of the ISO file that you downloaded.

5 Enter the following commands to start the installer:

```
cd /
/mnt/diskd/install_oracle.sh
```

The command copies the Oracle binaries into **/opt/aptare/oracle**.

6 Press **Enter** to read the entire EULA license agreement and the pre- acceptance process will begin.

This takes 3-5 minutes to complete, as it installs files into /opt/aptare/oracle19c.

```
A complete log of this session is in this file
/opt/aptare/logs/install/install_oracle_xxxxxxxxxxxxxxxxxxxx.log
***************************************************************************
*  IT Analytics ORACLE Installer Version 19.3.0.0.0
(xxxxxxxxxxxxx)
***************************************************************************
To use this software you must agree to the following terms and
 conditions. Press ENTER to continue:
Enter "accept" to accept these Terms and Conditions: accept
Creating group aptare ...groupadd: group 'aptare' already exists
Done.
Creating group dba ...groupadd: group 'dba' already exists
Done.
Adding user aptare to group dba ...Done.
Adding user aptare to group dba ...Done.



This Oracle database installer requires Oracle Database 19c zip
"LINUX.X64_193000_db_home.zip" to be available on this system.
Enter the absolute directory path containing the Oracle Universal
 Installer zip file:/tmp/oracle_zip/
Creating ORACLE_HOME directory in /opt/aptare/oracle ... Done.
Creating ORACLE_HOME/logs directory ...
Setting up IT Analytics database directories
/data01 /data02 /data03 /data04 /data05 /data06 ...Done.



Installing Oracle binaries in /opt/aptare/oracle ...
Extracting files ...
This process may take 3-5 minutes to complete ... Done.
.
.
   creating: 31281355/etc/config/
  inflating: 31281355/etc/config/actions.xml
  inflating: 31281355/etc/config/inventory.xml
  inflating: 31281355/README.html
  inflating: PatchSearch.xml
```

```
Oracle Interim Patch Installer version 12.2.0.1.21
Copyright (c) 2020, Oracle Corporation.  All rights reserved.



Oracle Home       : /opt/aptare/oracle
Central Inventory : /opt/oraInventory
   from           : /opt/aptare/oracle/oraInst.loc
OPatch version    : 12.2.0.1.21
OUI version       : 12.2.0.7.0
Log file location : /opt/aptare/oracle/cfgtoollogs
                    /opatch/opatchxxxxxxxxxxxxxxx.log

Verifying environment and performing prerequisite checks...
OPatch continues with these patches:   31281355

Do you want to proceed? [y|n]
Y (auto-answered by -silent)
User Responded with: Y
All checks passed.



Please shutdown Oracle instances running out of this
ORACLE_HOME on the local system.
(Oracle Home = '/opt/aptare/oracle')


Is the local system ready for patching? [y|n]
Y (auto-answered by -silent)
User Responded with: Y
Backing up files...
Applying interim patch '31281355' to OH '/opt/aptare/oracle'


Done.

A complete log of this session can be found at
 /opt/aptare/logs/install/install_oracle_xxxxxxxxxxxxxxxx.log
```

Oracle patches required to install the database on RHEL9 host

The following Oracle patches are required to install the binaries on a RHEL9 host. To download these 4 patches, login to the Oracle support site, click **Patches and update**. Wherever prompted by the installer, provide the absolute directory path of the folder containing these Oracle patches.

- patch 35775632 (`p35775632_190000_Linux-x86-64.zip`)
- patch 6880880 by selecting the 19.0.0.0.0 release (`p6880880_190000_Linux-x86-64.zip`)
- 19.20 DBRU Patch 35320081 (`p35320081_190000_Linux-x86-64.zip`)
- 19.20 DB MLR 35904951 (`p35904951_1920000DBRU_Linux-x86-64.zip`)

Task 4: Install the Portal application binaries (Linux)

This section covers the installation of the Portal application binaries. Typically, the Portal binaries are installed on the same server as the Oracle Database binaries, although in some cases, a separate server may be designated.

System: Portal Server

Note the instructions provided with your purchase agreement confirmation and consult Cohesity Support, if you require additional assistance.

To install the Portal binaries

1. Login as **root** on the server where IT Analytics Portal will be installed. Typically, this is the same server where you installed the Oracle binaries.
2. Go to the downloads section under Support at www.veritas.com and click the relevant download link.
3. Mount the ISO image that you downloaded.

   ```
   mkdir /mnt/diska

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

   where you substitute the relevant name of the ISO file that you downloaded.
4. Enter the following commands to start the installer:

   ```
   cd /
   /mnt/diska/Itanalyticsinstaller.sh
   ```

5 Determine what Portal server configuration you are deploying.

```
A complete log of this session is in this file
/opt/aptare/logs/install/aptareInstaller_xxxxxxxxxxxxxxxxxx.log
****************************************************************
* IT Analytics Intaller Vers 11.8
****************************************************************
Revision 11.8.xx.xxxxxxxxxxxxxxxxx build xxxxxxxx-xxxx

IT Analytics requires a Web Server and a Database server.
They can be on separate machines or on same machine.
This script will only install the Web Server components.
Will this machine be the Web Server (y/n)?
```

Enter **y** if the machine is going to be the Portal web server. Otherwise, enter **n** to cancel the installation.

6 Enter **y** if you have the mounted ISO image. Otherwise, enter **n** to cancel the installation.

Ensure the ISO is labeled **IT Analytics Portal Software** and is mounted.

7 Press **Enter** to continue the installation. The End User License Agreement (EULA) is displayed.

8 Read the EULA. At the end of the EULA, the following output is displayed:

```
Please type 'accept' to accept these Terms and Conditions:
```

9 Type **accept** (all lowercase) and press**Enter**. Otherwise, type any other key and **Enter** to cancel the installation.

The installer will now copy and unzip the files. This may take several minutes depending on the performance of your system. The overall duration of the Portal installation is typically between 15 - 25 minutes.

10 Enter your domain name.

```
We need to configure machine names and IP addresses for the
IT Analytics Portal, Agent and database server.
The portal and agent machines will be called
itanalyticsportal.yourdomain and
itanalyticsagent.yourdomain
Enter your domain name: (yourdomain.com)
```

If the domain name displayed in parentheses is correct, press **Enter**. Otherwise, enter the correct domain name and press **Enter**.

Note: The domain name value you enter here determines the URL that will be used to login to the IT Analytics Web GUI. For example, if you enter companyabc.com, the URL will be **http://itanalyticsportal.companyabc.com**. You must make a note of the domain value since you will be asked for this value during the installation of the Data Collection components that collect data from the servers in your enterprise.

---

11 Validate the system's IP address for the Portal.

```
Enter IP Address for itanalyticsportal.yourdomain: (N.N.N.N)
```

If the IP Address displayed in parentheses is correct, press **Enter**. Otherwise, enter the correct IP Address and press **Enter**.

Note: Throughout these steps, yourdomain refers to the full domain, including the suffix, such as .com or .net. (Example: MyNetworkCompany.net).

---

12 Validate the IP address of the database server. If you installed the Database component on a separate server, be sure to supply the correct IP address of that server.

```
Enter IP Address of your database server: (N.N.N.N)
```

Note: If your database server is using an IPv6 address, enter that within square brackets. For example: [fe80::250:56FF:febc:1F]

If the IP Address displayed in parentheses is correct, press **Enter**. Otherwise, enter the correct IP Address and press **Enter**.

13 If you are installing the Database on the same server, use **localhost** for the IP address or **localhost6** for an IPv6 environment.

14 Confirm the entered IP addresses

```
You have entered:
Hostname                      IP Address
itanalyticsportal.yourdomain N.N.N.N
itanalyticsagent.yourdomain  N.N.N.N
database server              N.N.N.N
Is this correct (y/n)?
```

If the hostnames and IP addresses listed are correct, enter **y** and press **Enter**. Otherwise, enter **n** and press **Enter**.

15 Confirm changes to be automatically made to `/etc/hosts`.

```
These names will be set up in /etc/hosts.
You can remove the entries and add them
to your local DNS later.
Would you like to add them to /etc/hosts (y/n)?
```

If you would like to set up the names in **/etc/hosts**, enter **y** and press **Enter**. Otherwise, enter **n** and press **Enter**.

16 Choose whether to run the database creation script. This avoids the manual step of running `create_itanalytics_database.sh` later.

```
You can create the Database schema as a part of this
installation or create it later using
create_itanalytics_database.sh script.
Do you want to create the Database schema as a part of
this installation (y/n)?
```

17 After specifying your choice, press **Enter** .

Java and Apache software components are installed irrespective of your choice specified for the database schema. Tomcat Java Servlet Engine is installed as apart of this installation and it may take 1-2 minutes to execute.

This completes the installation of theIT Analytics Portal. If you have not installed the database schema during the above procedure, you can proceed to install the database schema.

Task 5: Installing the database schema (Linux)

System: Database Server

This section covers the creation of the IT Analytics database. Follow these steps on the same server you installed the Oracle application binaries.

Note: This step is required only if you have not opted to run as a part of the `Itanalyticsinstaller.sh` script.

---

1. Log in as **aptare** to your IT Analytics Database server.

   You must be logged in as a database user. If you already are logged in as root:

   ```
   su - aptare
   ```

   ```
   source <INSTALL_PATH>/aptare/bin/aptare_env.sh
   ```

2. Run the database installation script to install the IT Analytics database objects and schema:

   ```
   mnt/portal/create_itanalytics_database.sh
   ```

   Note: The following dialog will only appear if you are re-installing the IT Analytics database (e.g., after a failed attempt)

   The installer launches and prompts you to enter the domain name:

   ```
   Enter your IT Analytics Portal Domain Name: yourcompany.com
   You entered the following of your IT analytics
   domain name: yourcompany.com
   Your IT Analytics Super User Login Account will be
   admin@yourdomain
   Is this the correct domain name (y/n)? y
   ```

3. Database files will be extracted and the database schema will be created. This step will take between 5 - 10 minutes to complete.
4. Next, the installer will load the database with Oracle packages. This step will take between 30 - 60 minutes to complete, depending on your system performance.
5. The Portal user and the database schema are now created. During this step Oracle may produce messages similar to the following:

   ```
   mv: cannot stat
   `/opt/aptare/oracle/lib/EVENT_PACKAGE__PORTAL__2.so': No such
   file or directory
   ```

Note: These messages can be ignored. Any other exceptions or errors however indicate a potential issue with the installation.

```
Creating IT Analytics Portal user ...
Completed creation of the IT Analytics Portal database user
Creating IT Analytics database schema tables ...
...
... (EACH STEP LOGS TO THE CONSOLE...)
...
Completed creation of the IT Analytics base schema tables
Creating IT Analytics <backup product> schema tables ...
```

6. The Packages are now validated:

   If you do not see the message “Successfully validated ALL Packages” at the end of this step, there is a possible problem with the install and you should save a copy of the installer log and contact the Cohesity Support.

```
Validating IT Analytics Packages...
Validating PACKAGE ADAPTOR_PACKAGE
Validating PACKAGE ADMINREP_PACKAGE
Validating PACKAGE ALL_ERROR_PKG
...
... (EACH PACKAGE IS LOGGED TO THE CONSOLE...)
...
Validating PACKAGE XML_REPORT_PKG
Package specifications have successfully been validated
...
Successfully validated ALL Packages.
```

7. The database creation is now complete.

```
Creation of IT Analytics Database completed at
Nov 11 18:31:46 PDT 2021
A complete log of this session can be found in the file:
/opt/aptare/logs/install/create_itanalytics_database_xxxxx.log
```

Note: If the installer reports errors during the install and you are unable to resolve the problem, you should save a copy of the installer log and contact the Cohesity Support.

If you do not have a IT Analytics license, you can install a trial license which is valid for 60 days with the this command as a root user:

```
/opt/aptare/utils/installlicenseUI.sh /mnt/portal/license.slf
```

```
/opt/aptare/utils/installlicenseUI.sh
/mnt/portal/foundation_license.slf
```

8. Installation of the Database components is now complete.

   The IT Analytics database is a container database with the pluggable database SCDB attached to it. The data files for the tablespaces are stored in the /data01-06/oradata/scdbpdb directory.

   Continue to the next section for the final step--License Key file installation.

If you have configured a custom OS user or a group for Oracle or portal, instead of the default users or groups:

- Update the OS user and group details in the environment file `/opt/aptare/bin/aptare_env.sh`.
- Ensure environment variables for Oracle, such as ORACLE_HOME, ORACLE_SID, PATH, LD_LIBRARY_PATH are set appropriately in `/opt/aptare/bin/aptare_env.sh` and are exported correctly.

Task 6: Start the Portal services (Linux)

Prior to installing the license key, you must start the Portal services to ensure that the installation was successful. You will not be able to log into the Portal yet, because you haven't installed the license key.

As user root, at the command line, enter this command: **`systemctl start aptare`**

This starts all the services required for IT Analytics that includes:

- Oracle
- TNS listener
- Kafka
- ZooKeeper
- Portal Tomcat instance
- Agent Tomcat instance
- Anomaly Tomcat instance
- Apache

Task 7: Request the license key file (Linux)

A valid license key file is required to run the IT Analytics application. Refer to the Licensing documentation for information.

See "Get the IT Analytics license key file" on page 11.

Task 8: Log into the Portal

Log into the Portal (http://itanalyticsportal.yourcompany.com) with your username as <admin@yourcompany.com>. The Portal has an initial default password **P@ssw0rd**. You must change this password after your first login.

Note: The default password contains a zero, not an uppercase O.

Task 9: Install the license key file (Linux)

A valid license key file is required to run the IT Analytics application. Refer to the Licensing documentation for information.

See "Install a license" on page 10.

Task 10: Performing a cold backup of the database (Linux)

Prior to deploying the Portal for operational use, perform a cold backup of the Oracle database. This offline, cold backup simply means that you'll physically copy or backup the files to another location. This cold backup will simplify the restore process, in the event of unanticipated data loss. With a cold backup, you simply have to restore the files and then import the most recent database export. In addition to this initial cold backup, you may consider performing a cold backup periodically--for example, after a significant software upgrade--to re-capture the database schema.

Recommended database backup process

1. Cold Backup
2. Daily Exports of the database
3. In the event of data loss, restore the database and then import the most recent database export.

Uninstall the IT Analytics Portal

This procedure uninstalls the application and removes the Oracle database, including all the data that resides on that database. If required, you can back up the database at a different location before the uninstallation.

1. Login as **root** to the IT Analytics server
2. From the root directory (/) stop the Portal services and run the uninstall script:

   ```
   systemctl stop aptare
   /opt/aptare/utils/uninstall_portal.sh
   ```

3. Follow the prompts as required to confirm deletion of the IT Analytics components.

Section 3

Data Collector Policy Configuration and Reports

- Chapter 4. Configure NetBackup appliance
- Chapter 5. Configure NetBackup Flex Appliance
- Chapter 6. Configure NetBackup Data Collector policy
- Chapter 7. Configure Backup Exec
- Appendix A. Foundation License OOTB Reports

Chapter 4

Configure 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.

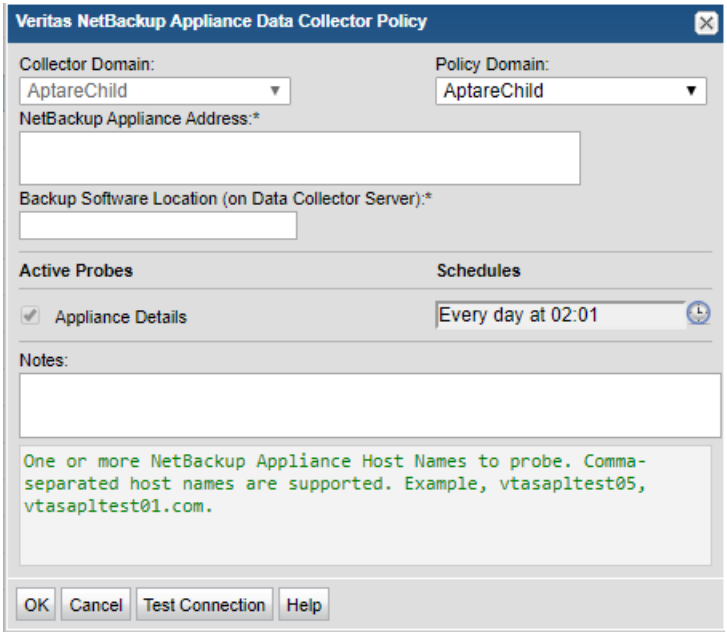
Adding a Veritas NetBackup Appliance Data Collector policy

- 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.
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

Field	Description
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.
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 5

Configure NetBackup 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.
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.

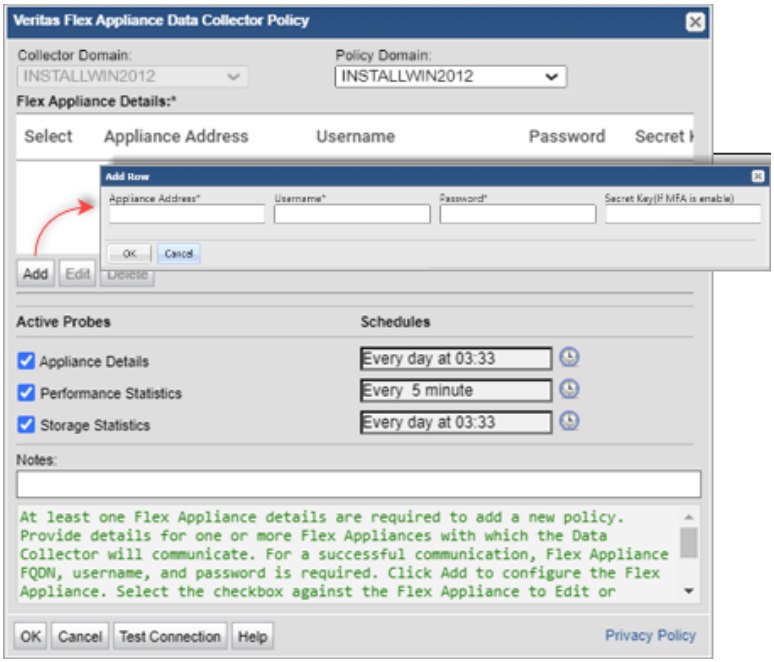
Table 5-1 Data collection based on appliance version

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 6

Configure NetBackup Data Collector policy

This chapter includes the following topics:

- Introduction
- General prerequisites for adding Data Collectors (Cohesity NetBackup)
- Add a Veritas NetBackup Data Collector policy

Introduction

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

Watch this video of how to configure a Data Collector and configure a policy for data collection.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6301527837001

General prerequisites for adding Data Collectors (Cohesity NetBackup)

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

- Supports Amazon Corretto 17. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- In support of near-real time collection for Veritas NetBackup, the following knowledge base article discusses additional information about nbu_monitor_util: https://www.veritas.com/support/en_US/article.100047232.
- Windows Only Requirement -
  If a Data Collector is required to collect data from Cohesity NetBackup Primary Server running on Windows System to non-English (United States) locale:
  - A Windows user must be created with the Administrative group of Windows system that will run the data Collector with culture set to English-US, and Region and Language set to English -US.
  - The current system locale must be set to the same language as the NetBackup Primary Server.
- For performance reasons, do not install Data Collectors on the same server as the Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).
- For most Backup Manager systems, install the Data Collector on a server that is in the same time zone as the backup server from which you are collecting data. For Cohesity NetBackup and IBM Spectrum Protect (TSM) collection, the Data Collector server and backup server can be in different time zones.
- Uses ports 443, 1556, and 13724 WMI range of ports, Linux ssh 22
- The NetBackup Event Monitor probe, enabled on the data collector policy screen, uses the nb_monitor_util executable. This executable is installed by default for all NetBackup 8.2 installations. It can be found in the /usr/openv/netbackup/bin/goodies directory on Linux and \Program Files\Veritas\Netbackup\bin\goodies on Windows. The Event Monitor probe collects events generated by the nb_monitor_util and handles create/update/delete events for Backup Policy, Storage Unit, Storage Unit Group and Storage Lifecycle Policy.
- The data collection, while executing the NetBackup probes, is supported even if the root/admin users does NOT have the CLI access permission in NetBackup.

Note: This scenario is applicable in the distributed environment.

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.

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.

- **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.

  If you use centralized NetBackup data collection, you must also configure the settings in the Remote Probe Login Details section of this Data Collector policy.

  This probe also collects historical incomplete SLP jobs. Images and copies can remain incomplete in IT Analytics after they age past the standard SLP lookback window. Regular SLP job collection no longer refreshes them. Historical collection updates these records from the NetBackup catalog during scheduled collection. Two advanced parameters control historical collection:

  - NBU_ENABLE_HISTORICAL_INCOMPLETE_SLP_JOB_COLLECTION enables or disables historical collection.

- NBU_HISTORICAL_INCOMPLETE_SLP_JOB_COLLECTION_INTERVAL_DAYS sets the number of days between historical collection runs.

Refer to Backup Manager advanced parameters section for more details on these parameters.

The historical date window is controlled by the **Look back for incomplete NetBackup Storage Lifecycle Policy (SLP) jobs (days)** and **Look back for historical incomplete NetBackup Storage Lifecycle Policy (SLP) jobs (days)** system parameters in the Portal.

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.

- **Client Attributes**: Select the check box to activate client attribute data collection from your NetBackup environment. This probe calls the NetBackup REST API host-properties endpoint on each NetBackup Primary Server to collect and persist server-level and client-level configuration attributes.
  - The attributes collected include client browse and restore permissions, free browse, maximum data streams (jobs), client-side deduplication and Client Direct settings, connect options, Windows Open File Backup (WOFB) provider, usage and error control settings, and the Offline for backup and Offline for restore values, including the date and time until which a client is offline.
  - This probe is not selected by default, for both newly created and upgraded policies. It must be enabled explicitly before scheduled collection can run.
  - The default schedule is once a day at midnight (CRON string 0 0 * * *). 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. Optimize performance by scheduling less frequent collection.
  - You can also run this probe on demand by selecting Client Attributes in the Run dialog on the **Admin** > **Data Collection** > **Collector Administration** page. An on-demand run executes immediately and does not change the saved policy setting or schedule.
- **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.

Chapter 7

Configure Backup Exec

This chapter includes the following topics:

- Introduction
- Architecture overview (Veritas Backup Exec)
- Backup Exec terminology
- Prerequisites for adding data collectors (Veritas Backup Exec)
- Upgrade troubleshooting: Microsoft SQL Server and Java 10
- Installation overview (Veritas Backup Exec)
- Enable TCP/IP for the SQL server
- Configure a Windows user
- Add Backup Exec servers
- Importing Backup Exec Server information
- Add a Veritas Backup Exec Data Collector policy

Introduction

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

Architecture overview (Veritas Backup Exec)

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

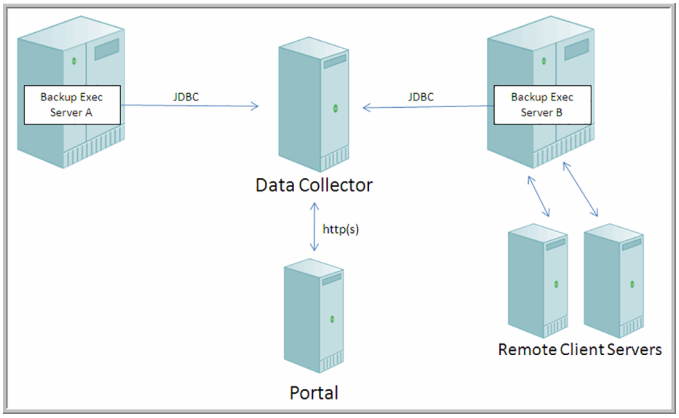


Figure 1 Data Collector in a Veritas Backup Exec Environment

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

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

Backup Exec terminology

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

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

Prerequisites for adding data collectors (Veritas Backup Exec)

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

Upgrade troubleshooting: Microsoft SQL Server and Java 10

With release version 10.3 introducing support for Java 10, older versions of MS SQL Server may encounter compatibility issues. The following section covers potential workarounds. Collection occurs from the Microsoft SQL Server database used by the system the data collector is collecting from. The version of Java used by IT Analytics version 10.3 disables some insecure TLS algorithms by default. If collection fails with the following error in the collector logs, the version of MS SQL Server may be incompatible and not allow collection using the TLS algorithms enabled by default with Java 10.

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

Upgrade MS SQL Server to the latest version to enable secure collection. Your MS SQL Server version may not be supported for IT Analytics version 10.3. If upgrade is not possible, a workaround can be attempted to restore compatibility. If the following steps do not resolve the issue, your version of MS SQL Server is not supported.

Use the following steps to modify the enabled algorithms to allow communication with the data collector:

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

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

4. Remove 3DES_EDE_CBC.

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

```
1024, \
EC keySize < 224, DES40_CBC, RC4_40
```

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

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

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

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

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

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

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

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

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

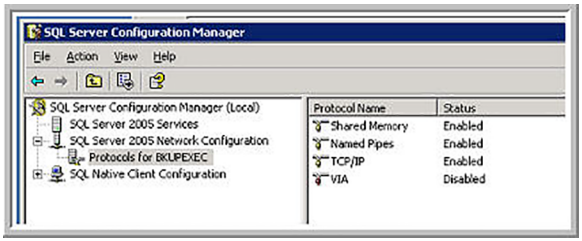
Installation overview (Veritas Backup Exec)

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

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

Enable TCP/IP for the SQL server

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

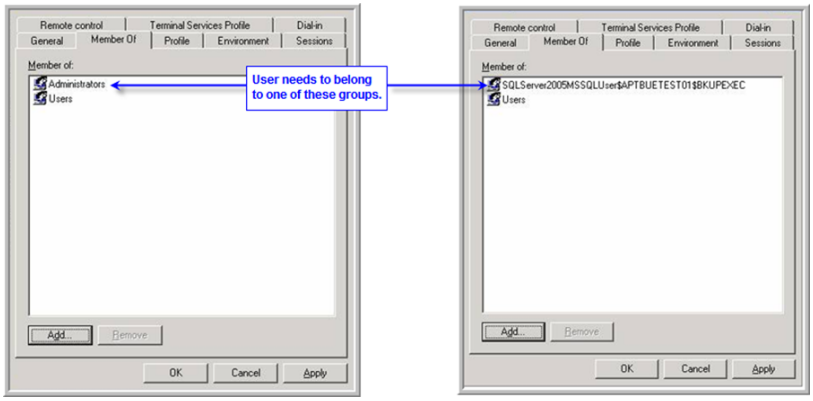


Configure a Windows user

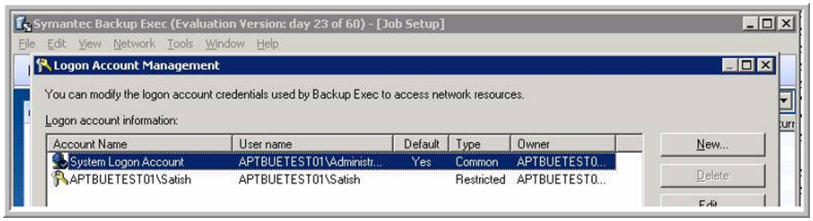
The Data Collector for Backup Exec requires a Windows User with privileges to access the SQL Server that is hosting the Backup Exec database.

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

- the local **Administrators** group
- a group named: **SQLServer2005MSSQLUser$ServerName$BKUPEXEC** where ServerName is the name of the server on which the SQL Server and Backup Exec reside, as shown in the following example.



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



Add Backup Exec servers

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

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

Importing Backup Exec Server information

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

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

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

   Each line in the CSV file should follow this format:

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

   Example CSV File:

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

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

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

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

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

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

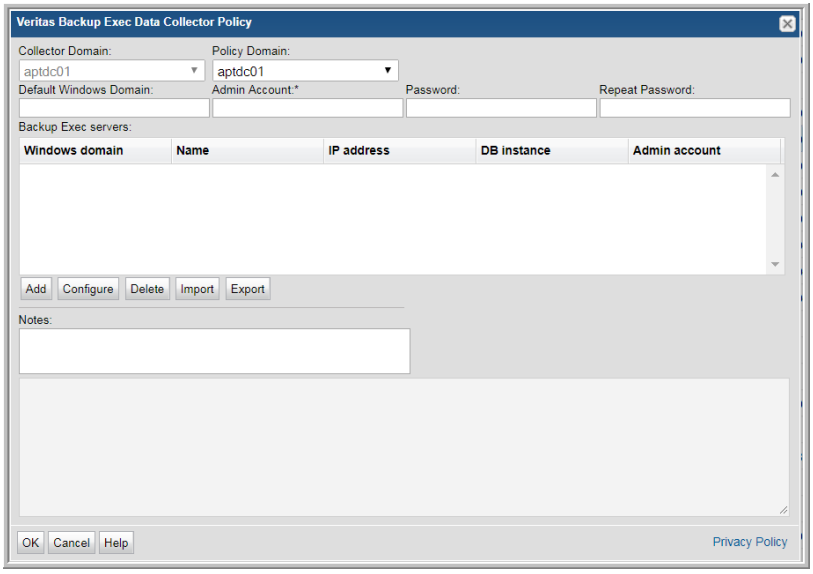
Add a Veritas Backup Exec Data Collector policy

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

To add the policy

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

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



5 Enter or select the parameters.

See See Table 7-1 on page 91.

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

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

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

Table 7-1 Policy Parameters

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

Table 7-1 Policy Parameters *(continued)*

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

Appendix A

Foundation License OOTB Reports

This appendix includes the following topics:

- IT Analytics reports and alerts supported in Foundation license

IT Analytics reports and alerts supported in Foundation license

Foundation license supports the following set of reports and alerts that are relevant to the Cohesity NetBackup and Cohesity Backup Exec policies.

System Administration Reports

1. Top Running Reports
2. Audit Events Details
3. Audit Events Summary
4. Data Collection Message Summary
5. Data Collection Performance Summary
6. Data Collection Schedule Summary
7. Data Collection Status Details
8. Data Collector Status Summary
9. Database Error Aggregation
10. Database Error Summary
11. License Summary

12. Oracle Job Overview
13. Portal Error Aggregation
14. Portal Error Detail
15. Report Activity Detail
16. Report Activity Summary
17. Scheduled Reports Summary
18. Version History
19. System Health Check
20. WMI Proxy Servers

Backup Administration Reports

1. Command Center Dashboard
2. Data Protection Dashboard
3. Job Histogram
4. Mission Control -Backup
5. NetBackup Audit Report
6. NetBackup Host Certificates
7. NetBackup License Summary
8. NetBackup Non-Host Certificates
9. Operations Dashboard

Backup Policies Reports

1. Application Storage Dashboard
2. Array Capacity and Utilization
3. Backup Volume by NetBackup Policy
4. NetBackup Policies
5. NetBackup Protection Plan

Billing and Usage Reports

1. Billing and Chargeback Summary
2. NetBackup Front End Size by Duration and Workload
3. NetBackup Front End Size by Workload
4. Server Consumption Summary

Forecasting and Capacity Planning Reports

1. Library Capacity Forecast
2. Media Availability Forecast
3. Media Consumption Forecast
4. Scratch pool Forecast
5. Tape Drive Usage and Forecast

Management Reports

1. Backup Executive Summary
2. Consecutive Errors
3. Error Log Summary
4. Error Log Summary by Policy
5. Error Log Summary by Server
6. Job Duration
7. Job Duration by Source
8. Job Error Code
9. Job Summary
10. Job Summary by Server
11. Job Summary by Source
12. Job Summary by Status
13. Job Throughput by Client
14. Job Type Summary
15. Job Volume Summary
16. Largest Backup Volume
17. Master Server Job Throughput
18. Monthly Backup Summary
19. NetBackup Deduplication to MSDP Savings - By Clients
20. NetBackup Deduplication to MSDP Savings - By Master Servers
21. NetBackup Deduplication to MSDP Savings - By Policy Type
22. NetBackup Deduplication to MSDP Savings Dashboard
23. NetBackup Deduplication to MSDP Savings Trend Over Time

24. NetBackup Media Server Job Throughput
25. NetBackup SLP Status
26. NetBackup SLP Status By Client
27. NetBackup SLP Status By Image Copy
28. NetBackup SLP Status By SLP
29. Running and Queued Job Summary
30. Source Backup Count Summary

Media Management Reports

1. Current Media Summary
2. Tape Media Summary

SLA Reports

1. Backup Duration SLA
2. Backup Start Time SLA
3. Backup Status SLA

Storage Utilization Reports

1. Drive Usage and performance
2. Drive Performance Summary
3. Drive Utilization and Performance
4. NetBackup Deduplication Efect
5. NetBackup Deduplication Savings Trend
6. NetBackup Deduplication Summary by Client
7. NetBackup Disk Pool Capacity and Usage
8. NetBackup Disk Pool Summary by Server
9. NetBackup Pre Vs Post Deduplication
10. NetBackup Storage Unit Summary
11. NetBackup Storage Unit Usage
12. Real Time Library and Drive Status
13. Storage Unit Detail
14. Tape Library and Drive Utilization

Alerts

1. Alert Delivery Failure
2. Alert Detail
3. Alert Detail History
4. Alert Summary
5. Alert Summary History
6. Alert Trend
7. Alert Dashboard