APTARE IT Analytics Data Collector Installation Guide for File Analytics

Release 10.5

VERITAS™

APTARE IT Analytics Data Collector installation guide for File Analytics

Last updated: 2021-12-01

Legal Notice

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

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Pre-Installation setup for File Analytics

This chapter includes the following topics:

Pre-Installation setup for File Analytics

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.

When the APTARE 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.

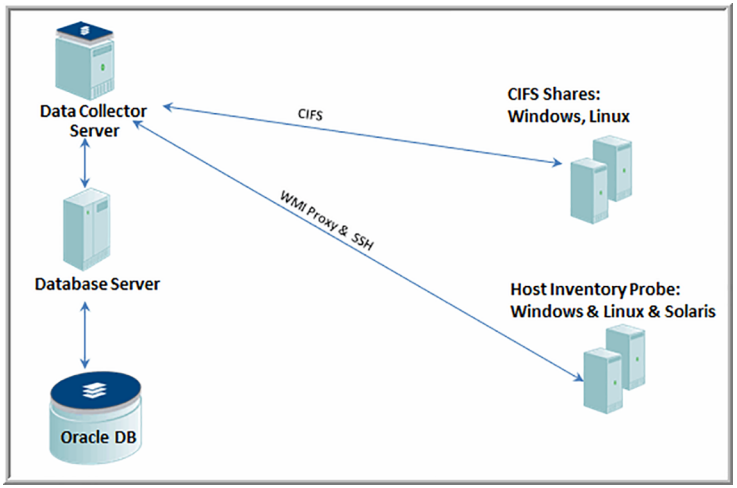
File Analytics Data Collection overview

File Analytics offers a highly optimized, lightweight data collector that uncovers files that are needlessly consuming storage. The bulk of wasted space often can be attributed to unstructured data--that is, files that contain data such as email, word processing documents, presentations, and digital media. Unlike structured data, which is managed by database administrators, unstructured data tends to proliferate with reckless abandon, resulting in stagnant and duplicated data. To assess the value of data files, whether they are critical to operations or are merely forgotten files, File Analytics provides data profiling. This data classification enables aggregation of file types and data growth forecasting. In addition, storage administrators can make archiving decisions based on the age of the data and its relevance to business objectives.

Once data collection completes, a number of reports provide insight into file profiles in your enterprise. Using built-in categorization and also file categories that you can customize, File Analytics becomes part of your arsenal of storage management tools. File Analytics aggregates the data, making it easy for you to identify offenders, such as:

- Deduplication candidates
- File ownership (or lack thereof)
- Largest files
- File Categories (Top file types by volume)

File Analytics Data Collection architecture



File Analytics Data Collector policies

File Analytics data collection can be configured in different ways, depending on the location of the files you want to profile in your enterprise. Determine which of the following approaches is relevant for your environment:

- Create a File Analytics Data Collector policy to configure a file shares probe. This Data Collector traverses the network CIFS shares to collect and categorize filesystem storage consumption metadata. This highly optimized traversal profiles unstructured data to enable you to identify storage that can be reclaimed. Use this for any CIFS share that is serving up files that you want to profile, regardless of manufacturer of the appliance.
- Host Discovery and Collection option directly interrogates hosts' attached storage to profile files. Configure a host probe for Windows (WMI Proxy) and Linux (SSH) collection of a host's locally attached storage.
  See "Host Discovery and Collection File Analytics probe" on page 10.

Prerequisites for adding Data Collectors (File Analytics)

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

- For Linux based Data Collectors, verify the rpm fontconfig is installed. Fontconfig is a library designed to provide system-wide font configuration, customization and application access. If the rpm fontconfig is not installed, the installer will not be able to load User Interface Mode. This is a prerequisite for a new Data Collector installation.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the APTARE 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).

CIFS shares

- This Data Collector can collect both Linux and Windows shares. The recommended Windows Data Collector server operating system is Windows Server. See the *Data Collector Supported Operating Systems* sections of the *APTARE IT Analytics Certified Configurations Guide* for supported OS versions.
- The Windows LAN Manager authentication level, in the local security policy security options, must be modified to: Send LM & NTLM - use NTLMv2 session security if negotiated. This allows the Data Collector to invoke the **net use** command with the password supplied on the command line. Without this setting, later versions of Windows will terminate with a system error 86 (invalid password).
- Windows CIFS Shares collection requires the Windows Domain User ID. This User ID must have Administrative privileges.
- Linux CIFS Shares collection requires super-user root privileges. Access control commands, such as sudo, sesudo, and pbrun are also supported. If using any of the access control commands, verify that the User ID has sudo, sesudo, or pbrun privileges.
- Collection of owner data for Windows and CIFS is configurable via Advanced Parameters. Data collection completes faster when owner data is not collected (the default). Although not recommended, you can configure an Advanced Parameter, FA_RESOLVE_OWNERS set to Y, to enable owner collection. To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Host Discovery and Collection File Analytics probe

Using Host Resources data collection, hosts are discovered and added to the Host Discovery and Collection list. Once a host is listed in the inventory, it can be selected and the File Analytics probe can be configured. To access the Host Inventory to enable File Analytics probes: **Admin > Data Collection > Host Discovery and Collection**

Note that by design, File Analytics host resources data collection occurs via activation of the probe in the Host Discovery and Collection window in the Portal.

File Analytics Probe Configurations by operating system

Refer to the *Certified Configurations Guide* for complete details.

Windows servers: A Domain Administrator user ID is required when collecting file-level data for File Analytics.

Linux servers: Linux is only supported with the following requirements:

- Root user access is supported.
- Non-root user access with sudo access control is supported.
- Non-root user access without sudo is not supported.
- Running collection with a sudo user on a Linux server requires the addition of an access control command for the server in the Host Discovery and Collection's Manage Access Control window: **Admin > Data Collection > Host Discovery and Collection**
  Also, an advanced parameter must be created: FA_USE_SUDO set to Y.
  To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Both Windows and Linux servers

If running collection via the checkinstall utility, verify the following:

- An advanced parameter must be created: FA_HOST_VALIDATE set to Y. To access Advanced Parameters in the Portal, select **Admin > Advanced > Parameters**.

Best practices for host Inventory File Analytics probes

Since most environments have hundreds, even thousands of hosts, it is recommended that File Analytics probes be configured in a staggered schedule so as not to overload the Data Collector server.

Adding a File Analytics Data Collector policy

One of the types of data collection that can be configured for File Analytics is collection of CIFS shares. The Data Collector will take the configuration that you specify, including the share names and credentials, and then traverse the file system structure to identify these shared resources on your network and collect the relevant metadata.

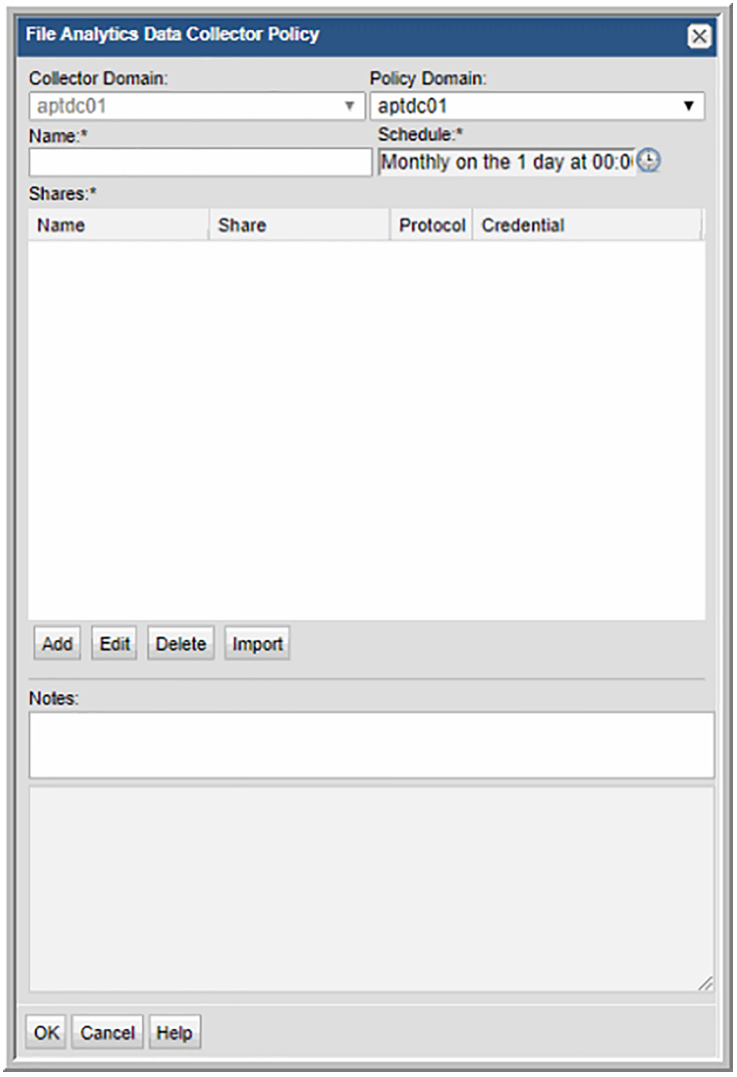
Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.

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

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.

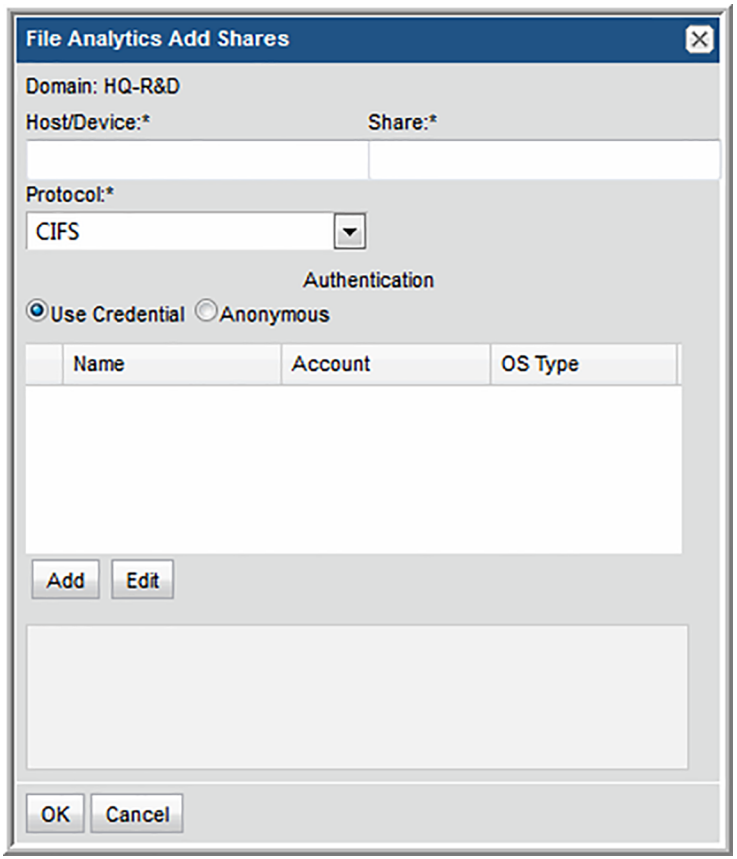
4 Click **Add Policy**, and then select File Analytics policy.



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

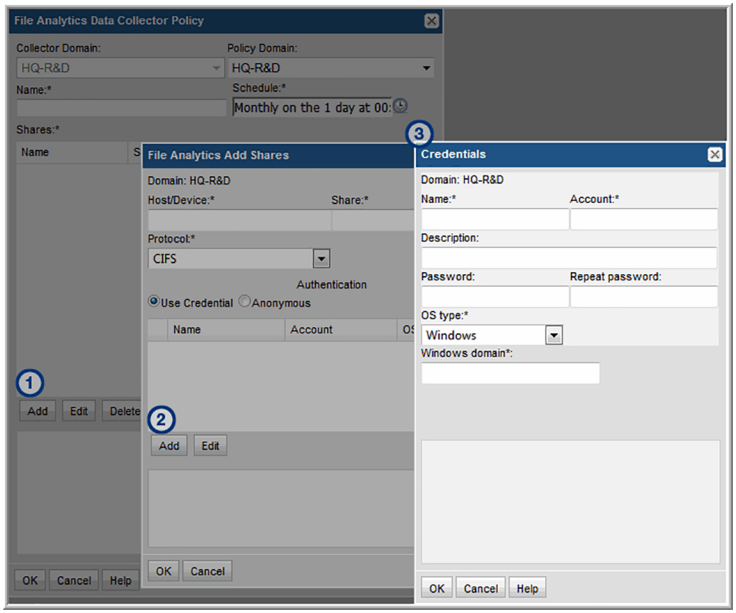
Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Collector Domain is the domain that was supplied during the Data Collector installation process. The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Name*	Enter a name that will be displayed in the list of Data Collector policies.
Schedule*	Click the clock icon to create a schedule. Every Minute, Hourly, Daily, Weekly, and Monthly schedules may be created. Advanced use of native CRON strings is also available. Examples of CRON expressions: */30 * * * * means every 30 minutes */20 9-18 * * * means every 20 minutes between the hours of 9am and 6pm */10 * * * 1-5 means every 10 minutes Mon - Fri. 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.
Shares*	Click **Add** to configure the CIFS shares that the collector will probe. Click **Edit** to modify a CIFS share configuration. Note that the Import button in this window enables bulk loading of CIFS shares. See “Importing the CIFS share configuration” on page 16.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

6 Enter or select CIFS shares configuration parameters in the **File Analytics Shares** window.



Field	Description	Sample Value
Host/Device*	Enter the host IP address or host name for the device that is being probed for CIFS shares. This also could be a non-host device, such as a NetApp array.	**172.1.1.1**
Share*	Enter the name of the CIFS share that the Data Collector will probe.	HOME
Protocol*	CIFS is currently the only option.	
Authentication	Click either Anonymous or Use Credentials. If you are using credentials, click **Add** to configure the CIFS share credentials, or select an existing credential definition and click **Edit**.	

7 Enter credentials in the **Credentials** window.



Field	Description	Sample Value
Name*	Assign a name to identify the set of credentials that you are defining.	
Account*	Enter the login account name used to log in to the hosts. If the policy includes a group of Windows hosts, use the Windows Domain user ID. This user ID must have administrative privileges. For Linux hosts, super-user root privileges are required. You also could use an access control command, such as sudo, sesudo, or pbrun. If using any of these access commands, ensure that the user ID has sudo, sesudo, or pbrun privileges. Some enterprises prefer to create a new user and provide access to commands via an access control command.	root
Description	Enter a note to help identify the credential.	
Password	Enter the password for the account	
OS Type*	Select either Windows, Linux, or NAS	
Windows Domain*	For Windows hosts only: Specify the Windows domain name. If the host is not a member of a domain, or to specify a local user account, use a period (.)	

Field	Description	Sample Value
Private Key File	For Linux hosts only: If you have configured a Public/Private Key between your Data Collector server and the hosts you intend to monitor, specify the location of the Private Key file on the Data Collector Server.	
Known Hosts File	For Linux hosts only: If you have configured a Public Key/Private Key between your Data Collector server and the hosts you intend to monitor, specify the location of the Known Hosts file on the Data Collector Server.	

8 Click **OK** to close and save the configuration in each window.

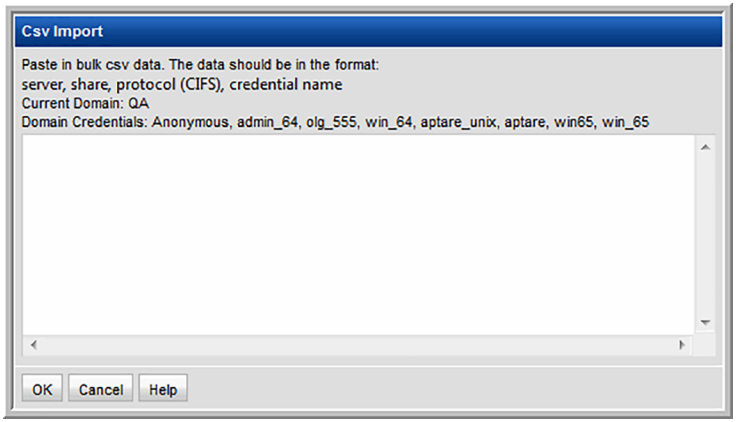
Importing the CIFS share configuration

The import feature facilitates entry of a large number of CIFS shares. Simply paste the details in comma-separated format into the window and click **OK**.

Data Format:

```
host, share, protocol (CIFS), credential name
```

The Credential Names, already configured for the current Domain, are displayed at the top of the window.



Chapter 2

Installing the Data Collector software

This chapter includes the following topics:

Introduction

This section includes the instructions for installing the Data Collector software on the Data Collector Server. In addition, if you are collecting data from host resources, you may need to install the WMI Proxy Service. The WMI Proxy Service is installed by default, as part of the storage array Data Collector installation on a Windows server.

In addition to the GUI version, the installer supports a console (command line) interface for Linux systems that do not have X-Windows installed. You will be directed to the console interface instructions, if appropriate.

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

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

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

Installing the WMI Proxy service (Windows host resources only)

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

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

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

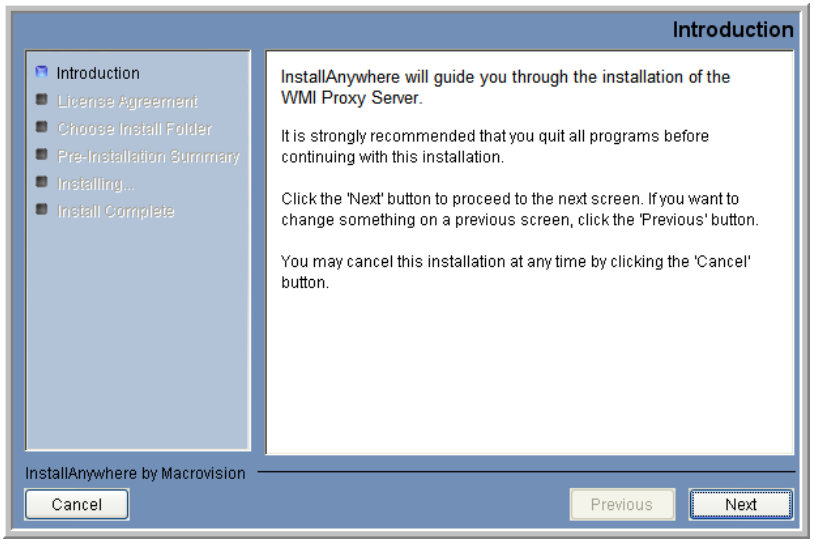
   On Windows:

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

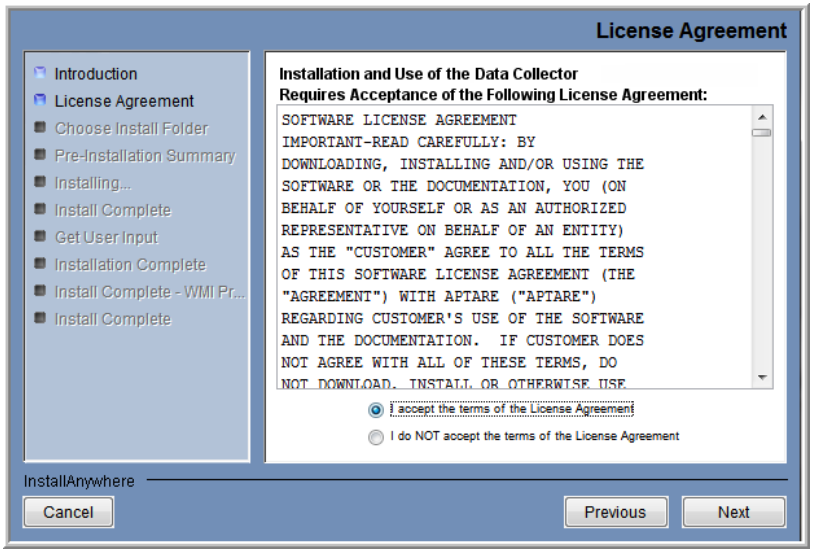
   On Linux:

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

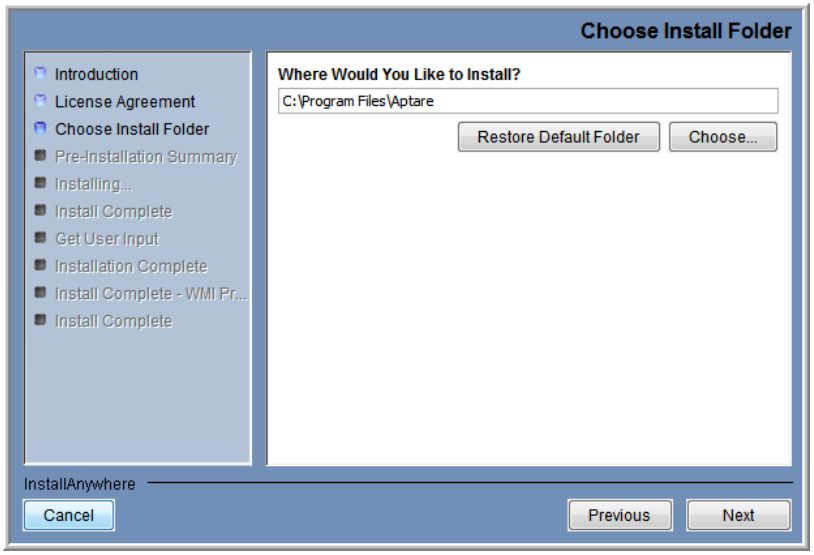
2. Install Anywhere will prepare to install the Data Collector Software. An Introduction dialog box will outline the installation process.



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



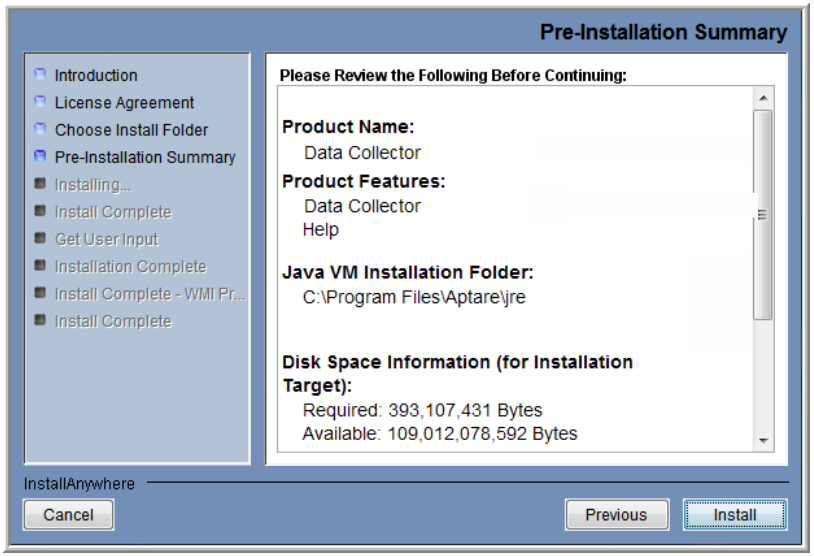
4. Read the agreement.
5. Click on the “I accept the terms of the License Agreement” radio button.
6. Click **Next** to display the window where you will choose the installation folder.



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

   Note: Accepting the default path is recommended.

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



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

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

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

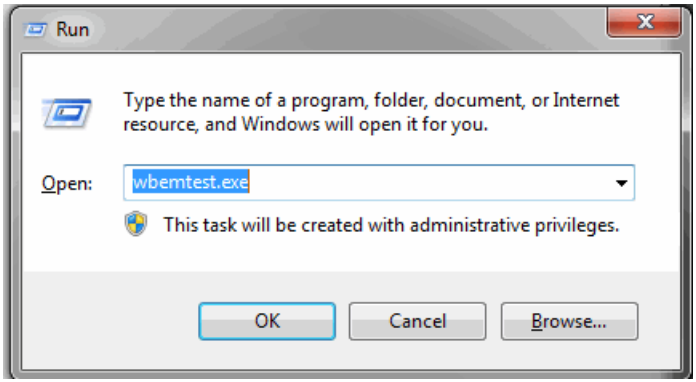
    Startup > Control Panel > Administrative Tools > Services
14. A window will be displayed when the installation is complete.
15. Click **Done** to complete the process.
16. It is recommended that you run the C:\Program Files\Aptare\mbs\bin\checkinstall.bat batch file to validate the Data Collector Installation.

Testing WMI connectivity

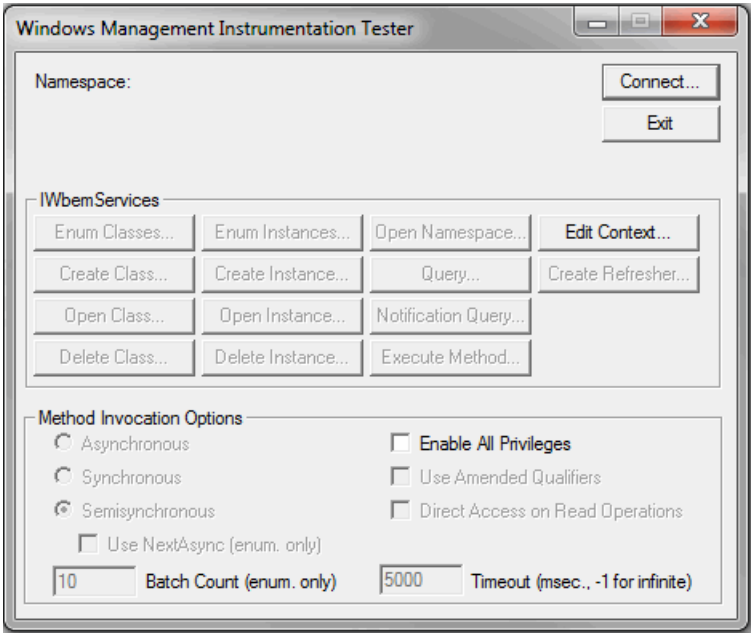
The Windows Management Instrumentation (WMI) Proxy is used by APTARE IT Analytics to collect data from Windows hosts. Should you have connectivity issues, these steps can be taken to test and troubleshoot connectivity.

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

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

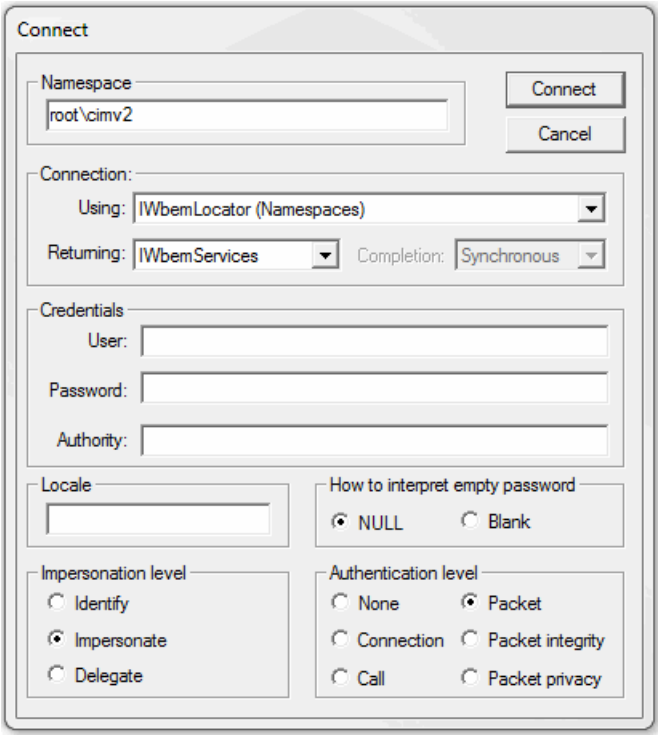


3. In the Windows Management Instrumentation Tester window, click **Connect**.



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

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



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

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

Installing Data Collector software: From the internet

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

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

If your Data Collector Server does not have Internet access or web browser access--for example, X-Windows not available, proceed to the following section.

See "Installing Data Collector software: No internet available from the Data Collector server" on page 25.

1. Start the web browser on the **Data Collector Server**.
2. Navigate to the Support website to access the relevant download link.
3. Select the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.
   - Linux: sc_datacollector_linux_<releaseversion>_<MMDDYYYY>.bin
   - Windows: sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe
4. Execute the OS-specific Data Collector installer.
5. Proceed to the UI Deployment of the Data Collector.

   See "Installing Data Collector software on Windows portal platform" on page 26.

Installing Data Collector software: No internet available from the Data Collector server

Use these instructions if you are installing via the Internet where Internet access is not available from the data collector server.

1. Note the Platform/OS of the **Data Collector Server**on which you want to install the Data Collector.
2. Open a browser on a client with web access (you will download the installer to this client, and then copy it to the **Data Collector Server**).
3. Navigate to the Support website to access the relevant download link.
4. Download the Data Collector Installer that corresponds to the platform of the **Data Collector Server**.
   - Linux: sc_datacollector_linux_<releaseversion>_<MMDDYYYY>.bin

- Windows: sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe

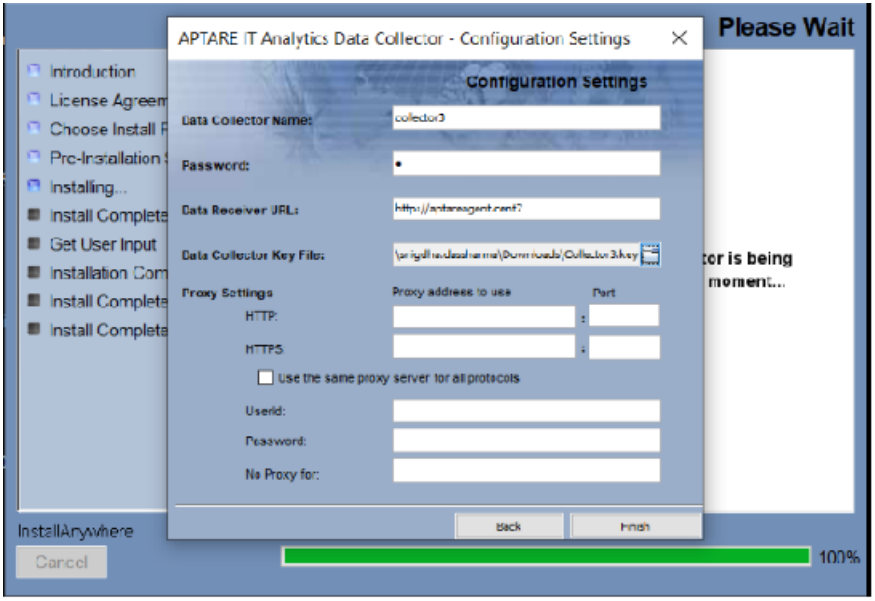
5. At the prompt, save the Data Collector Installer to a directory on the client.
6. Copy the Data Collector Installer to the Data Collector Server where the Data Collector is to be installed.
7. Go to the Data Collector Server and run the installer.
   - **On Windows:**
     Execute sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe
   - Proceed to the UI deployment.
     See "Installing Data Collector software on Windows portal platform" on page 26.
   - **On Linux:**
     If the **Data Collector Server** has X-Windows, take these steps, substituting the relevant Data Collector Installer name for **<installer_file>**
     chmod +x <installer_file>
     sh ./<installer_file> -i swing
   - Proceed to the UI deployment.
     See "Installing Data Collector software on Windows portal platform" on page 26.
     If the **Data Collector Server** does not have X-Windows:
   - Proceed to the Console Installation instructions.

Installing Data Collector software on Windows portal platform

InstallAnywhere will prepare to install the Data Collector software. After checking the available disk space and downloading the installer, an introduction dialog window outlines the installation process.

1. Review the installation process and click **Next**. The License Agreement displays for your acknowledgement.
2. Read the agreement and click the "I accept" radio button and then **Next**. The installer will display a window, which prompts you for an Install Folder.

3. Specify the directory where you would like to install the Data Collector software. Accepting the default paths is recommended. Windows default directory: `C:\Program Files\Aptare`
4. Click **Next** to display the Pre-Installation Summary.
5. Review the summary and click **Install**. The dialog tracks the installation as it progresses.
6. A Configuration Settings window will prompt you to select a Data Collection Task. The configuration choices are: Data Collector (includes WMI Proxy) or WMI Proxy Server (only). A single Data Collector can be installed for multiple products on a single server. When you select a backup product, if you are installing on a Windows server, the WMI Proxy Server is automatically included with the installation. When you select a storage array, the Host Resources setup is automatically included in the installation. The WMI Proxy Server also can be installed individually.
7. Enter the configuration settings for your particular environment.



8. After entering the configuration settings, click **Next**. At this point, the Data Collector has been successfully installed, however, to validate the Data Collector installation, it is recommended that you run the `C:\Program Files\Aptare\mbs\bin\checkinstall.bat` batch file.

9. Choose **Run now** and click **Done** in the **Get User Input** window to validate the installation and then quit the installer. The InstallAnywhere portion of the installation is now complete and the process continues with the command-line script execution.

Table 2-1 Configuration settings

Field	Description
Data Collector Name *	A unique name assigned to this Data Collector. This is the name that you used during the pre-Installation setup. The Data Collector will use this value for authentication purposes.
Password *	The password assigned to this Data Collector. The password is encrypted prior to saving in the APTARE IT Analytics database and is never visible in any part of the application.
Data Receiver URL*	This is the URL the Data Collector uses to communicate to the Portal server. The format of this URL should be: http://aptareagent.yourdomain.com It is similar to the URL you use to access the web-based Portal (http://aptareportal.yourdomain.com). **Note:** Be sure to enter the URL with the prefix aptareagent and NOT aptareportal.
Data Collector Key File	Enter or browse for the location of downloaded collector key file for encryption. **Note:** This is the key that was downloaded from the Portal during data collector creation. If the existing key file is not available during the reinstallation of the data collector, regenerate and download a new Data Collector key file from the portal and use its file path.
Proxy Settings (Optional)	Enter the proxy server details for both http and https, including the User ID and Password for the server. HTTP/HTTPS: Enter a hostname or IP address and a port number. Use the same proxy server for all protocols: Check this box if the proxy server is used for all. User ID & Password: Enter the credentials for the proxy server. No Proxy for: List hostnames or IP addresses that will not be proxied. Examples: 192.168.1.1/21, localhost

Installing Data Collector software on Linux portal platform

Follow these instructions when installing on a Linux server that does not have X-Windows. The Installer will guide you through the sequence of steps to install and configure the Data Collector. If at any time you need to go back a step, simply type ‘back’ at the prompt.

Note: The Data Collector installer does not support console-based installation for the Windows operating system.

---

1. From your telnet session **cd** to the location where the Data Collector Installer file has been saved.
2. Execute the following commands, substituting the relevant Data Collector Installer name for <installer_name>.bin.

   ```
   chmod +x <installer_name>.bin
   sh ./<installer_name>.bin -i console
   ```

3. InstallAnywhere will prepare to install the Data Collector software.
4. The License Agreement will be displayed.
5. Read the agreement and type **Y** to accept it.
6. The installer will prompt for the installation location.
7. A Pre-Installation Summary will be displayed.
8. The installation process will track the progress.
9. The installer will prompt for the **Data Collector Name**. This is the ID that will be used on the Portal side to authenticate the Data Collector. This value should be the same value you configured on the Portal for the field “ID” during the Pre-Installation step.
10. The installer will prompt for the **Data Collector Password**. This is the password that will be used on the Portal side to authenticate the Data Collector. This value should be the same value you configured on the Portal for the field “passcode” during the Pre-Installation step.
11. The installer will prompt for the **Data Receiver URL**. This is the URL the Data Collector uses to communicate to the Portal server. This is the URL the Data Collector uses to communicate to the Portal server. The format of this URL should be:

    http://aptareagent.yourdomain.com

It is similar to the URL you use to access the web-based Portal (http://aptareportal.yourdomain.com).

IMPORTANT NOTE: Be sure to enter the URL with the prefix aptareagent and NOT aptareportal

```
Configuration Settings - 3
        -------------------------
        Enter Data Receiver URL
        (Required Field)
        Data Receiver URL (DEFAULT: ):
http://aptareagent.yourdomain.com
        The installer will perform a post-install validation:
        The installer will now configure the installation.
        This may take a few minutes.
```

12. Installer will prompt for **Enter Data Collector's Key File path**. Enter the location of the downloaded collector key file for encryption.

Note: This is the key that was downloaded from the portal while creating the data collector. If the key file is not available during the reinstallation of the data collector, regenerate and download a new Data Collector key file from the portal and enter its file path.

```
        Configuration Settings- 4
        --------------------------
        Enter the file path to the Data Collector's Key File
        (Enter the correct path to the Data Collector's Key File

       including file name that was downloaded from the Portal.)

        (Required Field)

        Data Collector Key File:
```

13. Web Proxy (HTTP) settings can be configured.

```
Configuration Settings- 5
---------------------------
Connection Settings
Use Proxies? (Y/N) (DEFAULT: N): y
```

```
Configuration Settings - 6
---------------------------
Enter HTTP Proxy IP Address
(Please leave field empty if there is no Proxy/Firewall)

HTTP Proxy IP Address (DEFAULT: ): 10.2.2.116
```

```
Configuration Settings - 7
---------------------------
Enter HTTP Proxy Port
(Please leave field empty if there is no Proxy/Firewall)

HTTP Proxy Port (DEFAULT: ): 3128
```

```
Configuration Settings - 8
---------------------------
Enter HTTPs Proxy IP Address
(Please leave field empty if there is no Proxy/Firewall)

HTTPs Proxy IP Address (DEFAULT: ):
```

```
Configuration Settings - 9
---------------------------
Enter HTTPs Proxy Port
```

```
        (Please leave field empty if there is no Proxy/Firewall)

        HTTPs Proxy Port (DEFAULT: ):

================================================================

        Configuration Settings - 10
        ---------------------------
        Enter Proxy UserId
        (Please leave field empty if there is no Proxy/Firewall)

        Proxy UserId (DEFAULT: ):

================================================================

        Configuration Settings - 11
        ---------------------------
        Enter Proxy Password
        (Please leave field empty if there is no Proxy/Firewall)

        Proxy Password:

================================================================

        Configuration Settings - 12
        ---------------------------
        Enter comma separated IP Addresses to exclude from Proxy

        (Please leave field empty if there is no Proxy/Firewall)

        No Proxy for (DEFAULT: ):

================================================================

        The installer will now configure the installation.
        This may take a few minutes.
        PRESS <ENTER> TO
CONTINUE:==================================
        Installation Complete
        ---------------------------------
        To validate the Data Collector installation, it is
recommended that you run the
        <home>/mbs/bin/checkinstall.sh script.
```

Chapter 3

Validating Data Collection

This chapter includes the following topics:

Validation methods

Validation methods are initiated differently based on subsystem vendor associated with the Data Collector policy, but perform essentially the same functions. Refer to the following table for vendor-specific validation methods.

- Test Connection - Initiates a connection attempt directly from a data collector policy screen that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors.
- On-Demand data collection run - Initiates an immediate end-to-end run of the collection process from the Portal without waiting for the scheduled launch. This on-demand run also serves to validate the policy and its values (the same as Test Connection), providing a high-level check of the installation at the individual policy level, including a check for the domain, host group, URL, Data Collector policy and database connectivity. This is initiated at the policy-level from **Admin>Data Collection>Collector Administration.**
  See “Working with on-demand Data Collection” on page 36.

- CLI Checkinstall Utility- This legacy command line utility performs both the Test Connection function and On-Demand data collection run from the Data Collector server.
  See "Using the CLI check install utility" on page 38.

Note: APTARE IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

Data Collectors: Vendor-Specific validation methods

Table 3-1 Vendor specific validation requirements.

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Amazon Web Services (AWS)	x	x	
Brocade Switch		x	
Brocade Zone Alias	x	x	
Cisco Switch		x	
Cisco Zone Alias	x	x	
Cohesity DataProtect	x	x	
Commvault Simpana			x
Dell Compellent			x
Dell EMC Elastic Cloud Storage (ECS)	x	x	
Dell EMC NetWorker Backup & Recovery	x		
Dell EMC Unity	x	x	
EMC Avamar		x	
EMC Data Domain Backup	x	x	
EMC Data Domain Storage	x	x	
EMC Isilon		x	

Table 3-1 Vendor specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
EMC NetWorker			x
EMC Symmetrix	x	x	
EMC VNX CLARiiON	x	x	
EMC VNX Celerra			x
EMC VPLEX			x
EMC XtremIO	x	x	
HDS HCP	x	x	
HDS HNAS		x	
HP 3PAR			x
HP Data Protector			x
HP EVA			x
HPE Nimble Storage	x	x	
Hitachi Block			x
Hitachi Content Platform (HCP)	x	x	
Hitachi NAS	x	x	
Huawei OceanStor	x	x	
IBM Enterprise			x
IBM SVC			x
IBM Spectrum Protect (TSM)		x	
IBM VIO	x	x	
IBM XIV			x
INFINIDAT Infinibox	x	x	
Microsoft Azure	x	x	
Microsoft Hyper-V	x	x	

Table 3-1 Vendor specific validation requirements. *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
Microsoft Windows Server	x	x	
NAKIVO Backup & Replication	x	x	
NetApp E Series			x
Netapp		x	
Netapp Cluster Mode		x	
OpenStack Ceilometer	x	x	
OpenStack Swift	x Test Connection is included with the Get Nodes function.	x	
Oracle Recovery Manager (RMAN)	x	x	
Pure FlashArray	x	x	
Rubrik Cloud Data Management	x	x	
VMWare			x
Veeam Backup & Replication	x	x	
Veritas Backup Exec			x
Veritas NetBackup	x	x	
Veritas NetBackup Appliance	X	x	

Working with on-demand Data Collection

Collections can run on a schedule or on-demand using the **Run** button on the action bar. On-demand allows you to select which probes and devices to run. The on-demand run collects data just like a scheduled run plus additional logging information for troubleshooting. A stopped Policy still allows an on-demand collection run, provided the policy is assigned to one of the specified vendors and the collector is online.

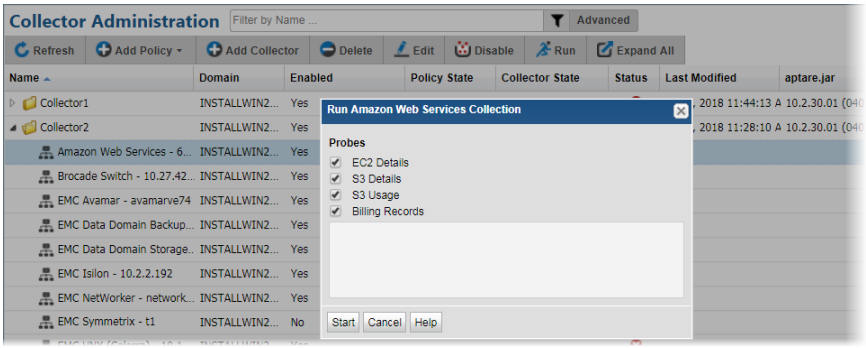
Note: On-demand data collection is not available for all policies.

On-Demand data collection serves multiple purposes. You can use it to:

- Validate the collection process is working end-to-end when you create a data collector policy
- Launch an immediate run of the collection process without waiting for the scheduled run
- Populate your database with new/fresh data

To initiate an on-demand data collection

1. Select **Admin > Data Collection > Collector Administration**. All Data Collectors are displayed.
2. Click **Expand All** to browse for a policy or use **Search**.
3. Select a data collector policy from the list. If the vendor is supported, the **Run** button is displayed on the action bar.
4. Click **Run**. A dialog allowing you to select servers and individual probes to test the collection run is displayed. The following example shows the Amazon Web Services dialog. See the vendor specific content for details on probes and servers.



5. Click **Start**. Data is collected just like a scheduled run plus additional logging information for troubleshooting. Once started, you can monitor the status of the run through to completion.

Note: If there is another data collection run currently in progress when you click **Start**, the On-Demand run will wait to start until the in-progress run is completed.

Using the CLI check install utility

This legacy utility performs both the Test Connection function and On-Demand data collection run from a command line interface launched from the Data Collector server.

Note: APTARE IT Analytics does not recommend using the CLI Checkinstall utility for any Data Collector subsystem vendor which supports On-Demand runs.

The following directions assume that the Data Collector files have been installed in their default location:

Windows (`C:\Program Files\Aptare`) or Linux (**/opt/aptare**).

If you have installed the files in a different directory, make the necessary path translations in the following instructions.

Note: Some of the following commands can take up to several hours, depending on the size of your enterprise.

To run Checkinstall

1. Open a session on the Data Collector server.

   Windows: Open a command prompt window.

   Linux: Open a telnet session logged in as root to the **Data Collector Server**.

2. Change to the directory where you'll run the validation script.

   Windows: At the command prompt, type:

   ```
   cd C:\Program Files\Aptare\mbs\bin <enter>
   ```

   Linux: In the telnet session, type:

   ```
   cd /opt/aptare/mbs/bin <enter>
   ```

3 Execute the validation script.

Windows: At the command prompt, type: `checkinstall.bat` <enter>

Linux: In the telnet session. type: `./checkinstall.sh` <enter>

The **checkinstall** utility performs a high-level check of the installation, including a check for the domain, host group and URL, Data Collector policy and database connectivity. This utility will fail if a Data Collector policy has not been configured in the Portal. For a component check, specifically for Host Resources, run the **hostresourcedetail.sh|bat**utility.

Checkinstall includes an option to run a probe for one or more specific devices. Note that certain Data Collectors will not allow individual selection of devices. Typically these are collectors that allow the entry of multiple server addresses or ranges of addresses in a single text box. These collectors include: Cisco Switch, EMC CLARiiON, EMC Data Domain, EMC VNX arrays, HP 3PAR, IBM mid-range arrays, IBM XIV arrays and VMWare. Data Collectors that probe all devices that are attached to a management server also do not allow individual selection of devices: EMC Symmetric, File Analytics, Hitachi arrays and IBM VIO.

4 If the output in the previous steps contains the word **FAILED**, then contact Support and have the following files ready for review:
`/opt/aptare/mbs/logs/validation/`

`C:\Program Files\Aptare\mbs\logs\validation\`

List Data Collector configurations

Use this utility to list the various child threads and their configurations encapsulated within a data collector configuration. This utility can be used in conjunction with other scripts, such as **checkinstall.[sh|bat]**.

On Linux: **./listcollectors.sh**

On Windows: **listcollectors.bat**

Chapter 4

Uninstalling the Data Collector

This chapter includes the following topics:

Uninstall the Data Collector on Linux

This uninstall process assumes that the Data Collector was installed using the standard installation process.

Uninstall the Data Collector on Windows

This uninstall process assumes that the Data Collector was installed using the standard installation process.

1. Login to the **Data Collector Server**. (User must have Administrator privileges.)
2. Stop the Data Collector services.
   - Click **Start** > **Settings** > **Control Panel**
   - Click **Administrative Tools**.
   - Click **Services**.
3. Click **Uninstall APTARE IT Analytics Data Collector in Start Menu/Programs/APTARE IT Analytics Data Collector**
4. Follow the prompts in the uninstall windows.

The uninstaller may not delete the entire Data Collector directory structure. Sometimes new files that were created after the installation are retained along with their parent directories. You may need to manually remove the root install folder (default `C:\Program Files\Aptare`) and its sub-folders after the uninstaller completes.

Chapter 5

Manually starting the Data Collector

This chapter includes the following topics:

Introduction

The installer configures the Data Collector to start automatically, however, it does not actually start it upon completion of the installation because you must first validate the installation.

Follow these steps, for the relevant operating system, to manually start the Data Collector service:

On Windows

The installer configures the Data Collector process as a Service.

To view the Data Collector Status:

1. Click **Start > Settings > Control Panel**
2. Click **Administrative Tools**.
3. Click **Services**. The Microsoft Services dialog is displayed. It should include entries for **Aptare Agent**. Start this service if it is not running.

On Linux

The installer automatically copies the Data Collector “start” and “stop” scripts to the appropriate directory, based on the vendor operating system.

To start the data collector, use the following command:

```
etc/init.d/aptare_agent start
```

Chapter 6

File Analytics Export folder size and folder depth

This chapter includes the following topics:

Extracting File Analytics export folder size

To extract the first-level folder size information from the File Analytics database:

1. At the Linux command prompt, run the following command:

   ```
   java
   -classpath/opt/aptare/portal/WEB-INF/lib/*:/opt/aptare/portal/WEB-INF/classes/
     ccom.aptare.sc.service.fa.FaSubDirectoryReport
   ```

   This generates an output file: **report.csv**

   Output format:

   ```
   Server Name, Volume Name, Folder name, Size in MB, Last Modified
   ```

   Where:

   - Folder name: The root-level folders in the volume
   - Size in MB: Sum of all the file sizes in the folder (recursively)
   - Last Modified: Maximum modified time stamp from within all the files in the folder (recursively)

Specifying the File Analytics folder depth

A parameter, **Dfa.export**, is available to specify folder depth for File Analytics.

- To specify the folder depth for the report summary, add the following parameter when executing the command `-Dfa.export.folderDepth=x` where `"x"` is the depth. By default the depth is set to 1.
- To turn off reporting on parents, add the following parameter when executing the command `-Dfa.export.includeParents=No`. By default reporting on parents is turned on.
- To specify the name of the output file use `-Dfa.export.reportFileName=SomeReportName.csv`. If this parameter is not specified the default output file will be report.csv.

For example:

```
java -classpath
/opt/aptare/portal/WEB-INF/lib/*:/opt/aptare/portal/WEB-INF/classes/
 -Dfa.export.folderDepth=2 -Dfa.export.includeParents=No
com.aptare.sc.service.fa.FaSubDirectoryReport
```

Sample Directory Structures and Results

As an example, the table that follows, uses these directory structures to show the results of different parameter values:

- D1
- D1/SD1
- D1/SD1/SD2
- D2/SD3
- D3

This table illustrates the expected results given the different parameter values:

Table 6-1

fa.export.folder Depth	fa.export.include Parents	Directories Included in Report
0	N/A	D1 D2 D3

Table 6-1 *(continued)*

fa.export.folder Depth	fa.export.include Parents	Directories Included in Report
1	N/A	D1 D1/SD1 D2 D2/SD3 D3
2	No	D1/SD1 D1/SD1/SD2 D2/SD3 D3

Appendix A

Firewall configuration: Default ports

This appendix includes the following topics:

Firewall configuration: Default ports

The following table describes the standard ports used by the Portal servers, the Data Collector servers, and any embedded third-party software products as part of a standard “out-of-the-box” installation.

Table A-1 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Linux Hosts	SSH 22, Telnet 23
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139
Oracle Oracle TNS listener port	1521

Table A-1 Components: Default Ports *(continued)*

Component	Default Ports
Tomcat - Data Receiver Apache connector port and shutdown port for Data Receiver instance of tomcat	8011, 8017
Tomcat - Portal Apache connector port and shutdown port for Portal instance of tomcat	8009, 8015
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445

Table A-2 Storage Vendors: Default Ports

Storage Vendor	Default Ports and Notes
Dell Compellent	1433 SMI-S http (5988) SMI-S https (5989)
Dell EMC Elastic Cloud Storage (ECS)	REST API 80/443
Dell EMC Unity	REST API version 4.3.0 on 443 or 8443
EMC Data Domain Storage	SSH 22
EMC Isilon	SSH 22
EMC Symmetrix	SymCLI over Fibre Channel 2707
EMC VNX (CLARiiON)	NaviCLI 443, 2163, 6389, 6390, 6391, 6392
EMC VNX (Celerra)	XML API 443, 2163, 6389, 6390, 6391, 6392
EMC VPLEX	https TCP 443
EMC XtremIO	REST API https 443
HP 3PAR	22 for CLI
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0

Table A-2 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
Hitachi Block Storage	TCP 2001 For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
Huawei OceanStor Enterprise Storage	8080
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778
INFINIDAT InfiniBox	REST API TCP 80, 443
Microsoft Windows Server	2012 R2, 2016 WMI 135 DCOM TCP/UDP > 1023
NetApp E-Series	SMCLI 2436
NetApp ONTAP 7-Mode and Cluster-Mode	ONTAP API 80/443
Pure Storage FlashArray	REST API https 443
Veritas NetBackup Appliance	1556

Table A-3 Data protection: Default ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023

Table A-3 Data protection: Default ports *(continued)*

Data Protection Vendor	Default Ports and Notes
Dell EMC Networker Backup & Recovery	Port used for Dell EMC NetWorker REST API connection. Default: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
EMC NetWorker	■ NSRADMIN TCP 7937-7940 ■ WMI Proxy range of ports ■ SSH 22 (Linux)
HP Data Protector	5555 WMI ports SSH 22 (Linux)
IBM Spectrum Protect (TSM)	1500
NAKIVO Backup & Replication	Director Web UI port (Default: 4443)
Oracle Recovery Manager (RMAN)	1521
Rubrik Cloud Data Management	REST API 443
Veeam Backup & Replication	9392
Veritas Backup Exec	1433
Veritas NetBackup	1556, 13724 WMI ports SSH 22 (Linux)

Table A-4 Network & Fabrics: Default Ports

Network & Fabrics Vendor	Default Ports and Notes
Brocade Switch	SMI-S 5988/5989
Cisco Switch	SMI-S 5988/5989

Table A-5 Virtualization Vendors: Default Ports

Virtualization Vendor	Default Ports and Notes
IBM VIO	SSH 22, Telnet 23
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESX or ESXi,vCenter,vSphere	vSphere VI SDK https TCP 443

Table A-6 Replication Vendors: Default Ports

Replication Vendor	Default Ports and Notes
NetApp ONTAP 7-Mode	ONTAP API 80/443

Table A-7 Cloud Vendors: Default Ports

Cloud Vendor	Default Ports and Notes
Amazon Web Services	https 443
Microsoft Azure	https 443
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22