APTARE IT Analytics Data Collector Installation Guide for the Cloud

Release 10.4.00

VERITAS™

APTARE IT Analytics Data Collector Installation Guide for the Cloud

Last updated: 2020-09-30

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 Amazon Web Services (AWS)

This chapter includes the following topics:

Pre-Installation Setup for Amazon Web Services (AWS)

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 (Amazon Web Services)

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

Prerequisite Amazon Web Services (AWS) Configurations

The Amazon Web Services Data Collector can collect from the following AWS entities:

- **S3 Bucket (Details and Usage)**- Simple Storage Service (S3) for storage in the cloud
- **EC2 Details** - Elastic Cloud Compute (EC2) for computing services, much like virtual servers
- **Billing Records** - Usage and corresponding charges, by service

For additional information about the type of data that is collected, refer to the Data Collector Policy configuration.

Note: Due to limitations on API request rates, multiple simultaneous processes may interfere with collection. Multiple Amazon Web Services (AWS) Data Collection processes as well as other AWS scripts should not be scheduled for the same period.

The following steps must be taken in Amazon Web Services (AWS) before a Data Collector can gain read-only access to retrieve data.

1. Configure an S3 Bucket to receive billing reports. See "Configure an S3 Bucket to Receive Billing Reports" on page 8.
2. Select cost allocation tags.See "Select Cost Allocation Tags" on page 9.
3. Create an AWS IAM user and generate access keys.See "Create an AWS IAM User" on page 9.
4. Link AWS acccounts for collection of consolidated billing data.See "Link AWS Accounts for Collection of Consolidated Billing Data" on page 11.
5. On the portal, install a collector.
6. On the portal, add a data collector policy.

See "Installation Overview (Amazon Web Services - AWS)" on page 13.

Configure an S3 Bucket to Receive Billing Reports

In Amazon Web Services (AWS), an S3 Bucket (Simple Storage Service Bucket) must be configured to receive billing reports with resources and tags.

1. Create an **S3 bucket** to collect billing records that will be accessed by the AWS Data Collector.
2. In the AWS Billing and Cost Management Preferences, configure the **S3 bucket** to Receive Billing Records.
3. Copy the text from the AWS-provided sample policy.

   This policy sets the permissions that enable AWS billing to create billing record files in the S3 bucket.
4. In the S3 bucket properties, add a bucket policy by pasting the sample into the policy.
5. Verify the S3 bucket.
6. Select cost allocation tags.

   See "Select Cost Allocation Tags" on page 9.

Select Cost Allocation Tags

The Amazon Web Services (AWS) Data Collector requires a Detailed Billing Report with Resources and Tags.

1. Once an S3 bucket is verified, select **Detailed billing report with resources and tags** and save the bucket's preferences.

   This is the only AWS report that is required by the Data Collector.

2. Select Cost Allocation Tags that have been assigned to your AWS resources so that they appear in the billing report and also so that they will be collected by the Data Collector. Tags are user-defined and enable groupings and totals for billing and reporting.

   User-defined tags are used for collection of EC2 and S3 resources. These tags are required for cost allocation reporting of the total cost of EC2 instances and S3 buckets.

   Note: Amazon Web Services generates a report once or more daily, with additions made daily over the month. Therefore, it may take up to 24 hours until a billing records file appears in the S3 bucket that is being collected by the APTARE IT Analytics Data Collector.

   ---

3. Create an AWS IAM user.

   See "Create an AWS IAM User" on page 9.

Create an AWS IAM User

Data collection requires an Amazon Web Services (AWS) Identity and Access Management (IAM) user with restricted permissions. This user must have read-only permission to collect billing records from the S3 bucket and also to access the AWS API methods to retrieve data about EC2 resources and any S3 bucket.

See "Link AWS Accounts for Collection of Consolidated Billing Data" on page 11.

1. In Amazon Web Services IAM Management Console, create an IAM user, specifically for use by the APTARE IT Analytics Data Collector.

   Click **Users > Create New Users >** enter a user name.

   Ensure that Generate an access key for each user is selected.

   This configuration results in the following security credentials: Access Key ID and Secret Access Key.

2. Download the credentials, which you will need later when configuring a Data Collector Policy.

   These credentials are required when configuring the APTARE IT Analytics AWS Data Collector Policy. The access key and secret access key will be used by the Data Collector to make read-only requests to AWS APIs.

3. In the IAM window, select the IAM User you just created and grant permissions by attaching the AWS-supplied ReadOnlyAccess policy.

   This read-only policy allows the Data Collector to retrieve data about EC2 resources and S3 buckets.

4. If you prefer to create a custom AWS policy, for example, to restrict access to buckets with sensitive data.

   See "Example of a Custom AWS Policy for APTARE IT Analytics AWS Collection" on page 10.

5. If you want to link AWS accounts, refer to the following.

   See "Link AWS Accounts for Collection of Consolidated Billing Data" on page 11.

Example of a Custom AWS Policy for APTARE IT Analytics AWS Collection

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::[Billing Bucket Name]",
                "arn:aws:s3:::[Billing Bucket Name]/*"
            ]
        },
        {
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeHosts",
```

```
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "iam:GetAccountAuthorizationDetails",
                "iam:GetUser",
                "iam:ListAccountAliases",
                "s3:GetBucketLocation",
                "s3:GetBucketLifecycleConfiguration",
                "s3:GetBucketLoggingConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketReplicationConfiguration",
                "s3:GetBucketTaggingConfiguration",
                "s3:GetBucketVersioningConfiguration",
                "s3:HeadBucket",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketVersions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Link AWS Accounts for Collection of Consolidated Billing Data

Some large organizations create separate AWS accounts for different cost centers and then link these accounts to a Payer Account. In this case, the billing records for all of these accounts are accumulated in the billing records for the Payer Account. If you want to have a single AWS IAM user to collect these billing records and all other information about EC2 and S3 buckets, you will need to grant the user cross-account API access. By linking accounts, you establish a trust relationship between the accounts.

Create a Role for APTARE IT Analytics Data Collection

1. Log in to the AWS account that is not the Payer Account.
2. In the AWS IAM window, select **Roles**.
3. Enter a role name that identifies it as the role specifically for data collection, such as readOnlyAccessForCollection. The name you enter cannot be changed once the role is created.
4. Select the Role Type: **Role for Cross-Account Access > Provide access between AWS accounts you own**.
5. Establish Trust using the Account ID of the Payer Account, but do not require the MFA.
6. Attach the AWS-supplied ReadOnlyAccess policy.
7. Before creating the role, review the role information to ensure that the following information is correct:
   - **Role Name**: Role named specifically for APTARE IT Analytics data collection.
   - **Trusted Entity**: ID of the Payer Account.
   - **Policy**: ReadOnlyAccess.
8. Copy the **Role ARN** to the clipboard. You will use this copied ARN (Amazon Resource Name) when you add the role to the IAM user.

   See "Add the Role to the IAM User" on page 12.
9. Click **Create Role** to link the accounts.
10. Add the roles to the IAM user.

Add the Role to the IAM User

1. Log in to the AWS Payer Account.
2. In the AWS IAM window, select the User that you created.

   See "Create an AWS IAM User" on page 9.
3. Under the user's permissions, in addition to the ReadOnlyAccess policy that is listed, create an **Inline Policy**.
4. Select Custom Policy and enter a **Policy Name**.
5. Customize permissions by editing the policy, replacing the Resource example (shown in **red** below) with the **Role ARN** that you copied to the clipboard, enclosed in straight quotes.

```
{"Statement":[
  {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource":
"arn:aws:iam::123456789012:role/accessForAPTARECollector"
  }
 ]
}
```

6. The AWS configuration is now complete. Proceed with the Data Collection Configuration.

Installation Overview (Amazon Web Services - AWS)

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

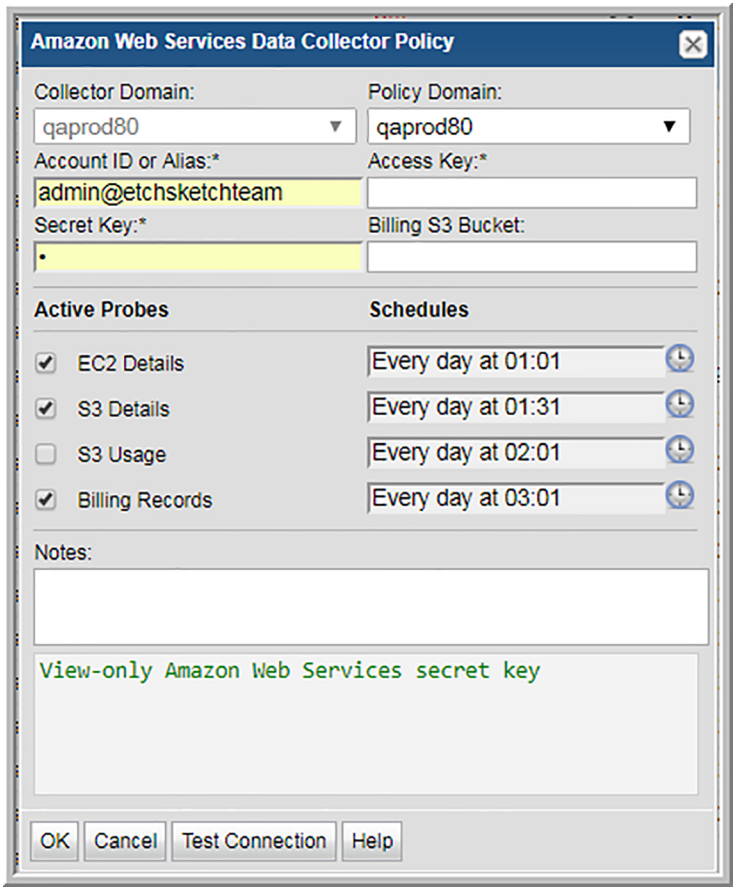
1. Update the Local Hosts file. This enables Portal access.
2. In the Portal, add a Data Collector, if one has not already been created.
3. In the Portal, add the Amazon Web Services Policy Data Collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector installation.

Add an Amazon Web Services (AWS) Policy

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

To add the policy

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



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

Note: Due to limitations on API request rates, multiple simultaneous processes may interfere with collection. Multiple Amazon Web Services (AWS) Data Collection processes as well as other AWS scripts should not be scheduled for the same period.

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name select **My Profile** in the User Account menu.
Account ID or Alias	Enter the AWS account ID number, as shown in the AWS Management Console. This is the ID of the account that pays for the Amazon account. If an account alias has been created, it can be used in lieu of the account ID.
Access Key	Enter the access key ID for the AWS IAM user.
Secret Key	Enter the secret access key for the AWS IAM user.
Billing S3 Bucket	This is the name of the S3 bucket that was created to specifically collect billing records for the APTARE IT Analytics AWS Data Collector policy.

Field	Description
EC2 Details	Collect EC2 instances, EBS volumes, and EBS volume snapshots (and the relationships among this objects), including details such as: ■ EC2 instance: name, tags, region, availability zone, when launched, status, type, virtualization, monitoring configuration. ■ EBS volumes: name, tags, region, availability zone, when created, status, type, size. ■ EBS volume snapshots: name, tags, region, when creation started, progress, status, volume size.
S3 Details	Collect S3 bucket details, such as name, tags, region, owner, when created, and version information.
S3 Usage	Collect S3 bucket usage, such as number of current objects, total size of current objects, number of versions, total size of all versions, number of delete markers, oldest modified current object, and newest modified current object. **Note:** For buckets that have a large number of objects, this collection may take a long time.
Billing Records	Collect all fields from the detailed billing report with resources and tags, such as invoice, resource, payer, linked account, usage type, and costs.

Field	Description
Schedule	**Note:** AWS billing records are updated once or more every 24 hours; therefore, it may take 24 hours after configuring this Data Collector Policy before billing records are available in APTARE IT Analytics. 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.

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to AWS 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 AWS. 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.

Note: For details about the initial data collection period, refer to the following.

Modifying the AWS Collection Period

On the first collection of Amazon Web Services (AWS) billing data, the Data Collector collects one month's worth of data. To override this period, set the AWS_BILLING_LOOKBACK_MONTHS advanced parameter to the number of months of billing history that should be retrieved during the first collection.

Chapter 2

Pre-Installation Setup for OpenStack Ceilometer

This chapter includes the following topics:

Pre-Installation Setup for OpenStack Ceilometer

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 (OpenStack Ceilometer)

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

- 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).

Installation Overview (OpenStack Ceilometer)

As a part of cloud-based data collection, APTARE IT Analytics supports OpenStack Ceilometer, which exposes metrics provided by the various other projects within OpenStack into a common retrieval mechanism for chargeback billing. Note, currently APTARE IT Analytics only captures metrics for OpenStack Compute (Nova). Ceilometer views are available for use in the SQL Template Designer and the Data Collector policy is classified under Cloud.

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 OpenStack Ceilometer data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Adding an OpenStack Ceilometer Data Collector Policy

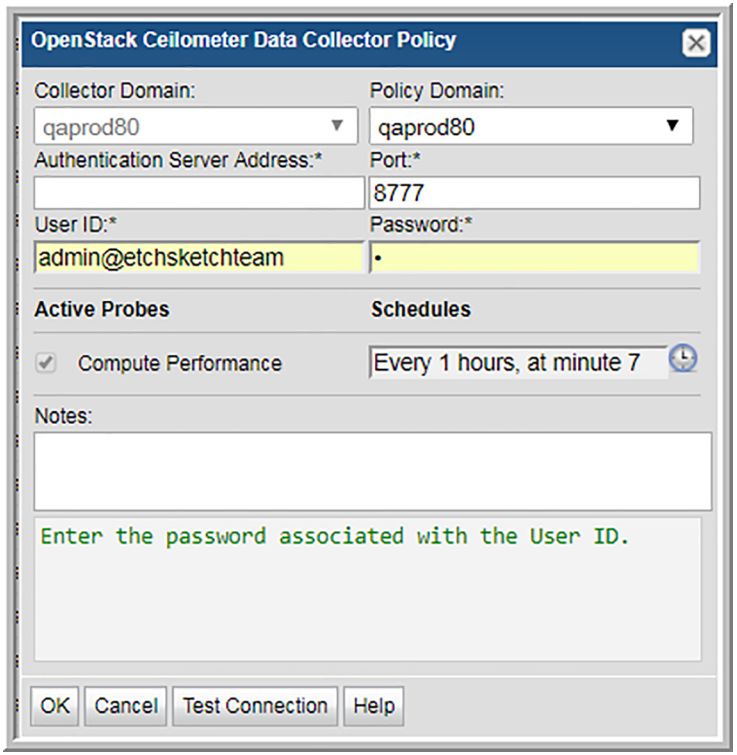
- Before adding the policy: A Data Collector must exist in the Portal, to which you will add Data Collector Policies.
  For specific prerequisites and supported configurations for a specific vendor, see the *Certified Configurations Guide*.
- After adding the policy: For some policies, collections can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

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

To add the policy

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

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



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

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Authentication Server Address*	Enter the IP address of the server with Identity Service and port number in the format: <ip address>:<port_number>. The port number is NOT required if you are running on the default port 35357. However, if you are running on a port other than the default, you must specify the port number.
Port	Ceilometer API service port.
User ID*	Enter a user ID that has access to the tenants/projects. This user must have an Admin role, which has access to all projects.
Password*	Enter the password associated with the User ID.
Compute Performance	Collect metrics based on the length of time since the last collection cycle to a maximum of one hour. One collection per hour is the recommended time period.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. 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 3

Pre-Installation Setup for OpenStack Swift

This chapter includes the following topics:

Pre-Installation Setup for OpenStack Swift

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 (OpenStack Swift)

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

- 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).

Installation Overview (OpenStack Swift)

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 OpenStack Swift data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

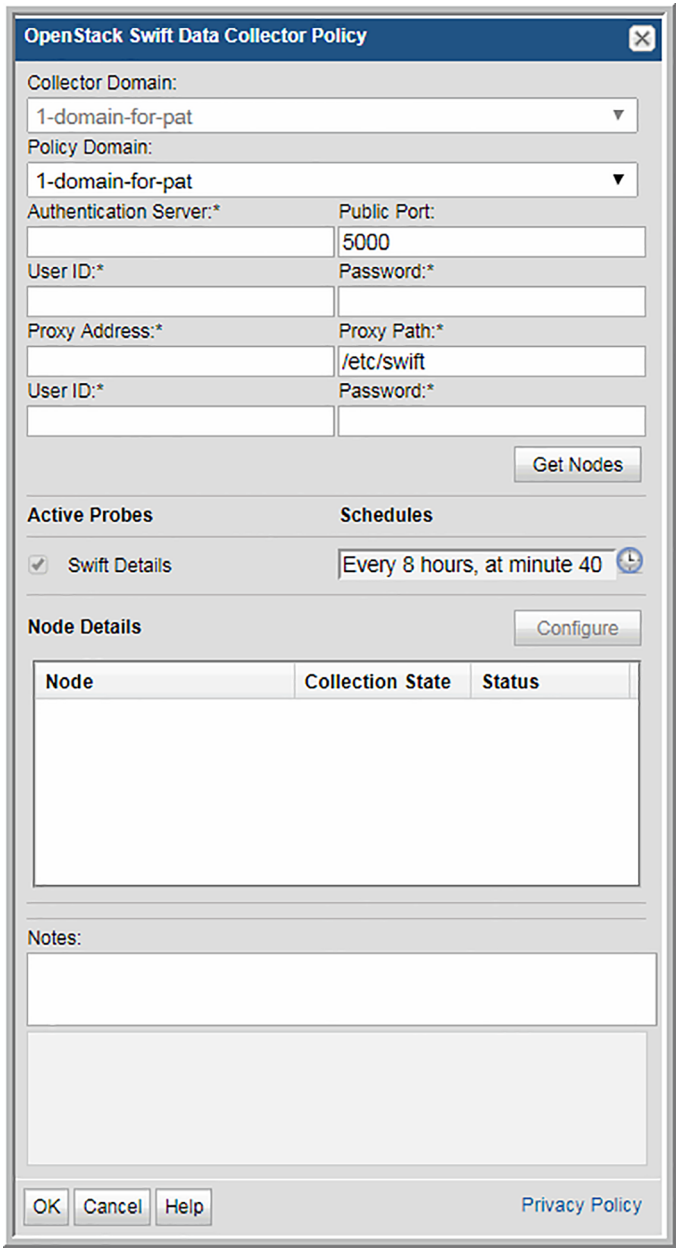
Adding an OpenStack Swift Data Collector Policy

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

To add the policy

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

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



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

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Authentication Server*	Enter the IP address of the Authentication Server and port number in the format: <ip address>:<port_number>. For V1, the port number is NOT required if you are running on the default port. However, if you are running on a port other than the default, you must specify the port number. If using V2 authentication, this port number is the Admin port of the authentication server with the default value of 35757.
Public Port	The public port for V2 authentication. Typically, the default value is 5000.
User ID*	Enter a user ID that has access to the tenants/projects. This user must have an Admin role, which has access to all projects. When you click Get Nodes, the credentials are verified to ensure this is a valid user.
Password*	Enter the password associated with the User ID.
Proxy IP*	Enter an IP address or host name for the OpenStack proxy server. This address/name may be the same as what is configured for the Controller.
Proxy Path*	This path identifies the location of the OpenStack Swift configuration files. Default: /etc/swift
User ID*	Enter a user ID for the Swift Proxy server. This user must have super-user root privileges (sudo, sesudo, and pbrun are supported). When you click Get Nodes, an SSH connection is made to the Proxy server and a list of node IP addresses is returned.
Password*	Enter the password associated with the Proxy's User ID.

Field	Description
Get Nodes	When you click **Get Nodes**, the Authentication Server credentials are verified. Next, an SSH connection is made to the Proxy server to return a list of node IP addresses that will be listed in the table. This process can take up to a minute to complete. When this processing is complete, click the **Details** link to list status and any errors, such as authentication failures, that prevented collection of the list of nodes. **Get Nodes** requires that Agent Services are running.
Configure	When you click **Configure**, the Data Collector policy is saved and the Host Inventory window is displayed so that you can take the following actions before collection can take place for the listed nodes: Manage Credentials, Manage Paths, and Manage Access Control. **Note:** Although a list of nodes has been identified, node collection will not complete successfully until all configurations have been set and collection is activated in the Host Inventory window. The following message may appear in the metadata log file, if configurations are not correct: “Could not find a host for this IP address: <ip_address>”
Active Probes	
Schedule	Click the clock icon to create a schedule. By default, it is collected every 8 hours. 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.
Collection State	Values listed for a storage node represent the state of the main Capacity probe for the host: On, Off, or N/A. After the initial Get Nodes action, the state will always be N/A because the Configure step must occur before data collection can be attempted.
Status	Values listed for a storage node represent the status of all probes for the host: Error, Success, or N/A. After the initial Get Nodes action, the state will always be N/A because the Configure step must occur before data collection can be attempted.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Chapter 4

Pre-Installation Setup for Microsoft Azure

This chapter includes the following topics:

Pre-Installation Setup for Microsoft Azure

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.

As a part of cloud-based data collection, APTARE IT Analytics supports Microsoft Azure. Policies identify backup, storage accounts, billing and VMs for Azure resources. To work with Azure, you need one or more Azure subscriptions. Azure

reports are available for billing, capacity and virtual machines. Azure database views are available in the SQL Template Designer to construct custom reports. Azure enterprise objects are also defined in the Dynamic Template Designer.

Note: The Data Collector only supports Azure resources deployed with the Resource Manager model.

Setting Up Credentials for Microsoft Azure Data Collection

To setup credentials for Azure data collection:

1. See "Install the Azure PowerShell Client on a Windows Computer" on page 32.
2. See "Find Your Tenant and Subscription ID" on page 32.
3. See "Register a New Application for the Data Collector" on page 33.
4. See "Create a Principal and Assign Contributor Role to the Application" on page 34.

Install the Azure PowerShell Client on a Windows Computer

Use the Azure with Windows PowerShell to access the information required for data collection. You must execute Windows PowerShell as administrator.

To install the Azure Client with Windows PowerShell

1 Navigate to http://go.microsoft.com/fwlink/p/?linkid=320376&clcid=0x409

2 Install and at the prompt enter the following to import modules:

```
Install and at the prompt enter the following to import modules:
Install-Module PowerShellGet -Force
Install-Module -Name AzureRM -AllowClobber
Import-Module -Name AzureRM
```

Find Your Tenant and Subscription ID

1. Execute Azure Windows PowerShell as an administrator.
2. Log into your Azure account:

```
Login-AzureRMAccount
```

3. View the Tenant ID and Subscription ID in the output:

```
Get-AzureRmSubscription
```

Register a New Application for the Data Collector

Azure requires a new Application be registered before you can interact with it.

To register a new Application for the Data Collector

You must be logged into your account within Azure Windows PowerShell. The following steps are performed at the Microsoft Azure PowerShell prompt.

1 Set the context using your Tenant ID and Subscription ID by entering:

```
Set-AzureRMContext -SubscriptionId <SUBSCRIPTIONID> -TenantId
<TENANTID>
```

2 Set the Password in a SecureString:

```
$securePwd = ConvertTo-SecureString "<PASSWORD>" -AsPlainText -Force
```

3 Revise the DisplayName, Hostname, and Azure Default Directory. Copy/paste the following at the prompt:

Note: Azure Default Directory can be found in your Azure account under Subscription>Overview.

```
$azureAdApplication = New-AzureRmADApplication -DisplayName
"<DISPLAYNAME>" -HomePage
"https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>" -IdentifierUris
"https://<HOSTNAME>.<AZURE-DEFAULT-DIRECTORY>" -Password
$securePwd -AvailableToOtherTenants $true
```

4 Enter the following to display your application parameters:

```
$azureAdApplication
```

5 Write down the Subscription ID, Tenant ID, Application ID, and the Password you chose. The Application ID is displayed in the output. The Data Collector requires those four parameters.

Create a Principal and Assign Contributor Role to the Application

This step enables the newly registered Application to have access rights to the Subscription.

1. Create a Principal for the Application:

```
New-AzureRmADServicePrincipal -ApplicationId <APPLICATIONID>
```

2. Create a Contributor role:

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor
-ServicePrincipalName <APPLICATIONID>
```

Prerequisites for Adding Data Collectors (Microsoft Azure)

- 64-bit OS. See the *Certified Configurations Guide* for supported operating systems.
- 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.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi-platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- 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.
- 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).
- Requires Port 443.

Installation Overview (Microsoft Azure)

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 Microsoft Azure data collector policy.
4. On the Data Collector Server, install the Data Collector software.
5. Validate the Data Collector Installation.

Adding a Microsoft Azure Data Collector Policy

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

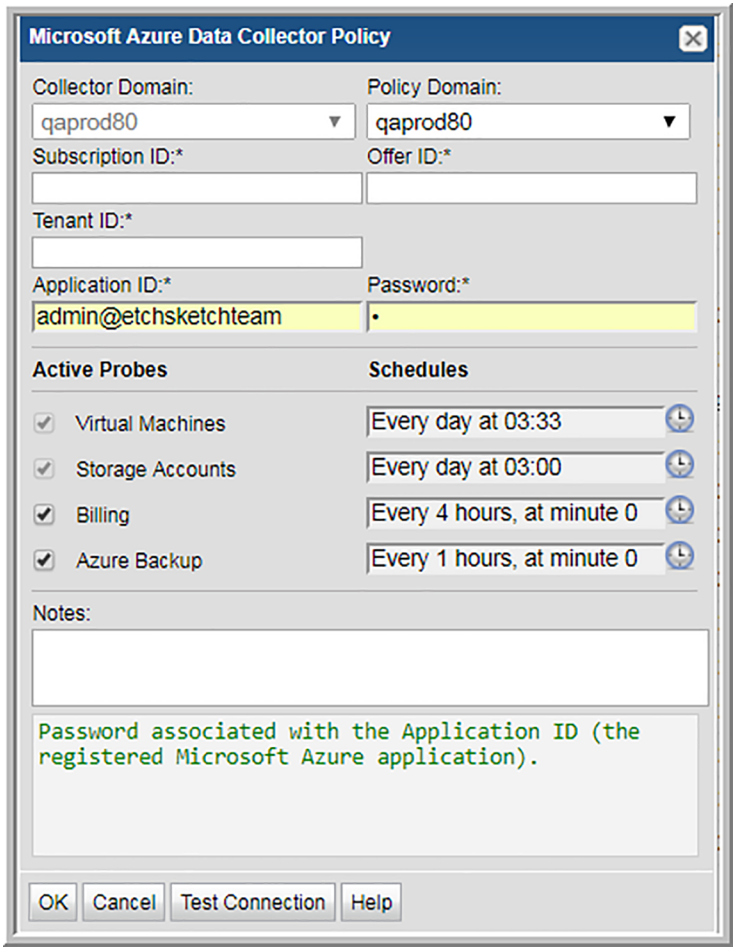
To add the policy

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

2 Search for a Collector if required.

3 Select a Data Collector from the list.

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



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

Field	Description
Collector Domain	The domain of the collector to which the collector backup policy is being added. This is a read-only field. By default, the domain for a new policy will be the same as the domain for the collector. This field is set when you add a collector.
Policy Domain	The Policy Domain is the domain of the policy that is being configured for the Data Collector. The Policy Domain must be set to the same value as the Collector Domain. The domain identifies the top level of your host group hierarchy. All newly discovered hosts are added to the root host group associated with the Policy Domain. Typically, only one Policy Domain will be available in the drop-down list. If you are a Managed Services Provider, each of your customers will have a unique domain with its own host group hierarchy. To find your Domain name, click your login name and select **My Profile** from the menu. Your Domain name is displayed in your profile settings.
Subscription ID*	Subscription ID of your Microsoft Azure Cloud account.
Offer ID*	Offer ID of your Microsoft Azure Cloud Subscription. To locate your Offer ID, log into your Azure portal and the Offer ID is listed as a parameter under your Subscription service.
Tenant ID*	Tenant ID of your Microsoft Azure Cloud account. Also known as the GUID.
Application ID*	Application ID associated with the registered Microsoft Azure application. Azure requires an application for the data collector to interact with it. Refer to See "To register a new Application for the Data Collector" on page 33.
Password*	Password associated with the Application ID (the registered Microsoft Azure application).
Virtual Machines	Select to set a collection schedule for Azure virtual machines.
Storage Accounts	Select to set a collection schedule for Azure storage accounts.
Billing	Select to set a collection schedule for Azure billing.
Azure Backup	Select to set a collection schedule for Azure Backup.
Notes	Enter or edit notes for your data collector policy. The maximum number of characters is 1024. Policy notes are retained along with the policy information for the specific vendor and displayed on the Collector Administration page as a column making them searchable as well.

Field	Description
Test Connection	Test Connection initiates a Data Collector process that attempts to connect to the subsystem using the IP addresses and credentials supplied in the policy. This validation process returns either a success message or a list of specific connection errors. Test Connection requires that Agent Services are running. Several factors affect the response time of the validation request, causing some requests to take longer than others. For example, there could be a delay when connecting to the subsystem. Likewise, there could be a delay when getting the response, due to other processing threads running on the Data Collector. 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

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

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

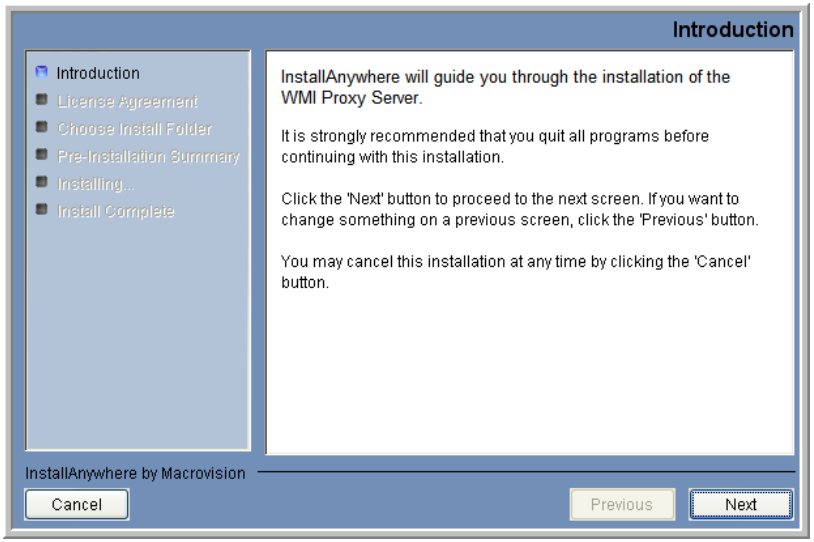
   On Windows:

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

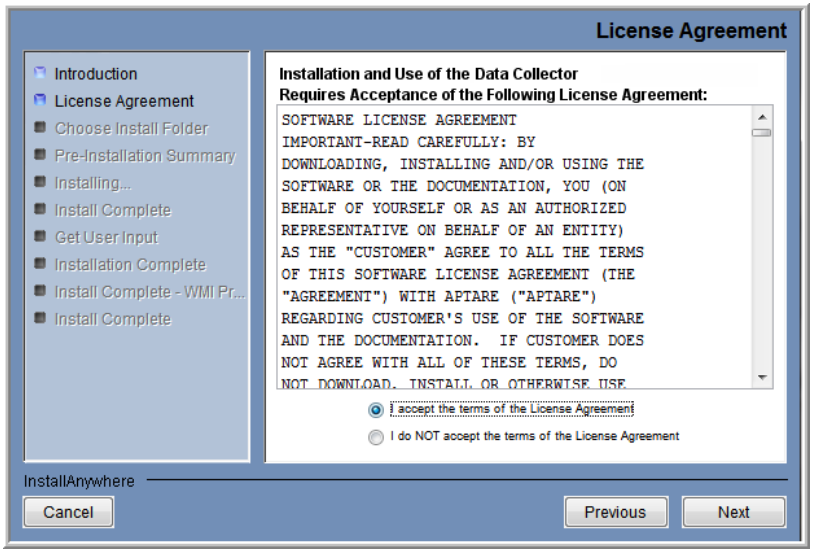
   On Linux:

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

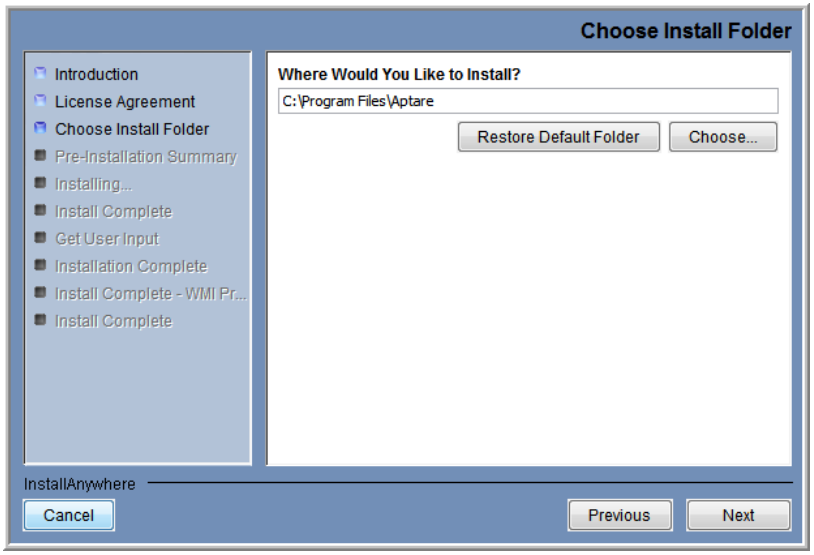
2. Install Anywhere will prepare to install the Data Collector Software. An Introduction dialog box will outline the installation process.



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



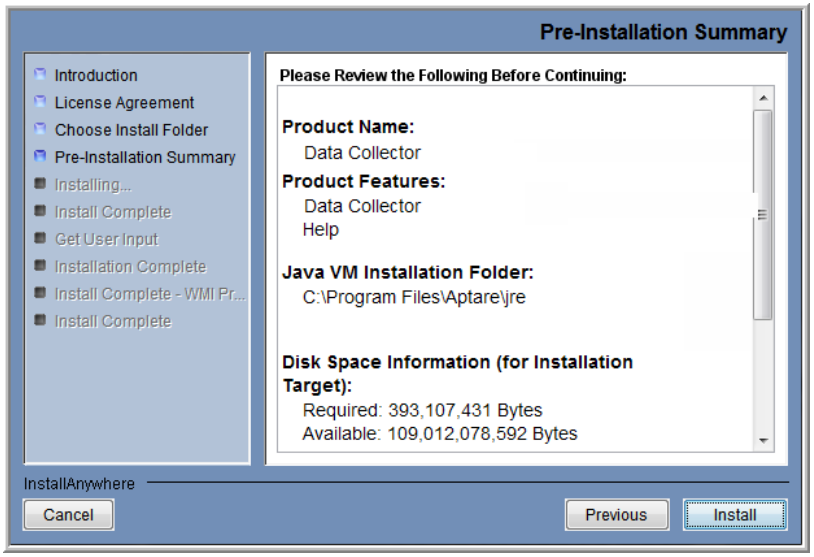
4. Read the agreement.
5. Click on the “I accept the terms of the License Agreement” radio button.
6. Click **Next** to display the window where you will choose the installation folder.



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

   Note: Accepting the default path is recommended.

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



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

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

    When the WMI Proxy installation completes, the 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:

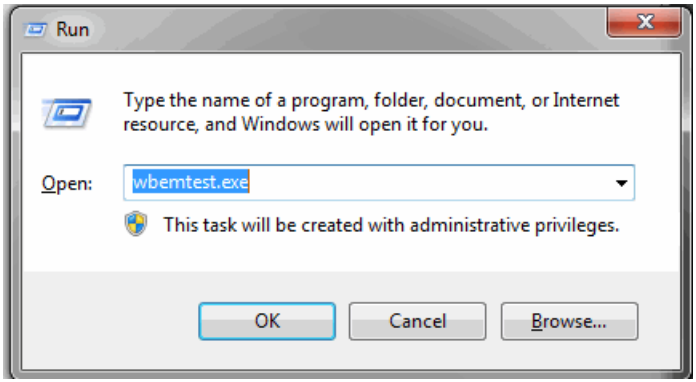
    Startup > Control Panel > Administrative Tools > Services
14. A window will be displayed when the installation is complete.
15. Click **Done** to complete the process.
16. It is recommended that you run the C:\Program Files\Aptare\mbs\bin\checkinstall.bat batch file to validate the Data Collector Installation.

Testing WMI Connectivity

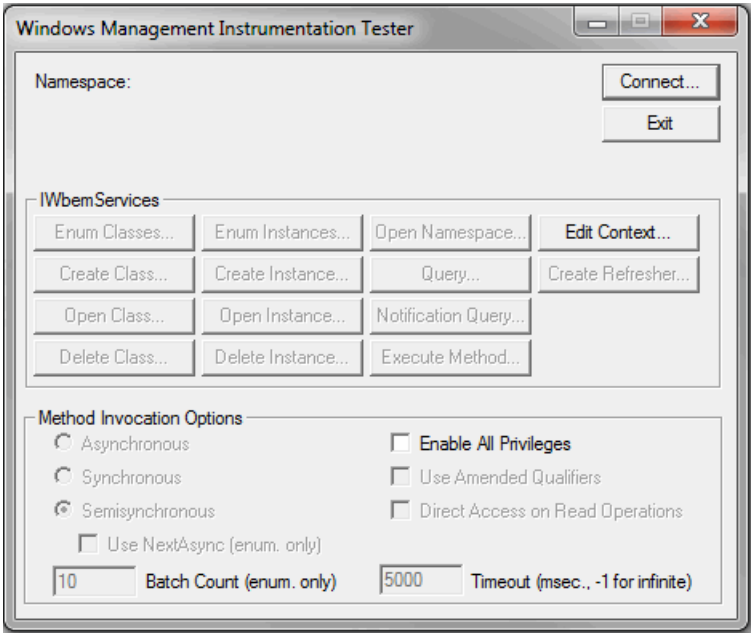
The Windows Management Instrumentation (WMI) Proxy is used by APTARE IT Analytics to collect data from Windows hosts. Should you have connectivity issues, these steps can be taken to test and troubleshoot connectivity.

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**.

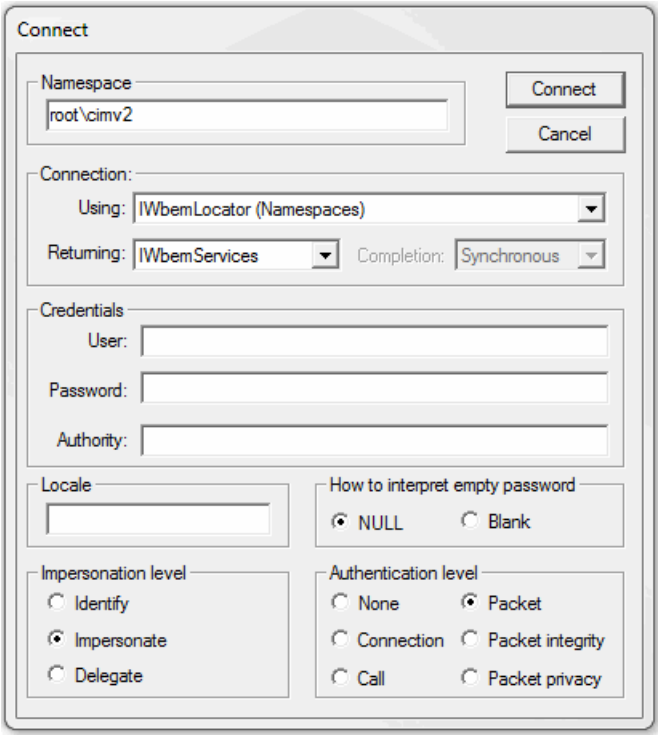


3. In the Windows Management Instrumentation Tester window, click **Connect**.



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 47.

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: UI Deployment " on page 48.

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

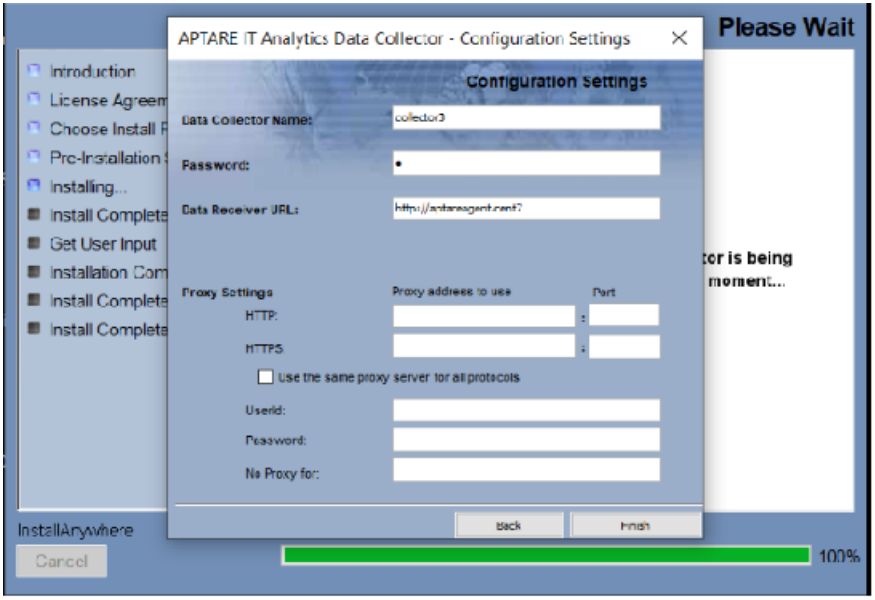
5. At the prompt, save the Data Collector Installer to a directory on the client.
6. Copy the Data Collector Installer to the Data Collector Server where the Data Collector is to be installed.
7. Go to the Data Collector Server and run the installer.
   - **On Windows:**
     Execute sc_datacollector_win_<releaseversion>_<MMDDYYYY>.exe
   - Proceed to the UI deployment.
     See “Installing Data Collector Software: UI Deployment ” on page 48.
   - **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: UI Deployment ” on page 48.
     If the **Data Collector Server** does not have X-Windows:
   - Proceed to the Console Installation instructions.

Installing Data Collector Software: UI Deployment

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.

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.
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: From the Console

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. Web Proxy (HTTP) settings can be configured.

```
Configuration Settings- 4
---------------------------
Connection Settings
Use Proxies? (Y/N) (DEFAULT: N): y
```

```
Configuration Settings - 5
---------------------------
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 - 6
---------------------------
Enter HTTP Proxy Port
(Please leave field empty if there is no Proxy/Firewall)

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

```
Configuration Settings - 7
---------------------------
Enter HTTPs Proxy IP Address
(Please leave field empty if there is no Proxy/Firewall)

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

```
Configuration Settings - 8
---------------------------
Enter HTTPs Proxy Port
```

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

        HTTPs Proxy Port (DEFAULT: ):

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

        Configuration Settings - 9
        --------------------------
        Enter Proxy UserId
        (Please leave field empty if there is no Proxy/Firewall)

        Proxy UserId (DEFAULT: ):

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

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

        Proxy Password:

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

        Configuration Settings - 11
        ---------------------------
        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 6

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 57.

- 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 Checkinstall Utility" on page 59.

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 6-1

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	

Table 6-1 *(continued)*

Vendor Name	Test Connection	On-Demand	CLI Checkinstall Utility
EMC Isilon		x	
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	

Table 6-1 *(continued)*

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

Working with On-Demand Data Collection

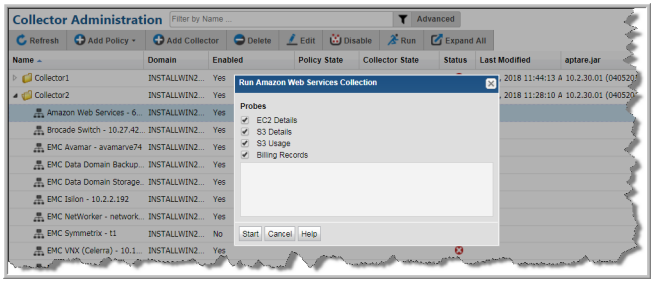
Note: On-Demand data collection is not available for all policies.

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
- 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, providing the policy is one of the specified vendors and the Collector is online.

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 individual probes and servers 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 Checkinstall 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 7

Uninstalling the Data Collector

This chapter includes the following topics:

Uninstall the Data Collector on Linux

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

1. Login to the **Data Collector Server** as **root**.
2. Stop the Data Collector service, using the command appropriate for the operating system.

```
[Data Collector Home Folder]/mbs/bin/aptare_agent stop
```

3. Run the `Uninstall Data Collector Agent` script, located in the following directory:

```
[Data Collector Home Folder]/UninstallerData
```

Uninstall the Data Collector on Windows

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.

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

Chapter 8

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
```

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

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

Storage Vendor	Default Ports and Notes
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0
Hitachi Block Storage	TCP 2001 For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
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

Table A-3 Data Protection: Default Ports *(continued)*

Data Protection Vendor	Default Ports and Notes
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023
Dell EMC Networker Backup & Recovery	Port used for Dell EMC NetWorker REST API connection. Default: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
EMC NetWorker	■ NSRADMIN TCP 7937-7940 ■ WMI Proxy range of ports ■ SSH 22 (Linux)
HP Data Protector	5555 WMI ports SSH 22 (Linux)
IBM Spectrum Protect (TSM)	1500
NAKIVO Backup & Replication	Director Web UI port (Default: 4443)
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