IT Analytics Data Collector Notes and Troubleshooting

Release 11.8

VERITAS
now part of Cohesity

IT Analytics Data Collector Notes and Troubleshooting

Last updated: 2026-07-09

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

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

Cohesity Software Running on Partner Hardware

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

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

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

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

Contents

Chapter 1

Data Collector Troubleshooting

This chapter includes the following topics:

- Host resources: Check the execution of a command on a remote server
- Host resources Data Collection
- Host resources: Collection in stand-alone mode
- Configuring parameters for SSH
- Identifying Windows file system access errors (File Analytics)
- Collect from remote shares (File Analytics)
- Adding a certificate to the Java keystore
- Override default Java Heap memory (XMX) value for Data Collector utilities

Resolving Data Collectors connections issues - Linux specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal.
2. Verify that the key file is generated when the data collector was created.
3. On the portal, perform `wget` to the URL of the data receiver. The expected response is: `Index.html` file.

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify that the data receiver URL resolves via `NSLOOKUP`. If not then specify the data receiver IP address and name to the data collector's host file.

   Verify using `wget` from the data collector that a response back, index.html page, is received. If not then ,verify if the firewall is blocking the access to port 80/443, depending upon configurations.

5. Execute the command `../mbs/bin/updateconfig`. The expected response is: quick return to the command prompt. If not then: verify that the /opt/aptare/datarcvrconf/collectorConfig.global.properties on the portal has the correct URL.
6. Execute the `checkinstall`. If there is initial communication but errors, confirm the data collector name, passcode, and URL are correct.

7. Examine the `<Data Collector home>/mbs/conf/collector.properties` file and verify that the collector name, collector password, and URL were specified appropriately during the installation.
8. Verify that the collector service is started, and **Watchdog** is running.
9. Ensure the understanding that if the portal is running a later upgrade than the GA data collector that upgrade will initiate right after DC connects, and the data collector will go offline for a period during the upgrade.

Resolving Data Collectors connections issues - Windows specific

Perform the following steps to resolves the data connections issues:

1. Verify that the *tomcat-agent* and *apache* services are running on the portal
2. Verify that the key file generated when the data collector was created.
3. On the portal, access a web browser to the URL of the data receiver. Expected response: `Veritas NetBackup IT Analytics Data Receiver`.

   Note: This step bypasses the network and validates that the data receiver is up and running.

4. On the data collector, verify the data receiver URL resolves via `NSLOOKUP`. If not, specify the data receiver IP address and name to the data collector's host file.
5. Verify the response by a browser session on the data collector to the URL. If not, verify if firewall is blocking access to port 80/443, based on the configuration.
6. Execute `<DC HOME>\mbs\bin\updateconfig`. The expected response is, quick return to the command prompt. If not, verify that the **<APTARE PORTAL HOME>datarcvrconf\collectorConfig.global.properties** on the portal has the correct URL.
7. Execute `checkinstall`. If there is initial communication with errors, verify the data collector name, passcode, and URL are correct.
8. Examine the `<Data Collector home>\mbs\conf\collector.properties` file and confirm the collector name, collector password, and URL were keyed in correctly at installation.
9. Verify that the collector service is started and running.

10. Ensure the understanding that if the portal is running a later upgrade than the GA data collector that upgrade will initiate right after DC connects, and the data collector will go offline for a period during the upgrade.

Portal upgrade performance issues

When the entropy of the system is very low, cryptographic functions takes considerable amount of time.

Following are the examples of low entropy:

- while adding new data collector on Portal, takes longer time to generate the key file.
- Upgrade of Portal hangs when upgrading internal objects.
- Aptare agent service takes longer time when started to get the `collectorconfig.xml` from data receiver side.
- `checkinstall.sh` file execution takes longer time than expecting.

These issues are observed on **Linux Platform**.

The following solution is recommended:

Note: Download and install **rng-tools rpm** on the Portal.

For **RHEL/OEL**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `yum install rng-tools` to install the rng-tools.
3. Type `systemctl start rngd` to start the services.
4. Type `systemctl enable rngd` to enable the services.

For **Suse**, execute the following steps to install the **rng-tools** and start the services:

1. Access command prompt.
2. Type `zypper install rng-tools` to install the rng-tools.
3. Type `systemctl start rng-tools` to start the services.
4. Type `systemctl enable rng-tools` to enable the services.

Verify the Data Collector configuration

The Data Collector configuration file contains key information captured during the installation process. If the information was entered incorrectly, this may be the cause of the failure.

To check the configuration file

1 Edit the configuration file.

Windows:

```
edit C:\Program Files\Aptare\mbs\conf\wrapper.conf”
```

Linux:

```
edit /opt/aptare/mbs/bin/startup.sh” and
"/opt/aptare/mbs/bin/updateconfig.sh"
```

2 Verify the values of the following parameters and update them, if necessary.

wrapper.app.parameter.2	Should match the Collector Name you specified when adding a collector policy.
wrapper.app.parameter.3	Should match the Passcode you specified when adding a collector policy.
wrapper.app.parameter.4	For IN-HOUSE installations: http://itanalyticsagent.yourdomain.com where: yourdomain.com has the appropriate value. For third-party HOSTED installations: http://itanalyticsagent.yourdomain.com where: domain.com has the appropriate value.

3 If you changed any of the configuration file parameters, you’ll need to:

- Restart the Data Collector service.
- Re-run the installation validation utility.

Verify Connectivity

To verify that the Data Collector Server can access the Portal Server:

1. Ping the Data Collector URL:

```
ping itanalyticsagent.yourdomain.com
```

2. Verify that the URL has been set up correctly in DNS or in the local hosts file, to resolve to the Portal Server.

Configuring web proxy updates

If you are using a proxy server to connect to the Portal, the Data Collector was configured during installation to use the proxy to connect to the Portal. If the web proxy configuration changes in your environment, the Data Collector must be aware of those changes in order to maintain connectivity. These settings can be found in:

```
/opt/aptare/mbs/conf/collectorsystem.properties
```

Collecting missed events for Veritas Backup Exec

Occasionally, there may be data that was missed by the scheduled Data Collection process. For example, the server may have been unavailable for a period of time. Or, you may want to capture data that was available before you actually installed the Backup Exec Data Collector software.

To capture data from a specific period, use the following utility:

```
buehistoricevents.{sh/bat} {AdministratorDomain} {AdministratorUser}
 {AdministratorPassword} [{Start Date} {End Date}] [verbose]
```

Where:

- Dates need to be in yyyy-mm-dd hh:mm:ss format.
- Specifying verbose will log the Backup Exec commands called to the eventcollector.log file.

Note: If the Start and End Dates are not specified, the utility will capture Events that occurred in the last 24 hours.

Substituting ODBC for JDBC to connect to SQL server for Veritas Backup Exec

The Backup Exec data collector, by default, uses JDBC (Java Database Connectivity) to connect to the SQL Server database. In most cases, this is the preferred mechanism for communicating with the SQL Server. However, in some

instances--for example, TCP/IP is disabled for the SQL Server--JDBC will not be feasible.

In these rare situations, you can configure ODBC (Open Database Connectivity) to connect. The main limitation of this option is that it requires that a DSN (Data Source Name) be set up for each Backup Exec server for which the data collector needs access.

Note: The data collector can be configured to use a mixture of JDBC and ODBC for specific servers.

Use the following steps to turn on ODBC for specific servers:

1. Obtain a copy the **servers.csv** file from the Portal Server (the one that you created to load the Backup Exec servers into the database).
2. Edit **servers.csv**anddelete those servers that you do not want to use ODBC. The format of the entry in the CSV file is:

   ```
   <windows_domain>, <host or ipaddress>, <ipaddress>, , , BKUPEXEC
   ```

3. Save the file to **$APTARE_HOME/mbs/conf** as **odbcservers.conf**on the Data Collector server.
4. Launch the ODBC Data Source Administrator window:

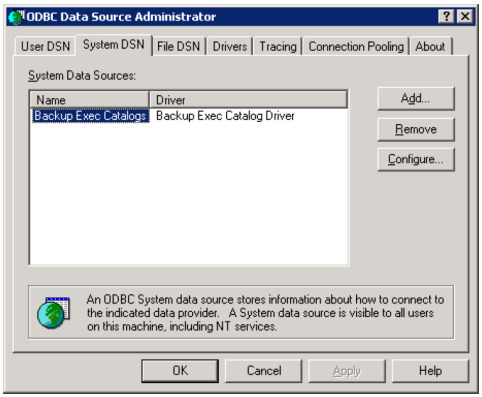
   ```
   Control Panel > Administrative Tools > Data Sources (ODBC)
   ```

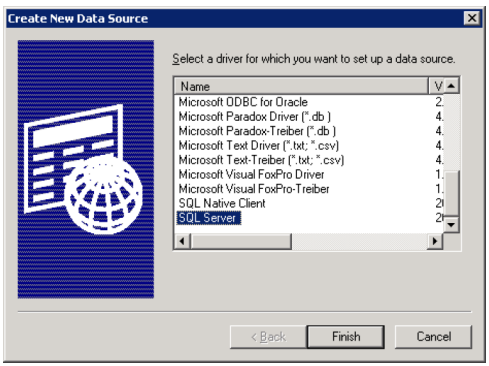
5. Set up the ODBC DSN for each of the Backup Exec servers in **odbcservers.conf**, as depicted in the following sequence of windows.

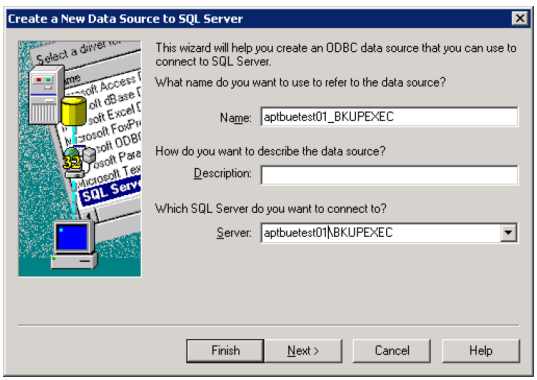
   The DSN needs to be of the form **hostname_BKUPEXEC**, where hostname is the second token in **odbcservers.conf**.

   Note: If the **hostname_BKUPEXEC** form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

   ```
   <windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
   ```



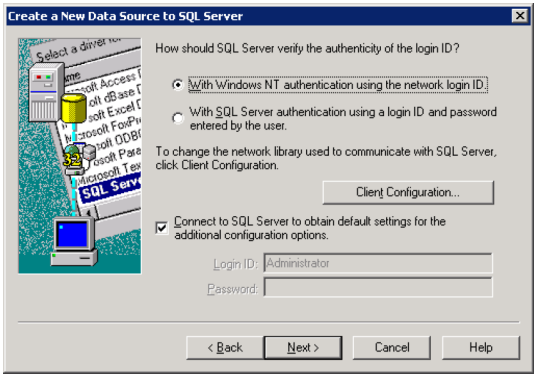


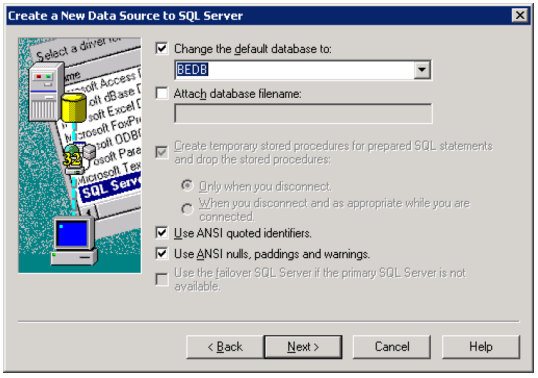


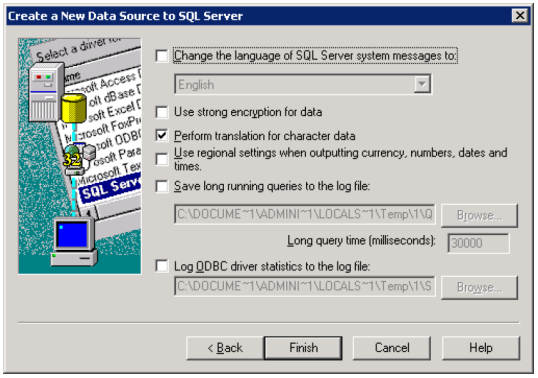
The DSN needs to be of the form hostname_BKUPEXEC, where hostname is the second token in **odbcservers.conf**.

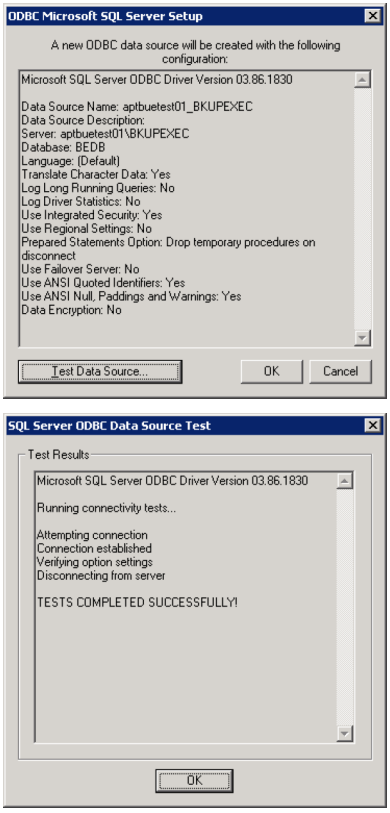
Note: If the **hostname_BKUPEXEC** form does not work (see the third window in the following example), try substituting the IP address for the hostname. If you use the IP address, be sure to make appropriate changes to the CSV file to comply with the following required format:

```
<windows_domain>, <ipaddress>, <ipaddress>, , , BKUPEXEC
```









Useful Data Collection scripts for capacity

The following data collection scripts are available by capacity product. These scripts execute the data collection threads to capture the data. These scripts typically are used only when working with the support and services teams while troubleshooting data collection issues.

Capacity Product	Scripts	Location
EMC VNX	emccheckinstall emcvnxactivedirectorydetails emcvnxarraydetails	Windows: C:\Program Files\Aptare\mbs\bin\emc
EMC Symmetrix	emcsymmetrixarrayperfdetails	Linux: /opt/<home_dir>/mbs/bin/emc

Capacity Product	Scripts	Location
EMC CLARiiON	emcclariionarrayperfdetails	
Hitachi	hitachicheckinstall	Windows:
	hitachiarrayperfdetails	C:\Program Files\Aptare\mbs\bin\hitachi
	hitachiarrayhdtdetails	Linux:
	hitachiarraydetails	/opt/<home_dir>/mbs/bin/hitachi
Host Resources	hostvalidate	Windows:
	hostresourcevalidate	C:\Program Files\Aptare\mbs\bin\hostresources
	hostresourcediscover	Linux:
	hostresourcedetail	/opt/<home_dir>/mbs/bin/hostresources
	hostresourhostresourceasmcollectorcecheckinstall	
HP EVA	hpevaarraydetails	Windows:
		C:\Program Files\Aptare\mbs\bin\hp
		Linux:
		/opt/<home_dir>/mbs/bin/hp
HP 3PAR	hp3parperf	Windows:
	hp3pardetails	C:\Program Files\Aptare\mbs\bin\hp3Par
		Linux:
		/opt/<home_dir>/mbs/bin/hp3Par
IBM XIV	ibmxivarrayperfdetails	Windows:
	ibmxivarraydetails	C:\Program Files\Aptare\mbs\bin\ibm
IBM VIO	ibmviodetail	Linux:
		/opt/<home_dir>/mbs/bin/ibm
IBM SVC	ibmsvcarrayperfdetails	
	ibmsvcarraydetails	
IBM Enterprise Arrays	ibmenterprisearraydetails	

Capacity Product	Scripts	Location
NetApp	netappsnapvaultdetails netappsnapmirrordetails netappcheckinstall netapparrayperfdetails netapparraydetails	Windows: C:\Program Files\Aptare\mbs\bin\netapp Linux: /opt/<home_dir>/mbs/bin/netapp

Host resources troubleshooting

Use the following sequence of steps to determine the source of host resources data collection issues. All commands--except for the SSH commands and the WMI Proxy command--report errors to **metadata.log**. After executing a command, check the **metadata.log** file for error messages. If there is an error noted, correct the problem and then re-issue the command. If the command succeeds, proceed to the next command in this sequence:

1. See "Host resources: Check the status of the WMI proxy server" on page 18.
2. See "Host resources: Post-Installation verification" on page 21.
3. See "Host resources: Check host connectivity using standard SSH" on page 21.
4. See "Host resources: Check host connectivity" on page 23.
5. See "Host resources: Check the execution of a command on a remote server" on page 26.
6. See "Host resources: Collection in stand-alone mode" on page 27.

Host resources: Check the status of the WMI proxy server

Use the following **checkwmiproxy**utility to verify that the WMI Proxy Server is up and running.

The WMI Proxy logs are written to:

```
C:\Program Files\Aptare\WMIProxyServer\logs\aptarewmiserver.log
```

Prerequisites

Either **checkinstall** or **updateconfig** must have been run before running **checkwmiproxy**. Otherwise, **checkwmiproxy** will not have access to the proxy server settings that are saved in the collector configuration file.

Usage

```
checkwmiproxy.[sh|bat] [wmiProxyServer wmiProxyPort remoteWinHost
DomainOfUserId UserId Password "Command"]
```

Where:

wmiProxyServer is the name of the WMI Proxy Server

wmiProxyPort is the proxy's port (default is 1248)

Simple usage

```
checkwmiproxy.[sh|bat]
```

By default, this utility will look for the WMI Proxy Server details in the Host Resources Collector section of the collector configuration file. If it does not find a Host Resources Collector section, the **checkwmiproxy** will terminate with an error and a recommendation to pass explicit parameters, as shown in the usage statement above.

Example 1:

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00
Connection to APTARE WMI Proxy server successfully validated.
```

Example 2: Remote WMI queries

This utility also can be used to execute remote WMI queries, as shown in the following example.

```
[root@aptaredev3 bin]# ./checkwmiproxy.sh 172.16.1.152
Administrator password 172.16.1.152 "select * from
Win32_OperatingSystem"
MetaDataChildThread.init(). Going to initialize.
Will try to connect to the APTARE WMI Proxy at 172.16.1.152:1248
   APTARE WMI Proxy Version: APTAREWMIServer 6.5.01 06/25/07 21:00:00

    Connection to APTARE WMI Proxy server successfully validated.

    APTAREWMIServer Response:
    instance of Win32_OperatingSystem
    {
         BootDevice = "\\Device\\HarddiskVolume1";
         BuildNumber = "3790";
```

```
        BuildType = "Multiprocessor Free";
        Caption = "Microsoft(R) Windows(R) Server 2003, Standard
Edition";
        CodeSet = "1252";
        CountryCode = "1";
        CreationClassName = "Win32_OperatingSystem";
        CSCreationClassName = "Win32_ComputerSystem";
        CSDVersion = "Service Pack 1";
        CSName = "APTARESTGRPT1";
        CurrentTimeZone = -420;
        DataExecutionPrevention_32BitApplications = TRUE;
        DataExecutionPrevention_Available = TRUE;
        DataExecutionPrevention_Drivers = TRUE;
        DataExecutionPrevention_SupportPolicy = 2;
        Debug = FALSE;
        Description = "aptarestgrpt1";
        Distributed = FALSE;
        EncryptionLevel = 168;
        ForegroundApplicationBoost = 2;
        FreePhysicalMemory = "160264";
        FreeSpaceInPagingFiles = "1967860";
        FreeVirtualMemory = "2084508";
        InstallDate = "20070212110938.000000-480";
        LargeSystemCache = 1;
        LastBootUpTime = "20080507115419.343750-420";
        LocalDateTime = "20080520142117.484000-420";
        Locale = "0409";
        Manufacturer = "Microsoft Corporation";
        MaxNumberOfProcesses = 4294967295;
        MaxProcessMemorySize = "2097024";
        Name = "Microsoft Windows Server 2003 R2 Standard
Edition|C:\\WINDOWS|\\Device\\Harddisk0\\Partition1";
        NumberOfLicensedUsers = 10;
        NumberOfProcesses = 90;
        NumberOfUsers = 8;
        Organization = "Aptare";
        OSLanguage = 1033;
        OSProductSuite = 272;
        OSType = 18;
        OtherTypeDescription = "R2";
        PAEEnabled = TRUE;
        Primary = TRUE;
        ProductType = 3;
```

```
        QuantumLength = 0;
        QuantumType = 0;
        RegisteredUser = "Aptare";
        SerialNumber = "69712-OEM-4418173-93136";
        ServicePackMajorVersion = 1;
        ServicePackMinorVersion = 0;
        SizeStoredInPagingFiles = "2039808";
        Status = "OK";
        SuiteMask = 272;
        SystemDevice = "\\Device\\HarddiskVolume1";
        SystemDirectory = "C:\\WINDOWS\\system32";
        SystemDrive = "C:";
        TotalVirtualMemorySize = "3256472";
        TotalVisibleMemorySize = "1363400";
        Version = "5.2.3790";
        WindowsDirectory = "C:\\WINDOWS";
};
```

Host resources: Post-Installation verification

Execute this utility to verify that the host resources installation was successful.

```
hostresourcecheckinstall.{sh|bat}
```

Host resources: Check host connectivity using standard SSH

IT Analytics uses SSH to communicate with devices to run SSH commands. Sometimes, a connectivity issue is simply an incorrect path to a host.

Note: Use the following SSH commands before attempting to collect data.

To check host connectivity using standard SSH:

1. Check that the connection to a Host is successful, using the credentials provided.

   ```
   [user@host ~] ssh <user>@<host> ls
   ```

   Similarly, if you are using Telnet, check your host access via Telnet and run **sudo** commands, as shown in the following step.

2. In access-controlled environments such as **sudo**, a sudo user must be set up. Ensure that the sudo user can run the commands required for the host operating system platform.

   To verify **sudo** access:

   ```
   [user@host ~] ssh <sudouser>@<host> "sudo <command>"
   ```

   If this command results in errors, such as command not found, set up the paths correctly and re-run this command.

   See "Checking Paths for SSH" on page 22.

   on page 11.

3. Paths should be set correctly for the commands to run.

Checking Paths for SSH

If you find messages in the metadata.log file that indicate that some of the commands are not found, then most likely the reason for it is the paths have not been set properly.

IT Analytics uses a non-interactive login shell to execute ssh commands on devices.

1. Check the environment setting for the shell by running the command.

   ```
   [user@host ~] ssh <user>@<host> "env"
   ```

   Check the PATH shown in the output and make sure that it contains the path to all the commands required for IT Analytics for the OS platform of the host.

   Sample PATH for each of the host operating system platforms:

   Linux: /bin:/sbin:/usr/bin:/usr/sbin

   Solaris: /usr/xpg4/bin:/usr/sbin:/usr/bin

   AIX: /usr/bin:/usr/sbin

   HPUX: /usr/bin:/usr/sbin:/opt/fcms/bin:/sbin

   Note: Since Veritas Volume Manager is supported, its path needs to be included in the PATH env variable.

   ---

2. In **sudo** environments, make sure that the sudo path is also in the PATH shown in the output of the above command.

Environment setting for bash users

1. Define all your settings in the file: **~/.bashrc**
2. Make sure that the file **~/.bash_profile** only contains the line: **source ~/.bashrc**

Host resources: Check host connectivity

This utility displays information on the connection status of a list of host names, IP addresses, or a range of IP addresses.

```
chkHostConnection.{sh|bat} HostAddresses userId password
[domain <domain>]
[exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

Table 1-1 Hosts resources and their values.

Host Addresses	**The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.**
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

As a result: for each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} HostAddresses userId password [domain
<domain>] [exclude <excludeHostAddresses>] [wmiserver <wmiserver>]
```

```
[cto <connectTimeout>] [sto socketTimeout>]
[accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, APTAREaix1]
172.16.1.10 ............. SUCCESS
172.16.1.12 ............. SUCCESS
```

Host resources: Check host connectivity using Host Resource Configuration file

This utility provides information on the connection status of a list of Host Addresses that are provided in the Host Resource Configuration file.

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>]
[cto <connectTimeout>] [sto <socketTimeout>]
```

Table 1-2 Hosts resources and their values.

HostResourceFile	The file should be located under the home directory: /mbs/conf/hostresourceconf
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds

Table 1-2 Hosts resources and their values. *(continued)*

HostResourceFile	The file should be located under the home directory: /mbs/conf/hostresourceconf
sto	Socket time-out in milliseconds

Result: For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ..... SUCCESS
172.16.1.12 ..... SUCCESS
```

Usage

```
chkHostConnection.{sh|bat} file <HostResourceFile> [wmiserver
<wmiserver>] [cto <connectTimeout>] [sto <socketTimeout>]
```

HostResourceFile	The file should be located under the home directory: **/mbs/conf/hostresourceconf**
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Result

For each host, the status of the connection is listed.

```
Connectivity Check Server List: [172.16.1.10, 172.16.1.12, aptareaix1]
172.16.1.10 ..... SUCCESS
172.16.1.12 ..... SUCCESS
```

Host resources: Generating host resource configuration files

This utility automatically generates the host resource configuration files and collector configuration file for each valid line provided in the input file.

```
genHostResourceConf.{sh|bat} {CollectorID} {fileName}
```

CollectorID	Identifier name used for the configuration files

filename	File containing the list of parameters--one per line--in the format: `HostAddresses:userId:password:domain:excludeHostAddress` Comments are allowed by using a # at the beginning of the line.
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds

Sample lines in an input file

```
# Sample configuration file to generate Host Resource Conf files
172.16.1.11-13,aptarelab3:root:adminpwd::172.16.1.12-13,apataredlab3
aptareaix1:root:superpwd::
apatrewin2k:samuel:adminpwd:aptarewin2kdomain:
```

Results

- For each valid line, a host resource configuration is created under the home directory: **/mbs/conf/hostresourceconf**. Lines that are not valid are sent to standard output.
- Creates a collector configuration xml file with Meta Data Collector child thread tags for each successfully created host resource configuration file. The file is saved in the home directory under **/mbs/conf**. The collector configuration xml is named in the following format:
  collectorconfig-<date>.xml where date is in DDMMMYYYHHMM format

Host resources: Check the execution of a command on a remote server

This utility provides the output of a command by running it on the specified remote server.

```
remoteExecCommand.{sh|bat} HostAddress [enc] userId password
[domain=<domain>]
[wmiserver=<wmiserver>] [cto=<connectTimeout>] [sto=socketTimeout>]
 [accessCmd=accessControlCommand>]
```

HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma-separated list of them.

userId password	Use the [enc] option to provide encrypted user ID and password arguments.
domain	The Domain for the Windows hosts (only for connecting to a Windows server)
wmiserver	Name of the WMI Proxy Server
cto	Connection time-out in milliseconds
sto	Socket time-out in milliseconds
accessCmd	An access control command such as **sudo**

Example

```
remoteExecCommand.sh 172.16.1.21 myuser mypasswd /usr/bin/df -k
remoteExecCommand.sh 172.16.1.21 myuser mypasswd accessCmd=sudo
cto=10000 /usr/bin/df -k
```

Host resources Data Collection

IT Analytics can collect the following types of host resources:

- Capacity
- Oracle
- SQL Server
- Exchange
- Network
- Processor
- Memory
- Process
- System

Host resources: Collection in stand-alone mode

This utility executes the data collection process against the specific host resources files.

Usage (3 options)

```
hostresourceDetail.{sh|bat} all
hostresourceDetail.{sh|bat} <MetaCollectorID> <HostResourcePolicyName>
hostresourceDetail.{sh|bat} HostAddresses uid=userId pwd=password
[<domain>]
[<excludeHostAddresses>]
```

all	This option runs host resource policies against all Meta Collectors.
MetaCollectorID	The ID used to identify the MetaCollector within the collector configuration xml file.
HostResourcePolicyName	The Policy ID within the Meta Collector ID specified.
HostAddresses	The hosts to verify. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.
domain	The Domain for the Windows hosts
excludeHostAddresses	The hosts to be excluded from the HostAddresses list. It can be hostname, IP address, or range of IP addresses, or a comma separated list of them.

Configuring parameters for SSH

To add any configurable SSH parameters, modify the following scripts:

```
hostResourceDetail.{sh|bat} and aptarecron.{sh|bat}
```

For example, to add the **channelWaitTime**parameter, insert the following after java:

```
-DchannelWaitTime=5000
```

Configure channelWaitTime

If you are experiencing slow connectivity from the Data Collector Server to the Host, update the scripts with this Configurable Parameter. This parameter is specified in milliseconds.

```
-DchannelWaitTime=5000 // This will set the wait time for data from
 the server.
```

Configure singleChannelSession

This will run each command in a separate session.

```
-DsingleChannelSession=true // This will run the each command in a
separate session.
```

Configure sudoWithPassword

In sudo environments, this will send the password without waiting for a prompt.

```
-DsudoWithPassword=true // This will allow running sudo with -S option
 to send the password without waiting for a prompt.
```

Identifying Windows file system access errors (File Analytics)

While profiling the Windows primary file table and file systems, a number of error messages may appear in the **MFT.Aptare_File_Inventory.log** file

These errors actually may require no follow-up actions. Typically, the errors are legitimate, such as a file being locked for exclusive use. Therefore, some files in the C:\Windows\System32 directory will not be profiled.

Example of a Log Error Message:

```
Unable To Access File C:\Windows\System32\Boot. Error 2. Skipping!!!
```

The following table lists System Errors with descriptions.

Table 1-3 Windows file system errors and its description

System Error	Description
2	System cannot find the file specified; This error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.

Table 1-3 Windows file system errors and its description *(continued)*

System Error	Description
3	System cannot find the path specified; This system error occurs when accessing certain files in: C:\Windows\System32. On a Windows 64-bit OS, access is redirected by the filesystem to a 64-bit directory where the files in question do not exist.
5	Access Denied; The file is accessible only to SYSTEM; for example, C:\Windows\System32\LogFiles\WMI\RtBackup
32	Another process has the file opened in exclusive mode; for example, database files used by the SQL server

Collect from remote shares (File Analytics)

The functionality of the host File Analytics probe excludes remote shares that are mounted to the target host, thereby capturing only local files and folders.

To collect from remote shares, an advanced parameter must be configured.

1. In the Portal, navigate to **Admin > Advanced > Parameters**.
2. Click **Add** to add an advanced parameter with a value of **FA_HOST_CAPTURE_REMOTE_SHARES** with a default value of **Y**, along with the target server host name.

Adding a certificate to the Java keystore

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

Keystore file location

Note: For the following commands, if you are not running in the default collector location (/usr/openv/analyticscollector or \Program Files\Veritas\AnalyticsCollector), substitute the appropriate APTARE_HOME in the command path.

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Copy the certificate file (certfile.txt) to the Data Collector. Run the following command to add the certificate:

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -import
 -alias "somealias" -file certfile.txt -keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -import -alias
"somealias" -file certfile.txt -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

When prompted, enter the default password to the keystore:

```
changeit
```

The results will be similar to the following example:

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

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

For Windows Data Collector:

```
C:\Program Files\Veritas\AnalyticsCollector\java\bin\keytool -list
-keystore
C:\Program Files\Veritas\AnalyticsCollector\java\lib\security\cacerts
```

For Linux Data Collector:

```
/usr/openv/analyticscollector/java/bin/keytool -list -keystore
/usr/openv/analyticscollector/java/lib/security/cacerts
```

Sample Linux Output

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
```

```
Your keystore contains 79 entries
digicertassuredidrootca, Apr 16, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
trustcenterclass2caii, Apr 29, 2008, trustedCertEntry,
Certificate fingerprint (SHA1):
AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
.....
```

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

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

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

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

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

Update XMX value in `dc_override_config.bat`

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

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

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

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

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

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

Update XMX value in `dc_override_config.sh`

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

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

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

Chapter 2

Firewall Configuration: Default Ports

This chapter 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 2-1 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139

Table 2-1 Components: Default Ports *(continued)*

Component	Default Ports
Oracle Oracle TNS listener port	1521
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
ZooKeeper	2181 **Note:** IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the local host where IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table 2-2 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 4443

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

Storage Vendor	Default Ports and Notes
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	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
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
Hitachi Vantara All-Flash and Hybrid Flash Storage	Hitachi Ops Center Configuration Manager REST API: 23450 for HTTP and 23451 for HTTPS. HIAA : 22015 for HTTP, and 22016 for HTTPS
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778

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

Storage Vendor	Default Ports and Notes
Microsoft Windows Server	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

Table 2-3 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
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
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

Table 2-4 Network & Fabrics: Default Ports

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

Table 2-5 Virtualization Vendors: Default Ports

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

Table 2-6 Replication Vendors: Default Ports

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

Table 2-7 Cloud Vendors: Default Ports

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

Chapter 3

CRON Expressions for Policy and Report Schedules

This chapter includes the following topics:

CRON expressions for policy probe schedules

Many Data Collector policy configurations require a schedule. Native CRON expressions are supported for fine-tuning a schedule. The CRON expression format for the policy configurations follows strings with five single space-separated time and date fields:

*	*	*	*	*
minutes	hours	day of month	month	day of the week

The following are the general guidelines when using special characters during the CRON expressions.

Table 3-1 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
minutes	0-59 (0 is “on the hour”)

Table 3-1 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)
■ IT Analytics supports a maximum of 80 characters in a CRON expression.	
Special Characters:	
■ A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the seconds and minutes position is not permitted, as this would excessively trigger the probe—every second or minute.	
■ A forward slash (/) can be used to specify intervals.	
■ Use a dash (-) to specify a range.	
■ The CRON expression for the last day of the month, denoted by the letter L, is not supported.	

Table 3-2 Probe Schedule field examples of string with five single space-separated time and date fields

Probe Schedule Examples	Scheduled Run Time
0 14-15 * * 1	On the hour, every Monday, between 2 and 3pm **Note:** A zero in the minutes position denotes the beginning of the hour.
30 9-13 * * 1-5	9:30, 10:30, 11:30, 12:30, and 13:30, Monday through Friday.
0 */2 * * *	To run the probe every 2 hours, put */2 in the hour position. This schedules the probe at 2am, 4am, 6am, 8am, 10am, 12pm, 2pm, and so on.
*/30 * * * *	Every 30 minutes
*/20 9-18 * * *	Every 20 minutes between 9 am and 6 pm
*/30 * * * 1-5	Every 30 minutes, Monday through Friday

Table 3-2 Probe Schedule field examples of string with five single space-separated time and date fields *(continued)*

Probe Schedule Examples	Scheduled Run Time
1 2 * * *	2:01 every day
30 9,11 * * *	9:30 and 11:30 every day

CRON expressions for scheduling reports

Many reports and dashboards may require a email or export schedule. Native CRON expressions are supported for fine-tuning a email or schedule. The format for scheduling reports and dashboard email and exports follows string with six single space-separated time and date fields:

*	*	*	*	*	*
second	minute	hour	day of the month	month	day of the week

The following are the general guidelines when using special characters during the CRON expressions.

Table 3-3 Probe Schedule Allowed Values and Allowed Special Characters

Field	Allowed Values
second	0-59 in string with six single space-separated time and date fields
minutes	0-59 (0 is “on the hour”)
hours	0-23
day of month	1-31
month	1-12
day of week	0-6 (0 is Sunday)
■ IT Analytics supports a maximum of 80 characters in a CRON expression.	
Special Characters:	

Table 3-3 Probe Schedule Allowed Values and Allowed Special Characters *(continued)*

Field	Allowed Values
■ A field may be an asterisk (*), which means the full range - i.e., “first” to “last”. However, a * in the seconds and minutes position is not permitted, as this would excessively trigger the probe—every second or minute.	
■ A forward slash (/) can be used to specify intervals.	
■ Use a dash (-) to specify a range.	
■ Use ? (“no specific value”) when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, to schedule the trigger on a particular day of the month (the 10th), but irrespective of the day-of-the-week that happens to be, specify “10” in the day-of-month field, and “?” in the day-of-week fie	
■ You can use forward slash (/) can be used to specify increments. For example, “0/15” in the seconds field means “the seconds 0, 15, 30, and 45”. And “5/15” in the seconds field means “the seconds 5, 20, 35, and 50”. You can also specify ‘/’ after the ‘’ character - in this case ‘’ is equivalent to having ‘0’ before the ‘/’. ‘1/3’ in the day-of-month field means “fire every 3 days starting on the first day of the month”.	
■ The CRON expression for the last day of the month, denoted by the letter L, is not supported.	

Table 3-4 Report Schedule field examples of string with six single space-separated time and date fields

Report Schedule Examples	Schedule Run Time
0 0 * * * *	the top of every hour of every day.
*/10 * * * * *	every ten seconds.
0 0 8-10 * * *	8, 9 and 10 o'clock of every day.
0 0 6,19 * * *	6:00 AM and 7:00 PM every day.
0 0/30 8-10 * * *	8:00, 8:30, 9:00, 9:30, 10:00 and 10:30 every day.
0 0 0 25 12 ?	every Christmas Day at midnight.
0 15 10 * * ? 2010	run at 10:15 AM every day during the year 2010.

Table 3-4 Report Schedule field examples of string with six single space-separated time and date fields *(continued)*

Report Schedule Examples	Schedule Run Time
0 0 12 1/5 * ?	run at 12 PM (noon) every 5 days every month, starting on the first day of the month.
0 0 0 1W * *	first weekday of the month at midnight
0 11 11 11 11 ?	run every November 11th at 11:11 AM.
0 0-5 14 * * ?	run every minute starting at 2 PM and ending at 2:05 PM, every day.

Chapter 4

Clustering Data Collectors with VCS and Veritas NetBackup (RHEL)

This chapter includes the following topics:

Clustering Data Collectors with VCS and Veritas NetBackup (RHEL)

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

Prerequisites

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

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

Getting started with Data Collector clustering

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

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

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

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

3. Substitute the name of the downloaded ISO image.

   ```
   cd /
   ```

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

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

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

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

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

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

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

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

Configuring the Data Collector

The Data Collector can be configured using:

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

Upgrading a clustered Data Collector

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

Manage Data Collector cluster configuration during NetBackup Upgrade (RHEL)

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

Considerations when Data Collector is pointing to Alta Domain Management

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

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

Chapter 5

Clustering Data Collectors with VCS and Veritas NetBackup (Windows)

This chapter includes the following topics:

Clustering Data Collectors with VCS and Veritas NetBackup (Windows)

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

Prerequisites

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

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

Getting Started with Data Collector Clustering

Data Collector clustering:

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

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

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

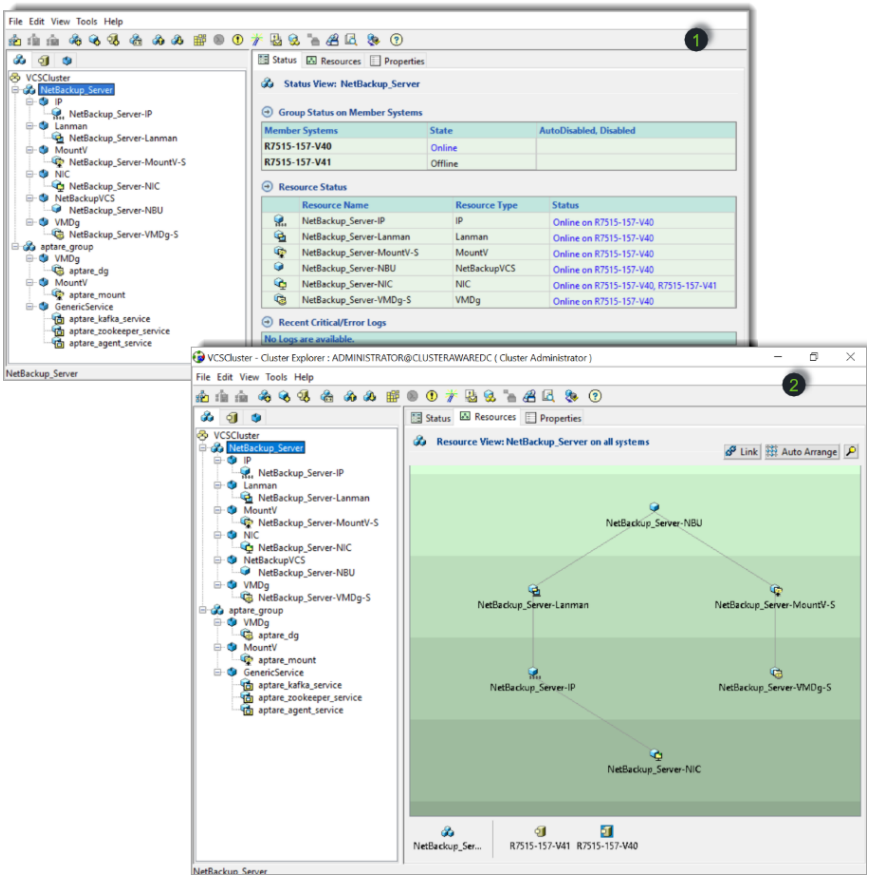
     ```
     silentinstall.cmd /INSTALL_TYPE:INSTALL /REMOVE_NON_OEM_DIR:Y
      /CLUSTER_CONFIG_PATH:<vcsclusterconfig.cmd-file-path>
     ```

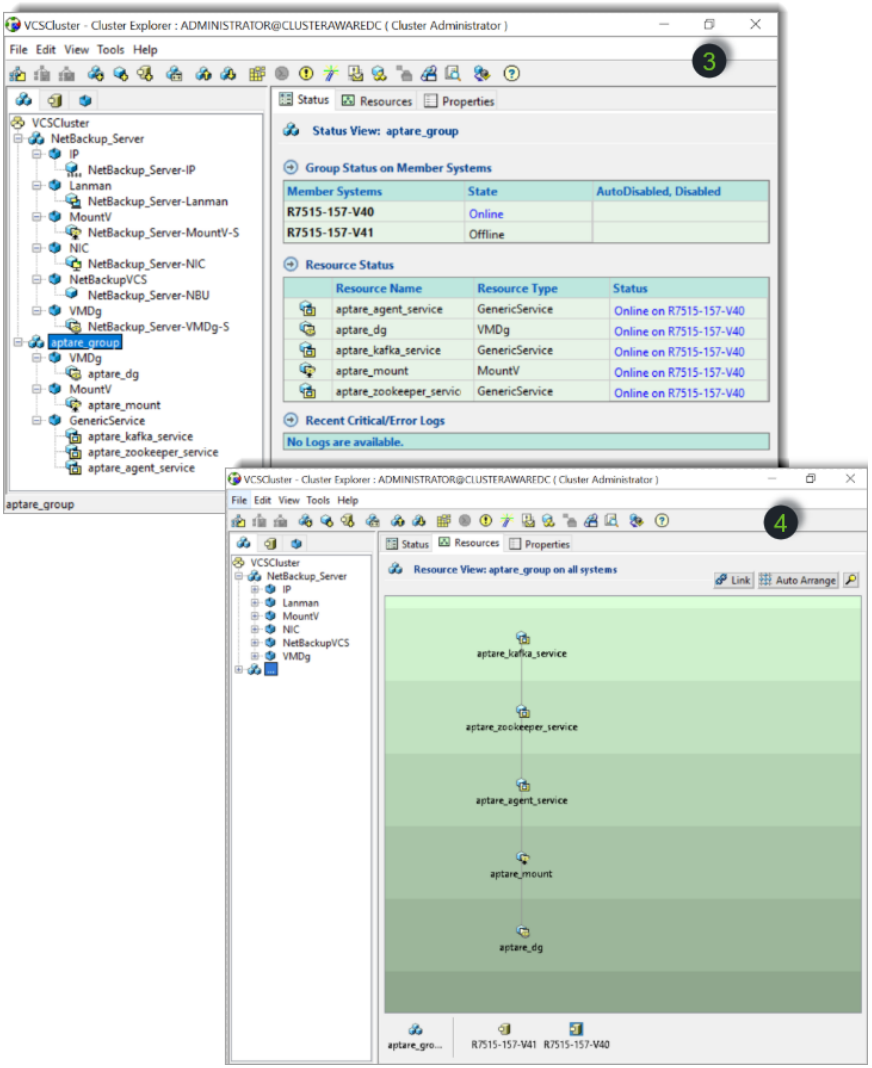
Note: Both the above commands install Data Collector on both active and passive nodes.

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

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

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





Main.cf

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

```
include "types.cf"

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

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

system R7515-157-V40 (
)

system R7515-157-V41 (
)

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

GenericService aptare_kafka_service (
ServiceName = AptareDCKafka
)

GenericService aptare_zookeeper_service (
ServiceName = AptareDCZooKeeper
)

GenericService aptare_agent_service (
ServiceName = aptareagent
)

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

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

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

```
aptare_zookeeper_service requires aptare_agent_service
aptare_agent_service requires aptare_mount

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

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


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


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

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

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

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

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

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

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

// resource dependency tree
//
// group NetBackup_Server
// {
// NetBackupVCS NetBackup_Server-NBU
//     {
//     MountV NetBackup_Server-MountV-S
//         {
//         VMDg NetBackup_Server-VMDg-S
//         }
//     Lanman NetBackup_Server-Lanman
//         {
//         IP NetBackup_Server-IP
//             {
//             NIC NetBackup_Server-NIC
```

```
//                }
//           }
//      }
// }
```

Upgrading a Clustered Data Collector

Irrespective of whether the Data Collector upgrade is done manually or through auto-upgrade, manual intervention is not required. The cluster Data Collector upgrade is taken care for both the paths.

Manage cluster configuration during NetBackup upgrade (Windows)

During NetBackup upgrade, the VCS cluster configurations are removed and recreated. Follow these steps before you upgrade NetBackup:

1. Invoke the script to clean Data Collector cluster configuration:

   ```
   <APTARE_HOME>\mbs\bin\vcscleanclusterconfig.bat
   ```

2. Upgrade NetBackup.
3. Invoke the script to recreate Data Collector cluster configuration:

   ```
   <APTARE_HOME>\mbs\bin\vcscreateclusterconfig.bat
   ```

Chapter 6

Install and configure IT Analytics Data Collector on MSCS environment

This chapter includes the following topics:

Cluster Data Collectors with MSCS on Windows

Prerequisites

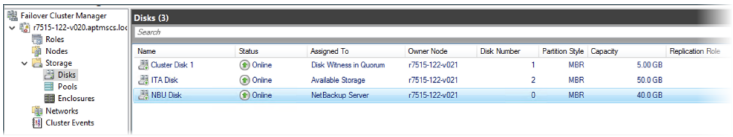
- Microsoft Cluster Server (MSCS) is already provisioned.
- NetBackup primary server is already clustered under MSCS and online on Node1.
- A disk of at-least 100 GB size is attached to all nodes in the cluster - to be used to install IT Analytics Data Collector.

Installing and configuring IT Analytics Data Collector in MSCS

Steps to be performed on Node1:

1. Verify whether a shared disk of minimum size of 100 GB is attached to Node1.
2. Create storage resource for the disk in the cluster. (**Storage** > **Disks** > **Actions** > <Disk name>)

   In the image below **ITA Disk** represents the shared disk for the Data Collector.



3. Get the shared disk (**ITA Disk**) online on Node1 and identify the drive letter.

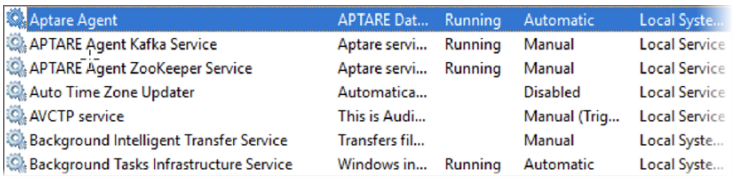
   Note: Ensure the disk has the same drive letter across all cluster nodes.

4. Optional: Add Agent URL to `C:\Windows\System32\drivers\etc\hosts` file. This step is required if the agent URL is not updated on the DNS.

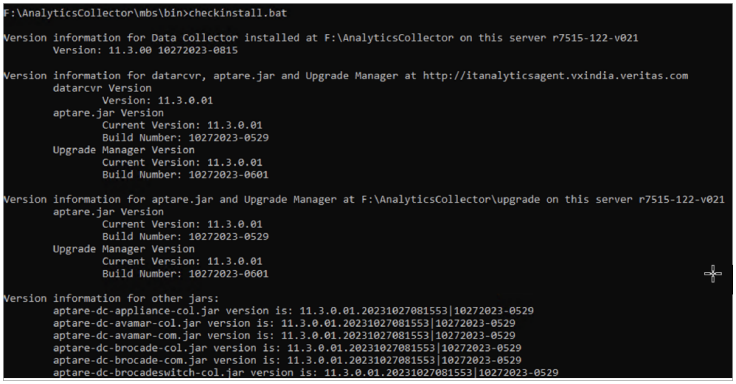
   Example:

   ```
   10.xx.yy.zz   itanalyticsportal.vxindia.veritas.com
   itanalyticsportal
   10.xx.yy.zz itanalyticsagent.vxindia.veritas.com itanalyticsagent
   ```

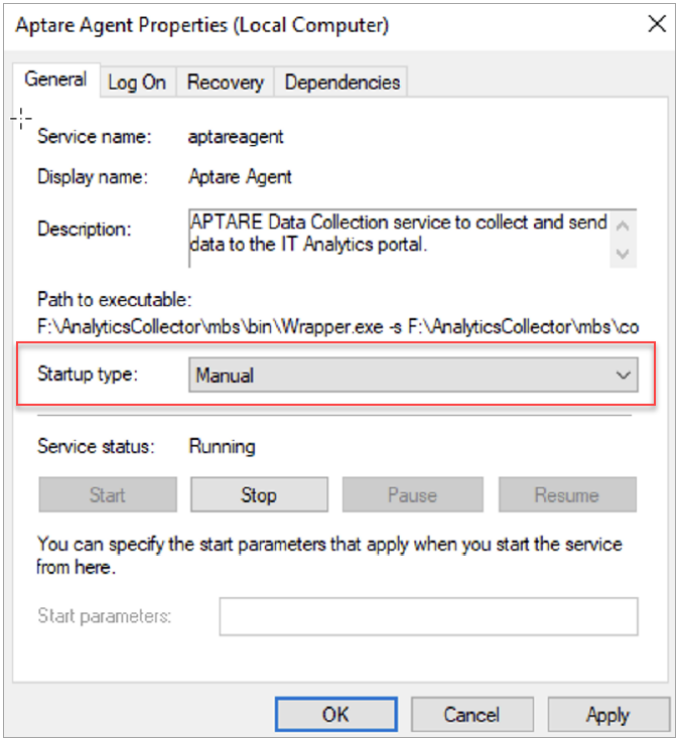
5. Install and Configure IT Analytics Data Collector on new shared drive (**ITA Disk**).
6. Verify that services Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper are created on services panel and are online.



7 Execute `checkinstall.bat` utility and ensure it is returning SUCCESS. The `checkinstall.bat` utility will be available at `<Shared disk drive>\veritas\AnalyticsCollector\mbs\bin`.



8 Change the service type for Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper services from **Automatic** to **Manual** from services panel.



9 Stop the services for Aptare Agent, Aptare Agent Kafka, and Aptare Agent Zookeeper on Node1.

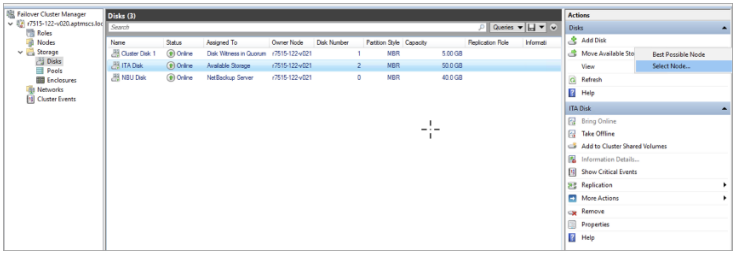
10 Move the storage resource to Node 2 on the cluster. Go to **Failover Cluster Manager** > **Storage** > **Disks** > select the shared disk (**ITA disk**) > on the right side below **Actions** > **Move Available Storage** > **Select Node**> select **Node 2**.

Steps to perform on Node 2:

1 Ensure to move the IT Analytics shared disk (**ITA disk**) from Node 1 to Node 2. Go to **FailOver cluster manager** > **Storage** > **Disks** > select the shared disk (**ITA Disk**).

2 Verify that the shared disk (**ITA disk**) is online and available on the Node 2.

3 On the right side below **Actions**, select **Move Available Storage** > **Select Node** > **Select Node 2**.



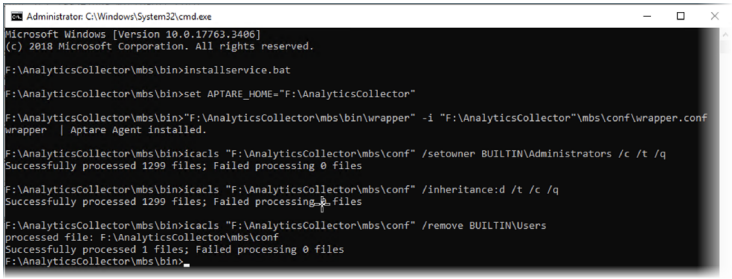
4 Optional: Add Agent URL to `C:\Windows\System32\drivers\etc\hosts` file. This step is required if the agent URL is not updated on the DNS.

Example:

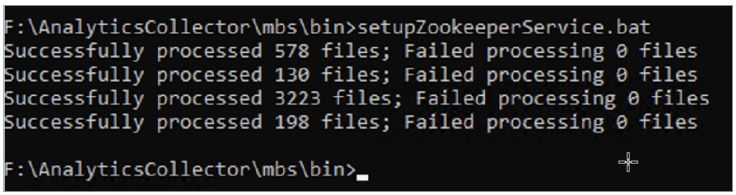
```
10.xx.yy.zz  itanalyticsportal.vxindia.veritas.com
itanalyticsportal
10.xx.yy.zz  itanalyticsagent.vxindia.veritas.com itanalyticsagent
```

5 Create services for Aptare Agent, Aptare Kafka, and Aptare ZooKeeper by executing:

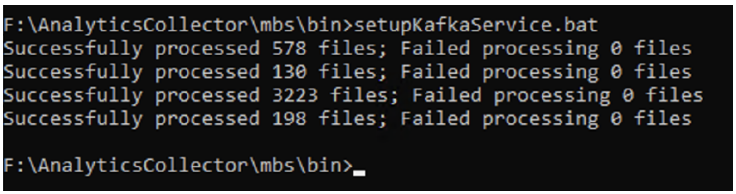
- For Aptare Agent: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\installservice.bat`.



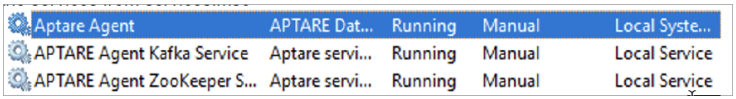
- For APTARE Agent ZooKeeper Service: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\setupZookeeperService.bat`.



- For APTARE Agent Kafka Service: `<Shared disk Drive>:\Veritas\AnalyticsCollector\mbs\bin\setupKafkaService.bat`.



- Change the service type from Automatic to manual from services panel.
- Start the services from `services.msc`.

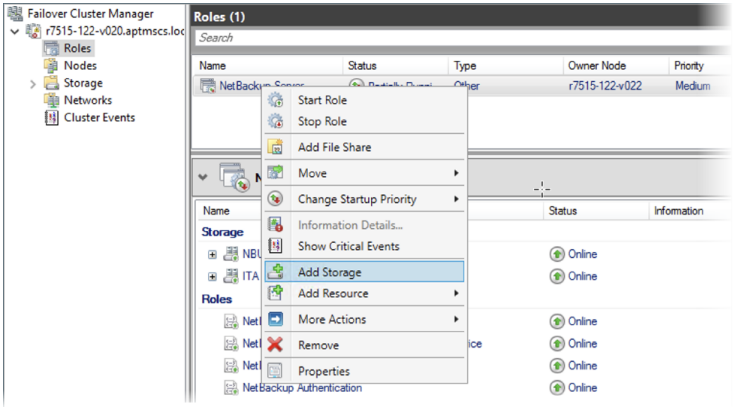


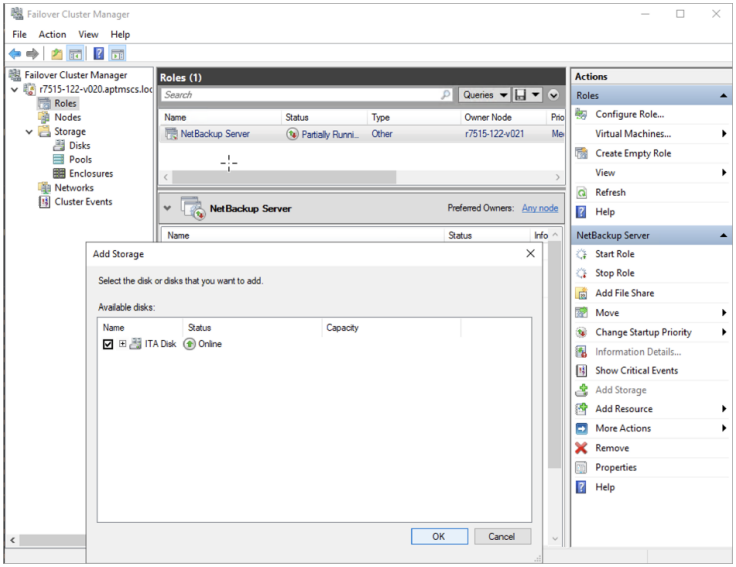
6 Execute `checkinstall` utility and ensure it returns SUCCESS. The `checkinstall.bat` utility will be available at `<Shared disk drive>:/veritas/AnalyticsCollector/mbs/bin`.

7 Stop the services for Aptare Agent, Aptare Agent Kafka, and Aptare Agent ZooKeeper on Node 2.

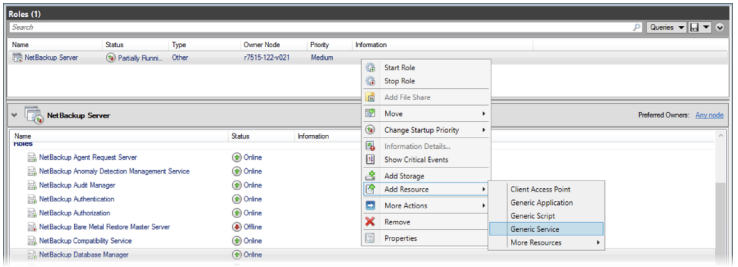
Perform cluster configurations

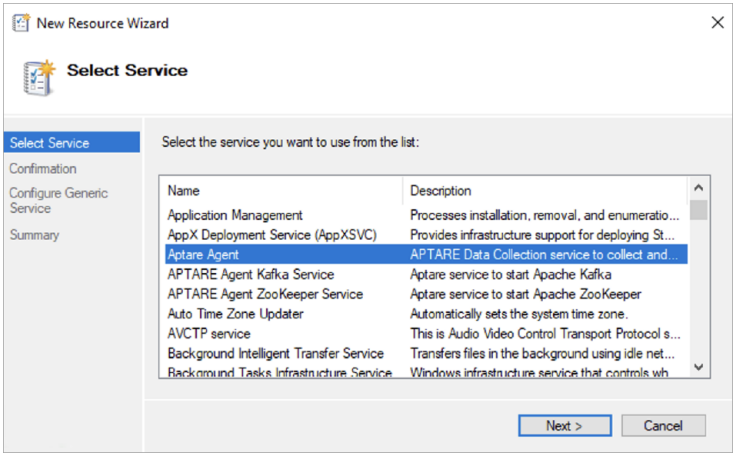
1. Ensure NetBackup Server Role is online on Node 1.
2. Update NetBackup Role:
   - Add IT Analytics shared disk (**ITA Disk**) into NetBackup Server Role from **Failover Cluster Manager**. Open **Failover Cluster Manager** > **Roles** > right-click on **NetBackup Server Role** > **Add Storage** > **ITA Disk** > **OK**.

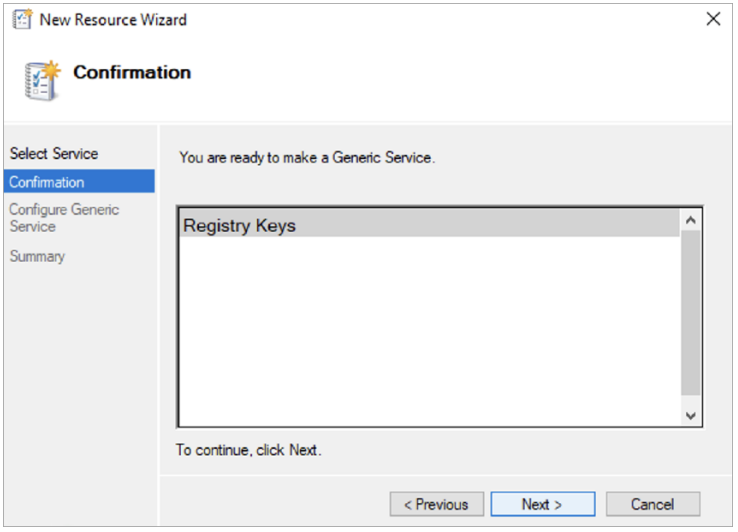


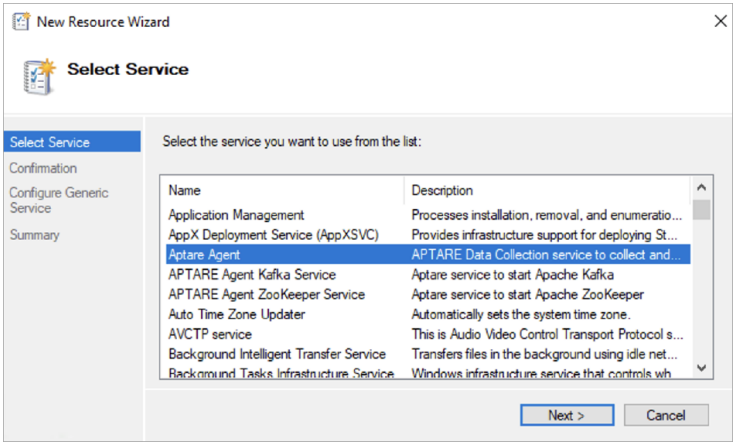


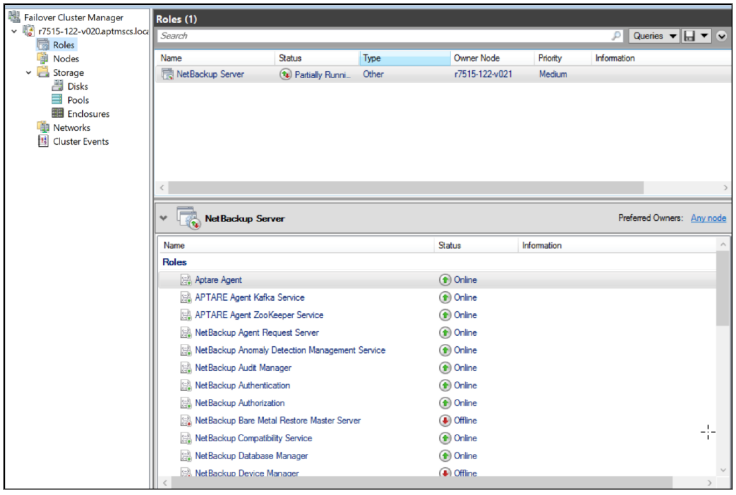
   - Add Roles for each IT Analytics service Aptare Agent, Kafka, and ZooKeeper to it. **Roles** > right-click on **NetBackup Server Role** > **Add Resource** > **Generic services**.


Roles (1)
Search
Queries
Name
Status
Type
Owner Node
Priority
Information
NetBackup Server
Partially Runni...
Other
r7515-122-v021
Medium
Start Role
Stop Role
Add File Share
Move
Change Startup Priority
Information Details...
Show Critical Events
Add Storage
Add Resource
More Actions
Remove
Properties
Client Access Point
Generic Application
Generic Script
Generic Service
More Resources
NetBackup Server
Preferred Owners:
Any node
Name
Status
Information
Roles
NetBackup Agent Request Server
NetBackup Anomaly Detection Management Service
NetBackup Audit Manager
NetBackup Authentication
NetBackup Authorization
NetBackup Bare Metal Restore Master Server
NetBackup Compatibility Service
NetBackup Database Manager
Online
Offline

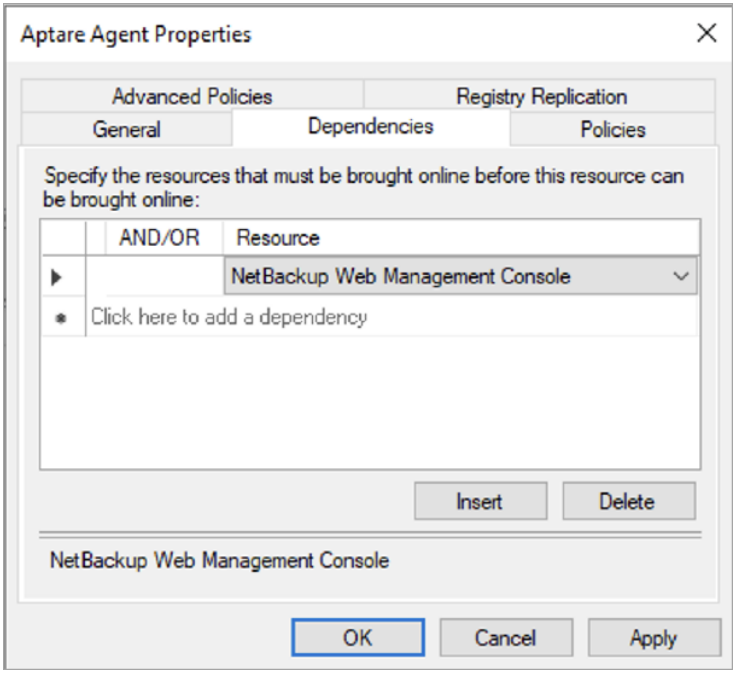

New Resource Wizard
Select Service
Select Service
Confirmation
Configure Generic Service
Summary
Select the service you want to use from the list:
Name
Description
Application Management
Processes installation, removal, and enumeratio...
AppX Deployment Service (AppXSVC)
Provides infrastructure support for deploying St...
Aptare Agent
APTARE Data Collection service to collect and...
APTARE Agent Kafka Service
Aptare service to start Apache Kafka
APTARE Agent ZooKeeper Service
Aptare service to start Apache ZooKeeper
Auto Time Zone Updater
Automatically sets the system time zone.
AVCTP service
This is Audio Video Control Transport Protocol s...
Background Intelligent Transfer Service
Transfers files in the background using idle net...
Background Tasks Infrastructure Service
Windows infrastructure service that controls wh
Next >
Cancel


New Resource Wizard
Confirmation
Select Service
Confirmation
Configure Generic Service
Summary
You are ready to make a Generic Service.
Registry Keys
To continue, click Next.
< Previous
Next >
Cancel

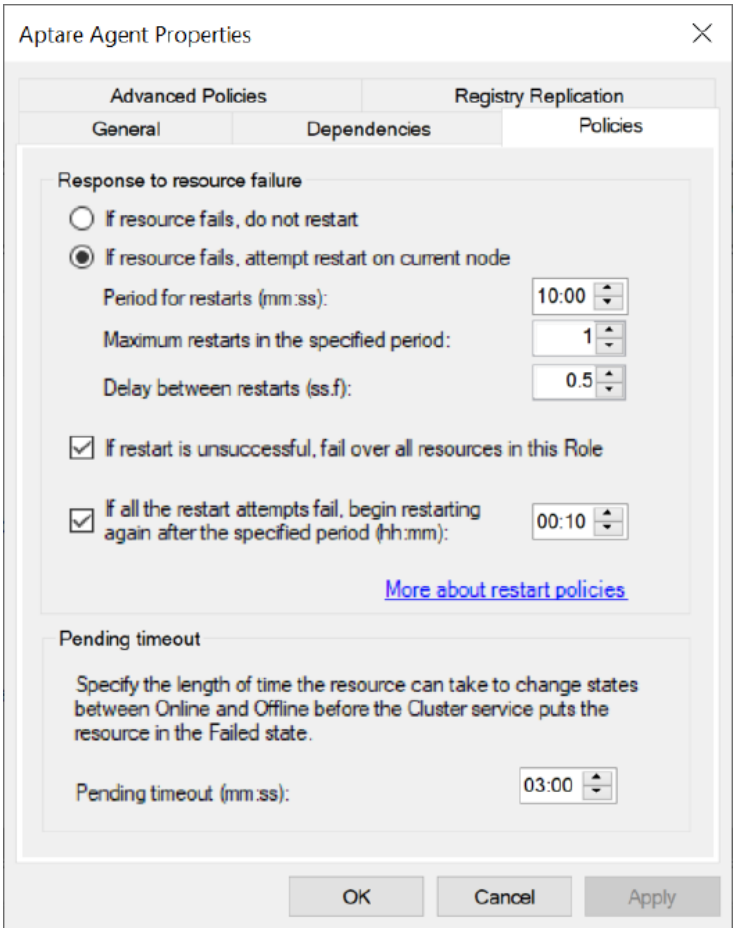




- Create dependency between services Netbackup Web Management Console and Aptare Agent.



- Ensure that the following failure policies are configured as below for Aptare Agent, Kafka, and Zookeeper Roles on NetBackup Role in MSCS cluster. Right-click on **Aptare service** > **Properties** > **Policies**.

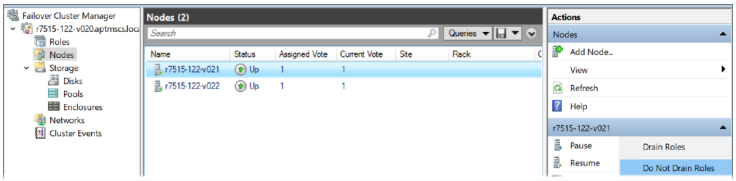


Upgrade IT Analytics Data Collector in MSCS

IT Analytics Data Collector performs auto-upgrade once the Portal is upgraded. As part of auto-upgrade, Data Collector services are stopped, binaries are updated, and then services are started. In order to avoid unwanted service restart/fail-over by MSCS cluster, it is advised to have the following manual interventions.

Before IT Analytics Portal is upgraded, ensure that the following steps are performed on each MSCS clusters where Data Collector is installed.

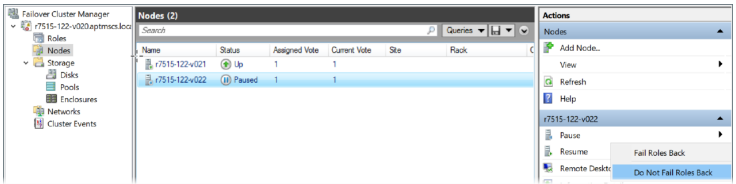
1 Pause the node on which Roles are online with **Do not drain Roles** option in MSCS cluster as given below. This will ensure cluster manager does not initiate failover of Roles when Data Collector upgrade is in progress.



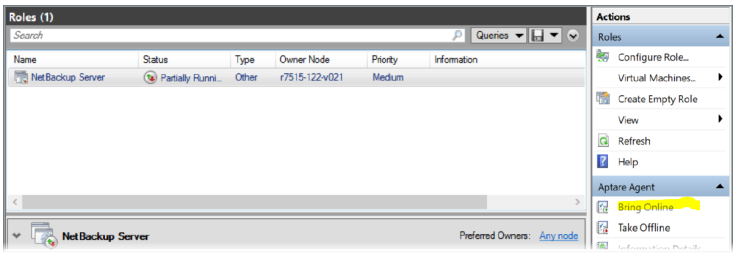
2 Perform Portal upgrade.

3 Once Data Collector contacts the Portal, it will perform auto-upgrade. During the auto-upgrade process, Data Collector services Aptare Agent, Kafka, and Zookeeper will be stopped and cluster detects this and marks the Roles as **Failed**. Once the auto upgrade is successfully completed, services Aptare Agent, Kafka, and ZooKeeper will be started, but the Roles on MSCS for Data Collector will be still marked as **Failed**.

4 Resume the Node that was paused earlier with option "Do not Fail Roles back".



5 For each Aptare Agent, Kafka, and Zookeeper Roles, perform **Bring Online**.



Uninstall IT Analytics Data Collector

1. Delete the Roles for IT Analytics services Aptare Agent, Kafka, and ZooKeeper from MSCS.
2. Identify the node on which "IT Analytics Data Collector" entry is present on the Add/Remove Programs (ARP) on control panel.
3. Fail over the NetBackup Role to other nodes and delete the services from command prompt.

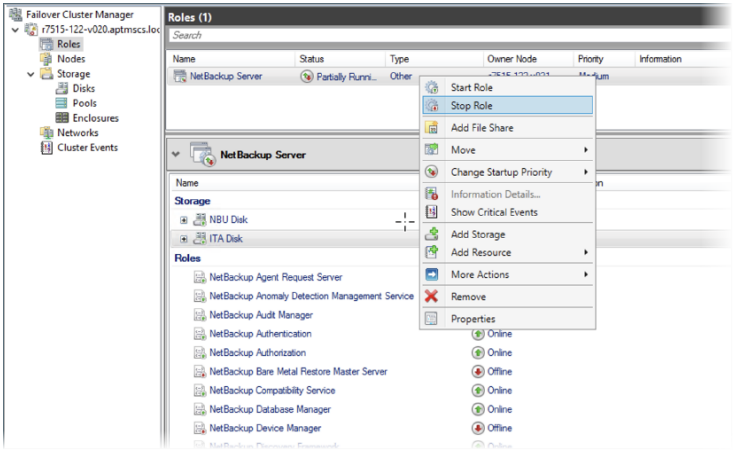
```
#SC DELETE AptareDCKafka
#SC DELETE AptareDCZooKeeper
#SC DELETE AptareAgent
```

4. Failback to the node where ARP entry is present.
5. Perform Uninstall of Data Collector from ARP.

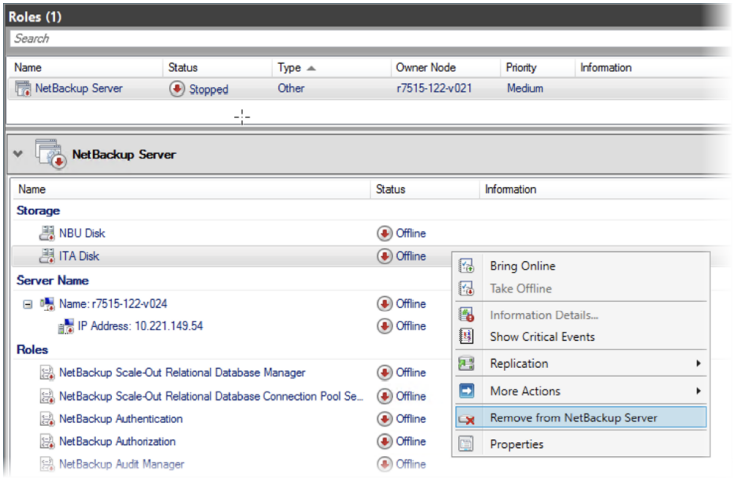
Steps to perform before and after NetBackup upgrade

Steps before upgrading NetBackup:

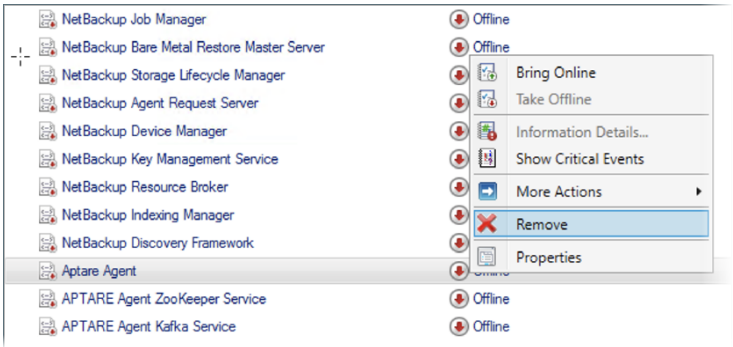
1 Stop the 'NetBackup Server' Role. This will bring down storage disk (both ITA and NetBackup disks) and both NetBackup and Aptare services.



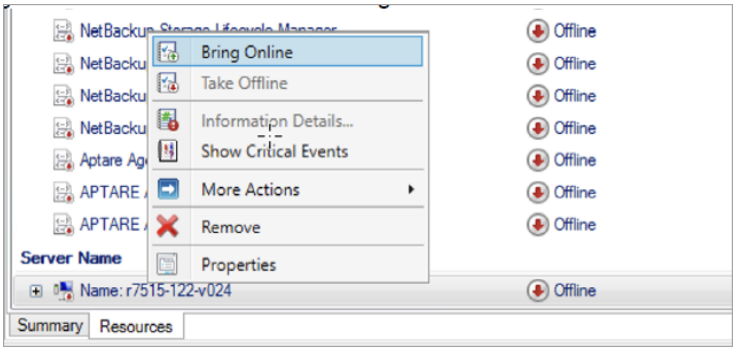
2 Remove IT Analytics disk from NetBackup Server Role.



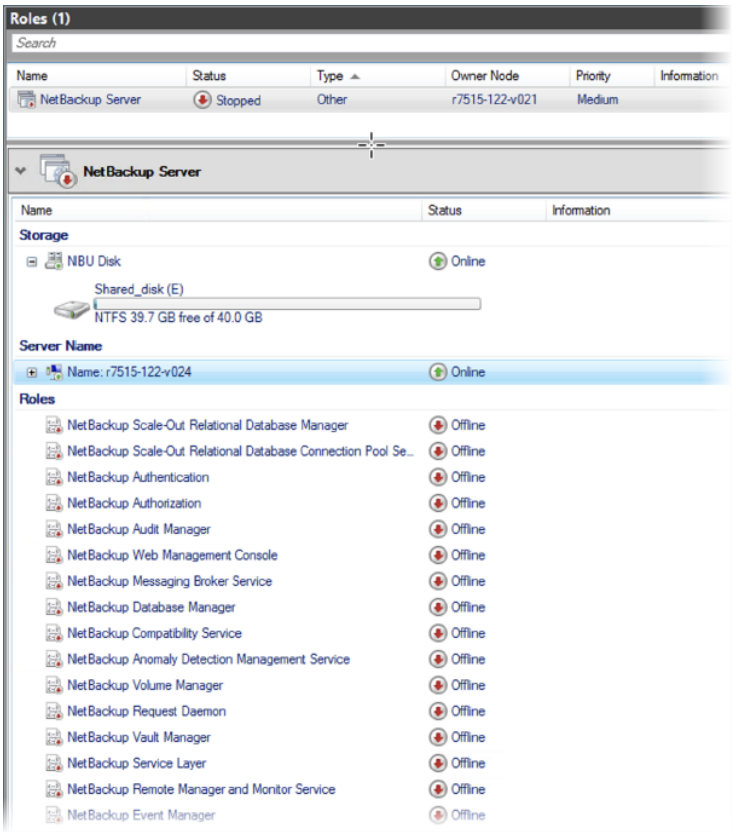
3 Remove Aptare Agent, ZooKeeper and Kafka services from NetBackup Server Role.



4 Bring Server Name online. This will bring NetBackup shared Disk online as well.



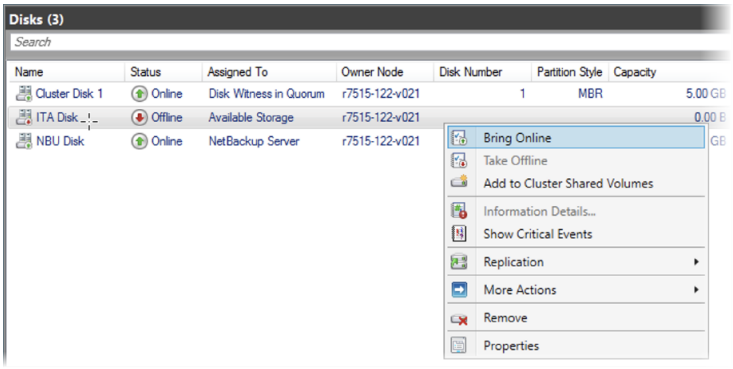
Final look of NetBackup Server Role.



5 Start with NetBackup Upgrade.

Steps after upgrading NetBackup

1 Bring the IT Analytics Disk online. Go to **Disks** > right-click on `ITA Disk` > **Bring online** (on the same node as NetBackup).



2 Now perform the steps from step#2 from section *Perform cluster configurations* .

See “Perform cluster configurations” on page 62.

Chapter 7

Firewall Configuration: Default Ports

This chapter 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 7-1 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139

Table 7-1 Components: Default Ports *(continued)*

Component	Default Ports
Oracle Oracle TNS listener port	1521
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
ZooKeeper	2181 **Note:** IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the local host where IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table 7-2 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 4443

Table 7-2 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
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	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
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
Hitachi Vantara All-Flash and Hybrid Flash Storage	Hitachi Ops Center Configuration Manager REST API: 23450 for HTTP and 23451 for HTTPS. HIAA : 22015 for HTTP, and 22016 for HTTPS
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778

Table 7-2 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
Microsoft Windows Server	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

Table 7-3 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
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
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

Table 7-4 Network & Fabrics: Default Ports

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

Table 7-5 Virtualization Vendors: Default Ports

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

Table 7-6 Replication Vendors: Default Ports

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

Table 7-7 Cloud Vendors: Default Ports

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