

Lab 07: Collecting Data for Backup

In this lab, you configure Data Collection Policies for Veritas Backup Exec and NetBackup. Additionally, you configure NetBackup Discovery and validate Data Collection.

Lab Exercises

This lab includes the following exercises:


- [Exercise A: Adding a Veritas Backup Exec Data Collector Policy](#)
- [Exercise B: Adding a Veritas NetBackup Data Collector Policy](#)
- [Exercise C: Validating Data Collection](#)

⚠ It is recommended to use **Google Chrome** to perform the lab exercises. After launching the lab, zoom out the lab browser window to 80% to fit the APTARE Portal interface and view all the tabs within the window.

Exercise A: Adding a Veritas Backup Exec Data Collector Policy

In this exercise, you add and configure a Data Collector policy for **Veritas Backup Exec**.

Adding Veritas Backup Exec Servers

- ☐ 1. Sign in to the  **console** system using the following credentials.

Username:

Password:

- ☐ 2. Double-click the **Aptare Portal** shortcut, located on the desktop of the **console.example.com** system, to launch the **APTARE IT Analytics Portal**.
- ☐ 3. When the **APTARE IT Analytics Portal** login page is displayed, login using the following credentials.

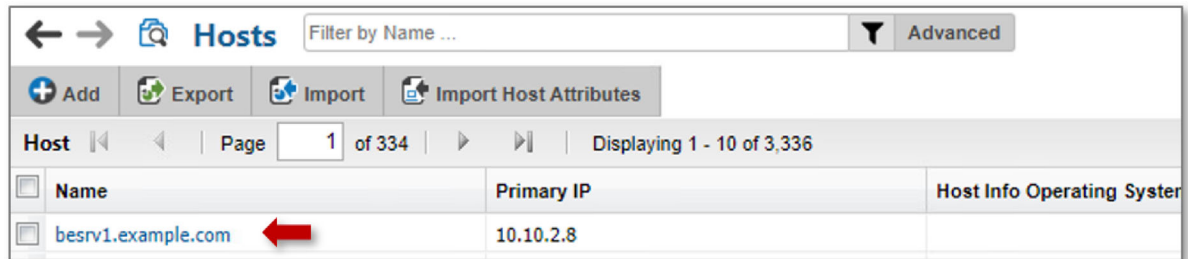
Username

Password

- ☐ 4. If required, In the **APTARE IT Analytics Portal**, click **Inventory** located on the menu bar to access the **Inventory**.
- ☐ 5. In the **Hierarchy Panel**, click **Hosts** and then in the right pane, click the **Go to Inventory List** button.
- ☐ 6. On the **Hosts** page, click **Add**. The **Add Host** dialog box is displayed.
- ☐ 7. In the **Add Host** dialog box, enter the following details and click **OK** to add host, **besrv1.example.com**.

Field	Value
Host Name	<input type="text" value="besrv1.example.com"/>
Internal Host Name	<input type="text" value="besrv1.example.com"/>
IP address	<input type="text" value="10.10.2.8"/>
Backup Type	BackupExec Server

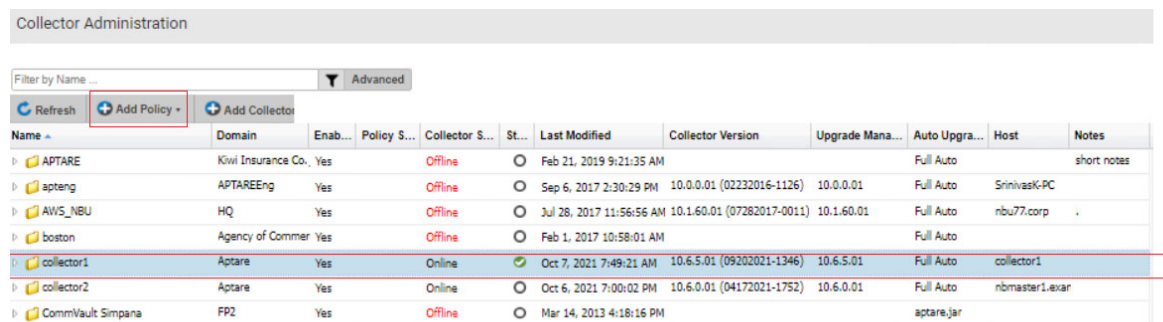
The host, **besrv1.example.com** is now listed on the **Hosts** page as illustrated in the following figure.



Host	Name	Primary IP	Host Info	Operating System
1	besrv1.example.com	10.10.2.8		

Adding a Veritas Backup Exec Data Collector Policy

- ☐ 8. In the **APTARE IT Analytics** Portal, navigate to **Admin > Data Collection > Collector Administration**. A list of currently configured Data Collectors is displayed.
- ☐ 9. Select **collector1** in the list of currently configured Data Collectors and then click **Add Policy** as illustrated in the following figure:




Name	Domain	Enab...	Policy S...	Collector S...	St...	Last Modified	Collector Version	Upgrade Mana...	Auto Upgra...	Host	Notes
APTARE	Kiwi Insurance Co.,	Yes		Offline	○	Feb 21, 2019 9:21:35 AM			Full Auto		short notes
apteng	APTAREEng	Yes		Offline	○	Sep 6, 2017 2:30:29 PM	10.0.0.01 (02232016-1126)	10.0.0.01	Full Auto	SrinivasK-PC	
AWS_NBU	HQ	Yes		Offline	○	Jul 28, 2017 11:56:56 AM	10.1.60.01 (07282017-0011)	10.1.60.01	Full Auto	nbu77.corp	
boston	Agency of Commer	Yes		Offline	○	Feb 1, 2017 10:58:01 AM			Full Auto		
collector1	Aptare	Yes		Online	●	Oct 7, 2021 7:49:21 AM	10.6.5.01 (09202021-1346)	10.6.5.01	Full Auto	collector1	
collector2	Aptare	Yes		Online	○	Oct 6, 2021 7:00:02 PM	10.6.0.01 (04172021-1752)	10.6.0.01	Full Auto	nbmaster1.exar	
CommVault Simpna	FP2	Yes		Offline	○	Mar 14, 2013 4:18:16 PM			aptare.jar		

- ☐ 10. In the resulting menu, select **Veritas Backup Exec** as illustrated in the figure below.

Storage	Data Protection	Network & Fabrics
Dell Compellent	Cohesity DataProtect	Brocade Switch
Dell EMC Elastic Cloud Storage (ECS)	Commvault Simpana	Brocade Zone Alias
Dell EMC Unity	EMC Avamar	Cisco Switch
EMC Data Domain Storage	EMC Data Domain Backup	Cisco Zone Alias
EMC Isilon	EMC NetWorker	Virtualization
EMC Symmetrix	Generic Backup	IBM VIO
EMC VNX (CLARiiON)	HP Data Protector	Microsoft Hyper-V
EMC VNX (Celerra)	IBM Spectrum Protect (TSM)	VMware
EMC VPLEX	Oracle Recovery Manager (RMAN)	File Analytics
EMC XtremIO	Rubrik Cloud Data Management	File Analytics
HP 3PAR	Veeam Backup & Replication	Replication
HP EVA	Veritas Backup Exec	NetApp
HPE Nimble Storage	Veritas NetBackup	Cloud
Hitachi Block Storage		Amazon Web Services
Hitachi Content Platform (HCP)		Microsoft Azure
Hitachi NAS		OpenStack Ceilometer
Huawei OceanStor		OpenStack Swift
IBM Enterprise		
IBM SVC		
IBM XIV		
INFINIDAT InfiniBox		
Microsoft Windows Server		
NetApp		
NetApp Cluster-Mode		
NetApp E-Series		
Pure Storage FlashArray		


- ☐ 11. In the **Veritas Backup Exec Data Collector Policy** dialog box that is displayed, Enter the following details:

Field	Value
Default Windows Domain	<input type="text" value="EXAMPLE"/>
Admin Account	<input type="text" value="Administrator"/>
Password	<input type="text" value="P@ssw0rd"/>
Repeat Password	<input type="text" value="P@ssw0rd"/>

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

- ☐ 12. In the **Veritas Backup Exec Data Collector Policy** dialog box, click **Add**. The **Server** dialog box is displayed.
- ☐ 13. In the **Server** dialog box, enter the following details:


Field	Value
Server name	<input type="text" value="besrv1.example.com"/>
Password	<input type="password" value="P@ssw0rd"/>
Repeat Password	<input type="password" value="P@ssw0rd"/>

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

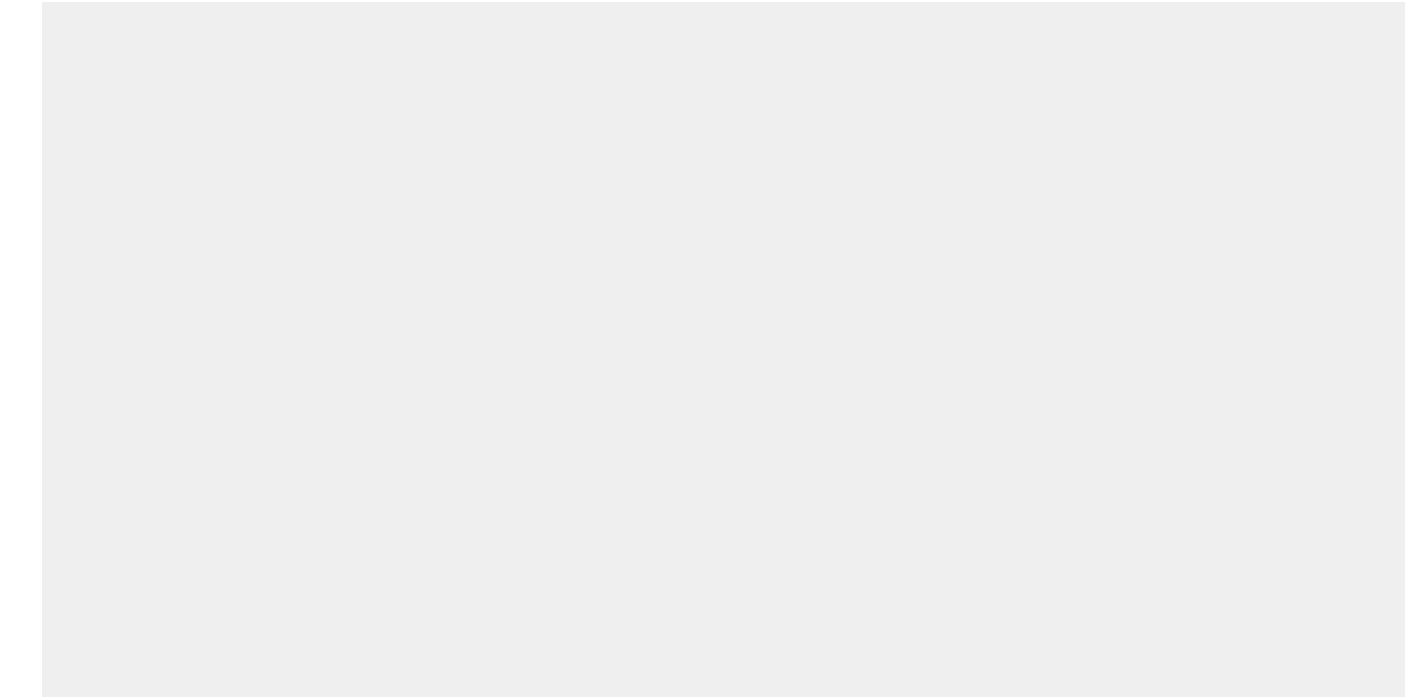
- ☐ 14. Leave all the other fields blank and click **OK**.
- You are returned to the **Veritas Backup Exec Data Collector Policy** dialog box and **besrv1.example.com** is now listed under **Backup Exec servers**.

- ☐ 15. Click **OK** to save the policy.

You are returned to the **Collector Administration** page, note that the new policy is assigned to **collector1**

 You might need to expand **collector1** on the **Collector Administration** page to view a list of assigned policies.

[Go to Lab Exercises](#)





Exercise B: Adding a Veritas NetBackup Data Collector Policy

In this exercise, you add and configure a Data Collector policy for **Veritas NetBackup**. Additionally, you also configure Discovery Policies for **Veritas NetBackup**.

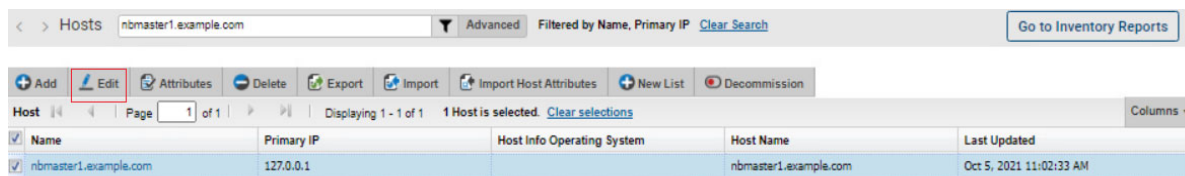
Adding Veritas NetBackup Servers

- ☐ 1. In the **APTARE IT Analytics** Portal, click **Inventory**.
- ☐ 2. If required, in the **Hierarchy Panel**, click **Hosts** to access the **Hosts** management page.
- ☐ 3. On the **Hosts** page, use the **Advanced Filter** located at the top of the **Hosts** page and search for **nbmaster1.example.com**.

 The Data Collector uses NetBackup CLIs to fetch information from the NetBackup Master server and therefore NetBackup binaries should be installed on the Data Collector Server. In this lab environment, the Data Collector Software was installed on the NetBackup Master Server, **nbmaster1.example.com**, this is why **nbmaster1.example.com** is already present in the **Inventory** and is listed on the **Hosts** management page.

 If your search does not return any results, then use the **Refresh** button located on the **Hierarchy Panel** to update the **Inventory**.

- ☐ 4. On the **Hosts** page, select **nbmaster1.example.com** and then click **Edit** as illustrated in the following figure:



- ☐ 5. In the **Edit Host** dialog box that is displayed, make the following changes:

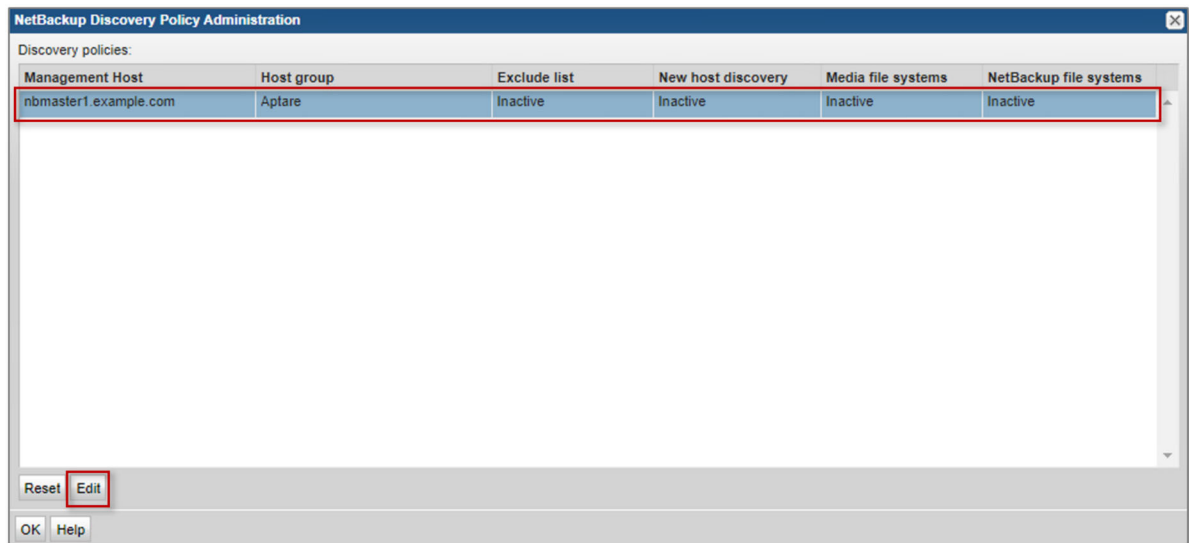
Field	Value
IP address	T 10.10.2.9
Backup Type	NetBackup Master
Time Zones	(UTC-5:00) Eastern Time (US & Canada)

- ☐ 6. In the **Edit Host** dialog box, click **OK** to save your changes and return to the **Hosts** management page.

Configuring Discovery Policies for Veritas NetBackup

- ☐ 7. In the **APTARE IT Analytics** Portal, navigate to **Admin > Reports > NetBackup Discovery**. The **NetBackup Discovery Policy Administration** window is displayed.

- ☐ 8. In the **NetBackup Discovery Policy Administration** window, select **nbmaster1.example.com** and click **Edit** as illustrated in the following figure.



- ☐ 9. In the **Edit NetBackup Policy** dialog box, add the following hosts in the **Host exclude list**.
- T 10.10.2.5,10.10.2.10,10.10.2.20,10.10.2.22,10.10.2.24**
- ☐ 10. Set the **Start Window** for the **New Host discovery**, **Media host file systems**, and **NetBackup host file system** discovery types to **T * * * * ***. This is equal to specifying a **24x7** start window.

The **Start Window** is five asterisks each separated by a space and without the leading and trailing quotes.

When configuring the start window, you need to consider the wake-up period of the Discovery processes. If you configure a window of **"* 2-3 1 * *"** (that is, between 2 and 3 am on the first day of each month) for the New Server Discovery process, the process might run twice if it wakes up at 2 am, takes 15 minutes to execute, sleeps for 40 minutes, then wakes up again at 2:55 am. Since the start window is still active at 2:55 am, it will run again.

- ☐ 11. Click **Add** to add an **IP address range** then enter **T 10.10.2.2** in the **IP address range** field and check both the **Active** and **Probe** checkboxes.
- ☐ 12. Click **Add** to add a second **IP address range** then enter **T 10.10.2.3** in the **IP address range** field and check both the **Active** and **Probe** check boxes.

The **IP address range** field supports enter either a single IP address or an IP address range. An IP range is in the format **nnn-nnn** (For example: 172.16.100-110.1-255 covers 11*255 = 2805 IP addresses). Multiple ranges can be added and each range can be independently activated or deactivated via the active check box.

- ☐ 13. Select the **Active** check box available under the **Media host file systems** and the **NetBackup host file system** discovery types to activate these discovery types.

The figure below illustrates the above listed configuration.

Edit NetBackup Policy

Host exclude list: (comma separated)
10.10.2.5,10.10.2.10,10.10.2.20,10.10.2.22,10.10.2.24

New Host discovery:
Last run date: Last run status: Start window: *****
see help for syntax

Active	IP address range	Probe
<input checked="" type="checkbox"/>	10.10.2.2	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	10.10.2.3	<input checked="" type="checkbox"/>

Add Delete

Media host file systems:
Last run date: Last run status: Start window: ***** Active: ☒
see help for syntax
Discover all media hosts associated with master host.

NetBackup host file systems:
Last run date: Last run status: Start window: ***** Active: ☒
see help for syntax
Discover all clients in NetBackup policies associated with master host.

OK Cancel Help

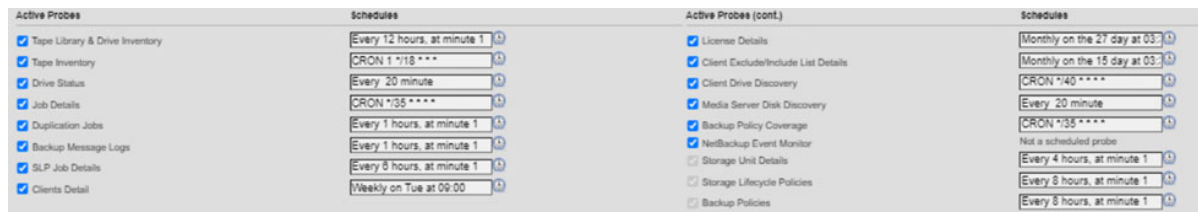
- ☐ 14. In the **Edit NetBackup Policy** dialog box, click **OK** to save your changes and return to the **NetBackup Discovery Policy Administration** window.
- ☐ 15. In the **NetBackup Discovery Policy Administration** window, click **OK** to close the **NetBackup Discovery Policy Administration** window and return to the **Admin** page.

Adding a Veritas NetBackup Data Collector Policy

- ☐ 16. In the **APTARE IT Analytics** Portal, navigate to **Admin > Data Collection > Collector Administration**. A list of currently configured Data Collectors is displayed.
- ☐ 17. On the **Collector Administration** page, select **collector2** in the list of currently configured Data Collectors and then click **Add Policy**.
- ☐ 18. In the resulting menu, select **Veritas NetBackup** listed under **Data Protection**.
- ☐ 19. In **Veritas NetBackup Data Collector Policy** dialog box that is displayed, Verify that the **Policy Domain** is set to **Aptare**.
- ☐ 20. Select **nbmaster1.example.com** in the **NetBackup Master Servers** list.
- ☐ 21. Enter the following details under the **Remote Probes Login Details** section.

Field	Value
Master Server Domain	<Leave this field blank>
Master Server User ID	<input type="text" value="T"/> root
Master Server Password	<input type="text" value="T"/> P@ssw0rd
Repeat Password	<input type="text" value="T"/> P@ssw0rd
WMI Proxy Address	<Leave this field blank>

- ☐ 22. Enter /usr/opensv in the **Backup Software Location on the Server (Data Collector or NetBackup Master)** field.
- ☐ 23. Select all probes listed under the **Active Probes** section as illustrated in the figure below.



- ☐ 24. Leave all the **Schedules** at their default values.
- ☐ 25. Click the **Test Connection** button located at the bottom of the **Veritas NetBackup Data Collector Policy** dialog box.
- ☐ 26. In the **Test Completed** dialog box that is displayed, verify that the test has been completed successfully and click **OK** to return to the **Veritas NetBackup Data Collector Policy** dialog box.
- ☐ 27. In the **Veritas NetBackup Data Collector Policy** dialog box, click **OK** to save the Data Collector policy.

You are returned to the **Collector Administration** page, note that the new policy is assigned to **collector2**

You might need to expand **collector2** on the **Collector Administration** page to view a list of assigned policies.


- ☐ 28. Remain logged into the **Aptare IT Analytics** Portal. You will return to it in the next exercise.

[Go to Lab Exercises](#)

Exercise C: Validating Data Collection

In this exercise, you validate the data collection process. Validation methods differ based on the subsystem vendor associated with the policy.

Validating Data Collection for Veritas Backup Exec

- ☐ 1. Sign in to the  **collector1** system using the following credentials:

Username:


Password:

- ☐ 2. Double-click the **Command Prompt** shortcut, located on the desktop of the **collector1** system, to launch the **Command Prompt**.
- ☐ 3. In the **Command Prompt** window, type the following command and press **Enter** to change directory to **C:\Program Files\Aptare\mbs\bin\backupexec**.

Command:


- ☐ 4. In the **Command Prompt** window, type the following command and press **Enter** to run the **CLI Checkinstall Utility**.

Command:

 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.

- ☐ 5. Verify that the **checkinstall** utility completes successfully.
- ☐ 6. In the **Command Prompt** window, type **exit** and press **Enter** to close the **Command Prompt** window.

Validating Data Collection for Veritas NetBackup

- ☐ 7. Access the desktop of the  **console** system.
- ☐ 8. If required, sign in to the **console.example.com** system using the credentials below.

Username:


Password:

- ☐ 9. Access the **APTARE IT Analytics Portal**.
- ☐ 10. If required, login to the **APTARE IT Analytics Portal** using the credentials below:


Username admin@example.com

Password P@ssw0rd

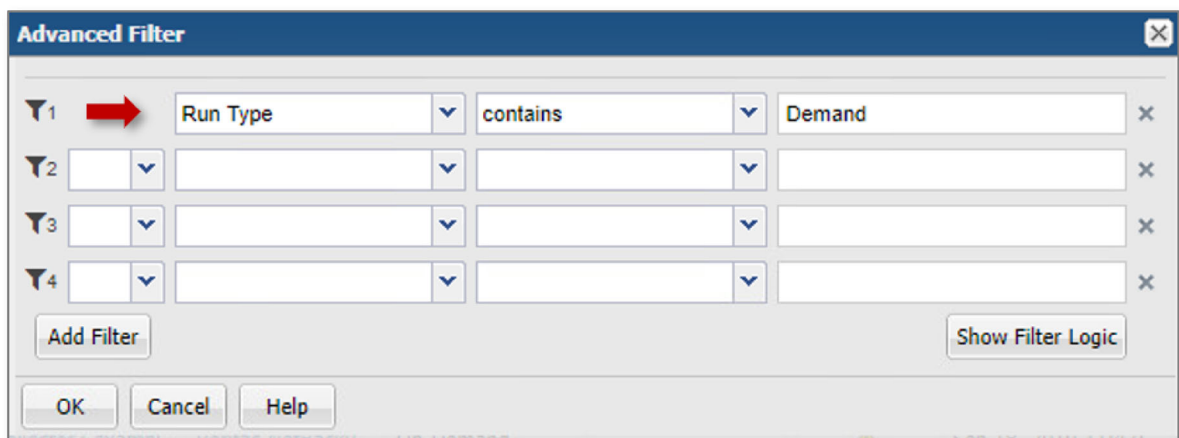
- ☐ 11. In the **APTARE IT Analytics Portal**, navigate to **Admin > Data Collection > Collector Administration**. A list of currently configured Data Collectors is displayed.
- ☐ 12. On the **Collector Administration** page, expand the entry for the **collector2** system and select the **Veritas NetBackup - nbmaster1.example.com** Data Collector policy.
- ☐ 13. Click the **Run** button.
- ☐ 14. In the **Run Veritas NetBackup Collection** dialog box that is displayed, verify that **nbmaster1.example.com** is selected in the **NetBackup Master Servers** list and that all the available **Probes** are selected.
- ☐ 15. In the **Run Veritas NetBackup Collection** dialog box, click **Start** to start the Data Collection.

 Data is collected just like a scheduled run plus additional logging information is gathered for troubleshooting purposes.


- ☐ 16. In the **APTARE IT Analytics Portal**, navigate to **Admin > Data Collection > Collection Status**. The **Collection Status** page is displayed.


 The **Collection Status** page can be used to monitor the health and progress of data collection. This view also contains probe runs and can be organized to suit your business requirements providing essential details that enable you to diagnose collection issues. Collection status, available at the data collector and policy level, provides results for the last time collection was attempted for enabled probes.

- ☐ 17. On the **Collection Status** page, click **Advanced** to access the **Advanced Filter**.
- ☐ 18. In the **Advanced Filter** dialog box that is displayed, configure the first filter as illustrated in the figure below



- ☐ 19. Click **OK** to apply the filter.
- ☐ 20. On the **Collection Status** page, monitor the status of all the **Probes** for **nbmaster1.example.com**.

 Initially, a **Failure** status might be displayed for all the probes. Use the **Refresh** button available on the **Collector Status** page to refresh the view and monitor the probes until they complete successfully.

 It might take 5-10 minutes for all the probes to complete successfully.

- ☐ 21. In the **APTARE IT Analytics Portal**, click **Inventory** located on the menu bar to navigate to the **Inventory**.
- ☐ 22. On the **Inventory** page, click **Refresh** located on the **Hierarchy Panel** to refresh the view.
- ☐ 23. In the **Hierarchy Panel**, note that:
 - The NetBackup Master Server, **nbmaster1.example.com** has been added to the **Backup Servers > Veritas NetBackup** host group.
 - All the NetBackup Clients have been added to the **Hosts > Veritas NetBackup** host group.
- ☐ 24. In the **APTARE IT Analytics** portal, click **System Administrator > Log Out** to log out.
- ☐ 25. Close the **Google Chrome** browser window.

End of Lab
