Lab 06: Collecting Data for Capacity and the Cloud

In this lab, you create a NetApp user with API privileges and configure a NetApp and a File Analytics Data Collector Policy. You also configure Host Discovery and Collection.

Lab Exercises

This lab includes the following exercises:

- Exercise A: Creating a NetApp User with API Privileges
- Exercise B: Adding a NetApp Data Collector Policy
- Exercise C: Adding a File Analytics Data Collector Policy
- Exercise D: Configuring Host Discovery and Collection
- Exercise E: Verifying Data Collection in the Portal

⚠ 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: Creating a NetApp User with API Privileges

In this exercise, you create a new NetApp user with API privileges.

☐ 1. Sign in to the console system using the credentials below.

User ID: T **EXAMPLE\Administrator**

Password: T **P@ssw0rd**

☐ 2. Double-click the **PuTTY** shortcut, located on the desktop of the **console** system, to launch **PuTTY**.

☐ 3. In the **PuTTY Configuration** window that is displayed, double-click the pre-configured entry for **netapp1.example.com**.

☐ 4. In the **PuTTY Security Alert** dialog box that is displayed, click **Yes** to continue with the connection. The login prompt is displayed in a new window.

☐ 5. Log in to the **netapp1.example.com** system using the credentials below.

User ID: T **root**

Password: T **P@ssw0rd**

☐ 6. In the **Terminal window** that is displayed, type the following command and press **Enter** to create a new user role.

Command: T useradmin role add apifarole -a cli-*,api-*,login-*,security-*

If **api-*** does not meet your security requirements, additional File Analytics privileges can be configured by executing the following command:

Command:
useradmin role add apifarole -a api-volume-list-info,api-nfs-exportfs-list-rules,api-cifs-share-list-iter-start,api-cifs-share-list-iter-next,api-cifs-share-list-iter-end,api-snapdiff-iter-start,api-snapdiff-iter-next,api-snapdiff-iter-end,login-http-admin,api-volume-options-list-info,api-snapshot-list-info,api-snapshot-delete,api-snapshot-create,api-nameservice-map-uid-to-user-name

☐ 7. In the **Terminal window**, type the following command and press **Enter** to create a new group.

Command: T useradmin group add apifagroup -r apifarole

- ☐ 8. In the **Terminal window**, type the following command and press **Enter** to create a new user.

  Command: T useradmin user add apifauser -g apifagroup

- ☐ 9. When prompted for **New password**, type T **P@ssw0rd** and press **Enter**.

- ☐ 10. When prompted to **Retype new password**, type T **P@ssw0rd** and press **Enter**.

  The new user is added and you are returned to the shell prompt.

- ☐ 11. At the shell prompt, type **exit** and press **Enter** to log out of the **netapp1.example.com** system.

  You are returned to the desktop of the **console.example.com** system.

Go to Lab Exercises

Exercise B: Adding a NetApp Data Collector Policy

In this exercise, you add a NetApp Data Collector Policy and perform an **On-Demand** run of the policy.

- [ ] 1. Double-click the **Aptare Portal** shortcut, located on the desktop of the **console.example.com** system, to launch the **APTARE IT Analytics Portal**.

- [ ] 2. When the **APTARE IT Analytics Portal** page is displayed, Sign-in using the following credentials.

Username	T admin@example.com
Password	T P@ssw0rd

- [ ] 3. In the **APTARE IT Analytics Portal**, navigate to **Admin > Data Collection > Collector Administration**. The **Collector Administration** page is displayed.

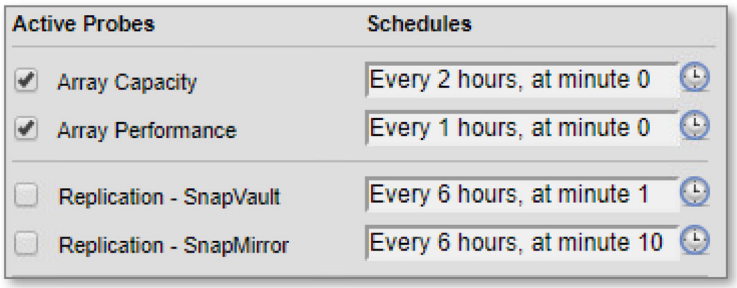
- [ ] 4. On the **Collector Administration** page, select **collector1** in the list of currently configured Data Collectors and then click **Add Policy**.

- [ ] 5. In the resulting menu, select **NetApp** present under **Replication** section. The **NetApp Data Collector Policy** dialog box is displayed.

- [ ] 6. In the **NetApp Data Collector Policy** dialog box, select **Aptare** in the **Policy Domain** drop-down list and enter T **netapp1.example.com** in the **NetApp Address** field.

- [ ] 7. Enter T **apifauser** in the **User ID** field and T **P@ssw0rd** in the **Password** and **Repeat password** fields.

- [ ] 8. Configure the **Active Probes** and **Schedules** as illustrated in the figure below.



- [ ] 9. In the **NetApp Data Collector Policy** dialog box, click **OK** to save the policy.

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

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

- [ ] 10. On the **Collector Administration** page, expand **collector1.example.com**, select the **NetApp - netapp1.example.com** data collection policy, and right click > **Run**.

- [ ] 11. In the **Run NetApp Collection** dialog box that is displayed, deselect the **Array Performance** probe and click **Start** without making any other changes.

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

- [ ] 13. On the **Collection Status** page, monitor the status of the **Array Capacity** probe for **netapp1.example.com**.

> Initially, a **Failure** status might be displayed for the **Array Capacity** probe. Use the **Refresh** button available on the **Collector Status** page to refresh the view and monitor the probe until it completes successfully.

> It might take 5-7 minutes for the **Array Capacity** probe to complete.

- [ ] 14. After the **Array Capacity** probe is complete, navigate to **Admin** > **Data Collection** > **Collector Administration**.

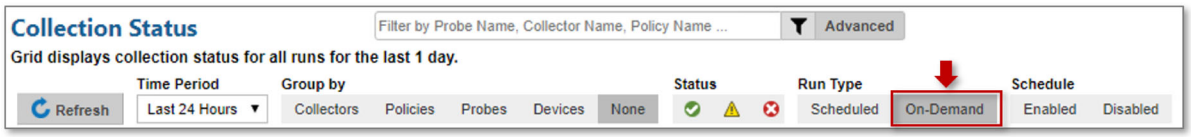
- [ ] 15. On the **Collector Administration** page, expand **collector1.example.com**, select the **NetApp - netapp1.example.com** data collection policy, click **Run** to run the policy for a second time.

- [ ] 16. In the **Run NetApp Collection** dialog box that is displayed, deselect the **Array Capacity** probe and click **Start** without making any other changes.

> At least one collection from this array must be performed before **Array Performance** data can be collected.

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

- [ ] 18. On the **Collection Status** page, click the **On-Demand** filter available under the **Run Type** category to display only **On-Demand** probes.



- [ ] 19. On the **Collection Status** page, monitor the status of the **Array Performance** probe for **netapp1.example.com**.

> Initially, a **Failure** status might be displayed for the **Array Performance** probe. Use the **Refresh** button available on the **Collector Status** page to refresh the view and monitor the probe until it completes successfully.

> It might take 2-3 minutes for the **Array Performance** probe to complete.

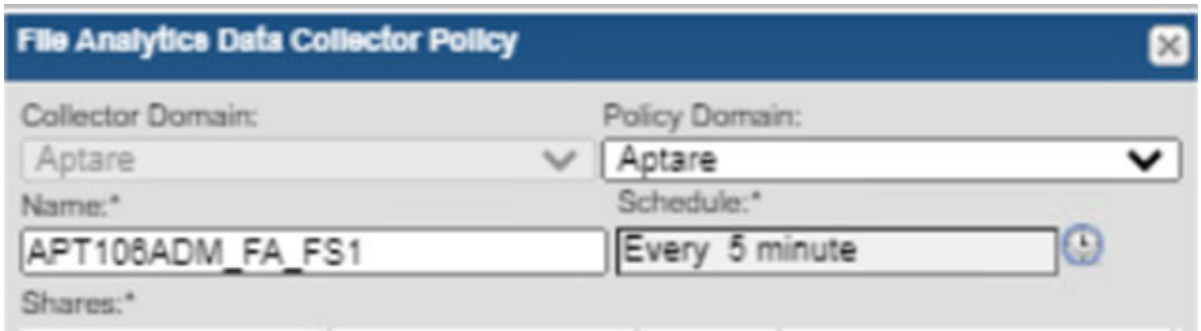
- [ ] 20. After the **Array Performance** probe is complete, navigate to **Admin** > **Data Collection** > **Collector Administration**.

Go to Lab Exercises

Exercise C: Adding a File Analytics Data Collector Policy

In this exercise, you add a File Analytics Data Collector Policy and perform a **Scheduled** run of the policy.

- [ ] 1. On the **Collector Administration** page, select **collector1.example.com** in the list of Data Collectors and then click **Add Policy**.
- [ ] 2. In the resulting menu, select **File Analytics**. The **File Analytics Data Collector Policy** dialog box is displayed.
- [ ] 3. In the **File Analytics Data Collector Policy** dialog box, select **Aptare** in the **Policy Domain** drop-down list and enter T **APT106ADM_FA_FS1** in the **Name** field.
- [ ] 4. Configure the **File Analytics Data Collector Policy** to run every **5 minutes** as illustrated in the figure below.



- [ ] 5. In the **File Analytics Data Collector Policy** dialog box, click **Add**. The **File Analytics Add Shares** dialog box is displayed.
- [ ] 6. Enter T **fileserver1.example.com** in the **Host/Device** field and T **Share1** in the **Share** field.
- [ ] 7. Select **CIFS** in the **Protocol** drop-down list and click **Add**. The **Credentials** dialog box is displayed.
- [ ] 8. In the **Credentials** dialog box, enter the following details:

Name	T APT106ADM_Windows_Credentials
Account	T Administrator
Password	T P@ssw0rd
Repeat Password	T P@ssw0rd
OS type	Windows
Windows domain	T EXAMPLE

- [ ] 9. In the **Credentials** dialog box, click **OK** to return to the **File Analytics Add Shares** dialog box.
- [ ]

10. In the **File Analytics Add Shares** dialog box, click **OK** to return to the **File Analytics Data Collector Policy** dialog box.

☐ 11. In the **File Analytics Data Collector Policy** dialog box, verify that **Share1** is listed in the **Shares** section and click **OK** to save the policy.

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

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

Go to Lab Exercises

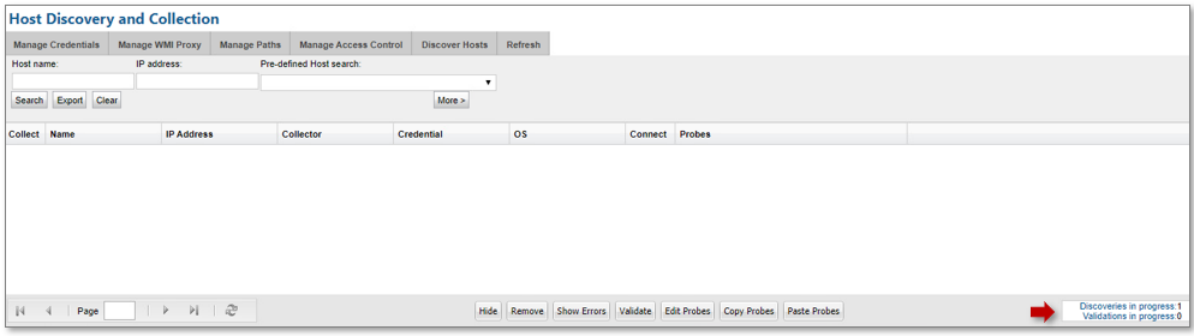
Exercise D: Configuring Host Discovery and Collection

In this exercise, you configure Host Discovery and Collection to gather system information from hosts.

- [ ] 1. In the **APTARE IT Analytics Portal**, navigate to **Admin > Data Collection > Host Discovery and Collection**. The **Host Discovery and Collection** page is displayed.
- [ ] 2. On the **Host Discovery and Collection** page, click **Manage WMI Proxy**. The **WMI Proxies** dialog box is displayed.
- [ ] 3. In the **WMI Proxies** dialog box, click **Add**. The **Add WMI Proxies** dialog box is displayed.
- [ ] 4. In the **Add WMI Proxies** dialog box, select **Aptare** in the **Domain** drop-down list and enter T **APT106ADM_WMI_Proxy** in the **Name** field.
- [ ] 5. Enter T **collector1.example.com** in the **WMI Proxy Server** field and click **OK** to return to the **WMI Proxies** dialog box.
- [ ] 6. In the **WMI Proxies** dialog box, verify that **APT106ADM_WMI_Proxy** is listed and click **OK** to return to the **Host Discovery and Collection** page.
- [ ] 7. On the **Host Discovery and Collection** page, click **Discover Hosts**. The **Host Discovery Policies** dialog box is displayed.
- [ ] 8. In the **Host Discovery Policies** dialog box, click **Add**. The **Add Host Discovery Policies** dialog box is displayed.
- [ ] 9. In the **Add Host Discovery Policies** dialog box, enter T **fileserver1.example.com** in the **Name** field.
- [ ] 10. Select **Aptare** in the **Domain** drop-down list, verify that **collector1** is selected in the **Collector** drop-down list, and enter T **fileserver1.example.com** in the **Host addresses** field.

  > You can add multiple hosts in a single discovery policy.

- [ ] 11. Under **Configuration options**, select **APT106ADM_Windows_Credentials** located under **Credentials** and **APT106ADM_WMI_Proxy** located under **WMI Proxies**.
- [ ] 12. In the **Add Host Discovery Policies** dialog box, click **OK** to save the discovery policy and return to the **Host Discovery Policies** dialog box.
- [ ] 13. In the **Host Discovery Policies** dialog box, select **fileserver1.example.com** and click **Start** to execute the discovery policy.
- [ ] 14. At the **Are you sure you wish to start the selected discovery** browser prompt, click **OK**.
- [ ] 15. In the **Host Discovery Policies** dialog box, click **OK** to return to the **Host Discovery and Collection** page.
- [ ] 16. On the **Host Discovery and Collection** page, click the **Discoveries in progress** link located at the bottom right corner of the **Host Discovery and Collection** page.



- [ ] 17. In the **Host Discovery Policies** dialog box that is displayed, verify that the discovery for **fileserver1.example.com** has been completed successfully.

> The discovery might take 5-7 minutes to complete. If the discovery is not yet complete, close the **Host Discovery Policies** dialog box and click the **Discoveries in progress** link again to refresh the status as there is no refresh option available in the **Host Discovery Policies** dialog box.

- [ ] 18. In the **Host Discovery Policies** dialog box, click **OK** to return to the **Host Discovery and Collection** page.
- [ ] 19. On the **Host Discovery and Collection** page, enter T **fileserver1.example.com** in the **Host name** field and click **Search**.
- [ ] 20. In the search results that are displayed, select **fileserver1.example.com** and click **Edit Probes** present at the bottom of the screen.
- [ ] 21. In the **Host Probe Settings** dialog box that is displayed, select the **Memory**, **Network**, **Process**, **Performance**, and **System** probes and configure each probe to execute every **5 minutes** as illustrated in the figure below.
- [ ] 22. Select the **File Analytics** tab, note that an option to enable **File Analytics** collection is available under the **File Analytics** tab.
- [ ] 23. Select the **Collect** option under **File Analytics** tab and configure the **File Analytics** probe to execute every **5 minutes** as illustrated in the figure below.
- [ ] 24. In the **Host Probe Settings** dialog box, click **OK** to save the configuration and return to the **Host Discovery and Collection** page.
- [ ] 25. On the **Host Discovery and Collection** page, select **fileserver1.example.com** and click the button currently showing red under Collect column. **Activate Collection**.
- [ ] 26. On the **Host Discovery and Collection** page with **fileserver1.example.com** selected, click **Validate**.

> The **Validate** step provides feedback to troubleshoot host connectivity and data collection issues and for the **File Analytics** probe, by design, the **Validate** option only runs a connectivity check; it does not collect **File Analytics** data.

- [ ] 27. At the **Are you sure you wish to validate the selected hosts** browser prompt, click **OK**.
- [ ] 28. On the **Host Discovery and Collection** page with **fileserver1.example.com** selected, click **Show Errors**. The **Messages** dialog box is displayed.

> Any errors encountered during the validation are logged in the **Messages** dialog box.

- [ ] 29. Verify that no errors are listed in the **Messages** dialog box and click **OK** to return to the **Host Discovery and Collection** page.

- [ ] 30. Wait for the File Analytics data collection to execute and complete. The status of the data collection can be monitored by running the **File Analytics Collection Status** report located in the **System Administration Reports** folder.

> It might take 15-30 minutes for the **File Analytics Data Collection** to complete.

Go to Lab Exercises

Exercise E: Verifying Data Collection in the Portal

In this exercise, you verify NetApp and File Analytics data in the Portal.

- [ ] 1. In the **APTARE IT Analytics Portal**, click **Inventory** located on the menu bar to navigate to the **Inventory** page.
- [ ] 2. On the **Inventory** page, click **Refresh** located on the **Hierarchy Panel** to update the **Inventory** and click **Default Hierarchy** icon.
- [ ] 3. In the **Hierarchy Panel**, note that:
    - The **NetApp** host **netapp1** has been added under **Arrays > NetApp**.
    - All the 4 LUNs configured on **netapp1** are visible under **Arrays > NetApp > netapp1**.

      > You can click on any of the LUNs that are listed under **Arrays > NetApp > netapp1** to view the **LUN Host Mapping Detail**. No data will be displayed in the **LUN Host Mapping Detail** if the LUNs are unallocated.

    - The file share, **Share1** has been added under **File Share & Volumes > Shares**.
    - The C drive from **fileserver1.example.com** has been added under **File Share & Volumes > Volumes**.

      > The **C** drive from the **fileserver1.example.com** will not be visible under **File Share & Volumes > Volumes** if the File Analytics Data Collection is not complete. Run the **File Analytics Collection Status** report to view the status of the collection.

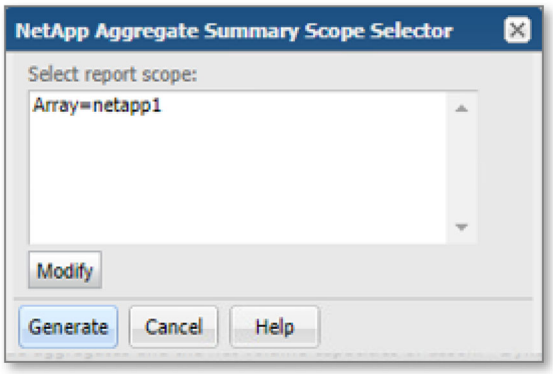
      The figure below illustrates the contents of the **File Analytics Collection Status** report when the File Analytics Data Collection is complete.

    - The file server, **fileserver1.example.com** has been added under **Hosts > File Analytics**.
- [ ] 4. In the **Hierarchy Panel**, navigate to **Hosts > File Analytics** and click **fileserver1.example.com**.
- [ ] 5. On the **fileserver1.example.com** management page that is displayed in the right pane, review the **CPU**, **Memory**, and **File System Utilization** graphs. This data is populated when the probes defined under **Host Discovery and Collection** were executed.
- [ ] 6. In the **APTARE IT Analytics Portal**, navigate to **Admin > File List > Export**. The **File List Export** window is displayed.
- [ ] 7. In the **File List Export** window, click **New Export Request**. The **New Export Request** dialog box is displayed.
- [ ] 8. In the **New Export Request** dialog box, enter T **APT106ADM_File_List_Export** in the **Name** field and select the **Text Files** file category.
- [ ] 9. To Set the **Scope** click **Modify**. Report Scope Selector window will appear.
- [ ] 10. On the Report Scope Selector window expand **File Shares & Volumes>All Devices>fileserver1.example.com>Volumes**. Double click volume **C**. Volume C has been added into **In scope** section. Click **Ok**.

- [ ] 11. Click **OK** to submit the export and return to the **File List Export** window.
- [ ] 12. In the **File List Export** window, select **APT106ADM_File_List_Export** and click **Download** to download the file list.
- [ ] 13. In the **File List Export** window, click **OK** to close the **File List Export** window and return to the **Admin** page.

> The exported file list is available for review in the **Downloads** folder on the **console.example.com** system.

- [ ] 14. In the **APTARE IT Analytics Portal**, click **Reports** located on the menu bar to navigate to the **Reports** page.
- [ ] 15. On the **Reports** page, click **Capacity Manager > Array Capacity & Utilization** located in the **Reports Navigation Panel**. The available reports are displayed in the **Reports** view panel.
- [ ] 16. In the **Reports** view panel, double-click the **NetApp Aggregate Summary** report. The **NetApp Aggregate Summary Scope Selector** dialog box is displayed.
- [ ] 17. In the **NetApp Aggregate Summary Scope Selector** dialog box, change the report scope to **Array=netapp1** as illustrated in the figure below.



> Host **netapp1** is located under the **Storage Arrays > Storage Array Vendors > NetApp > Product Names > SIMBOX** host group.

- [ ] 18. In the **NetApp Aggregate Summary Scope Selector** dialog box, click **Generate** to generate the **NetApp Aggregate Summary** report.

  The contents of the **NetApp Aggregate Summary** report are displayed in a new tab.

  The **NetApp Aggregate Summary** report shows all the Aggregates configured on **netapp1** along with the **Total Capacity**, **Available Size**, etc.

  On the **NetApp Aggregate Summary** tab that displays the contents of the report, the links provided under **Aggregate**, **# of Vols**, **List of Plexes**, can be used to run the **NetApp Aggregate Detail**, **NetApp Volume Summary**,and the **NetApp Plex Details** report respectively.

  Similarly, there will be links available in the above mentioned reports which will allow to fetch other details from the Array. For example, the **NetApp Volume Summary** report contains a link to the **# Shares**, **# Exports**, etc which can be used to run the **NetApp CIFS Summary**, and the **NetApp NFS Summary** reports respectively.

Feel free to run any of the available reports and review the contents.

- [ ] 19. In the **APTARE IT Analytics Portal**, click **System Administrator > Log Out** to log out of the **APTARE IT Analytics Portal**.

- [ ] 20. Close the **Google Chrome** browser window and log out of the **console.example.com** system.

End of Lab