Set up basic monitoring tasks
ONTAP 9
NetApp
November 28, 2022
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up basic monitoring tasks</td>
<td>1</td>
</tr>
<tr>
<td>Perform daily monitoring</td>
<td>1</td>
</tr>
<tr>
<td>Use weekly and monthly performance trends to identify performance issues</td>
<td>1</td>
</tr>
<tr>
<td>Use performance thresholds to generate event notifications</td>
<td>1</td>
</tr>
<tr>
<td>Set performance thresholds</td>
<td>2</td>
</tr>
<tr>
<td>Add alerts</td>
<td>2</td>
</tr>
</tbody>
</table>
Set up basic monitoring tasks

Perform daily monitoring

You can perform daily monitoring to ensure that you do not have any immediate performance issues that require attention.

Steps
1. From the Active IQ Unified Manager UI, go to the Event Inventory page to view all current and obsolete events.
2. From the View option, select Active Performance Events and determine what action is required.

Use weekly and monthly performance trends to identify performance issues

Identifying performance trends can assist you in identifying whether the cluster is being overused or underused by analyzing volume latency. You can use similar steps to identify CPU, network, or other system bottlenecks.

Steps
1. Locate the volume that you suspect is being underused or overused.
2. On the Volume Details tab, click 30 d to display the historical data.
3. In the "Break down data by" drop-down menu, select Latency, and then click Submit.
4. Deselect Aggregate in the cluster components comparison chart, and then compare the cluster latency with the volume latency chart.
5. Select Aggregate and deselect all other components in the cluster components comparison chart, and then compare the aggregate latency with the volume latency chart.
6. Compare the reads/writes latency chart to the volume latency chart.
7. Determine whether client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine whether the aggregate is overused and causing contention and rebalance workloads as needed.

Use performance thresholds to generate event notifications

Events are notifications that the Active IQ Unified Manager generates automatically when a predefined condition occurs, or when a performance counter value crosses a threshold. Events help you identify performance issues in the clusters you are monitoring. You can configure alerts to send email notification automatically when events of certain severity types occur.
Set performance thresholds

You can set performance thresholds to monitor critical performance issues. User-defined thresholds trigger a warning or a critical event notification when the system approaches or exceeds the defined threshold.

Steps

1. Create the Warning and Critical event thresholds:
   a. Select `Configuration > Performance Thresholds`.
   b. Click `Create`.
   c. Select the object type and specify a name and description of the policy.
   d. Select the object counter condition and specify the limit values that define Warning and Critical events.
   e. Select the duration of time that the limit values must be breached for an event to be sent, and then click `Save`.

2. Assign the threshold policy to the storage object.
   a. Go to the Inventory page for the same cluster object type that you previously selected and choose the `Performance` from the View option.
   b. Select the object to which you want to assign the threshold policy, and then click `Assign Threshold Policy`.
   c. Select the policy you previously created, and then click `Assign Policy`.

Example

You can set user-defined thresholds to learn about critical performance issues. For example, if you have a Microsoft Exchange Server and you know that it crashes if volume latency exceeds 20 milliseconds, you can set a warning threshold at 12 milliseconds and a critical threshold at 15 milliseconds. With this threshold setting, you can receive notifications when the volume latency exceeds the limit.

Add alerts

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

What you'll need

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Scripts page.
You must have the Application Administrator or Storage Administrator role.

About this task
You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Alert Setup page, as described here.

Steps
1. In the left navigation pane, click **Storage Management > Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.
   
   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.
   
   To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.
   
   If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert
This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains "abc" and excludes all volumes whose name contains "xyz"
- Events: includes all critical health events
- Actions: includes "sample@domain.com", a "Test" script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter HealthTest in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter abc in the **Name contains** field to display the volumes whose name contains "abc".
   b. Select "<<All Volumes whose name contains 'abc'>>" from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter xyz in the **Name contains** field, and then click **Add**.

3. Click **Events**, and select **Critical** from the Event Severity field.

4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.

5. Click **Actions**, and enter sample@domain.com in the **Alert these users** field.

6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test script**.

8. Click **Save**.