NetApp

Monitor the health of your system

ONTAP 9

NetApp
June 21, 2022

Table of Contents

Monitor the health of your system

Monitor the health of your system overview

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

For details on how ONTAP supports cluster switches for system health monitoring in your cluster, you can refer to the *Hardware Universe*.

Supported switches in the Hardware Universe

For details on the causes of Cluster Switch Health Monitor (CSHM) AutoSupport messages, and the necessary actions required to resolve these alerts, you can refer to the Knowledgebase article.

AutoSupport Message: Health Monitor Process CSHM

How health monitoring works

Individual health monitors have a set of policies that trigger alerts when certain conditions occur. Understanding how health monitoring works can help you respond to problems and control future alerts.

Health monitoring consists of the following components:

- Individual health monitors for specific subsystems, each of which has its own health status

  For example, the Storage subsystem has a node connectivity health monitor.

- An overall system health monitor that consolidates the health status of the individual health monitors

  A degraded status in any single subsystem results in a degraded status for the entire system. If no subsystems have alerts, the overall system status is OK.

Each health monitor is made up of the following key elements:

- Alerts that the health monitor can potentially raise

  Each alert has a definition, which includes details such as the severity of the alert and its probable cause.

- Health policies that identify when each alert is triggered

Each health policy has a rule expression, which is the exact condition or change that triggers the alert.

A health monitor continuously monitors and validates the resources in its subsystem for condition or state changes. When a condition or state change matches a rule expression in a health policy, the health monitor raises an alert. An alert causes the subsystem's health status and the overall system health status to become degraded.

Ways to respond to system health alerts

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the "Acknowledger."
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

  Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as "ok-with-suppressed." when the suppressed alert occurs.

System health alert customization

You can control which alerts a health monitor generates by enabling and disabling the system health policies that define when alerts are triggered. This enables you to customize the health monitoring system for your particular environment.

You can learn the name of a policy either by displaying detailed information about a generated alert or by displaying policy definitions for a specific health monitor, node, or alert ID.

Disabling health policies is different from suppressing alerts. When you suppress an alert, it does not affect the subsystem's health status, but the alert can still occur.

If you disable a policy, the condition or state that is defined in its policy rule expression no longer triggers an alert.

Example of an alert that you want to disable

For example, suppose an alert occurs that is not useful to you. You use the `system health alert show -instance` command to obtain the Policy ID for the alert. You use the policy ID in the `system health`

`policy definition show` command to view information about the policy. After reviewing the rule expression and other information about the policy, you decide to disable the policy. You use the `system health policy definition modify` command to disable the policy.

How health alerts trigger AutoSupport messages and events

System health alerts trigger AutoSupport messages and events in the Event Management System (EMS), enabling you to monitor the health of the system using AutoSupport messages and the EMS in addition to using the health monitoring system directly.

Your system sends an AutoSupport message within five minutes of an alert. The AutoSupport message includes all alerts generated since the previous AutoSupport message, except for alerts that duplicate an alert for the same resource and probable cause within the previous week.

Some alerts do not trigger AutoSupport messages. An alert does not trigger an AutoSupport message if its health policy disables the sending of AutoSupport messages. For example, a health policy might disable AutoSupport messages by default because AutoSupport already generates a message when the problem occurs. You can configure policies to not trigger AutoSupport messages by using the `system health policy definition modify` command.

You can view a list of all of the alert-triggered AutoSupport messages sent in the previous week using the `system health autosupport trigger history show` command.

Alerts also trigger the generation of events to the EMS. An event is generated each time an alert is created and each time an alert is cleared.

Available cluster health monitors

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within ONTAP systems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch(cluster-switch)	Switch (Switch-Health)	Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting. ⓘ Beginning with ONTAP 9.2, this monitor can detect and report when a cluster switch has rebooted since the last polling period.
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity(node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

Receive system health alerts automatically

You can manually view system health alerts by using the `system health alert show` command. However, you should subscribe to specific Event Management System (EMS) messages to automatically receive notifications when a health monitor generates an alert.

About this task

The following procedure shows you how to set up notifications for all hm.alert.raised messages and all hm.alert.cleared messages.

All hm.alert.raised messages and all hm.alert.cleared messages include an SNMP trap. The names of the SNMP traps are `HealthMonitorAlertRaised` and `HealthMonitorAlertCleared`. For information about SNMP traps, see the *Network Management Guide*.

Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

   ```
   cluster1::> event destination create -name health_alerts -mail
   admin@example.com
   ```

2. Use the `event route add-destinations` command to route the `hm.alert.raised` message and the `hm.alert.cleared` message to a destination.

   ```
   cluster1::> event route add-destinations -messagename hm.alert*
   -destinations health_alerts
   ```

Related information

[Network management](#)

Respond to degraded system health

When your system's health status is degraded, you can show alerts, read about the probable cause and corrective actions, show information about the degraded subsystem, and resolve the problem. Suppressed alerts are also shown so that you can modify them and see whether they have been acknowledged.

About this task

You can discover that an alert was generated by viewing an AutoSupport message or an EMS event, or by using the `system health` commands.

Steps

1. Use the `system health alert show` command to view the alerts that are compromising the system's health.

2. Read the alert's probable cause, possible effect, and corrective actions to determine whether you can

resolve the problem or need more information.

3. If you need more information, use the `system health alert show -instance` command to view additional information available for the alert.

4. Use the `system health alert modify` command with the `-acknowledge` parameter to indicate that you are working on a specific alert.

5. Take corrective action to resolve the problem as described by the `Corrective Actions` field in the alert.

   The corrective actions might include rebooting the system.

   When the problem is resolved, the alert is automatically cleared. If the subsystem has no other alerts, the health of the subsystem changes to `OK`. If the health of all subsystems is OK, the overall system health status changes to `OK`.

6. Use the `system health status show` command to confirm that the system health status is `OK`.

   If the system health status is not `OK`, repeat this procedure.

Example of responding to degraded system health

By reviewing a specific example of degraded system health caused by a shelf that lacks two paths to a node, you can see what the CLI displays when you respond to an alert.

After starting ONTAP, you check the system health and you discover that the status is degraded:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

You show alerts to find out where the problem is, and see that shelf 2 does not have two paths to node1:

```
cluster1::>system health alert show
              Node: node1
          Resource: Shelf ID 2
          Severity: Major
    Indication Time: Mon Nov 10 16:48:12 2013
    Probable Cause: Disk shelf 2 does not have two paths to controller
                    node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                    lost with a single hardware component failure (e.g.
                    cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                    2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                    3. Reboot the halted controllers.
                    4. Contact support personnel if the alert persists.
```

You display details about the alert to get more information, including the alert ID:

```
   cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                    Node: node1
                 Monitor: node-connect
                Alert ID: DualPathToDiskShelf_Alert
       Alerting Resource: 50:05:0c:c1:02:00:0f:02
               Subsystem: SAS-connect
         Indication Time: Mon Mar 21 10:26:38 2011
      Perceived Severity: Major
          Probable Cause: Connection_establishment_error
             Description: Disk shelf 2 does not have two paths to controller
node1.
      Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                          2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                          3. Reboot the halted controllers.
                          4. Contact support personnel if the alert
persists.
         Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
             Acknowledge: false
                Suppress: false
                  Policy: DualPathToDiskShelf_Policy
             Acknowledger: -
               Suppressor: -
  Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                          Shelf id: 2
                          Shelf Name: 4d.shelf2
                          Number of Paths: 1
                          Number of Disks: 6
                          Adapter connected to IOMA:
                          Adapter connected to IOMB: 4d
  Alerting Resource Name: Shelf ID 2
```

You acknowledge the alert to indicate that you are working on it.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

You fix the cabling between shelf 2 and node1, and then reboot the system. Then you check system health again, and see that the status is OK:

```
cluster1::>system health status show
  Status
  --------------
  OK
```

Configure discovery of cluster and management network switches

The cluster switch health monitor automatically attempts to discover your cluster and management network switches using the Cisco Discovery Protocol (CDP). You must configure the health monitor if it cannot automatically discover a switch or if you do not want to use CDP for automatic discovery.

About this task

The `system cluster-switch show` command lists the switches that the health monitor discovered. If you do not see a switch that you expected to see in that list, then the health monitor cannot automatically discover it.

Steps

1. If you want to use CDP for automatic discovery, do the following; otherwise, go to step 2:

   a. Ensure that the Cisco Discovery Protocol (CDP) is enabled on your switches.

   Refer to your switch documentation for instructions.

   b. Run the following command on each node in the cluster to verify whether CDP is enabled or disabled:

   run -node *node_name* -command options cdpd.enable

   If CDP is enabled, go to step d. If CDP is disabled, go to step c.

   c. Run the following command to enable CDP:

   run -node *node_name* -command options cdpd.enable on

   Wait five minutes before you go to the next step.

   d. Use the `system cluster-switch show` command to verify whether ONTAP can now automatically discover the switches.

2. If the health monitor cannot automatically discover a switch, use the `system cluster-switch create` command to configure discovery of the switch:

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Wait five minutes before you go to the next step.

3. Use the `system cluster-switch show` command to verify that ONTAP can discover the switch for which you added information.

After you finish

Verify that the health monitor can monitor your switches.

Verify the monitoring of cluster and management network switches

The cluster switch health monitor automatically attempts to monitor the switches that it discovers; however, monitoring might not happen automatically if the switches are not configured correctly. You should verify that the health monitor is properly configured to monitor your switches.

Steps

1. Use the `system health cluster-switch show` command to identify the switches that the cluster switch health monitor discovered.

   If the `Model` column displays the value `OTHER`, then ONTAP cannot monitor the switch. ONTAP sets the value to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.

   > (i) If a switch does not display in the command output, then you must configure discovery of the switch.

2. Upgrade to the latest supported switch software and reference the configuration file (RCF) from the NetApp Support Site.

   [Cisco Ethernet Switch page](#)

   The community string in the switch's RCF must match the community string that the health monitor is configured to use. By default, the health monitor uses the community string `cshm1!`.

   If you need to change information about a switch that the cluster monitors, you can modify the community string that the health monitor uses by using the `system health cluster-switch modify` command.

3. Verify that the switch's management port is connected to the management network.

   This connection is required to perform SNMP queries.

Commands for monitoring the health of your system

You can use the `system health` commands to display information about the health of system resources, to respond to alerts, and to configure future alerts. Using the CLI commands enables you to view in-depth information about how health monitoring is configured. The man pages for the commands contain more information.

Display the status of system health

If you want to…	Use this command…
Display the health status of the system, which reflects the overall status of individual health monitors	`system health status show`
Display the health status of subsystems for which health monitoring is available	`system health subsystem show`

Display the status of node connectivity

If you want to…	Use this command…
Display details about connectivity from the node to the storage shelf, including port information, HBA port speed, I/O throughput, and the rate of I/O operations per second	`storage shelf show -connectivity` Use the `-instance` parameter to display detailed information about each shelf.
Display information about drives and array LUNs, including the usable space, shelf and bay numbers, and owning node name	`storage disk show` Use the `-instance` parameter to display detailed information about each drive.
Display detailed information about storage shelf ports, including port type, speed, and status	`storage port show` Use the `-instance` parameter to display detailed information about each adapter.

Manage the discovery of cluster and management network switches

If you want to…	Use this command…
Display the switches that the cluster monitors	`system cluster-switch show`
Display the switches that the cluster currently monitors, including switches that you deleted (shown in the Reason column in the command output), and configuration information that you need for network access to the cluster and management network switches. This command is available at the advanced privilege level.	`system cluster-switch show-all`
Configure discovery of an undiscovered switch	`system cluster-switch create`

If you want to…	Use this command…
Modify information about a switch that the cluster monitors (for example, device name, IP address, SNMP version, and community string)	`system cluster-switch modify`
Disable monitoring of a switch	`system cluster-switch modify -disable -monitoring`
Display the interval in which the health monitor polls switches to gather information	`system cluster-switch polling-interval show`
Modify the interval in which the health monitor polls switches to gather information. This command is available at the advanced privilege level.	`system cluster-switch polling-interval modify`
Disable discovery and monitoring of a switch and delete switch configuration information	`system cluster-switch delete`
Permanently remove the switch configuration information which is stored in the database (doing so reenables automatic discovery of the switch)	`system cluster-switch delete -force`
Enable automatic logging to send with AutoSupport messages. This command is available at the advanced privilege level.	`system cluster-switch log`

Respond to generated alerts

If you want to…	Use this command…
Display information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause	`system health alert show`
Display information about each generated alert	`system health alert show -instance`
Indicate that someone is working on an alert	`system health alert modify`
Acknowledge an alert	`system health alert modify -acknowledge`
Suppress a subsequent alert so that it does not affect the health status of a subsystem	`system health alert modify -suppress`

If you want to…	Use this command…
Delete an alert that was not automatically cleared	`system health alert delete`
Display information about the AutoSupport messages that alerts triggered within the last week, for example, to determine whether an alert triggered an AutoSupport message	`system health autosupport trigger history show`

Configure future alerts

If you want to…	Use this command…
Enable or disable the policy that controls whether a specific resource state raises a specific alert	`system health policy definition modify`

Display information about how health monitoring is configured

If you want to…	Use this command…
Display information about health monitors, such as their nodes, names, subsystems, and status	`system health config show` (i) Use the `-instance` parameter to display detailed information about each health monitor.
Display information about the alerts that a health monitor can potentially generate	`system health alert definition show` (i) Use the `-instance` parameter to display detailed information about each alert definition.
Display information about health monitor policies, which determine when alerts are raised	`system health policy definition show` (i) Use the `-instance` parameter to display detailed information about each policy. Use other parameters to filter the list of alerts—for example, by policy status (enabled or not), health monitor, alert, and so on.

Downgrade software versions between minor releases

When downgrading a cluster from Data ONTAP 8.2.1 to Data ONTAP 8.2, ONTAP clears the history of deleted switches. It also sets the `Model` column to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.

If you want to…	Use this command…
Downgrade the software version command	`system cluster-switch prepare-to-downgrade`