运行状况监控
ONTAP 9

NetApp
April 24, 2024

目录

运行状况监控 1
监控系统运行状况概述 1
运行状况监控的工作原理 1
响应系统运行状况警报的方式 2
系统运行状况警报自定义 2
运行状况警报如何触发 AutoSupport 消息和事件 2
可用的集群运行状况监控器 3
自动接收系统运行状况警报 4
响应降级的系统运行状况 4
响应降级的系统运行状况的示例 5
配置集群和管理网络交换机的发现 8
验证对集群和管理网络交换机的监控 9
用于监控系统运行状况的命令 10
显示环境信息 12

运行状况监控

监控系统运行状况概述

运行状况监控器会主动监控集群中的某些严重情况，并在检测到故障或风险时发出警报。如果存在活动警报，则系统运行状况状态将报告集群的已降级状态。警报包含响应降级的系统运行状况所需的信息。

如果状态为 degraded ，则可以查看有关问题的详细信息，包括可能的发生原因和建议的恢复操作。解决此问题后，系统运行状况将自动恢复为 OK 。

系统运行状况反映了多个单独的运行状况监控器。单个运行状况监控器中的降级状态会导致整个系统运行状况处于降级状态。

有关 ONTAP 如何支持集群交换机在集群中监控系统运行状况的详细信息，请参见 *cluster* Hardware Universe 。

"Hardware Universe 中支持的交换机"

有关集群交换机运行状况监控器（ Cluster Switch Health Monitor ， CSHM ） AutoSupport 消息的原因以及解决这些警报所需采取的必要操作的详细信息，您可以参阅知识库文章。

"AutoSupport 消息：运行状况监控器进程 CSHM"

运行状况监控的工作原理

各个运行状况监控器都有一组策略，可在发生特定情况时触发警报。了解运行状况监控的工作原理有助于您对问题做出响应并控制未来的警报。

运行状况监控包括以下组件：

- 单独监控特定子系统的运行状况，每个子系统都有自己的运行状况

  例如，存储子系统具有一个节点连接运行状况监控器。

- 一个整体系统运行状况监控器，用于整合各个运行状况监控器的运行状况

  任何一个子系统中的降级状态都会导致整个系统处于降级状态。如果没有子系统出现警报，则整体系统状态为 OK 。

每个运行状况监控器都由以下关键要素组成：

- 运行状况监控器可能会发出的警报

  每个警报都有一个定义，其中包括警报严重性及其可能的发生原因等详细信息。

- 用于确定何时触发每个警报的运行状况策略

  每个运行状况策略都有一个规则表达式，这是触发警报的确切条件或更改。

运行状况监控器会持续监控并验证其子系统中的资源，以查看其状况或状态是否发生变化。如果条件或状态更改与运行状况策略中的规则表达式匹配，则运行状况监控器将发出警报。警报会导致子系统的运行状况和整体系统运行状况降级。

响应系统运行状况警报的方式

发生系统运行状况警报时，您可以确认该警报，了解其详细信息，修复基本状况并防止其再次发生。

当运行状况监控器发出警报时，您可以通过以下任一方式做出响应：

- 获取有关警报的信息，其中包括受影响的资源，警报严重性，可能的发生原因，可能的影响以及更正操作。
- 获取有关警报的详细信息，例如发出警报的时间以及是否有任何其他人已确认警报。
- 获取有关受影响资源或子系统的状态的运行状况信息，例如特定磁盘架或磁盘。
- 确认警报以指示有人正在处理此问题，并将您自己标识为 "`确认者。`
- 通过采取警报中提供的更正操作解决问题，例如修复布线以解决连接问题。
- 如果系统未自动清除警报，请将其删除。
- 禁止警报以防止其影响子系统的运行状况。

  当您了解问题时，禁止非常有用。禁止警报后，警报可能仍会发生，但在出现禁止的警报时，子系统运行状况显示为 "`ok-on-suppressed 。` " 。

系统运行状况警报自定义

您可以通过启用和禁用定义何时触发警报的系统运行状况策略来控制运行状况监控器生成的警报。这样，您就可以根据特定环境自定义运行状况监控系统。

您可以通过显示有关生成的警报的详细信息或显示特定运行状况监控器，节点或警报 ID 的策略定义来了解策略名称。

禁用运行状况策略与禁止警报不同。禁止警报时，它不会影响子系统的运行状况，但警报仍可能发生。

如果禁用某个策略，则在其策略规则表达式中定义的条件或状态将不再触发警报。

要禁用的警报示例

例如，假设出现对您不有用的警报。您可以使用 `system health alert show -instance` 命令以获取警报的策略ID。您可以在中使用策略ID `system health policy definition show` 命令以查看有关策略的信息。查看规则表达式以及有关策略的其他信息后，您决定禁用此策略。您可以使用 `system health policy definition modify` 命令以禁用策略。

运行状况警报如何触发 **AutoSupport** 消息和事件

系统运行状况警报会在事件管理系统（ EMS ）中触发 AutoSupport 消息和事件，使您不仅可以直接使用运行状况监控系统，还可以使用 AutoSupport 消息和 EMS 监控系统的运行状况。

您的系统会在收到警报后五分钟内发送 AutoSupport 消息。AutoSupport 消息包括自上次 AutoSupport 消息以来生成的所有警报，但在前一周内为同一资源和可能的发生原因复制警报的警报除外。

某些警报不会触发 AutoSupport 消息。如果警报的运行状况策略禁止发送 AutoSupport 消息，则该警报不会触发 AutoSupport 消息。例如，默认情况下，运行状况策略可能会禁用 AutoSupport 消息，因为在发生问题时，AutoSupport 已生成消息。您可以使用将策略配置为不触发AutoSupport消息 `system health policy definition modify` 命令：

您可以使用查看前一周发送的所有警报触发的AutoSupport消息的列表 `system health autosupport trigger history show` 命令：

警报还会触发 EMS 事件的生成。每次创建警报以及清除警报时都会生成事件。

可用的集群运行状况监控器

有多个运行状况监控器可监控集群的不同部分。运行状况监控器可以检测事件，向您发送警报以及在清除事件后删除事件，从而帮助您从 ONTAP 系统中的错误中恢复。

运行状况监控器名称（标识符）	子系统名称（标识符）	目的
集群交换机（集群交换机）	交换机（交换机运行状况）	监控集群网络交换机和管理网络交换机的温度，利用率，接口配置，冗余（仅限集群网络交换机）以及风扇和电源运行情况。集群交换机运行状况监控器通过 SNMP 与交换机通信。SNMPv2c 是默认设置。 从 ONTAP 9.2 开始，此监控器可以检测并报告自上次轮询期间以来集群交换机重新启动的时间。
MetroCluster 网络结构	交换机	监控 MetroCluster 配置后端网络结构拓扑并检测错误配置，例如布线和分区不正确以及 ISL 故障。
MetroCluster 运行状况	互连， RAID 和存储	监控 FC-VI 适配器， FC 启动程序适配器，左后聚合和磁盘以及集群间端口
节点连接（节点连接）	CIFS 无中断运行（ CIFS-NDO ）	监控 SMB 连接，确保 Hyper-V 应用程序无中断运行。
存储（ SAS 连接）	监控节点级别的磁盘架，磁盘和适配器，以查看适当的路径和连接。	系统

运行状况监控器名称（标识符）	子系统名称（标识符）	目的
不适用	聚合来自其他运行状况监控器的信息。	系统连接（ system-connect ）

自动接收系统运行状况警报

您可以使用手动查看系统运行状况警报 `system health alert show` 命令：但是，您应订阅特定事件管理系统（ EMS ）消息，以便在运行状况监控器生成警报时自动接收通知。

关于此任务

以下操作步骤介绍了如何为所有 hm.alert.raised 消息和所有 hm.alert.cleared 消息设置通知。

所有 hm.alert.raised 消息和所有 hm.alert.cleared 消息均包含 SNMP 陷阱。SNMP陷阱的名称是 `HealthMonitorAlertRaised` 和 `HealthMonitorAlertCleared`。有关 SNMP 陷阱的信息，请参见 *Network Management Guide* 。

步骤

1. 使用 `event destination create` 命令以定义要将EMS消息发送到的目标。

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

2. 使用 `event route add-destinations` 用于路由的命令 `hm.alert.raised` 消息和 `hm.alert.cleared` 发送到目标的消息。

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

相关信息

"网络管理"

响应降级的系统运行状况

当系统的运行状况处于降级状态时，您可以显示警报，阅读可能的发生原因和更正操作，显示有关降级子系统的信息并解决问题。此外，还会显示禁止的警报，以便您可以修改这些警报并查看它们是否已确认。

关于此任务

您可以通过查看AutoSupport消息或EMS事件或使用来发现已生成警报 `system health` 命令

步骤

1. 使用 `system health alert show` 命令以查看影响系统运行状况的警报。
2. 阅读警报的可能发生原因，可能影响和更正操作，确定您是可以解决问题还是需要更多信息。
3. 如果需要详细信息、请使用 `system health alert show -instance` 命令以查看可用于警报的追加信息。
4. 使用 `system health alert modify` 命令 `-acknowledge` 参数表示您正在处理特定警报。
5. 按照中所述、采取更正操作以解决问题 `Corrective Actions` 字段。

   更正操作可能包括重新启动系统。

   解决问题后，系统将自动清除警报。如果此子系统没有其他警报、则此子系统的运行状况将更改为 `OK`。如果所有子系统的运行状况均正常、则整体系统运行状况将更改为 `OK`。

6. 使用 `system health status show` 命令以确认系统运行状况是否为 `OK`。

   如果系统运行状况不是 `OK`，重复此操作步骤。

响应降级的系统运行状况的示例

通过查看因磁盘架缺少节点的两个路径而导致系统运行状况降级的具体示例，您可以查看在响应警报时命令行界面显示的内容。

启动 ONTAP 后，您将检查系统运行状况并发现状态为 degraded：

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

您将显示警报以查明问题所在，并看到磁盘架 2 没有两个指向 node1 的路径：

```
      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.
```

您可以显示有关警报的详细信息以获取更多信息，包括警报 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
```

您确认警报以指示您正在处理该警报。

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

修复磁盘架 2 和节点 1 之间的布线，然后重新启动系统。然后、您再次检查系统运行状况、发现其状态为 `OK`：

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

配置集群和管理网络交换机的发现

集群交换机运行状况监控器会自动尝试使用 Cisco 发现协议（ CDP ）发现集群和管理网络交换机。如果运行状况监控器无法自动发现交换机，或者您不想使用 CDP 进行自动发现，则必须对其进行配置。

关于此任务

。 `system cluster-switch show` 命令可列出运行状况监控器发现的交换机。如果未在该列表中看到预期显示的交换机，则运行状况监控器将无法自动发现它。

步骤

1. 如果要使用CDP进行自动发现、请执行以下操作：

   a. 确保已在交换机上启用 Cisco 发现协议（ CDP ）。

      有关说明，请参见交换机文档。

   b. 在集群中的每个节点上运行以下命令，以验证是否已启用 CDP ：

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

      如果启用了 CDP ，请转至步骤 d如果 CDP 已禁用，请转至步骤 C

   c. 运行以下命令以启用 CDP ：

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

   请等待五分钟，然后再执行下一步。

   a. 使用 `system cluster-switch show` 命令以验证ONTAP现在是否可以自动发现交换机。

2. 如果运行状况监控器无法自动发现交换机、请使用 `system cluster-switch create` 用于配置交换机发现的命令：

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

   请等待五分钟，然后再执行下一步。

3. 使用 `system cluster-switch show` 命令以验证ONTAP是否可以发现您为其添加了信息的交换机。

完成后

验证运行状况监控器是否可以监控您的交换机。

验证对集群和管理网络交换机的监控

集群交换机运行状况监控器会自动尝试监控其发现的交换机；但是，如果交换机配置不正确，监控可能不会自动进行。您应验证是否已正确配置运行状况监控器以监控交换机。

步骤

1. 要确定集群交换机运行状况监控器发现的交换机、请输入以下命令：

   ONTAP 9.8及更高版本

   ```
   system switch ethernet show
   ```

   ONTAP 9.7及更早版本

   ```
   system cluster-switch show
   ```

   如果 `Model` 列显示值 `OTHER`，则ONTAP无法监控交换机。ONTAP会将此值设置为 `OTHER` 如果自动发现的交换机不支持运行状况监控。

   > 如果命令输出中未显示交换机、则必须配置交换机发现。

2. 升级到支持的最新交换机软件，并参考 NetApp 支持站点上的配置文件 (RCF)。

   "NetApp支持下载页面"

   交换机 RCF 中的社区字符串必须与配置为运行状况监控器使用的社区字符串匹配。默认情况下、运行状况监控器使用社区字符串 `cshm1!`。

   > 目前、运行状况监控器仅支持SNMPv2。

   如果需要更改有关集群监控的交换机的信息、可以使用以下命令修改运行状况监控器使用的社区字符串：

   ONTAP 9.8及更高版本

   ```
   system switch ethernet modify
   ```

   ONTAP 9.7及更早版本

   ```
   system cluster-switch modify
   ```

3. 验证交换机的管理端口是否已连接到管理网络。

   要执行 SNMP 查询，需要此连接。

用于监控系统运行状况的命令

您可以使用 `system health` 用于显示系统资源运行状况信息、响应警报以及配置未来警报的命令。使用命令行界面命令，您可以深入查看有关如何配置运行状况监控的信息。这些命令的手册页包含更多信息。

显示系统运行状况的状态

如果您要 ...	使用此命令 ...
显示系统的运行状况，其中反映了各个运行状况监控器的整体状态	`system health status show`
显示运行状况监控可用的子系统的运行状况	`system health subsystem show`

显示节点连接的状态

如果您要 ...	使用此命令 ...
显示有关从节点到存储架的连接的详细信息，包括端口信息， HBA 端口速度， I/O 吞吐量以及每秒 I/O 操作速率	`storage shelf show -connectivity` 使用 `-instance` 用于显示每个磁盘架详细信息的参数。
显示有关驱动器和阵列 LUN 的信息，包括可用空间，磁盘架和托架编号以及所属节点名称	`storage disk show` 使用 `-instance` 用于显示每个驱动器的详细信息的参数。
显示有关存储架端口的详细信息，包括端口类型，速度和状态	`storage port show` 使用 `-instance` 用于显示每个适配器详细信息的参数。

管理集群、存储和管理网络交换机的发现

如果您要 ...	使用此命令。**(ONTAP 9.8**及更高版本**)**	使用此命令。**(ONTAP 9.7**及更早版本**)**
显示集群监控的交换机	`system switch ethernet show`	`system cluster-switch show`

如果您要 ...	使用此命令。(ONTAP 9.8及更高版本)	使用此命令。(ONTAP 9.7及更早版本)
显示集群当前监控的交换机，包括您删除的交换机（显示在命令输出的原因列中）以及通过网络访问集群和管理网络交换机所需的配置信息。 此命令可在高级权限级别下使用。	`system switch ethernet show-all`	`system cluster-switch show-all`
配置发现未发现的交换机	`system switch ethernet create`	`system cluster-switch create`
修改有关集群监控的交换机的信息（例如，设备名称， IP 地址，SNMP 版本和社区字符串）	`system switch ethernet modify`	`system cluster-switch modify`
禁用对交换机的监控	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
禁用对交换机的发现和监控，并删除交换机配置信息	`system switch ethernet delete`	`system cluster-switch delete`
永久删除存储在数据库中的交换机配置信息（这样做会重新启用交换机的自动发现）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
启用自动日志记录以随 AutoSupport 消息一起发送。	`system switch ethernet log`	`system cluster-switch log`

响应生成的警报

如果您要 ...	使用此命令 ...
显示有关生成的警报的信息，例如触发警报的资源和节点，警报的严重性和可能的发生原因	`system health alert show`
显示有关生成的每个警报的信息	`system health alert show -instance`
指示有人正在处理警报	`system health alert modify`
确认警报	`system health alert modify -acknowledge`
禁止后续警报，使其不会影响子系统的运行状况	`system health alert modify -suppress`

如果您要 ...	使用此命令 ...
删除未自动清除的警报	`system health alert delete`
显示有关上周触发警报的 AutoSupport 消息的信息，例如，确定警报是否触发 AutoSupport 消息	`system health autosupport trigger history show`

配置未来警报

如果您要 ...	使用此命令 ...
启用或禁用控制特定资源状态是否引发特定警报的策略	`system health policy definition modify`

显示有关如何配置运行状况监控的信息

如果您要 ...	使用此命令 ...
显示有关运行状况监控器的信息，例如其节点，名称，子系统和状态	`system health config show` 使用 `-instance` 参数、用于显示有关每个运行状况监控器的详细信息。
显示有关运行状况监控器可能生成的警报的信息	`system health alert definition show` 使用 `-instance` 用于显示有关每个警报定义的详细信息的参数。
显示有关运行状况监控策略的信息，这些策略可确定何时发出警报	`system health policy definition show` 使用 `-instance` 参数以显示有关每个策略的详细信息。使用其他参数筛选警报列表，例如，按策略状态（是否已启用），运行状况监控器，警报等进行筛选。

显示环境信息

传感器可帮助您监控系统的环境组件。您可以显示的环境传感器信息包括其类型，名称，状态，值和阈值警告。

步骤

1. 要显示有关环境传感器的信息、请使用 `system node environment sensors show` 命令：