



Monitoring des Systemzustands

ONTAP 9

NetApp
April 24, 2024

Inhalt

Monitoring des Systemzustands	1
Überwachen Sie den Systemzustand Ihrer Systemübersicht	1
Funktionsweise der Statusüberwachung	1
Möglichkeiten zur Reaktion auf Systemzustandsmeldungen	2
Anpassung der Systemzustandsmeldung	2
Wie Systemzustandsmeldungen AutoSupport Meldungen und Ereignisse auslösen	3
Verfügbare Cluster-Zustandsmonitore	3
Automatisches Empfangen von SystemSystemzustandsmeldungen	5
Reagieren Sie auf den eingeschränkten Systemzustand	5
Beispiel der Reaktion auf den eingeschränkten Systemzustand	6
Konfigurieren der Erkennung von Cluster- und Management-Netzwerk-Switches	9
Überprüfen Sie die Überwachung von Cluster- und Managementnetzwerk-Switches	10
Befehle für das Monitoring des Systemzustands Ihres Systems	11
Zeigt Umgebungsinformationen an	14

Monitoring des Systemzustands

Überwachen Sie den Systemzustand Ihrer Systemübersicht

Zustandsüberwachung überwachen proaktiv bestimmte kritische Bedingungen in Ihrem Cluster und Warnmeldungen, wenn ein Fehler oder Risiko erkannt wird, aus. Wenn aktive Meldungen vorliegen, wird der Systemzustand den Status des Systems für das Cluster mit einem Status „beeinträchtigt“ angezeigt. Die Meldungen enthalten die Informationen, die Sie benötigen, um auf den beeinträchtigten Systemzustand zu reagieren.

Wenn der Status „beeinträchtigt“ lautet, können Sie Details zum Problem anzeigen, einschließlich der wahrscheinlichen Ursache und der empfohlenen Wiederherstellungsmaßnahmen. Nachdem Sie das Problem behoben haben, kehrt der Systemzustand automatisch zu OK zurück.

Der Systemzustand gibt mehrere separate Integritätsmonitore wieder. Ein Status „beeinträchtigt“ in einer einzelnen Systemzustandsüberwachung bewirkt einen Status „beeinträchtigt“ für den gesamten Systemzustand.

Details dazu, wie ONTAP Cluster Switches für die Überwachung des Systemzustands im Cluster unterstützt, finden Sie unter *Hardware Universe*.

["Unterstützte Switches im Hardware Universe"](#)

Einzelheiten zu den Ursachen von AutoSupport-Meldungen (Cluster Switch Health Monitor, CSHM) und den zur Behebung dieser Warnmeldungen erforderlichen Maßnahmen finden Sie im Knowledgebase Artikel.

["AutoSupport Meldung: Health Monitor Prozess CSHM"](#)

Funktionsweise der Statusüberwachung

Individuelle Systemzustandsüberwachung verfügen über eine Reihe von Richtlinien, die Warnungen auslösen, wenn bestimmte Bedingungen auftreten. Wenn Sie verstehen, wie das Statusüberwachung funktioniert, können Sie auf Probleme reagieren und zukünftige Warnmeldungen steuern.

Die Statusüberwachung besteht aus den folgenden Komponenten:

- Individuelle Gesundheitsmonitore für bestimmte Subsysteme, von denen jeder seinen eigenen Gesundheitszustand hat

Beispielsweise verfügt das Storage-Subsystem über eine Systemzustandsüberwachung für die Node-Konnektivität.

- Eine allgemeine Systemzustandsüberwachung, die den Systemzustand der einzelnen Systemzustandsüberwachung konsolidiert

Ein Status „beeinträchtigt“ in einem einzelnen Subsystem führt zu einem Status „beeinträchtigt“ für das gesamte System. Wenn keine Subsysteme Warnmeldungen enthalten, ist der gesamte Systemstatus OK.

Jede Systemzustandsüberwachung setzt sich aus den folgenden wichtigen Elementen zurück:

- Meldungen, die von der Systemzustandsüberwachung potenziell angehoben werden können

Jede Meldung hat eine Definition, die Details wie den Schweregrad der Warnmeldung und die wahrscheinliche Ursache enthält.

- Integritätsrichtlinien, die festlegen, wann jede Meldung ausgelöst wird

Jede Systemzustandsüberwachung verfügt über einen Regelausdruck. Dies ist die genaue Bedingung oder Änderung, durch die die Meldung ausgelöst wird.

Eine Systemzustandsüberwachung überwacht kontinuierlich die Ressourcen in ihrem Subsystem auf ihre Zustandsänderungen. Wenn eine Änderung einer Bedingung oder eines Status mit einem Regelausdruck in einer Systemzustandsüberwachung übereinstimmt, erhöht die Systemzustandsüberwachung eine Meldung. Eine Meldung bewirkt, dass der Systemzustand des Subsystems und der gesamte Systemzustand beeinträchtigt werden.

Möglichkeiten zur Reaktion auf Systemzustandsmeldungen

Wenn eine Systemzustandsmeldung auftritt, können Sie sie bestätigen, mehr darüber erfahren, den zugrunde liegenden Zustand reparieren und verhindern, dass er erneut auftritt.

Wenn eine Systemzustandsüberwachung eine Meldung aufwirft, können Sie auf folgende Arten reagieren:

- Informieren Sie sich über die Meldung, zu der die betroffene Ressource, der Schweregrad der Warnmeldung, die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen gehören.
- Detaillierte Informationen über die Warnmeldung, z. B. den Zeitpunkt, zu dem die Warnmeldung ausgegeben wurde und ob jemand anderer die Warnmeldung bereits bestätigt hat.
- Abrufen von Systemzustandsinformationen zum Status der betroffenen Ressource oder Subsysteme, z. B. ein bestimmtes Shelf oder eine bestimmte Festplatte
- Bestätigen Sie den Alarm, um anzuzeigen, dass jemand an dem Problem arbeitet und identifizieren Sie sich als „Danker“.
- Beheben Sie das Problem, indem Sie die in der Warnmeldung angegebenen Korrekturmaßnahmen ergreifen, z. B. Kabelbefestigung zur Behebung eines Verbindungsproblems.
- Löschen Sie die Meldung, wenn sie vom System nicht automatisch gelöscht wurde.
- Unterdrücken einer Meldung, um zu verhindern, dass sie den Integritätsstatus eines Subsystems beeinflusst.

Das Unterdrücken ist nützlich, wenn Sie ein Problem verstehen. Nachdem Sie eine Meldung unterdrückt haben, kann sie weiterhin auftreten, der Systemzustand des Subsystems wird jedoch als „ok-with-underdrückung“ angezeigt, wenn die unterdrückte Meldung auftritt.

Anpassung der Systemzustandsmeldung

Sie können steuern, welche Meldungen eine Systemzustandsüberwachung generiert, indem Sie die Systemintegritätsrichtlinien aktivieren und deaktivieren, die definieren, wann Meldungen ausgelöst werden. So können Sie das System zur Statusüberwachung

für Ihre spezifische Umgebung anpassen.

Sie können den Namen einer Richtlinie erlernen, indem Sie ausführliche Informationen über eine generierte Meldung anzeigen oder Richtliniendefinitionen für eine bestimmte Systemzustandsüberwachung, Node oder Alarm-ID anzeigen.

Das Deaktivieren von Integritätsrichtlinien unterscheidet sich vom Unterdrücken von Meldungen. Wenn Sie eine Meldung unterdrücken, hat dies keine Auswirkung auf den Systemzustand des Subsystems, aber die Meldung kann immer noch auftreten.

Wenn Sie eine Richtlinie deaktivieren, löst die im Richtlinienausdruck definierte Bedingung oder der Status keine Meldung mehr aus.

Beispiel für eine Meldung, die Sie deaktivieren möchten

Angenommen, eine Meldung tritt auf, die für Sie nicht hilfreich ist. Sie verwenden das `system health alert show -instance` Befehl zum Abrufen der Richtlinien-ID für die Meldung. Sie verwenden die Richtlinien-ID im `system health policy definition show` Befehl zum Anzeigen von Informationen zur Richtlinie. Nachdem Sie den Regelausdruck und andere Informationen über die Richtlinie geprüft haben, entscheiden Sie, die Richtlinie zu deaktivieren. Sie verwenden das `system health policy definition modify` Befehl zum Deaktivieren der Richtlinie

Wie Systemzustandsmeldungen AutoSupport Meldungen und Ereignisse auslösen

Systemzustandsmeldungen lösen AutoSupport-Meldungen und Ereignisse im Event Management System (EMS) aus, so dass Sie den Systemzustand mithilfe von AutoSupport-Meldungen und dem EMS sowie die direkte Verwendung des Integritätsüberwachungssystems überwachen können.

Das System sendet eine AutoSupport Meldung innerhalb von fünf Minuten nach einer Meldung. Die AutoSupport Meldung enthält alle seit der letzten AutoSupport Meldung generierten Warnmeldungen, mit Ausnahme von Warnungen, die eine Meldung für dieselbe Ressource und wahrscheinliche Ursache innerhalb der vorherigen Woche duplizieren.

Einige Meldungen lösen keine AutoSupport-Meldungen aus. Eine Meldung löst keine AutoSupport Meldung aus, wenn ihre Integritätsrichtlinie das Senden von AutoSupport Meldungen deaktiviert. Beispielsweise kann eine Systemzustandsüberwachung standardmäßig AutoSupport Meldungen deaktivieren, da AutoSupport bereits eine Meldung generiert, wenn das Problem auftritt. Sie können Richtlinien so konfigurieren, dass AutoSupport-Meldungen nicht mit dem ausgelöst werden `system health policy definition modify` Befehl.


Sie können eine Liste aller AutoSupport Meldungen, die in der vorherigen Woche über die gesendet wurden, anzeigen `system health autosupport trigger history show` Befehl.

Warnmeldungen auslösen außerdem die Generierung von Ereignissen an das EMS. Jedes Mal, wenn eine Meldung erstellt wird, wird ein Ereignis generiert, wenn eine Meldung gelöscht wird.

Verfügbare Cluster-Zustandsmonitore

Verschiedene Systemzustandsüberwachung überwachen verschiedene Teile eines Clusters. Die Zustandsüberwachung unterstützen Sie bei der Wiederherstellung nach

Fehlern in ONTAP Systemen. Dazu werden Ereignisse erkannt, Warnmeldungen an Sie gesendet und Ereignisse gelöscht, sobald sie gelöscht werden.

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Cluster-Switch (Cluster-Switch)	Switch (Switch-Health)	<p>Überwacht Cluster-Netzwerk-Switches und Management-Netzwerk-Switches auf Temperatur, Auslastung, Schnittstellenkonfiguration, Redundanz (nur Cluster-Netzwerk-Switches) sowie Lüfter- und Netzteilbetrieb. Die Cluster-Switch-Systemzustandsüberwachung kommuniziert mit Switches über SNMP. SNMPv2c ist die Standardeinstellung.</p> <div>  <p>Ab ONTAP 9.2 kann dieser Monitor erkennen und melden, wenn ein Cluster-Switch seit der letzten Abrufzeit neu gestartet wurde.</p> </div>
MetroCluster Fabric	Switch	Überwacht die Back-End-Fabric-Topologie der MetroCluster Konfiguration und erkennt Fehlkonfigurationen wie falsche Verkabelung und Zoning oder ISL-Ausfälle.
Systemzustand von MetroCluster	Interconnect, RAID und Storage	Überwacht FC-VI-Adapter, FC Initiator-Adapter, Aggregate und Festplatten im Hintergrund sowie Cluster-Ports
Node-Konnektivität (Node-Connect)	Unterbrechungsfreier CIFS-Betrieb (CIFS-NDO)	Überwachung von SMB-Verbindungen für unterbrechungsfreien Betrieb von Hyper-V Applikationen
Storage (SAS-Connect)	Überwacht Shelves, Festplatten und Adapter auf Node-Ebene für entsprechende Pfade und Verbindungen.	System

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Keine Angabe	Fasst Informationen aus anderen Zustandsmonitoren zusammen.	Systemkonnektivität (System-connect)

Automatisches Empfangen von Systemzustandsmeldungen

Sie können Systemzustandsmeldungen manuell mit der `anzeigen system health alert show` Befehl. Sie sollten jedoch bestimmte EMS-Meldungen (Event Management System) abonnieren, um Benachrichtigungen automatisch zu erhalten, wenn eine Systemzustandsüberwachung eine Meldung generiert.

Über diese Aufgabe

Das folgende Verfahren zeigt Ihnen, wie Sie Benachrichtigungen für alle `hm.alert.alert.hopped` Nachrichten und alle `hm.alert.cleaned` Nachrichten einrichten.

Alle `hm.alert.alerted` Nachrichten und alle `hm.alert.cleaned` Nachrichten enthalten einen SNMP-Trap. Die Namen der SNMP-Traps sind `HealthMonitorAlertRaised` Und `HealthMonitorAlertCleared`. Informationen zu SNMP-Traps finden Sie im *Network Management Guide*.

Schritte

1. Verwenden Sie die `event destination create` Befehl zum Festlegen des Ziels, an das Sie die EMS-Nachrichten senden möchten.

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

2. Verwenden Sie die `event route add-destinations` Befehl zum Umleiten des `hm.alert.raised` Botschaft und der `hm.alert.cleaned` Nachricht an ein Ziel senden.

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

Verwandte Informationen

["Netzwerkmanagement"](#)

Reagieren Sie auf den eingeschränkten Systemzustand

Wenn der Systemzustand des Systems beeinträchtigt ist, können Sie Meldungen anzeigen, die wahrscheinliche Ursache und die möglichen Korrekturmaßnahmen lesen, Informationen zum beeinträchtigten Subsystem anzeigen und das Problem lösen.

Unterdrückte Warnungen werden ebenfalls angezeigt, damit Sie sie ändern und sehen können, ob sie bestätigt wurden.

Über diese Aufgabe

Sie können feststellen, dass eine Meldung durch die Anzeige einer AutoSupport Meldung, eines EMS-Ereignisses oder mithilfe des generiert wurde `system health` Befehle.

Schritte

1. Verwenden Sie die `system health alert show` Befehl zum Anzeigen der Meldungen, die den Systemzustand beeinträchtigen.
2. Lesen Sie die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen der Meldung, um zu ermitteln, ob Sie das Problem beheben oder weitere Informationen benötigen.
3. Wenn Sie weitere Informationen benötigen, verwenden Sie das `system health alert show -instance` Befehl zum Anzeigen weiterer Informationen, die für die Meldung verfügbar sind.
4. Verwenden Sie die `system health alert modify` Befehl mit dem `-acknowledge` Parameter, um anzugeben, dass Sie an einer bestimmten Warnmeldung arbeiten.
5. Führen Sie Korrekturmaßnahmen durch, um das Problem zu lösen, wie im beschriebenen `Corrective Actions` Feld in der Meldung.

Die Korrekturmaßnahmen können ein Neubooten des Systems umfassen.

Nach Behebung des Problems wird die Meldung automatisch behoben. Wenn das Subsystem keine weiteren Warnmeldungen aufweist, ändert sich der Systemzustand des Subsystems in `OK`. Wenn der Systemzustand aller Subsysteme in Ordnung ist, ändert sich der Gesamtzustand des Systems in `OK`.

6. Verwenden Sie die `system health status show` Befehl zur Bestätigung, dass der Systemzustand lautet `OK`.

Wenn der Systemstatus nicht lautet `OK`, Wiederholen Sie dieses Verfahren.

Beispiel der Reaktion auf den eingeschränkten Systemzustand

Durch Überprüfung eines bestimmten Beispiels des beeinträchtigten Systemzustands, der durch ein Shelf verursacht wurde, in dem zwei Pfade zu einem Node fehlen, werden Sie sehen, was die CLI zeigt, wenn Sie auf eine Meldung antworten.

Nach dem Starten von ONTAP überprüfen Sie den Systemzustand, und Sie stellen fest, dass der Status „beeinträchtigt“ lautet:

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

Sie zeigen die Meldungen an, um herauszufinden, wo das Problem ist, und sehen, dass Shelf 2 keine zwei

Pfade zu node1 hat:

```
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.
```

Sie zeigen Details über die Meldung an, um weitere Informationen zu erhalten, einschließlich der Warn-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

```

Sie bestätigen die Meldung, dass Sie daran arbeiten.

```

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

```

Sie reparieren die Verkabelung zwischen Shelf 2 und node1 und booten das System dann neu. Anschließend überprüfen Sie den Systemzustand wieder und sehen, dass der Status lautet OK:

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

Konfigurieren der Erkennung von Cluster- und Management-Netzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Cluster- und Management-Netzwerk-Switches mithilfe des Cisco Discovery Protocol (CDP) zu erkennen. Sie müssen die Systemzustandsüberwachung konfigurieren, wenn ein Switch nicht automatisch erkannt werden kann oder wenn Sie nicht für die automatische Erkennung CDP verwenden möchten.

Über diese Aufgabe

Der `system cluster-switch show` Mit dem Befehl werden die Switches aufgeführt, die die Systemzustandsüberwachung erkannt hat. Wenn für Sie keinen Schalter in der Liste angezeigt wird, kann die Systemzustandsüberwachung ihn nicht automatisch erkennen.

Schritte

1. Wenn Sie CDP für die automatische Erkennung verwenden möchten, gehen Sie wie folgt vor:

a. Stellen Sie sicher, dass das Cisco Discovery Protocol (CDP) auf Ihren Switches aktiviert ist.

Anweisungen hierzu finden Sie in der Switch-Dokumentation.

b. Führen Sie für jeden Knoten im Cluster den folgenden Befehl aus, um zu überprüfen, ob CDP aktiviert oder deaktiviert ist:

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

Wenn CDP aktiviert ist, fahren Sie mit Schritt d. fort Wenn CDP deaktiviert ist, mit Schritt c fortfahren

c. Führen Sie den folgenden Befehl aus, um CDP zu aktivieren:

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

Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

a. Verwenden Sie die `system cluster-switch show` Befehl zum Überprüfen, ob ONTAP die Switches jetzt automatisch erkennen kann.

2. Wenn die Systemzustandsüberwachung keinen Switch automatisch erkennt, verwenden Sie den `system cluster-switch create` Befehl zum Konfigurieren der Erkennung des Switches:

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

Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

3. Verwenden Sie die `system cluster-switch show` Befehl um zu überprüfen, ob ONTAP den Switch erkennen kann, für den Sie Informationen hinzugefügt haben.

Nachdem Sie fertig sind

Überprüfen Sie, ob die Systemzustandsüberwachung Ihre Switches überwachen kann.

Überprüfen Sie die Überwachung von Cluster- und Managementnetzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Switches zu überwachen, die sie erkannt haben. Die Überwachung erfolgt jedoch möglicherweise nicht automatisch, wenn die Switches nicht richtig konfiguriert sind. Sie sollten überprüfen, ob die Systemzustandsüberwachung ordnungsgemäß für das Monitoring Ihrer Switches konfiguriert ist.

Schritte

1. Geben Sie den folgenden Befehl ein, um die Switches zu identifizieren, die die Systemzustandsüberwachung des Cluster-Switch erkannt haben:

ONTAP 9.8 und höher

```
system switch ethernet show
```

ONTAP 9.7 und früher

```
system cluster-switch show
```

Wenn der `Model` Spalte zeigt den Wert an `OTHER`, Dann kann ONTAP den Schalter nicht überwachen. ONTAP setzt den Wert auf `OTHER` Wenn ein automatisch erkannte Switch nicht für das Monitoring des Systemzustands unterstützt wird.



Wenn in der Befehlsausgabe des Befehls kein Switch angezeigt wird, müssen Sie die Erkennung des Switches konfigurieren.

2. Führen Sie ein Upgrade auf die neueste unterstützte Switch-Software durch, und verwenden Sie die Konfigurationsdatei (RCF) von der NetApp Support Site.

["NetApp Support Downloads Seite"](#)

Die Community-Zeichenfolge in der RCF des Switches muss mit der Community-Zeichenfolge übereinstimmen, die die Systemzustandsüberwachung konfiguriert ist. Standardmäßig verwendet die Systemzustandsüberwachung die Community-Zeichenfolge `cshml!`.



Derzeit unterstützt die Systemzustandsüberwachung nur SNMPv2.

Wenn Sie Informationen über einen Switch ändern müssen, der vom Cluster überwacht wird, können Sie den Community-String, den die Systemzustandsüberwachung mit dem folgenden Befehl verwendet, ändern:

ONTAP 9.8 und höher

```
system switch ethernet modify
```

ONTAP 9.7 und früher

```
system cluster-switch modify
```

3. Vergewissern Sie sich, dass der Managementport des Switch mit dem Managementnetzwerk verbunden ist.

Diese Verbindung ist erforderlich, um SNMP-Abfragen durchzuführen.

Befehle für das Monitoring des Systemzustands Ihres Systems

Sie können das verwenden `system health` Befehle zum Anzeigen von Informationen über den Systemzustand der Systemressourcen, zum Reagieren auf Meldungen und zum Konfigurieren zukünftiger Warnmeldungen. Mithilfe der CLI-Befehle können Sie detaillierte Informationen über das Konfigurieren des Systemzustands anzeigen. Die man-Pages für die Befehle enthalten weitere Informationen.

Zeigt den Status des Systemzustands an

Ihr Ziel ist	Befehl
Anzeigen des Integritätsstatus des Systems, der den Gesamtstatus einzelner Integritätsmonitore wiedergibt	<code>system health status show</code>
Anzeigen des Funktionszustands von Subsystemen, für die ein Zustandsüberwachung verfügbar ist	<code>system health subsystem show</code>

Zeigt den Status der Node-Konnektivität an

Ihr Ziel ist	Befehl
Zeigt Details zur Konnektivität vom Node zum Storage Shelf an, einschließlich Portinformationen, HBA-Port-Geschwindigkeit, I/O-Durchsatz und der Geschwindigkeit von I/O-Vorgängen pro Sekunde	<code>storage shelf show -connectivity</code> Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jedem Shelf.

Ihr Ziel ist	Befehl
Anzeigen von Informationen zu Laufwerken und Array-LUNs, einschließlich des nutzbaren Speicherplatzes, Shelf- und Einschubnummern sowie des eigenen Node-Namens	<code>storage disk show</code> Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jedem Laufwerk.
Zeigt detaillierte Informationen über Storage-Shelf-Ports an, einschließlich Porttyp, Geschwindigkeit und Status	<code>storage port show</code> Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu den einzelnen Adaptern.

Managen Sie die Erkennung von Cluster-, Storage- und Management-Netzwerk-Switches

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Zeigen Sie die Switches an, die das Cluster überwacht	<code>system switch ethernet show</code>	<code>system cluster-switch show</code>
Zeigen Sie die Switches an, die das Cluster derzeit überwacht, einschließlich der von Ihnen gelöschten Switches (siehe Spalte „Grund“ der Befehlsausgabe), und Konfigurationsinformationen, die Sie für den Netzwerkzugriff auf das Cluster und auf die Management-Netzwerk-Switches benötigen. Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.	<code>system switch ethernet show-all</code>	<code>system cluster-switch show-all</code>
Konfigurieren Sie die Erkennung eines nicht erkannten Switches	<code>system switch ethernet create</code>	<code>system cluster-switch create</code>
Ändern von Informationen über einen vom Cluster überwachten Switch (z. B. Gerätenamen, IP-Adresse, SNMP-Version und Community String)	<code>system switch ethernet modify</code>	<code>system cluster-switch modify</code>
Deaktivieren Sie die Überwachung eines Switches	<code>system switch ethernet modify -disable-monitoring</code>	<code>system cluster-switch modify -disable-monitoring</code>

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Deaktivieren Sie die Erkennung und Überwachung eines Switch und löschen Sie die Switch-Konfigurationsinformationen	<code>system switch ethernet delete</code>	<code>system cluster-switch delete</code>
Entfernen Sie die in der Datenbank gespeicherten Switch-Konfigurationsinformationen dauerhaft (wodurch die automatische Erkennung des Switch wieder möglich ist).	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
Aktivieren Sie die automatische Protokollierung zum Senden mit AutoSupport-Nachrichten.	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>




Reagieren Sie auf generierte Warnmeldungen

Ihr Ziel ist	Befehl
Anzeige von Informationen zu generierten Meldungen, z. B. Ressource und Node, auf dem die Meldung ausgelöst wurde, sowie des Schweregrads und der wahrscheinlichen Ursache der Meldung	<code>system health alert show</code>
Zeigt Informationen zu jeder generierten Meldung an	<code>system health alert show -instance</code>
Geben Sie an, dass jemand an einer Warnung arbeitet	<code>system health alert modify</code>
Bestätigen Sie eine Meldung	<code>system health alert modify -acknowledge</code>
Unterdrücken Sie eine nachfolgende Meldung, damit sie den Integritätsstatus eines Subsystems nicht beeinflusst	<code>system health alert modify -suppress</code>
Löschen Sie eine Meldung, die nicht automatisch gelöscht wurde	<code>system health alert delete</code>
Informationen zu den AutoSupport Meldungen, die innerhalb der letzten Woche ausgelöst wurden, anzeigen, um z. B. zu bestimmen, ob eine Meldung eine AutoSupport Meldung ausgelöst hat	<code>system health autosupport trigger history show</code>

Konfigurieren Sie zukünftige Warnmeldungen

Ihr Ziel ist	Befehl
Aktivieren oder deaktivieren Sie die Richtlinie, die steuert, ob ein bestimmter Ressourcenzustand eine bestimmte Warnmeldung ausgibt	<code>system health policy definition modify</code>

Zeigt Informationen zur Konfiguration der Systemzustandsüberwachung an

Ihr Ziel ist	Befehl
Anzeigen von Informationen über Systemzustandsüberwachung, z. B. ihre Nodes, Namen, Subsysteme und Status	<code>system health config show</code>  Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Systemzustandsüberwachung.
Zeigen Sie Informationen zu den Meldungen an, die eine Systemzustandsüberwachung möglicherweise generiert werden kann	<code>system health alert definition show</code>  Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Meldungsdefinition.
Anzeigen von Informationen über Richtlinien der Systemzustandsüberwachung, die bestimmen, wann Meldungen ausgegeben werden	<code>system health policy definition show</code>  Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Richtlinie. Verwenden Sie andere Parameter, um die Meldungsliste zu filtern, z. B. nach Richtlinienstatus (aktiviert oder nicht), Systemzustandsüberwachung, Meldung usw.

Zeigt Umgebungsinformationen an

Sensoren helfen Ihnen dabei, die Umgebungskomponenten Ihres Systems zu überwachen. Die Informationen, die Sie zu Umgebungssensoren anzeigen können, umfassen ihren Typ, ihren Namen, den Zustand, ihren Wert und ihre Schwellenwerte.

Schritt

1. Verwenden Sie das, um Informationen zu Umgebungssensoren anzuzeigen `system node environment sensors show` Befehl.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.