



# **Monitoring des Systemzustands**

## **ONTAP 9**

NetApp  
January 08, 2026

# Inhalt

Monitoring des Systemzustands .....	1
Erfahren Sie mehr über die Überwachung des Systemzustands mit ONTAP .....	1
Erfahren Sie mehr über die Monitoring-Komponenten von ONTAP .....	1
Erfahren Sie mehr über die Reaktion von ONTAP Systemzustandsmeldungen .....	2
Erfahren Sie mehr über die Anpassung von ONTAP Systemzustandswarnmeldungen .....	3
Weitere Informationen zu ONTAP AutoSupport-Systemzustandswarnauslösern .....	3
Erfahren Sie mehr über verfügbare Systemzustandsüberwacher für ONTAP Cluster .....	4
Automatischer Empfang von ONTAP Systemzustandsmeldungen .....	5
Reaktion auf beeinträchtigten Zustand des ONTAP-Systems .....	6
Erfahren Sie mehr über die Reaktion auf den beeinträchtigten Zustand des ONTAP-Systems .....	7
Befehle zum Monitoring des Systemzustands Ihres ONTAP Systems .....	9
Zeigt den Status des Systemzustands an .....	9
Zeigt den Status der Node-Konnektivität an .....	9
Monitoring von Cluster- und Storage-Netzwerk-Switches .....	10
Reagieren Sie auf generierte Warnmeldungen .....	11
Konfigurieren Sie zukünftige Warnmeldungen .....	11
Zeigt Informationen zur Konfiguration der Systemzustandsüberwachung an .....	11
Zeigen Sie Umgebungsinformationen zu ONTAP an .....	12

# Monitoring des Systemzustands

## Erfahren Sie mehr über die Überwachung des Systemzustands mit ONTAP

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"](#)

## Erfahren Sie mehr über die Monitoring-Komponenten von ONTAP

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.

## **Erfahren Sie mehr über die Reaktion von ONTAP 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.

# Erfahren Sie mehr über die Anpassung von ONTAP Systemzustandswarmmeldungen

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 den `system health alert show -instance` Befehl, um die Richtlinien-ID für die Meldung zu erhalten. Sie verwenden die Richtlinien-ID im `system health policy definition show` Befehl, um Informationen zur Richtlinie anzuzeigen. Nachdem Sie den Regelausdruck und andere Informationen über die Richtlinie geprüft haben, entscheiden Sie, die Richtlinie zu deaktivieren. Sie verwenden den `system health policy definition modify` Befehl, um die Richtlinie zu deaktivieren.

## Verwandte Informationen

- ["Systemzustandswarnung anzeigen"](#)

# Weitere Informationen zu ONTAP AutoSupport-Systemzustandswarnauslösern

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 konfigurieren, damit keine AutoSupport Meldungen mit dem `system health policy definition modify` Befehl ausgelöst werden.

Mit dem `system health autosupport trigger history show` Befehl können Sie eine Liste aller warnungsausgelösten AutoSupport-Meldungen anzeigen, die in der vergangenen Woche gesendet wurden.

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.

## Erfahren Sie mehr über verfügbare Systemzustandsüberwacher für ONTAP Cluster

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
Ethernet-Switch	Switch (Switch-Health)	<p>Der ONTAP-Netzwerkswitch-Funktionsmonitor (CSHM) überwacht den Status von Cluster- und Speichernetzwerk-Switches, während er Protokolle zur Analyse erfasst. Standardmäßig fragt CSHM jeden Switch alle 5 Minuten über SNMPv2c ab, um Ressourcentabellen mit Informationen zu Supportfähigkeit, Überwachungsstatus, Temperatursensoren, CPU-Auslastung, Schnittstellenkonfigurationen und -Verbindungen, Cluster-Switch-Redundanz sowie Lüfter- und Netzteilvorgängen zu aktualisieren. Darüber hinaus erfasst CSHM bei entsprechender Konfiguration stündlich Protokolle über SSH/SCP, die zur weiteren Analyse über AutoSupport gesendet werden. Auf Anfrage kann CSHM auch eine ausführlichere Tech-Support-Protokollsammlung mithilfe von SSH/SCP durchführen.</p> <p>Weitere Informationen finden Sie unter <a href="#">"Überwachung des Switch-Systemzustands"</a> .</p>

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

## Automatischer Empfang von ONTAP Systemzustandsmeldungen

Sie können Systemzustandsmeldungen mit dem `system health alert show` Befehl manuell anzeigen. 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 lauten `HealthMonitorAlertRaised` und `HealthMonitorAlertCleared`.

Erfahren Sie mehr über `system health alert show` in der ["ONTAP-Befehlsreferenz"](#).

### Schritte

1. ``event destination create`` Definieren Sie mit dem Befehl das Ziel, an das die EMS-Meldungen gesendet werden sollen.

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

Erfahren Sie mehr über `event destination create` in der ["ONTAP-Befehlsreferenz"](#).

2. Verwenden Sie den `event route add-destinations` Befehl, um die `hm.alert.raised` `hm.alert.cleared` Meldung und die Meldung an ein Ziel weiterzuleiten.

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

Erfahren Sie mehr über `event route add-destinations` in der ["ONTAP-Befehlsreferenz"](#).

### Verwandte Informationen

- ["Visualisierung des ONTAP Netzwerks mit System Manager"](#)
- ["So konfigurieren Sie die SNMP-Überwachung auf DATA ONTAP"](#)

## Reaktion auf beeinträchtigten Zustand des ONTAP-Systems

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 Anzeigen einer AutoSupport Nachricht, eines EMS-Ereignisses oder mithilfe der `system health` Befehle generiert wurde.

### Schritte

1. Mit dem `system health alert show` Befehl können Sie die Warnungen anzeigen, 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, können Sie mit dem `system health alert show -instance` Befehl weitere Informationen anzeigen, die für die Meldung verfügbar sind.
4. Verwenden Sie den `system health alert modify` Befehl mit dem `-acknowledge` Parameter, um anzugeben, dass Sie an einer bestimmten Meldung arbeiten.
5. Führen Sie Korrekturmaßnahmen durch, um das Problem gemäß dem `Corrective Actions` Feld in der Meldung zu lösen.

Die Korrekturmaßnahmen können ein Neubooten des Systems umfassen.

Nach Behebung des Problems wird die Meldung automatisch behoben. Wenn das Subsystem keine



anderen Warnungen hat, ändert sich der Systemzustand des Subsystems in OK. Wenn der Funktionszustand aller Subsysteme in Ordnung ist, ändert sich der Gesamtzustand OK des Systems in.

6. `system health status show` Überprüfen Sie mit dem Befehl, ob der Systemzustandsstatus lautet `OK`.

Wenn der Systemstatus nicht lautet OK, wiederholen Sie diesen Vorgang.

#### Verwandte Informationen

- ["Systemzustandswarnung ändern"](#)

## Erfahren Sie mehr über die Reaktion auf den beeinträchtigten Zustand des ONTAP-Systems

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. Dann überprüfen Sie die Systemintegrität erneut und sehen, dass der Status lautet OK:

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

#### Verwandte Informationen

- ["Systemzustandswarnung ändern"](#)

## Befehle zum Monitoring des Systemzustands Ihres ONTAP Systems

Sie können die `system health` Befehle verwenden, um Informationen zum Zustand der Systemressourcen anzuzeigen, auf Warnmeldungen zu antworten und zukünftige Warnmeldungen zu konfigurieren. Mithilfe der CLI-Befehle können Sie detaillierte Informationen über das Konfigurieren des Systemzustands anzeigen. Erfahren Sie mehr über `system health` in der ["ONTAP-Befehlsreferenz"](#).

### 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 den <code>-instance</code> Parameter, um detaillierte Informationen zu jedem Shelf anzuzeigen.
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 den <code>-instance</code> Parameter, um detaillierte Informationen zu jedem Laufwerk anzuzeigen.

Ihr Ziel ist	Befehl
Zeigt detaillierte Informationen über Storage-Shelf-Ports an, einschließlich Porttyp, Geschwindigkeit und Status	<pre>storage port show</pre> <p>Verwenden Sie den <code>-instance</code> Parameter, um detaillierte Informationen zu den einzelnen Adaptern anzuzeigen.</p>

## Monitoring von Cluster- und Storage-Netzwerk-Switches

Ihr Ziel ist	Befehl (ONTAP 9.8 und höher)	Befehl (ONTAP 9.7 und früher)
Zeigen Sie die Switches an, die das Cluster überwacht	<pre>system switch ethernet show</pre>	<pre>system cluster-switch show</pre>
<p>Zeigt die Switches an, die das Cluster derzeit überwacht, einschließlich der von Ihnen gelöschten Switches (in der Spalte „Reason“ der Befehlsausgabe angezeigt)</p> <p>Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar</p>	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
Konfigurieren Sie die Überwachung eines nicht erkannten Switches	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
Ändern von Informationen über einen vom Cluster überwachten Switch (z. B. Gerätenamen, IP-Adresse, SNMP-Version und Community String)	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
Deaktivieren Sie die Überwachung eines Switches	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
Löschen Sie einen Schalter aus der Überwachung	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>
Entfernen Sie die in der Datenbank gespeicherten Switch-Konfigurationsinformationen dauerhaft (wodurch die automatische Erkennung des Switch wieder möglich ist).	<pre>system switch ethernet delete -force</pre>	<pre>system cluster-switch delete -force</pre>

Ihr Ziel ist	Befehl (ONTAP 9.8 und höher)	Befehl (ONTAP 9.7 und früher)
Führen Sie die Protokollerfassung mit einem Switch durch	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>



Weitere Informationen finden Sie unter ["Überwachung des Switch-Systemzustands"](#) und ["Konfigurieren der Protokollerfassung"](#).




## 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	<pre>system health config show</pre> <div>  <p>Verwenden Sie den <code>-instance</code> Parameter, um detaillierte Informationen zu jeder Systemzustandsüberwachung anzuzeigen.</p> </div>
Zeigen Sie Informationen zu den Meldungen an, die eine Systemzustandsüberwachung möglicherweise generiert werden kann	<pre>system health alert definition show</pre> <div>  <p>Verwenden Sie den <code>-instance</code> Parameter, um detaillierte Informationen zu den einzelnen Meldungsdefinitionen anzuzeigen.</p> </div>
Anzeigen von Informationen über Richtlinien der Systemzustandsüberwachung, die bestimmen, wann Meldungen ausgegeben werden	<pre>system health policy definition show</pre> <div>  <p>Mit dem <code>-instance</code> Parameter können Sie detaillierte Informationen zu den einzelnen Richtlinien anzeigen. Verwenden Sie andere Parameter, um die Meldungsliste zu filtern, z. B. nach Richtlinienstatus (aktiviert oder nicht), Systemzustandsüberwachung, Meldung usw.</p> </div>

#### Verwandte Informationen

- ["Speicherport anzeigen"](#)
- ["Lagerregal anzeigen"](#)
- ["Systemzustandswarnung löschen"](#)

## Zeigen Sie Umgebungsinformationen zu ONTAP an

Sensoren helfen Ihnen dabei, die Umgebungskomponenten Ihres Systems zu überwachen. Zu den Informationen, die Sie über Umgebungssensoren anzeigen können, gehören Typ, Name, Status, Wert und Schwellenwertwarnungen.

#### Schritt

1. Um Informationen zu Umgebungssensoren anzuzeigen, verwenden Sie den `system node environment sensors show` Befehl.

## Copyright-Informationen

Copyright © 2026 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.