



# Fehler im System beheben

## Element Software

NetApp  
October 01, 2024

# Inhalt

- Fehler im System beheben ..... 1
  - Finden Sie weitere Informationen ..... 1
  - Zeigt Informationen zu Systemereignissen an ..... 1
  - Status der ausgeführten Aufgaben anzeigen ..... 5
  - Anzeigen von Systemmeldungen ..... 6
  - Zeigen Sie die Node-Performance-Aktivitäten an ..... 24
  - Anzeigen der Volume-Performance ..... 24
  - Anzeigen von iSCSI-Sitzungen ..... 26
  - Zeigen Sie Fibre-Channel-Sitzungen an ..... 28
  - Fehlerbehebung bei Laufwerken ..... 29
  - Fehlerbehebung für Nodes ..... 32
  - Storage-Nodes: Dienstprogramme pro Node unterstützen ..... 34
  - Erläuterung der Cluster-Auslastungsebenen ..... 41

# Fehler im System beheben

Sie müssen das System zu Diagnosezwecken überwachen und Informationen zu Performance-Trends und Status verschiedener Systemvorgänge erhalten. Möglicherweise müssen Sie Nodes oder SSDs zu Wartungszwecken ersetzen.

- ["Zeigt Informationen zu Systemereignissen an"](#)
- ["Status der ausgeführten Aufgaben anzeigen"](#)
- ["Anzeigen von Systemmeldungen"](#)
- ["Zeigen Sie die Node-Performance-Aktivitäten an"](#)
- ["Anzeigen der Volume-Performance"](#)
- ["Anzeigen von iSCSI-Sitzungen"](#)
- ["Zeigen Sie Fibre-Channel-Sitzungen an"](#)
- ["Fehlerbehebung bei Laufwerken"](#)
- ["Fehlerbehebung für Nodes"](#)
- ["Storage-Nodes: Dienstprogramme pro Node unterstützen"](#)
- ["Arbeiten Sie mit dem Management-Node"](#)
- ["Erläuterung der Cluster-Auslastungsebenen"](#)

## Finden Sie weitere Informationen

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

## Zeigt Informationen zu Systemereignissen an

Sie können Informationen zu verschiedenen im System erkannten Ereignissen anzeigen. Das System aktualisiert die Ereignismeldungen alle 30 Sekunden. Im Ereignisprotokoll werden wichtige Ereignisse für das Cluster angezeigt.

1. Wählen Sie in der Element-UI die Option **Berichterstellung > Ereignisprotokoll**.

Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eindeutige ID, die jedem Ereignis zugeordnet ist.
Art Des Events	Der Typ des protokollierten Ereignisses, z. B. API-Ereignisse oder Klonereignisse.
Nachricht	Dem Ereignis zugeordnete Nachricht.

Details	Informationen, mit denen der Grund des Ereignisses ermittelt werden kann.
Service-ID	Der Dienst, der das Ereignis gemeldet hat (falls zutreffend).
Knoten	Der Node, der das Ereignis gemeldet hat (falls zutreffend).
Laufwerks-ID	Das Laufwerk, das das Ereignis gemeldet hat (falls zutreffend).
Ereigniszeit	Die Zeit, zu der das Ereignis aufgetreten ist.

## Weitere Informationen

### Ereignistypen

## Ereignistypen

Das System meldet mehrere Ereignistypen. Jedes Ereignis ist ein Vorgang, den das System abgeschlossen hat. Ereignisse können Routine-, normale Ereignisse oder Ereignisse sein, die vom Administrator beachtet werden müssen. Die Spalte Ereignistypen auf der Seite Ereignisprotokoll gibt an, in welchem Teil des Systems das Ereignis aufgetreten ist.



Das System protokolliert keine schreibgeschützten API-Befehle im Ereignisprotokoll.

In der folgenden Liste werden die Arten von Ereignissen beschrieben, die im Ereignisprotokoll angezeigt werden:

- **ApiEvent**

Ereignisse, die von einem Benutzer über eine API oder eine Web-Benutzeroberfläche initiiert werden, die Einstellungen ändern.

- **BinAssignmentsEvent**

Ereignisse im Zusammenhang mit der Zuordnung von Datenfächern. Fächer sind im Wesentlichen Container, in denen Daten gespeichert und über das gesamte Cluster hinweg zugeordnet sind.

- **BinSyncEvent**

Systemereignisse zur Neuzuweisung von Daten zwischen Block-Services.

- **BsCheckEvent**

Systemereignisse im Zusammenhang mit Blockserviceüberprüfungen.

- **BsKilEvent**

Systemereignisse im Zusammenhang mit Blockdienstterminen.

- **BulkOpEvent**

Ereignisse im Zusammenhang mit Vorgängen, die auf einem gesamten Volume ausgeführt werden, z. B. Backups, Wiederherstellungen, Snapshots oder Klone

- **KlonEvent**

Ereignisse im Zusammenhang mit dem Klonen von Volumes.

- **ClusterMasterEvent**

Ereignisse, die bei der Initialisierung des Clusters oder bei Änderungen der Konfiguration im Cluster angezeigt werden, z. B. Hinzufügen oder Entfernen von Nodes

- **cSumEvent**

Ereignisse im Zusammenhang mit der Erkennung einer nicht übereinstimmenden Prüfsumme bei der Überprüfung der lückenlosen Prüfsumme.

Dienste, die eine Prüfsummenkongruenz erkennen, werden automatisch angehalten und nach der Generierung dieses Ereignisses nicht neu gestartet.

- **Datenergebnis**

Ereignisse im Zusammenhang mit dem Lesen und Schreiben von Daten.

- **DbEvent**

Veranstaltungen im Zusammenhang mit der globalen Datenbank, die von Ensemble-Knoten im Cluster gepflegt wird.

- **Auffahrt**

Ereignisse in Verbindung mit Laufwerksoperationen

- **VerschlüsselungAtRestEvent**

Ereignisse im Zusammenhang mit dem Verschlüsselungsvorgang auf einem Cluster.

- **EnsembleEvent**

Ereignisse, die sich auf die Erhöhung oder Verringerung der Anzahl der Knoten in einem Ensemble beziehen.

- **Fiber ChannelEvent**

Ereignisse in Verbindung mit der Konfiguration von und Verbindungen zu den Nodes.

- **GcEvent**

Ereignisse, die auf Prozessen zurückzuführen sind, werden alle 60 Minuten ausgeführt, um Speicher auf Blocklaufwerken zurückzugewinnen. Dieser Prozess wird auch als Garbage Collection bezeichnet.

- **leEvent**

Interner Systemfehler.

- **Installationsereignis**

Automatische Softwareinstallationsereignisse. Die Software wird automatisch auf einem ausstehenden Node installiert.

- **ISCSIEvent**

Ereignisse im Zusammenhang mit iSCSI-Problemen im System.

- **EndEvent**

Ereignisse im Zusammenhang mit der Anzahl von Volumes oder virtuellen Volumes in einem Konto oder im Cluster, die sich dem maximal zulässigen Wert nähern.

- **WartungModeEvent**

Ereignisse im Zusammenhang mit dem Wartungsmodus des Node, z. B. Deaktivieren des Node.

- **NetworkEvent**

Ereignisse im Zusammenhang mit der Netzwerkfehlerberichterstattung für jede Schnittstelle der physischen Netzwerkschnittstelle (NIC).

Diese Ereignisse werden ausgelöst, wenn eine Fehleranzahl für eine Schnittstelle einen Standardschwellenwert von 1000 in einem 10-minütigen Überwachungsintervall überschreitet. Diese Ereignisse gelten für Netzwerkfehler wie empfangene Fehlschläge, zyklische Redundanzprüfung (CRC)-Fehler, Längenfehler, Überlauffehler und Frame-Fehler.

- **HardwareEvent**

Ereignisse im Zusammenhang mit Problemen, die auf Hardware-Geräten erkannt wurden.

- \* Remote ClusterEvent\*

Ereignisse im Zusammenhang mit der Paarung von Remote-Clustern.

- **Termin**

Ereignisse im Zusammenhang mit geplanten Snapshots.

- **ServiceEvent**

Ereignisse im Zusammenhang mit dem Systemstatus.

- **SliceEvent**

Ereignisse im Zusammenhang mit dem Slice Server, z. B. Entfernen eines Metadatenlaufwerks oder eines Volumes.

Es gibt drei Arten von Ereignissen zur Umverteilung in Schichten, die Informationen über den Service enthalten, dem ein Volume zugewiesen wird:

- Umdrehen: Ändern des primären Dienstes zu einem neuen primären Service

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

- Verschieben: Ändern des sekundären Service zu einem neuen sekundären Service

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

- Beschneidung: Entfernen eines Volumes aus einer Gruppe von Diensten

```
sliceID {oldSecondaryServiceID(s)}
```

- **SnmptTrapEvent**

Ereignisse im Zusammenhang mit SNMP-Traps.

- **StatEvent**

Ereignisse in Verbindung mit Systemstatistiken.

- **TsEvent**

Ereignisse im Zusammenhang mit dem Systemtransportdienst.

- **UnexpectedException**

Ereignisse im Zusammenhang mit unerwarteten Systemausnahmen.

- **UreEvent**

Ereignisse im Zusammenhang mit nicht behebbaren Lesefehlern, die beim Lesen vom Speichergerät auftreten.

- **VasaProviderEvent**

Ereignisse in Verbindung mit einem VASA Provider (vSphere APIs for Storage Awareness)

## Status der ausgeführten Aufgaben anzeigen

Sie können den Fortschritt und den Abschlussstatus der ausgeführten Aufgaben in der Web-Benutzeroberfläche anzeigen, die von den API-Methoden ListSyncJobs und ListBulkVolumeJobs gemeldet werden. Über die Registerkarte „Reporting“ der Element-Benutzeroberfläche können Sie auf die Seite „ausgeführte Aufgaben“ zugreifen.

Wenn eine große Anzahl von Aufgaben vorhanden ist, kann das System sie in Warteschlange stellen und in Batches ausführen. Auf der Seite laufende Aufgaben werden die aktuell synchronisierten Dienste angezeigt. Wenn eine Aufgabe abgeschlossen ist, wird sie durch die nächste Synchronisierungsaufgabe in der Warteschlange ersetzt. Die Synchronisierung von Aufgaben wird möglicherweise weiterhin auf der Seite

laufende Aufgaben angezeigt, bis keine Aufgaben mehr abgeschlossen sind.



Auf der Seite laufende Aufgaben des Clusters, der das Ziel-Volume enthält, werden die Replikationsdaten für Volumes angezeigt, die die Replikation durchlaufen.

## Anzeigen von Systemmeldungen

Sie können Benachrichtigungen zu Cluster-Fehlern oder -Fehlern im System anzeigen. Warnmeldungen können Informationen, Warnungen oder Fehler sein und ein guter Indikator für die inwieweit das Cluster läuft. Die meisten Fehler lösen sich automatisch.

Sie können die API-Methode ListClusterStandards verwenden, um die Alarmüberwachung zu automatisieren. So können Sie über alle auftretenden Warnmeldungen benachrichtigt werden.

1. Wählen Sie in der Element-UI die Option **Berichterstellung > Alarme** aus.

Das System aktualisiert die Alarme auf der Seite alle 30 Sekunden.

Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eine eindeutige ID, die einer Cluster-Warnmeldung zugeordnet ist.
Schweregrad	Der Grad der Wichtigkeit des Alarms. Mögliche Werte: <ul style="list-style-type: none"><li>• Warnung: Ein kleines Problem, das bald Aufmerksamkeit erfordert. Upgrades des Systems sind weiterhin zulässig.</li><li>• Fehler: Ein Ausfall, der zu einer Performance-Verschlechterung oder einem Verlust von Hochverfügbarkeit führen kann. Fehler sollten in der Regel den Dienst nicht anderweitig beeinträchtigen.</li><li>• Kritisch: Ein schwerwiegender Fehler, der den Dienst beeinträchtigt. Das System kann keine API- oder Client-I/O-Anfragen bereitstellen. Ein Betrieb in diesem Zustand kann zu einem potenziellen Datenverlust führen.</li><li>• BestPractice: Eine empfohlene Best Practice für die Systemkonfiguration wird nicht verwendet.</li></ul>
Typ	Die Komponente, die sich auf den Fehler auswirkt. Nodes, Laufwerk, Cluster, Service oder Volume können verwendet werden.



Knoten	Node-ID für den Node, auf den sich dieser Fehler bezieht. Bei Knoten- und Laufwerkfehlern enthalten, andernfalls auf - (Dash) gesetzt.
Laufwerks-ID	Laufwerk-ID für das Laufwerk, auf das sich dieser Fehler bezieht. Bei Fahrfehlern enthalten, ansonsten auf - (Dash) eingestellt.
Fehlercode	Ein beschreibenden Code, der angibt, was den Fehler verursacht hat.
Details	Eine Beschreibung des Fehlers mit zusätzlichen Details.
Datum	Datum und Uhrzeit der Fehlerprotokollierung.

2. Klicken Sie auf **Details anzeigen**, um eine individuelle Warnung anzuzeigen, um Informationen über den Alarm anzuzeigen.
3. Um die Details aller Warnmeldungen auf der Seite anzuzeigen, klicken Sie auf die Spalte Details.

Nachdem das System eine Meldung beseitigt hat, werden alle Informationen über die Warnmeldung einschließlich des Datums, an dem sie behoben wurde, in den aufgelösten Bereich verschoben.

## Weitere Informationen

- [Cluster-Fehlercodes](#)
- ["Storage-Management mit der Element API"](#)

## Cluster-Fehlercodes

Das System meldet einen Fehler oder einen Status, der durch das Generieren eines Fehlercodes, der auf der Seite „Meldungen“ aufgeführt ist, von Interesse sein könnte. Anhand dieser Codes können Sie ermitteln, welche Komponente des Systems die Warnmeldung erfahren hat und warum die Warnmeldung generiert wurde.

In der folgenden Liste werden die verschiedenen Arten von Codes beschrieben:

- **AuthentifizierungServiceFault**

Der Authentifizierungsdienst auf einem oder mehreren Clusterknoten funktioniert nicht wie erwartet.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VerfügbarVirtualNetworkIPAdresseLow**

Die Anzahl der virtuellen Netzwerkadressen im Block der IP-Adressen ist gering.

Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- \* BlockClusterFull\*

Es ist nicht ausreichend freier Block-Speicherplatz zur Unterstützung eines Single-Node-Verlusts vorhanden. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der GetClusterFullThreshold API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Stage3Low (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
- Stage4Critical (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
- Stage5CompletelyConsumed (kritisch)<sup>1</sup>; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird.

Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.

- **BlocksDegradiert**

Blockdaten werden aufgrund eines Ausfalls nicht mehr vollständig repliziert.

Schweregrad	Beschreibung
Warnung	Auf nur zwei vollständige Kopien der Blockdaten kann zugegriffen werden.
Fehler	Auf nur eine vollständige Kopie der Blockdaten kann zugegriffen werden.
Kritisch	Auf vollständige Kopien der Blockdaten kann nicht zugegriffen werden.

**Hinweis:** der Warnstatus kann nur auf einem Triple Helix System auftreten.

Um diesen Fehler zu beheben, stellen Sie alle Offline Nodes oder Block-Services wieder her oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **BlockServiceTooFull**

Ein Block-Service benötigt zu viel Speicherplatz.

Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **BlockServiceUnHealthy**

Ein Blockdienst wurde als fehlerhaft erkannt:

- Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in cTimeUntilBSIsKilledMSec=330000 Millisekunden ab.
- Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke.
- Schweregrad = kritisch: Es gibt fehlerhafte Blockdienste auf mehreren Knoten, die größer oder gleich

der Replikationszahl sind (2 für Doppelhelix). Die Daten sind nicht verfügbar, und die bin-Synchronisierung wird nicht beendet.

Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Blockservice aufgerufen wird oder wenn der Dienst deaktiviert wurde.

- **BmcSelfTestFailed**

Der Baseboard Management Controller (BMC) hat einen Selbsttest nicht bestanden.

Wenden Sie sich an den NetApp Support, wenn Sie Hilfe benötigen.

Bei einem Upgrade auf Element 12.5 oder höher wird der `BmcSelfTestFailed` Fehler nicht für einen Node generiert, der bereits eine ausgefallene BMC hat, oder wenn die BMC eines Node während des Upgrades ausfällt. Die BMCs, die die Selbsttests während des Upgrades nicht durchführen, geben einen Warnfehler aus `BmcSelfTestFailed`, nachdem das gesamte Cluster das Upgrade abgeschlossen hat.

- **ClockSkewExceedsFaultThreshold**

Zeitverzerrung zwischen dem Cluster-Master und dem Node, der ein Token enthält, übersteigt den empfohlenen Schwellenwert. Storage Cluster kann die Zeitverzerrung zwischen den Nodes nicht automatisch korrigieren.

Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie einen internen NTP-Server verwenden, wenden Sie sich an den NetApp Support.

- \* ClusterCannotSync\*

Es ist ein nicht genügend Speicherplatz vorhanden, und Daten auf den Offline-Blockspeicherlaufwerken können nicht mit Laufwerken synchronisiert werden, die noch aktiv sind.

Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- \* ClusterFull\*

Es ist kein freier Speicherplatz im Storage-Cluster mehr verfügbar.

Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- **ClusterIOPSAreüberProvisiert**

Cluster-IOPS werden überprovisioniert. Die Summe aller minimalen QoS-IOPS ist größer als die erwarteten IOPS des Clusters. Eine minimale QoS kann nicht für alle Volumes gleichzeitig aufrechterhalten werden.

Senken Sie zur Behebung dieses Problems die Mindesteinstellungen für QoS-IOPS für Volumes.

- **CpuThermalEventThreshold**

Die Anzahl der thermischen CPU-Ereignisse auf einer oder mehreren CPUs überschreitet den konfigurierten Schwellenwert.

Wenn innerhalb von zehn Minuten keine neuen thermischen CPU-Ereignisse erkannt werden, löst sich die Warnung.

- **AbleDriveSecurityFailed**

Das Cluster ist nicht für das Aktivieren der Laufwerksicherheit konfiguriert (Verschlüsselung im Ruhezustand), aber mindestens ein Laufwerk ist die Laufwerksicherheit aktiviert, was bedeutet, dass die Laufwerksicherheit auf diesen Laufwerken deaktiviert ist. Dieser Fehler wird mit dem Schweregrad „Warnung“ protokolliert.

Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerksicherheit nicht deaktiviert werden konnte. Mögliche Gründe sind:

- Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselsever.
- Der Vorgang zum Deaktivieren des Laufwerks ist fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde.

Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich deaktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **DisconnectedClusterpaar**

Ein Cluster-Paar ist getrennt oder falsch konfiguriert.

Überprüfen Sie die Netzwerkverbindung zwischen den Clustern.

- **Verbindung abschaltenRemoteNode**

Ein Remote-Knoten ist entweder getrennt oder falsch konfiguriert.

Überprüfen Sie die Netzwerkverbindung zwischen den Nodes.

- **DemconnectedSnapMirrorEndpoint**

Ein Remote-SnapMirror-Endpunkt wird getrennt oder falsch konfiguriert.

Überprüfen Sie die Netzwerkverbindung zwischen dem Cluster und dem Remote-SnapMirrorEndpoint.

- **Auffahrt verfügbar**

Ein oder mehrere Laufwerke sind im Cluster verfügbar. Im Allgemeinen sollten alle Cluster alle Laufwerke hinzugefügt werden und keine im Status „verfügbar“. Sollte dieser Fehler unerwartet auftreten, wenden Sie sich an den NetApp Support.

Um diesen Fehler zu beheben, fügen Sie alle verfügbaren Laufwerke zum Speicher-Cluster hinzu.

- **\* Auffahrt nicht möglich\***

Das Cluster gibt diesen Fehler zurück, wenn ein oder mehrere Laufwerke ausgefallen sind und einer der folgenden Bedingungen anzeigt:

- Der Laufwerksmanager kann nicht auf das Laufwerk zugreifen.

- Der Slice- oder Block-Service ist zu oft ausgefallen, vermutlich aufgrund von Lese- oder Schreibfehlern des Laufwerks und kann nicht neu gestartet werden.
- Das Laufwerk fehlt.
- Der Master-Service für den Node ist nicht verfügbar (alle Laufwerke im Node gelten als fehlend/ausgefallen).
- Das Laufwerk ist gesperrt und der Authentifizierungsschlüssel für das Laufwerk kann nicht erworben werden.
- Das Laufwerk ist gesperrt, und der Entsperrvorgang schlägt fehl.

So lösen Sie dieses Problem:

- Überprüfen Sie die Netzwerkverbindung für den Node.
- Ersetzen Sie das Laufwerk.
- Stellen Sie sicher, dass der Authentifizierungsschlüssel verfügbar ist.

#### • **DriveHealthFault**

Die SMART-Integritätsprüfung auf einem Laufwerk ist fehlgeschlagen, sodass die Funktionen des Laufwerks verringert werden. Es gibt einen kritischen Schweregrad für diesen Fehler:

- Laufwerk mit serieller Verbindung: <Seriennummer> in Steckplatz: <Node-Steckplatz><Laufwerksfach> hat die INTELLIGENTE allgemeine Integritätsprüfung nicht bestanden.

Um diesen Fehler zu beheben, ersetzen Sie das Laufwerk.

#### • **DriveWearFault**

Die Restlebensdauer eines Laufwerks ist unter die Schwellenwerte gesunken, funktioniert aber immer noch. Es gibt zwei mögliche Schweregrade für diesen Fehler: Kritisch und Warnung:

- Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerk-Steckplatz> verfügt über einen kritischen Verschleiß.
- Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerksfach> verfügt über geringe Verschleißreserven.

Um diesen Fehler zu beheben, tauschen Sie das Laufwerk bald aus.

#### • \* DuplicateClusterMasterCandidates\*

Es wurden mehr als ein Master-Kandidat für Speichercluster erkannt.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **EnableDriveSecurityFailed**

Das Cluster ist so konfiguriert, dass es Laufwerkssicherheit (Verschlüsselung im Ruhezustand) benötigt, die Laufwerkssicherheit konnte jedoch auf mindestens einem Laufwerk nicht aktiviert werden. Dieser Fehler wird mit dem Schweregrad „Warnung“ protokolliert.

Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerkssicherheit nicht aktiviert werden konnte. Mögliche Gründe sind:

- Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselservers.

- Der Vorgang zum Aktivieren ist auf dem Laufwerk fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde. Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich aktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **EnsembleDegraded**

Die Netzwerk-Konnektivität oder -Stromversorgung wurde auf einen oder mehrere der Ensemble-Knoten verloren.

Um diesen Fehler zu beheben, stellen Sie die Netzwerkverbindung oder den Netzstrom wieder her.

- **Ausnahme**

Ein Fehler wurde gemeldet, der sich nicht auf einen Routinefehler ausstellt. Diese Fehler werden nicht automatisch aus der Fehlerwarteschlange gelöscht.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **AusfallenSpaceTooFull**

Ein Blockservice reagiert nicht auf Datenschreibanfragen. Dadurch verfügt der Slice Service über keinen freien Speicherplatz zum Speichern ausgefallener Schreibvorgänge.

Um diesen Fehler zu beheben, stellen Sie die Funktion zur Wiederherstellung von Blockdiensten wieder her, damit Schreibvorgänge normal fortgesetzt werden und der fehlerhafte Speicherplatz aus dem Schichtdienst entfernt werden kann.

- **FanSensor**

Ein Lüftersensor ist ausgefallen oder fehlt.

Um diesen Fehler zu beheben, ersetzen Sie eine fehlerhafte Hardware.

- **Fiber ChannelAccessDegraded**

Ein Fibre Channel-Node reagiert nicht auf andere Nodes im Storage-Cluster über einen bestimmten Zeitraum. In diesem Status gilt der Node als nicht ansprechbar und generiert einen Cluster-Fehler.

Überprüfen Sie die Netzwerkverbindung.

- **FaserChannelAccessUnverfügbar**

Alle Fibre-Channel-Nodes reagieren nicht mehr. Die Node-IDs werden angezeigt.

Überprüfen Sie die Netzwerkverbindung.

- **FiberChannelActiveIxL**

Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 8000 aktiven Sitzungen pro Fibre-Channel-Node.

- Best Practice-Grenze ist 5500.
- Warngrenze ist 7500.
- Die maximale Obergrenze (nicht erzwungen) beträgt 8192.

Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 5500.

#### • **Fiber ChannelConfig**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- An einem PCI-Steckplatz befindet sich ein unerwarteter Fibre Channel-Port.
- Es gibt ein unerwartetes Fibre Channel HBA-Modell.
- Ein Problem mit der Firmware eines Fibre Channel HBA ist aufgetreten.
- Ein Fibre-Channel-Port ist nicht online.
- Bei der Konfiguration von Fibre Channel Passthrough müssen hartnäckige Probleme aufgetreten sein.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **FiberChannelIOPS**

Die IOPS-Gesamtzahl nähert sich dem IOPS-Limit für Fibre Channel Nodes im Cluster. Die Grenzen sind:

- FC0025: 50.000 IOPS bei 4-KB-Blockgröße pro Fibre Channel Node.
- FCN001: Grenzwert von 625.000 OPS bei einer Blockgröße von 4 KB pro Fibre Channel Node.

Um diesen Fehler zu beheben, verteilen Sie die Last auf alle verfügbaren Fibre Channel Nodes.

#### • **FiberChannelStaticiXL**

Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 16000 statischen Sitzungen pro Fibre-Channel-Node.

- Best Practice-Grenze ist 11000.
- Warngrenze ist 15000.
- Die maximale Obergrenze (erzwungen) ist 16384.

Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 11000.

#### • **DateiSystemkapazitätNiedrig**

Auf einem der Dateisysteme ist nicht genügend Platz vorhanden.

Um diesen Fehler zu beheben, fügen Sie dem Dateisystem mehr Kapazität hinzu.

#### • **FileSystemsReadOnly**

Ein Dateisystem ist in einen schreibgeschützten Modus umgestiegen.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **FipsDrivesMismatch**

Ein Laufwerk ohne FIPS wurde physisch in einen FIPS-fähigen Storage-Node eingesetzt oder ein FIPS-Laufwerk wurde physisch in einen Storage-Node außerhalb von FIPS eingesetzt. Pro Node wird ein einziger Fehler generiert und alle betroffenen Laufwerke aufgelistet.

Um diesen Fehler zu beheben, entfernen oder ersetzen Sie das nicht übereinstimmende Laufwerk oder die betreffenden Laufwerke.

#### • **FipsDriveOutOfCompliance**

Das System hat erkannt, dass die Verschlüsselung im Ruhezustand nach Aktivierung der FIPS-Festplattenfunktion deaktiviert wurde. Dieser Fehler wird auch generiert, wenn die FIPS-Laufwerksfunktion aktiviert ist und ein Laufwerk oder ein Node außerhalb von FIPS im Storage-Cluster vorhanden ist.

Um diesen Fehler zu beheben, aktivieren Sie die Verschlüsselung im Ruhezustand oder entfernen Sie die nicht-FIPS-Hardware aus dem Storage-Cluster.

#### • **FipsSelfTestFailure**

Das FIPS-Subsystem hat während des Self-Tests einen Ausfall erkannt.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **HardwareConfigMismatch**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Die Konfiguration stimmt nicht mit der Knotendefinition überein.
- Für diesen Node-Typ gibt es eine falsche Laufwerksgröße.
- Es wurde ein nicht unterstütztes Laufwerk erkannt. Ein möglicher Grund ist, dass die installierte Element-Version dieses Laufwerk nicht erkennt. Es wird empfohlen, die Element Software auf diesem Node zu aktualisieren.
- Es stimmt nicht überein, dass die Laufwerk-Firmware nicht stimmt.
- Der Status für die Laufwerksverschlüsselung stimmt nicht mit dem Node überein.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **IdPCertificateExpiration**

Das SSL-Zertifikat des Diensteanbieters des Clusters zur Verwendung mit einem Drittanbieter-Identitätsanbieter (IdP) nähert sich dem Ablaufdatum oder ist bereits abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

Um diesen Fehler zu beheben, aktualisieren Sie das SSL-Zertifikat, bevor es abläuft. Verwenden Sie die



UpdateIpConfiguration API-Methode mit `refreshCertificateExpirationTime=true`, um das aktualisierte SSL-Zertifikat bereitzustellen.

- **Inkonsistenz BondModes**

Die Bond-Modi auf dem VLAN-Gerät fehlen. Dieser Fehler zeigt den erwarteten Bond-Modus und den derzeit verwendeten Bond-Modus an.

- **Inkonsistent Mtus**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Bond1G-Diskrepanz: Inkonsistente MTUs wurden an Bond1G-Schnittstellen erkannt.
- Bond10G-Diskrepanz: Inkonsistente MTUs wurden an Bond10G-Schnittstellen erkannt.

Dieser Fehler zeigt den betreffenden Node oder die betreffenden Knoten zusammen mit dem zugehörigen MTU-Wert an.

- **UnstimmigeDie Routenregeln**

Die Routingregeln für diese Schnittstelle sind inkonsistent.

- **Inkonsistent SubnetMasken**

Die Netzwerkmaske auf dem VLAN-Gerät stimmt nicht mit der intern aufgezeichneten Netzwerkmaske für das VLAN überein. Dieser Fehler zeigt die erwartete Netzwerkmaske und die aktuell verwendete Netzwerkmaske an.

- **IncorrectBondPortCount**

Die Anzahl der Bond-Ports ist falsch.

- **InvalidConfiguredFiberChannelNodeCount**

Eine der beiden erwarteten Fibre-Channel-Node-Verbindungen ist beeinträchtigt. Dieser Fehler wird angezeigt, wenn nur ein Fibre-Channel-Knoten verbunden ist.

Um diesen Fehler zu beheben, überprüfen Sie die Cluster-Netzwerkonnektivität und die Netzwerkverkabelung und überprüfen Sie, ob Services ausgefallen sind. Falls keine Netzwerk- oder Serviceprobleme auftreten, wenden Sie sich an den NetApp Support, um einen Fibre Channel-Node zu ersetzen.

- **IrqBalanceFailed**

Beim Versuch, Interrupts auszugleichen, ist eine Ausnahme aufgetreten.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **KmZertifizierungFault**

- Das Zertifikat der Root Certification Authority (CA) nähert sich dem Ablaufdatum.

Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie `ModifyKeyServerKmpip`, um das aktualisierte Root CA-Zertifikat bereitzustellen.

- Das Clientzertifikat nähert sich dem Ablaufdatum.

Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit `GetClientCertificateSigningRequest`, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie `ModifyKeyServerKmpip`, um das auslaufende KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

- Das Zertifikat der Root Certification Authority (CA) ist abgelaufen.

Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie `ModifyKeyServerKmpip`, um das aktualisierte Root CA-Zertifikat bereitzustellen.

- Client-Zertifikat ist abgelaufen.

Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit `GetClientCertificateSigningRequest`, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie `ModifyKeyServerKmpip`, um das abgelaufene KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

- Fehler bei der Root Certification Authority (CA)-Zertifizierung.

Um diesen Fehler zu beheben, überprüfen Sie, ob das richtige Zertifikat bereitgestellt wurde und, falls erforderlich, das Zertifikat von der Stammzertifizierungsstelle erneut erwerben. Verwenden Sie `ModifyKeyServerKmpip`, um das richtige KMIP-Client-Zertifikat zu installieren.

- Fehler beim Client-Zertifikat.

Um diesen Fehler zu beheben, überprüfen Sie, ob das korrekte KMIP-Client-Zertifikat installiert ist. Die Root-CA des Client-Zertifikats sollte auf dem EKS installiert werden. Verwenden Sie `ModifyKeyServerKmpip`, um das richtige KMIP-Client-Zertifikat zu installieren.

- **KmpipServerFault**

- Verbindungsfehler

Um diesen Fehler zu beheben, überprüfen Sie, ob der externe Schlüsselservers aktiv ist und über das Netzwerk erreichbar ist. Verwenden Sie `TestKeyServerKimp` und `TestKeyProviderKmpip`, um Ihre Verbindung zu testen.

- Authentifizierungsfehler

Um diesen Fehler zu beheben, überprüfen Sie, ob die richtige Root-CA- und KMIP-Client-Zertifikate verwendet werden und ob der private Schlüssel und das KMIP-Client-Zertifikat übereinstimmen.

- Serverfehler

Um diesen Fehler zu beheben, überprüfen Sie die Details auf den Fehler. Möglicherweise ist aufgrund des zurückgegebenen Fehlers eine Fehlerbehebung auf dem externen Schlüsselservers erforderlich.

- \* MemoryEccThreshold\*

Es wurden eine große Anzahl von korrigierbaren oder nicht korrigierbaren ECC-Fehlern erkannt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Ereignis	Schweregrad	Beschreibung
----------	-------------	--------------

Ein einzelnes DIMM cErrorCount erreicht cDimmCorrectableErrWarnThreshold.	Warnung	Korrigierbare ECC-Speicherfehler über dem Schwellenwert auf DIMM: <Prozessor> <DIMM Slot>
Ein einzelnes DIMM cErrorCount bleibt über cDimmCorrectableErrWarnThreshold bis cErrorFaultTimer für das DIMM abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein Speicher-Controller meldet cErrorCount über cMemCtrlCorrectableErrWarnThreshold und cMemCtrlCorrectableErrWarnDauer wird angegeben.	Warnung	Korrigierbare ECC-Speicherfehler oberhalb des Schwellenwerts für Speicher-Controller: <Prozessor> <Speicher-Controller>
Ein Speicher-Controller meldet cErrorCount über cMemCtrlCorrectableErrWarnThreshold bis cErrorFaultTimer für den Speicher-Controller abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein einzelnes DIMM meldet einen uErrorCount über Null, aber kleiner als cDimmUncorrectTableErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein einzelnes DIMM meldet einen uErrorCount von mindestens cDimmUncorrectTableErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein Speicher-Controller meldet einen uErrorCount über Null, aber kleiner als cMemCtrlUncorregictErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt
Ein Speicher-Controller meldet einen uErrorCount von mindestens cMemCtrlUncorregictErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- **SpeichernUsageThreshold**

Die Speicherauslastung ist über dem Normalwert. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:



Weitere Informationen zum Fehlertyp finden Sie in der Überschrift **Details** im Fehlerfehler.

Schweregrad	Beschreibung
Warnung	Der Systemspeicher ist schwach.
Fehler	Der Systemspeicher ist sehr gering.
Kritisch	Der Systemspeicher wird vollständig verbraucht.

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- **\* MetadataClusterFull\***

Es ist nicht ausreichend freier Speicherplatz für Metadaten vorhanden, um einen Ausfall eines einzelnen Nodes zu unterstützen. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der `GetClusterFullThreshold` API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- `Stage3Low` (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
- `Stage4Critical` (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
- `Stage5CompletelyConsumed` (kritisch)<sup>1</sup>; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird. Löschen oder Löschen von Daten oder Hinzufügen weiterer Nodes

Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.

- **MtuCheckFailure**

Ein Netzwerkgerät ist nicht für die richtige MTU-Größe konfiguriert.

Um diesen Fehler zu beheben, stellen Sie sicher, dass alle Netzwerkschnittstellen und Switch-Ports für Jumbo Frames konfiguriert sind (MTUs mit einer Größe von bis zu 9000 Byte).

- **NetworkConfig**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Eine erwartete Schnittstelle ist nicht vorhanden.
- Es ist eine doppelte Schnittstelle vorhanden.
- Eine konfigurierte Schnittstelle ist ausgefallen.
- Ein Netzwerkneustart ist erforderlich.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NoVerfügbarVirtualNetzwerkIPAddresses**

Im Block der IP-Adressen sind keine virtuellen Netzwerkadressen verfügbar.

- VirtualNetworkID # TAG(###) hat keine Speicher-IP-Adressen. Dem Cluster können keine weiteren Nodes hinzugefügt werden.

Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- **NodeHardwareFault (Netzwerkschnittstelle <Name> ist ausgefallen oder das Kabel ist nicht angeschlossen)**

Eine Netzwerkschnittstelle ist entweder ausgefallen oder das Kabel ist nicht angeschlossen.

Um diesen Fehler zu beheben, überprüfen Sie die Netzwerkverbindung für den Knoten oder Knoten.

- **NodeHardwareFault (Laufwerksverschlüsselungsstatus entspricht dem Verschlüsselungsstatus des Node für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub>)**

Ein Laufwerk entspricht nicht den Verschlüsselungsfunktionen des in installierten Storage-Nodes.

- **NodeHardwareFault (Falscher <Laufwerkstyp> Laufwerksgröße <tatsächliche Größe> für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub> für diesen Node-Typ - erwartete <erwartete Größe>)**

Ein Storage-Node enthält ein Laufwerk, das die falsche Größe für diesen Node hat.

- **NodeHardwareFault (nicht unterstütztes Laufwerk in Steckplatz <Node Slot><Drive Slot> gefunden; Laufwerksstatistiken und Integritätsinformationen sind nicht verfügbar)**

Ein Storage-Node enthält ein Laufwerk, das nicht unterstützt wird.

- **NodeHardwareFault (das Laufwerk in Slot <Node Slot><Drive Slot> sollte die Firmware-Version <erwartete Version> verwenden, wird aber nicht unterstützte Version <tatsächliche Version> verwenden)**

Ein Speicherknoten enthält ein Laufwerk, auf dem eine nicht unterstützte Firmware-Version ausgeführt wird.

- **NoteWartungs-Modus**

Ein Node wurde im Wartungsmodus versetzt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Gibt an, dass sich der Node noch im Wartungsmodus befindet.
Fehler	Zeigt an, dass der Wartungsmodus nicht deaktiviert wurde, wahrscheinlich aufgrund von fehlgeschlagenen oder aktiven Standardys.

Um diesen Fehler zu beheben, deaktivieren Sie den Wartungsmodus nach Abschluss der Wartung. Wenn

der Fehler auf der Fehlerebene weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NodeOffline**

Element Software kann nicht mit dem angegebenen Node kommunizieren. Überprüfen Sie die Netzwerkverbindung.

- **NotusingLACPBondMode**

LACP Bonding-Modus ist nicht konfiguriert.

Um diesen Fehler zu beheben, verwenden Sie LACP Bonding bei der Implementierung von Storage-Nodes. Es kann zu Performance-Problemen kommen, wenn LACP nicht aktiviert und ordnungsgemäß konfiguriert ist.

- **NtpServerUnerreichbar**

Das Storage-Cluster kann nicht mit dem angegebenen NTP-Server oder den angegebenen Servern kommunizieren.

Um diesen Fehler zu beheben, überprüfen Sie die Konfiguration für den NTP-Server, das Netzwerk und die Firewall.

- **NtpTimeNotInSync**

Der Unterschied zwischen der Storage-Cluster-Zeit und der angegebenen NTP-Serverzeit ist zu groß. Der Speichercluster kann die Differenz nicht automatisch korrigieren.

Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie interne NTP-Server verwenden und das Problem weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NvramDeviceStatus**

Ein NVRAM-Gerät weist einen Fehler auf, ist ausgefallen oder ist ausgefallen. Dieser Fehler weist folgende Schweregrade auf:

Schweregrad	Beschreibung
Warnung	Die Hardware hat eine Warnung erkannt. Dieser Zustand kann vorübergehend sein, z. B. eine Temperaturwarnung. <ul style="list-style-type: none"><li>• NvmLifetimeFehler</li><li>• NvmLifetimeStatus</li><li>• EnergiengySourceLifetimeStatus</li><li>• EnergiengySourceTemperatureStatus</li><li>• WarningThresholdExceeded</li></ul>

Fehler	<p>Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt. Zusätzlich zu den Warnungsebenen-Fehlern zurückgegebene Fehler:</p> <ul style="list-style-type: none"> <li>• Der Mount-Punkt für NVRAM-Gerät ist nicht vorhanden.</li> <li>• Die NVRAM-Gerätepartition ist nicht vorhanden.</li> <li>• Die NVRAM-Gerätepartition ist vorhanden, aber nicht angehängt.</li> </ul>
Kritisch	<p>Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt.</p> <ul style="list-style-type: none"> <li>• Persistenz verloren</li> <li>• ArmStatusSaveNArmed</li> <li>• CsaveStatusfehler</li> </ul>

Ersetzen Sie alle fehlerhaften Hardware im Node. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **PowerSupplyError**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Es ist kein Netzteil vorhanden.
- Ein Netzteil ist fehlgeschlagen.
- Ein Netzteileingang fehlt oder außerhalb des zulässigen Bereichs liegt.

Um diesen Fehler zu beheben, überprüfen Sie, ob alle Knoten mit redundanter Stromversorgung versorgt werden. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **ProvisionedSpaceTooFull**

Die insgesamt bereitgestellte Kapazität des Clusters ist zu voll.

Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellten Speicherplatz hinzu oder löschen und löschen Sie Volumes.

#### • **EntferntRepAsyncDelayExceeded**

Die konfigurierte asynchrone Verzögerung der Replikation wurde überschritten. Überprüfen Sie die Netzwerkverbindung zwischen Clustern.

- **EntfernteRepClusterFull**

Die Remote-Replikation der Volumes wurde angehalten, da der Ziel-Storage-Cluster zu voll ist.

Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntfernteRepSnapshotClusterFull**

Die Remote-Replizierung der Snapshots wurde durch die Volumes unterbrochen, weil der Ziel-Storage-Cluster zu voll ist.

Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntferntRepSnapshotsExceedLimit**

Die Volumes haben die Remote-Replizierung von Snapshots angehalten, da das Ziel-Storage-Cluster-Volumen seine Snapshot-Grenze überschritten hat.

Um diesen Fehler zu beheben, erhöhen Sie die Snapshot-Grenze auf dem Ziel-Speicher-Cluster.

- **Fehler beim PlaneActionError**

Mindestens eine der geplanten Aktivitäten wurde ausgeführt, ist aber fehlgeschlagen.

Der Fehler wird gelöscht, wenn die geplante Aktivität erneut ausgeführt wird und erfolgreich ist, wenn die geplante Aktivität gelöscht wird oder wenn die Aktivität angehalten und fortgesetzt wird.

- **SensorReadingFailed**

Ein Sensor konnte nicht mit dem Baseboard Management Controller (BMC) kommunizieren.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **ServiceNotRunning**

Ein erforderlicher Dienst wird nicht ausgeführt.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **SliceServiceTooFull**

Einem Schichtdienst ist zu wenig provisionierte Kapazität zugewiesen.

Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **SchliceServiceUngesund**

Das System hat erkannt, dass ein Schichtdienst ungesund ist und ihn automatisch stillsetzt.

- Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in 6 Minuten ab.
- Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke.

Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Schichtdienst



verfügbar ist oder wenn der Dienst deaktiviert wurde.

- **Sshenenabled**

Der SSH-Service ist auf einem oder mehreren Nodes im Storage-Cluster aktiviert.

Um diesen Fehler zu beheben, deaktivieren Sie den SSH-Service auf dem entsprechenden Node oder Nodes oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **SslCertificateExpiration**

Das mit diesem Knoten verknüpfte SSL-Zertifikat nähert sich dem Ablaufdatum oder ist abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

Um diesen Fehler zu beheben, erneuern Sie das SSL-Zertifikat. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- \* Stranddecacity\*

Ein einzelner Node verursacht mehr als die Hälfte der Storage-Cluster-Kapazität.

Um die Datenredundanz aufrechtzuerhalten, reduziert das System die Kapazität des größten Node, sodass einige seiner Blockkapazitäten ungenutzt (nicht verwendet) sind.

Fügen Sie zur Behebung dieses Fehlers weitere Laufwerke zu vorhandenen Speicher-Nodes hinzu oder fügen Sie dem Cluster Storage-Nodes hinzu.

- **TempSensor**

Ein Temperatursensor meldet höhere Temperaturen als normale Temperaturen. Dieser Fehler kann in Verbindung mit PowerSupplyError oder FanSensor Fehlern ausgelöst werden.

Um diesen Fehler zu beheben, prüfen Sie, ob Luftstrombehinderungen in der Nähe des Storage-Clusters vorhanden sind. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- **Upgrade**

Ein Upgrade läuft seit mehr als 24 Stunden.

Setzen Sie das Upgrade fort, oder wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **UnresponsiveService**

Ein Dienst reagiert nicht mehr.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **VirtualNetworkConfig**

Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

- Eine Schnittstelle ist nicht vorhanden.
- Ein falscher Namespace auf einer Schnittstelle.
- Eine falsche Netzmaske ist vorhanden.
- Eine falsche IP-Adresse ist vorhanden.
- Eine Schnittstelle ist nicht verfügbar und wird nicht ausgeführt.
- Es gibt eine überflüssige Schnittstelle auf einem Knoten.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

#### • **VolumesDegradiert**

Die Replikation und Synchronisierung der sekundären Volumes ist nicht abgeschlossen. Die Meldung wird gelöscht, wenn die Synchronisierung abgeschlossen ist.

#### • **VolumesOffline**

Ein oder mehrere Volumes im Storage-Cluster sind offline. Der Fehler **volumeDegraded** ist ebenfalls vorhanden.

Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

## Zeigen Sie die Node-Performance-Aktivitäten an

Sie können Performance-Aktivitäten für jeden Node in einem grafischen Format anzeigen. Diese Information bietet Echtzeitstatistiken für CPU und Lese-/Schreib-I/O-Vorgänge pro Sekunde (IOPS) für jedes Laufwerk des Node. Das Auslastungsdiagramm wird alle fünf Sekunden aktualisiert, und das Laufwerksstatistiken-Diagramm aktualisiert alle zehn Sekunden.

1. Klicken Sie Auf **Cluster > Knoten**.
2. Klicken Sie auf **Aktionen** für den Knoten, den Sie anzeigen möchten.
3. Klicken Sie Auf **Details Anzeigen**.



Sie können bestimmte Punkte in der Zeit auf den Linien- und Balkendiagrammen sehen, indem Sie den Cursor über die Linie oder den Balken positionieren.

## Anzeigen der Volume-Performance

Sie können detaillierte Performance-Informationen für alle Volumes im Cluster anzeigen. Sie können die Informationen nach der Volume-ID oder einer der Performance-Spalten sortieren. Sie können die Informationen auch nach bestimmten Kriterien filtern.

Sie können ändern, wie oft das System Performanceinformationen auf der Seite aktualisiert, indem Sie auf die Liste **Aktualisieren alle** klicken und einen anderen Wert auswählen. Das Standard-Aktualisierungsintervall ist 10 Sekunden, wenn das Cluster weniger als 1000 Volumes hat, andernfalls beträgt die Standardeinstellung 60 Sekunden. Wenn Sie einen Wert von „nie“ wählen, ist die automatische Aktualisierung der Seite deaktiviert.

Sie können die automatische Aktualisierung durch Klicken auf **Aktivieren der automatischen Aktualisierung** wieder aktivieren.

1. Wählen Sie in der Element UI die Option **Berichterstellung > Volume Performance**.
2. Klicken Sie in der Liste Volume auf das Aktionen-Symbol für ein Volume.
3. Klicken Sie Auf **Details Anzeigen**.

Unten auf der Seite wird ein Fach mit allgemeinen Informationen zum Volume angezeigt.

4. Um weitere Informationen zum Volumen anzuzeigen, klicken Sie auf **Weitere Details**.

Das System zeigt detaillierte Informationen sowie Performance-Diagramme für das Volume an.

## Weitere Informationen

[Volume Performance im Detail](#)

### Volume Performance im Detail

Auf der Seite Volume Performance auf der Registerkarte Reporting in der Element UI können Sie Performancestatistiken der Volumes anzeigen.

In der folgenden Liste werden die Details beschrieben, die Ihnen zur Verfügung stehen:

- **ID**

Die vom System generierte ID für das Volume.

- **Name**

Der Name, der dem Volume bei seiner Erstellung gegeben wurde.

- **Konto**

Der Name des Kontos, das dem Volume zugewiesen wurde.

- **Zugriffsgruppen**

Der Name der Zugriffsgruppe oder der Gruppen des Volumes, der das Volume angehört.

- **Volume-Nutzung**

Ein Prozentwert, der beschreibt, wie viel der Client das Volume verwendet.

Mögliche Werte:

- 0 = der Client verwendet das Volume nicht
- 100 = der Client verwendet das Maximum

- >100 = der Kunde verwendet den Burst

- **IOPS insgesamt**

Gesamtzahl der derzeit ausgeführten IOPS (Lese- und Schreibvorgänge) gegenüber dem Volume

- **Lese-IOPS**

Gesamtzahl der Lese-IOPS, die derzeit auf dem Volume ausgeführt wird

- **Schreib-IOPS**

Die Gesamtzahl der momentan ausgeführten Schreib-IOPS gegenüber dem Volume.

- **Gesamtdurchsatz**

Der aktuell ausgeführte Gesamtdurchsatz (Lese- und Schreibvorgänge) gegenüber dem Volume.

- **Lesedurchsatz**

Gesamtmenge des aktuell ausgeführten Lese-Durchsatzes gegenüber dem Volume.

- **Schreibdurchsatz**

Der Gesamtdurchsatz, der derzeit für das Volume ausgeführt wird.

- **Gesamte Latenz**

Die durchschnittliche Zeit in Mikrosekunden, die Lese- und Schreibvorgänge auf einem Volume abzuschließen.

- **Leselatenz**

Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge in dem Volume in den letzten 500 Millisekunden abzuschließen.

- **Schreiblatenz**

Der durchschnittliche Zeitaufwand in Mikrosekunden, um Schreibvorgänge in einem Volume in den letzten 500 Millisekunden abzuschließen.

- **Warteschlangentiefe**

Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf dem Volume.

- **Durchschnittliche I/O-Größe**

Durchschnittliche Größe in Byte der letzten I/O-Vorgänge für das Volume in den letzten 500 Millisekunden.

## Anzeigen von iSCSI-Sitzungen

Sie können die iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind. Sie können die Informationen filtern, um nur die gewünschten Sitzungen einzubeziehen.

1. Wählen Sie in der Element UI die Option **Reporting > iSCSI-Sitzungen**.

2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

## Weitere Informationen

[Details zur iSCSI-Sitzung](#)

### Details zur iSCSI-Sitzung

Sie können Informationen zu den iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie zu den iSCSI-Sitzungen finden können:

- **Knoten**

Der Node, der die primäre Metadatenpartition für das Volume hostet.

- **Konto**

Der Name des Kontos, zu dem das Volume gehört. Wenn der Wert leer ist, wird ein Strich (-) angezeigt.

- **Lautstärke**

Der auf dem Node angegebene Volume-Name.

- **Volumen-ID**

ID des Volumes, das mit der Ziel-IQN verknüpft ist.

- **Initiator ID**

Eine vom System generierte ID für den Initiator.

- **Initiator-Alias**

Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Initiator IP**

Die IP-Adresse des Endpunkts, der die Sitzung initiiert.

- **Initiator IQN**

Der IQN des Endpunkts, der die Sitzung initiiert.

- **Ziel-IP**

Die IP-Adresse des Node, der das Volume hostet.

- **Ziel-IQN**

Die IQN des Volume.

- **Erstellt Am**

Datum, an dem die Sitzung eingerichtet wurde.

## Zeigen Sie Fibre-Channel-Sitzungen an

Sie können die Fibre Channel-Sitzungen (FC) anzeigen, die mit dem Cluster verbunden sind. Sie können Informationen so filtern, dass nur die Verbindungen berücksichtigt werden, die im Fenster angezeigt werden sollen.

1. Wählen Sie in der Element-UI die Option **Reporting > FC-Sitzungen**.
2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

### Weitere Informationen

[Details zur Fibre Channel-Sitzung](#)

### Details zur Fibre Channel-Sitzung

Sie können Informationen zu den aktiven Fibre Channel-Sitzungen (FC) finden, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie über die mit dem Cluster verbundenen FC-Sitzungen finden:

- **Knoten-ID**

Der Node, der die Sitzung für die Verbindung hostet.

- **Knotenname**

Vom System generierter Node-Name.

- **Initiator ID**

Eine vom System generierte ID für den Initiator.

- **Initiator WWPN**

Der weltweite Port-Name des Initiierenden.

- **Initiator-Alias**

Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Ziel-WWPN**

Der weltweite Zielname des Ports.

- **Volume Access Group**

Name der Zugriffsgruppe des Volumes, der die Sitzung angehört.

- **Volume Access Group ID**

Vom System generierte ID für die Zugriffsgruppe.

## Fehlerbehebung bei Laufwerken

Fehlerhafte Solid State-Laufwerke (SSD) können durch ein Ersatzlaufwerk ersetzt werden. SSDs für SolidFire Storage-Nodes sind Hot-Swap-fähig. Wenn Sie vermuten, dass eine SSD ausgefallen ist, wenden Sie sich an den NetApp Support, um den Fehler zu überprüfen und gehen Sie durch das entsprechende Lösungsverfahren. NetApp Support bietet Ihnen auch Ersatzlaufwerk nach Ihren Service Level Agreements.

So kann ein ausgefallenes Laufwerk eines aktiven Nodes entfernt und durch ein neues SSD-Laufwerk von NetApp ersetzt werden. Es wird nicht empfohlen, nicht ausgefallene Laufwerke in einem aktiven Cluster zu entfernen.

Sie sollten die von NetApp Support vorgeschlagenen vor-Ort-Ersatzteile aufrecht erhalten, um bei einem Ausfall einen sofortigen Austausch des Laufwerks zu ermöglichen.



Wenn Sie zu Testzwecken einen Laufwerksausfall simulieren, indem Sie ein Laufwerk von einem Node entfernen, müssen Sie 30 Sekunden warten, bevor Sie das Laufwerk wieder in den Laufwerkschacht einsetzen.

Wenn ein Laufwerk ausfällt, verteilt Double Helix die Daten auf dem Laufwerk auf die Nodes, die im Cluster verbleiben. Mehrere Laufwerksausfälle auf demselben Node stellen kein Problem dar, da die Element Software vor zwei Kopien von Daten auf demselben Node schützt. Ein ausgefallenes Laufwerk führt zu den folgenden Ereignissen:

- Daten werden vom Laufwerk migriert.
- Die Gesamtkapazität des Clusters wird nach der Kapazität des Laufwerks verringert.
- Double Helix Datensicherung stellt sicher, dass zwei gültige Kopien der Daten vorhanden sind.



SolidFire Storage-Systeme unterstützen das Entfernen eines Laufwerks nicht, wenn zu wenig Storage für die Datenmigration erforderlich ist.

### Finden Sie weitere Informationen

- [Entfernen ausgefallener Laufwerke aus dem Cluster](#)
- [Grundlegende Fehlersuche bei MDSS-Laufwerken](#)
- [Entfernen Sie MDSS-Laufwerke](#)
- ["Austausch von Laufwerken für SolidFire Storage-Nodes"](#)
- ["Austausch von Laufwerken für Storage-Nodes der Serie H600S"](#)
- ["H410S und H610S Hardware-Informationen"](#)
- ["Hardwareinformationen zur SF-Series"](#)

### Entfernen ausgefallener Laufwerke aus dem Cluster

Das SolidFire-System setzt ein Laufwerk in den Status „ausgefallen“, wenn die Selbstdiagnose des Laufwerks den Node angibt, an dem es ausgefallen ist, oder ob die

Kommunikation mit dem Laufwerk fünf oder anderthalb Minuten lang unterbrochen wird. Das System zeigt eine Liste der ausgefallenen Laufwerke an. Sie müssen ein ausgefallenes Laufwerk von der Liste ausgefallener Laufwerke in der NetApp Element-Software entfernen.

Laufwerke in der Liste **Alerts** werden als **blockServiceUnHealthy** angezeigt, wenn ein Knoten offline ist. Wenn der Node und seine Laufwerke beim Neustart innerhalb von fünf und anderthalb Minuten wieder online sind, werden die Laufwerke automatisch aktualisiert und fortgesetzt, wenn die aktiven Laufwerke im Cluster wieder verfügbar sind.

1. Wählen Sie in der Element UI die Option **Cluster > Laufwerke**.
2. Klicken Sie auf **fehlgeschlagen**, um die Liste der fehlgeschlagenen Laufwerke anzuzeigen.
3. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks.

Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden.

4. Entfernen Sie die ausgefallenen Laufwerke mithilfe einer der folgenden Methoden:

Option	Schritte
Um einzelne Laufwerke zu entfernen	<ol style="list-style-type: none"> <li>a. Klicken Sie auf <b>Aktionen</b> für das Laufwerk, das Sie entfernen möchten.</li> <li>b. Klicken Sie Auf <b>Entfernen</b>.</li> </ol>
Um mehrere Laufwerke zu entfernen	<ol style="list-style-type: none"> <li>a. Wählen Sie alle Laufwerke aus, die Sie entfernen möchten, und klicken Sie auf <b>Massenaktionen</b>.</li> <li>b. Klicken Sie Auf <b>Entfernen</b>.</li> </ol>

## Grundlegende Fehlersuche bei MDSS-Laufwerken

Metadaten (oder Slice)-Laufwerke können wiederhergestellt werden, indem sie zu dem Cluster hinzugefügt werden, wenn ein oder beide Metadaten-Laufwerke ausfallen. Sie können den Wiederherstellungsvorgang in der NetApp Element-Benutzeroberfläche ausführen, wenn die MDSS-Funktion bereits auf dem Knoten aktiviert ist.

Wenn es bei einem oder beiden Metadatenlaufwerken in einem Node zu einem Ausfall kommt, wird der Slice-Service heruntergefahren und Daten von beiden Laufwerken werden auf unterschiedlichen Laufwerken im Node gesichert.

In den folgenden Szenarien werden mögliche Fehler-Szenarien beschrieben und grundlegende Empfehlungen zur Behebung des Problems bereitgestellt:

### Systemscheibe schlägt fehl

- In diesem Szenario wird der Steckplatz 2 überprüft und in einen verfügbaren Status zurückgeführt.
- Das Systemschichtlaufwerk muss neu befüllt werden, bevor der Schichtdienst wieder in den Online-Modus versetzt werden kann.



- Sie sollten das System-Slice-Laufwerk ersetzen, wenn das System-Slice-Laufwerk verfügbar ist, fügen Sie das Laufwerk und das Steckplatz-2-Laufwerk gleichzeitig hinzu.



Sie können das Laufwerk in Steckplatz 2 nicht selbst als Metadatenlaufwerk hinzufügen. Sie müssen beide Laufwerke gleichzeitig zum Node hinzufügen.

### Steckplatz 2 fällt aus

- In diesem Szenario wird das Systemschichtlaufwerk überprüft und in einen verfügbaren Zustand zurückgeführt.
- Sie sollten Steckplatz 2 durch ein Ersatzlaufwerk ersetzen, wenn Steckplatz 2 verfügbar ist, fügen Sie das SystemSlice-Laufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

### System-Slice-Laufwerk und Steckplatz 2 schlägt fehl

- Sie sollten beide Systemscheiben-Laufwerke und Steckplatz 2 durch ein Ersatzlaufwerk ersetzen. Wenn beide Laufwerke verfügbar sind, fügen Sie das Systemlaufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

### Reihenfolge der Vorgänge

- Ersetzen Sie das ausgefallene Hardwarelaufwerk durch ein Ersatzlaufwerk (ersetzen Sie beide Laufwerke, wenn beide ausgefallen sind).
- Fügen Sie wieder Laufwerke zum Cluster hinzu, wenn sie wieder gefüllt wurden und sich in einem verfügbaren Zustand befinden.

### Überprüfung des Betriebs

- Überprüfen Sie, ob die Laufwerke in Steckplatz 0 (oder intern) und Steckplatz 2 in der Liste „Aktive Laufwerke“ als Metadatenlaufwerke identifiziert werden.
- Vergewissern Sie sich, dass der gesamte Schichtausgleich abgeschlossen ist (es sind mindestens 30 Minuten lang keine weiteren Verschieben von Slices im Ereignisprotokoll vorhanden).

### Finden Sie weitere Informationen

[Fügen Sie MDSS-Laufwerke hinzu](#)

### Fügen Sie MDSS-Laufwerke hinzu

Sie können ein zweites Metadatenlaufwerk auf einem SolidFire-Knoten hinzufügen, indem Sie das Blocklaufwerk in Steckplatz 2 in ein Slice-Laufwerk konvertieren. Dies wird durch die Aktivierung der MDSS-Funktion (Multi-Drive Slice Service) erreicht. Um diese Funktion zu aktivieren, müssen Sie sich an den NetApp Support wenden.

Wenn Sie ein Slice-Laufwerk in einen verfügbaren Zustand bringen, muss möglicherweise ein ausgefallenes Laufwerk durch ein neues oder ein neues Ersatzlaufwerk ersetzt werden. Sie müssen das System-Slice-Laufwerk gleichzeitig hinzufügen, wenn Sie das Laufwerk für Steckplatz 2 hinzufügen. Wenn Sie versuchen, das Slice-Laufwerk für Steckplatz 2 allein oder vor dem Hinzufügen des Slice-Laufwerks hinzuzufügen, wird das System einen Fehler generieren.

1. Klicken Sie Auf **Cluster > Laufwerke**.

2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Wählen Sie die zu addieren Slice-Laufwerke aus.
4. Klicken Sie Auf **Massenaktionen**.
5. Klicken Sie Auf **Hinzufügen**.
6. Bestätigen Sie auf der Registerkarte \* Aktive Laufwerke\*, dass die Laufwerke hinzugefügt wurden.

## Entfernen Sie MDSS-Laufwerke

Sie können die MDSS-Laufwerke (Slice Service) mit mehreren Laufwerken entfernen. Dieser Vorgang gilt nur, wenn der Knoten über mehrere Slice-Laufwerke verfügt.



Wenn das System-Slice-Laufwerk und das Steckplatz-2-Laufwerk ausfallen, schaltet das System die Services ab und entfernt die Laufwerke. Wenn kein Ausfall auftritt und Sie die Laufwerke entfernen, müssen beide Laufwerke gleichzeitig entfernt werden.

1. Klicken Sie Auf **Cluster > Laufwerke**.
2. Klicken Sie auf der Registerkarte **Available** Drives auf das Kontrollkästchen für die zu entfernenden Slice Drives.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie Auf **Entfernen**.
5. Bestätigen Sie die Aktion.

## Fehlerbehebung für Nodes

Sie können Nodes zu Wartungs- oder Austauschzwecken aus einem Cluster entfernen. Sie sollten die NetApp Element-UI oder -API verwenden, um Nodes zu entfernen, bevor Sie sie in den Offline-Modus versetzen.

Ein Überblick über das Verfahren zum Entfernen von Storage-Nodes:

- Stellen Sie sicher, dass im Cluster genügend Kapazität verfügbar ist, um eine Kopie der Daten auf dem Node zu erstellen.
- Entfernen Sie Laufwerke aus dem Cluster mithilfe der UI oder der RemoveDrives API-Methode.

Daher werden Daten im System von Laufwerken des Node auf andere Laufwerke im Cluster migriert. Die Dauer dieses Prozesses hängt davon ab, wie viele Daten migriert werden müssen.

- Entfernen Sie den Node aus dem Cluster.

Beachten Sie die folgenden Überlegungen, bevor Sie einen Node herunterfahren oder hochfahren:

- Das Herunterfahren von Nodes und Clustern birgt Risiken, wenn die Performance nicht ordnungsgemäß erbracht wird.

Das Herunterfahren eines Node sollte unter Anleitung von NetApp Support erfolgen.

- Wenn ein Node unter jeder Art von Herunterfahren länger als 5.5 Minuten ausgefallen ist, beginnt die Double Helix Datensicherung mit der Aufgabe, einzelne replizierte Blöcke auf einen anderen Node zu

schreiben, um die Daten zu replizieren. In diesem Fall wenden Sie sich an den NetApp Support, um Hilfe bei der Analyse des ausgefallenen Nodes zu erhalten.

- Um einen Knoten sicher neu zu starten oder herunterzufahren, können Sie den API-Befehl Herunterfahren verwenden.
- Wenn ein Node sich in einem „down“ oder „Off“ befindet, müssen Sie den NetApp Support kontaktieren, bevor Sie ihn wieder in den Online-Status versetzen.
- Nachdem ein Node wieder online geschaltet wurde, müssen Sie die Laufwerke je nach Dauer des Service zurück zum Cluster hinzufügen.

## Finden Sie weitere Informationen

["Austausch eines fehlerhaften SolidFire-Chassis"](#)

["Austausch eines fehlerhaften H600S-Series-Knotens"](#)

## Schalten Sie ein Cluster aus

Gehen Sie wie folgt vor, um ein gesamtes Cluster herunterzufahren.

### Schritte

1. (Optional) Wenden Sie sich an den NetApp Support, um Hilfe beim Abschluss der ersten Schritte zu erhalten.
2. Vergewissern Sie sich, dass alle I/O-Vorgänge angehalten wurden.
3. Trennen Sie alle iSCSI-Sitzungen:
  - a. Navigieren Sie zur Management Virtual IP (MVIP)-Adresse auf dem Cluster, um die Element-UI zu öffnen.
  - b. Beachten Sie die in der Liste Knoten aufgeführten Knoten.
  - c. Führen Sie die Shutdown-API-Methode mit der Stopp-Option aus, die für jede Node-ID im Cluster angegeben ist.

Wenn Sie das Cluster neu starten, müssen Sie bestimmte Schritte durchführen, um zu überprüfen, ob alle Nodes online sind:

1. Vergewissern Sie sich, dass alle kritischen Schweregrade und `volumesOffline` Cluster-Fehler gelöst sind.
2. Warten Sie 10 bis 15 Minuten, bis sich das Cluster absetzen lässt.
3. Starten Sie, um die Hosts für den Zugriff auf die Daten aufzurufen.



Wenn Sie beim Einschalten der Knoten mehr Zeit einplanen und überprüfen möchten, ob sie nach der Wartung ordnungsgemäß sind, wenden Sie sich an den technischen Support, um Hilfe bei der Verzögerung der Datensynchronisierung zu erhalten, um unnötige bin-Synchronisierung zu vermeiden.

## Weitere Informationen

["Ordnungsgemäß Herunterfahren und Einschalten eines NetApp SolidFire/HCI Storage-Clusters"](#)

# Storage-Nodes: Dienstprogramme pro Node unterstützen

Sie können die Dienstprogramme pro Node verwenden, um Netzwerkprobleme zu beheben, wenn die Standard-Monitoring-Tools der NetApp Element-Software nicht genügend Informationen zur Fehlerbehebung enthalten. Dienstprogramme pro Node bieten spezifische Informationen und Tools, die Sie bei der Fehlerbehebung bei Netzwerkproblemen zwischen Nodes oder mit dem Management-Node unterstützen.

## Weitere Informationen

- [Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen](#)
- [Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node](#)
- [Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node](#)
- [Führen Sie Systemtests über die UI pro Node aus](#)
- [Führen Sie Systemdienstprogramme über die UI pro Node aus](#)

## Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen

Nach Eingabe der Management-Node-IP und Authentifizierung haben Sie in der Benutzeroberfläche per Node Zugriff auf Netzwerkeinstellungen, Cluster-Einstellungen sowie Systemtests und Dienstprogramme.

Wenn Sie die Einstellungen für einen Node in einem aktiven Status ändern möchten, der Teil eines Clusters ist, müssen Sie sich als Cluster-Administrator-Benutzer einloggen.



Sie sollten Nodes jeweils einzeln konfigurieren oder ändern. Sie sollten sicherstellen, dass die angegebenen Netzwerkeinstellungen den erwarteten Effekt haben und dass das Netzwerk stabil und gut funktioniert, bevor Sie Änderungen an einem anderen Node vornehmen.

1. Öffnen Sie die UI pro Node mit einer der folgenden Methoden:

- Geben Sie die Management-IP-Adresse gefolgt von :442 in einem Browser-Fenster ein, und melden Sie sich mit einem Admin-Benutzernamen und -Passwort an.
- Wählen Sie in der Element UI **Cluster > Nodes** aus und klicken Sie auf den Link Management-IP-Adresse für den Knoten, den Sie konfigurieren oder ändern möchten. Im geöffneten Browser-Fenster können Sie die Einstellungen des Node bearbeiten.



# Node01

**NETWORK SETTINGS** CLUSTER SETTINGS SYSTEM TESTS SYSTEM UTILITIES

## Network Settings

**Bond1G** Bond10G [Reset Changes](#)

Method	Link Speed
<input type="text" value="static"/>	<input type="text" value="1000"/>
IPv4 Address	IPv4 Subnet Mask
<input type="text"/>	<input type="text" value="255.255.255.0"/>
IPv4 Gateway Address	IPv6 Address
<input type="text"/>	<input type="text"/>
IPv6 Gateway Address	MTU
<input type="text"/>	<input type="text" value="1500"/>
DNS Servers	
<input type="text"/>	
Search Domains	
<input type="text"/>	

Bond Mode Status

### Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node

Sie können die Netzwerkeinstellungen des Storage-Nodes ändern, um dem Node einen neuen Satz an Netzwerkattributen zuzuweisen.

Sie können die Netzwerkeinstellungen für einen Speicherknoten auf der Seite **Netzwerkeinstellungen** sehen, wenn Sie sich beim Knoten `IP>:442/hcc/Node/Network-settings` anmelden(<https://<node>>). Sie können entweder **Bond1G** (Management) oder **Bond10G** (Storage) Einstellungen auswählen. In der folgenden Liste werden die Einstellungen beschrieben, die Sie ändern können, wenn sich ein Speicherknoten im Status „verfügbar“, „Ausstehend“ oder „aktiv“ befindet:

- **Methode**

Die Methode zum Konfigurieren der Schnittstelle. Mögliche Methoden:

- Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren.
- Manuell: Wird verwendet, um Schnittstellen zu definieren, für die keine Konfiguration standardmäßig erfolgt.
- dhcp: Wird verwendet, um eine IP-Adresse über DHCP zu erhalten.
- Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.

#### • **Verbindungsgeschwindigkeit**

Die von der virtuellen NIC ausgehandelte Geschwindigkeit.

#### • \* IPv4-Adresse\*

Die IPv4-Adresse für das eth0-Netzwerk.

#### • **IPv4-Subnetzmaske**

Adressbereiche des IPv4-Netzwerks.

#### • \* IPv4 Gateway-Adresse\*

Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

#### • \* IPv6-Adresse\*

Die IPv6-Adresse für das eth0-Netzwerk.

#### • \* IPv6 Gateway-Adresse\*

Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

#### • **MTU**

Größte Paketgröße, die ein Netzwerkprotokoll übertragen kann. Muss größer als oder gleich 1500 sein. Wenn Sie eine zweite Speicher-NIC hinzufügen, sollte der Wert 9000 sein.

#### • \* DNS-Server\*

Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

#### • **Domänen Suchen**

Suche nach zusätzlichen MAC-Adressen, die dem System zur Verfügung stehen.

#### • **Bond-Modus**

Dies kann einer der folgenden Modi sein:

- ActivePassive (Standard)
- ALB
- LACP

#### • **Status**

Mögliche Werte:

- UpAndRunning
- Runter
- Hoch

#### • **Virtual Network Tag**

Das Tag wurde beim Erstellen des virtuellen Netzwerks zugewiesen.

#### • **Routen**

Statische Routen zu bestimmten Hosts oder Netzwerken über die zugewiesene Schnittstelle, die die Routen für die Verwendung konfiguriert sind.

## **Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node**

Sie können die Cluster-Einstellungen für einen Storage-Node nach der Cluster-Konfiguration überprüfen und den Node-Hostnamen ändern.

In der folgenden Liste werden die Clustereinstellungen für einen Speicherknoten beschrieben, die auf der Seite **Cluster Settings** der UI pro Knoten-IP>:442/hcc/Node/Cluster-settings angegeben (<https://<nodesind.>

#### • \* Rolle\*

Rolle, die der Node im Cluster hat. Mögliche Werte:

- Storage: Storage oder Fibre Channel-Node
- Management: Node ist ein Management-Node.

#### • **Hostname**

Der Name des Node.

#### • \* Cluster\*

Der Name des Clusters.

#### • **Cluster Mitgliedschaft**

Status des Node. Mögliche Werte:

- Verfügbar: Der Node ist keinem Cluster-Namen zugeordnet und ist noch nicht Teil eines Clusters.
- Ausstehend: Der Node ist konfiguriert und kann einem bestimmten Cluster hinzugefügt werden. Für den Zugriff auf den Node ist keine Authentifizierung erforderlich.
- PendingActive: Das System installiert gerade kompatible Software auf dem Knoten. Nach Abschluss der Migration wird der Node in den Status „aktiv“ verschoben.
- Aktiv: Der Knoten nimmt an einem Cluster teil. Zum Ändern des Node ist eine Authentifizierung erforderlich.

#### • **Version**

Version der Element Software, die auf dem Node ausgeführt wird

- **Ensemble**

Knoten, die Teil des Datenbankensembles sind.

- **Knoten-ID**

ID wird zugewiesen, wenn dem Cluster ein Node hinzugefügt wird.

- \* Clusterschnittstelle\*

Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

- **Management-Schnittstelle**

Management-Netzwerkschnittstelle. Dies ist standardmäßig Bond1G, kann aber auch Bond10G verwenden.

- **Storage-Schnittstelle**

Storage-Netzwerk-Schnittstelle mit Bond10G.

- **Verschlüsselungsfähig**

Gibt an, ob der Node die Laufwerkverschlüsselung unterstützt.

## Führen Sie Systemtests über die UI pro Node aus

Sie können Änderungen an den Netzwerkeinstellungen testen, nachdem Sie sie zur Netzwerkkonfiguration übergeben haben. Sie können die Tests durchführen, um sicherzustellen, dass der Storage-Node stabil ist und ohne Probleme online geschaltet werden kann.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemtests**.
2. Klicken Sie neben dem Test, den Sie ausführen möchten, auf **Test ausführen** oder wählen Sie **Alle Tests ausführen**.



Alle Testvorgänge können zeitaufwändig sein und sollten nur Richtung NetApp Support ausgeführt werden.

- **Angeschlossenes Ensemble Testen**

Testet und überprüft die Verbindung zu einem Datenbankensemble. Standardmäßig verwendet der Test das Ensemble für den Cluster, dem der Knoten zugeordnet ist. Alternativ können Sie auch ein anderes Ensemble zur Prüfung der Konnektivität bereitstellen.

- \* Testen Sie Connect Mvip\*

Sendet eine Pings der angegebenen MVIP-Adresse (Management Virtual IP) und führt dann einen einfachen API-Aufruf an das MVIP aus, um die Konnektivität zu überprüfen. Standardmäßig verwendet der Test das MVIP für das Cluster, dem der Node zugeordnet ist.



- \* Testen Sie Connect Svip\*

Pings der angegebenen virtuellen Speicher-IP-Adresse (SVIP) mit ICMP-Paketen (Internet Control Message Protocol), die mit der auf dem Netzwerkadapter festgelegten Maximum Transmission Unit (MTU)-Größe übereinstimmen. Er stellt dann eine Verbindung zum SVIP als iSCSI-Initiator her. Standardmäßig verwendet der Test das SVIP für das Cluster, dem der Node zugeordnet ist.

- **Hardware-Konfiguration Testen**

Testet die Richtigkeit aller Hardware-Konfigurationen, validiert die richtigen Firmware-Versionen und bestätigt, dass alle Laufwerke installiert und ordnungsgemäß ausgeführt werden. Dies ist das gleiche wie bei den werkseitigen Tests.



Dieser Test ist ressourcenintensiv und sollte nur auf Anfrage des NetApp Supports ausgeführt werden.

- \* Testen Sie Lokale Konnektivität\*

Testet die Verbindung zu allen anderen Knoten im Cluster, indem an jeden Knoten die Cluster-IP (CIP) pinging. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

- **Test Lokalisieren Cluster**

Überprüft, ob der Node das in der Cluster-Konfiguration angegebene Cluster finden kann.

- **Netzwerk-Konfiguration Testen**

Stellt sicher, dass die konfigurierten Netzwerkeinstellungen mit den im System verwendeten Netzwerkeinstellungen übereinstimmen. Dieser Test dient nicht zur Erkennung von Hardwarefehlern, wenn ein Node aktiv an einem Cluster teilnimmt.

- **Ping Testen**

Gibt eine angegebene Liste von Hosts aus oder, wenn keine angegeben werden, erstellt dynamisch eine Liste aller registrierten Nodes im Cluster und pings für einfache Konnektivität.

- **Remote-Verbindung Testen**

Testet die Verbindung zu allen Knoten in Remote-gekoppelten Clustern durch Ping-Signal der Cluster-IP (CIP) an jedem Knoten. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

## Führen Sie Systemdienstprogramme über die UI pro Node aus

Über die UI pro Node kann der Storage-Node Supportpakete erstellen oder löschen, Konfigurationseinstellungen für Laufwerke zurücksetzen und Netzwerk- oder Cluster-Services neu starten.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemdienstprogramme**.
2. Klicken Sie auf die Schaltfläche für das Systemdienstprogramm, das Sie ausführen möchten.

## ◦ **Steuerleistung**

Neubooten, aus- und wieder einschalten oder den Node herunterfahren.



Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

Geben Sie die folgenden Parameter an:

- **Aktion:** Optionen umfassen Neustart und Anhalten (Ausschalten).
- **Aufwachsverzögerung:** Alle zusätzlichen Zeit, bevor der Node wieder online geht.

## ◦ **Node Logs Sammeln**

Erstellt ein Supportpaket unter dem Verzeichnis /tmp/Bundles des Node.

Geben Sie die folgenden Parameter an:

- **Bundle-Name:** Eindeutiger Name für jedes erstellte Support-Bundle. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.
- **Zusätzliche Args:** Dieser Parameter wird dem skript `sf_Make_Support_Bundle` zugeführt. Dieser Parameter sollte nur auf Anfrage des NetApp Support verwendet werden.
- **Timeout sec:** Geben Sie die Anzahl der Sekunden an, die auf jede einzelne Ping-Antwort warten sollen.

## ◦ **Node Logs Löschen**

Löscht alle aktuellen Supportpakete auf dem Knoten, die mit **Cluster Support Bundle erstellen** oder der `CreateSupportBundle` API-Methode erstellt wurden.

## ◦ **Laufwerke Zurücksetzen**

Initialisiert die Laufwerke und entfernt alle auf dem Laufwerk vorhandenen Daten. Sie können das Laufwerk in einem vorhandenen Knoten oder einem aktualisierten Knoten wiederverwenden.

Geben Sie den folgenden Parameter an:

- **Laufwerke:** Liste der Gerätenamen (keine Fahrererkennung) zum Zurücksetzen.

## ◦ **Netzwerk-Konfiguration Zurücksetzen**

Unterstützt die Behebung von Netzwerkkonfigurationsproblemen für einen einzelnen Knoten und setzt die Netzwerkkonfiguration eines einzelnen Knotens auf die Werkseinstellungen zurück.

## ◦ **Knoten Zurücksetzen**

Setzt einen Knoten auf die Werkseinstellungen zurück. Alle Daten werden entfernt, die Netzwerkeinstellungen für den Node jedoch während dieses Vorgangs erhalten. Nodes können nur zurückgesetzt werden, wenn sie einem Cluster nicht zugewiesen sind und sich im verfügbaren Status befinden.



Bei Verwendung dieser Option werden alle Daten, Pakete (Software-Upgrades), Konfigurationen und Protokolldateien vom Knoten gelöscht.

## ◦ **Netzwerk Neu Starten**

Startet alle Netzwerkdienste auf einem Node neu.



Dieser Vorgang kann zu einem vorübergehenden Verlust der Netzwerkverbindung führen.

#### ◦ **Neustart Service**

Startet die Element Softwareservices auf einem Node neu.



Dieser Vorgang kann zu einer temporären Node-Serviceunterbrechung führen. Sie sollten diesen Vorgang nur auf Anweisung des NetApp Supports durchführen.

Geben Sie die folgenden Parameter an:

- Dienst: Dienstname, der neu gestartet werden soll.
- Aktion: Aktion, die auf dem Dienst ausgeführt werden soll. Die Optionen umfassen Start, Stopp und Neustart.

## **Arbeiten Sie mit dem Management-Node**

Sie können den Management-Node (mNode) verwenden, um Systemservices zu aktualisieren, Cluster-Assets und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen, Active IQ für das System-Monitoring zu konfigurieren und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.



Als Best Practice wird nur ein Management Node mit einer VMware vCenter Instanz verknüpft, sodass nicht dieselben Storage- und Computing-Ressourcen oder vCenter Instanzen in mehreren Management Nodes definiert werden müssen.

Weitere Informationen finden Sie unter "[Dokumentation des Management-Node](#)".

## **Erläuterung der Cluster-Auslastungsebenen**

Der Cluster, auf dem Element Software ausgeführt wird, generiert Cluster-Fehler, um den Storage-Administrator zu warnen, wenn die Kapazität des Clusters knapp wird. Es gibt drei Ebenen der Cluster-Fülle, die alle in der NetApp Element UI angezeigt werden: Warnung, Fehler und kritisch.

Das System verwendet den BlockClusterFull-Fehlercode, um vor der Speicherfülle des Clusterblocks zu warnen. Sie können die Schweregrade für die Cluster-Fülle über die Registerkarte Meldungen der Element UI anzeigen.

Die folgende Liste enthält Informationen zum Schweregrad BlockClusterFull:

### • **Warnung**

Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Blockgröße des Clusters dem Fehlergrad nähert. Diese Stufe wird standardmäßig auf drei Prozent unter der Fehlerebene festgelegt und kann über die Element-UI und -API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für Cluster. Sie müssen mehr Kapazität hinzufügen oder sofort Kapazität freigeben.

- \* Kritisch\*

Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.

Das System verwendet den MetadaClusterFull Fehlercode, um über die Speicherfülle des Clusters zu warnen. Sie können die Cluster-Metadaten-Storage-Fülle im Abschnitt Cluster-Kapazität auf der Übersichtsseite der Registerkarte Berichterstellung in der Element UI anzeigen.

Die folgende Liste enthält Informationen zu den Schweregraden für MetadatenClusterFull:

- **Warnung**

Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Metadatenkapazität des Clusters dem Schweregrad „Fehler“ nähert. Standardmäßig wird diese Ebene auf drei Prozent unter der Fehlerebene gesetzt und kann über die Element-API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für Cluster. Sie müssen mehr Kapazität hinzufügen oder sofort Kapazität freigeben.

- \* Kritisch\*

Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.



Folgendes gilt für Cluster-Schwellenwerte mit zwei Nodes:

- Metadaten-Fehler liegt 20 % unter dem kritischen Wert.
- Unter dem kritischen Block-Auslastungsfehler liegt ein Block-Laufwerk (einschließlich ungenutzter Kapazität). Das bedeutet, dass es sich um zwei Blocklaufwerke handelt, die weniger kritisch sind.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.