Überwachen Sie die System-Performance

VCP

NetApp
November 18, 2025

Inhalt

Überwachen Sie die System-Performance

Überwachung der Systemleistung mit Berichtsoptionen

Sie können Informationen über die Komponenten und die Performance des Clusters mithilfe der Berichtsseiten des NetApp Element Plug-ins für VMware vCenter Server anzeigen.

Mit dem vCenter Plug-in können Sie Clusterkomponenten und die Performance auf folgende Weise überwachen:

- "Überwachen Sie den allgemeinen Cluster-Zustand auf der Seite Übersicht"
- "Überwachen Sie Systemmeldungen"
- "Überwachen Sie Ereignisprotokolle zur Fehlerbehebung"
- "Monitoring der Volume Performance"
- "Überwachen Sie iSCSI-Sitzungen, um den Verbindungsstatus zu ermitteln"
- "Überwachen Sie das VM Performance Tiering mit QoSSIOC-Ereignissen"

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Überwachen Sie den allgemeinen Cluster-Zustand auf der Seite Übersicht

Sie können allgemeine Cluster-Informationen für den ausgewählten Cluster anzeigen, einschließlich Gesamtkapazität, Effizienz und Performance. Sie finden sie auf der Seite Übersicht der Registerkarte Berichterstellung über den Erweiterungspunkt NetApp Element Management des NetApp Element Plug-ins für VMware vCenter Server.

Schritte

1. Öffnen Sie über das vCenter Plug-in die Registerkarte **Reporting**:
   - Ab Element vCenter Plug-in 5.0 wählen Sie **NetApp Element Remote Plugin > Management > Reporting**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Reporting** aus.
2. Überwachen Sie die Daten auf der Seite **Übersicht**.

Berichtsübersicht Seitendaten

Die folgenden Daten werden auf der Seite Berichtsübersicht angezeigt:

- **Clusterkapazität**: Die verbleibende Kapazität für Block-Speicher, Metadaten und bereitgestellten Speicherplatz. Bewegen Sie den Zeiger über den Fortschrittsbalken, um Informationen zu

Schwellenwerten anzuzeigen.

- **Clusterinformationen**: Für den Cluster spezifische Informationen wie Clustername, Version der auf dem Cluster ausgeführten NetApp Element-Software, MVIP- und SVIP-Adressen sowie Anzahl der Knoten, 4k IOPS, Volumes und Sitzungen auf dem Cluster.
  - **Cluster Name**: Der Name für den Cluster.
  - **Speicher-IP (SVIP)**: Die virtuelle Speicher-IP-Adresse (SVIP).
  - **Management-IP (MVIP)**: Die virtuelle Management-IP-Adresse (MVIP).
  - **SVIP VLAN Tag**: Die VLAN-Kennung für die Master-SVIP-Adresse.
  - **MVIP VLAN Tag**: Die VLAN-Kennung für die Master MVIP-Adresse.
  - **Knotenanzahl**: Die Anzahl der aktiven Knoten im Cluster.
  - **Cluster 4K IOPS**: Die Anzahl der 4096 (4K) Blöcke, die vom Cluster in einer Sekunde gelesen/geschrieben werden können.
  - **Element OS Version**: Die Version der NetApp Element Software, die der Cluster ausführt.
  - **Anzahl der Volumes**: Die Gesamtzahl der Volumes, ohne virtuelle Volumes, auf dem Cluster.
  - **Anzahl virtueller Volumes**: Die Gesamtzahl der virtuellen Volumes auf dem Cluster.
  - **ISCSI-Sitzungen**: Die iSCSI-Sitzungen, die mit dem Cluster verbunden sind.
  - **Fibre Channel-Sitzungen**: Die Fibre Channel-Sitzungen, die mit dem Cluster verbunden sind.
- **Cluster-Effizienz**: Insgesamt genutzte Systemkapazität unter Berücksichtigung von Thin Provisioning, Deduplizierung und Komprimierung. Der berechnete Vorteil für das Cluster wird durch einen Vergleich der Kapazitätsauslastung auf einem herkömmlichen Storage-System ohne Thin Provisioning, Deduplizierung und Komprimierung berechnet.
- **Protection Domains**: Eine Zusammenfassung der Schutz-Domänen-Überwachung für den Cluster.

  Die Funktion der Sicherungsdomänen ist nicht mit Clustern mit zwei Knoten kompatibel.

  - **Protection Domains Monitoring Level**: Die vom Benutzer ausgewählten Schutz-Domain-Resiliency-Level. Mögliche Werte sind Chassis oder Node. Grün zeigt an, dass das Cluster in der Lage ist, die ausgewählte Überwachungsstufe zu erreichen. Rot zeigt an, dass das Cluster nicht mehr in der Lage ist, den ausgewählten Monitoring-Level zu überwachen und dass eine Korrekturmaßnahme erforderlich ist.
  - **Verbleibende Blockkapazität**: Gibt den Prozentsatz der Blockkapazität an, die zur Aufrechterhaltung des ausgewählten Stabilitätsniveaus verbleibt.
  - **Metadatenkapazität**: Gibt an, ob es genügend Metadaten-Kapazität zur Heilung nach einem Ausfall gibt, während gleichzeitig die Datenverfügbarkeit nicht unterbrochen wird. „Normal“ (grün) zeigt an, dass das Cluster über ausreichende Metadaten verfügt, um die ausgewählte Überwachungsebene beizubehalten. Voll (rot) zeigt an, dass das Cluster nicht mehr in der Lage ist, den ausgewählten Monitoring-Level zu überwachen und dass eine Korrekturmaßnahme erforderlich ist.
- **Systemzustand der benutzerdefinierten Schutzdomäne**: Zeigt den Integritätsstatus der benutzerdefinierten Schutzdomäne für den Cluster an, wenn eine benutzerdefinierte Schutzdomäne auf dem Cluster konfiguriert ist.

  Die folgenden Daten zeigen den Schutz an, der gegen den Ausfall einer der benutzerdefinierten Schutzdomänen für das Cluster verfügbar ist.

  - **Schutzstufe**: Gibt den Status des gesamten Schutzniveaus an.

- **Block Capacity**: Zeigt den aktuellen Status des Schutzniveaus des Block Services Subsystems an.

  Sie gibt außerdem den Schwellenwert für die Gesamtkapazität an, bei dem die Ausfallsicherheit verloren geht.

- **Metadaten-Kapazität**: Zeigt den aktuellen Status des Metadaten-Services-Subsystems an.
- **Ensemble Nodes**: Gibt den aktuellen Status des Schutzniveaus des Teilsystems Ensemblemitglieder an.

- **Bereitgestellte IOPS**: Eine Zusammenfassung, wie die IOPS des Volumes auf dem Cluster überprovisioniert werden können. Bereitgestellte IOPS-Berechnungen basieren auf der Summe der minimalen IOPS-Werte, der maximalen IOPS-Werte und des IOPS-Burst für alle Volumes im Cluster geteilt durch die für das Cluster ermittelten maximalen IOPS-Werte.

  Wenn beispielsweise vier Volumes im Cluster vorhanden sind, jedes mit einem Minimum von 500 IOPS, einem Maximum an IOPS von 15,000 und einem Burst-IOPS von 15,000, würde die Gesamtzahl der IOPS-Minimum 2,000 beträgt, die maximale IOPS insgesamt 60,000 und der IOPS-Burst insgesamt 60,000. Wenn der Cluster mit einem maximalen IOPS von 50,000 bewertet wird, dann wären die Berechnungen folgendes: **Minimum IOPS**: 2000/50000 = 0.04x **maximale IOPS**: 60000/50000 = 1,20x **Burst IOPS**: 60000/50000 = 1.20x 1.00x 1.00x ist die Baseline, mit der bereitgestellte IOPS den bewerteten IOPS für den Cluster entsprechen.

- **Clusterzustand**: Die Hardware, Kapazität und Sicherheitskomponenten des Funktionszustands des Clusters. Farbcodes zeigen Folgendes an:
  - **Grün**: Gesund
  - **Gelb**: Kritisch
  - **Rot**: Fehler
- **Cluster Input/Output**: Der I/O, der derzeit auf dem Cluster läuft. Die Werte werden auf Basis der vorherigen E/A-Messung mit den aktuellen E/A-Messungen berechnet. Dies sind die im Diagramm angezeigten Messungen:
  - **Gesamt**: Die kombinierten Lese- und Schreib-IOPS im System.
  - **Read**: Die Anzahl der Lese-IOPS.
  - **Schreiben**: Die Anzahl der Schreib-IOPS.
- **Clusterdurchsatz**: Die Bandbreitenaktivität für Lese-, Schreib- und Gesamtbandbreite auf dem Cluster:
  - **Gesamt**: Die Gesamtzahl der MB/s, die für Lese- und Schreibaktivität im Cluster verwendet werden.
  - **Lesen**: Die Leseaktivität in MB/s für den Cluster.
  - **Write**: Die Schreibaktivität in MB/s für den Cluster.
- **Performance-Auslastung**: Der Prozentsatz der verbrauchten Cluster-IOPS. Ein 250.000 IOPS-Cluster mit 100.000 IOPS würde einen Verbrauch von 40 % belegen.

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Überwachen Sie Systemmeldungen

Sie können Warnungen überwachen, d. h. Informationen, Warnungen oder Fehler, die angeben, wie gut das Cluster ausgeführt wird.

Warnmeldungen sind Cluster-Fehler oder -Fehler und werden bei Auftreten gemeldet. Die meisten Fehler lösen sich automatisch, bei manchen ist jedoch unter Umständen ein manuelles Eingreifen erforderlich. Das System meldet bei jeder Meldung auf der Seite „Meldungen“ Alarmfehlercodes. Fehlercodes helfen Ihnen dabei festzustellen, welche Komponente des Systems die Warnmeldung erfahren hat und warum die Warnmeldung generiert wurde. Siehe "Liste der Systemwarnmeldungen" Für eine Beschreibung und Schritte zur Problembehebung.

Nachdem Sie das Problem behoben haben, fragt das System sich ab und identifiziert das Problem als gelöst. Anschließend werden alle Informationen über die Warnmeldung einschließlich des Datums, an dem sie behoben wurde, in die aufgelöste Ansicht verschoben.

Schritte

1. Öffnen Sie über das vCenter Plug-in die Registerkarte **Management**:
   - Ab Element vCenter Plug-in 5.0 wählen Sie **NetApp Element Remote Plugin > Management > Management**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Verwaltung** aus.
2. Wählen Sie **Reporting** > **Alerts**.
3. Überwachen Sie die folgenden Cluster-Warnungsinformationen:
   - **ID**: Eindeutige ID für eine Clusterwarnung.
   - **Severity**
     - **Warnung**: Ein kleines Problem, das bald Aufmerksamkeit erfordert. System-Upgrades sind nach wie vor auf dieser Schweregrade zulässig.
     - **Fehler**: Ein Ausfall, der zu Performance-Verschlechterung oder Verlust von Hochverfügbarkeit führen kann. Fehler sollten in der Regel den Dienst nicht anderweitig beeinträchtigen.
     - **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.
     - **BestPractice**: Eine empfohlene Best Practice für die Systemkonfiguration wird nicht verwendet.
   - **Typ**
     - **Knoten**: Fehler, der einen ganzen Knoten betrifft.
     - **Drive**: Störung bei einem einzelnen Antrieb.
     - **Cluster**: Fehler, die den gesamten Cluster betreffen.
     - **Service**: Fehler, der einen Dienst auf dem Cluster betrifft.
     - **Volumen**: Fehler, der ein Volumen auf dem Cluster beeinflusst.
   - **Knoten**: Knoten-ID für den Knoten, auf den sich dieser Fehler bezieht. Bei Knoten- und Laufwerkfehlern enthalten, andernfalls auf - (Dash) gesetzt.
   - **Laufwerk-ID**: Laufwerk-ID für das Laufwerk, auf das sich dieser Fehler bezieht. Bei Fahrfehlern enthalten, ansonsten auf - (Dash) eingestellt.

- **Fehlercode**: Ein beschreibender Code, der angibt, was den Fehler verursacht hat.
- **Details**: Detaillierte Beschreibung des Fehlers.
- **Zeit**: Diese Überschrift ist nur in der Active Filteransicht sichtbar. Datum und Uhrzeit der Fehlerprotokollierung.
- **Auflösungsdatum**: Diese Überschrift ist nur in der aufgelösten Filteransicht sichtbar. Datum und Uhrzeit, zu der der Fehler behoben wurde.

4. Um zu überprüfen, ob das Problem behoben wurde, suchen Sie in der Ansicht „gelöst“ nach dem Problem.

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Liste der Systemwarnmeldungen

Das System meldet bei jeder Warnmeldung Fehlercodes, mit denen Sie feststellen können, welche Komponente des Systems die Warnmeldung erfahren hat und warum die Warnmeldung generiert wurde. Sie können die Fehlercodes mit dem Plug-in-Erweiterungspunkt anzeigen:

- Ab dem Element vCenter Plug-in 5.0 wählen Sie **NetApp Remote Plugin > Management > Reporting > Alerts** aus.
- Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Berichte > Alarme** aus.

In der folgenden Liste werden die verschiedenen Typen von Systemwarnmeldungen aufgeführt.

- **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)1; 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` Ein Fehler wird nicht bei einem Knoten generiert, der bereits über einen BMC-Fehler verfügt, oder wenn der BMC eines Knotens während des Upgrades ausfällt. Die BMCs, die die Selbsttests während des Upgrades nicht bestanden haben, geben eine aus `BmcSelfTestFailed` Warnfehler, 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.

- **ClusterIOPSAreüberProvistiert**

  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 Schlüsselserver.
- 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 Laufwerksicherheit 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 Schlüsselserver.
  - 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.

- **FileSystemIsReadOnly**

  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 Dienstanbieters 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 UpdateIdpConfiguration 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-Netzwerkkonnektivität 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 ModifyKeyServerkmip, 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 ModifyKeyServerkmip, 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 ModifyKeyServerkmip, 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 ModifyKeyServerkmip, 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 ModifyKeyServerkmip, 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 ModifyKeyServerkmip, um das richtige KMIP-Client-Zertifikat zu installieren.

- **KmipServerFault**
  - Verbindungsfehler

    Um diesen Fehler zu beheben, überprüfen Sie, ob der externe Schlüsselserver aktiv ist und über das Netzwerk erreichbar ist. Verwenden Sie TestKeyServerKimp und TestKeyProviderKmip, 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 Schlüsselserver 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 cMemCtlrCorrectableErrWarnThreshold und cMemCtlrCorrectableErrWarnDauer wird angegeben.	Warnung	Korrigierbare ECC-Speicherfehler oberhalb des Schwellenwerts für Speicher-Controller: <Prozessor> <Speicher-Controller>
Ein Speicher-Controller meldet cErrorCount über cMemCtlrCorrectableErrWarnThreshold 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 cMemCtlrUncorregictErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt
Ein Speicher-Controller meldet einen uErrorCount von mindestens cMemCtlrUncorregictErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt

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

- **SpeichernUserageThreshold**

  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)1; 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. • NvmLifetimeFehler • NvmLifetimeStatus • EnergiengySourceLifetimeStatus • EnergiengySourceTemperatureStatus • WarningThresholdExceped

Fehler	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: • Der Mount-Punkt für NVRAM-Gerät ist nicht vorhanden. • Die NVRAM-Gerätepartition ist nicht vorhanden. • Die NVRAM-Gerätepartition ist vorhanden, aber nicht angehängt.
Kritisch	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. • Persistenz verloren • ArmStatusSaveNArmed • CsaveStatusfehler

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-Volume 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.

Überwachen Sie Ereignisprotokolle zur Fehlerbehebung

Sie können Ereignisprotokolle zusammen mit eventuell auftretenden Cluster-Fehlern auf Vorgänge prüfen, die am ausgewählten Cluster durchgeführt werden. Die meisten Fehler werden automatisch vom System behoben. Für andere Fehler ist unter Umständen ein manuelles Eingreifen erforderlich.

Schritte

1. Öffnen Sie über das vCenter Plug-in die Registerkarte **Management**:
   - Ab Element vCenter Plug-in 5.0 wählen Sie **NetApp Element Remote Plugin > Management > Management**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Verwaltung** aus.
2. Wählen Sie **Berichterstellung** > **Ereignisprotokoll**.
3. Um Details zu überprüfen, wählen Sie ein Ereignis aus und klicken Sie auf **Details**.
4. Überprüfen Sie die Ereignisinformationen, einschließlich der folgenden:
   - **Ereignistyp**: Die Art des protokollierten Ereignisses, z. B. API-Ereignisse oder Klonereignisse.
   - **Service-ID**: Die ID des Dienstes, der das Ereignis gemeldet hat (falls zutreffend). Der Wert ist Null, wenn der Fehler nicht einem Dienst zugeordnet ist.
   - **Node** oder **Drive ID**: Die ID des Knotens oder Laufwerks, der das Ereignis gemeldet hat (falls

zutreffend).

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 Ereignistyp 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 können.

- **ApiEvent**: Ereignisse, die von einem Benutzer über eine API oder eine Web-Benutzeroberfläche initiiert werden, die Einstellungen ändern.
- **BinAssignmentsEreignis**: Ereignisse im Zusammenhang mit der Zuweisung von Datenfächern. Fächer sind im Wesentlichen Container, in denen Daten gespeichert und über das gesamte Cluster hinweg zugeordnet sind.
- **BinSyncEvent**: Systemereignisse, die sich auf eine Neuzuweisung von Daten zwischen Blockdiensten beziehen.
- **BsCheckEvent**: Systemereignisse im Zusammenhang mit Blockservice-Prüfungen.
- **BsKillEvent**: Systemereignisse im Zusammenhang mit Blockterminationen.
- **BulkOpEvent**: Ereignisse im Zusammenhang mit Operationen, die auf einem ganzen Volume ausgeführt werden, wie z.B. Backup, Wiederherstellung, Snapshot oder Klon.
- **CloneEvent**: Ereignisse im Zusammenhang mit Volume Cloning.
- **ClusterMasterEvent**: Ereignisse, die bei der Clusterinitialisierung oder bei Konfigurationsänderungen am Cluster auftreten, wie das Hinzufügen oder Entfernen von Knoten.
- **CsumEvent**: Ereignisse im Zusammenhang mit ungültigen Daten-Prüfsummen auf der Platte.
- **DataEvent**: Ereignisse zum Lesen und Schreiben von Daten.
- **DbEvent**: Ereignisse im Zusammenhang mit der globalen Datenbank, die von Ensemble-Knoten im Cluster gepflegt werden.
- **DriveEvent**: Ereignisse im Zusammenhang mit dem Fahrbetrieb.
- **VerschlüsselungAtRestEvent**: Ereignisse im Zusammenhang mit dem Verschlüsselungsvorgang auf einem Cluster.
- **EnsembleEvent**: Ereignisse im Zusammenhang mit der Erhöhung oder Verringerung der Anzahl der Knoten in einem Ensemble.
- **Fiber ChannelEvent**: Ereignisse im Zusammenhang mit der Konfiguration und Verbindungen zu den Knoten.
- **GcEvent**: Ereignisse im Zusammenhang mit Prozessen laufen alle 60 Minuten, um Speicher auf Blocklaufwerken zurückzugewinnen. Dieser Prozess wird auch als Garbage Collection bezeichnet.
- **IeEvent**: Interner Systemfehler.
- **InstallEvent**: Automatische Softwareinstallationsereignisse. Die Software wird automatisch auf einem ausstehenden Node installiert.
- **ISCSIEvent**: Ereignisse im Zusammenhang mit iSCSI-Problemen im System.

- **LimitEvent**: Ereignisse im Zusammenhang mit der Anzahl von Volumes oder virtuellen Volumes in einem Konto oder im Cluster, die sich dem maximal zulässigen Wert nähern.
- **MaincenanceModeEvent**: Ereignisse im Zusammenhang mit dem Node-Wartungsmodus, z. B. Deaktivieren des Node.
- **NetworkEvent**: Ereignisse zum Status virtueller Netzwerke.
- **HardwareHardware-Event**: Veranstaltungen zu Problemen, die auf Hardware-Geräten erkannt werden.
- **RemoteClusterEvent**: Ereignisse im Zusammenhang mit der Remote-Cluster-Kopplung.
- **SchedulerEvent**: Ereignisse im Zusammenhang mit geplanten Snapshots.
- **ServiceEvent**: Ereignisse im Zusammenhang mit dem System-Service-Status.
- **SliceEvent**: Ereignisse im Zusammenhang mit dem Slice Server, z. B. Entfernen eines Metadatenlaufwerks oder -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)}
  ```

- **SnmpTrapEvent**: Veranstaltungen im Zusammenhang mit SNMP-Traps.
- **StatEvent**: Ereignisse im Zusammenhang mit Systemstatistiken.
- **TsEvent**: Veranstaltungen 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**: Veranstaltungen in Verbindung mit einem VASA-Provider (vSphere APIs for Storage Awareness).

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Monitoring der Volume Performance

Sie können Leistungsinformationen für alle Volumes im ausgewählten Cluster auf der Registerkarte „Reporting“ des Plug-in-Erweiterungspunkts anzeigen.

Schritte

1. Öffnen Sie über das vCenter Plug-in die Registerkarte **Reporting**:
   - Ab Element vCenter Plug-in 5.0 wählen Sie **NetApp Element Remote Plugin > Management > Reporting**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Reporting** aus.
2. Wählen Sie **Volumenleistung**.
3. Um zu ändern, wie oft die Daten auf der Seite aktualisiert werden, klicken Sie auf **jede Liste aktualisieren** und wählen Sie einen Wert aus.

   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.

Volume Performance-Daten

- **Name**: Name des Volumens, als es erstellt wurde.
- **Konto**: Der Name des Kontos, der dem Volume zugewiesen ist.
- **Access Groups**: Der Name der Volume Access Group oder der Gruppen, zu denen das Volume gehört.
- **Auslastung des Volumens %**: Ein Prozentwert, der beschreibt, wie viel der Client das Volume nutzt.

  Mögliche Werte:

- 0 = der Client verwendet das Volume nicht
- 100 = der Client verwendet das Maximum
- >100 = der Kunde verwendet den Burst
- **IOPS insgesamt**: Die Gesamtzahl der IOPS (Lese- und Schreibvorgänge), die derzeit auf dem Volume ausgeführt werden.
- **Lese-IOPS**: Die Gesamtzahl der derzeit ausgeführten Lese-IOPS gegen das Volume.
- **Schreib-IOPS**: Die Gesamtzahl der Schreib-IOPS, die derzeit auf dem Volume ausgeführt werden.
- **Gesamtdurchsatz**: Der Gesamtdurchsatz (Lesen und Schreiben), der derzeit mit dem Volumen ausgeführt wird.
- **Lesedurchsatz**: Die Gesamtmenge des aktuell ausgeführten Lesedurchsatzes gegen das Volumen.
- **Schreibdurchsatz**: Die Gesamtmenge des derzeit ausgeführten Schreibdurchsatzes gegen das Volumen.
- **Gesamte Latenz (ms)**: Die durchschnittliche Zeit in Mikrosekunden, um Lese- und Schreibvorgänge auf einem Volumen abzuschließen.
- **Lese-Latenz (ms)**: Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge auf das Volumen in den letzten 500 Millisekunden abzuschließen.
- **Schreiblatenz (ms)**: Die durchschnittliche Zeit in Mikrosekunden, um Schreibvorgänge auf ein Volumen in den letzten 500 Millisekunden abzuschließen.
- **Warteschlangentiefe**: Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf das Volume.
- **Durchschnittliche I/O-Größe**: Durchschnittliche Größe in Bytes der letzten I/O auf das Volumen in den letzten 500 Millisekunden.

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Überwachen Sie iSCSI-Sitzungen, um den Verbindungsstatus zu ermitteln

Im NetApp Element-Plug-in für VMware vCenter Server können Sie Informationen zu iSCSI-Sitzungen anzeigen, die mit dem ausgewählten Cluster verbunden sind.

Schritte

1. Öffnen Sie über das vCenter Plug-in die Registerkarte **Reporting**:
   - Ab Element vCenter Plug-in 5.0 wählen Sie **NetApp Element Remote Plugin > Management > Reporting**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Verwaltung > Reporting** aus.
2. Wählen Sie **iSCSI-Sitzungen**.

ISCSI-Sitzungsdaten

- **Node**: Der Node, der die primäre Metadatenpartition für das Volume hostet.
- **Konto**: Der Name des Kontos, der das Volumen besitzt. Wenn der Wert leer ist, wird ein Bindestrich (-) angezeigt.
- **Volume**: Der auf dem Knoten angegebene Volumenname.
- **Volumen-ID**: ID des Volumes, das mit dem Ziel-IQN verknüpft ist.
- **Initiator-ID**: Eine vom System generierte ID für den Initiator.
- **Initiator Alias**: Ein optionaler Name für den Initiator, der das Finden des Initiators in einer langen Liste erleichtert.
- **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 Knotens, der das Volume hostet.
- **Ziel-IQN**: Der IQN des Volumens.
- **Erstellt am**: Datum der Gründung der Sitzung.

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"

Überwachen Sie das VM Performance Tiering mit QoSSIOC-Ereignissen

Sie können Ereignisse in Bezug auf QoSSIOC anzeigen, wenn eine VM mit einem QoS-

fähigen Datastore neu konfiguriert oder ein Strom- oder Gastereignis ausgegeben wird.

Sie können QoSSIOC-Ereignisse vom Plug-in-Erweiterungspunkt im NetApp Element Plug-in für vCenter Server anzeigen.

QoSSIOC-Ereignisse werden von lokal hinzugefügten Clustern angezeigt. Melden Sie sich in einer Linked Mode-Umgebung beim vSphere Web Client an, der den Cluster lokal hinzugefügt hat, um QoSSIOC-Ereignisse für diesen Cluster anzuzeigen.

- Beginnend mit dem Element vCenter Plug-in 5.0, zu nutzen "VCenter Linked Mode", Sie registrieren das Element Plug-in über einen separaten Management-Node für jeden vCenter Server, der NetApp SolidFire Storage Cluster managt.
- Mit dem NetApp Element Plug-in für vCenter Server 4.10 und früher verwalten Sie Clusterressourcen von anderen vCenter Servern mithilfe "VCenter Linked Mode" Ist auf lokale Storage-Cluster beschränkt

Was Sie benötigen

- Mindestens ein Cluster muss hinzugefügt und ausgeführt werden.
- Der QoSSIOC-Dienst muss über die Seite QoSSIOC-Einstellungen für das Plug-in konfiguriert und verifiziert werden.
- Mindestens ein Datastore muss die QoSSIOC-Automatisierung aktiviert haben.

Schritte

1. Öffnen Sie in Ihrem vSphere Web Client die Registerkarte * QoSSIOC Events*:
   - Beginnend mit Element vCenter Plug-in 5.0, wählen Sie **NetApp Element Remote Plugin > Konfiguration > QoSSIOC Ereignisse**.
   - Wählen Sie für Element vCenter Plug-in 4.10 und früher die Option **NetApp Element-Konfiguration > QoSSIOC-Ereignisse** aus.

QoSSIOC-Ereignisdaten

- **Datum**: Datum und Uhrzeit des QoSSIOC-Events.
- **Datenspeichername**: Der benutzerdefinierte Datenspeichername.
- **Cluster IP**: Die IP-Adresse des Clusters, der den Datenspeicher enthält, aus dem das Ereignis stammt.
- **Volume ID**: Die vom System generierte ID für das zugehörige Volume.
- **Min IOPS**: Die aktuelle IOPS-QoS-Einstellung für das Volume.
- **Max IOPS**: Die aktuelle maximale IOPS QoS Einstellung des Volumes.
- **Burst IOPS**: Die aktuelle maximale Burst-QoS-Einstellung des Volumes.
- **Burst Time**: Die Länge der Zeit, die ein Burst erlaubt.

Weitere Informationen

- "NetApp HCI-Dokumentation"
- "Seite „SolidFire und Element Ressourcen“"