Ereignisse verwalten

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

Ereignisse verwalten

Ereignisse helfen Ihnen, Probleme in den überwachten Clustern zu identifizieren.

Was sind Active IQ Plattformereignisse?

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden erstellt, indem ein Regelsatz für AutoSupport -Nachrichten ausgeführt wird, die von allen von Unified Manager überwachten Speichersystemen generiert werden.

Weitere Informationen finden Sie unter "So werden Active IQ Plattformereignisse generiert".

Unified Manager sucht automatisch nach einer neuen Regeldatei und lädt nur dann eine neue Datei herunter, wenn neuere Regeln vorhanden sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Speicherverwaltung** > **Ereigniseinrichtung** > **Regeln hochladen** hochladen.

Diese Active IQ -Ereignisse überschneiden sich nicht mit vorhandenen Unified Manager-Ereignissen und identifizieren Vorfälle oder Risiken in Bezug auf Systemkonfiguration, Verkabelung, bewährte Methoden und Verfügbarkeitsprobleme.

Weitere Informationen zum Aktivieren von Plattformereignissen finden Sie unter"Aktivieren von Active IQ Portalereignissen" . Weitere Informationen zum Hochladen von Regeldateien finden Sie unter"Hochladen einer neuen Active IQ Regeldatei" .

NetApp Active IQ ist ein Cloud-basierter Service, der prädiktive Analysen und proaktiven Support zur Optimierung des Speichersystembetriebs in der NetApp Hybrid Cloud bietet. Sehen "NetApp Active IQ" für weitere Informationen.

Was sind Event Management System-Ereignisse?

Das Event Management System (EMS) sammelt Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und stellt Mechanismen zur Ereignisweiterleitung bereit. Diese ONTAP -Ereignisse können als EMS-Ereignisse im Unified Manager gemeldet werden. Zentralisierte Überwachung und Verwaltung erleichtern die Konfiguration kritischer EMS-Ereignisse und Warnbenachrichtigungen basierend auf diesen EMS-Ereignissen.

Die Unified Manager-Adresse wird dem Cluster als Benachrichtigungsziel hinzugefügt, wenn Sie den Cluster zu Unified Manager hinzufügen. Ein EMS-Ereignis wird gemeldet, sobald das Ereignis im Cluster auftritt.

Es gibt zwei Methoden zum Empfangen von EMS-Ereignissen in Unified Manager:

- Eine bestimmte Anzahl wichtiger EMS-Ereignisse wird automatisch gemeldet.
- Sie können den Empfang einzelner EMS-Ereignisse abonnieren.

Die von Unified Manager generierten EMS-Ereignisse werden je nach der Methode, mit der das Ereignis generiert wurde, unterschiedlich gemeldet:

Funktionalität	Automatische EMS-Nachrichten	Abonnierte EMS-Nachrichten
Verfügbare EMS-Ereignisse	Teilmenge der EMS-Ereignisse	Alle EMS-Veranstaltungen
Name der EMS-Nachricht bei Auslösung	Unified Manager-Ereignisname (konvertiert vom EMS-Ereignisnamen)	Unspezifisch im Format „Fehler EMS empfangen“. Die detaillierte Meldung enthält das Punktnotationsformat des tatsächlichen EMS-Ereignisses
Empfangene Nachrichten	Sobald der Cluster entdeckt wurde	Nach dem Hinzufügen jedes erforderlichen EMS-Ereignisses zu Unified Manager und nach dem nächsten 15-minütigen Abfragezyklus
Ereignislebenszyklus	Wie bei anderen Unified Manager-Ereignissen: Status „Neu“, „Bestätigt“, „Gelöst“ und „Veraltet“	Das EMS-Ereignis wird nach der Aktualisierung des Clusters, 15 Minuten nach der Erstellung des Ereignisses, obsolet.
Erfasst Ereignisse während der Ausfallzeit von Unified Manager	Ja, wenn das System startet, kommuniziert es mit jedem Cluster, um fehlende Ereignisse abzurufen	Nein
Veranstaltungsdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um konsistente Lösungen zu gewährleisten	Korrekturmaßnahmen sind auf der Seite „Ereignisdetails“ nicht verfügbar

Einige der neuen automatischen EMS-Ereignisse sind Informationsereignisse, die darauf hinweisen, dass ein vorheriges Ereignis behoben wurde. Beispielsweise zeigt das Informationsereignis „FlexGroup -Bestandteile – Speicherplatzstatus alles in Ordnung“ an, dass das Fehlerereignis „FlexGroup -Bestandteile haben Speicherplatzprobleme“ behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus wie andere Ereignisschweretypen verwaltet werden. Das Ereignis wird jedoch automatisch verworfen, wenn auf demselben Datenträger ein weiteres Fehlerereignis vom Typ „Speicherplatzprobleme“ auftritt.

EMS-Ereignisse, die automatisch zu Unified Manager hinzugefügt werden

Die folgenden ONTAP EMS-Ereignisse werden automatisch zu Unified Manager hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf einem Cluster ausgelöst werden, den Unified Manager überwacht.

Die folgenden EMS-Ereignisse sind bei der Überwachung von Clustern mit ONTAP 9.5 oder höher verfügbar:

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
Zugriff auf Cloud-Ebene für Aggregatverlagerung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung während Speicher-Failover verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
Neusynchronisierung der FabricPool -Spiegelreplikation abgeschlossen	wafl.ca.resync.complete	Cluster	Fehler
FabricPool -Speicherplatz fast voll	fabricpool.nearly.full	Cluster	Fehler
NVMe-oF-Karenzzeitraum gestartet	nvmf.graceperiod.start	Cluster	Warnung
NVMe-oF-Gnadenfrist aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-oF-Karenzzeit abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN zerstört	lun.destroy	LUN	Information
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Node	Fehler
Cloud AWS IAMCredsAbgelaufen	cloud.aws.iamCredsExpired	Node	Fehler
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Node	Fehler
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Node	Fehler
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Node	Information
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Node	Fehler

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Node	Fehler
Cloud Tier Host nicht auflösbar	objstore.host.unresolvable	Node	Fehler
Cloud Tier Intercluster-Netzwerkschnittstelle ausgefallen	objstore.interclusterlifDown	Node	Fehler
Anforderung stimmt nicht mit Cloud-Tier-Signatur überein	osc.signatureMismatch	Node	Fehler
Einer der NFSv4-Pools ist erschöpft	Nblade.nfsV4PoolExhaust	Node	Kritisch
QoS-Monitor-Speicher maximal	qos.monitor.memory.maxed	Node	Fehler
QoS-Monitor-Speicher verringert	qos.monitor.memory.abated	Node	Information
NVMeNS zerstören	NVMeNS.destroy	Namensraum	Information
NVMeNS Online	NVMeNS.offline	Namensraum	Information
NVMeNS Offline	NVMeNS.online	Namensraum	Information
NVMeNS hat keinen Platz mehr	Kein Speicherplatz mehr für NVMeNS	Namensraum	Warnung
Synchrone Replikation nicht synchron	SMS-Status nicht synchron	SnapMirror -Beziehung	Warnung
Synchrone Replikation wiederhergestellt	sms.status.in.sync	SnapMirror -Beziehung	Information
Automatische Neusynchronisierung der synchronen Replikation fehlgeschlagen	SMS-Neusynchronisierungsversuch fehlgeschlagen	SnapMirror -Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
Maximale CIFS-Verbindung überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler
Maximale Anzahl von CIFS-Verbindungen pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS-Namenskonflikt	Nblade.cifsNbNameConflict	SVM	Fehler
Versuche, eine nicht vorhandene CIFS-Freigabe zu verbinden	Nblade.cifsNoPrivShare	SVM	Kritisch
CIFS-Schattenkopie-Vorgang fehlgeschlagen	cifs.shadowcopy.failure	SVM	Fehler
Vom AV-Server gefundener Virus	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Serververbindung für Virenscan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV-Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine reagierende AV-Serververbindung	Nblade.vscanConnInactive	SVM	Information
AV-Server zu beschäftigt, um neue Scan-Anforderungen anzunehmen	Nblade.vscanConnBackPressure	SVM	Fehler
Versuch eines nicht autorisierten Benutzers, den AV-Server zu beschädigen	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup -Bestandteile haben Platzprobleme	Flexgroup-Bestandteile haben Platzprobleme	Volumen	Fehler
FlexGroup -Bestandteile Raumstatus Alles OK	flexgroup.constituents.space.status.all.ok	Volumen	Information

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
FlexGroup -Bestandteile haben Inodes-Probleme	Flexgroup.Bestandteile.haben.Inodes.Probleme	Volumen	Fehler
FlexGroup -Bestandteile Inodes Status Alle OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Information
Logischer Speicherplatz des Volumes fast voll	monitor.vol.nearFull.inc.sav	Volumen	Warnung
Logischer Speicherplatz des Volumes voll	monitor.vol.full.inc.sav	Volumen	Fehler
Volumen Logischer Speicherplatz Normal	monitor.vol.one.ok.inc.sav	Volumen	Information
WAFL -Volume-AutoSize -Fehler	wafl.vol.autoSize.fail	Volumen	Fehler
WAFL Volume AutoSize Fertig	wafl.vol.autoSize.done	Volumen	Information
WAFL READDIR-Dateivorgang-Timeout	wafl.readdir.expired	Volumen	Fehler

Abonnieren Sie ONTAP EMS-Events

Sie können den Empfang von Event Management System (EMS)-Ereignissen abonnieren, die von Systemen generiert werden, auf denen ONTAP -Software installiert ist. Eine Teilmenge der EMS-Ereignisse wird automatisch an Unified Manager gemeldet, zusätzliche EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie diese Ereignisse abonniert haben.

Bevor Sie beginnen

Abonnieren Sie keine EMS-Ereignisse, die bereits automatisch zu Unified Manager hinzugefügt wurden, da dies zu Verwirrung führen kann, wenn Sie zwei Ereignisse für dasselbe Problem erhalten.

Sie können beliebig viele EMS-Events abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert und nur die validierten Ereignisse werden auf die Cluster angewendet, die Sie in Unified Manager überwachen. Der *ONTAP 9 EMS-Ereigniskatalog* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite „ONTAP 9-Produktdokumentation“ nach der entsprechenden Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Ereignisse zu erhalten.

"ONTAP 9 Produktbibliothek"

Sie können Warnmeldungen für die ONTAP EMS-Ereignisse konfigurieren, die Sie abonnieren, und Sie können benutzerdefinierte Skripte erstellen, die für diese Ereignisse ausgeführt werden.

Wenn Sie die abonnierten ONTAP EMS-Ereignisse nicht erhalten, liegt möglicherweise ein Problem mit der DNS-Konfiguration des Clusters vor, das verhindert, dass der Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Clusteradministrator die DNS-Konfiguration des Clusters korrigieren und anschließend Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse auf den Unified Manager-Server übertragen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Klicken Sie auf der Seite „Ereigniseinrichtung“ auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld „EMS-Ereignisse abonnieren“ den Namen des ONTAP EMS-Ereignisses ein, das Sie abonnieren möchten.

   Um die Namen der EMS-Ereignisse anzuzeigen, die Sie abonnieren können, können Sie in der ONTAP Cluster-Shell die folgenden Befehle verwenden: `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher).

   "So konfigurieren und empfangen Sie Warnungen vom ONTAP EMS Event Subscription in Active IQ Unified Manager"

4. Klicken Sie auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste „Abonnierte EMS-Ereignisse“ hinzugefügt, aber in der Spalte „Gilt für Cluster“ wird für das von Ihnen hinzugefügte EMS-Ereignis der Status „Unbekannt“ angezeigt.

5. Klicken Sie auf **Speichern und schließen**, um das EMS-Ereignisabonnement beim Cluster zu registrieren.
6. Klicken Sie erneut auf **EMS-Events abonnieren**.

   Für das von Ihnen hinzugefügte EMS-Ereignis wird in der Spalte „Gilt für Cluster“ der Status „Ja“ angezeigt.

   Wenn der Status nicht „Ja“ lautet, überprüfen Sie die Schreibweise des ONTAP EMS-Ereignisnamens. Wenn der Name falsch eingegeben wurde, müssen Sie das falsche Ereignis entfernen und das Ereignis anschließend erneut hinzufügen.

Wenn das ONTAP EMS-Ereignis eintritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um Details zum EMS-Ereignis auf der Seite „Ereignisdetails“ anzuzeigen. Sie können auch die Disposition des Ereignisses verwalten oder Warnungen für das Ereignis erstellen.

Was passiert, wenn ein Ereignis empfangen wird?

Wenn Unified Manager ein Ereignis empfängt, wird es auf der Dashboard-Seite, auf der Inventarseite „Event Management“, auf den Registerkarten „Zusammenfassung“ und „Explorer“ der Seite „Cluster/Leistung“ und auf der objektspezifischen Inventarseite (z. B. der Inventarseite „Volumes/Health“) angezeigt.

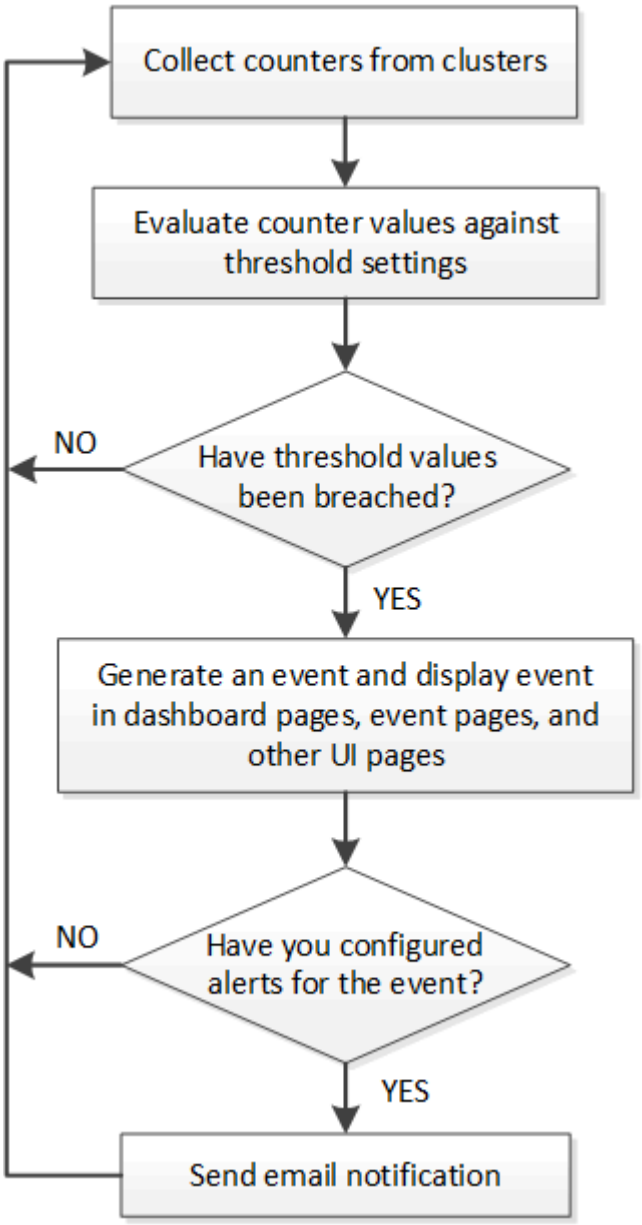
Wenn Unified Manager mehrere aufeinanderfolgende Vorkommen derselben Ereignisbedingung für dieselbe Clusterkomponente erkennt, behandelt es alle Vorkommen als ein einzelnes Ereignis und nicht als separate Ereignisse. Die Dauer des Ereignisses wird erhöht, um anzuzeigen, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie die Einstellungen auf der Seite „Alarm-Setup“ konfigurieren, können Sie andere Benutzer

über diese Ereignisse benachrichtigen. Der Alarm führt dazu, dass die folgenden Aktionen eingeleitet werden:

- Eine E-Mail über das Ereignis kann an alle Unified Manager Administrator-Benutzer gesendet werden.
- Das Ereignis kann an zusätzliche E-Mail-Empfänger gesendet werden.
- An den Trap-Empfänger kann ein SNMP-Trap gesendet werden.
- Zur Durchführung einer Aktion kann ein benutzerdefiniertes Skript ausgeführt werden.

Dieser Arbeitsablauf ist im folgenden Diagramm dargestellt.



Anzeigen von Ereignissen und Ereignisdetails

Sie können Details zu einem Ereignis anzeigen, das von Unified Manager ausgelöst wird, um Korrekturmaßnahmen zu ergreifen. Wenn beispielsweise ein Integritätsereignis „Volume offline“ vorliegt, können Sie auf dieses Ereignis klicken, um die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Ereignisdetails umfassen Informationen wie die Quelle des Ereignisses, die Ursache des Ereignisses und alle Hinweise zum Ereignis.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden in der Ansicht „Alle aktiven Ereignisse“ die neuen und bestätigten (aktiven) Ereignisse angezeigt, die in den letzten 7 Tagen generiert wurden und die Auswirkungsstufe „Vorfall“ oder „Risiko“ aufweisen.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen anzeigen möchten, beispielsweise Kapazitätsereignisse oder Leistungsereignisse, klicken Sie auf **Anzeigen** und wählen Sie aus dem Menü der Ereignistypen aus.
3. Klicken Sie auf den Namen des Ereignisses, dessen Details Sie anzeigen möchten.

   Die Ereignisdetails werden auf der Seite „Ereignisdetails“ angezeigt.

Nicht zugewiesene Ereignisse anzeigen

Sie können nicht zugewiesene Ereignisse anzeigen und dann jedes davon einem Benutzer zuweisen, der sie lösen kann.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Bereich **Filter** im Bereich **Zugewiesen an** die Filteroption **Nicht zugewiesen** aus.

Ereignisse bestätigen und beheben

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Arbeit an dem Problem beginnen, das das Ereignis verursacht hat, damit Sie nicht weiterhin wiederholt Warnmeldungen erhalten. Nachdem Sie Korrekturmaßnahmen für ein bestimmtes Ereignis ergriffen haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können Informationsereignisse nicht bestätigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Führen Sie in der Ereignisliste die folgenden Aktionen aus, um die Ereignisse zu bestätigen:

Wenn Sie wollen…	Machen Sie Folgendes…
Bestätigen und markieren Sie ein einzelnes Ereignis als gelöst	a. Klicken Sie auf den Ereignisnamen. b. Ermitteln Sie auf der Seite „Ereignisdetails“ die Ursache des Ereignisses. c. Klicken Sie auf **Bestätigen**. d. Ergreifen Sie entsprechende Korrekturmaßnahmen. e. Klicken Sie auf **Als gelöst markieren**.
Mehrere Ereignisse bestätigen und als gelöst markieren	a. Ermitteln Sie die Ursache der Ereignisse auf der jeweiligen Seite mit den Ereignisdetails. b. Wählen Sie die Ereignisse aus. c. Klicken Sie auf **Bestätigen**. d. Ergreifen Sie entsprechende Korrekturmaßnahmen. e. Klicken Sie auf **Als gelöst markieren**.

   Nachdem das Ereignis als gelöst markiert wurde, wird es in die Liste der gelösten Ereignisse verschoben.

3. **Optional**: Fügen Sie im Bereich **Notizen und Aktualisierungen** eine Notiz darüber hinzu, wie Sie auf das Ereignis reagiert haben, und klicken Sie dann auf **Posten**.

Zuweisen von Ereignissen zu bestimmten Benutzern

Sie können nicht zugewiesene Ereignisse sich selbst oder anderen Benutzern, einschließlich Remotebenutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer neu zuweisen. Wenn beispielsweise bei einem Speicherobjekt häufig Probleme auftreten, können Sie die Ereignisse für diese Probleme dem Benutzer zuweisen, der dieses Objekt verwaltet.

Bevor Sie beginnen

- Der Name und die E-Mail-ID des Benutzers müssen korrekt konfiguriert sein.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** ein oder mehrere Events aus, die Sie zuweisen möchten.
3. Weisen Sie das Ereignis zu, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie das Ereignis zuweisen möchten an…	Dann tun Sie Folgendes …
Selbst	Klicken Sie auf **Zuweisen an** > **Mir**.
Ein anderer Benutzer	a. Klicken Sie auf **Zuweisen an** > **Anderer Benutzer**. b. Geben Sie im Dialogfeld „Besitzer zuweisen“ den Benutzernamen ein oder wählen Sie einen Benutzer aus der Dropdownliste aus. c. Klicken Sie auf **Zuweisen**. Dem Benutzer wird eine E-Mail-Benachrichtigung gesendet. Wenn Sie keinen Benutzernamen eingeben oder keinen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt das Ereignis unzugeordnet.

Deaktivieren Sie unerwünschte Ereignisse

Alle Ereignisse sind standardmäßig aktiviert. Sie können Ereignisse global deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können deaktivierte Ereignisse aktivieren, wenn Sie den Empfang von Benachrichtigungen dafür wieder aufnehmen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie Ereignisse deaktivieren, werden die zuvor generierten Ereignisse im System als veraltet markiert und die für diese Ereignisse konfigurierten Warnungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

Wenn Sie ein Ereignis für ein Objekt deaktivieren (z. B. das `vol offline` Ereignis) und Sie das Ereignis später aktivieren, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline gingen, als das Ereignis deaktiviert war. Unified Manager generiert nur dann ein neues Ereignis, wenn sich der Objektstatus ändert, nachdem das Ereignis erneut aktiviert wurde.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Deaktivieren oder aktivieren Sie Ereignisse auf der Seite **Ereignis-Setup**, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Wählen Sie im Dialogfeld „Ereignisse deaktivieren“ den Schweregrad des Ereignisses aus. c. Wählen Sie in der Spalte „Übereinstimmende Ereignisse“ die Ereignisse aus, die Sie basierend auf dem Schweregrad des Ereignisses deaktivieren möchten, und klicken Sie dann auf den Rechtspfeil, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und schließen**. e. Überprüfen Sie, ob die von Ihnen deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Aktivieren Sie das Kontrollkästchen für das oder die Ereignisse, die Sie aktivieren möchten. b. Klicken Sie auf **Aktivieren**.

Beheben Sie Probleme mit der automatischen Korrektur durch Unified Manager

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und mithilfe der Schaltfläche **Fix It** eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen im Dashboard, auf der Seite mit den Ereignisdetails und in der Auswahl „Workload-Analyse“ im linken Navigationsmenü angezeigt.

Für die meisten Ereignisse gibt es eine Reihe möglicher Lösungen, die auf der Seite mit den Ereignisdetails angezeigt werden, sodass Sie mit dem ONTAP System Manager oder der ONTAP CLI die beste Lösung implementieren können. Eine **Fix It**-Aktion ist verfügbar, wenn Unified Manager festgestellt hat, dass es eine einzige Lösung zur Behebung des Problems gibt und dass es mit einem ONTAP CLI-Befehl behoben werden kann.

Schritte

1. Um Ereignisse anzuzeigen, die über das **Dashboard** behoben werden können, klicken Sie auf **Dashboard**.

2. Um alle Probleme zu beheben, die Unified Manager beheben kann, klicken Sie auf die Schaltfläche **Fix It**. Um ein Problem zu beheben, das bei mehreren Objekten auftritt, klicken Sie auf die Schaltfläche **Alle beheben**.

Informationen zu den Problemen, die durch automatische Korrektur behoben werden können, finden Sie unter"Welche Probleme kann Unified Manager beheben?" .

Aktivieren und Deaktivieren der Active IQ -Ereignisberichterstattung

Active IQ Plattformereignisse werden standardmäßig generiert und in der Benutzeroberfläche des Unified Managers angezeigt. Wenn Sie feststellen, dass diese Ereignisse zu „laut“ sind oder Sie diese Ereignisse nicht in Unified Manager anzeigen möchten, können Sie die Generierung dieser Ereignisse deaktivieren. Sie können sie zu einem späteren Zeitpunkt aktivieren, wenn Sie diese Benachrichtigungen weiterhin erhalten möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn Sie diese Funktion deaktivieren, empfängt Unified Manager sofort keine Active IQ Plattformereignisse mehr.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager, basierend auf der Zeitzone des Clusters, kurz nach Mitternacht mit dem Empfang von Active IQ -Plattformereignissen. Die Startzeit basiert darauf, wann Unified Manager AutoSupport Nachrichten von jedem Cluster empfängt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Funktionseinstellungen** Active IQ -Plattformereignisse, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Deaktivieren von Active IQ Plattformereignissen	Bewegen Sie im Bereich * Active IQ Portalereignisse* den Schieberegler nach links.
Aktivieren von Active IQ Plattformereignissen	Bewegen Sie im Bereich * Active IQ Portalereignisse* den Schieberegler nach rechts.

Laden Sie eine neue Active IQ Regeldatei hoch

Unified Manager sucht automatisch nach einer neuen Active IQ Ereignisdatei (Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln vorhanden sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeldatei jedoch manuell hochladen.

Active IQ Regeln werden auch als sichere Config Advisor (CA)-Regeln bezeichnet.

Wenn Sie Unified Manager an einem Standort ohne Netzwerkverbindung installieren oder auf eine bestimmte Version aktualisieren, stehen die gebündelten Active IQ Regeln automatisch zum Hochladen zur Verfügung. Es wird jedoch empfohlen, etwa einmal im Monat eine neue Regeldatei von der Support-Site von NetApp herunterzuladen, um sicherzustellen, dass aktualisierte Ereignisse generiert werden und Ihre Speichersysteme weiterhin optimal funktionieren.

Bevor Sie beginnen

- Die Ereignisberichterstattung des Active IQ Portals muss aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter"Aktivieren von Active IQ Portalereignissen" .
- Sie müssen die Regeldatei von der NetApp Support-Site herunterladen.

  Die Regeldatei befindet sich unter: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Schritte

1. Navigieren Sie auf einem Computer mit Netzwerkzugriff zur NetApp -Support-Site und laden Sie die aktuellen Regeln herunter `.zip` Datei.

   Das gebündelte Regelpaket umfasst das Regelrepository, Datenquellen und einen NetApp -KB-Artikel.

   > Auf Windows-Systemen ist der NetApp -KB-Artikel an einem Standort ohne Netzwerkkonnektivität nicht standardmäßig im Installationsprogramm enthalten. Sie können die Datei *secure_rules.zip* von der Support-Site herunterladen und hochladen, um den KB-Artikel mit allen Regeln anzuzeigen.

2. Übertragen Sie die Regeldatei auf ein Medium, das Sie in den sicheren Bereich bringen können, und kopieren Sie es dann auf ein System im sicheren Bereich.
3. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
4. Klicken Sie auf der Seite **Ereigniseinrichtung** auf die Schaltfläche **Regeln hochladen**.
5. Navigieren Sie im Dialogfeld **Upload-Regeln** zu den Regeln und wählen Sie sie aus `.zip` Datei, die Sie heruntergeladen haben, und klicken Sie auf **Hochladen**.

   Dieser Vorgang kann einige Minuten dauern.

Die Regeldatei wird auf dem Unified Manager-Server entpackt. Nachdem Ihre verwalteten Cluster nach Mitternacht eine AutoSupport Datei generiert haben, prüft Unified Manager die Cluster anhand der Regeldatei und generiert bei Bedarf neue Risiko- und Vorfallereignisse.

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel (KB): "So aktualisieren Sie AIQCASecure-Regeln manuell in Active IQ Unified Manager" .

So werden Active IQ Plattformereignisse generiert

Vorfälle und Risiken der Active IQ -Plattform werden in Unified Manager-Ereignisse umgewandelt, wie im folgenden Diagramm dargestellt.

Wie Sie sehen, wird die auf der Active IQ Plattform kompilierte Regeldatei auf dem neuesten Stand gehalten, Cluster- AutoSupport -Nachrichten werden täglich generiert und Unified Manager aktualisiert die Liste der Ereignisse täglich.

Beheben Sie Active IQ Plattformereignisse

Vorfälle und Risiken der Active IQ -Plattform ähneln anderen Unified Manager-Ereignissen, da sie zur Lösung anderen Benutzern zugewiesen werden können und über dieselben verfügbaren Status verfügen. Wenn Sie diese Art von Ereignissen jedoch mit

der Schaltfläche **Fix It** beheben, können Sie die Lösung innerhalb weniger Stunden überprüfen.

Das folgende Diagramm zeigt die Aktionen, die Sie ausführen müssen (in Grün) und die Aktion, die Unified Manager ausführt (in Schwarz), wenn Ereignisse aufgelöst werden, die von der Active IQ Plattform generiert wurden.

Wenn Sie eine manuelle Lösung durchführen, müssen Sie sich beim System Manager oder der ONTAP Befehlszeilenschnittstelle anmelden, um das Problem zu beheben. Sie können das Problem erst überprüfen, nachdem der Cluster um Mitternacht eine neue AutoSupport -Nachricht generiert hat.

Wenn Sie eine halbautomatische Lösung mit der Schaltfläche **Fix It** durchführen, können Sie innerhalb weniger Stunden überprüfen, ob die Lösung erfolgreich war.

Konfigurieren der Ereignisaufbewahrungseinstellungen

Sie können die Anzahl der Monate angeben, die ein Ereignis auf dem Unified Manager-Server aufbewahrt wird, bevor es automatisch gelöscht wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Das Aufbewahren von Ereignissen für mehr als 6 Monate kann die Serverleistung beeinträchtigen und wird nicht empfohlen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenaufbewahrung**.
2. Wählen Sie auf der Seite **Datenaufbewahrung** den Schieberegler im Bereich „Ereignisaufbewahrung“ aus, verschieben Sie ihn auf die Anzahl der Monate, die Ereignisse aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Was ein Unified Manager-Wartungsfenster ist

Sie definieren ein Unified Manager-Wartungsfenster, um Ereignisse und Warnungen für einen bestimmten Zeitraum zu unterdrücken, wenn Sie eine Clusterwartung geplant haben und keine Flut unerwünschter Benachrichtigungen erhalten möchten.

Wenn das Wartungsfenster beginnt, wird auf der Inventarseite der Ereignisverwaltung ein Ereignis „Wartungsfenster für Objekte gestartet“ veröffentlicht. Dieses Ereignis wird automatisch verworfen, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden die Ereignisse im Zusammenhang mit allen Objekten in diesem Cluster weiterhin generiert, sie werden jedoch auf keiner der UI-Seiten angezeigt und es werden keine Warnungen oder andere Arten von Benachrichtigungen für diese Ereignisse gesendet. Sie können jedoch die Ereignisse anzeigen, die während eines Wartungsfensters für alle Speicherobjekte generiert wurden, indem Sie auf der Inventarseite der Ereignisverwaltung eine der Anzeigeoptionen auswählen.

Sie können ein Wartungsfenster für die Zukunft planen, Sie können die Start- und Endzeiten für ein geplantes Wartungsfenster ändern und Sie können ein geplantes Wartungsfenster abbrechen.

Planen Sie ein Wartungsfenster, um Cluster-Ereignisbenachrichtigungen zu deaktivieren

Wenn Sie für einen Cluster eine Ausfallzeit planen, beispielsweise um den Cluster zu aktualisieren oder einen der Knoten zu verschieben, können Sie die Ereignisse und Warnungen unterdrücken, die normalerweise während dieses Zeitraums generiert würden, indem Sie ein Wartungsfenster für Unified Manager planen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Während eines Wartungsfensters werden die Ereignisse, die sich auf alle Objekte in diesem Cluster beziehen, weiterhin generiert, sie werden jedoch nicht auf der Ereignisseite angezeigt und es werden keine Warnungen oder andere Arten von Benachrichtigungen für diese Ereignisse gesendet.

Die von Ihnen für das Wartungsfenster eingegebene Zeit basiert auf der Zeit auf dem Unified Manager-Server.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Wählen Sie in der Spalte **Wartungsmodus** für den Cluster den Schieberegler aus und verschieben Sie ihn nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Wählen Sie Start- und Enddatum sowie -uhrzeit für das Wartungsfenster aus und klicken Sie auf **Übernehmen**.

   Neben dem Schieberegler erscheint die Meldung „Geplant“.

Wenn die Startzeit erreicht ist, wechselt der Cluster in den Wartungsmodus und ein Ereignis „Object Maintenance Window Started“ wird generiert.

Ändern oder Abbrechen eines geplanten Wartungsfensters

Wenn Sie ein zukünftiges Wartungsfenster für Unified Manager konfiguriert haben, können Sie die Start- und Endzeiten ändern oder das Wartungsfenster abbrechen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das Abbrechen eines aktuell laufenden Wartungsfensters ist nützlich, wenn Sie die Clusterwartung vor dem geplanten Ende des Wartungsfensters abgeschlossen haben und wieder Ereignisse und Warnungen vom Cluster empfangen möchten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Wenn Sie wollen…	Führen Sie diesen Schritt aus…
Ändern des Zeitrahmens für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „Geplant“. b. Ändern Sie das Start- und/oder Enddatum und die Uhrzeit und klicken Sie auf **Übernehmen**.
Verlängern Sie die Länge eines aktiven Wartungsfensters	a. Klicken Sie neben dem Schieberegler auf den Text „Aktiv“. b. Ändern Sie das Enddatum und die Endzeit und klicken Sie auf **Übernehmen**.
Abbrechen eines geplanten Wartungsfensters	Wählen Sie den Schieberegler aus und verschieben Sie ihn nach links.
Abbrechen eines aktiven Wartungsfensters	Wählen Sie den Schieberegler aus und verschieben Sie ihn nach links.

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Speicherobjekte generiert wurden. Die meisten Ereignisse werden im Status „Veraltet“ angezeigt, sobald das Wartungsfenster abgeschlossen ist und alle Systemressourcen wieder betriebsbereit sind.

Bevor Sie beginnen

Es muss mindestens ein Wartungsfenster abgeschlossen sein, bevor Ereignisse verfügbar sind.

Ereignisse, die während eines Wartungsfensters aufgetreten sind, werden standardmäßig nicht auf der Inventarseite der Ereignisverwaltung angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisse**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Ansichtsbereich die Option **Alle während der Wartung generierten Ereignisse**.

   Die Liste der Ereignisse, die in den letzten 7 Tagen von allen Wartungsfenstersitzungen und von allen Clustern ausgelöst wurden, wird angezeigt.

3. Wenn für einen einzelnen Cluster mehrere Wartungsfenster vorhanden waren, können Sie auf das Kalendersymbol **Ausgelöste Zeit** klicken und den Zeitraum für die Wartungsfenstereereignisse auswählen, die Sie anzeigen möchten.

Verwalten von Hostsystemressourcenereignissen

Unified Manager enthält einen Dienst, der Ressourcenprobleme auf dem Hostsystem überwacht, auf dem Unified Manager installiert ist. Probleme wie fehlender verfügbarer Speicherplatz oder Speichermangel auf dem Hostsystem können Verwaltungsstationsereignisse auslösen, die als Bannermeldungen oben auf der Benutzeroberfläche angezeigt werden.

Ereignisse der Verwaltungsstation weisen auf ein Problem mit dem Hostsystem hin, auf dem Unified Manager installiert ist. Zu den Problemen der Verwaltungsstation zählen beispielsweise zu wenig Speicherplatz auf dem Hostsystem, ein fehlender regelmäßiger Datenerfassungszyklus von Unified Manager und die Nichterfüllung oder verspätete Durchführung der Statistikanalyse, weil die nächste Datenerfassungsabfrage eingeleitet wurde.

Im Gegensatz zu allen anderen Ereignismeldungen des Unified Manager werden diese speziellen Warnungen und kritischen Ereignisse der Verwaltungsstation in Bannermeldungen angezeigt.

Schritt

1. Um Ereignisinformationen zur Verwaltungsstation anzuzeigen, führen Sie die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Details zur Veranstaltung anzeigen	Klicken Sie auf das Ereignisbanner, um die Seite mit den Ereignisdetails anzuzeigen, die Lösungsvorschläge für das Problem enthält.
Alle Ereignisse der Verwaltungsstation anzeigen	a. Klicken Sie im linken Navigationsbereich auf **Event Management**. b. Klicken Sie im Bereich „Filter“ auf der Inventarseite der Ereignisverwaltung in der Liste „Quelltyp“ auf das Kontrollkästchen für die Verwaltungsstation.

Erfahren Sie mehr über Ereignisse

Wenn Sie die Konzepte zu Ereignissen verstehen, können Sie Ihre Cluster und Clusterobjekte effizienter verwalten und Warnmeldungen entsprechend definieren.

Ereignisstatusdefinitionen

Anhand des Status eines Ereignisses können Sie feststellen, ob eine entsprechende Korrekturmaßnahme erforderlich ist. Ein Ereignis kann „Neu“, „Bestätigt“, „Gelöst“ oder „Veraltet“ sein. Beachten Sie, dass sowohl neue als auch bestätigte Ereignisse als aktive Ereignisse betrachtet werden.

Die Ereigniszustände sind wie folgt:

- **Neu**

Der Status eines neuen Ereignisses.

- **Anerkannt**

  Der Status eines Ereignisses, wenn Sie es bestätigt haben.

- **Gelöst**

  Der Status eines Ereignisses, wenn es als gelöst markiert ist.

- **Veraltet**

  Der Status eines Ereignisses, wenn es automatisch korrigiert wird oder wenn die Ursache des Ereignisses nicht mehr gültig ist.

  Sie können ein veraltetes Ereignis weder bestätigen noch beheben.

Beispiel für verschiedene Zustände eines Ereignisses

Die folgenden Beispiele veranschaulichen die manuellen und automatischen Ereignisstatusänderungen.

Wenn das Ereignis „Cluster nicht erreichbar“ ausgelöst wird, ist der Ereignisstatus „Neu“. Wenn Sie das Ereignis bestätigen, ändert sich der Ereignisstatus in „Bestätigt“. Wenn Sie eine entsprechende Korrekturmaßnahme ergriffen haben, müssen Sie das Ereignis als gelöst markieren. Der Ereignisstatus ändert sich dann in „Gelöst“.

Wenn das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls generiert wird, nimmt der Cluster nach Wiederherstellung der Stromversorgung seinen Betrieb ohne Eingriff des Administrators wieder auf. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig und der Ereignisstatus ändert sich im nächsten Überwachungszyklus in „Veraltet“.

Unified Manager sendet eine Warnung, wenn ein Ereignis den Status „Veraltet“ oder „Gelöst“ hat. Die Betreffzeile und der Inhalt einer E-Mail-Benachrichtigung geben Auskunft über den Ereignisstatus. Ein SNMP-Trap enthält auch Informationen zum Ereignisstatus.

Beschreibung der Ereignisschweregrade

Jedem Ereignis ist ein Schweregrad zugeordnet, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die sofortige Korrekturmaßnahmen erfordern.

- **Kritisch**

  Es ist ein Problem aufgetreten, das zu einer Dienstunterbrechung führen kann, wenn nicht sofort Abhilfemaßnahmen ergriffen werden.

  Leistungskritische Ereignisse werden nur ab benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

  Die Ereignisquelle funktioniert noch, es sind jedoch Korrekturmaßnahmen erforderlich, um eine Dienstunterbrechung zu vermeiden.

- **Warnung**

Bei der Ereignisquelle ist ein Vorfall aufgetreten, den Sie kennen sollten, oder ein Leistungsindikator für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads verursachen keine Dienstunterbrechung und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.

Leistungswarnungsereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

  Das Ereignis tritt ein, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein Speicherobjekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

  Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Beschreibung der Ereignisauswirkungsstufen

Jedem Ereignis ist eine Auswirkungsstufe (Vorfall, Risiko, Ereignis oder Upgrade) zugeordnet, damit Sie die Ereignisse priorisieren können, die sofortige Korrekturmaßnahmen erfordern.

- **Vorfall**

  Ein Vorfall ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster dem Client keine Daten mehr bereitstellt und nicht mehr genügend Speicherplatz für die Daten zur Verfügung steht. Ereignisse mit der Auswirkungsstufe „Vorfall“ sind die schwerwiegendsten. Um eine Unterbrechung des Dienstes zu vermeiden, sollten umgehend Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die möglicherweise dazu führen können, dass ein Cluster keine Daten mehr an den Client liefert und nicht mehr genügend Speicherplatz für die Daten zur Verfügung steht. Ereignisse mit der Auswirkungsstufe „Risiko“ können zu Dienstunterbrechungen führen. Möglicherweise sind Korrekturmaßnahmen erforderlich.

- **Ereignis**

  Ein Ereignis ist eine Zustands- oder Statusänderung von Speicherobjekten und ihren Attributen. Ereignisse mit der Auswirkungsstufe „Ereignis“ haben informativen Charakter und erfordern keine Korrekturmaßnahmen.

- **Upgrade**

  Upgrade-Ereignisse sind ein bestimmter Ereignistyp, der von der Active IQ Plattform gemeldet wird. Diese Ereignisse identifizieren Probleme, für deren Lösung Sie ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) benötigen. Bei einigen dieser Probleme möchten Sie möglicherweise sofort Abhilfemaßnahmen ergreifen, während andere Probleme möglicherweise bis zu Ihrer nächsten planmäßigen Wartung warten können.

Beschreibung der Ereignisauswirkungsbereiche

Ereignisse werden in sechs Auswirkungsbereiche (Verfügbarkeit, Kapazität, Konfiguration, Leistung, Schutz und Sicherheit) kategorisiert, damit Sie sich auf die Ereignistypen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse benachrichtigen Sie, wenn ein Speicherobjekt offline geht, ein Protokolldienst ausfällt, ein Problem mit dem Speicherfailover auftritt oder ein Problem mit der Hardware auftritt.

- **Kapazität**

  Kapazitätsereignisse benachrichtigen Sie, wenn Ihre Aggregate, Volumes, LUNs oder Namespaces sich einem Größenschwellenwert nähern oder diesen bereits erreicht haben oder wenn die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, Löschung, Hinzufügung, Entfernung oder Umbenennung Ihrer Speicherobjekte. Konfigurationsereignisse haben die Auswirkungsstufe „Ereignis“ und den Schweregrad „Information“.

- **Leistung**

  Leistungsereignisse benachrichtigen Sie über Ressourcen-, Konfigurations- oder Aktivitätsbedingungen in Ihrem Cluster, die sich negativ auf die Geschwindigkeit der Datenspeichereingabe oder des Datenabrufs Ihrer überwachten Speicherobjekte auswirken können.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Vorfälle oder Risiken im Zusammenhang mit SnapMirror -Beziehungen, Problemen mit der Zielkapazität, Problemen mit SnapVault -Beziehungen oder Problemen mit Schutzaufträgen. Alle ONTAP Objekte (insbesondere Aggregate, Volumes und SVMs), die sekundäre Volumes und Schutzbeziehungen hosten, werden im Bereich „Schutzauswirkungen“ kategorisiert.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes sind, basierend auf den im "NetApp Security Hardening Guide für ONTAP 9" .

  Darüber hinaus enthält dieser Bereich Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden.

So wird der Objektstatus berechnet

Der Objektstatus wird durch das schwerwiegendste Ereignis bestimmt, das derzeit den Status „Neu“ oder „Bestätigt“ aufweist. Wenn beispielsweise der Status eines Objekts „Fehler“ lautet, weist eines der Ereignisse des Objekts den Schweregrad „Fehler“ auf. Wenn Korrekturmaßnahmen ergriffen wurden, wechselt der Ereignisstatus zu „Gelöst“.

Details zum dynamischen Leistungsereignisdiagramm

Bei dynamischen Leistungsereignissen werden im Abschnitt „Systemdiagnose“ der Seite „Ereignisdetails“ die wichtigsten Workloads mit der höchsten Latenz oder Nutzung der umkämpften Clusterkomponente aufgelistet.

Die Leistungsstatistiken basieren auf dem Zeitpunkt, zu dem das Leistungsereignis erkannt wurde, bis zum Zeitpunkt der letzten Ereignisanalyse. Die Diagramme zeigen auch historische Leistungsstatistiken für die umstrittene Clusterkomponente an.

Sie können beispielsweise Workloads mit hoher Auslastung einer Komponente identifizieren, um zu bestimmen, welche Workload auf eine weniger ausgelastete Komponente verschoben werden soll. Durch die Verschiebung der Arbeitslast würde der Arbeitsaufwand für die aktuelle Komponente verringert und die Komponente möglicherweise aus dem Wettbewerb genommen. Oben in diesem Abschnitt stehen der Zeit- und Datumsbereich, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird die letzte analysierte Zeit aktualisiert.

Die Latenz- und Aktivitätsdiagramme zeigen die Namen der wichtigsten Workloads an, wenn Sie mit dem Cursor über das Diagramm fahren. Wenn Sie auf das Menü „Workload-Typ“ rechts neben dem Diagramm klicken, können Sie die Workloads nach ihrer Rolle im Ereignis sortieren, einschließlich *Haie*, *Mobber* oder *Opfer*. Außerdem werden Details zu ihrer Latenz und ihrer Nutzung der umstrittenen Clusterkomponente angezeigt. Sie können den tatsächlichen Wert mit dem erwarteten Wert vergleichen, um zu sehen, wann die Arbeitslast außerhalb des erwarteten Latenz- oder Nutzungsbereichs lag. Weitere Informationen finden Sie unter"Von Unified Manager überwachte Workloadtypen" .

> Wenn Sie nach der Spitzenabweichung der Latenz sortieren, werden systemdefinierte Workloads nicht in der Tabelle angezeigt, da die Latenz nur für benutzerdefinierte Workloads gilt. Workloads mit sehr niedrigen Latenzwerten werden in der Tabelle nicht angezeigt.

Weitere Informationen zu den dynamischen Leistungsschwellenwerten finden Sie unter"Analysieren von Ereignissen anhand dynamischer Leistungsschwellenwerte" .

Informationen dazu, wie Unified Manager die Arbeitslasten bewertet und die Sortierreihenfolge bestimmt, finden Sie unter"So ermittelt Unified Manager die Leistungsauswirkungen eines Ereignisses" .

Die Daten in den Diagrammen zeigen Leistungsstatistiken der letzten 24 Stunden vor der letzten Ereignisanalyse. Die tatsächlichen und erwarteten Werte für jede Arbeitslast basieren auf der Zeit, in der die Arbeitslast am Ereignis beteiligt war. Beispielsweise kann eine Arbeitslast in ein Ereignis verwickelt werden, nachdem das Ereignis erkannt wurde, sodass ihre Leistungsstatistiken möglicherweise nicht mit den Werten zum Zeitpunkt der Ereigniserkennung übereinstimmen. Standardmäßig werden die Workloads nach der Spitzenabweichung (höchsten Abweichung) bei der Latenz sortiert.

> Da Unified Manager maximal 30 Tage lang 5-minütige historische Leistungs- und Ereignisdaten speichert, werden keine Leistungsdaten angezeigt, wenn das Ereignis älter als 30 Tage ist.

- **Spalte „Workload sortieren“**
  - **Latenzdiagramm**

    Zeigt die Auswirkungen des Ereignisses auf die Latenz der Arbeitslast während der letzten Analyse an.
  - **Spalte „Komponentennutzung“**

Zeigt Details zur Arbeitslastnutzung der konkurrierenden Clusterkomponente an. In den Diagrammen ist die tatsächliche Nutzung als blaue Linie dargestellt. Ein roter Balken hebt die Ereignisdauer vom Erkennungszeitpunkt bis zum letzten analysierten Zeitpunkt hervor. Weitere Informationen finden Sie unter "Messwerte für die Workload-Leistung".

Für die Netzwerkkomponente wird diese Spalte nicht angezeigt, da die Netzwerkleistungsstatistiken aus Aktivitäten außerhalb des Clusters stammen.

- **Komponentenverwendung**

  Zeigt den Nutzungsverlauf in Prozent für die Netzwerkverarbeitung, Datenverarbeitung und Aggregatkomponenten oder den Aktivitätsverlauf in Prozent für die QoS-Richtliniengruppenkomponente an. Für die Netzwerk- oder Verbindungskomponenten wird das Diagramm nicht angezeigt. Sie können auf die Statistiken zeigen, um die Nutzungsstatistiken zu einem bestimmten Zeitpunkt anzuzeigen.

- **Gesamtverlauf der Schreibvorgänge in MB/s**

  Zeigt nur für die MetroCluster -Ressourcenkomponente den gesamten Schreibdurchsatz in Megabyte pro Sekunde (MBps) für alle Volume-Workloads an, die in einer MetroCluster -Konfiguration auf den Partnercluster gespiegelt werden.

- **Ereignisverlauf**

  Zeigt rot schattierte Linien an, um die historischen Ereignisse für die umstrittene Komponente anzuzeigen. Bei veralteten Ereignissen zeigt das Diagramm Ereignisse an, die vor der Erkennung des ausgewählten Ereignisses und nach seiner Lösung aufgetreten sind.

Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, damit Sie feststellen können, ob eine Änderung ein Leistungsereignis verursacht oder dazu beigetragen hat. Auf den Seiten des Performance Explorers wird ein Symbol für Änderungsereignisse angezeigt ( ), um das Datum und die Uhrzeit anzugeben, wann die Änderung erkannt wurde.

Sie können die Leistungsdiagramme auf den Seiten des Leistungs-Explorers und auf der Seite „Arbeitslastanalyse“ überprüfen, um zu sehen, ob sich das Änderungsereignis auf die Leistung des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung ungefähr zur gleichen Zeit wie ein Leistungsereignis erkannt wurde, hat die Änderung möglicherweise zu dem Problem beigetragen, das zur Auslösung der Ereigniswarnung geführt hat.

Unified Manager kann die folgenden Änderungsereignisse erkennen, die als Informationsereignisse kategorisiert werden:

- Ein Volumen wird zwischen Aggregaten verschoben.

  Unified Manager kann erkennen, wann die Verschiebung läuft, abgeschlossen ist oder fehlgeschlagen ist. Wenn Unified Manager während einer Volumeverschiebung ausfällt, erkennt es die Volumeverschiebung, wenn es wieder verfügbar ist, und zeigt ein Änderungsereignis dafür an.

- Die Durchsatzgrenze (MB/s oder IOPS) einer QoS-Richtliniengruppe, die eine oder mehrere überwachte Workloads enthält, ändert sich.

Das Ändern eines Richtliniengruppenlimits kann zu zeitweiligen Spitzen in der Latenz (Reaktionszeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich und alle durch die Spitzen verursachten Ereignisse werden obsolet.

- Ein Knoten in einem HA-Paar übernimmt den Speicher seines Partnerknotens oder gibt ihn zurück.

  Unified Manager kann erkennen, wann die Übernahme-, Teilübernahme- oder Rückgabeoperation abgeschlossen ist. Wenn die Übernahme durch einen in Panik geratenen Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein ONTAP -Upgrade- oder Wiederherstellungsvorgang wurde erfolgreich abgeschlossen.

  Es werden die vorherige und die neue Version angezeigt.

Liste der Ereignisse und Schweregrade

Sie können die Ereignisliste verwenden, um sich mit den Ereigniskategorien, Ereignisnamen und dem Schweregrad jedes Ereignisses vertraut zu machen, die Sie möglicherweise in Unified Manager sehen. Ereignisse werden in alphabetischer Reihenfolge nach Objektkategorie aufgelistet.

Aggregierte Ereignisse

Aggregatereignisse liefern Ihnen Informationen zum Status von Aggregaten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregat offline (ocumEvtAggregateStateOffline)	Vorfall	Aggregat	Kritisch
Aggregat fehlgeschlagen (ocumEvtAggregateStateFailed)	Vorfall	Aggregat	Kritisch
Aggregat eingeschränkt (ocumEvtAggregateStateRestricted)	Risiko	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregatrekonstruktion (ocumEvtAggregateRaidStateReconstructing)	Risiko	Aggregat	Warnung
Aggregat herabgestuft (ocumEvtAggregateRaidStateDegraded)	Risiko	Aggregat	Warnung
Cloud-Ebene teilweise erreichbar (ocumEventCloudTierPartiallyReachable)	Risiko	Aggregat	Warnung
Cloud-Ebene nicht erreichbar (ocumEventCloudTierUnreachable)	Risiko	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung verweigert *(arlNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung während Speicher-Failover verweigert *(gbNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Zurückgelassenes MetroCluster -Aggregat (ocumEvtMetroClusterAggregateLeftBehind)	Risiko	Aggregat	Fehler
MetroCluster -Aggregatspiegelung beeinträchtigt (ocumEvtMetroClusterAggregateMirrorDegraded)	Risiko	Aggregat	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregatspeicherplatz fast voll (ocumEvtAggregateNearlyFull)	Risiko	Aggregat	Warnung
Aggregatspeicher voll (ocumEvtAggregateFull)	Risiko	Aggregat	Fehler
Aggregierte Tage bis zur Vollendung (ocumEvtAggregateDaysUntilFullSoon)	Risiko	Aggregat	Fehler
Aggregat überbelegt (ocumEvtAggregateOvercommitted)	Risiko	Aggregat	Fehler
Aggregat fast überlastet (ocumEvtAggregateAlmostOvercommitted)	Risiko	Aggregat	Warnung
Aggregierte Snapshot-Reserve voll (ocumEvtAggregateSnapReserveFull)	Risiko	Aggregat	Warnung
Anormale Gesamtwachstumsrate (ocumEvtAggregateGrowthRateAbnormal)	Risiko	Aggregat	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregat entdeckt (Nicht zutreffend)	Ereignis	Aggregat	Information
Aggregat umbenannt (Nicht zutreffend)	Ereignis	Aggregat	Information
Aggregat gelöscht (Nicht zutreffend)	Ereignis	Node	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für aggregierte IOPS überschritten (ocumAggregateIopsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für aggregierte IOPS überschritten (ocumAggregateIopsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für aggregierte MB/s überschritten (ocumAggregateMbpsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für aggregierte MB/s überschritten (ocumAggregateMbpsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für aggregierte Latenz überschritten (ocumAggregateLatencyIncident)	Vorfall	Aggregat	Kritisch
Schwellenwert für Warnung vor aggregierter Latenz überschritten (ocumAggregateLatencyWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für genutzte Gesamtleistungskapazität überschritten (ocumAggregatePerfCapacityUsedIncident)	Vorfall	Aggregat	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für genutzte Gesamtleistungskapazität überschritten (ocumAggregatePerfCapacityUsedWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für Gesamtauslastung überschritten (ocumAggregateUtilizationIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für aggregierte Auslastung überschritten (ocumAggregateUtilizationWarning)	Risiko	Aggregat	Warnung
Schwellenwert für Überauslastung aggregierter Datenträger überschritten (ocumAggregateDisksOverUtilizedWarning)	Risiko	Aggregat	Warnung
Aggregierter dynamischer Schwellenwert überschritten (ocumAggregateDynamicEventWarning)	Risiko	Aggregat	Warnung

Cluster-Ereignisse

Clusterereignisse liefern Informationen zum Status von Clustern, sodass Sie die Cluster auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Im Cluster fehlen Ersatzfestplatten (ocumEvtDisksNoSpares)	Risiko	Cluster	Warnung
Cluster nicht erreichbar (ocumEvtClusterUnreachable)	Risiko	Cluster	Fehler
Clusterüberwachung fehlgeschlagen (ocumEvtClusterMonitoringFailed)	Risiko	Cluster	Warnung
Lizenzkapazitätsgrenzen des Cluster FabricPool überschritten (ocumEvtExternalCapacityTierSpaceFull)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeitraum gestartet *(nvmfGracePeriodStart)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeitraum aktiv *(nvmfGracePeriodActive)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeit abgelaufen *(nvmfGracePeriodExpired)	Risiko	Cluster	Warnung
Objektwartungsfenster gestartet (objectMaintenanceWindowStarted)	Ereignis	Cluster	Kritisch
Objektwartungsfenster beendet (objectMaintenanceWindowEnded)	Ereignis	Cluster	Information
Zurückgelassene MetroCluster -Ersatzfestplatten (ocumEvtSpareDiskLeftBehind)	Risiko	Cluster	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Automatische ungeplante Umschaltung von MetroCluster deaktiviert (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risiko	Cluster	Warnung
Cluster-Benutzerkennwort geändert *(cluster.passwd.changed)	Ereignis	Cluster	Information

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schwellenwert für Cluster-Kapazitätsungleichgewicht überschritten (ocumConformanceNodeImbalanceWarning)	Risiko	Cluster	Warnung
Cluster-Cloud-Tier-Planung (clusterCloudTierPlanningWarning)	Risiko	Cluster	Warnung
Neusynchronisierung der FabricPool -Spiegelreplikation abgeschlossen *(waflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool -Speicherplatz fast voll *(fabricpoolNearlyFull)	Risiko	Cluster	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten hinzugefügt (nicht zutreffend)	Ereignis	Cluster	Information

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten entfernt (Nicht zutreffend)	Ereignis	Cluster	Information
Cluster entfernt (Nicht zutreffend)	Ereignis	Cluster	Information
Cluster hinzufügen fehlgeschlagen (Nicht zutreffend)	Ereignis	Cluster	Fehler
Clustername geändert (Nicht zutreffend)	Ereignis	Cluster	Information
Notfall-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Kritischer EMS-Einsatz empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
EMS-Alarm erhalten (Nicht zutreffend)	Ereignis	Cluster	Fehler
Fehler EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
Warnung EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Debug-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
EMS-Benachrichtigung erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Informatives EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS-Ereignisse werden in drei Unified Manager-Ereignisschweregrade eingeteilt.

Unified Manager-Ereignisschweregrad	ONTAP EMS-Ereignisschweregrad
Kritisch	Notfall Kritisch

Fehler	Alarm
Warnung	Fehler Warnung Debuggen Beachten Informativ

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schwellenwert für Cluster-Lastungleichgewicht überschritten()	Risiko	Cluster	Warnung
Kritischer Cluster-IOPS-Schwellenwert überschritten (ocumClusterIopsIncident)	Vorfall	Cluster	Kritisch
Cluster-IOPS-Warnschwelle überschritten (ocumClusterIopsWarning)	Risiko	Cluster	Warnung
Kritischer Schwellenwert für Cluster-MB/s überschritten (ocumClusterMbpsIncident)	Vorfall	Cluster	Kritisch
Cluster-MB/s-Warnschwelle überschritten (ocumClusterMbpsWarning)	Risiko	Cluster	Warnung
Dynamischer Cluster-Schwellenwert überschritten (ocumClusterDynamicEventWarning)	Risiko	Cluster	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfiguredDisabled)	Risiko	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt (ocumClusterAuditLogUnencrypted)	Risiko	Cluster	Warnung
Standardmäßiger lokaler Administratorbenutzer aktiviert (ocumClusterDefaultAdminEnabled)	Risiko	Cluster	Warnung
FIPS-Modus deaktiviert (ocumClusterFipsDisabled)	Risiko	Cluster	Warnung
Anmeldebanner deaktiviert (ocumClusterLoginBannerDisabled)	Risiko	Cluster	Warnung
Anmeldebanner geändert (ocumClusterLoginBannerChanged)	Risiko	Cluster	Warnung
Ziele für die Protokollweiterleitung geändert (ocumLogForwardDestinationsChanged)	Risiko	Cluster	Warnung
NTP-Servernamen geändert (ocumNtpServerNamesChanged)	Risiko	Cluster	Warnung
Die Anzahl der NTP-Server ist niedrig (securityConfigNTPServerCountLowRisk)	Risiko	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cluster-Peer-Kommunikation nicht verschlüsselt (ocumClusterPeerEncryptionDisabled)	Risiko	Cluster	Warnung
SSH verwendet unsichere Chiffren (ocumClusterSSHInsecure)	Risiko	Cluster	Warnung
Telnet-Protokoll aktiviert (ocumClusterTelnetEnabled)	Risiko	Cluster	Warnung
Passwörter einiger ONTAP Benutzerkonten verwenden die weniger sichere MD5-Hash-Funktion (ocumClusterMD5PasswordHashUsed).	Risiko	Cluster	Warnung
Cluster verwendet selbstsigniertes Zertifikat (ocumClusterSelfSignedCertificate)	Risiko	Cluster	Warnung
Cluster-Remote-Shell ist aktiviert (ocumClusterRshDisabled)	Risiko	Cluster	Warnung
Cluster-Zertifikat läuft bald ab (ocumEvtClusterCertificateAboutToExpire)	Risiko	Cluster	Warnung
Cluster-Zertifikat abgelaufen (ocumEvtClusterCertificateExpired)	Risiko	Cluster	Fehler

Datenträgerereignisse

Datenträgerereignisse liefern Ihnen Informationen zum Status von Datenträgern, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach

Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Flash-Festplatten – Ersatzblöcke fast aufgebraucht (ocumEvtClusterFlashDiskFewerSpareBlockError)	Risiko	Cluster	Fehler
Flash-Disks – Keine Ersatzblöcke (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Datenträger (ocumEvtClusterUnassignedDisksSome)	Risiko	Cluster	Warnung
Einige ausgefallene Datenträger (ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Anlagen Veranstaltungen

Gehäuseereignisse liefern Ihnen Informationen zum Status der Festplattengehäuse in Ihrem Rechenzentrum, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Festplatten-Shelf-Lüfter ausgefallen (ocumEvtShelfFanFailed)	Vorfall	Ablageboden	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ausfall der Stromversorgung des Festplattenregals (ocumEvtShelfPowerSupplyFailed)	Vorfall	Ablageboden	Kritisch
Disk Shelf Multipath nicht konfiguriert (ocumDiskShelfConnectivityNotInMultiPath) Dieses Ereignis gilt nicht für: • Cluster, die sich in einer MetroCluster -Konfiguration befinden • Die folgenden Plattformen: FAS2554, FAS2552, FAS2520 und FAS2240	Risiko	Node	Warnung
Disk Shelf-Pfadfehler (ocumDiskShelfConnectivityPathFailure)	Risiko	Lagerregal	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Disk Shelf erkannt (Nicht zutreffend)	Ereignis	Node	Information
Festplattenregale entfernt (nicht zutreffend)	Ereignis	Node	Information

Fan-Events

Lüfterereignisse liefern Ihnen Informationen zum Status der Lüfter auf Knoten in Ihrem Rechenzentrum, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ein oder mehrere ausgefallene Lüfter (ocumEvtFansOneOrMoreFailed)	Vorfall	Node	Kritisch

Flashkartenereignisse

Flashkartenereignisse liefern Ihnen Informationen zum Status der auf den Knoten in Ihrem Rechenzentrum installierten Flashkarten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Karteikarten offline (ocumEvtFlashCardOffline)	Vorfall	Node	Kritisch

Inodes-Ereignisse

Inode-Ereignisse liefern Informationen, wenn der Inode voll oder fast voll ist, sodass Sie ihn auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Inodes fast voll (ocumEvtInodesAlmostFull)	Risiko	Volumen	Warnung
Inodes voll (ocumEvtInodesFull)	Risiko	Volumen	Fehler

Netzwerkschnittstellenereignisse (LIF)

Netzwerkschnittstellenereignisse liefern Informationen zum Status Ihrer Netzwerkschnittstelle (LIFs), sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Netzwerkschnittstellenstatus „Down“ (ocumEvtLifStatusDown)	Risiko	Schnittstelle	Fehler
FC/FCoE-Netzwerkschnittstellenstatus „Down“ (ocumEvtFCLifStatusDown)	Risiko	Schnittstelle	Fehler
Failover der Netzwerkschnittstelle nicht möglich (ocumEvtLifFailoverNotPossible)	Risiko	Schnittstelle	Warnung
Netzwerkschnittstelle nicht am Home-Port (ocumEvtLifNotAtHomePort)	Risiko	Schnittstelle	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Netzwerkschnittstellenroute nicht konfiguriert (Nicht zutreffend)	Ereignis	Schnittstelle	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkschnittstelle MB/s überschritten (ocumNetworkLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
Warnschwelle für Netzwerkschnittstelle in MB/s überschritten (ocumNetworkLifMbpsWarning)	Risiko	Schnittstelle	Warnung
Kritischer Schwellenwert für FC-Netzwerkschnittstelle MB/s überschritten (ocumFcpLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
Warnschwelle für FC-Netzwerkschnittstelle (MB/s) überschritten (ocumFcpLifMbpsWarning)	Risiko	Schnittstelle	Warnung
NVMf FC-Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumNvmfFcLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
NVMf FC-Netzwerkschnittstelle MB/s-Warnschwelle überschritten (ocumNvmfFcLifMbpsWarning)	Risiko	Schnittstelle	Warnung

LUN-Ereignisse

LUN-Ereignisse liefern Ihnen Informationen zum Status Ihrer LUNs, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN offline (ocumEvtLunOffline)	Vorfall	LUN	Kritisch
LUN zerstört *(lunDestroy)	Ereignis	LUN	Information
LUN mit nicht unterstütztem Betriebssystem in igroup (igroupUnsupportedOsType) zugeordnet	Vorfall	LUN	Warnung
Einzelner aktiver Pfad zum Zugriff auf LUN (ocumEvtLunSingleActivePath)	Risiko	LUN	Warnung
Keine aktiven Pfade zum Zugriff auf LUN (ocumEvtLunNotReachable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade für den Zugriff auf LUN (ocumEvtLunOptimizedPathInactive)	Risiko	LUN	Warnung
Keine Pfade für den Zugriff auf LUN vom HA-Partner (ocumEvtLunHaPathInactive)	Risiko	LUN	Warnung
Kein Pfad zum Zugriff auf LUN von einem Knoten im HA-Paar (ocumEvtLunNodePathStatusDown)	Risiko	LUN	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Nicht genügend Speicherplatz für LUN-Snapshot-Kopie (ocumEvtLunSnapshotNotPossible)	Risiko	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN mit nicht unterstütztem Betriebssystem in igroup (igroupUnsupportedOsType) zugeordnet	Risiko	LUN	Warnung

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer LUN-IOPS-Schwellenwert überschritten (ocumLunIopsIncident)	Vorfall	LUN	Kritisch
LUN-IOPS-Warnschwelle überschritten (ocumLunIopsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN MB/s überschritten (ocumLunMbpsIncident)	Vorfall	LUN	Kritisch
LUN-MB/s-Warnschwelle überschritten (ocumLunMbpsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz ms/op überschritten (ocumLunLatencyIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN-Latenz ms/op-Warnschwelle überschritten (ocumLunLatencyWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und IOPS überschritten (ocumLunLatencyIopsIncident)	Vorfall	LUN	Kritisch
Schwellenwert für LUN-Latenz und IOPS-Warnung überschritten (ocumLunLatencyIopsWarning)	Risiko	LUN	Warnung
LUN-Latenz und kritischer MB/s-Schwellenwert überschritten (ocumLunLatencyMbpsIncident)	Vorfall	LUN	Kritisch
LUN-Latenz und MB/s-Warnschwelle überschritten (ocumLunLatencyMbpsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für LUN-Latenz und Gesamtauslastung überschritten (ocumLunLatencyAggregateUtilizationIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Gesamtauslastung überschritten (ocumLunLatencyAggregateUtilizationWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und genutzte Knotenleistungskapazität überschritten (ocumLunLatencyNodePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Knotenleistung bei genutzter Kapazität überschritten (ocumLunLatencyNodePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Verwendete LUN-Latenz und Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Verwendete LUN-Latenz und Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Knotenauslastung überschritten (ocumLunLatencyNodeUtilizationIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Knotenauslastung überschritten (ocumLunLatencyNodeUtilizationWarning)	Risiko	LUN	Warnung
Warnschwelle für maximale IOPS von QoS LUN überschritten (ocumQosLunMaxIopsWarning)	Risiko	LUN	Warnung
QoS LUN Max MB/s-Warnschwelle überschritten (ocumQosLunMaxMbpsWarning)	Risiko	LUN	Warnung
Der Latenzschwellenwert der Workload-LUN wurde gemäß der Leistungs-Servicelevel-Richtlinie überschritten (ocumConformanceLatencyWarning).	Risiko	LUN	Warnung

Ereignisse der Verwaltungsstation

Ereignisse der Verwaltungsstation liefern Ihnen Informationen zum Status des Servers, auf dem Unified Manager installiert ist, sodass Sie ihn auf potenzielle Probleme

überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherplatz des Verwaltungsservers fast voll (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risiko	Verwaltungsstation	Warnung
Verwaltungsserver-Festplattenspeicher voll (ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Verwaltungsstation	Kritisch
Wenig Arbeitsspeicher auf dem Verwaltungsserver (ocumEvtUnifiedManagerMemoryLow)	Risiko	Verwaltungsstation	Warnung
Verwaltungsserver hat fast keinen Speicher mehr (ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Verwaltungsstation	Kritisch
Größe der MySQL-Protokolldatei erhöht; Neustart erforderlich (ocumEvtMysqlLogFileSizeWarning)	Vorfall	Verwaltungsstation	Warnung
Die Gesamtzuweisungsgröße für das Überwachungsprotokoll ist fast erschöpft	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Zertifikat läuft bald ab	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Zertifikat abgelaufen	Risiko	Verwaltungsstation	Fehler
Audit-Protokolldatei manipuliert	Risiko	Verwaltungsstation	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Audit-Protokolldatei gelöscht	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Verbindungsfehler	Risiko	Verwaltungsstation	Fehler
Syslog-Serverkonfiguration geändert	Ereignis	Verwaltungsstation	Warnung

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Analyse der Leistungsdaten ist beeinträchtigt (ocumEvtUnifiedManagerDataMissingAnalyze)	Risiko	Verwaltungsstation	Warnung
Die Leistungsdatenerfassung ist beeinträchtigt (ocumEvtUnifiedManagerDataMissingCollection)	Vorfall	Verwaltungsstation	Kritisch

Diese letzten beiden Leistungsereignisse waren nur für Unified Manager 7.2 verfügbar. Wenn eines dieser Ereignisse im Status „Neu“ vorhanden ist und Sie dann auf eine neuere Version der Unified Manager-Software aktualisieren, werden die Ereignisse nicht automatisch gelöscht. Sie müssen die Ereignisse manuell in den Status „Gelöst“ verschieben.

MetroCluster Bridge-Ereignisse

MetroCluster Bridge-Ereignisse liefern Ihnen Informationen zum Status der Bridges, sodass Sie potenzielle Probleme in einer MetroCluster über-FC-Konfiguration überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Brücke nicht erreichbar (ocumEvtBridgeUnreachable)	Vorfall	MetroCluster Brücke	Kritisch
Brückentemperatur anormal (ocumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster Brücke	Kritisch

MetroCluster -Konnektivitätsereignisse

Konnektivitätsereignisse liefern Ihnen Informationen zur Konnektivität zwischen den Komponenten eines Clusters und zwischen Clustern in MetroCluster over FC- und MetroCluster over IP-Konfigurationen, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

In beiden Konfigurationen gemeinsame Ereignisse

Diese Konnektivitätsereignisse sind sowohl für MetroCluster über FC- als auch für MetroCluster über IP-Konfigurationen üblich.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Alle Links zwischen MetroCluster Partnern ausgefallen (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Vorfall	MetroCluster -Beziehung	Kritisch
MetroCluster Partner über Peering-Netzwerk nicht erreichbar (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Vorfall	MetroCluster -Beziehung	Kritisch
MetroCluster Disaster-Recovery-Funktion beeinträchtigt (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster -Beziehung	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
MetroCluster -Konfiguration umgeschaltet (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster -Beziehung	Warnung

MetroCluster über FC-Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster über FC-Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Alle Inter-Switch-Verbindungen ausgefallen (ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster Inter-Switch-Verbindung	Kritisch
FC-SAS-Bridge zum Speicherstapel-Link Down (ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster -Konfiguration teilweise umgeschaltet (ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risiko	MetroCluster -Beziehung	Fehler
Knoten zum FC-Switch: Alle FC-VI-Verbindungsverbindungen unterbrochen (ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster -Knoten -Switch-Verbindung	Kritisch
Knoten zum FC-Switch: Eine oder mehrere FC-Initiator-Verbindungen ausgefallen (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risiko	MetroCluster -Knoten -Switch-Verbindung	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten zum FC-Switch: Alle FC-Initiator-Verbindungen unterbrochen (ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster -Knoten -Switch-Verbindung	Kritisch
Wechseln Sie zur FC-SAS-Bridge. FC-Link ausgefallen (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	MetroCluster -Switch -Bridge-Verbindung	Kritisch
Zwischen Knoten: Alle FC VI-InterConnect-Verbindungen ausgefallen (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen Knoten	Kritisch
Zwischen Knoten: Eine oder mehrere FC VI-InterConnect-Verbindungen ausgefallen (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risiko	Verbindung zwischen Knoten	Warnung
Knoten zur Bridge-Verbindung unterbrochen (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Knotenbrückenverbindung	Kritisch
Knoten zum Speicherstapel: Alle SAS-Verbindungen unterbrochen (ocumEvtMccNodeStackLinksDown)	Vorfall	Knotenstapelverbindung	Kritisch
Knoten zum Speicherstapel: Eine oder mehrere SAS-Verbindungen unterbrochen (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risiko	Knotenstapelverbindung	Warnung

MetroCluster über IP-Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster -over-IP-Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Der Status der IP-Verbindung zwischen den Standorten von MetroCluster ist deaktiviert (mccIntersiteconnectivityStatusDown).	Risiko	MetroCluster -Beziehung	Kritisch
MetroCluster– IP-Knoten zum Offline-Schalten der Verbindung (mccIpPortStatusOffline)	Risiko	Node	Fehler

MetroCluster -Switch-Ereignisse

MetroCluster Switch-Ereignisse für MetroCluster über FC-Konfigurationen liefern Ihnen Informationen zum Status der MetroCluster -Switches, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schaltertemperatur abnormal (ocumEvtSwitchTemperatureAbnormal)	Vorfall	MetroCluster Switch	Kritisch
Switch nicht erreichbar (ocumEvtSwitchUnreachable)	Vorfall	MetroCluster Switch	Kritisch
Lüfterschalter ausgefallen (ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Fehler bei der Stromversorgung des Switches (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Schaltertemperatursensoren ausgefallen (ocumEvtSwitchTemperatureSensorFailed) Dieses Ereignis gilt nur für Cisco -Switches.	Vorfall	MetroCluster Switch	Kritisch

NVMe-Namespace-Ereignisse

NVMe-Namespace-Ereignisse liefern Ihnen Informationen zum Status Ihrer Namespaces, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVMeNS Offline *(nvmeNamespaceStatusOffline)	Ereignis	Namensraum	Information
NVMeNS Online *(nvmeNamespaceStatusOnline)	Ereignis	Namensraum	Information
Nicht genügend Speicherplatz für NVMeNS *(nvmeNamespaceSpaceOutOfSpace)	Risiko	Namensraum	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVMeNS zerstören *(nvmeNamespaceDestroy)	Ereignis	Namensraum	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer IOPS-Schwellenwert für NVMe-Namespace überschritten (ocumNvmeNamespaceIopsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-IOPS-Warnschwelle überschritten (ocumNvmeNamespaceIopsWarning)	Risiko	Namensraum	Warnung
Kritischer Schwellenwert für NVMe-Namespace MB/s überschritten (ocumNvmeNamespaceMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace MB/s-Warnschwelle überschritten (ocumNvmeNamespaceMbpsWarning)	Risiko	Namensraum	Warnung
NVMe-Namespace-Latenz ms/op – kritischer Schwellenwert überschritten (ocumNvmeNamespaceLatencyIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-Latenz-ms/op-Warnschwelle überschritten (ocumNvmeNamespaceLatencyWarning)	Risiko	Namensraum	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVMe-Namespace-Latenz und kritischer IOPS-Schwellenwert überschritten (ocumNvmeNamespaceLatencyIopsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-Latenz- und IOPS-Warnschwelle überschritten (ocumNvmeNamespaceLatencyIopsWarning)	Risiko	Namensraum	Warnung
NVMe-Namespace-Latenz und kritischer MB/s-Schwellenwert überschritten (ocumNvmeNamespaceLatencyMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-Latenz und MB/s-Warnschwelle überschritten (ocumNvmeNamespaceLatencyMbpsWarning)	Risiko	Namensraum	Warnung

Knotenereignisse

Knotenereignisse liefern Ihnen Informationen zum Knotenstatus, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherplatz des Knotenstammvolumes fast voll (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risiko	Node	Fehler
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risiko	Node	Fehler
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risiko	Node	Fehler
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risiko	Node	Fehler
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Ereignis	Node	Information
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risiko	Node	Fehler
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risiko	Node	Fehler
Cloud Tier-Host nicht auflösbar *(ocumObjstoreHostUnresolvable)	Risiko	Node	Fehler
Cloud Tier Intercluster-Netzwerkschnittstelle ausgefallen *(ocumObjstoreInterClusterLifDown)	Risiko	Node	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Einer der NFSv4-Pools erschöpft *(nbladeNfsv4PoolEXhaust)	Vorfall	Node	Kritisch
Anforderung stimmt nicht mit Cloud-Tier-Signatur überein *(oscSignatureMismatch)	Risiko	Node	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
QoS-Monitor-Speicher maximal *(ocumQosMonitorMemoryMaxed)	Risiko	Node	Fehler
QoS-Monitor-Speicher verringert *(ocumQosMonitorMemoryAbated)	Ereignis	Node	Information

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten umbenannt (Nicht zutreffend)	Ereignis	Node	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Knoten-IOPS-Schwellenwert überschritten (ocumNodeIopsIncident)	Vorfall	Node	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten-IOPS-Warnschwelle überschritten (ocumNodeIopsWarning)	Risiko	Node	Warnung
Kritischer Knoten-MB/s-Schwellenwert überschritten (ocumNodeMbpsIncident)	Vorfall	Node	Kritisch
Knoten-MB/s-Warnschwelle überschritten (ocumNodeMbpsWarning)	Risiko	Node	Warnung
Knotenlatenz ms/op – kritischer Schwellenwert überschritten (ocumNodeLatencyIncident)	Vorfall	Node	Kritisch
Knotenlatenz ms/op-Warnschwelle überschritten (ocumNodeLatencyWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für genutzte Knotenleistungskapazität überschritten (ocumNodePerfCapacityUsedIncident)	Vorfall	Node	Kritisch
Warnschwelle für genutzte Knotenleistungskapazität überschritten (ocumNodePerfCapacityUsedWarning)	Risiko	Node	Warnung
Ausgenutzte Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumNodePerfCapacityUsedTakeoverIncident)	Vorfall	Node	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ausgenutzte Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumNodePerfCapacityUsedTakeoverWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knotenauslastung überschritten (ocumNodeUtilizationIncident)	Vorfall	Node	Kritisch
Warnschwelle für Knotenauslastung überschritten (ocumNodeUtilizationWarning)	Risiko	Node	Warnung
Schwellenwert für überbeanspruchtes Knoten-HA-Paar überschritten (ocumNodeHaPairOverUtilizedInformation)	Ereignis	Node	Information
Schwellenwert für die Fragmentierung der Knotenfestplatte überschritten (ocumNodeDiskFragmentationWarning)	Risiko	Node	Warnung
Schwellenwert für genutzte Leistungskapazität überschritten (ocumNodeOverUtilizedWarning)	Risiko	Node	Warnung
Dynamischer Knotenschwellenwert überschritten (ocumNodeDynamicEventWarning)	Risiko	Node	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Hinweis-ID: NTAP-<*advisory ID*>(ocumx)	Risiko	Node	Kritisch

NVRAM -Batterieereignisse

NVRAM Batterieereignisse liefern Ihnen Informationen zum Status Ihrer Batterien, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVRAM -Batterie schwach (ocumEvtNvramBatteryLow)	Risiko	Node	Warnung
NVRAM -Batterie entladen (ocumEvtNvramBatteryDischarged)	Risiko	Node	Fehler
NVRAM -Batterie überladen (ocumEvtNvramBatteryOverCharged)	Vorfall	Node	Kritisch

Hafenereignisse

Portereignisse liefern Ihnen den Status von Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, beispielsweise ob der Port ausgefallen ist.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Portstatus deaktiviert (ocumEvtPortStatusDown)	Vorfall	Node	Kritisch

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkport MB/s überschritten (ocumNetworkPortMbpsIncident)	Vorfall	Hafen	Kritisch
Warnschwelle für Netzwerkport MB/s überschritten (ocumNetworkPortMbpsWarning)	Risiko	Hafen	Warnung
FCP-Port MB/s kritischer Schwellenwert überschritten (ocumFcpPortMbpsIncident)	Vorfall	Hafen	Kritisch
FCP-Port MB/s-Warnschwelle überschritten (ocumFcpPortMbpsWarning)	Risiko	Hafen	Warnung
Kritischer Schwellenwert für Netzwerk-Port-Auslastung überschritten (ocumNetworkPortUtilizationIncident)	Vorfall	Hafen	Kritisch
Warnschwelle für Netzwerk-Port-Auslastung überschritten (ocumNetworkPortUtilizationWarning)	Risiko	Hafen	Warnung
Kritischer Schwellenwert für FCP-Portauslastung überschritten (ocumFcpPortUtilizationIncident)	Vorfall	Hafen	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für FCP-Portauslastung überschritten (ocumFcpPortUtilizationWarning)	Risiko	Hafen	Warnung

Netzteilereignisse

Netzteilereignisse liefern Ihnen Informationen zum Status Ihrer Hardware, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ein oder mehrere Netzteile ausgefallen (ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Node	Kritisch

Schutzereignisse

Schutzereignisse informieren Sie darüber, ob ein Job fehlgeschlagen ist oder abgebrochen wurde, sodass Sie ihn auf Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schutzauftrag fehlgeschlagen (ocumEvtProtectionJobTaskFailed)	Vorfall	Volumen- oder Speicherdienst	Kritisch
Schutzauftrag abgebrochen (ocumEvtProtectionJobAborted)	Risiko	Volumen- oder Speicherdienst	Warnung

Qtree-Ereignisse

Qtree-Ereignisse liefern Ihnen Informationen zur Qtree-Kapazität und den Datei- und Festplattenlimits, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Qtree-Speicherplatz fast voll (ocumEvtQtreeSpaceNearlyFull)	Risiko	Qtree	Warnung
Qtree-Speicherplatz voll (ocumEvtQtreeSpaceFull)	Risiko	Qtree	Fehler
Qtree Space Normal (ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Information
Qtree-Dateien-Hardlimit erreicht (ocumEvtQtreeFilesHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree-Dateien Soft-Limit überschritten (ocumEvtQtreeFilesSoftLimitBreached)	Risiko	Qtree	Warnung
Qtree-Speicherplatz-Hartgrenze erreicht (ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree Space Soft Limit überschritten (ocumEvtQtreeSpaceSoftLimitBreached)	Risiko	Qtree	Warnung

Serviceprozessorereignisse

Serviceprozessorereignisse liefern Ihnen Informationen zum Status Ihres Prozessors, sodass Sie ihn auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die

Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Serviceprozessor nicht konfiguriert (ocumEvtServiceProcessorNotConfigured)	Risiko	Node	Warnung
Serviceprozessor offline (ocumEvtServiceProcessorOffline)	Risiko	Node	Fehler

SnapMirror -Beziehungsereignisse

SnapMirror Beziehungsereignisse liefern Ihnen Informationen zum Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage-VMs als auch für Volumes generiert, synchrone SnapMirror -Beziehungsereignisse werden jedoch nur für Volume-Beziehungen generiert. Für Bestandteilvolumes, die Teil von Storage-VM-Notfallwiederherstellungsbeziehungen sind, werden keine Ereignisse generiert. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Die SnapMirror -Beziehungsereignisse werden für Storage-VMs generiert, die durch die Notfallwiederherstellung von Storage-VMs geschützt sind, jedoch nicht für Beziehungen zwischen Bestandteilobjekten.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Spiegelreplikation fehlerhaft (ocumEvtSnapmirrorRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Abgebrochene Spiegelreplikation (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Initialisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Verzögerungsfehler bei der Spiegelreplikation (ocumEvtSnapMirrorRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Warnung bei Verzögerung bei Spiegelreplikation (ocumEvtSnapMirrorRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Neusynchronisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler
Synchrone Replikation nicht synchron *(syncSnapmirrorRelationshipOutofsync)	Risiko	SnapMirror -Beziehung	Warnung
Synchrone Replikation wiederhergestellt *(syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror -Beziehung	Information
Automatische Neusynchronisierung der synchronen Replikation fehlgeschlagen *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ontap Mediator wird zum Cluster hinzugefügt (snapmirrorMediatorAdded)	Ereignis	Cluster	Information
Ontap Mediator wird aus dem Cluster entfernt (snapmirrorMediatorRemoved)	Ereignis	Cluster	Information
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorUnreachable)	Risiko	Vermittler	Warnung
Auf Ontap Mediator kann vom Cluster aus nicht zugegriffen werden (SnapmirrorMediator falsch konfiguriert).	Risiko	Vermittler	Fehler
Die Ontap Mediator-Konnektivität wurde wiederhergestellt, ist neu synchronisiert und bereit für die aktive Synchronisierung mit SnapMirror (snapmirrorMediatorInQuorum).	Ereignis	Vermittler	Information

Asynchrone Mirror- und Vault-Beziehungsereignisse

Ereignisse für asynchrone Mirror- und Vault-Beziehungen liefern Ihnen Informationen zum Status Ihrer asynchronen SnapMirror und Vault-Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Asynchrone Spiegel- und Vault-Beziehungsereignisse werden sowohl für Volume- als auch für Storage-VM-Schutzbeziehungen unterstützt. Für die Notfallwiederherstellung von Storage-VMs werden jedoch nur Vault-Beziehungen nicht unterstützt. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Die SnapMirror und Vault-Beziehungsereignisse werden auch für Storage-VMs generiert, die durch die Notfallwiederherstellung von Storage-VMs geschützt sind, jedoch nicht für Beziehungen zwischen Bestandteilobjekten.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchroner Spiegel und Tresor fehlerhaft (ocumEvtMirrorVaultRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Asynchroner Spiegel und Tresor abgebrochen (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegelung und Vault-Initialisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegel- und Vault-Aktualisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchroner Mirror- und Vault-Lag-Fehler (ocumEvtMirrorVaultRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegel- und Vault-Verzögerungswarnung (ocumEvtMirrorVaultRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Asynchrone Spiegelung und Vault-Neusynchronisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler

Das Ereignis „SnapMirror -Updatefehler“ wird vom Active IQ Portal (Config Advisor) ausgelöst.

Snapshot-Ereignisse

Snapshot-Ereignisse liefern Informationen zum Status von Snapshots, sodass Sie die Snapshots auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Automatisches Löschen von Snapshots deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Automatisches Löschen von Snapshots aktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Snapshot-Konfiguration automatisch löschen, geändert (nicht zutreffend)	Ereignis	Volumen	Information

SnapVault -Beziehungsereignisse

SnapVault Beziehungsereignisse liefern Ihnen Informationen zum Status Ihrer SnapVault -Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchroner Tresor fehlerhaft (ocumEvtSnapVaultRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Asynchroner Tresor abgebrochen (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchrone Vault-Initialisierung fehlgeschlagen (ocumEvtSnapVaultRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Vault-Aktualisierung fehlgeschlagen (ocumEvtSnapVaultRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchroner Vault-Lag-Fehler (ocumEvtSnapVaultRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Vault-Verzögerungswarnung (ocumEvtSnapVaultRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Asynchrone Vault-Neusynchronisierung fehlgeschlagen (ocumEvtSnapvaultRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisse der Speicherfailovereinstellungen

Ereignisse der Speicherfailover-Einstellungen (SFO) liefern Ihnen Informationen darüber, ob Ihr Speicherfailover deaktiviert oder nicht konfiguriert ist, sodass Sie es auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicher-Failover-Verbindung: Eine oder mehrere Verbindungen sind ausgefallen (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risiko	Node	Warnung
Speicherfailover deaktiviert (ocumEvtSfoSettingsDisabled)	Risiko	Node	Fehler
Speicherfailover nicht konfiguriert (ocumEvtSfoSettingsNotConfigured)	Risiko	Node	Fehler
Speicher-Failover-Status – Übernahme (ocumEvtSfoStateTakeover)	Risiko	Node	Warnung
Speicherfailoverstatus – teilweise Rückgabe (ocumEvtSfoStatePartialGiveback)	Risiko	Node	Fehler
Speicher-Failover-Knotenstatus „Down“ (ocumEvtSfoNodeStatusDown)	Risiko	Node	Fehler
Speicher-Failover-Übernahme nicht möglich (ocumEvtSfoTakeoverNotPossible)	Risiko	Node	Fehler

Speicherdienstereignisse

Speicherdienstereignisse liefern Ihnen Informationen zur Erstellung und zum Abonnement von Speicherdiensten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherdienst erstellt (Nicht zutreffend)	Ereignis	Lagerservice	Information
Abonnierter Speicherdienst (Nicht zutreffend)	Ereignis	Lagerservice	Information
Speicherdienst abgemeldet (Nicht zutreffend)	Ereignis	Lagerservice	Information

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Unerwartete Löschung der verwalteten SnapMirror -BeziehungocumEvtStorageServiceUnsupportedRelationshipDeletion	Risiko	Lagerservice	Warnung
Unerwartete Löschung des Storage Service Member Volumes (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Vorfall	Lagerservice	Kritisch

Lagerregalereignisse

Durch Speicherregalereignisse werden Sie über ungewöhnliche Zustände Ihres Speicherregals informiert, sodass Sie es auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Abnormaler Spannungsbereich (ocumEvtShelfVoltageAbnormal)	Risiko	Ablageboden	Warnung
Abnormaler Strombereich (ocumEvtShelfCurrentAbnormal)	Risiko	Ablageboden	Warnung
Abnormale Temperatur (ocumEvtShelfTemperatureAbnormal)	Risiko	Ablageboden	Warnung

Speicher-VM-Ereignisse

Storage-VM-Ereignisse (Storage Virtual Machine, auch als SVM bezeichnet) liefern Ihnen Informationen zum Status Ihrer Storage-VMs (SVMs), sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
CIFS-Dienst der Speicher-VM ausgefallen (ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
Versuche, eine Verbindung zu einer nicht vorhandenen CIFS-Freigabe herzustellen *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
CIFS-NetBIOS-Namenskonflikt *(nbladeCifsNbNameConflict)	Risiko	SVM	Fehler
CIFS-Schattenkopie-Vorgang fehlgeschlagen *(cifsShadowCopyFailure)	Risiko	SVM	Fehler
Viele CIFS-Verbindungen *(nbladeCifsManyAuths)	Risiko	SVM	Fehler
Maximale CIFS-Verbindung überschritten *(nbladeCifsMaxOpenSameFile)	Risiko	SVM	Fehler
Maximale Anzahl von CIFS-Verbindungen pro Benutzer überschritten *(nbladeCifsMaxSessPerUsrConn)	Risiko	SVM	Fehler
SVM FC/FCoE-Dienst ausgefallen (ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM-iSCSI-Dienst ausgefallen (ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
NFS-Dienst der Speicher-VM ausgefallen (ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM FC/FCoE-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
SVM-iSCSI-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
SVM NFS-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
Speicher-VM gestoppt (ocumEvtVserverDown)	Risiko	SVM	Warnung
AV-Server zu beschäftigt, um neue Scan-Anforderung anzunehmen *(nbladeVscanConnBackPressure)	Risiko	SVM	Fehler
Keine AV-Serververbindung für Virenscan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Risiko	SVM	Fehler
Keine reagierende AV-Serververbindung *(nbladeVscanConnInactive)	Ereignis	SVM	Information
Versuch eines nicht autorisierten Benutzers, den AV-Server zu beschädigen *(nbladeVscanBadUserPrivAccess)	Risiko	SVM	Fehler
Virus vom AV-Server gefunden *(nbladeVscanVirusDetected)	Risiko	SVM	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
SVM erkannt (Nicht zutreffend)	Ereignis	SVM	Information

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
SVM gelöscht (Nicht zutreffend)	Ereignis	Cluster	Information
SVM umbenannt (Nicht zutreffend)	Ereignis	SVM	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer SVM-IOPS-Schwellenwert überschritten (ocumSvmIopsIncident)	Vorfall	SVM	Kritisch
SVM-IOPS-Warnschwelle überschritten (ocumSvmIopsWarning)	Risiko	SVM	Warnung
Kritischer Schwellenwert für SVM MB/s überschritten (ocumSvmMbpsIncident)	Vorfall	SVM	Kritisch
SVM MB/s-Warnschwelle überschritten (ocumSvmMbpsWarning)	Risiko	SVM	Warnung
Kritischer Schwellenwert für SVM-Latenz überschritten (ocumSvmLatencyIncident)	Vorfall	SVM	Kritisch
SVM-Latenzwarnschwelle überschritten (ocumSvmLatencyWarning)	Risiko	SVM	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Überwachungsprotokoll deaktiviert (ocumVserverAuditLogDisabled)	Risiko	SVM	Warnung
Anmeldebanner deaktiviert (ocumVserverLoginBannerDisabled)	Risiko	SVM	Warnung
SSH verwendet unsichere Chiffren (ocumVserverSSHInsecure)	Risiko	SVM	Warnung
Anmeldebanner geändert (ocumVserverLoginBannerChanged)	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage-VM ist deaktiviert (antiRansomwareSvmStateDisabled).	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage-VM ist aktiviert (Lernmodus) (antiRansomwareSvmStateDryrun)	Ereignis	SVM	Information
Für die Anti-Ransomware-Überwachung geeignete Speicher-VM (Lernmodus) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Information

Benutzer- und Gruppenkontingentereignisse

Benutzer- und Gruppenkontingentereignisse liefern Ihnen Informationen zur Kapazität des Benutzer- und Benutzergruppenkontingents sowie zu den Datei- und Datenträgerlimits, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Soft-Limit für Benutzer- oder Gruppenkontingentspeicherplatz überschritten (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Hartes Speicherplatzlimit für Benutzer- oder Gruppenkontingente erreicht (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch
Soft-Limit für die Anzahl der Dateien im Benutzer- oder Gruppenkontingent überschritten (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Festes Limit für die Anzahl der Dateien im Benutzer- oder Gruppenkontingent erreicht (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch

Volumenereignisse

Volume-Ereignisse liefern Informationen zum Status von Volumes, sodass Sie diese auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volumen eingeschränkt (ocumEvtVolumeRestricted)	Risiko	Volumen	Warnung
Volume offline (ocumEvtVolumeOffline)	Vorfall	Volumen	Kritisch
Volume teilweise verfügbar (ocumEvtVolumePartiallyAvailable)	Risiko	Volumen	Fehler
Volume nicht gemountet (Nicht zutreffend)	Ereignis	Volumen	Information
Volume gemountet (Nicht zutreffend)	Ereignis	Volumen	Information
Volume erneut bereitgestellt (Nicht zutreffend)	Ereignis	Volumen	Information
Volume-Junction-Pfad inaktiv (ocumEvtVolumeJunctionPathInactive)	Risiko	Volumen	Warnung
Automatische Volume-Größenanpassung aktiviert (Nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volume-Größenanpassung deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volume-Größenanpassung – Maximale Kapazität geändert (Nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volumengrößenerhöhung – Größe geändert (nicht zutreffend)	Ereignis	Volumen	Information

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Gefährdeter Speicherplatz auf Thin-Provisioned-Volume (ocumThinProvisionVolumeSpaceAtRisk)	Risiko	Volumen	Warnung
Fehler beim Volume-Effizienz-Vorgang (ocumEvtVolumeEfficiencyOperationError)	Risiko	Volumen	Fehler
Volume-Speicherplatz voll (ocumEvtVolumeFull)	Risiko	Volumen	Fehler
Volume-Speicherplatz fast voll (ocumEvtVolumeNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Datenträgers voll *(volumeLogicalSpaceFull)	Risiko	Volumen	Fehler
Logischer Speicherplatz des Volumes fast voll *(volumeLogicalSpaceNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Volumes Normal *(volumeLogicalSpaceAllOK)	Ereignis	Volumen	Information
Reservespeicherplatz für Volume-Snapshot voll (ocumEvtSnapshotFull)	Risiko	Volumen	Warnung
Zu viele Snapshot-Kopien (ocumEvtSnapshotTooMany)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume-Qtree-Kontingent überbelegt (ocumEvtVolumeQtreeQuotaOvercommitted)	Risiko	Volumen	Fehler
Volume-Qtree-Kontingent fast überlastet (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risiko	Volumen	Warnung
Abnormale Volumenwachstumsrate (ocumEvtVolumeGrowthRateAbnormal)	Risiko	Volumen	Warnung
Volumen in Tagen bis zur Vollendung (ocumEvtVolumeDaysUntilFullSoon)	Risiko	Volumen	Fehler
Volume-Speicherplatzgarantie deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Volume-Speicherplatzgarantie aktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Garantie für Speicherplatz geändert (nicht zutreffend)	Ereignis	Volumen	Information
Volume-Snapshot-Reservetage bis zur Vollendung (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risiko	Volumen	Fehler
FlexGroup -Bestandteile haben Platzprobleme *(flexGroupConstituentsHaveSpaceIssues)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
FlexGroup -Bestandteil -Raumstatus Alle OK *(flexGroupConstituentsSpaceStatusAllOK)	Ereignis	Volumen	Information
FlexGroup -Bestandteile haben Inodes-Probleme *(flexGroupConstituentsHaveInodesIssues)	Risiko	Volumen	Fehler
FlexGroup -Bestandteile -Inodes-Status: Alle OK *(flexGroupConstituentsInodesStatusAllOK)	Ereignis	Volumen	Information
WAFL -Volume-AutoSize -Fehler *(waflVolAutoSizeFail)	Risiko	Volumen	Fehler
WAFL -Volume-AutoSize erledigt *(waflVolAutoSizeDone)	Ereignis	Volumen	Information
FlexGroup -Volumen ist zu über 80 % ausgelastet*	Vorfall	Volumen	Fehler
FlexGroup Volumen ist zu über 90 % ausgelastet*	Vorfall	Volumen	Kritisch
Anomalie der Volume-Speichereffizienz (ocumVolumeAbnormalStorageEfficiencyWarning)	Risiko	Volumen	Warnung
Volume-Snapshot-Reserve nicht ausreichend genutzt (volumeSnaphotReserveUnderutilizedWarning)	Ereignis	Volumen	Warnung
Volume-Snapshot-Reserve nicht ausreichend genutzt (volumeSnaphotReserveUnderutilizedCleared)	Ereignis	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume umbenannt (Nicht zutreffend)	Ereignis	Volumen	Information
Erkanntes Volumen (Nicht zutreffend)	Ereignis	Volumen	Information
Volume gelöscht (Nicht zutreffend)	Ereignis	Volumen	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für maximale IOPS des QoS-Volumes überschritten (ocumQosVolumeMaxIopsWarning)	Risiko	Volumen	Warnung
Warnschwelle für maximales QoS-Volumen (MB/s) überschritten (ocumQosVolumeMaxMbpsWarning)	Risiko	Volumen	Warnung
Warnschwelle für maximale IOPS/TB des QoS-Volumes überschritten (ocumQosVolumeMaxIopsPerTbWarning)	Risiko	Volumen	Warnung
Latenzschwelle für Workload-Volumen überschritten, wie in der Richtlinie zum Leistungs-Servicelevel definiert (ocumConformanceLatencyWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Volume-IOPS-Schwellenwert überschritten (ocumVolumeIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volume-IOPS-Warnung überschritten (ocumVolumeIopsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume MB/s überschritten (ocumVolumeMbpsIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume MB/s überschritten (ocumVolumeMbpsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz überschritten (ocumVolumeLatencyIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volume-Latenzwarnung überschritten (ocumVolumeLatencyWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Cache-Miss-Ratio überschritten (ocumVolumeCacheMissRatioIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Cache-Miss-Ratio überschritten (ocumVolumeCacheMissRatioWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und IOPS überschritten (ocumVolumeLatencyIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volume-Latenz und IOPS-Warnung überschritten (ocumVolumeLatencyIopsWarning)	Risiko	Volumen	Warnung
Volume-Latenz und kritischer MB/s-Schwellenwert überschritten (ocumVolumeLatencyMbpsIncident)	Vorfall	Volumen	Kritisch
Volume-Latenz und MB/s-Warnschwelle überschritten (ocumVolumeLatencyMbpsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationIncident)	Vorfall	Volumen	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und genutzte Knotenleistungskapazität überschritten (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und Knotenleistung bei genutzter Kapazität überschritten (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Verwendete Volume-Latenz und Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	Volumen	Kritisch
Verwendete Volume-Latenz und Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und Knotenauslastung überschritten (ocumVolumeLatencyNodeUtilizationIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und Knotenauslastung überschritten (ocumVolumeLatencyNodeUtilizationWarning)	Risiko	Volumen	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Volume-Anti-Ransomware-Überwachung ist aktiviert (aktiver Modus) (antiRansomwareVolumeStateEnabled)	Ereignis	Volumen	Information
Die Volume-Anti-Ransomware-Überwachung ist deaktiviert (antiRansomwareVolumeStateDisabled).	Risiko	Volumen	Warnung
Volume-Anti-Ransomware-Überwachung ist aktiviert (Lernmodus) (antiRansomwareVolumeStateDryrun)	Ereignis	Volumen	Information
Die Volume-Anti-Ransomware-Überwachung ist angehalten (Lernmodus) (antiRansomwareVolumeStateDryrunPaused)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Volume-Anti-Ransomware-Überwachung ist angehalten (aktiver Modus) (antiRansomwareVolumeStateEnablePaused)	Risiko	Volumen	Warnung
Die Volume-Anti-Ransomware-Überwachung wird deaktiviert (antiRansomwareVolumeStateDisableInProgress)	Risiko	Volumen	Warnung
Ransomware-Aktivität erkannt (callHomeRansomwareActivitySeen)	Vorfall	Volumen	Kritisch
Für die Anti-Ransomware-Überwachung geeignetes Volume (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Volumen	Information
Für die Anti-Ransomware-Überwachung geeignetes Volume (Aktivmodus) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risiko	Volumen	Warnung
Das Volume weist laute Anti-Ransomware-Warnmeldungen auf (antiRansomwareFeatureNoisyVolume)	Risiko	Volumen	Warnung

Wirkungsbereich: Datenschutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionWarning)	Risiko	Volumen	Warnung
Das Volume verfügt über keinen ausreichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionCleared)	Risiko	Volumen	Warnung

Statusereignisse für die Volumeverschiebung

Statusereignisse zur Volumeverschiebung informieren Sie über den Status Ihrer Volumeverschiebung, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Status der Datenträgerverschiebung: In Bearbeitung (Nicht zutreffend)	Ereignis	Volumen	Information
Status der Volumeverschiebung – Fehlgeschlagen (ocumEvtVolumeMoveFailed)	Risiko	Volumen	Fehler
Status der Datenträgerverschiebung: Abgeschlossen (Nicht zutreffend)	Ereignis	Volumen	Information
Volume-Verschiebung – Umstellung verschoben (ocumEvtVolumeMoveCutoverDeferred)	Risiko	Volumen	Warnung

Beschreibung der Ereignisfenster und Dialogfelder

Ereignisse benachrichtigen Sie über alle Probleme in Ihrer Umgebung. Sie können die Inventarseite und die Seite mit den Ereignisdetails der Ereignisverwaltung verwenden, um alle Ereignisse zu überwachen. Sie können die Benachrichtigung im Dialogfeld „Benachrichtigungs-Setup-Optionen“ konfigurieren. Auf der Seite „Ereigniseinrichtung“ können Sie Ereignisse deaktivieren oder aktivieren.

Benachrichtigungsseite

Sie können den Unified Manager-Server so konfigurieren, dass er Benachrichtigungen sendet, wenn ein Ereignis generiert oder einem Benutzer zugewiesen wird. Sie können auch die Benachrichtigungsmechanismen konfigurieren. Beispielsweise können Benachrichtigungen als E-Mails oder SNMP-Traps versendet werden.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

E-Mail

In diesem Bereich können Sie die folgenden E-Mail-Einstellungen für Warnbenachrichtigungen konfigurieren:

- **Absenderadresse**

  Gibt die E-Mail-Adresse an, von der die Warnbenachrichtigung gesendet wird. Dieser Wert wird auch als Absenderadresse für einen Bericht verwendet, wenn dieser freigegeben wird. Wenn die Absenderadresse bereits mit der Adresse „ActiveIQUnifiedManager@localhost.com“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.

SMTP-Server

In diesem Bereich können Sie die folgenden SMTP-Servereinstellungen konfigurieren:

- **Hostname oder IP-Adresse**

  Gibt den Hostnamen Ihres SMTP-Hostservers an, der zum Senden der Warnbenachrichtigung an die angegebenen Empfänger verwendet wird.

- **Benutzername**

  Gibt den SMTP-Benutzernamen an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH im SMTP-Server aktiviert ist.

- **Passwort**

  Gibt das SMTP-Passwort an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH im SMTP-Server aktiviert ist.

- **Hafen**

  Gibt den Port an, der vom SMTP-Hostserver zum Senden von Warnbenachrichtigungen verwendet wird.

Der Standardwert ist 25.

- **START/TLS verwenden**

  Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe der TLS/SSL-Protokolle (auch als start_tls und StartTLS bezeichnet) gewährleistet.

- **SSL verwenden**

  Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe des SSL-Protokolls gewährleistet.

SNMP

In diesem Bereich können Sie die folgenden SNMP-Trap-Einstellungen konfigurieren:

- **Version**

  Gibt die SNMP-Version an, die Sie je nach der Art der erforderlichen Sicherheit verwenden möchten. Zu den Optionen gehören Version 1, Version 3, Version 3 mit Authentifizierung und Version 3 mit Authentifizierung und Verschlüsselung. Der Standardwert ist Version 1.

- **Trap-Zielhost**

  Gibt den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) an, die die vom Verwaltungsserver gesendeten SNMP-Traps empfängt. Um mehrere Trap-Ziele anzugeben, trennen Sie jeden Host durch ein Komma.

  Alle anderen SNMP-Einstellungen, wie beispielsweise „Version“ und „Ausgehender Port“, müssen für alle Hosts in der Liste gleich sein.

- **Ausgehender Trap-Port**

  Gibt den Port an, über den der SNMP-Server die Traps empfängt, die vom Management-Server gesendet werden.

  Der Standardwert ist 162.

- **Gemeinschaft**

  Der Community-String für den Zugriff auf den Host.

- **Motor-ID**

  Gibt die eindeutige Kennung des SNMP-Agenten an und wird automatisch vom Verwaltungsserver generiert. Engine ID ist mit SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Benutzername**

  Gibt den SNMP-Benutzernamen an. Der Benutzername ist mit SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungsprotokoll**

Gibt das zur Authentifizierung eines Benutzers verwendete Protokoll an. Zu den Protokolloptionen gehören MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungskennwort**

  Gibt das Kennwort an, das bei der Authentifizierung eines Benutzers verwendet wird. Das Authentifizierungskennwort ist mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzprotokoll**

  Gibt das Datenschutzprotokoll an, das zum Verschlüsseln von SNMP-Nachrichten verwendet wird. Zu den Protokolloptionen gehören AES 128 und DES. Der Standardwert ist AES 128. Das Datenschutzprotokoll ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutz-Passwort**

  Gibt das Kennwort bei Verwendung des Datenschutzprotokolls an. Ein Datenschutzkennwort ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Weitere Informationen zu SNMP-Objekten und Traps finden Sie im Downloadbereich"Active IQ Unified Manager MIB" von der NetApp Support-Site.

Inventarseite für die Ereignisverwaltung

Auf der Inventarseite der Ereignisverwaltung können Sie eine Liste der aktuellen Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie das Bestätigen, Auflösen und Zuweisen von Ereignissen ausführen. Sie können auch eine Benachrichtigung für bestimmte Ereignisse hinzufügen.

Die Informationen auf dieser Seite werden alle 5 Minuten automatisch aktualisiert, um sicherzustellen, dass die aktuellsten neuen Ereignisse angezeigt werden.

Filterkomponenten

Ermöglicht Ihnen, die in der Ereignisliste angezeigten Informationen anzupassen. Sie können die Liste der angezeigten Ereignisse mithilfe der folgenden Komponenten verfeinern:

- Menü „Ansicht“ zur Auswahl aus einer vordefinierten Liste mit Filterauswahlen.

  Dazu gehören Elemente wie alle aktiven (neuen und bestätigten) Ereignisse, aktive Leistungsereignisse, mir (dem angemeldeten Benutzer) zugewiesene Ereignisse und alle während aller Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Ereignisliste durch Eingabe ganzer oder teilweiser Begriffe.
- Filterschaltfläche, die den Filterbereich öffnet, sodass Sie aus allen verfügbaren Feldern und Feldattributen auswählen können, um die Liste der Ereignisse zu verfeinern.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zuweisen an**

  Ermöglicht Ihnen, den Benutzer auszuwählen, dem das Ereignis zugewiesen ist. Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der Sie das Ereignis zugewiesen haben, der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  - Mich

    Weist das Ereignis dem aktuell angemeldeten Benutzer zu.

  - Ein anderer Benutzer

    Zeigt das Dialogfeld „Besitzer zuweisen“ an, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können. Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Eigentümerfeld leer lassen.

- **Anerkennen**

  Bestätigt die ausgewählten Ereignisse.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der Sie das Ereignis bestätigt haben, der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, sind Sie für die Verwaltung dieses Ereignisses verantwortlich.

  Sie können Informationsereignisse nicht bestätigen.

- **Als gelöst markieren**

  Ermöglicht Ihnen, den Ereignisstatus in „Gelöst“ zu ändern.

  Wenn Sie ein Ereignis lösen, werden Ihr Benutzername und der Zeitpunkt der Lösung des Ereignisses der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Benachrichtigung hinzufügen**

  Zeigt das Dialogfeld „Warnung hinzufügen“ an, in dem Sie Warnungen für die ausgewählten Ereignisse hinzufügen können.

- **Berichte**

  Ermöglicht Ihnen, Details der aktuellen Ereignisansicht in eine CSV-Datei (Comma-Separated Values) oder ein PDF-Dokument zu exportieren.

- **Spaltenauswahl ein-/ausblenden**

  Ermöglicht Ihnen, die auf der Seite anzuzeigenden Spalten auszuwählen und die Reihenfolge auszuwählen, in der sie angezeigt werden.

Ereignisliste

Zeigt Details aller Ereignisse sortiert nach Auslösezeit an.

Standardmäßig wird die Ansicht „Alle aktiven Ereignisse“ angezeigt, um die neuen und bestätigten Ereignisse der letzten sieben Tage anzuzeigen, die die Auswirkungsstufe „Vorfall“ oder „Risiko“ aufweisen.

- **Ausgelöste Zeit**

  Der Zeitpunkt, zu dem das Ereignis generiert wurde.

- **Schwere**

  Der Schweregrad des Ereignisses: Kritisch ( ), Fehler ( ), Warnung ( ) und Informationen ( ).

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Gelöst oder Veraltet.

- **Auswirkungsebene**

  Die Auswirkungsstufe des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Auswirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Leistung, Schutz, Konfiguration oder Sicherheit.

- **Name**

  Der Name des Ereignisses. Sie können den Namen auswählen, um die Seite mit den Ereignisdetails für dieses Ereignis anzuzeigen.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist. Sie können den Namen auswählen, um die Seite mit den Integritäts- oder Leistungsdetails für dieses Objekt anzuzeigen.

  Wenn ein Verstoß gegen die gemeinsame QoS-Richtlinie auftritt, wird in diesem Feld nur das Workload-Objekt angezeigt, das die meisten IOPS oder MB/s verbraucht. Zusätzliche Workloads, die diese Richtlinie verwenden, werden auf der Seite „Ereignisdetails“ angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. Storage VM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- **Zugewiesen an**

  Der Name des Benutzers, dem das Ereignis zugewiesen ist.

- **Ereignisursprung**

  Ob das Ereignis vom „Active IQ Portal“ oder direkt vom „Active IQ Unified Manager“ stammt.

- **Anmerkungsname**

  Der Name der Anmerkung, die dem Speicherobjekt zugewiesen ist.

- **Anmerkungen**

  Die Anzahl der Notizen, die für ein Ereignis hinzugefügt werden.

- **Ausstehende Tage**

Die Anzahl der Tage seit der ersten Generierung des Ereignisses.

- **Zugewiesene Zeit**

  Die Zeit, die vergangen ist, seit das Ereignis einem Benutzer zugewiesen wurde. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, wann das Ereignis einem Benutzer zugewiesen wurde.

- **Bestätigt von**

  Der Name des Benutzers, der das Ereignis bestätigt hat. Das Feld ist leer, wenn das Ereignis nicht bestätigt wurde.

- **Bestätigte Zeit**

  Die Zeit, die seit der Bestätigung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis bestätigt wurde.

- **Gelöst von**

  Der Name des Benutzers, der das Ereignis gelöst hat. Das Feld ist leer, wenn das Ereignis nicht behoben ist.

- **Gelöst Zeit**

  Die Zeit, die seit der Lösung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis behoben wurde.

- **Veraltete Zeit**

  Der Zeitpunkt, zu dem der Status des Ereignisses „Veraltet“ wurde.

Seite mit Veranstaltungsdetails

Auf der Seite „Ereignisdetails“ können Sie die Details eines ausgewählten Ereignisses anzeigen, z. B. den Schweregrad des Ereignisses, die Auswirkungsstufe, den Auswirkungsbereich und die Ereignisquelle. Sie können auch zusätzliche Informationen zu möglichen Abhilfemaßnahmen zur Behebung des Problems anzeigen.

- **Veranstaltungsname**

  Der Name des Ereignisses und die Uhrzeit, zu der das Ereignis zuletzt gesehen wurde.

  Bei Nichtleistungsereignissen sind die zuletzt angezeigten Informationen nicht bekannt, solange sich das Ereignis im Status „Neu“ oder „Bestätigt“ befindet, und werden daher ausgeblendet.

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung des Ereignisses.

  In einigen Fällen wird in der Ereignisbeschreibung ein Grund für die Auslösung des Ereignisses angegeben.

- **Umstrittene Komponente**

Bei dynamischen Leistungsereignissen werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente umstritten ist, wird ihr Symbol eingekreist und rot hervorgehoben.

Eine Beschreibung der hier angezeigten Komponenten finden Sie unter *Clusterkomponenten und warum sie miteinander in Konflikt geraten können*.

Die Abschnitte „Ereignisinformationen“, „Systemdiagnose“ und „Vorgeschlagene Maßnahmen“ werden in anderen Themen beschrieben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizensymbol**

  Ermöglicht Ihnen, eine Notiz zum Ereignis hinzuzufügen oder zu aktualisieren und alle von anderen Benutzern hinterlassenen Notizen zu überprüfen.

Aktionsmenü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Besitzer zuweisen“, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Name des Benutzers und die Uhrzeit der Ereigniszuweisung in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Eigentümerfeld leer lassen.

- **Anerkennen**

  Bestätigt die ausgewählten Ereignisse, sodass Sie nicht weiterhin wiederholt Warnbenachrichtigungen erhalten.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der Sie das Ereignis bestätigt haben, der Ereignisliste (Bestätigt von) für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für die Verwaltung dieses Ereignisses.

- **Als gelöst markieren**

  Ermöglicht Ihnen, den Ereignisstatus in „Gelöst“ zu ändern.

  Wenn Sie ein Ereignis lösen, werden Ihr Benutzername und der Zeitpunkt der Lösung des Ereignisses in der Ereignisliste (Gelöst von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Benachrichtigung hinzufügen**

  Zeigt das Dialogfeld „Warnung hinzufügen“ an, in dem Sie eine Warnung für das ausgewählte Ereignis

hinzufügen können.

Was im Abschnitt „Ereignisinformationen“ angezeigt wird

Im Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ können Sie die Details zu einem ausgewählten Ereignis anzeigen, z. B. den Schweregrad des Ereignisses, die Auswirkungsstufe, den Auswirkungsbereich und die Ereignisquelle.

Felder, die für den Ereignistyp nicht relevant sind, werden ausgeblendet. Sie können die folgenden Ereignisdetails anzeigen:

- **Ereignisauslösezeit**

  Der Zeitpunkt, zu dem das Ereignis generiert wurde.

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Gelöst oder Veraltet.

- **Veraltete Ursache**

  Die Aktionen, die dazu geführt haben, dass das Ereignis veraltet ist, z. B. wurde das Problem behoben.

- **Veranstaltungsdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen ist dies die Zeit zwischen der Erkennung und dem Zeitpunkt der letzten Analyse des Ereignisses. Bei veralteten Ereignissen ist dies die Zeit zwischen der Erkennung und der Lösung des Ereignisses.

  Dieses Feld wird für alle Leistungsereignisse und für andere Ereignistypen nur angezeigt, nachdem sie gelöst oder veraltet wurden.

- **Zuletzt gesehen**

  Das Datum und die Uhrzeit, zu der das Ereignis zuletzt als aktiv angesehen wurde.

  Bei Leistungsereignissen kann dieser Wert aktueller sein als die Ereignisauslösezeit, da dieses Feld nach jeder neuen Erfassung von Leistungsdaten aktualisiert wird, solange das Ereignis aktiv ist. Bei anderen Ereignistypen wird dieser Inhalt im Status „Neu“ oder „Bestätigt“ nicht aktualisiert und das Feld ist daher ausgeblendet.

- **Schwere**

  Der Schweregrad des Ereignisses: Kritisch ( ), Fehler ( ), Warnung ( ) und Informationen ( ).

- **Auswirkungsebene**

  Die Auswirkungsstufe des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Auswirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Leistung, Schutz, Konfiguration oder Sicherheit.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist.

  Beim Anzeigen der Details für ein freigegebenes QoS-Richtlinienereignis werden in diesem Feld bis zu drei der Workload-Objekte aufgelistet, die die meisten IOPS oder MBps verbrauchen.

  Sie können auf den Link zum Quellennamen klicken, um die Seite mit den Integritäts- oder Leistungsdetails für dieses Objekt anzuzeigen.

- **Quellenanmerkungen**

  Zeigt den Namen und Wert der Anmerkung für das Objekt an, mit dem das Ereignis verknüpft ist.

  Dieses Feld wird nur für Integritätsereignisse auf Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, zu denen das betroffene Objekt gehört.

  Dieses Feld wird nur für Integritätsereignisse auf Clustern, SVMs und Volumes angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. SVM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- **Auf Cluster**

  Der Name des Clusters, auf dem das Ereignis aufgetreten ist.

  Sie können auf den Link zum Clusternamen klicken, um die Seite mit den Integritäts- oder Leistungsdetails für diesen Cluster anzuzeigen.

- **Anzahl der betroffenen Objekte**

  Die Anzahl der vom Ereignis betroffenen Objekte.

  Sie können auf den Objektlink klicken, um die Inventarseite mit den Objekten anzuzeigen, die derzeit von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Leistungsereignisse angezeigt.

- **Betroffene Bände**

  Die Anzahl der Datenträger, die von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Leistungsereignisse auf Knoten oder Aggregaten angezeigt.

- **Ausgelöste Richtlinie**

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgelöst hat.

  Sie können den Cursor über den Richtliniennamen bewegen, um die Details der Schwellenwertrichtlinie anzuzeigen. Bei adaptiven QoS-Richtlinien werden auch die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener Speicherplatz oder verwendeter Speicherplatz) angezeigt.

Dieses Feld wird nur für Leistungsereignisse angezeigt.

- **Regel-ID**

  Bei Active IQ -Plattformereignissen ist dies die Nummer der Regel, die zum Generieren des Ereignisses ausgelöst wurde.

- **Bestätigt von**

  Der Name der Person, die das Ereignis bestätigt hat, und der Zeitpunkt der Bestätigung des Ereignisses.

- **Gelöst von**

  Der Name der Person, die das Ereignis gelöst hat, und der Zeitpunkt der Lösung des Ereignisses.

- **Zugewiesen an**

  Der Name der Person, die mit der Arbeit an der Veranstaltung beauftragt ist.

- **Alarmeinstellungen**

  Die folgenden Informationen zu Warnungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnungen zugeordnet sind, wird der Link **Warnung hinzufügen** angezeigt.

    Sie können das Dialogfeld „Warnung hinzufügen“ öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis eine Warnung zugeordnet ist, wird der Name der Warnung angezeigt.

    Sie können das Dialogfeld „Warnung bearbeiten“ öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis mehr als eine Warnung zugeordnet ist, wird die Anzahl der Warnungen angezeigt.

    Sie können die Seite „Alarm-Setup“ öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Alarmen anzuzeigen.

  Deaktivierte Warnungen werden nicht angezeigt.

- **Letzte Benachrichtigung gesendet**

  Datum und Uhrzeit der letzten Warnmeldung.

- **Senden per**

  Der Mechanismus, der zum Senden der Alarmbenachrichtigung verwendet wurde: E-Mail oder SNMP-Trap.

- **Vorheriger Skriptlauf**

  Der Name des Skripts, das beim Generieren der Warnung ausgeführt wurde.

Was im Abschnitt „Vorgeschlagene Aktionen“ angezeigt wird

Der Abschnitt „Vorgeschlagene Maßnahmen“ auf der Seite mit den Ereignisdetails enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu beheben. Die vorgeschlagenen Maßnahmen werden je nach Art des Ereignisses oder der Art des überschrittenen Schwellenwerts individuell angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen werden auf der Seite **Hilfe**-Links bereitgestellt, die auf zusätzliche Informationen zu vielen vorgeschlagenen Aktionen verweisen, einschließlich Anweisungen zum Ausführen einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools beinhalten.

Sie sollten die hier vorgeschlagenen Maßnahmen lediglich als Anleitung zur Lösung dieses Ereignisses betrachten. Die Maßnahmen, die Sie zur Lösung dieses Ereignisses ergreifen, sollten auf dem Kontext Ihrer Umgebung basieren.

Wenn Sie das Objekt und das Ereignis detaillierter analysieren möchten, klicken Sie auf die Schaltfläche **Arbeitslast analysieren**, um die Seite „Arbeitslastanalyse“ anzuzeigen.

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen mit der Schaltfläche **Fix It** angezeigt. Klicken Sie auf diese Schaltfläche, damit Unified Manager das Problem behebt, das das Ereignis verursacht.

Bei Active IQ -Plattformereignissen kann dieser Abschnitt einen Link zu einem NetApp Knowledgebase-Artikel enthalten, sofern verfügbar, der das Problem und mögliche Lösungen beschreibt. An Standorten ohne externen Netzwerkzugriff wird lokal eine PDF-Datei des Knowledgebase-Artikels geöffnet. Die PDF-Datei ist Teil der Regeldatei, die Sie manuell auf die Unified Manager-Instanz herunterladen.

Was der Abschnitt „Systemdiagnose“ anzeigt

Der Abschnitt „Systemdiagnose“ auf der Seite „Ereignisdetails“ enthält Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur bei manchen Veranstaltungen angezeigt.

Einige Leistungsereignisse stellen Diagramme bereit, die für das jeweilige ausgelöste Ereignis relevant sind. Normalerweise umfasst dies ein IOPS- oder MBps-Diagramm und ein Latenzdiagramm für die letzten zehn Tage. Bei dieser Anordnung können Sie sehen, welche Speicherkomponenten die Latenz am stärksten beeinflussen oder von der Latenz betroffen sind, wenn das Ereignis aktiv ist.

Für dynamische Leistungsereignisse werden die folgenden Diagramme angezeigt:

- Arbeitslastlatenz – Zeigt den Verlauf der Latenz für die Arbeitslasten der Top-Opfer, Bullys oder Sharks bei der umstrittenen Komponente an.
- Workload-Aktivität – Zeigt Details zur Workload-Nutzung der konkurrierenden Clusterkomponente an.
- Ressourcenaktivität – Zeigen Sie historische Leistungsstatistiken für die umstrittene Clusterkomponente an.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten miteinander konkurrieren.

Andere Ereignisse liefern eine kurze Beschreibung der Art der Analyse, die das System am Speicherobjekt durchführt. In einigen Fällen gibt es eine oder mehrere Zeilen, eine für jede analysierte Komponente, für systemdefinierte Leistungsrichtlinien, die mehrere Leistungsindikatoren analysieren. In diesem Szenario wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob bei dieser bestimmten Diagnose ein Problem gefunden wurde oder nicht.

Seite „Ereigniseinrichtung“

Auf der Seite „Ereigniseinrichtung“ wird die Liste der deaktivierten Ereignisse angezeigt und es werden Informationen wie der zugehörige Objekttyp und der Schweregrad des Ereignisses bereitgestellt. Sie können auch Aufgaben wie das globale Deaktivieren oder Aktivieren von Ereignissen ausführen.

Sie können auf diese Seite nur zugreifen, wenn Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für ausgewählte Ereignisse die folgenden Aufgaben ausführen:

- **Deaktivieren**

  Öffnet das Dialogfeld „Ereignisse deaktivieren“, in dem Sie Ereignisse deaktivieren können.

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **Upload-Regeln**

  Öffnet das Dialogfeld „Regeln hochladen“, das es Sites ohne externen Netzwerkzugriff ermöglicht, die Active IQ Regeldatei manuell in Unified Manager hochzuladen. Die Regeln werden für Cluster-AutoSupport -Nachrichten ausgeführt, um Ereignisse für Systemkonfiguration, Verkabelung, Best Practice und Verfügbarkeit zu generieren, wie von der Active IQ Plattform definiert.

- **EMS-Events abonnieren**

  Startet das Dialogfeld „EMS-Ereignisse abonnieren“, in dem Sie den Empfang bestimmter Event Management System (EMS)-Ereignisse von den Clustern abonnieren können, die Sie überwachen. Das EMS sammelt Informationen zu Ereignissen, die im Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis eingeht, wird ein Unified Manager-Ereignis mit dem entsprechenden Schweregrad generiert.

Listenansicht

In der Listenansicht werden (in Tabellenform) Informationen zu deaktivierten Ereignissen angezeigt. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen.

- **Ereignis**

  Zeigt den Namen des deaktivierten Ereignisses an.

- **Schwere**

Zeigt den Schweregrad des Ereignisses an. Der Schweregrad kann „Kritisch“, „Fehler“, „Warnung“ oder „Information“ sein.

- **Quellentyp**

  Zeigt den Quelltyp an, für den das Ereignis generiert wird.

Dialogfeld „Ereignisse deaktivieren“

Im Dialogfeld „Ereignisse deaktivieren“ wird die Liste der Ereignistypen angezeigt, für die Sie Ereignisse deaktivieren können. Sie können Ereignisse für einen Ereignistyp basierend auf einem bestimmten Schweregrad oder für eine Reihe von Ereignissen deaktivieren.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Bereich „Ereigniseigenschaften“

Im Bereich „Ereigniseigenschaften“ werden die folgenden Ereigniseigenschaften angegeben:

- **Ereignisschwere**

  Ermöglicht Ihnen die Auswahl von Ereignissen basierend auf dem Schweregradtyp, der „Kritisch“, „Fehler“, „Warnung“ oder „Information“ sein kann.

- **Ereignisname enthält**

  Ermöglicht Ihnen, Ereignisse zu filtern, deren Name die angegebenen Zeichen enthält.

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem Schweregrad des Ereignisses und der von Ihnen angegebenen Textzeichenfolge entsprechen.

- **Ereignisse deaktivieren**

  Zeigt die Liste der Ereignisse an, die Sie zum Deaktivieren ausgewählt haben.

  Neben dem Ereignisnamen wird auch der Schweregrad des Ereignisses angezeigt.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für die ausgewählten Ereignisse die folgenden Aufgaben ausführen:

- **Speichern und schließen**

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.