Verwalten von Ereignissen und Warnmeldungen

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/events/concept_what_active_iq_platform_events_are.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Verwalten von Ereignissen und Warnmeldungen . . . 1
Ereignisse managen . . . 1
Informationen zu Active IQ Plattformereignissen in Active IQ Unified Manager . . . 1
Was Event Management System Ereignisse sind . . . 1
Hier wird erläutert, wie Active IQ Unified Manager ein empfangenes Ereignis verarbeitet . . . 6
Ereignisdetails in Active IQ Unified Manager . . . 7
Nicht zugewiesene Ereignisse in Active IQ Unified Manager . . . 8
Bestätigen und Beheben von Ereignissen in Active IQ Unified Manager . . . 8
Zuweisung von Ereignissen an bestimmte Benutzer in Active IQ Unified Manager . . . 9
Unerwünschte Ereignisse in Active IQ Unified Manager deaktivieren . . . 10
Probleme lassen sich mithilfe der automatischen Fehlerbehebung in Active IQ Unified Manager beheben . . . 11
Aktivieren und Deaktivieren der Active IQ Ereignisberichterstattung in Active IQ Unified Manager . . . 12
Hochladen einer neuen Active IQ Regeldatei in Active IQ Unified Manager . . . 13
Wie Active IQ Unified Manager Active IQ-Plattformereignisse generiert . . . 14
Active IQ Plattformereignisse in Active IQ Unified Manager beheben . . . 14
Konfiguration der Einstellungen zur Ereignisaufbewahrung in Active IQ Unified Manager . . . 15
Was ein Wartungsfenster für Unified Manager ist . . . 15
Verwalten von Hostsystemressourcenereignissen in Active IQ Unified Manager . . . 18
Mehr über Ereignisse . . . 18
Liste der Ereignisse und Schweregrade . . . 24
Beschreibung von Ereignisfenstern und Dialogfeldern . . . 76
Benachrichtigungen verwalten . . . 89
Informationen zu Warnmeldungen in Active IQ Unified Manager . . . 89
Informationen in einer Active IQ Unified Manager Benachrichtigungs-E-Mail . . . 89
Benachrichtigungen hinzufügen . . . 90
Hinzufügen von Warnmeldungen für Leistungsereignisse in Active IQ Unified Manager . . . 93
Warnungen in Active IQ Unified Manager testen . . . 94
Benachrichtigungen für gelöste und veraltete Ereignisse in Active IQ Unified Manager deaktivieren . . . 95
Ausschluss von Ziel-Volumes für die Notfallwiederherstellung von der Generierung von Warnmeldungen in Active IQ Unified Manager . . . 95
Anzeigen von Warnmeldungen in Active IQ Unified Manager . . . 96
Benachrichtigungen in Active IQ Unified Manager bearbeiten . . . 96
Warnmeldungen in Active IQ Unified Manager löschen . . . 97
Beschreibung von Warnfenstern und Dialogfeldern . . . 97
Skripte managen . . . 103
Skripte in Active IQ Unified Manager verwalten . . . 103
Wie Skripte mit Warnmeldungen in Active IQ Unified Manager funktionieren . . . 104
Skripte in Active IQ Unified Manager hinzufügen . . . 105
Skripte in Active IQ Unified Manager löschen . . . 106
Ausführung des Testskripts in Active IQ Unified Manager . . . 106
Informationen zu den unterstützten Active IQ Unified Manager CLI Befehlen . . . 107
Beschreibung der Skriptfenster und Dialogfelder . . . 112

Verwalten von Ereignissen und Warnmeldungen

Ereignisse managen

Informationen zu Active IQ Plattformereignissen in Active IQ Unified Manager

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden durch die Anwendung einer Reihe von Regeln auf AutoSupport Meldungen erstellt, die von allen von Unified Manager überwachten Storage-Systemen generiert werden.

Weitere Informationen sind unter "Wie Plattformereignisse von Active IQ generiert werden" verfügbar.

Unified Manager prüft automatisch, ob eine neue Regeldatei vorhanden ist, und lädt eine neue Datei nur dann herunter, wenn neuere Regeln verfügbar sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Storage Management** > **Event Setup** > **Upload Rules** hochladen.

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

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

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

Was Event Management System Ereignisse sind

Informationen zu Ereignissen des Event Management System in Active IQ Unified Manager

Das Event Management System (EMS) erfasst Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und stellt Mechanismen zur Ereignisweiterleitung bereit. Diese ONTAP Ereignisse können im Unified Manager als EMS Ereignisse gemeldet werden. Die zentrale Überwachung und Verwaltung vereinfacht die Konfiguration kritischer EMS Ereignisse und Warnbenachrichtigungen auf der Grundlage dieser EMS Ereignisse.

Beim Hinzufügen des Clusters zu Unified Manager wird dem Cluster die Unified Manager-Adresse als Benachrichtigungsziel hinzugefügt. Ein EMS-Ereignis wird gemeldet, sobald es im Cluster auftritt.

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

- Eine bestimmte Anzahl wichtiger EMS Ereignisse wird automatisch gemeldet.
- Sie können einzelne 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 Meldungen	Abonnierte EMS-Nachrichten
Verfügbare EMS-Ereignisse	Teilmenge der EMS-Ereignisse	Alle EMS-Ereignisse
Name der EMS-Meldung bei Auslösung	Unified Manager Ereignisname (konvertiert aus dem EMS Ereignisnamen)	Unspezifisch im Format "Error EMS received". Die detaillierte Meldung enthält die Punktnotation des tatsächlichen EMS-Ereignisses.
Empfangene Nachrichten	Sobald der Cluster erkannt 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“, „Behoben“ und „Veraltet“	Das EMS-Ereignis ist nach der Aktualisierung des Clusters, 15 Minuten nach seiner Erstellung, obsolet
Erfasst Ereignisse während der Ausfallzeit von Unified Manager	Ja, beim Systemstart kommuniziert das System mit jedem Cluster, um fehlende Ereignisse abzurufen	Nein
Ereignisdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um einheitliche Lösungen zu gewährleisten.	Korrekturmaßnahmen sind auf der Seite „Ereignisdetails“ nicht verfügbar

Einige der neuen automatischen EMS-Ereignisse sind Informationsereignisse, die anzeigen, dass ein vorheriges Ereignis behoben wurde. Beispielsweise zeigt das Informationsereignis "FlexGroup Constituents Space Status All OK" an, dass das Fehlerereignis "FlexGroup Constituents Have Space Issues" behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus verwaltet werden wie andere Ereignisse nach Typ des Schweregrads; das Ereignis wird jedoch automatisch als veraltet markiert, wenn dasselbe Volume ein weiteres Fehlerereignis “Space Issues” erhält.

EMS-Ereignisse, die automatisch zu Active IQ 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 verfügbar, auf denen ONTAP 9.5 oder höher ausgeführt wird:

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Zugriff auf die Cloud-Ebene für die Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Zugriff auf Cloud Tier bei Aggregatverlagerung während Storage Failover verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
FabricPool Spiegelreplikations-Resynchronisierung abgeschlossen	wafl.ca.resync.complete	Cluster	Fehler
FabricPool Speicherplatz fast voll	fabricpool.nearly.full	Cluster	Fehler
NVMe-oF Schonfrist gestartet	nvmf.graceperiod.start	Cluster	Warnung
NVMe-oF Kulanzfrist aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-oF Kulanzfrist abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN zerstört	lun.destroy	LUN	Informationen
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Node	Fehler
Cloud AWS IAMCredsExpired	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	Informationen
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Node	Fehler
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
Anfrage stimmt nicht mit der Cloud-Tier-Signatur überein	osc.signatureMismatch	Node	Fehler
Einer der NFSv4 Pools ist erschöpft	Nblade.nfsV4PoolExhaust	Node	Kritisch
QoS Monitor Speicher maximal belegt	qos.monitor.memory.maxed	Node	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
QoS Monitor-Speicher reduziert	qos.monitor.memory.abated	Node	Informationen
NVMeNS zerstören	NVMeNS.destroy	Namensraum	Informationen
NVMeNS Online	NVMeNS.offline	Namensraum	Informationen
NVMeNS offline	NVMeNS.online	Namensraum	Informationen
NVMeNS hat keinen Speicherplatz mehr	NVMeNS.out.of.space	Namensraum	Warnung
Synchrone Replikation nicht synchron	sms.status.out.of.sync	SnapMirror Beziehung	Warnung
Synchrone Replikation wiederhergestellt	sms.status.in.sync	SnapMirror Beziehung	Informationen
Automatische Resynchronisierung der synchronen Replikation fehlgeschlagen	sms.resync.attempt.failed	SnapMirror Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler
Maximale Anzahl an CIFS-Verbindungen 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 zum Verbinden einer nicht vorhandenen CIFS-Freigabe	Nblade.cifsNoPrivShare	SVM	Kritisch
CIFS Shadow Copy Operation fehlgeschlagen	cifs.shadowcopy.failure	SVM	Fehler
Virus vom AV Server erkannt	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Serververbindung für Virenscan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine Verbindung zu einem antwortenden AV-Server	Nblade.vscanConnInactive	SVM	Informationen
AV Server ist zu ausgelastet, um neue Scan-Anfragen anzunehmen	Nblade.vscanConnBackPressure	SVM	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Unbefugter Benutzer versucht, auf den AV Server zuzugreifen	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup Bestandteile haben Platzprobleme.	flexgroup.constituents.have.space.issues	Volumen	Fehler
FlexGroup Status des Speicherplatzes der Bestandteile, alles OK	flexgroup.constituents.space.status.all.ok	Volumen	Informationen
FlexGroup Bestandteile haben Inode-Probleme	flexgroup.constituents.have.inodes.issues	Volumen	Fehler
FlexGroup Konstituenten Inode-Status alle OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Informationen
Logischer Speicherplatz des Volume nahezu voll	monitor.vol.nearFull.inc.sav	Volumen	Warnung
Logischer Speicherplatz des Volume voll	monitor.vol.full.inc.sav	Volumen	Fehler
Normaler logischer Speicherplatz des Volume	monitor.vol.one.ok.inc.sav	Volumen	Informationen
WAFL Volume AutoSize Fehler	wafl.vol.autoSize.fail	Volumen	Fehler
WAFL Volume AutoSize abgeschlossen	wafl.vol.autoSize.done	Volumen	Informationen
Timeout der WAFL READDIR Dateioperation	wafl.readdir.expired	Volumen	Fehler

Abonnement von ONTAP EMS Ereignissen in Active IQ Unified Manager

Sie können Ereignisse des Event Management System (EMS) abonnieren, die von Systemen generiert werden, auf denen ONTAP Software installiert ist. Ein Teil der EMS-Ereignisse wird automatisch an Unified Manager gemeldet, weitere EMS-Ereignisse jedoch nur, wenn Sie diese Ereignisse abonniert haben.

Bevor Sie beginnen

Ein Abonnement von EMS-Ereignissen, die Unified Manager bereits automatisch hinzufügt, sollte vermieden werden, da der Empfang von zwei Ereignissen für dasselbe Problem zu Verwirrung führen kann.

Sie können eine beliebige Anzahl von EMS-Ereignissen 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* enthält detaillierte Informationen zu allen EMS-Meldungen für die angegebene Version der ONTAP 9 Software. Die entsprechende Version des *EMS-Ereigniskatalogs* mit einer Liste der anwendbaren Ereignisse ist auf der Seite zur ONTAP 9 Produktdokumentation verfügbar.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die ONTAP EMS-Ereignisse konfigurieren, die Sie abonniert haben, und

benutzerdefinierte Skripte erstellen, die bei diesen Ereignissen ausgeführt werden.

> Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, nicht erhalten, liegt möglicherweise ein Problem mit der DNS-Konfiguration des Clusters vor, das verhindert, dass das Cluster den Unified Manager-Server erreicht. Zur Behebung dieses Problems muss der Clusteradministrator die DNS-Konfiguration des Clusters korrigieren und anschließend Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server weitergeleitet.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite „Event Setup“ erfolgt die Auswahl der Schaltfläche **Subscribe to EMS events**.
3. Im Dialogfeld „EMS-Ereignisse abonnieren“ geben Sie den Namen des ONTAP EMS-Ereignisses ein, das Sie abonnieren möchten.

   In der ONTAP Cluster-Shell lässt sich zum Anzeigen der Namen der EMS-Ereignisse, die Sie abonnieren können, der `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher) verwenden.

   "Konfiguration und Empfang von Warnmeldungen aus ONTAP EMS Event Subscription in Active IQ Unified Manager"

4. Klicken Sie auf **Add**.

   Das hinzugefügte EMS-Ereignis wird in der Liste der abonnierten EMS-Ereignisse aufgeführt, in der Spalte "Gilt für Cluster" wird jedoch der Status “Unknown” angezeigt.

5. Durch Klicken auf **Save and Close** wird das EMS-Ereignisabonnement beim Cluster registriert.
6. **EMS-Ereignisse abonnieren** erneut auswählen.

   In der Spalte „Gilt für Cluster“ erscheint für das von Ihnen hinzugefügte EMS-Ereignis der Status „`Ja`“.

   Wenn der Status nicht „`Yes`“ lautet, ist die Schreibweise des ONTAP EMS Ereignisnamens zu prüfen. Wenn der Name falsch eingegeben wurde, muss das betreffende Ereignis entfernt und anschließend erneut hinzugefügt werden.

Wenn das ONTAP EMS-Ereignis auftritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um auf der Seite „Ereignisdetails“ Details zum EMS-Ereignis anzuzeigen. Sie können außerdem den Status des Ereignisses managen oder Benachrichtigungen für das Ereignis erstellen.

Hier wird erläutert, wie Active IQ Unified Manager ein empfangenes Ereignis verarbeitet

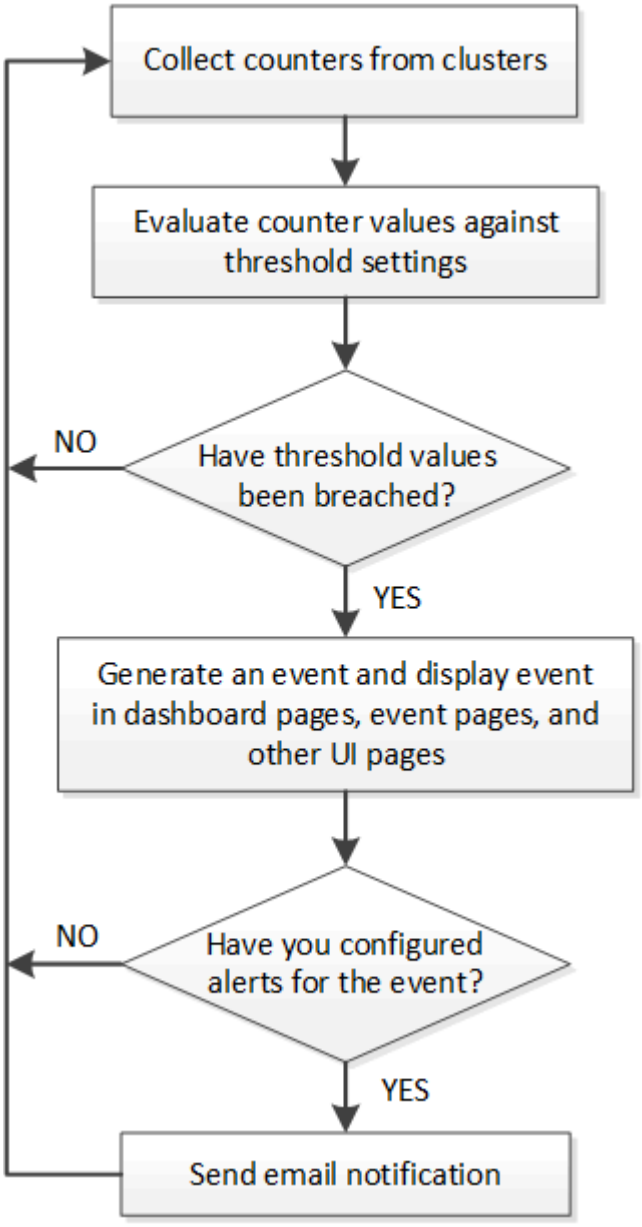
Wenn Unified Manager ein Ereignis empfängt, erscheint es auf der Dashboard-Seite, auf der Inventarseite „Event Management“, auf den Registerkarten „Summary“ und „Explorer“ der Seite „Cluster/Performance“ sowie auf der objektspezifischen Inventarseite (z. B. der Inventarseite „Volumes/Health“).

Wenn Unified Manager mehrere aufeinanderfolgende Vorkommen desselben Ereigniszustands für dieselbe Clusterkomponente erkennt, behandelt er alle Vorkommen als ein einziges Ereignis und nicht als separate Ereignisse. Die Dauer des Ereignisses erhöht sich, um anzuzeigen, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie die Einstellungen auf der Seite „Benachrichtigungseinrichtung“ konfigurieren, können Sie andere Benutzer über diese Ereignisse benachrichtigen. Die Benachrichtigung löst folgende Aktionen aus:

- Eine E-Mail über das Ereignis kann an alle Benutzer mit der Rolle Unified Manager Administrator gesendet werden.
- Das Ereignis kann an zusätzliche E-Mail-Empfänger gesendet werden.
- Ein SNMP Trap lässt sich an den Trap-Empfänger senden.
- Mit einem benutzerdefinierten Skript lässt sich eine Aktion ausführen.

Das folgende Diagramm zeigt diesen Arbeitsablauf.



Ereignisdetails in Active IQ Unified Manager

Sie können Details zu einem Ereignis anzeigen, das Unified Manager auslöst, damit Korrekturmaßnahmen ergriffen werden können. Wenn beispielsweise das Systemstatusereignis Volume Offline vorliegt, können Sie auf dieses Ereignis klicken, um

die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

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

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   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 „Incident“ oder „Risiko“ aufweisen.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen, z. B. Kapazitätsereignisse oder Performance Ereignisse, anzeigen möchten, können Sie auf **View** klicken und im Menü der Ereignistypen eine Auswahl treffen.
3. Details lassen sich anzeigen, indem der Name des entsprechenden Ereignisses ausgewählt wird.

   Die Ereignisdetails werden auf der Seite „Ereignisdetails“ angezeigt.

Nicht zugewiesene Ereignisse in Active IQ Unified Manager

Sie können nicht zugewiesene Ereignisse anzeigen und jedes einzelne einem Benutzer zuweisen, der es beheben kann.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig zeigt die Inventarseite „Event Management“ neue und bestätigte Ereignisse an.

2. Im Bereich **Filter** erfolgt die Auswahl der Filteroption **Nicht zugewiesen** im Abschnitt **Zugewiesen an**.

Bestätigen und Beheben von Ereignissen in Active IQ Unified Manager

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Bearbeitung des Problems beginnen, durch das das Ereignis ausgelöst wurde, damit Sie nicht weiterhin wiederholte Alarmbenachrichtigungen erhalten. Nachdem Sie für ein bestimmtes Ereignis eine Korrekturmaßnahme durchgeführt haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Information Ereignisse können nicht quittiert werden.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. In der Ereignisliste stehen zum Bestätigen der Ereignisse die folgenden Aktionen zur Verfügung:

Wenn Sie möchten…	Folgendes ist zu tun…
Ein einzelnes Ereignis bestätigen und als gelöst markieren	a. Den Ereignisnamen auswählen. b. Auf der Seite mit den Ereignisdetails lässt sich die Ursache des Ereignisses ermitteln. c. Auf **Bestätigen** klicken. d. Eine geeignete Korrekturmaßnahme ist einzuleiten. e. Anschließend **Als gelöst markieren** auswählen.
Bestätigung und Kennzeichnung mehrerer Ereignisse als gelöst	a. Die Ermittlung der Ursache der Ereignisse erfolgt auf der jeweiligen Ereignisdetailseite. b. Auswählen der Ereignisse. c. Auf **Bestätigen** klicken. d. Es sind geeignete Korrekturmaßnahmen einzuleiten. e. Anschließend **Als gelöst markieren** auswählen.

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

3. **Optional**: Im Bereich **Notizen und Aktualisierungen** lässt sich eine Notiz dazu hinzufügen, wie das Ereignis behandelt wurde; anschließend kann auf **Post** geklickt werden.

Zuweisung von Ereignissen an bestimmte Benutzer in Active IQ Unified Manager

Sie können nicht zugewiesene Ereignisse sich selbst oder anderen Benutzern, einschließlich Remote-Benutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer neu zuweisen. Wenn beispielsweise bei einem Storage Objekt 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-Adresse des Benutzers müssen korrekt konfiguriert sein.
- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Auf der Inventarseite **Event Management** erfolgt die Auswahl eines oder mehrerer Events, die zugewiesen werden sollen.
3. Die Zuweisung des Ereignisses erfolgt durch Auswahl einer der folgenden Optionen:

Wenn das Ereignis zugewiesen werden soll …	Fahren Sie dann wie folgt fort…
Sie selbst	Anschließend erfolgt die Auswahl von **Zuweisen an** > **Mich**.
Ein anderer Benutzer	a. Die Auswahl erfolgt über **Zuweisen an** > **Anderer Benutzer**. b. Im Dialogfeld „Besitzer zuweisen“ können Sie den Benutzernamen eingeben oder einen Benutzer aus der Dropdown-Liste auswählen. c. **Zuweisen** auswählen. Der Benutzer erhält eine E-Mail-Benachrichtigung. Wenn Sie keinen Benutzernamen eingeben oder keinen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt das Ereignis nicht zugewiesen.

Unerwünschte Ereignisse in Active IQ Unified Manager deaktivieren

Alle Ereignisse sind standardmäßig aktiviert. Sie können Ereignisse global deaktivieren, um zu verhindern, dass Benachrichtigungen für Ereignisse generiert werden, die in Ihrer Umgebung nicht relevant sind. Sie können deaktivierte Ereignisse wieder aktivieren, wenn Sie wieder Benachrichtigungen darüber erhalten möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie Ereignisse deaktivieren, werden die zuvor im System generierten Ereignisse als veraltet markiert, und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse wieder 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 es später wieder aktivieren, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline waren, als das Ereignis deaktiviert war. Unified Manager generiert nur dann ein neues Ereignis, wenn sich der Objektstatus nach der Reaktivierung des Ereignisses ändert.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite **Event Setup** können Sie Ereignisse deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Im Dialogfeld „Ereignisse deaktivieren“ erfolgt die Auswahl des Schweregrads des Ereignisses. c. In der Spalte „Übereinstimmende Ereignisse“ sind die Ereignisse auszuwählen, die auf Grundlage des Schweregrads des Ereignisses deaktiviert werden sollen. Anschließend werden diese Ereignisse mit dem Pfeil nach rechts in die Spalte „Ereignisse deaktivieren“ verschoben. d. Anschließend erfolgt die Auswahl von **Save and Close**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Für das oder die zu aktivierenden Ereignisse ist das Kästchen auszuwählen. b. Klicken Sie auf **Enable**.

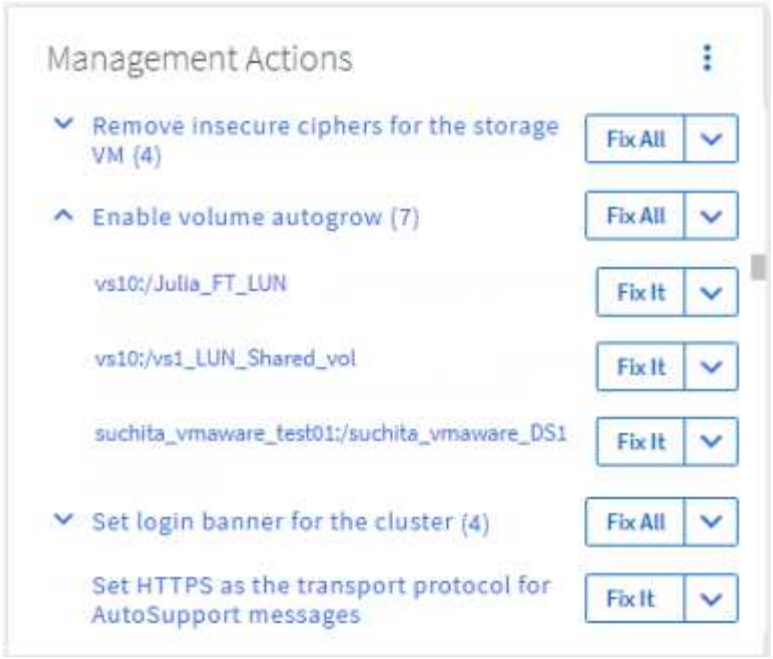
Probleme lassen sich mithilfe der automatischen Fehlerbehebung in Active IQ Unified Manager beheben

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

Die meisten Ereignisse bieten verschiedene Lösungsmöglichkeiten, die auf der Seite „Ereignisdetails“ angezeigt werden, sodass Sie die beste Lösung mit ONTAP System Manager oder der ONTAP CLI implementieren können. Die Aktion **Fix It** ist verfügbar, wenn Unified Manager festgestellt hat, dass es nur eine Lösung zur Behebung des Problems gibt und dass diese mit einem ONTAP CLI-Befehl implementiert werden kann.

Schritte

1. Ereignisse, die über das **Dashboard** behoben werden können, lassen sich durch Klicken auf **Dashboard** anzeigen.



2. Zum Beheben von Problemen, die Unified Manager lösen kann, dient die Schaltfläche **Fix It**. Zum Beheben eines Problems, das auf mehreren Objekten vorhanden ist, dient die Schaltfläche **Fix All**.

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

Aktivieren und Deaktivieren der Active IQ Ereignisberichterstattung in Active IQ Unified Manager

Ereignisse der Active IQ Plattform werden standardmäßig in der Benutzeroberfläche des Unified Manager generiert und angezeigt. Falls diese Ereignisse als zu häufig empfunden werden oder sie in Unified Manager nicht angezeigt werden sollen, kann ihre Generierung deaktiviert werden. Sie können sie später wieder aktivieren, wenn Sie diese Benachrichtigungen erneut erhalten möchten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie diese Funktion deaktivieren, empfängt Unified Manager sofort keine Ereignisse der Active IQ Plattform mehr.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager kurz nach Mitternacht, basierend auf der Zeitzone des Clusters, Active IQ Plattformereignisse zu empfangen. Der Startzeitpunkt richtet sich danach, wann Unified Manager AutoSupport Nachrichten von den einzelnen Clustern empfängt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Funktionseinstellungen** können Sie Active IQ Plattformereignisse deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Active IQ Plattformereignisse deaktivieren	Im Bereich **Active IQ Portal Events** den Schieberegler nach links verschieben.
Aktivieren von Active IQ Plattformereignissen	Im Bereich **Active IQ Portal Events** wird der Schieberegler nach rechts verschoben.

Hochladen einer neuen Active IQ Regeldatei in Active IQ Unified Manager

Unified Manager sucht automatisch nach einer neuen Active IQ-Ereignisdatei (Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln verfügbar sind. An Standorten ohne externen Netzwerkzugriff ist jedoch ein manuelles Hochladen der Regeldatei erforderlich.

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

Bei der Installation oder dem Upgrade von Unified Manager auf eine bestimmte Version an einem Standort ohne Netzwerkverbindung sind die mitgelieferten Active IQ-Regeln automatisch zum Upload verfügbar. 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 Storage Systeme weiterhin optimal funktionieren.

Bevor Sie beginnen

- Die Ereignisberichterstattung im Active IQ portal muss aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Informationen hierzu enthält "Aktivieren von Active IQ Portalereignissen".
- Sie müssen die Regeldatei von der NetApp Support Site herunterladen.

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

Schritte

1. Auf einem Computer mit Netzwerkzugriff können Sie die NetApp Support Site aufrufen und die aktuelle rules `.zip`-Datei herunterladen.

   Das mitgelieferte Regelpaket umfasst das Regel-Repository, Datenquellen und einen NetApp KB-Artikel.

   Auf Windows-Systemen an einem Standort ohne Netzwerkverbindung ist der NetApp KB-Artikel standardmäßig nicht im Installationsprogramm enthalten. Die Datei *secure_rules.zip* kann von der Support-Website heruntergeladen und hochgeladen werden, um den KB-Artikel für alle Regeln anzuzeigen.

2. Die Regeldatei wird auf ein Medium übertragen, das in den Sicherheitsbereich mitgenommen werden kann, und anschließend auf ein System im Sicherheitsbereich kopiert.
3. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
4. Auf der Seite **Event Setup** ist auf die Schaltfläche **Upload Rules** zu klicken.
5. Im Dialogfeld **Upload Rules** können Sie zu der Regel `.zip`datei navigieren, die Sie heruntergeladen haben, sie auswählen und auf **Upload** klicken.

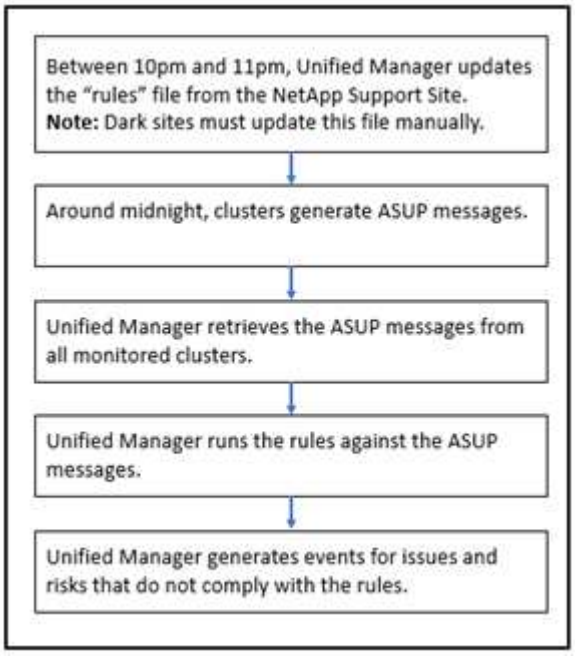
   Dieser Vorgang kann einige Minuten dauern.

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 Incident-Ereignisse.

Weitere Informationen enthält dieser Knowledge Base (KB)-Artikel: "Manuelles Aktualisieren von AIQCASecure-Regeln in Active IQ Unified Manager".

Wie Active IQ Unified Manager Active IQ-Plattformereignisse generiert

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

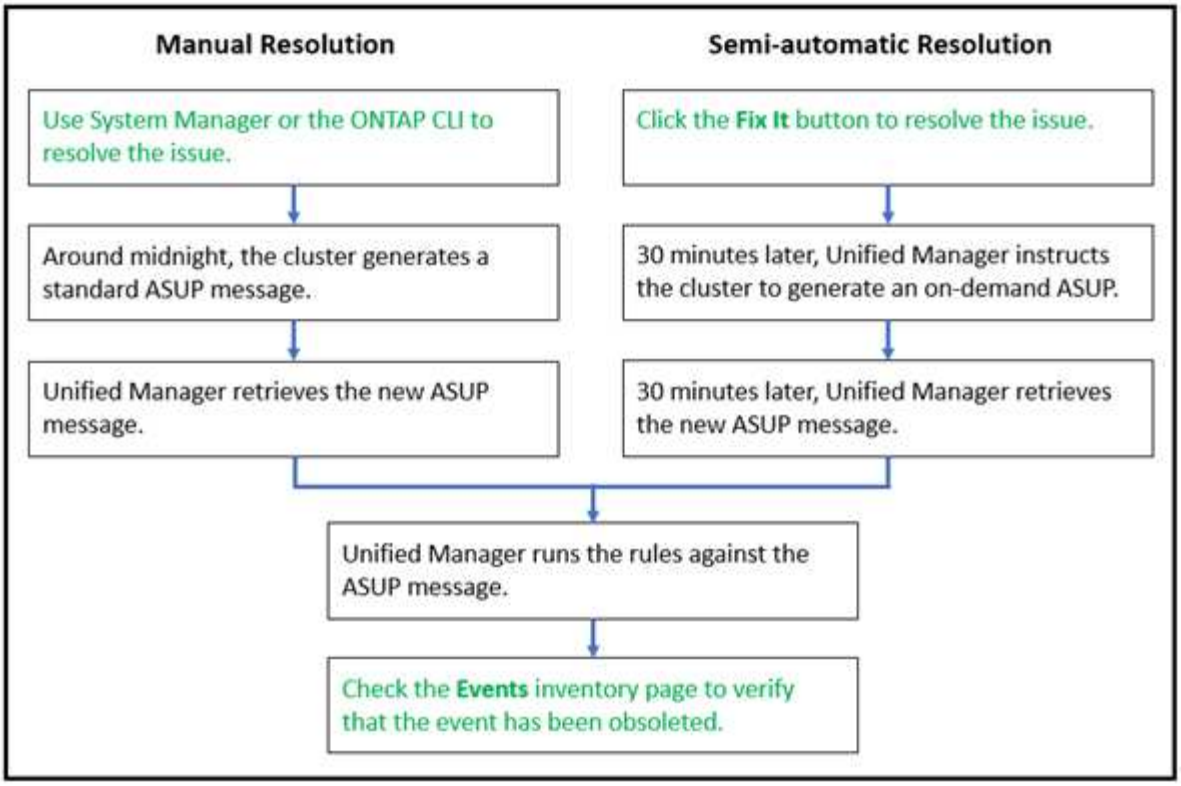


Wie Sie sehen können, wird die auf der Active IQ Plattform kompilierte Regeldatei stets aktuell gehalten, Cluster AutoSupport Meldungen werden täglich generiert, und Unified Manager aktualisiert die Liste der Ereignisse täglich.

Active IQ Plattformereignisse in Active IQ Unified Manager beheben

Vorfälle und Risiken der Active IQ Plattform ähneln anderen Unified Manager Ereignissen, da sie anderen Benutzern zur Behebung zugewiesen werden können und dieselben verfügbaren Status aufweisen. Wenn diese Ereignisse jedoch mit der Schaltfläche **Fix It** behoben werden, kann die Behebung innerhalb weniger Stunden überprüft werden.

Das folgende Diagramm zeigt die Maßnahmen, die Sie ergreifen müssen (grün), und die Maßnahmen, die Unified Manager ergreift (schwarz), wenn Ereignisse behoben werden, die von der Active IQ Plattform generiert wurden.



Bei einer manuellen Behebung müssen Sie sich bei System Manager oder der ONTAP Befehlszeilenschnittstelle anmelden, um das Problem zu beheben. Die Überprüfung des Problems ist erst möglich, nachdem der Cluster um Mitternacht eine neue AutoSupport Meldung generiert hat.

Bei einer halbautomatischen Behebung mithilfe der Schaltfläche **Fix It** können Sie innerhalb weniger Stunden überprüfen, ob die Behebung erfolgreich war.

Konfiguration der Einstellungen zur Ereignisaufbewahrung in Active IQ Unified Manager

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

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Das Speichern von Ereignissen über einen Zeitraum von mehr als 6 Monaten hinaus kann die Server Performance beeinträchtigen und wird daher nicht empfohlen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **General** > **Data Retention**.
2. Auf der Seite **Datenaufbewahrung** den Schieberegler im Bereich Ereignisaufbewahrung auf die Anzahl der Monate einstellen, für die Ereignisse aufbewahrt werden sollen, und anschließend auf **Speichern** klicken.

Was ein Wartungsfenster für Unified Manager ist

Informationen zu den Wartungsfenstern von Active IQ Unified Manager

Sie definieren ein Unified Manager Wartungsfenster, um Ereignisse und Warnmeldungen 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 von Event Management ein Ereignis mit dem Namen „Object Maintenance Window Started“ protokolliert. Dieses Ereignis wird automatisch als veraltet markiert, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden zwar weiterhin Ereignisse für alle Objekte in diesem Cluster generiert, sie werden jedoch auf keiner der UI Seiten angezeigt, und für diese Ereignisse werden keine Warnungen oder andere Arten von Benachrichtigungen gesendet. Die während eines Wartungsfensters für alle Storage Objekte generierten Ereignisse können jedoch angezeigt werden, indem auf der Bestandsseite „Ereignisverwaltung“ eine der Anzeigeoptionen ausgewählt wird.

Sie können ein Wartungsfenster so planen, dass es zu einem späteren Zeitpunkt gestartet wird, die Start- und Endzeiten für ein geplantes Wartungsfenster ändern und ein geplantes Wartungsfenster abbrechen.

Planen Sie ein Wartungsfenster, um Cluster-Ereignisbenachrichtigungen in Active IQ Unified Manager zu deaktivieren

Wenn Sie für einen Cluster eine geplante Ausfallzeit haben, beispielsweise für ein Cluster-Upgrade oder das Verschieben eines der Knoten, können Sie die Ereignisse und Warnungen, die normalerweise während dieses Zeitraums generiert würden, durch das Planen eines Wartungsfensters in Unified Manager unterdrücken.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

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

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

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster erfolgt die Auswahl der Schieberegler-Schaltfläche und das Verschieben nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Das Start- und Enddatum sowie die Uhrzeit für das Wartungsfenster können festgelegt werden; anschließend ist **Apply** auszuwählen.

   Neben dem Schieberegler erscheint die Meldung „Geplant“.

Wenn der Startzeitpunkt erreicht ist, wechselt der Cluster in den Wartungsmodus und es wird ein Ereignis mit dem Titel „Object Maintenance Window Started“ generiert.

Ändern oder Stornieren eines geplanten Wartungsfensters in Active IQ Unified Manager

Wenn Sie ein Unified Manager Wartungsfenster konfiguriert haben, das in der Zukunft stattfinden soll, können Sie die Start- und Endzeiten ändern oder das Stattfinden des Wartungsfensters abbrechen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

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

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Wenn Sie möchten…	Ausführung dieses Schritts…
Ändern des Zeitrahmens für ein geplantes Wartungsfenster	a. Neben dem Schieberegler befindet sich der Text „Geplant“. b. Start- und/oder Enddatum sowie -uhrzeit ändern und **Anwenden** auswählen.
Verlängerung der Dauer eines aktiven Wartungsfensters	a. Der Text „Active“ neben dem Schieberegler wird ausgewählt. b. Das Enddatum und die Endzeit werden geändert, und anschließend wird auf **Anwenden** geklickt.
Abbrechen eines geplanten Wartungsfensters	Der Schieberegler wird ausgewählt und nach links bewegt.
Abbrechen eines aktiven Wartungsfensters	Der Schieberegler wird ausgewählt und nach links bewegt.

Anzeigen von Ereignissen, die während eines Wartungsfensters in Active IQ Unified Manager generiert wurden

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse erscheinen nach Abschluss des Wartungsfensters und nachdem alle Systemressourcen wieder betriebsbereit sind im Status „Veraltet“.

Bevor Sie beginnen

Bevor Ereignisse verfügbar sind, muss mindestens ein Wartungsfenster abgeschlossen sein.

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

Schritte

1. Im linken Navigationsbereich ist **Ereignisse** zu wählen.

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

2. Im Ansichtsbereich kann die Option **Alle während der Wartung generierten Ereignisse** ausgewählt werden.

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

3. Falls für einen einzelnen Cluster mehrere Wartungsfenster stattgefunden haben, können Sie auf das Kalendersymbol **Triggered Time** klicken und den Zeitraum für die Ereignisse des Wartungsfensters auswählen, die Sie anzeigen möchten.

Verwalten von Hostsystemressourcenereignissen in Active IQ Unified Manager

Unified Manager enthält einen Dienst, der Ressourcenprobleme auf dem Hostsystem überwacht, auf dem Unified Manager installiert ist. Probleme wie unzureichender Speicherplatz oder Arbeitsspeicher auf dem Hostsystem können Ereignisse der Managementstation auslösen, die als Bannermeldungen am oberen Rand der Benutzeroberfläche angezeigt werden.

Ereignisse der Managementstation weisen auf ein Problem mit dem Hostsystem hin, auf dem Unified Manager installiert ist. Beispiele für Probleme mit der Managementstation sind geringer Speicherplatz auf dem Hostsystem, ein fehlender regulärer Datenerfassungszyklus von Unified Manager sowie eine nicht oder verspätet abgeschlossene Statistikanalyse, weil die nächste Datenerfassungsabfrage gestartet wurde.

Im Gegensatz zu allen anderen Unified Manager Ereignismeldungen erscheinen diese speziellen Warnungs- und kritischen Ereignisse der Managementstation als Bannermeldungen.

Schritt

1. Zum Anzeigen von Ereignisinformationen der Managementstation sind folgende Schritte erforderlich:

Wenn Sie möchten…	Folgendes ist zu tun…
Details des Ereignisses anzeigen	Durch Klicken auf das Ereignisbanner wird die Seite mit den Ereignisdetails angezeigt, die Lösungsvorschläge für das Problem enthält.
Alle Ereignisse der Managementstation anzeigen	a. Im linken Navigationsbereich auf **Event Management** klicken. b. Im Filterbereich auf der Inventarseite „Ereignisverwaltung“ befindet sich in der Liste „Quelltyp“ das Kästchen für „Verwaltungsstation“.

Mehr über Ereignisse

Ereigniszustände in Active IQ Unified Manager

Der Status eines Ereignisses hilft Ihnen festzustellen, ob eine geeignete Korrekturmaßnahme erforderlich ist. Ein Ereignis kann neu, bestätigt, gelöst oder veraltet sein. Dabei gilt, 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 Zustand eines Ereignisses, wenn Sie es zur Kenntnis genommen haben.

- **Gelöst**

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

- **Veraltet**

  Der Zustand eines Ereignisses, wenn es automatisch korrigiert wird oder wenn die Ursache des Ereignisses nicht mehr vorliegt.

  Ein veraltetes Ereignis kann weder bestätigt noch behoben werden.

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 zu „Bestätigt“. Nachdem Sie eine geeignete Korrekturmaßnahme ergriffen haben, müssen Sie das Ereignis als behoben markieren. Der Ereignisstatus ändert sich dann zu „Behoben“.

Wird das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls ausgelöst, nimmt der Cluster nach Wiederherstellung der Stromversorgung ohne Eingreifen eines Administrators den Betrieb wieder auf. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig, und sein Status ändert sich im nächsten Überwachungszyklus zu „Veraltet“.

Unified Manager sendet eine Benachrichtigung, wenn sich ein Ereignis im Status „Veraltet“ oder „Gelöst“ befindet. Die E-Mail-Betreffzeile und der E-Mail-Inhalt einer Benachrichtigung enthalten Informationen über den Ereignisstatus. Ein SNMP-Trap enthält ebenfalls Informationen über den Ereignisstatus.

Informationen zu Ereignis-Schweregradtypen in Active IQ Unified Manager

Jedem Ereignis ist ein Typ des Schweregrads zugeordnet, der Sie bei der Priorisierung der Ereignisse unterstützt, die eine sofortige Korrekturmaßnahme erfordern.

- **Kritisch**

  Es ist ein Problem aufgetreten, das zu einer Serviceunterbrechung führen könnte, wenn nicht umgehend eine Korrekturmaßnahme ergriffen wird.

  Performance-kritische Ereignisse werden nur auf Grundlage benutzerdefinierter Schwellenwerte gesendet.

- **Fehler**

Die Ereignisquelle funktioniert weiterhin; jedoch ist eine Korrekturmaßnahme erforderlich, um eine Dienstunterbrechung zu vermeiden.

- **Warnung**

  Bei der Ereignisquelle ist ein Ereignis aufgetreten, dessen Sie sich bewusst sein sollten, oder ein Performance-Zähler für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads führen nicht zu einer Dienstunterbrechung, und sofortige Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Performance-Warnereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Informationen**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein beliebiges Storage Objekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird ein Ereignis mit dem Typ des Schweregrads Information generiert.

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

Informationen zu den Auswirkungsstufen von Ereignissen in Active IQ Unified Manager

Jedem Ereignis ist ein Auswirkungslevel (Incident, Risiko, Ereignis oder Upgrade) zugeordnet, damit Sie die Ereignisse priorisieren können, die eine sofortige Korrekturmaßnahme erfordern.

- **Incident**

  Ein Incident ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster keine Daten mehr an den Client bereitstellt und nicht mehr genügend Speicherplatz zum Speichern von Daten verfügbar ist. Ereignisse mit einer Auswirkungsstufe vom Level Incident sind am schwerwiegendsten. Um eine Dienstunterbrechung zu vermeiden, sollten umgehend Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die potenziell dazu führen können, dass ein Cluster keine Daten mehr an den Client bereitstellt und der Speicherplatz zum Speichern von Daten knapp wird. Ereignisse mit einer Auswirkungsstufe von Risiko können zu Dienstunterbrechungen führen. Gegebenenfalls sind Korrekturmaßnahmen erforderlich.

- **Ereignis**

  Ein Ereignis ist eine Zustands- oder Statusänderung von Storage Objekten und ihren Attributen. Ereignisse mit einem Auswirkungs-Level von Event dienen der Information und erfordern keine Korrekturmaßnahme.

- **Upgrade**

  Upgrade-Ereignisse sind eine spezielle Art von Ereignissen, die von der Active IQ-Plattform gemeldet werden. Diese Ereignisse kennzeichnen Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (aufgrund von Sicherheitshinweisen) erfordert. Bei einigen dieser Probleme ist möglicherweise eine sofortige Korrekturmaßnahme erforderlich, während andere bis zur nächsten planmäßigen Wartung warten können.

Informationen zu Ereignisauswirkungsbereichen in Active IQ Unified Manager

Ereignisse sind in sechs Auswirkungsbereiche (Verfügbarkeit, Kapazität, Konfiguration, Performance, Schutz und Sicherheit) eingeteilt, sodass Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse benachrichtigen Sie, wenn ein Storage-Objekt offline geht, ein Protokolldienst ausfällt, ein Problem mit Storage Failover auftritt oder ein Hardwareproblem auftritt.

- **Kapazität**

  Kapazitätsereignisse benachrichtigen Sie, wenn Ihre Aggregate, Volumes, LUNs oder Namespaces sich einer Größenschwelle nähern oder diese erreicht haben, oder wenn die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, Löschung, Hinzufügung, Entfernung oder Umbenennung Ihrer Storage Objekte. Konfigurationsereignisse haben ein Auswirkungslevel von Event und den Typ des Schweregrads Information.

- **Leistung**

  Performance-Ereignisse informieren Sie über Ressourcen-, Konfigurations- oder Aktivitätsbedingungen in Ihrem Cluster, die sich negativ auf die Geschwindigkeit der Datenspeicherung oder des Datenabrufs bei Ihren überwachten Storage-Objekten auswirken könnten.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Incidents oder Risiken im Zusammenhang mit SnapMirror Beziehungen, Probleme mit der Zielkapazität, Probleme mit SnapVault Beziehungen oder Probleme mit Schutzaufträgen. Alle ONTAP Objekte, insbesondere Aggregate, Volumes und SVMs, die sekundäre Volumes und Schutzbeziehungen hosten, zählen zum Schutzauswirkungsbereich.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes auf der Grundlage der in der "NetApp Security Hardening Guide für ONTAP 9" definierten Parameter sind.

  Zusätzlich umfasst dieser Bereich Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden.

Wie Active IQ Unified Manager den Objektstatus berechnet

Der Objektstatus wird durch das schwerwiegendste Ereignis bestimmt, das aktuell den Status „Neu“ oder „Bestätigt“ aufweist. Wenn der Objektstatus beispielsweise „Fehler“ lautet, hat eines der Ereignisse des Objekts den Typ des Schweregrads „Fehler“. Sobald eine Korrekturmaßnahme ergriffen wurde, ändert sich der Ereignisstatus zu „Behoben“.

Informationen zu dynamischen Leistungsereignissen in Active IQ Unified Manager

Bei dynamischen Performance-Ereignissen werden im Abschnitt „Systemdiagnose“ auf der Seite mit den Ereignisdetails die wichtigsten Workloads mit der höchsten Latenz oder Auslastung der Clusterkomponente aufgelistet, um die ein Ressourcenkonflikt besteht.

Die Performance Statistiken basieren auf dem Zeitraum von der Erkennung des Performance-Ereignisses bis zur letzten Analyse des Ereignisses. Die Diagramme zeigen außerdem historische Performance Statistiken für die Clusterkomponente, um die ein Konflikt besteht.

Sie können beispielsweise Workloads mit hoher Auslastung einer Komponente identifizieren, um zu bestimmen, welcher Workload auf eine weniger ausgelastete Komponente verschoben werden sollte. Durch das Verschieben des Workloads würde sich die Arbeitslast auf der aktuellen Komponente verringern, wodurch die Komponente möglicherweise nicht mehr um Ressourcen konkurriert. Oben in diesem Abschnitt werden der Uhrzeit- und Datumsbereich angezeigt, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird der Zeitpunkt der letzten Analyse aktualisiert.

Die Diagramme zu Latenz und Aktivität zeigen die Namen der wichtigsten Workloads an, wenn Sie den Mauszeiger über das Diagramm bewegen. Über das Menü „Workload Type“ rechts neben dem Diagramm können Sie die Workloads nach ihrer Rolle im Ereignis sortieren, darunter „Haie“, „Angreifer“ oder „Opfer“, und Details zu ihrer Latenz sowie zu ihrer Auslastung auf der betroffenen Clusterkomponente anzeigen. Sie können den Istwert mit dem erwarteten Wert vergleichen, um zu erkennen, wann sich der Workload außerhalb seines erwarteten Latenz- oder Auslastungsbereichs befand. Informationen dazu enthält "Von Unified Manager überwachte Workload-Typen".

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

Weitere Informationen zu den dynamischen Performance-Schwellenwerten finden Sie unter "Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte".

Informationen darüber, wie Unified Manager die Workloads einstuft und die Sortierreihenfolge bestimmt, finden Sie unter "Wie Unified Manager die Performance-Auswirkungen eines Ereignisses ermittelt".

Die Daten in den Diagrammen zeigen 24 Stunden Performance Statistiken vor dem letzten Zeitpunkt, zu dem das Ereignis analysiert wurde. Die tatsächlichen Werte und erwarteten Werte für jede Arbeitslast basieren auf dem Zeitpunkt, zu dem die Arbeitslast an dem Ereignis beteiligt war. Beispielsweise kann eine Arbeitslast erst nach der Erkennung des Ereignisses an einem Ereignis beteiligt sein, sodass ihre Performance Statistiken möglicherweise nicht mit den Werten zum Zeitpunkt der Ereigniserkennung übereinstimmen. Standardmäßig sind die Arbeitslasten nach der Spitzenabweichung (höchsten Abweichung) bei der Latenz sortiert.

> Da Unified Manager maximal 30 Tage an historischen Performance- und Ereignisdaten im 5-Minuten-Takt speichert, werden keine Performance-Daten angezeigt, wenn das Ereignis älter als 30 Tage ist.

- **Spalte „Arbeitslastsortierung“**
  - **Latenzdiagramm**

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

Zeigt Details zur Auslastung der Clusterkomponente im Konfliktfall an. In den Diagrammen stellt die blaue Linie die tatsächliche Auslastung dar. Ein roter Balken markiert die Ereignisdauer vom Zeitpunkt der Erkennung bis zum Zeitpunkt der letzten Analyse. Weitere Informationen sind unter "Messwerte zur Workload Performance" verfügbar.

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

- **Komponentenverwendung**

  Zeigt den Nutzungsverlauf in Prozent für die Netzwerk-, Datenverarbeitungs- und Aggregatkomponenten bzw. den Aktivitätsverlauf in Prozent für die QoS-Richtliniengruppenkomponente an. Für die Netzwerk- und Interconnect-Komponenten wird kein Diagramm angezeigt. Durch Zeigen auf die Statistiken können die Nutzungsstatistiken zu einem bestimmten Zeitpunkt angezeigt werden.

- **Verlauf der gesamten Schreibvorgänge in MB/s**

  Nur für die Komponente „MetroCluster Resources“ wird der gesamte Schreibdurchsatz in Megabyte pro Sekunde (MBps) für alle Volume-Workloads angezeigt, die in einer MetroCluster Konfiguration auf den Partner-Cluster gespiegelt werden.

- **Ereignisverlauf**

  Zeigt rot schattierte Linien an, um die historischen Ereignisse der betroffenen Komponente darzustellen. Bei veralteten Ereignissen werden Ereignisse angezeigt, die vor der Erkennung des ausgewählten Ereignisses und nach dessen Behebung stattfanden.

Vom Active IQ Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, um festzustellen, ob eine Änderung ein Performance Ereignis verursacht hat oder dazu beigetragen haben könnte. Die Seiten des Performance Explorer zeigen ein Änderungssymbol ( ) an, das das Datum und die Uhrzeit angibt, zu denen die Änderung erkannt wurde.

Auf den Seiten von Performance Explorer und auf der Seite Workload Analysis können die Performance-Diagramme geprüft werden, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung gleichzeitig oder ungefähr zur selben Zeit wie ein Performance-Ereignis erkannt wurde, hat sie möglicherweise zu dem Problem beigetragen, das die Ereigniswarnung ausgelöst hat.

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

- Ein Volume bewegt sich zwischen Aggregaten.

  Unified Manager kann erkennen, ob eine Volume Verschiebung ausgeführt wird, abgeschlossen wurde oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume Verschiebung nicht verfügbar ist, erkennt er die Volume Verschiebung nach der Wiederverfügbarkeit und zeigt ein entsprechendes Änderungsereignis an.

- Der Durchsatzgrenzwert (MB/s oder IOPS) einer QoS-Richtliniengruppe, die einen oder mehrere überwachte Workloads enthält, ändert sich.

  Die Änderung eines Grenzwerts einer Richtliniengruppe kann zu vorübergehenden Spitzen bei der Latenz

(Antwortzeit) führen, die wiederum Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich wieder, und alle durch die Spitzen verursachten Ereignisse verlieren ihre Relevanz.

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

  Unified Manager kann erkennen, wann eine Übernahme, Teilübernahme oder Rückgabe abgeschlossen wurde. Wenn die Übernahme durch einen ausgefallenen Knoten verursacht wird, erkennt Unified Manager dieses Ereignis nicht.

- Ein ONTAP Upgrade oder ein Revert-Vorgang wird erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Liste der Ereignisse und Schweregrade

Informationen zu Aggregatereignissen in Active IQ Unified Manager

Aggregatereignisse liefern Ihnen Informationen über den Status von Aggregaten, sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

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

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregat Offline(ocumEvtAggregateStateOffline)	Vorfall	Aggregat	Kritisch
Aggregat fehlgeschlagen(ocumEvtAggregateStateFailed)	Vorfall	Aggregat	Kritisch
Aggregat eingeschränkt(ocumEvtAggregateStateRestricted)	Risiko	Aggregat	Warnung
Aggregatrekonstruktion(ocumEvtAggregateRaidStateReconstructing)	Risiko	Aggregat	Warnung
Aggregate beeinträchtigt(ocumEvtAggregateRaidStateDegraded)	Risiko	Aggregat	Warnung
Teilweise erreichbare Cloud-Ebene(ocumEventCloudTierPartiallyReachable)	Risiko	Aggregat	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cloud Tier nicht erreichbar(ocumEventCloudTierUnreachable)	Risiko	Aggregat	Fehler
Zugriff auf Cloud Tier für Aggregatverlagerung verweigert *(arlNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Cloud Tier Zugriff für Aggregatverlagerung während Storage Failover verweigert *(gbNetraCaCheckFailed)	Risiko	Aggregat	Fehler
MetroCluster Zurückgelassenes Aggregat (ocumEvtMetroClusterAggregateLeftBehind)	Risiko	Aggregat	Fehler
MetroCluster Aggregate Mirroring beeinträchtigt(ocumEvtMetroClusterAggregateMirrorDegraded)	Risiko	Aggregat	Fehler

Wirkungsbereich: Kapazität

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregatsspeicherplatz nahezu voll(ocumEvtAggregateNearlyFull)	Risiko	Aggregat	Warnung
Aggregat-Speicherplatz voll(ocumEvtAggregateFull)	Risiko	Aggregat	Fehler
Tage, bis das Aggregat voll ist(ocumEvtAggregateDaysUntilFullSoon)	Risiko	Aggregat	Fehler
Aggregate überbelegt(ocumEvtAggregateOvercommitted)	Risiko	Aggregat	Fehler
Aggregat nahezu überbucht(ocumEvtAggregateAlmostOvercommitted)	Risiko	Aggregat	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Snapshot Reserve des Aggregats voll(ocumEvtAggregateSnapReserveFull)	Risiko	Aggregat	Warnung
Anomale Aggregatwachstumsrate(ocumEvtAggregateGrowthRateAbnormal)	Risiko	Aggregat	Warnung

Wirkungsbereich: Konfiguration

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregat erkannt(nicht zutreffend)	Ereignis	Aggregat	Informationen
Aggregat umbenannt(Nicht zutreffend)	Ereignis	Aggregat	Informationen
Aggregat gelöscht(Nicht zutreffend)	Ereignis	Node	Informationen

Wirkungsbereich: Performance

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Aggregat-IOPS überschritten(ocumAggregateIopsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für Aggregat-IOPS überschritten(ocumAggregateIopsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für Aggregat MB/s überschritten(ocumAggregateMbpsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für Aggregat MB/s überschritten(ocumAggregateMbpsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für die Aggregatlatenz überschritten(ocumAggregateLatencyIncident)	Vorfall	Aggregat	Kritisch

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnschwellenwert für die Aggregat-Latenz überschritten(ocumAggregateLatencyWarning)	Risiko	Aggregat	Warnung
Verwendete Aggregat Performance-Kapazität: Kritischer Schwellenwert überschritten(ocumAggregatePerfCapacityUsedIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für die genutzte Aggregat Performance-Kapazität überschritten(ocumAggregatePerfCapacityUsedWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für die Aggregat-Auslastung überschritten (ocumAggregateUtilizationIncident)	Vorfall	Aggregat	Kritisch
Warnschwellenwert für die Auslastung des Aggregats überschritten (ocumAggregateUtilizationWarning)	Risiko	Aggregat	Warnung
Schwellenwert für übermäßige Auslastung von Aggregat-Festplatten überschritten (ocumAggregateDisksOverUtilizedWarning)	Risiko	Aggregat	Warnung
Dynamischer Schwellenwert des Aggregats überschritten (ocumAggregateDynamicEventWarning)	Risiko	Aggregat	Warnung

Informationen zu Clusterereignissen in Active IQ Unified Manager

Clusterereignisse liefern Informationen über den Status von Clustern und ermöglichen so die Überwachung der Cluster auf potenzielle Probleme. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

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

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cluster verfügt nicht über Ersatzfestplatten(ocumEvtDisksNoSpares)	Risiko	Cluster	Warnung
Cluster nicht erreichbar(ocumEvtClusterUnreachable)	Risiko	Cluster	Fehler
Clusterüberwachung fehlgeschlagen(ocumEvtClusterMonitoringFailed)	Risiko	Cluster	Warnung
Kapazitätsgrenzen der Cluster FabricPool Lizenz überschritten (ocumEvtExternalCapacityTierSpaceFull)	Risiko	Cluster	Warnung
NVMe-oF Kulanzfrist gestartet *(nvmfGracePeriodStart)	Risiko	Cluster	Warnung
NVMe-oF-Kulanzfrist aktiv *(nvmfGracePeriodActive)	Risiko	Cluster	Warnung
NVMe-oF Kulanzfrist abgelaufen *(nvmfGracePeriodExpired)	Risiko	Cluster	Warnung
Objektwartungsfenster gestartet(objectMaintenanceWindowStarted)	Ereignis	Cluster	Kritisch
Objektwartungsfenster beendet(objectMaintenanceWindowEnded)	Ereignis	Cluster	Informationen
MetroCluster Zurückgelassene Ersatzfestplatten(ocumEvtSpareDiskLeftBehind)	Risiko	Cluster	Fehler
MetroCluster Automatische ungeplante Umschaltung deaktiviert(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risiko	Cluster	Warnung
Passwort des Cluster-Benutzers geändert *(cluster.passwd.changed)	Ereignis	Cluster	Informationen

Wirkungsbereich: Kapazität

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schwellenwert für das Ungleichgewicht der Clusterkapazität überschritten(ocumConformanceNodeImbalanceWarning)	Risiko	Cluster	Warnung
Planung der Cluster Cloud Tier (clusterCloudTierPlanningWarning)	Risiko	Cluster	Warnung
FabricPool Spiegelreplikations-Resynchronisierung abgeschlossen *(waflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool Platz fast voll *(fabricpoolNearlyFull)	Risiko	Cluster	Fehler

Wirkungsbereich: Konfiguration

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Knoten hinzugefügt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Knoten entfernt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Cluster entfernt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Cluster hinzufügen fehlgeschlagen(Nicht zutreffend)	Ereignis	Cluster	Fehler
Clustername geändert(Nicht zutreffend)	Ereignis	Cluster	Informationen
Notfall-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Kritische EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Warnmeldung EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Fehler
EMS-Fehler empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
EMS-Warnung empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
Debug EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
EMS Benachrichtigung erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Informative EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS Ereignisse werden in drei Unified Manager Ereignisschweregrade kategorisiert.

Schweregrad-Level des Unified Manager Events	ONTAP EMS Level des Ereignis Schweregrads
Kritisch	Notfall Kritisch
Fehler	Alarm
Warnung	Fehler Warnung Debug Hinweis Informationen

Wirkungsbereich: Performance

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

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cluster MB/s Warnschwelle überschritten(ocumClusterMbpsWarning)	Risiko	Cluster	Warnung
Dynamischer Schwellenwert des Clusters überschritten(ocumClusterDynamicEventWarning)	Risiko	Cluster	Warnung

Wirkungsbereich: Sicherheit

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfiguredDisabled)	Risiko	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt(ocumClusterAuditLogUnencrypted)	Risiko	Cluster	Warnung
Standardmäßig ist der lokale 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
Protokollweiterleitungsziele geändert(ocumLogForwardDestinationsChanged)	Risiko	Cluster	Warnung
NTP-Servernamen geändert(ocumNtpServerNamesChanged)	Risiko	Cluster	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anzahl der NTP-Server ist niedrig(securityConfigNTPServerCountLowRisk)	Risiko	Cluster	Warnung
Cluster Peer-Kommunikation nicht verschlüsselt(ocumClusterPeerEncryptionDisabled)	Risiko	Cluster	Warnung
SSH verwendet unsichere Verschlüsselungsalgorithmen(ocumClusterSSHInsecure)	Risiko	Cluster	Warnung
Telnet-Protokoll aktiviert(ocumClusterTelnetEnabled)	Risiko	Cluster	Warnung
Die Passwörter einiger ONTAP Benutzerkonten verwenden die weniger sichere MD5-Hashfunktion(ocumClusterMD5PasswordHashUsed)	Risiko	Cluster	Warnung
Der Cluster verwendet ein selbstsigniertes Zertifikat(ocumClusterSelfSignedCertificate)	Risiko	Cluster	Warnung
Cluster Remote Shell ist aktiviert(ocumClusterRshDisabled)	Risiko	Cluster	Warnung
Das Cluster-Zertifikat läuft demnächst ab(ocumEvtClusterCertificateAboutToExpire)	Risiko	Cluster	Warnung
Clusterzertifikat abgelaufen(ocumEvtClusterCertificateExpired)	Risiko	Cluster	Fehler

Informationen zu Datenträgerereignissen in Active IQ Unified Manager

Datenträgerereignisse liefern Ihnen Informationen über den Status der Datenträger, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Flash Disks - Reserveblöcke fast vollständig verbraucht(ocumEvtClusterFlashDiskFewerSpareBlockError)	Risiko	Cluster	Fehler
Flash Disks - Keine Ersatzblöcke(ocumEvtClusterFlashDiskNoSpareBlockCritical)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Datenträger(ocumEvtClusterUnassignedDisksSome)	Risiko	Cluster	Warnung
Einige ausgefallene Festplatten(ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Informationen zu Gehäuseereignissen in Active IQ Unified Manager

Gehäuseereignisse liefern Ihnen Informationen über den Status von Disk Shelf Gehäusen in Ihrem Datacenter, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Lüfter des Disk Shelf ausgefallen(ocumEvtShelfFanFailed)	Vorfall	Storage Shelf	Kritisch
Netzteile des Disk Shelf ausgefallen(ocumEvtShelfPowerSupplyFailed)	Vorfall	Storage Shelf	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
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
Shelf-Pfadfehler(ocumDiskShelfConnectivityPathFailure)	Risiko	Storage-Shelf	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Disk Shelf entdeckt(nicht zutreffend)	Ereignis	Node	Informationen
Disk Shelves entfernt(Nicht zutreffend)	Ereignis	Node	Informationen

Informationen zu Lüfterereignissen in Active IQ Unified Manager

Lüfterereignisse liefern Ihnen Informationen zum Status der Lüfter auf den Knoten in Ihrem Datacenter, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ein oder mehrere defekte Lüfter(ocumEvtFansOneOrMoreFailed)	Vorfall	Node	Kritisch

Informationen zu Flash-Karten-Ereignissen in Active IQ Unified Manager

Flash Kartenereignisse liefern Ihnen Informationen über den Status der auf Knoten in Ihrem Datacenter installierten Flash Karten, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Flash-Karten offline(ocumEvtFlashCardOffline)	Vorfall	Node	Kritisch

Informationen zu Inode-Ereignissen in Active IQ Unified Manager

Inode-Ereignisse liefern Informationen dazu, wann ein Inode voll oder nahezu voll ist, sodass eine Überwachung auf potenzielle Probleme möglich ist. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

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

Netzwerkschnittstellenereignisse in Active IQ Unified Manager

Ereignisse für Netzwerkschnittstellen liefern Informationen über den Status Ihrer Netzwerkschnittstellen (LIFs), sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Netzwerkschnittstellenstatus ausgefallen(ocumEvtLifStatusDown)	Risiko	Schnittstelle	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
FC/FCoE Netzwerkschnittstellenstatus ausgefallen(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)	Auswirkungs-Level	Quellentyp	Schwere
Netzwerkschnittstellenroute nicht konfiguriert(nicht zutreffend)	Ereignis	Schnittstelle	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkschnittstelle MB/s überschritten(ocumNetworkLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
Warnschwelle für Netzwerkschnittstelle MB/s überschritten(ocumNetworkLifMbpsWarning)	Risiko	Schnittstelle	Warnung
Kritischer Schwellenwert für die FC Netzwerkschnittstelle in MB/s überschritten(ocumFcpLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
FC Netzwerkschnittstelle MB/s Warnschwelle überschritten(ocumFcpLifMbpsWarning)	Risiko	Schnittstelle	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVMf FC Netzwerkschnittstelle MB/s Kritischer Schwellenwert überschritten(ocumNvmfFcLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
NVMf FC Netzwerkschnittstelle MB/s Warnschwelle überschritten(ocumNvmfFcLifMbpsWarning)	Risiko	Schnittstelle	Warnung

Informationen zu LUN-Ereignissen in Active IQ Unified Manager

LUN-Ereignisse liefern Ihnen Informationen über den Status Ihrer LUNs, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

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

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN offline (ocumEvtLunOffline)	Vorfall	LUN	Kritisch
LUN zerstört *(lunDestroy)	Ereignis	LUN	Informationen
LUN mit nicht unterstütztem Betriebssystem in Initiatorgruppe(igroupUnsupportedOsType)	Vorfall	LUN	Warnung
Einzelner aktiver Pfad zum Zugriff auf LUN(ocumEvtLunSingleActivePath)	Risiko	LUN	Warnung
Keine aktiven Pfade für den Zugriff auf LUN(ocumEvtLunNotReachable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade für den Zugriff auf LUN(ocumEvtLunOptimizedPathInactive)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Keine Pfade für den Zugriff auf LUN vom HA Partner(ocumEvtLunHaPathInactive)	Risiko	LUN	Warnung
Kein Zugriffspfad auf die LUN von einem Knoten im HA-Paar(ocumEvtLunNodePathStatusDown)	Risiko	LUN	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Unzureichender Speicherplatz für LUN-Snapshot-Kopie(ocumEvtLunSnapshotNotPossible)	Risiko	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN mit nicht unterstütztem Betriebssystem in Initiatorgruppe(igroupUnsupportedOsType)	Risiko	LUN	Warnung

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für LUN IOPS überschritten(ocumLunIopsIncident)	Vorfall	LUN	Kritisch
LUN IOPS Warnschwelle überschritten(ocumLunIopsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN MB/s überschritten(ocumLunMbpsIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN MB/s Warnschwelle überschritten(ocumLunMbpsWarning)	Risiko	LUN	Warnung
LUN-Latenz ms/op Kritischer Schwellenwert überschritten(ocumLunLatencyIncident)	Vorfall	LUN	Kritisch
LUN-Latenz ms/op Warnschwelle überschritten(ocumLunLatencyWarning)	Risiko	LUN	Warnung
Kritische Schwellenwerte für LUN-Latenz und IOPS überschritten(ocumLunLatencyIopsIncident)	Vorfall	LUN	Kritisch
LUN-Latenz- und IOPS-Warnschwellenwert 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
LUN-Latenz und genutzte Aggregate Performance-Kapazität, kritischer Schwellenwert überschritten(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwellenwert für LUN Latenz und verwendete Performance-Kapazität des Aggregats überschritten(ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Aggregatauslastung überschritten(ocumLunLatencyAggregateUtilizationIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnschwellenwert für LUN-Latenz und Aggregat-Auslastung überschritten(ocumLunLatencyAggregateUtilizationWarning)	Risiko	LUN	Warnung
LUN-Latenz und verwendete Knoten-Performance-Kapazität, kritischer Schwellenwert überschritten(ocumLunLatencyNodePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
LUN-Latenz und verwendete Knoten-Performance-Kapazität, Warnschwellenwert überschritten(ocumLunLatencyNodePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Ausgelastete LUN-Latenz und Knotenleistungskapazität, kritischer Schwellenwert für die Übernahme überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node Performance Capacity - Schwellenwert für die Takeover-Warnung überschritten(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Knotenauslastung überschritten(ocumLunLatencyNodeUtilizationIncident)	Vorfall	LUN	Kritisch
Schwellenwert für LUN-Latenz und Knotenauslastung überschritten(ocumLunLatencyNodeUtilizationWarning)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS LUN Max IOPS Warnschwelle überschritten(ocumQosLunMaxIopsWarning)	Risiko	LUN	Warnung
QoS LUN Max MB/s Warnschwelle überschritten(ocumQosLunMaxMbpsWarning)	Risiko	LUN	Warnung
Schwellenwert für die Workload LUN Latenz gemäß der Performance Service Level Policy überschritten (ocumConformanceLatencyWarning)	Risiko	LUN	Warnung

Informationen zu Management Stationsereignissen in Active IQ Unified Manager

Die Ereignisse der Managementstation liefern Ihnen Informationen über den Status des Servers, auf dem Unified Manager installiert ist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Speicherplatz auf dem Management Server fast voll(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risiko	Managementstation	Warnung
Speicherplatz auf dem Verwaltungsserver voll(ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Managementstation	Kritisch
Management Server mit wenig Arbeitsspeicher(ocumEvtUnifiedManagerMemoryLow)	Risiko	Managementstation	Warnung
Management Server fast ohne freien Speicher(ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Managementstation	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Größe der MySQL-Protokolldatei erhöht; Neustart erforderlich(ocumEvtMysqlLogFileSizeWarning)	Vorfall	Managementstation	Warnung
Die insgesamt zugewiesene Größe des Audit-Protokolls ist fast ausgeschöpft.	Risiko	Managementstation	Warnung
Zertifikat des Syslog-Servers läuft demnächst ab	Risiko	Managementstation	Warnung
Zertifikat des Syslog Server abgelaufen	Risiko	Managementstation	Fehler
Überwachungsprotokolldatei manipuliert	Risiko	Managementstation	Warnung
Audit-Protokolldatei gelöscht	Risiko	Managementstation	Warnung
Verbindungsfehler beim Syslog-Server	Risiko	Managementstation	Fehler
Konfiguration des Syslog-Servers geändert	Ereignis	Managementstation	Warnung

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Analyse von Leistungsdaten ist beeinträchtigt(ocumEvtUnifiedManagerDataMissingAnalyze)	Risiko	Managementstation	Warnung
Die Erfassung von Leistungsdaten ist beeinträchtigt(ocumEvtUnifiedManagerDataMissingCollection)	Vorfall	Managementstation	Kritisch

Diese beiden letzten Performance-Ereignisse waren nur für Unified Manager 7.2 verfügbar. Wenn eines dieser Ereignisse den Status „Neu“ aufweist und Sie anschließend 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.

Informationen zu MetroCluster Bridge Ereignissen in Active IQ Unified Manager

MetroCluster Bridge-Ereignisse liefern Informationen zum Status der Bridges, sodass Sie

potenzielle Probleme in einer MetroCluster over FC Konfiguration überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, den Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Brücke nicht erreichbar(ocumEvtBridgeUnreachable)	Vorfall	MetroCluster Brücke	Kritisch
Brückentemperatur abnormal(ocumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster Brücke	Kritisch

Informationen zu MetroCluster Verbindungsereignissen in Active IQ Unified Manager

Konnektivitätsereignisse liefern Informationen über die Konnektivität zwischen den Komponenten eines Clusters sowie zwischen Clustern in MetroCluster over FC und MetroCluster over IP Konfigurationen, sodass potenzielle Probleme überwacht werden können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Impact Level, Quelltyp und Schweregrad.

In beiden Konfigurationen gemeinsame Ereignisse

Diese Verbindungsereignisse sind sowohl für MetroCluster over FC als auch für MetroCluster over IP Konfigurationen üblich.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Alle Verbindungen zwischen MetroCluster Partnern unterbrochen(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Partner über Peering-Netzwerk nicht erreichbar (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Disaster Recovery Fähigkeit beeinträchtigt (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster Beziehung	Kritisch

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

MetroCluster über FC Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster over FC Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Alle Verbindungen zwischen den Switches ausgefallen(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster Verbindung zwischen den Switches	Kritisch
Verbindung der FC-SAS Bridge zum Storage Stack unterbrochen(ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster Konfiguration teilweise umgeschaltet(ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risiko	MetroCluster Beziehung	Fehler
Knoten zu FC Switch: Alle FC-VI-Verbindungslinks ausgefallen(ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster Node Switch Verbindung	Kritisch
Knoten zu FC Switch: Eine oder mehrere FC-Initiatorverbindungen unterbrochen(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risiko	MetroCluster Node Switch Verbindung	Warnung
Knoten zu FC Switch: Alle FC-Initiator-Verbindungen ausgefallen(ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster Node Switch Verbindung	Kritisch
Switch zu FC-SAS-Brücke FC-Verbindung unterbrochen (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	MetroCluster Switch Bridge Verbindung	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Inter Node Alle FC VI InterConnect Verbindungen ausgefallen (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen den Knoten	Kritisch
Zwischen Knoten eine oder mehrere FC VI InterConnect Verbindungen ausgefallen (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risiko	Verbindung zwischen den Knoten	Warnung
Verbindung zwischen Knoten und Brücke unterbrochen (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Node-Bridge-Verbindung	Kritisch
Knoten zu Storage Stack: Alle SAS Verbindungen ausgefallen (ocumEvtMccNodeStackLinksDown)	Vorfall	Node-Stack-Verbindung	Kritisch
Knoten zu Storage Stack: Ein oder mehrere SAS-Links ausgefallen (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risiko	Node-Stack-Verbindung	Warnung

MetroCluster over IP Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster over IP Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
MetroCluster IP-Standort-zu-Standort-Konnektivitätsstatus ist unterbrochen (mccIntersiteconnectivityStatusDown)	Risiko	MetroCluster Beziehung	Kritisch
MetroCluster IP Knoten-zu-Switch-Verbindung offline (mccIpPortStatusOffline)	Risiko	Node	Fehler

Informationen zu MetroCluster Switch-Ereignissen in Active IQ Unified Manager

MetroCluster Switch-Ereignisse für MetroCluster over FC Konfigurationen bieten Informationen zum Status der MetroCluster Switches, um potenzielle Probleme zu überwachen. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Impact Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Abnormale Switch-Temperatur(ocumEvtSwitchTemperatureAbnormal)	Vorfall	MetroCluster Switch	Kritisch
Switch nicht erreichbar(ocumEvtSwitchUnreachable)	Vorfall	MetroCluster Switch	Kritisch
Lüfter des Switches ausgefallen(ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Netzteile des Switches ausgefallen(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Temperatursensoren des Switches ausgefallen(ocumEvtSwitchTemperatureSensorFailed) Dieses Ereignis gilt nur für Cisco Switches.	Vorfall	MetroCluster Switch	Kritisch

Informationen zu NVMe Namespace Ereignissen in Active IQ Unified Manager

NVMe Namespace Ereignisse liefern Ihnen Informationen über den Status Ihrer Namespaces, sodass potenzielle Probleme überwacht werden können. Die Ereignisse sind nach Wirkungsbereichen gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

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

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVMeNS offline *(nvmeNamespaceStatusOffline)	Ereignis	Namensraum	Informationen
NVMeNS online *(nvmeNamespaceStatusOnline)	Ereignis	Namensraum	Informationen
NVMeNS Kein Speicherplatz mehr *(nvmeNamespaceSpaceOutOfSpace)	Risiko	Namensraum	Warnung
NVMeNS löschen *(nvmeNamespaceDestroy)	Ereignis	Namensraum	Informationen

Wirkungsbereich: Performance

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

Ereignisname (Trap-Name)	Auswirkungs-Level	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
Latenz des NVMe Namespace und kritischer MB/s-Schwellenwert überschritten(ocumNvmeNamespaceLatencyMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace Latenz und MB/s-Warnschwelle überschritten(ocumNvmeNamespaceLatencyMbpsWarning)	Risiko	Namensraum	Warnung

Informationen zu Knotenereignissen in Active IQ Unified Manager

Knotenereignisse liefern Ihnen Informationen zum Knotenstatus, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, Level, den Quelltyp und Schweregrad.

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

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Speicherplatz des Node Root Volume nahezu voll(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risiko	Node	Warnung
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risiko	Node	Fehler

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

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS Monitor Speicher voll ausgeschöpft *(ocumQosMonitorMemoryMaxed)	Risiko	Node	Fehler
QoS Monitor-Speicher reduziert *(ocumQosMonitorMemoryAbated)	Ereignis	Node	Informationen

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Knoten umbenannt(Nicht zutreffend)	Ereignis	Node	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer IOPS-Schwellenwert des Knotens überschritten(ocumNodeIopsIncident)	Vorfall	Node	Kritisch
Knoten-IOPS-Warnschwelle überschritten(ocumNodeIopsWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knoten MB/s überschritten(ocumNodeMbpsIncident)	Vorfall	Node	Kritisch
Knoten-MB/s-Warnschwelle überschritten(ocumNodeMbpsWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knotenlatenz ms/op überschritten(ocumNodeLatencyIncident)	Vorfall	Node	Kritisch
Warnschwelle für Knotenlatenz ms/op überschritten(ocumNodeLatencyWarning)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für die genutzte Knoten-Performance-Kapazität überschritten(ocumNodePerfCapacityUsedIncident)	Vorfall	Node	Kritisch
Warnschwelle für die genutzte Node-Performance-Kapazität überschritten(ocumNodePerfCapacityUsedWarning)	Risiko	Node	Warnung
Genutzte Knoten-Performance-Kapazität - kritischer Schwellenwert für Übernahme überschritten(ocumNodePerfCapacityUsedTakeoverIncident)	Vorfall	Node	Kritisch
Genutzte Knoten-Performancekapazität - Schwellenwert für die Übernahmewarnung überschritten(ocumNodePerfCapacityUsedTakeoverWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für die Knotenauslastung überschritten (ocumNodeUtilizationIncident)	Vorfall	Node	Kritisch
Schwellenwert für die Knotenauslastungswarnung überschritten (ocumNodeUtilizationWarning)	Risiko	Node	Warnung
Überlastungsschwelle des Knoten-HA-Paares überschritten (ocumNodeHaPairOverUtilizedInformation)	Ereignis	Node	Informationen
Schwellenwert für die Festplattenfragmentierung des Knotens überschritten (ocumNodeDiskFragmentationWarning)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schwellenwert für die genutzte Performance-Kapazität überschritten (ocumNodeOverUtilizedWarning)	Risiko	Node	Warnung
Dynamischer Schwellenwert des Knotens überschritten (ocumNodeDynamicEventWarning)	Risiko	Node	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Beratungs-ID: NTAP-<*advisory ID*>(ocumx)	Risiko	Node	Kritisch

Informationen zu NVRAM Batterieereignissen in Active IQ Unified Manager

NVRAM Batterieereignisse liefern Ihnen Informationen über den Status Ihrer Batterien, damit Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVRAM Batterie schwach(ocumEvtNvramBatteryLow)	Risiko	Node	Warnung
NVRAM Batterie entladen(ocumEvtNvramBatteryDischarged)	Risiko	Node	Fehler
NVRAM Batterie übermäßig geladen(ocumEvtNvramBatteryOverCharged)	Vorfall	Node	Kritisch

Informationen zu Portereignissen in Active IQ Unified Manager

Portereignisse liefern Ihnen Statusinformationen zu Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, z. B. ob der Port ausgefallen ist.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Port-Status nicht verfügbar(ocumEvtPortStatusDown)	Vorfall	Node	Kritisch

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkport MB/s überschritten(ocumNetworkPortMbpsIncident)	Vorfall	Port	Kritisch
Warnschwelle für Netzwerkport MB/s überschritten(ocumNetworkPortMbpsWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert für FCP Port MB/s überschritten(ocumFcpPortMbpsIncident)	Vorfall	Port	Kritisch
FCP Port MB/s Warnschwelle überschritten(ocumFcpPortMbpsWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert für die Netzwerkportauslastung überschritten(ocumNetworkPortUtilizationIncident)	Vorfall	Port	Kritisch
Warnschwellenwert für Netzwerkportauslastung überschritten(ocumNetworkPortUtilizationWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert der FCP Port Auslastung überschritten(ocumFcpPortUtilizationIncident)	Vorfall	Port	Kritisch
Warnschwellenwert für FCP Port Auslastung überschritten(ocumFcpPortUtilizationWarning)	Risiko	Port	Warnung

Informationen zu Ereignissen im Zusammenhang mit der Stromversorgung in Active IQ Unified Manager

Ereignisse zu Netzteilen liefern Ihnen Informationen zum Status Ihrer Hardware, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ein oder mehrere ausgefallene Netzteile(ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Node	Kritisch

Informationen zu Schutzereignissen in Active IQ Unified Manager

Schutzereignisse zeigen, ob ein Auftrag fehlgeschlagen oder abgebrochen worden ist, sodass sich Probleme überwachen lassen. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schutzaufgabe fehlgeschlagen(ocumEvtProtectionJobTaskFailed)	Vorfall	Volume oder Storage Service	Kritisch
Schutzauftrag abgebrochen(ocumEvtProtectionJobAborted)	Risiko	Volume oder Storage Service	Warnung

Informationen zu Qtree-Ereignissen in Active IQ Unified Manager

Qtree Ereignisse liefern Ihnen Informationen über die qtree Kapazität sowie über Datei- und Festplattenbeschränkungen, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Qtree-Speicher fast voll(ocumEvtQtreeSpaceNearlyFull)	Risiko	Qtree	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Qtree-Speicherplatz voll (ocumEvtQtreeSpaceFull)	Risiko	Qtree	Fehler
Qtree-Speicherplatz normal (ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Informationen
Qtree-Dateien: Hartes Limit erreicht(ocumEvtQtreeFilesHardLimitReached)	Vorfall	Qtree	Kritisch
Soft Limit von Qtree Dateien überschritten(ocumEvtQtreeFilesSoftLimitBreached)	Risiko	Qtree	Warnung
Hartes Qtree Speicherplatzlimit erreicht(ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Softlimit für den Qtree-Speicherbereich überschritten(ocumEvtQtreeSpaceSoftLimitBreached)	Risiko	Qtree	Warnung

Informationen zu Service Processor Ereignissen in Active IQ Unified Manager

Serviceprozessorereignisse liefern Ihnen Informationen über den Status Ihres Prozessors, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Dienstprozessor nicht konfiguriert(ocumEvtServiceProcessorNotConfigured)	Risiko	Node	Warnung
Dienstprozessor offline(ocumEvtServiceProcessorOffline)	Risiko	Node	Fehler

Informationen zu SnapMirror Beziehung Ereignissen in Active IQ Unified Manager

SnapMirror Beziehungsereignisse liefern Ihnen Informationen über den Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie potenzielle Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage VMs als auch für Volumes generiert, synchrone SnapMirror Beziehungsereignisse dagegen nur für Volume Beziehungen. Für einzelne Volumes, die Teil von Disaster-Recovery-Beziehungen von Storage VMs sind, werden keine Ereignisse generiert. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

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

Die SnapMirror Beziehungsereignisse werden für Storage VMs generiert, die durch die Disaster Recovery von Storage VMs geschützt sind, jedoch nicht für Beziehungen zwischen einzelnen Objekten.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ungesunde Spiegelreplikation(ocumEvtSnapmirrorRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Spiegelreplikation abgebrochen(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Initialisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Fehler bei der Spiegelreplikationsverzögerung(ocumEvtSnapMirrorRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler
Warnung vor Verzögerungen bei der Spiegelreplikation(ocumEvtSnapMirrorRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Resynchronisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler
Synchrone Replikation nicht synchron *(syncSnapmirrorRelationshipOutofsync)	Risiko	SnapMirror Beziehung	Warnung
Synchrone Replikation wiederhergestellt *(syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror Beziehung	Informationen
Automatische Resynchronisierung der synchronen Replikation fehlgeschlagen *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risiko	SnapMirror Beziehung	Fehler
Ontap Mediator wurde dem Cluster hinzugefügt (snapmirrorMediatorAdded)	Ereignis	Cluster	Informationen
Ontap Mediator wird aus dem Cluster entfernt (snapmirrorMediatorRemoved)	Ereignis	Cluster	Informationen
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorUnreachable)	Risiko	Mediator	Warnung
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorMisconfigured)	Risiko	Mediator	Fehler
Die Ontap Mediator Connectivity wurde wiederhergestellt, ist erneut synchronisiert und bereit für die aktive SnapMirror Synchronisierung (snapmirrorMediatorInQuorum)	Ereignis	Mediator	Informationen

Informationen zu Ereignissen der asynchronen Spiegelung und der Vault Beziehung in Active IQ Unified Manager

Ereignisse für Asynchronous Mirror- und Vault-Beziehungen liefern Ihnen Informationen über den Status Ihrer Asynchronous SnapMirror- und Vault-Beziehungen, sodass Sie potenzielle Probleme überwachen können. Ereignisse für Asynchronous Mirror- und Vault-Beziehungen werden sowohl für Volume- als auch für Storage VM-Schutzbeziehungen unterstützt. Nur Vault-Beziehungen werden für die Storage VM-Notfallwiederherstellung nicht unterstützt. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Auswirkungsstufe, Quelltyp und Schweregrad.

Wirkungsbereich: Schutz

Die Ereignisse für SnapMirror und Vault Beziehungen werden auch für Storage VMs generiert, die durch Storage VM Disaster Recovery geschützt sind, jedoch nicht für Beziehungen zwischen Teilobjekten.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Asynchrone Spiegelung und Vault fehlerhaft(ocumEvtMirrorVaultRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Asynchroner Mirror und Vault abgebrochen(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Spiegelung und Vault Initialisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Mirror- und Vault-Aktualisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchroner Spiegelungs- und Vault Verzögerungsfehler(ocumEvtMirrorVaultRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnung vor Verzögerungen bei asynchronem Spiegeln und Vault (ocumEvtMirrorVaultRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung
Asynchrone Spiegelung und Vault-Resynchronisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler

Das Ereignis "SnapMirror update failure" wird vom Active IQ Portal (Config Advisor) ausgelöst.

Informationen zu Snapshot-Ereignissen in Active IQ Unified Manager

Snapshot-Ereignisse liefern Informationen zum Status von Snapshots und ermöglichen so die Überwachung der Snapshots auf potenzielle Probleme. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Impact Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Automatische Snapshot-Löschung deaktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Automatische Snapshot Löschung aktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Snapshot Auto-delete-Konfiguration geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen

Informationen zu SnapVault Beziehung Ereignissen in Active IQ Unified Manager

SnapVault Beziehungsereignisse liefern Ihnen Informationen über den Status Ihrer SnapVault Beziehungen, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Asynchroner Vault-Fehler(ocumEvtSnapVaultRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Asynchrones Vault unterbrochen(ocumEvtSnapVaultRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Vault-Initialisierung fehlgeschlagen(ocumEvtSnapVaultRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Vault Aktualisierung fehlgeschlagen(ocumEvtSnapVaultRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchroner Vault-Verzögerungsfehler(ocumEvtSnapVaultRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler
Warnung vor asynchroner Vault-Verzögerung(ocumEvtSnapVaultRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung
Asynchrone Vault Resynchronisierung fehlgeschlagen(ocumEvtSnapvaultRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler

Informationen zu Ereignissen bei Storage-Failover-Einstellungen in Active IQ Unified Manager

Ereignisse zu den Storage Failover Einstellungen (SFO) liefern Ihnen Informationen darüber, ob Ihr Storage Failover deaktiviert oder nicht konfiguriert ist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und umfassen den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage Failover Interconnect: Eine oder mehrere Verbindungen ausgefallen(ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risiko	Node	Warnung
Storage Failover deaktiviert(ocumEvtSfoSettingsDisabled)	Risiko	Node	Fehler
Storage Failover nicht konfiguriert(ocumEvtSfoSettingsNotConfigured)	Risiko	Node	Fehler
Storage Failover Status - Übernahme(ocumEvtSfoStateTakeover)	Risiko	Node	Warnung
Storage Failover Status - Teilweise Rückgabe(ocumEvtSfoStatePartialGiveback)	Risiko	Node	Fehler
Storage Failover Node-Status ausgefallen(ocumEvtSfoNodeStatusDown)	Risiko	Node	Fehler
Storage Failover Übernahme nicht möglich(ocumEvtSfoTakeoverNotPossible)	Risiko	Node	Fehler

Informationen zu Speicherdienstereignissen in Active IQ Unified Manager

Storage Services Ereignisse liefern Ihnen Informationen zur Erstellung und zum Abonnement von Storage Services, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage Service erstellt(Nicht zutreffend)	Ereignis	Speicherservice	Informationen
Storage Service abonniert(nicht zutreffend)	Ereignis	Speicherservice	Informationen
Storage Service abgemeldet(Nicht zutreffend)	Ereignis	Speicherservice	Informationen

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Unerwartete Löschung der verwalteten SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Risiko	Speicherservice	Warnung
Unerwartete Löschung eines Speicherdienstmitglieds-Volumes(ocumEvtStorageServiceUnexpectedVolumeDeletion)	Vorfall	Speicherservice	Kritisch

Informationen zu Storage Shelf Ereignissen in Active IQ Unified Manager

Storage Shelf Ereignisse zeigen an, ob Ihr Storage Shelf Anomalien aufweist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Abnormaler Spannungsbereich(ocumEvtShelfVoltageAbnormal)	Risiko	Storage Shelf	Warnung
Abnormaler Strombereich(ocumEvtShelfCurrentAbnormal)	Risiko	Storage Shelf	Warnung
Abnormale Temperatur(ocumEvtShelfTemperatureAbnormal)	Risiko	Storage Shelf	Warnung

Informationen zu Storage VM Ereignissen in Active IQ Unified Manager

Ereignisse für Storage VM (storage virtual machine, auch als SVM bezeichnet) liefern Ihnen Informationen zum Status Ihrer Storage VMs (SVMs), sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

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

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage VM CIFS-Service ausgefallen(ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS Service nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Informationen
Versuche, eine nicht vorhandene CIFS-Freigabe zu verbinden *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch
CIFS NetBIOS Namenskonflikt *(nbladeCifsNbNameConflict)	Risiko	SVM	Fehler
CIFS Shadow Copy Vorgang fehlgeschlagen *(cifsShadowCopyFailure)	Risiko	SVM	Fehler
Viele CIFS-Verbindungen *(nbladeCifsManyAuths)	Risiko	SVM	Fehler
Maximale Anzahl CIFS-Verbindungen überschritten *(nbladeCifsMaxOpenSameFile)	Risiko	SVM	Fehler
Maximale Anzahl der CIFS-Verbindungen pro Benutzer überschritten *(nbladeCifsMaxSessPerUsrConn)	Risiko	SVM	Fehler
SVM FC/FCoE-Service ausgefallen(ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM iSCSI Service ausgefallen(ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
NFS-Service der Storage VM ausgefallen(ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM FC/FCoE-Service nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
SVM iSCSI Service nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen
SVM NFS-Dienst nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen
Storage VM gestoppt(ocumEvtVserverDown)	Risiko	SVM	Warnung
AV Server ist zu ausgelastet, um neue Scan-Anfragen anzunehmen *(nbladeVscanConnBackPressure)	Risiko	SVM	Fehler
Keine AV-Server-Verbindung für Virenscan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Risiko	SVM	Fehler
Keine reagierende AV-Serververbindung *(nbladeVscanConnInactive)	Ereignis	SVM	Informationen
Unbefugter Benutzerzugriffsversuch auf den AV-Server *(nbladeVscanBadUserPrivAccess)	Risiko	SVM	Fehler
Virus vom AV-Server gefunden *(nbladeVscanVirusDetected)	Risiko	SVM	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
SVM gefunden(Nicht zutreffend)	Ereignis	SVM	Informationen
SVM gelöscht(Nicht zutreffend)	Ereignis	Cluster	Informationen
SVM umbenannt(Nicht zutreffend)	Ereignis	SVM	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für SVM IOPS überschritten(ocumSvmIopsIncident)	Vorfall	SVM	Kritisch
SVM IOPS-Warnschwelle überschritten(ocumSvmIopsWarning)	Risiko	SVM	Warnung
SVM MB/s Kritischer Schwellenwert 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 Latenzwarnungsschwelle überschritten(ocumSvmLatencyWarning)	Risiko	SVM	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Audit-Protokoll deaktiviert(ocumVserverAuditLogDisabled)	Risiko	SVM	Warnung
Anmeldebanner deaktiviert(ocumVserverLoginBannerDisabled)	Risiko	SVM	Warnung
SSH verwendet unsichere Cipher(ocumVserverSSHInsecure)	Risiko	SVM	Warnung
Anmeldebanner geändert(ocumVserverLoginBannerChanged)	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage VM ist deaktiviert (antiRansomwareSvmStateDisabled)	Risiko	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Überwachung von Storage VMs mit Anti-Ransomware ist aktiviert (Lernmodus) (antiRansomwareSvmStateDryrun)	Ereignis	SVM	Informationen
Storage VM geeignet für die Überwachung von Anti-Ransomware (Lernmodus) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Informationen

Informationen zu Benutzer- und Gruppenkontingentereignissen in Active IQ Unified Manager

Ereignisse zu Benutzer- und Gruppenkontingenten liefern Ihnen Informationen über die Kapazität der Benutzer- und Gruppenkontingente sowie über Datei- und Festplattenlimits, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Benutzer- oder Gruppenkontingent: Soft-Limit für Speicherplatz überschritten(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Hartes Speicherplatzlimit für Benutzer- oder Gruppenkontingente erreicht(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch
Soft-Limit für die Dateianzahl des Benutzer- oder Gruppenkontingents überschritten(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Hartes Limit der Dateianzahl für Benutzer- oder Gruppenkontingent erreicht(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch

Informationen zu Volume-Ereignissen in Active IQ Unified Manager

Volume-Ereignisse liefern Informationen über den Status von Volumes und ermöglichen so die Überwachung potenzieller Probleme. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Level, Quelltyp und Schweregrad.

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

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume beschränkt(ocumEvtVolumeRestricted)	Risiko	Volumen	Warnung
Volume offline (ocumEvtVolumeOffline)	Vorfall	Volumen	Kritisch
Volume teilweise verfügbar(ocumEvtVolumePartiallyAvailable)	Risiko	Volumen	Fehler
Volume nicht eingehängt(nicht zutreffend)	Ereignis	Volumen	Informationen
Volume gemountet (nicht zutreffend)	Ereignis	Volumen	Informationen
Volume erneut eingehängt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volumenverbindungspfad inaktiv(ocumEvtVolumeJunctionPathInactive)	Risiko	Volumen	Warnung
Automatische Volumengrößenanpassung aktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Autosize deaktiviert (nicht zutreffend)	Ereignis	Volumen	Informationen

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Maximale Kapazität der automatischen Volume Größenanpassung geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Inkrementgröße für Volume Autosize geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Gefährdeter Speicherplatz eines Thin-Provisioned Volume(ocumThinProvisionVolumeSpaceAtRisk)	Risiko	Volumen	Warnung
Fehler bei der Volumeneffizienzoperation(ocumEvtVolumeEfficiencyOperationError)	Risiko	Volumen	Fehler
Volume-Speicher voll(ocumEvtVolumeFull)	Risiko	Volumen	Fehler
Volume Speicherplatz nahezu voll(ocumEvtVolumeNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Volume voll *(volumeLogicalSpaceFull)	Risiko	Volumen	Fehler
Logischer Speicherplatz des Volume nahezu voll *(volumeLogicalSpaceNearlyFull)	Risiko	Volumen	Warnung
Logischer Volume-Speicherplatz normal *(volumeLogicalSpaceAllOK)	Ereignis	Volumen	Informationen
Volume Snapshot Reserve-Speicherplatz voll (ocumEvtSnapshotFull)	Risiko	Volumen	Warnung
Zu viele Snapshot-Kopien(ocumEvtSnapshotTooMany)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume-Qtree-Quota überzeichnet (ocumEvtVolumeQtreeQuotaOvercommitted)	Risiko	Volumen	Fehler
Volume Qtree Quota fast überbelegt(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risiko	Volumen	Warnung
Anomale Wachstumsrate des Volumens(ocumEvtVolumeGrowthRateAbnormal)	Risiko	Volumen	Warnung
Volume Tage bis voll(ocumEvtVolumeDaysUntilFullSoon)	Risiko	Volumen	Fehler
Volume Speicherplatzgarantie deaktiviert(nicht anwendbar)	Ereignis	Volumen	Informationen
Speicherplatzgarantie für Volumes aktiviert(nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Space Guarantee geändert(nicht zutreffend)	Ereignis	Volumen	Informationen
Tage bis zur vollständigen Füllung der Volume Snapshot Reserve(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risiko	Volumen	Fehler
FlexGroup Bestandteile haben Platzprobleme *(flexGroupConstituentsHaveSpaceIssues)	Risiko	Volumen	Fehler
FlexGroup Status des Speicherplatzes aller Bestandteile OK *(flexGroupConstituentsSpaceStatusAllOK)	Ereignis	Volumen	Informationen
FlexGroup Konstituenten haben Inode-Probleme *(flexGroupConstituentsHaveInodesIssues)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
FlexGroup Konstituenten Inodes Status Alle OK *(flexGroupConstituentsInodesStatusAllOK)	Ereignis	Volumen	Informationen
WAFL Volume AutoSize Fehler *(waflVolAutoSizeFail)	Risiko	Volumen	Fehler
WAFL Volume AutoSize abgeschlossen *(waflVolAutoSizeDone)	Ereignis	Volumen	Informationen
FlexGroup Volume ist zu über 80 % ausgelastet*	Vorfall	Volumen	Fehler
FlexGroup Volume ist zu mehr als 90 % ausgelastet*	Vorfall	Volumen	Kritisch
Anomalie der Storage-Effizienz des Volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risiko	Volumen	Warnung
Volume Snapshot Reserve Unterauslastung (volumeSnaphotReserveUnderutilizedWarning)	Ereignis	Volumen	Warnung
Unzureichende Auslastung der Volume Snapshot Reserve (volumeSnaphotReserveUnderutilizedCleared)	Ereignis	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume umbenannt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume erkannt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume gelöscht(Nicht zutreffend)	Ereignis	Volumen	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS Volume Max IOPS Warnschwelle überschritten(ocumQosVolumeMaxIopsWarning)	Risiko	Volumen	Warnung
QoS Volume Max MB/s Warnschwelle überschritten(ocumQosVolumeMaxMbpsWarning)	Risiko	Volumen	Warnung
QoS Volume Max IOPS/TB Warnschwelle überschritten(ocumQosVolumeMaxIopsPerTbWarning)	Risiko	Volumen	Warnung
Der in der Performance Service Level Policy definierte Schwellenwert für die Latenz des Workload-Volumes wurde überschritten (ocumConformanceLatencyWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-IOPS überschritten(ocumVolumeIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für die Volume IOPS-Warnung überschritten(ocumVolumeIopsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Datenvolumen in 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
Warnschwelle für Volumenlatenz überschritten(ocumVolumeLatencyWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für die Cache-Miss-Rate des Volumens überschritten(ocumVolumeCacheMissRatioIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für die Warnung zur Volume Cache Miss Ratio überschritten(ocumVolumeCacheMissRatioWarning)	Risiko	Volumen	Warnung
Kritische Schwellenwerte für Volumenlatenz und IOPS überschritten(ocumVolumeLatencyIopsIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und IOPS überschritten(ocumVolumeLatencyIopsWarning)	Risiko	Volumen	Warnung
Volume-Latenz und kritischer MB/s-Schwellenwert überschritten(ocumVolumeLatencyMbpsIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und MB/s überschritten(ocumVolumeLatencyMbpsWarning)	Risiko	Volumen	Warnung
Volume Latenz und verwendete Aggregate Performance Capacity: Kritischer Schwellenwert überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volumenlatenz und genutzte aggregierte Performance-Kapazität überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und Aggregatauslastung überschritten(ocumVolumeLatencyAggregateUtilizationIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volumenlatenz und Knotenkapazität für die genutzte Performance überschritten(ocumVolumeLatencyNodePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und genutzte Node-Performance-Kapazität überschritten(ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Volume-Latenz und verwendete Knoten-Performance-Kapazität - kritischer Schwellenwert für Takeover überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	Volumen	Kritisch
Volumenlatenz und genutzte Knoten-Performance-Kapazität - Schwellenwert für die Übernahmewarnung überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	Volumen	Warnung

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

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anti-Ransomware-Überwachung des Volume ist aktiviert (aktiver Modus) (antiRansomwareVolumeStateEnabled)	Ereignis	Volumen	Informationen
Die Überwachung des Volumens mit Anti-Ransomware ist deaktiviert (antiRansomwareVolumeStateDisabled)	Risiko	Volumen	Warnung
Die Anti-Ransomware-Überwachung des Volumes ist aktiviert (Lernmodus) (antiRansomwareVolumeStateDryrun)	Ereignis	Volumen	Informationen
Die Überwachung des Volumens mit Anti-Ransomware ist pausiert (Lernmodus) (antiRansomwareVolumeStateDryrunPaused)	Risiko	Volumen	Warnung
Die Anti-Ransomware-Überwachung des Volumes ist pausiert (Aktiver Modus) (antiRansomwareVolumeStateEnablePaused)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anti-Ransomware-Überwachung des Volumes wird deaktiviert (antiRansomwareVolumeStateDisableInProgress)	Risiko	Volumen	Warnung
Ransomware-Aktivität festgestellt (callHomeRansomwareActivitySeen)	Vorfall	Volumen	Kritisch
Volume geeignet für die Anti-Ransomware-Überwachung (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Volumen	Informationen
Für die Anti-Ransomware-Überwachung geeignetes Volume (Aktivmodus) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risiko	Volumen	Warnung
Volume weist übermäßig viele Anti-Ransomware-Warnungen auf (antiRansomwareFeatureNoisyVolume)	Risiko	Volumen	Warnung

Wirkungsbereich: Datenschutz

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

Informationen zu Statusereignissen bei Volume Moves in Active IQ Unified Manager

Statusereignisse für Volume Verschiebungen informieren Sie über den Status Ihrer Volume Verschiebung, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und

Trap-Namen, das Auswirkungs Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Status der Volume Verschiebung: In Bearbeitung(Nicht zutreffend)	Ereignis	Volumen	Informationen
Status der Volume-Verschiebung - Fehlgeschlagen(ocumEvtVolumeMoveFailed)	Risiko	Volumen	Fehler
Status der Volumenverschiebung: Abgeschlossen(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Move - Umstellung verschoben(ocumEvtVolumeMoveCutoverDeferred)	Risiko	Volumen	Warnung

Beschreibung von Ereignisfenstern und Dialogfeldern

Informationen zur Benachrichtigungsseite in Active IQ Unified Manager

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 gesendet werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

E-Mail

In diesem Bereich ist die Konfiguration der folgenden E-Mail-Einstellungen für Warnungsbenachrichtigungen möglich:

- **Absenderadresse**

  Gibt die E-Mail-Adresse an, von der die Warnungsbenachrichtigung gesendet wird. Dieser Wert wird auch als Absenderadresse für einen Bericht verwendet, wenn dieser freigegeben wird. Wenn die Absenderadresse mit „ActiveIQUnifiedManager@localhost.com“ vorbelegt ist, sollte sie in eine gültige, funktionsfähige E-Mail-Adresse geändert werden, damit 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, mit dem die Warnbenachrichtigung an die angegebenen Empfänger gesendet wird.

- **Benutzername**

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

- **Passwort**

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

- **Port**

  Gibt den Port an, den der SMTP-Hostserver zum Senden von Warnmeldungen verwendet.

  Der Standardwert ist 25.

- **START/TLS verwenden**

  Durch Aktivieren dieses Kontrollkästchens erfolgt die sichere Kommunikation zwischen dem SMTP-Server und dem Management-Server mithilfe der TLS/SSL-Protokolle (auch bekannt als start_tls und StartTLS).

- **SSL verwenden**

  Wenn dieses Kontrollkästchen aktiviert ist, erfolgt die sichere Kommunikation zwischen dem SMTP-Server und dem Management-Server über das SSL-Protokoll.

SNMP

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

- **Version**

  Legt die gewünschte SNMP-Version je nach Sicherheitsanforderung fest. Zur Auswahl stehen 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 Management-Server gesendeten SNMP-Traps empfängt. Mehrere Trap-Ziele können angegeben werden, indem die einzelnen Hosts durch Kommas getrennt werden.

  > Alle anderen SNMP-Einstellungen, wie z. B. „Version“ und „Outbound Port“, müssen für alle Hosts in der Liste gleich sein.

- **Ausgehender Trap Port**

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

  Der Standardwert ist 162.

- **Gemeinschaft**

  Die Community-String für den Zugriff auf den Host.

- **Engine-ID**

  Gibt die eindeutige Kennung des SNMP-Agenten an und wird automatisch vom Management-Server generiert. Die Engine-ID ist in 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**

  Legt das Protokoll zur Benutzerauthentifizierung fest. Zu den Protokolloptionen gehören MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist in SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungskennwort**

  Gibt das Passwort an, das zur Authentifizierung eines Benutzers verwendet wird. Das Authentifizierungspasswort ist in SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzprotokoll**

  Legt das Datenschutzprotokoll für die Verschlüsselung von SNMP-Nachrichten fest. 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.

- **Datenschutzpasswort**

  Gibt das Passwort bei Verwendung des Datenschutzprotokolls an. Das Datenschutzpasswort ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Weitere Informationen zu SNMP-Objekten und -Traps können Sie die "Active IQ Unified Manager MIB" von der NetApp Support Site herunterladen.

Informationen zur Inventarseite für die Ereignisverwaltung in Active IQ Unified Manager

Die Bestandsseite von Event Management ermöglicht Ihnen die Anzeige einer Liste der aktuellen Ereignisse und ihrer Eigenschaften. Sie können Aufgaben wie das Bestätigen, Beheben und Zuweisen von Ereignissen ausführen. Außerdem können Sie für bestimmte Ereignisse eine Warnung hinzufügen.

Die Informationen auf dieser Seite aktualisieren sich alle 5 Minuten automatisch, damit die aktuellsten neuen Ereignisse angezeigt werden.

Filterkomponenten

Damit lassen sich die in der Ereignisliste angezeigten Informationen anpassen. Sie können die Liste der angezeigten Ereignisse mithilfe der folgenden Komponenten verfeinern:

- Menü „Ansicht“ zum Auswählen aus einer vordefinierten Liste von Filteroptionen.

  Dies umfasst Elemente wie alle aktiven (neuen und bestätigten) Ereignisse, aktive Performance Ereignisse, mir (dem angemeldeten Benutzer) zugewiesene Ereignisse und alle während sämtlicher Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Ereignisliste durch Eingabe vollständiger oder teilweiser Begriffe.
- Schaltfläche „Filter“, die den Filterbereich öffnet, in dem Sie aus allen verfügbaren Feldern und Feldattributen auswählen können, um die Ereignisliste einzugrenzen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Zuweisen an**

  Hiermit können Sie den Benutzer auswählen, dem das Ereignis zugewiesen wird. Wenn Sie einem Benutzer ein Ereignis zuweisen, erscheinen der Benutzername und der Zeitpunkt der Zuweisung in der Ereignisliste für die ausgewählten Ereignisse.

  - Mich

    Weist das Ereignis dem aktuell angemeldeten Benutzer zu.

  - Ein anderer Benutzer

    Es wird das Dialogfeld „Besitzer zuweisen“ angezeigt, in dem Sie das Ereignis anderen Benutzern zuweisen oder erneut zuweisen können. Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Feld „Besitzer“ leer lassen.

- **Bestätigen**

  Bestätigt die ausgewählten Ereignisse.

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

  Information Ereignisse können nicht quittiert werden.

- **Als gelöst markieren**

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

  Wenn Sie ein Ereignis beheben, werden Ihr Benutzername und der Zeitpunkt der Behebung in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie eine Korrekturmaßnahme für das Ereignis ergriffen haben, müssen Sie das Ereignis als behoben markieren.

- **Warnung hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem Sie Warnungen für die ausgewählten Ereignisse hinzufügen können.

- **Berichte**

Ermöglicht den Export von Details der aktuellen Ereignisansicht in eine Datei mit kommagetrennten Werten (.csv) oder ein PDF-Dokument.

- **Spaltenauswahl ein-/ausblenden**

  Ermöglicht die Auswahl der auf der Seite angezeigten Spalten sowie ihrer Anzeigereihenfolge.

Ereignisliste

Zeigt Details aller Ereignisse geordnet nach Auslösezeitpunkt an.

Standardmäßig wird die Ansicht „Alle aktiven Ereignisse“ angezeigt, um die neuen und quittierten Ereignisse der letzten sieben Tage mit dem Impact Level „Vorfall“ oder „Risiko“ anzuzeigen.

- **Auslösezeit**

  Der Zeitpunkt, zu dem das Ereignis ausgelöst wurde.

- **Schweregrad**

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

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Behoben oder Veraltet.

- **Auswirkungslevel**

  Der Auswirkungs-Level des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Auswirkungsbereich**

  Der Wirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration oder Sicherheit.

- **Name**

  Der Name des Ereignisses. Durch Auswählen des Namens wird die Seite mit den Ereignisdetails für dieses Ereignis angezeigt.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist. Die Auswahl des Namens zeigt die Seite mit den Systemstatus- oder Performance-Details für dieses Objekt an.

  Bei einem Verstoß gegen eine gemeinsame QoS-Richtlinie wird in diesem Feld nur das Workload-Objekt angezeigt, das die meisten IOPS oder MB/s verbraucht. Weitere Workloads, die diese Richtlinie verwenden, werden auf der Seite mit den Ereignisdetails angezeigt.

- **Quellentyp**

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

- **Zugewiesen an**

  Der Name des Benutzers, dem das Ereignis zugewiesen ist.

- **Ereignisursprung**

  Unabhängig davon, ob das Ereignis vom "Active IQ Portal" oder direkt von "Active IQ Unified Manager" stammt.

- **Anmerkungsname**

  Der Name der Annotation, die dem Storage Objekt zugewiesen ist.

- **Anmerkungen**

  Die Anzahl der für ein Ereignis hinzugefügten Notizen.

- **Ausstehende Tage**

  Die Anzahl der Tage seit der erstmaligen Generierung des Ereignisses.

- **Zugewiesene Zeit**

  Die seit der Zuweisung des Ereignisses an einen Benutzer verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem 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 seit der Bestätigung des Ereignisses verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis bestätigt wurde.

- **Gelöst durch**

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

- **Zeitpunkt der Behebung**

  Die seit der Behebung des Ereignisses verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis behoben wurde.

- **Zeitpunkt der Außerkraftsetzung**

  Der Zeitpunkt, an dem der Status des Ereignisses zu Obsolete wurde.

Seite mit Ereignisdetails

Informationen zur Seite „Ereignisdetails“ in Active IQ Unified Manager

Auf der Seite mit den Ereignisdetails lassen sich die Details eines ausgewählten Ereignisses anzeigen, z. B. der Schweregrad des Ereignisses, das Auswirkungs-Level, der Auswirkungsbereich und die Ereignisquelle. Außerdem lassen sich zusätzliche Informationen zu möglichen Korrekturmaßnahmen zur Behebung des Problems anzeigen.

- **Ereignisname**

  Der Name des Ereignisses und der Zeitpunkt, zu dem das Ereignis zuletzt beobachtet wurde.

  Bei nicht auf die Performance bezogenen Ereignissen sind die Informationen zum letzten Auftreten nicht bekannt, solange sich das Ereignis im Status „Neu“ oder „Bestätigt“ befindet, und werden daher ausgeblendet.

- **Ereignisbeschreibung**

  Eine kurze Beschreibung des Ereignisses.

  In einigen Fällen enthält die Ereignisbeschreibung einen Grund für das Auslösen des Ereignisses.

- **Komponente in Konflikt**

  Bei dynamischen Performance-Ereignissen werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente in einem Konflikt steht, ist ihr Symbol eingekreist und rot hervorgehoben.

  Eine Beschreibung der hier angezeigten Komponenten ist unter *Cluster-Komponenten und warum sie in Konflikt geraten können* verfügbar.

Beschreibungen der Abschnitte Ereignisinformationen, Systemdiagnose und Vorgeschlagene Maßnahmen finden sich in anderen Themen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Notizen-Symbol**

  Ermöglicht es Ihnen, eine Notiz zum Ereignis hinzuzufügen oder zu aktualisieren sowie alle von anderen Benutzern hinterlassenen Notizen einzusehen.

Aktionsmenü

- **Mir zuweisen**

  Ordnet Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Besitzer zuweisen“, über das sich das Ereignis anderen Benutzern zuweisen oder neu zuweisen lässt.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Name des Benutzers und der Zeitpunkt der Zuweisung in die Ereignisliste für die ausgewählten Ereignisse aufgenommen.

  Die Zuweisung von Ereignissen kann auch aufgehoben werden, indem das Feld „Eigentümer“ leer gelassen wird.

- **Bestätigen**

  Bestätigung der ausgewählten Ereignisse, damit keine wiederholten Alarmbenachrichtigungen mehr eingehen.

Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und der Zeitpunkt der Bestätigung in der Ereignisliste (Bestätigt von) für die ausgewählten Ereignisse angezeigt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für dessen Verwaltung.

- **Als gelöst markieren**

  Ermöglicht es Ihnen, den Ereignisstatus in Resolved zu ändern.

  Wenn Sie ein Ereignis beheben, werden Ihr Benutzername und der Zeitpunkt, zu dem Sie das Ereignis behoben haben, in der Ereignisliste (Behoben von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie eine Korrekturmaßnahme für das Ereignis ergriffen haben, müssen Sie das Ereignis als behoben markieren.

- **Warnung hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Informationen über den Abschnitt „Ereignisinformationen“ in Active IQ Unified Manager

Im Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ finden Sie Details zu einem ausgewählten Ereignis, z. B. den Schweregrad, das Auswirkungs-Level, den Auswirkungsbereich und die Ereignisquelle.

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

- **Zeitpunkt der Ereignisauslösung**

  Der Zeitpunkt, zu dem das Ereignis ausgelöst wurde.

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Behoben oder Veraltet.

- **Veraltete Ursache**

  Die Maßnahmen, die dazu führten, dass das Ereignis als veraltet markiert wurde, beispielsweise die Behebung des Problems.

- **Ereignisdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen ist dies die Zeitspanne zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis zuletzt analysiert wurde. Bei veralteten Ereignissen ist dies die Zeitspanne zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis gelöst wurde.

  Dieses Feld erscheint bei allen Performance-Ereignissen und bei anderen Ereignistypen erst, nachdem sie behoben wurden oder veraltet sind.

- **Zuletzt gesehen**

  Datum und Uhrzeit, zu der das Ereignis zuletzt als aktiv erkannt wurde.

  Bei Performance Ereignissen kann dieser Wert aktueller sein als der Auslösezeitpunkt des Ereignisses, da dieses Feld nach jeder neuen Erfassung von Performance Daten 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.

- **Schweregrad**

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

- **Auswirkungslevel**

  Der Auswirkungs-Level des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Auswirkungsbereich**

  Der Wirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration oder Sicherheit.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis stattgefunden hat.

  Bei der Anzeige der Details eines gemeinsam genutzten QoS-Richtlinienereignisses werden in diesem Feld bis zu drei der Workload-Objekte aufgelistet, die die meisten IOPS oder MBps verbrauchen.

  Über den Link mit dem Quellnamen lässt sich die Detailseite zum Systemstatus oder zur Performance dieses Objekts aufrufen.

- **Quellenanmerkungen**

  Zeigt den Namen und den Wert der Annotation für das Objekt an, dem das Ereignis zugeordnet ist.

  Dieses Feld wird nur bei Systemstatusereignissen auf Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

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

  Dieses Feld wird nur bei Systemstatusereignissen auf Clustern, SVMs und Volumes angezeigt.

- **Quellentyp**

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

- **Im Cluster**

  Der Name des Clusters, auf dem das Ereignis stattfand.

  Sie können auf den Link mit dem Clusternamen klicken, um die Detailseite für den Systemstatus oder die Performance dieses Clusters anzuzeigen.

- **Anzahl der betroffenen Objekte**

  Die Anzahl der von dem Ereignis betroffenen Objekte.

  Über den Objektlink lässt sich die Inventarseite anzeigen, die mit den Objekten gefüllt ist, die aktuell von diesem Ereignis betroffen sind.

Dieses Feld wird nur für Performance-Ereignisse angezeigt.

- **Betroffene Volumina**

  Die Anzahl der von diesem Ereignis betroffenen Bände.

  Dieses Feld wird nur für Performance Ereignisse auf Knoten oder Aggregaten angezeigt.

- **Ausgelöste Richtlinie**

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgelöst hat.

  Wenn sich der Mauszeiger über dem Richtliniennamen befindet, sind die Details der Schwellenwertrichtlinie zu sehen. Bei adaptiven QoS-Richtlinien werden außerdem die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener oder belegter Speicherplatz) angezeigt.

  Dieses Feld wird nur für Performance-Ereignisse angezeigt.

- **Regel-ID**

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

- **Bestätigt von**

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

- **Behoben durch**

  Name der Person, die den Vorfall gelöst hat, und Zeitpunkt der Lösung des Vorfalls.

- **Zugewiesen an**

  Der Name der Person, die mit der Bearbeitung des Ereignisses beauftragt ist.

- **Warnungseinstellungen**

  Die folgenden Informationen zu Warnmeldungen werden angezeigt:

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

    Sie können das Dialogfeld „Warnung hinzufügen“ durch Klicken auf den Link öffnen.

  - 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.

  - Falls dem ausgewählten Ereignis mehrere Warnmeldungen zugeordnet sind, wird die Anzahl der Warnmeldungen angezeigt.

    Die Seite „Alert Setup“ kann über den Link geöffnet werden, über den weitere Details zu diesen Warnmeldungen angezeigt werden.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung gesendet**

  Datum und Uhrzeit, zu der die letzte Warnmeldung versendet wurde.

- **Versand per**

  Der Mechanismus, mit dem die Warnmeldung gesendet wurde: E-Mail oder SNMP-Trap.

- **Vorheriger Skriptlauf**

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

Informationen zu empfohlenen Aktionen in Active IQ Unified Manager

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite mit den Ereignisdetails bietet mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit das Ereignis selbst behoben werden kann. Die empfohlenen Maßnahmen sind auf die Art des Ereignisses oder auf die Art des Schwellenwerts zugeschnitten, der überschritten wurde.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen enthält die Seite **Hilfe**-Links mit weiterführenden Informationen zu vielen vorgeschlagenen Aktionen, einschließlich Anleitungen zur Durchführung bestimmter Aktionen. Einige dieser Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools erfordern.

Die hier vorgeschlagenen Maßnahmen sollten nur als Orientierungshilfe bei der Behebung dieses Ereignisses betrachtet werden. Die Maßnahmen, die Sie zur Behebung dieses Ereignisses ergreifen, sollten sich nach den Gegebenheiten Ihrer Umgebung richten.

Für eine detailliertere Analyse von Objekt und Ereignis steht die Schaltfläche **Analyze Workload** zur Verfügung, über die die Seite Workload Analysis angezeigt wird.

Bestimmte Ereignisse kann Unified Manager umfassend diagnostizieren und eine einzelne Lösung bereitstellen. Sofern verfügbar, werden diese Lösungen mit einer Schaltfläche **Fix It** angezeigt. Mit dieser Schaltfläche behebt Unified Manager das Problem, das das Ereignis verursacht.

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

Informationen zur Systemdiagnose in Active IQ Unified Manager

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

Dieser Bereich wird nur bei einigen Ereignissen angezeigt.

Einige Performance Ereignisse liefern Diagramme, die für das jeweils ausgelöste Ereignis relevant sind. Dazu gehören in der Regel ein IOPS- oder MB/s-Diagramm sowie ein Latenzdiagramm für die vorangegangenen zehn Tage. In dieser Anordnung lässt sich erkennen, welche Storage Komponenten die Latenz am stärksten beeinflussen oder von der Latenz betroffen sind, wenn das Ereignis aktiv ist.

Bei dynamischen Performance-Ereignissen werden folgende Diagramme angezeigt:

- Workload-Latenz - Zeigt den Verlauf der Latenz für die wichtigsten Opfer-, Bully- oder Shark-Workloads an der Komponente mit Ressourcenkonflikt an.
- Workload-Aktivität - Zeigt Details zur Workload-Nutzung der Clusterkomponente bei Ressourcenkonflikten an.
- Ressourcenaktivität - Anzeige historischer Performance Statistiken für die Clusterkomponente im Engpass.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten um Ressourcen konkurrieren.

Andere Ereignisse liefern eine kurze Beschreibung der Art der Analyse, die das System für das Storage Objekt durchführt. In manchen Fällen gibt es bei systemdefinierten Performance-Richtlinien, die mehrere Performance-Zähler analysieren, eine oder mehrere Zeilen, eine für jede analysierte Komponente. In diesem Szenario zeigt ein grünes oder rotes Symbol neben der Diagnose an, ob in dieser bestimmten Diagnose ein Problem gefunden wurde oder nicht.

Informationen zur Seite „Ereigniseinrichtung“ in Active IQ Unified Manager

Die Seite „Ereigniseinstellungen“ zeigt die Liste der deaktivierten Ereignisse an und bietet Informationen wie den zugehörigen Objekttyp und den Schweregrad des Ereignisses. Sie können auch Aufgaben wie das globale Deaktivieren oder Aktivieren von Ereignissen ausführen.

Auf diese Seite kann nur zugegriffen werden, wenn Sie die Rolle „Application Administrator“ oder „Storage Administrator“ haben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen lassen sich für ausgewählte Ereignisse folgende Aufgaben ausführen:

- **Deaktivieren**

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

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **Upload-Regeln**

  Das Dialogfeld „Upload Rules“ wird geöffnet, über das Standorte ohne externen Netzwerkzugriff die Active IQ Regeldatei manuell in Unified Manager hochladen können. Die Regeln werden auf Cluster AutoSupport Meldungen angewendet, um Ereignisse für Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeit gemäß den Definitionen der Active IQ Plattform zu generieren.

- **EMS-Ereignisse abonnieren**

  Öffnet das Dialogfeld „EMS-Ereignisse abonnieren“, über das Sie bestimmte Ereignisse des Event Management System (EMS) von den Clustern abonnieren können, die Sie überwachen. Das EMS erfasst Informationen über Ereignisse, die im Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis eingeht, wird ein Unified Manager Ereignis mit dem entsprechenden Schweregrad generiert.

Listenansicht

Die Listenansicht zeigt (in Tabellenform) Informationen zu deaktivierten Ereignissen an. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen.

- **Ereignis**

  Zeigt den Namen des deaktivierten Ereignisses an.

- **Schweregrad**

  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 wurde.

Das Dialogfeld „Ereignisse“ in Active IQ Unified Manager wird deaktiviert

Im Dialogfeld „Ereignisse deaktivieren“ wird die Liste der Ereignistypen angezeigt, für die Sie Ereignisse deaktivieren können. Sie können Ereignisse für einen Ereignistyp auf Grundlage eines bestimmten Schweregrads oder für eine Gruppe von Ereignissen deaktivieren.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Bereich „Ereigniseigenschaften“

Der Bereich „Ereigniseigenschaften“ enthält die folgenden Ereigniseigenschaften:

- **Ereignisschweregrad**

  Ermöglicht die Auswahl von Ereignissen anhand des Typs des Schweregrads, der Kritisch, Fehler, Warnung oder Information sein kann.

- **Ereignisname enthält**

  Ermöglicht das Filtern von Ereignissen, deren Name die angegebenen Zeichen enthält.

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem von Ihnen angegebenen Typ des Schweregrads des Ereignisses und dem Text-String entsprechen.

- **Ereignisse deaktivieren**

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

  Der Schweregrad des Ereignisses wird auch zusammen mit dem Ereignisnamen angezeigt.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie für die ausgewählten Ereignisse folgende Aufgaben ausführen:

- **Speichern und schließen**

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Benachrichtigungen verwalten

Informationen zu Warnmeldungen in Active IQ Unified Manager

Obwohl Ereignisse kontinuierlich auftreten, generiert der Unified Manager nur dann eine Warnung, wenn ein Ereignis festgelegte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnungen generiert werden sollen—beispielsweise, wenn ein Speicherplatzschwellenwert überschritten wird oder ein Objekt offline geht. Sie können eine Warnung auch mit einem Skript verknüpfen, das beim Auslösen einer Warnung ausgeführt wird.

Zu den Filterkriterien gehören Objektklasse, Name oder Ereignisschweregrad.

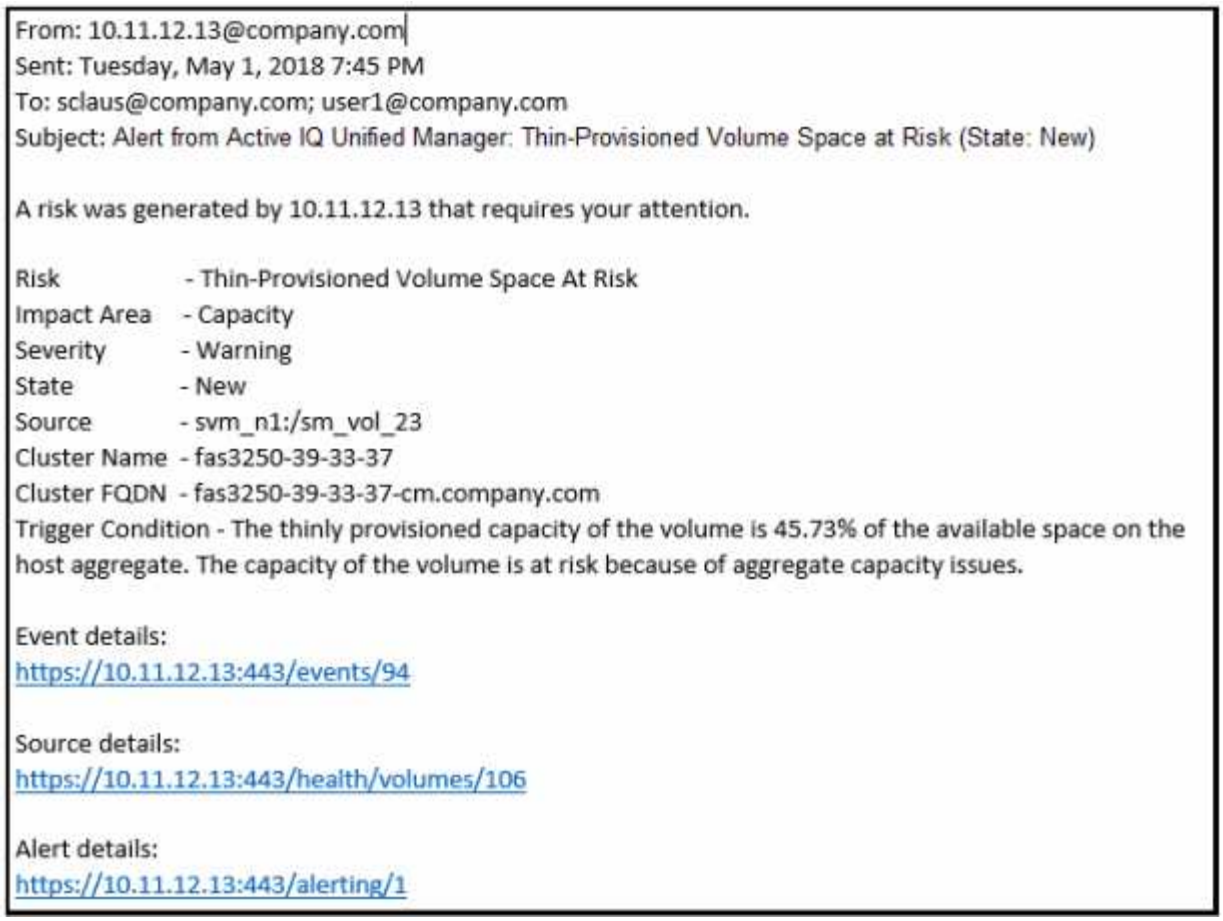
Informationen in einer Active IQ Unified Manager Benachrichtigungs-E-Mail

Unified Manager Benachrichtigungs-E-Mails enthalten den Typ des Ereignisses, den Schweregrad des Ereignisses, den Namen der Richtlinie oder des Schwellenwerts, deren bzw. dessen Überschreitung das Ereignis verursacht hat, sowie eine Beschreibung des Ereignisses. Die E-Mail-Nachricht enthält außerdem für jedes Ereignis einen Hyperlink, über den sich die Detailseite des Ereignisses in der UI anzeigen lässt.

Alle Benutzer, die den Erhalt von Alerts abonniert haben, erhalten Benachrichtigungs-E-Mails.

Wenn sich ein Performance-Zähler oder ein Kapazitätswert während eines Erfassungszeitraums stark ändert, kann dies dazu führen, dass gleichzeitig ein kritisches und ein Warnereignis für dieselbe Schwellenwertrichtlinie ausgelöst werden. In diesem Fall erhalten Sie möglicherweise eine E-Mail für das Warnereignis und eine weitere für das kritische Ereignis. Dies liegt daran, dass Unified Manager es Ihnen ermöglicht, Benachrichtigungen für Warn- und kritische Schwellenwertüberschreitungen separat zu abonnieren.

Nachfolgend ist ein Beispiel für eine Benachrichtigungs-E-Mail dargestellt:



Benachrichtigungen hinzufügen

Hinzufügen von Benachrichtigungen in Active IQ Unified Manager

Sie können Warnmeldungen so konfigurieren, dass Sie benachrichtigt werden, wenn ein bestimmtes Ereignis generiert wird. Sie können Warnmeldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse eines bestimmten Typs des Schweregrads konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und der Warnmeldung ein Skript zuordnen.

Bevor Sie beginnen

- Es müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, der SMTP-Server und der SNMP-Trap-Host konfiguriert sein, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Benachrichtigung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn ein Skript basierend auf dem Ereignis ausgeführt werden soll, muss das Skript zuvor über die Seite „Skripte“ zu Unified Manager hinzugefügt worden sein.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Es besteht die Möglichkeit, eine Benachrichtigung direkt auf der Seite „Ereignisdetails“ nach dem Empfang eines Ereignisses zu erstellen, zusätzlich zur Erstellung einer Benachrichtigung über die Seite „Benachrichtigungseinrichtung“, wie hier beschrieben.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.
3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. **Ressourcen** auswählen und die Ressourcen bestimmen, die in die Benachrichtigung einbezogen oder von ihr ausgeschlossen werden.

   Ein Filter kann festgelegt werden, indem im Feld **Name enthält** ein Text-String angegeben wird, um eine Gruppe von Ressourcen auszuwählen. Basierend auf dem angegebenen Text-String werden in der Liste der verfügbaren Ressourcen nur die Ressourcen angezeigt, die der Filterregel entsprechen. Der angegebene Text-String ist Groß-/Kleinschreibungs-empfindlich.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und die Warnung wird für Ereignisse, die sich auf die ausgeschlossene Ressource beziehen, nicht generiert.

5. Auf **Ereignisse** klicken und die Ereignisse anhand des Ereignisnamens oder des Typs des Schweregrads auswählen, für die ein Alarm ausgelöst werden soll.

   Um mehr als ein Ereignis auszuwählen, die Strg-Taste gedrückt halten, während die Auswahl getroffen wird.

6. Auf **Aktionen** klicken, die Benutzer auswählen, die benachrichtigt werden sollen, die Benachrichtigungshäufigkeit festlegen, auswählen, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und ein Skript zuweisen, das ausgeführt wird, wenn eine Warnung generiert wird.

   Wenn die für den Benutzer angegebene E-Mail-Adresse geändert und die Benachrichtigung erneut zum Bearbeiten geöffnet wird, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert wurde, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

   Alternativ ist es möglich, die Benutzer auch über SNMP-Traps zu benachrichtigen.

7. Auf **Speichern** klicken.

Beispiel für das Hinzufügen einer Benachrichtigung

Dieses Beispiel zeigt, wie eine Benachrichtigung erstellt wird, die die folgenden Anforderungen erfüllt:

- Name der Warnung: HealthTest
- Ressourcen: Umfasst alle Volumes, deren Name „abc“ enthält, und schließt alle Volumes aus, deren Name „xyz“ enthält.
- Ereignisse: umfasst alle kritischen Gesundheitsereignisse
- Aktionen: Enthält "sample@domain.com", ein "Test" Skript und der Benutzer muss alle 15 Minuten benachrichtigt werden

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

1. Nach Auswahl von **Name** erfolgt die Eingabe von **`HealthTest`** in das Feld **Alert Name**.

2. **Ressourcen** auswählen und im Tab „Einschließen“ **Volumes** aus der Dropdown-Liste wählen.
   a. Die Eingabe von **`abc`** in das Feld **Name enthält** zeigt die Volumes an, deren Name "abc" enthält.
   b. **<<All Volumes whose name contains 'abc'>>** im Bereich „Verfügbare Ressourcen“ auswählen und in den Bereich „Ausgewählte Ressourcen“ verschieben.
   c. Nach Auswahl von **Ausschließen** ist **`xyz`** in das Feld **Name enthält** einzugeben; anschließend ist **Hinzufügen** auszuwählen.
3. Auf **Ereignisse** klicken und im Feld **Ereignisschweregrad Kritisch** auswählen.
4. Im Bereich „Übereinstimmende Ereignisse“ **Alle kritischen Ereignisse** auswählen und in den Bereich „Ausgewählte Ereignisse“ verschieben.
5. Unter **Aktionen** im Feld „Diese Benutzer benachrichtigen“ **`sample@domain.com`** eingeben.
6. **Alle 15 Minuten erinnern** benachrichtigt den Benutzer alle 15 Minuten.

   Sie können eine Benachrichtigung so konfigurieren, dass sie über einen festgelegten Zeitraum wiederholt an die Empfänger gesendet wird. Es sollte der Zeitpunkt festgelegt werden, ab dem die Ereignisbenachrichtigung für die Benachrichtigung aktiv ist.
7. Im Menü „Auszuführendes Skript auswählen“ das Skript **Test** auswählen.
8. Auf **Speichern** klicken.

Richtlinien zum Hinzufügen von Warnmeldungen in Active IQ Unified Manager

Sie können Warnungen basierend auf einer Ressource, z. B. einem Cluster, Knoten, Aggregat oder Volume, sowie auf Ereignissen eines bestimmten Typs des Schweregrads hinzufügen. Es empfiehlt sich, eine Warnung für jedes Ihrer kritischen Objekte hinzuzufügen, nachdem Sie den Cluster hinzugefügt haben, zu dem das Objekt gehört.

Mithilfe der folgenden Richtlinien und Überlegungen lassen sich Warnmeldungen erstellen, um Ihre Systeme effektiv zu managen:

- Alarmbeschreibung

  Sie sollten eine Beschreibung für die Warnmeldung angeben, damit Sie Ihre Warnmeldungen effektiv nachverfolgen können.

- Ressourcen

  Sie sollten entscheiden, für welche physische oder logische Ressource eine Warnung erforderlich ist. Ressourcen können nach Bedarf ein- oder ausgeschlossen werden. Wenn beispielsweise Aggregate durch die Konfiguration einer Warnung genau überwacht werden sollen, müssen die erforderlichen Aggregate aus der Ressourcenliste ausgewählt werden.

  Wenn Sie eine Ressourcenkategorie auswählen, zum Beispiel **<<All User or Group Quotas>>**, dann erhalten Sie Warnmeldungen für alle Objekte in dieser Kategorie.

> Die Auswahl eines Clusters als Ressource wählt die Storage Objekte innerhalb dieses Clusters nicht automatisch aus. Wenn Sie beispielsweise eine Warnung für alle kritischen Ereignisse für alle Cluster erstellen, erhalten Sie nur Warnungen für kritische Cluster-Ereignisse. Sie erhalten keine Warnungen für kritische Ereignisse auf Knoten, Aggregaten usw.

- Schweregrad

  Sie legen fest, ob ein Ereignis eines bestimmten Typs des Schweregrads (Kritisch, Fehler, Warnung) die Warnung auslösen soll und, falls ja, welcher Typ des Schweregrads.

- Ausgewählte Ereignisse

  Wenn Sie eine Warnmeldung basierend auf dem Typ des generierten Ereignisses hinzufügen, sollten Sie entscheiden, welche Ereignisse eine Warnmeldung erfordern.

  Wenn Sie einen Ereignisschweregrad auswählen, aber keine einzelnen Ereignisse auswählen (wenn Sie die Spalte „Ausgewählte Ereignisse“ leer lassen), erhalten Sie Benachrichtigungen für alle Ereignisse in der Kategorie.

- Aktionen

  Sie müssen die Benutzernamen und E-Mail-Adressen der Benutzer angeben, die die Benachrichtigung erhalten. Sie können auch einen SNMP-Trap als Benachrichtigungsmodus festlegen. Sie können Ihre Skripte mit einer Warnung verknüpfen, sodass sie ausgeführt werden, wenn eine Warnung generiert wird.

- Benachrichtigungshäufigkeit

  Sie können einen Alert so konfigurieren, dass für einen festgelegten Zeitraum wiederholt Benachrichtigungen an die Empfänger gesendet werden. Sie sollten den Zeitpunkt festlegen, ab dem die Ereignisbenachrichtigung für den Alert aktiv ist. Wenn die Ereignisbenachrichtigung wiederholt werden soll, bis das Ereignis bestätigt wird, sollten Sie festlegen, wie oft die Benachrichtigung wiederholt werden soll.

- Skript ausführen

  Sie können Ihr Skript mit einer Warnung verknüpfen. Ihr Skript wird ausgeführt, wenn die Warnung generiert wird.

Hinzufügen von Warnmeldungen für Leistungsereignisse in Active IQ Unified Manager

Sie können Benachrichtigungen für einzelne Performance-Ereignisse genauso konfigurieren wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Wenn Sie außerdem alle Performance-Ereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Benachrichtigung erstellen, die Sie informiert, sobald kritische oder Warnungs-Performance-Ereignisse ausgelöst werden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das folgende Beispiel zeigt, wie ein Ereignis für alle kritischen Latenz-, IOPS- und MBps-Ereignisse erstellt wird. Mit derselben Methode können Ereignisse aus allen Performance-Zählern und für alle Warnereignisse ausgewählt werden.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.

3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. Auf der Seite **Ressourcen** werden keine Ressourcen ausgewählt.

   Da keine Ressourcen ausgewählt sind, gilt die Warnung für alle Cluster, Aggregate, Volumes usw., für die diese Ereignisse empfangen werden.

5. Nach Auswahl von **Events** können die folgenden Aktionen durchgeführt werden:
   a. In der Liste „Ereignisschweregrad“ erfolgt die Auswahl von **Kritisch**.
   b. Im Feld „Ereignisname enthält“ können Sie `latency` eingeben und anschließend auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
   c. Im Feld „Ereignisname enthält“ `iops` eingeben und anschließend auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
   d. Im Feld „Ereignisname enthält“ können Sie `mbps` eingeben und dann auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
6. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
7. Auf dieser Seite können Sie alle weiteren Optionen für das Senden von SNMP-Traps und das Ausführen eines Skripts konfigurieren.
8. Auf **Speichern** klicken.

Warnungen in Active IQ Unified Manager testen

Sie können eine Warnung testen, um zu überprüfen, ob Sie sie korrekt konfiguriert haben. Wenn ein Ereignis ausgelöst wird, wird eine Warnung generiert, und eine Warnungs-E-Mail wird an die konfigurierten Empfänger gesendet. Mithilfe der Testwarnung können Sie überprüfen, ob die Benachrichtigung gesendet wird und ob Ihr Skript ausgeführt wird.

Bevor Sie beginnen

- Die Benachrichtigungseinstellungen wie die E-Mail-Adresse der Empfänger, der SMTP-Server und der SNMP-Trap müssen konfiguriert sein.

  Der Unified Manager Server kann diese Einstellungen verwenden, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.

- Sie müssen ein Skript zugewiesen und dieses so konfiguriert haben, dass es ausgeführt wird, wenn die Warnung generiert wird.
- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alert Setup** können Sie den Alert auswählen, der getestet werden soll, und anschließend auf **Test** klicken.

   An die E-Mail-Adressen, die Sie beim Erstellen der Warnung angegeben haben, wird eine Test-E-Mail für Warnungen gesendet.

Benachrichtigungen für gelöste und veraltete Ereignisse in Active IQ Unified Manager deaktivieren

Für alle Ereignisse, für die Sie Benachrichtigungen konfiguriert haben, wird eine Benachrichtigung versendet, wenn diese Ereignisse alle verfügbaren Status durchlaufen: Neu, Erledigt und Veraltet. Wenn Sie keine Benachrichtigungen für Ereignisse erhalten möchten, die in die Status Erledigt und Veraltet wechseln, können Sie eine globale Einstellung konfigurieren, um diese Benachrichtigungen zu unterdrücken.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Standardmäßig werden keine Warnmeldungen für Ereignisse gesendet, wenn diese in den Status „Resolved“ oder „Obsolete“ wechseln.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Benachrichtigungseinstellungen** steht neben dem Element **Benachrichtigungen für behobene und veraltete Ereignisse** ein Schieberegler zur Verfügung, mit dem eine der folgenden Aktionen ausgeführt werden kann:

Zu…	Folgendes ist zu tun…
Benachrichtigungen nicht mehr senden, sobald Ereignisse behoben oder veraltet sind	Den Schieberegler nach links bewegen
Versand von Warnmeldungen, sobald Ereignisse behoben oder obsolet sind	Den Schieberegler nach rechts bewegen

Ausschluss von Ziel-Volumes für die Notfallwiederherstellung von der Generierung von Warnmeldungen in Active IQ Unified Manager

Bei der Konfiguration von Volume-Warnungen können Sie im Warndialogfeld eine Zeichenfolge angeben, die ein Volume oder eine Gruppe von Volumes identifiziert. Wenn Sie jedoch die Notfallwiederherstellung für SVMs konfiguriert haben, haben Quell- und Zielvolume denselben Namen, sodass Sie Warnungen für beide Volumes erhalten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können Warnmeldungen für Disaster-Recovery-Ziel-Volumes deaktivieren, indem Sie Volumes ausschließen, die den Namen der Ziel-SVM tragen. Dies ist möglich, da die Kennung für Volume-Ereignisse sowohl den SVM-Namen als auch den Volume-Namen im Format "<svm_name>:/<volume_name>" enthält.

Das folgende Beispiel zeigt, wie Warnungen für das Volume "vol1" auf der primären SVM "vs1" erstellt werden können, wobei die Generierung der Warnung für ein Volume mit demselben Namen auf der SVM "vs1-dr" ausgeschlossen wird.

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

Schritte

1. Unter **Name** lassen sich ein Name und eine Beschreibung für die Warnung eingeben.
2. Nach dem Klick auf **Ressourcen** können Sie die Registerkarte **Einschließen** auswählen.
   a. Nach Auswahl von **Volume** in der Dropdown-Liste ist **`vol1`** in das Feld **Name enthält** einzugeben, damit die Volumes angezeigt werden, deren Name "vol1" enthält.
   b. Sie wählen **<<All Volumes whose name contains 'vol1'>>** im Bereich **Verfügbare Ressourcen** aus und verschieben es in den Bereich **Ausgewählte Ressourcen**.
3. Die Registerkarte **Ausschließen** auswählen, **Volume** auswählen, **`vs1-dr`** in das Feld **Name enthält** eingeben und anschließend auf **Hinzufügen** klicken.

   Dadurch wird verhindert, dass für das Volume "vol1" auf der SVM "vs1-dr" eine Warnung generiert wird.
4. Nach dem Klicken auf **Events** können Sie das Ereignis bzw. die Ereignisse auswählen, das bzw. die Sie auf das Volume bzw. die Volumes anwenden möchten.
5. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
6. Auf dieser Seite können alle weiteren Optionen zum Ausgeben von SNMP-Traps und zum Ausführen eines Skripts konfiguriert werden; anschließend kann **Speichern** ausgewählt werden.

Anzeigen von Warnmeldungen in Active IQ Unified Manager

Auf der Seite „Alert Setup“ können Sie die Liste der für verschiedene Ereignisse erstellten Warnmeldungen einsehen. Dort finden Sie auch Eigenschaften der Warnmeldungen wie die Beschreibung, die Benachrichtigungsmethode und -häufigkeit, die Ereignisse, die die Warnmeldung auslösen, die E-Mail-Empfänger der Warnmeldungen sowie betroffene Ressourcen wie Cluster, Aggregate und Volumes.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritt

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.

   Die Liste der Warnmeldungen wird auf der Seite „Benachrichtigungseinrichtung“ angezeigt.

Benachrichtigungen in Active IQ Unified Manager bearbeiten

Sie können Alarmeigenschaften bearbeiten, wie z. B. die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Empfänger, Benachrichtigungsoptionen, Benachrichtigungshäufigkeit und zugehörige Skripte.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alert Setup** die zu bearbeitende Benachrichtigung auswählen und auf **Edit** klicken.
3. Im Dialogfeld **Warnung bearbeiten** können Sie die Abschnitte Name, Ressourcen, Ereignisse und Aktionen nach Bedarf bearbeiten.

Sie können das mit der Warnung verknüpfte Skript ändern oder entfernen.

4. Auf **Speichern** klicken.

Warnmeldungen in Active IQ Unified Manager löschen

Sie können eine Warnung löschen, wenn sie nicht mehr benötigt wird. Beispielsweise können Sie eine Warnung löschen, die für eine bestimmte Ressource erstellt wurde, wenn diese Ressource nicht mehr von Unified Manager überwacht wird.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Benachrichtigungseinstellungen** die zu löschenden Benachrichtigungen auswählen und auf **Löschen** klicken.
3. Mit **Ja** wird die Löschanfrage bestätigt.

Beschreibung von Warnfenstern und Dialogfeldern

Informationen zur Seite „Warnungseinrichtung“ in Active IQ Unified Manager

Die Seite „Alert Setup“ zeigt eine Liste der Warnmeldungen an und bietet Informationen zum Namen, Status, zur Benachrichtigungsmethode und zur Benachrichtigungshäufigkeit der Warnmeldung. Auf dieser Seite können außerdem Warnmeldungen hinzugefügt, bearbeitet, entfernt, aktiviert oder deaktiviert werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Befehlsschaltflächen

- **Hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem neue Warnungen hinzugefügt werden können.

- **Bearbeiten**

  Das Dialogfeld „Warnung bearbeiten“ wird angezeigt, in dem ausgewählte Warnungen bearbeitet werden können.

- **Löschen**

  Ausgewählte Warnmeldungen löschen.

- **Aktivieren**

  Ermöglicht das Versenden von Benachrichtigungen für die ausgewählten Alarme.

- **Deaktivieren**

Deaktiviert die ausgewählten Warnmeldungen, wenn Benachrichtigungen vorübergehend nicht gesendet werden sollen.

- **Test**

  Dient zur Überprüfung der Konfiguration der ausgewählten Warnmeldungen nach dem Hinzufügen oder Bearbeiten.

- **Benachrichtigungen über behobene und veraltete Ereignisse**

  Damit lässt sich festlegen, ob Benachrichtigungen gesendet werden, wenn Ereignisse in die Status „Behoben“ oder „Veraltet“ verschoben werden. Dies kann dazu beitragen, dass Benutzer keine unnötigen Benachrichtigungen erhalten.

Listenansicht

Die Listenansicht zeigt Informationen zu den erstellten Warnmeldungen in tabellarischer Form an. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen. Außerdem können Sie eine Warnmeldung auswählen, um im Detailbereich weitere Informationen dazu anzuzeigen.

- **Status**

  Gibt an, ob eine Warnung aktiviert ( ) oder deaktiviert ( ) ist.

- **Alarm**

  Zeigt den Namen der Warnung an.

- **Beschreibung**

  Zeigt eine Beschreibung der Warnung an.

- **Benachrichtigungsmethode**

  Zeigt die für die Warnung ausgewählte Benachrichtigungsmethode an. Sie können Benutzer per E-Mail oder SNMP-Traps benachrichtigen.

- **Benachrichtigungshäufigkeit**

  Legt die Häufigkeit (in Minuten) fest, mit der der Verwaltungsserver weiterhin Benachrichtigungen sendet, bis das Ereignis bestätigt oder behoben ist oder den Status „Veraltet“ erhält.

Detailbereich

Der Detailbereich enthält weitere Informationen zur ausgewählten Warnung.

- **Alarmname**

  Zeigt den Namen der Warnung an.

- **Warnungsbeschreibung**

  Zeigt eine Beschreibung der Warnung an.

- **Ereignisse**

Zeigt die Ereignisse an, für die Sie eine Benachrichtigung auslösen möchten.

- **Ressourcen**

  Zeigt die Ressourcen an, für die die Warnmeldung ausgelöst werden soll.

- **Beinhaltet**

  Zeigt die Ressourcengruppe an, für die die Warnung ausgelöst werden soll.

- **Ausgenommen**

  Zeigt die Gruppe von Ressourcen an, für die Sie keine Warnung auslösen möchten.

- **Benachrichtigungsmethode**

  Anzeige der Benachrichtigungsmethode für die Warnung.

- **Benachrichtigungshäufigkeit**

  Zeigt an, wie häufig der Managementserver weiterhin Warnmeldungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „Obsolete“ verschoben wird.

- **Skriptname**

  Zeigt den Namen des Skripts an, das mit der ausgewählten Warnung verknüpft ist. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

- **E-Mail-Empfänger**

  Zeigt die E-Mail-Adressen der Benutzer an, die die Warnungsbenachrichtigung erhalten.

Informationen zum Dialogfeld „Warnung hinzufügen“ in Active IQ Unified Manager

Sie können Warnmeldungen erstellen, die Sie benachrichtigen, wenn ein bestimmtes Ereignis generiert wird, sodass Sie das Problem schnell beheben und die Auswirkungen auf Ihre Umgebung minimieren können. Sie können Warnmeldungen für eine einzelne Ressource oder eine Gruppe von Ressourcen sowie für Ereignisse eines bestimmten Typs des Schweregrads erstellen. Außerdem können Sie die Benachrichtigungsmethode und -häufigkeit der Warnmeldungen festlegen.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Name

In diesem Bereich können Sie einen Namen und eine Beschreibung für die Warnmeldung angeben:

- **Alarmname**

  Damit können Sie einen Alert-Namen angeben.

- **Warnungsbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

Ressourcen

In diesem Bereich können Sie einzelne Ressourcen auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die eine Warnung ausgelöst werden soll. Eine dynamische Regel ist die Menge an Ressourcen, die anhand des von Ihnen angegebenen Text-Strings gefiltert wird. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen, oder Sie können den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

Wenn Sie eine Benachrichtigung auf einer der Detailseiten eines Storage Objekts erstellen, wird das Storage Objekt automatisch in die Benachrichtigung aufgenommen.

- **Enthalten**

  Ermöglicht das Einschließen der Ressourcen, für die Warnungen ausgelöst werden sollen. Es kann ein Text-String angegeben werden, um Ressourcen zu gruppieren, die mit diesem String übereinstimmen, und diese Gruppe kann für die Warnung eingeschlossen werden. Beispielsweise können alle Volumes gruppiert werden, deren Name den String „abc“ enthält.

- **Ausschließen**

  Ermöglicht das Ausschließen von Ressourcen, für die keine Warnmeldungen ausgelöst werden sollen. Beispielsweise können Sie alle Volumes ausschließen, deren Name die Zeichenfolge „xyz“ enthält.

  Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen: zum Beispiel <<All Volumes>> oder <<All Volumes whose name contains 'xyz'>>.

  Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und für das Ereignis wird keine Warnung generiert.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie die Warnmeldungen erstellen möchten. Sie können Warnmeldungen für Ereignisse auf der Grundlage eines bestimmten Schweregrads oder für eine Reihe von Ereignissen erstellen.

Um mehr als ein Ereignis auszuwählen, sollten Sie während der Auswahl die Strg-Taste gedrückt halten.

- **Ereignisschweregrad**

  Damit können Sie Ereignisse anhand des Typs des Schweregrads auswählen, der Kritisch, Fehler oder Warnung sein kann.

- **Ereignisname enthält**

  Ermöglicht die Auswahl von Ereignissen, deren Name bestimmte Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benutzer festlegen, die benachrichtigt werden sollen, wenn ein Alarm ausgelöst wird. Außerdem können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit festlegen.

- **Benachrichtigung dieser Benutzer**

Damit können Sie die E-Mail-Adresse oder den Benutzernamen des Benutzers angeben, der Benachrichtigungen erhalten soll.

Wenn Sie die für den Benutzer hinterlegte E-Mail-Adresse ändern und die Benachrichtigung erneut zum Bearbeiten öffnen, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

- **Benachrichtigungshäufigkeit**

  Ermöglicht es Ihnen, die Häufigkeit festzulegen, mit der der Management-Server Benachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „veraltet“ verschoben wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung mit einer festgelegten Häufigkeit
  - Benachrichtigung mit einer festgelegten Häufigkeit innerhalb des angegebenen Zeitraums

- **SNMP-Trap senden**

  Durch Aktivieren dieses Kontrollkästchens können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht das Hinzufügen Ihres benutzerdefinierten Skripts zur Warnung. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, wurde die Funktionalität von Ihrem Administrator deaktiviert. Bei Bedarf kann diese Funktionalität unter **Storage Management** > **Feature Settings** aktiviert werden.

Befehlsschaltflächen

- **Speichern**

  Erstellt eine Warnung und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Bearbeiten der Alarmeigenschaften in Active IQ Unified Manager

Sie können Alarmeigenschaften wie die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Skripte und Benachrichtigungsoptionen bearbeiten.

Name

In diesem Bereich können Sie den Namen und die Beschreibung der Warnung bearbeiten.

- **Alarmname**

Ermöglicht die Bearbeitung des Alert-Namens.

- **Warnungsbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

- **Alarmzustand**

  Ermöglicht das Aktivieren oder Deaktivieren der Warnung.

Ressourcen

In diesem Bereich können Sie einzelne Ressourcen auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die Sie die Warnung auslösen möchten. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen, oder Sie können den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

- **Enthalten**

  Ermöglicht Ihnen, die Ressourcen einzubeziehen, für die Warnungen ausgelöst werden sollen. Sie können einen Text-String angeben, um Ressourcen zu gruppieren, die mit diesem String übereinstimmen, und diese Gruppe zur Aufnahme in die Warnung auswählen. Beispielsweise können Sie alle Volumes gruppieren, deren Name den String “vol0” enthält.

- **Ausschließen**

  Ermöglicht das Ausschließen von Ressourcen, für die keine Warnmeldungen ausgelöst werden sollen. Beispielsweise können alle Volumes ausgeschlossen werden, deren Name die Zeichenfolge „`xyz`“ enthält.

> Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen, zum Beispiel <<All Volumes>> oder <<All Volumes whose name contains 'xyz'>>.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Benachrichtigungen ausgelöst werden sollen. Sie können Benachrichtigungen für Ereignisse basierend auf einem bestimmten Schweregrad oder für eine Gruppe von Ereignissen auslösen.

- **Ereignisschweregrad**

  Damit können Sie Ereignisse anhand des Typs des Schweregrads auswählen, der Kritisch, Fehler oder Warnung sein kann.

- **Ereignisname enthält**

  Ermöglicht die Auswahl von Ereignissen, deren Name die angegebenen Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit festlegen.

- **Benachrichtigung dieser Benutzer**

  Hier können Sie die E-Mail-Adresse oder den Benutzernamen bearbeiten oder eine neue E-Mail-Adresse

oder einen neuen Benutzernamen angeben, um Benachrichtigungen zu erhalten.

- **Benachrichtigungshäufigkeit**

  Damit lässt sich die Häufigkeit bearbeiten, mit der der Management-Server Benachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „Veraltet“ verschoben wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung mit einer festgelegten Häufigkeit
  - Benachrichtigung mit einer festgelegten Häufigkeit innerhalb des angegebenen Zeitraums

- **SNMP-Trap senden**

  Damit können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht es Ihnen, ein Skript mit der Warnung zu verknüpfen. Dieses Skript wird beim Generieren einer Warnung ausgeführt.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Skripte managen

Skripte in Active IQ Unified Manager verwalten

Sie können Skripte verwenden, um mehrere Storage Objekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, führt Unified Manager das Skript aus. Sie können benutzerdefinierte Skripte hochladen und ihre Ausführung beim Erstellen einer Warnung testen.

Das Hochladen und Ausführen von Skripten in Unified Manager ist standardmäßig aktiviert. Falls Ihr Unternehmen diese Funktion aus Sicherheitsgründen nicht zulassen möchte, können Sie sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren.

Verwandte Informationen

"Aktivieren und Deaktivieren der Möglichkeit zum Hochladen von Skripten"

Wie Skripte mit Warnmeldungen in Active IQ Unified Manager funktionieren

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn in Unified Manager für ein Ereignis eine Warnung ausgelöst wird. Mithilfe der Skripte lassen sich Probleme mit Storage Objekten beheben oder die Storage Objekte identifizieren, die die Ereignisse generieren.

Wenn in Unified Manager eine Warnung für ein Ereignis generiert wird, wird eine Benachrichtigungs-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie einer Warnung ein Skript zugeordnet haben, wird das Skript ausgeführt. Die Details der an das Skript übergebenen Argumente sind in der Benachrichtigungs-E-Mail enthalten.

Wenn Sie ein benutzerdefiniertes Skript erstellt und es einer Warnung für einen bestimmten Ereignistyp zugeordnet haben, richten sich die Maßnahmen für diesen Ereignistyp nach Ihrem benutzerdefinierten Skript, und die **Fix it**-Aktionen sind standardmäßig auf der Seite „Management Actions“ oder im Unified Manager Dashboard nicht verfügbar.

Das Skript verwendet für die Ausführung die folgenden Argumente:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden sowie zugehörige Ereignisinformationen erfassen oder Storage Objekte ändern.

Beispiel für das Abrufen von Argumenten aus Skripten

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Wenn eine Warnmeldung generiert wird, führt das System dieses Skript aus, und die folgende Ausgabe wird angezeigt:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Skripte in Active IQ Unified Manager hinzufügen

Sie können in Unified Manager Skripte hinzufügen und diese mit Warnmeldungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnmeldung generiert wird, und ermöglichen es Ihnen, Informationen zu den Storage Objekten abzurufen, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte, die Sie dem Unified Manager Server hinzufügen möchten, erstellt und gespeichert haben.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell, Python und `.bat`Dateien.

Plattform, auf der Unified Manager installiert ist	Unterstützte Sprachen
VMware	Perl- und Shell-Skripte
Linux	Perl, Python und Shell Skripte
Windows	PowerShell, Perl-, Python- und .bat-Skripte

  - Für Perl Skripte muss Perl auf dem Unified Manager Server installiert sein. Bei VMware Installationen ist Perl 5 standardmäßig installiert, und die Skripte unterstützen nur die von Perl 5 unterstützten Funktionen. Wenn Perl nach Unified Manager installiert wurde, muss der Unified Manager Server neu gestartet werden.
  - Für PowerShell-Skripte muss auf dem Windows-Server die entsprechende PowerShell-Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

> Wenn Ihr Skript Protokolldateien erstellt, um den Fortschritt des Alarmskripts zu verfolgen, müssen Sie sicherstellen, dass sich die Protokolldateien nicht irgendwo im Unified Manager Installationsordner befinden.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung erfassen.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, wurde die Funktionalität von Ihrem Administrator deaktiviert. Bei Bedarf kann diese Funktionalität unter **Storage Management** > **Feature Settings** aktiviert werden.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** erfolgt die Auswahl von **Hinzufügen**.
3. Im Dialogfeld **Skript hinzufügen** wird mit **Durchsuchen** die Skriptdatei ausgewählt.
4. Geben Sie für das ausgewählte Skript eine Beschreibung ein.
5. Klicken Sie auf **Add**.

Verwandte Informationen

"Aktivieren und Deaktivieren der Möglichkeit zum Hochladen von Skripten"

Skripte in Active IQ Unified Manager löschen

Sie können ein Skript aus dem Unified Manager löschen, wenn das Skript nicht mehr benötigt wird oder ungültig ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Das Skript darf nicht mit einer Warnmeldung verknüpft sein.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** wählen Sie das Skript aus, das Sie löschen möchten, und klicken dann auf **Löschen**.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

Ausführung des Testskripts in Active IQ Unified Manager

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Storage-Objekt generiert wird.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen ein Skript im unterstützten Dateiformat in Unified Manager hochgeladen haben.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** können Sie Ihr Testskript hinzufügen.
3. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
4. Auf der Seite **Alert Setup** können Sie eine der folgenden Aktionen auswählen:

Zu…	Folgendes ist zu tun…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Add**. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.
Eine Warnmeldung bearbeiten	a. Eine Benachrichtigung auswählen und dann auf **Bearbeiten** klicken. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.

5. Auf **Speichern** klicken.
6. Auf der Seite **Alert Setup** den hinzugefügten oder geänderten Alarm auswählen und anschließend auf **Test** klicken.

   Das Skript wird mit dem Argument "-test" ausgeführt, und eine Benachrichtigungswarnung wird an die E-Mail-Adressen gesendet, die beim Erstellen der Warnung angegeben wurden.

Informationen zu den unterstützten Active IQ Unified Manager CLI Befehlen

Als Storage Administrator können Sie mithilfe der CLI-Befehle Abfragen für die Storage Objekte ausführen, beispielsweise für Cluster, Aggregate, Volumes, qtrees und LUNs. Sie können die CLI-Befehle auch verwenden, um die interne Datenbank von Unified Manager und die ONTAP Datenbank abzufragen. Darüber hinaus können Sie CLI-Befehle in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs ausgeführt werden oder wenn eine Warnung ausgelöst wird.

Allen Befehlen müssen der Befehl `um cli login` sowie ein gültiger Benutzername und ein gültiges Passwort für die Authentifizierung vorangestellt werden.

Zum Ausführen des Befehls *um run* benötigt Ihr Konto Zugriff auf die Applikation *console*.

CLI Befehl	Beschreibung	Ausgabe
`um cli login -u <username> [-p <password>]`	Dient zur Anmeldung an der CLI. Aus Sicherheitsgründen sollten Sie nach der Option „-u“ nur den Benutzernamen angeben. Bei dieser Verwendung werden Sie zur Eingabe des Passworts aufgefordert, und das Passwort wird weder im Verlauf noch in der Prozesstabelle erfasst. Die Sitzung läuft drei Stunden nach der Anmeldung ab; danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Meldet den Benutzer von der CLI ab.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle des ersten Levels an.	Zeigt alle Unterbefehle des ersten Levels an.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Wird hauptsächlich für Alarmskripte verwendet, um auf ONTAP einen Vorgang abzurufen oder auszuführen. Das optionale Argument Zeitüberschreitung legt ein maximales Zeitlimit (in Sekunden) fest, innerhalb dessen der Befehl auf dem Client abgeschlossen werden muss. Der Standardwert ist 0 (unbegrenzt warten).	Wie von ONTAP empfangen.

CLI Befehl	Beschreibung	Ausgabe
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen zulässig, die Daten aus der Datenbank lesen. Aktualisierungs-, Einfüge- oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in Tabellenform angezeigt. Bei einer leeren Ergebnismenge sowie bei Syntaxfehlern oder fehlerhaften Anfragen wird die entsprechende Fehlermeldung angezeigt.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der verwalteten Storage Systeme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Storage Systemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -u (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protokoll) gibt das Protokoll an, das für die Kommunikation mit dem Cluster verwendet wird (http oder https). Wird kein Protokoll angegeben, werden beide Protokolle versucht. Die Option -p (Port) gibt den Port an, der für die Kommunikation mit dem Cluster verwendet wird. Wird kein Port angegeben, wird der Standardwert des entsprechenden Protokolls versucht. Dieser Befehl kann nur vom storage admin ausgeführt werden.	Das System fordert den Benutzer auf, das Zertifikat zu akzeptieren, und gibt die entsprechende Meldung aus.
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Storage Systeme an.	Zeigt die folgenden Werte in Tabellenform an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle (Cluster) aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Dies ist eine Auflistung aller Optionen, die Sie mit dem Befehl „set“ konfigurieren können.	Zeigt die folgenden Werte in Tabellenform an: `Name, Value, Default Value, and Requires Restart.`

CLI Befehl	Beschreibung	Ausgabe
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Legt eine oder mehrere Optionen fest. Nur der Storage-Administrator kann den Befehl ausführen.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Unified Manager Softwareversion an.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Listet die LUNs nach dem Filtern nach dem angegebenen Objekt auf. -q ist für alle Befehle anwendbar, um keine Kopfzeile anzuzeigen. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um lun list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle LUNs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Listet die Storage VMs nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um svm list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Storage VMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `Name and Cluster ID.`

CLI Befehl	Beschreibung	Ausgabe
`um qtree list [-q] [ -ObjectType <object-id>]`	Listet die Qtrees nach dem Filtern nach dem angegebenen Objekt auf. Die Option `-q` ist für alle Befehle anwendbar, um keine Kopfzeile anzuzeigen. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um qtree list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Qtrees innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Listet die Datenträger nach dem Filtern anhand des angegebenen Objekts auf. ObjectType kann disk, aggr, node oder cluster sein. Beispiel: **`um disk list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an `ObjectType and object-id`.
`um cluster list [-q] [-ObjectType <object-id>]`	Listet die Cluster nach dem Filtern anhand des angegebenen Objekts auf. ObjectType kann disk, aggr, node, cluster, lun, qtree, volume, quota oder svm sein. Beispiel: **`um cluster list -aggr 1`** In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl zeigt den Cluster an, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte in Tabellenform an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`

CLI Befehl	Beschreibung	Ausgabe
`um cluster node list [-q] [-ObjectType <object-id>]`	Zeigt die Clusterknoten nach der Filterung auf das angegebene Objekt an. ObjectType kann disk, aggr, node oder cluster sein. Beispiel: **`um cluster node list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Knoten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann lun, qtree, cluster, volume, quota, svm oder aggregate sein. Beispiel: **`um volume list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes innerhalb des Clusters mit der ID 1 auf.	Die folgenden Werte werden in Tabellenform angezeigt `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann qtree, cluster, volume, quota oder svm sein. Beispiel: **`um quota user list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform `ID, Name, SID and Email`.

CLI Befehl	Beschreibung	Ausgabe
`um aggr list [-q] [-ObjectType <object-id>]`	Listet die Aggregate nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann disk, aggr, node, cluster oder volume sein. Beispiel: **`um aggr list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Die folgenden Werte werden in Tabellenform angezeigt `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Behebt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtert Ereignisse anhand von Quelle, Status und IDs.	Zeigt die folgenden Werte in Tabellenform an `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Stellt eine MySQL Datenbanksicherung mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.

Beschreibung der Skriptfenster und Dialogfelder

Informationen zur Seite „Skripte“ in Active IQ Unified Manager

Die Seite „Skripte“ ermöglicht es Ihnen, Ihre benutzerdefinierten Skripte zu Unified Manager hinzuzufügen. Sie können diese Skripte mit Warnmeldungen verknüpfen, um die automatische Neukonfiguration von Storage Objekten zu ermöglichen.

Auf der Seite „Skripte“ lassen sich Skripte in Unified Manager hinzufügen oder löschen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld „Skript hinzufügen“ an, in dem Skripte hinzugefügt werden können.

- **Löschen**

  Löscht das ausgewählte Skript.

Listenansicht

Die Listenansicht zeigt die Skripte, die Sie zu Unified Manager hinzugefügt haben, in Tabellenform an.

- **Name**

  Zeigt den Namen des Skripts an.

- **Beschreibung**

  Zeigt die Beschreibung des Skripts an.

Dialogfeld „Skript hinzufügen“ in Active IQ Unified Manager

Im Dialogfeld „Skript hinzufügen“ können Sie Skripte zu Unified Manager hinzufügen. Sie können Warnungen mit Ihren Skripten so konfigurieren, dass Ereignisse, die für Storage Objekte generiert werden, automatisch behoben werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

- **Auswahl der Skriptdatei**

  Ermöglicht die Auswahl eines Skripts für die Warnmeldung.

- **Beschreibung**

  Hier können Sie eine Beschreibung für das Skript angeben.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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