Verwalten von Ereignissen

Active IQ Unified Manager

NetApp
June 23, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager/events/concept_what_active_iq_platform_events_are.html on June 23, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten von Ereignissen . . . 1
Was sind die Active IQ Plattform-Ereignisse . . . 1
Die Ereignisse des Event Management-Systems sind . . . 1
EMS-Ereignisse, die automatisch dem Unified Manager hinzugefügt werden . . . 2
Abonnieren von ONTAP EMS-Veranstaltungen . . . 6
Was passiert, wenn ein Ereignis empfangen wird . . . 7
Anzeigen von Ereignissen und Ereignisdetails . . . 9
Anzeigen nicht zugewiesener Ereignisse . . . 9
Bestätigen und Beheben von Ereignissen . . . 9
Zuweisen von Ereignissen zu bestimmten Benutzern . . . 10
Deaktivieren unerwünschter Ereignisse . . . 11
Behebung von Problemen mithilfe der automatischen Problembehebung in Unified Manager . . . 12
Aktivieren und Deaktivieren der Active IQ-Ereignisberichterstellung . . . 13
Eine neue Datei für Active IQ-Regeln wird hochgeladen . . . 13
Generieren von Active IQ-Plattformereignissen . . . 14
Ereignisse auf der Active IQ Plattform werden aufgelöst . . . 14
Konfigurieren von Einstellungen für die Ereignisaufbewahrung . . . 15
Was für ein Unified Manager-Wartungsfenster ist . . . 15
Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen . . . 16
Ändern oder Abbrechen eines geplanten Wartungsfensters . . . 16
Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind . . . 17
Verwalten von Ressourcenereignissen des Host-Systems . . . 18
Allgemeines zu Ereignissen . . . 18
Definition des Ereignisstatus . . . 18
Beschreibung der Ereignistypen . . . 19
Beschreibung der Level der Ereignisauswirkungen . . . 20
Beschreibung der Bereiche für Ereignisauswirkungen . . . 21
Wie der Objektstatus berechnet wird . . . 21
Details des dynamischen Performance-Ereignidiagramms . . . 22
Von Unified Manager erkannte Konfigurationsänderungen . . . 23
Liste von Ereignissen und Schweregraden . . . 24
Aggregieren von Ereignissen . . . 24
Cluster-Ereignisse . . . 28
Festplatten-Ereignisse . . . 35
Gehäuse-Ereignisse . . . 35
Fan-Events . . . 36
Flash-Kartenereignisse . . . 37
Inodes-Events . . . 37
Ereignisse der Netzwerkschnittstelle (LIF) . . . 37
LUN-Ereignisse . . . 39
Management Station-Events . . . 44
Veranstaltungen auf der MetroCluster Bridge . . . 46
Veranstaltungen für MetroCluster-Konnektivität . . . 46

Ereignisse auf dem MetroCluster-Switch . . . 49
NVMe Namespace-Ereignisse . . . 50
Node-Ereignisse . . . 52
Ereignisse der NVRAM-Batterie . . . 57
Port-Ereignisse . . . 58
Netzteile . . . 59
Schutzereignisse . . . 59
Qtree Ereignisse . . . 60
Ereignisse des Service-Prozessors . . . 61
SnapMirror Beziehungsereignisse . . . 61
Ereignisse für asynchrone Spiegelung und Vault Beziehungen . . . 63
Snapshot Ereignisse . . . 65
SnapVault Beziehungsereignisse . . . 65
Ereignisse auf Storage-Failover-Einstellungen . . . 66
Ereignisse auf Storage-Services . . . 67
Storage-Shelf-Ereignisse . . . 68
Ereignisse von Storage-VM . . . 69
Ereignisse für Benutzer- und Gruppenkontingente . . . 73
Volume-Ereignisse . . . 74
Statusereignisse für Volume-Verschiebung . . . 85
Beschreibung der Ereignisfenster und Dialogfelder . . . 86
Benachrichtigungsseite . . . 86
Inventarseite des Ereignismanagements . . . 88
Seite mit den Veranstaltungsdetails . . . 91
Seite „Ereignis-Einrichtung“ . . . 97
Dialogfeld „Ereignisse deaktivieren“ . . . 98

Verwalten von Ereignissen

Ereignisse unterstützen Sie bei der Erkennung von Problemen in den überwachten Clustern.

Was sind die Active IQ Plattform-Ereignisse

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden durch Regelwerke gegen AutoSupport Meldungen erstellt, die von allen Storage-Systemen, die von Unified Manager überwacht werden, generiert werden.

Weitere Informationen finden Sie unter "Generieren von Active IQ-Plattformereignissen".

Unified Manager prüft automatisch auf eine neue Regeldatei und lädt nur eine neue Datei herunter, wenn neuere Regeln vorliegen. Bei Sites ohne externen Netzwerkzugriff müssen Sie die Regeln manuell von **Speicherverwaltung** > **Event-Setup** > **Upload-Regeln** hochladen.

Diese Active IQ Ereignisse überschneiden sich nicht mit bestehenden Unified Manager Ereignissen, und sie ermitteln Vorfälle oder Risiken bei Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeitsproblemen.

Weitere Informationen zum Aktivieren von Plattformereignissen finden Sie unter "Aktivieren von Active IQ Portal-Ereignissen". Weitere Informationen zum Hochladen der Regeldatei finden Sie unter "Eine neue Datei für Active IQ-Regeln wird hochgeladen".

NetApp Active IQ ist ein Cloud-basierter Service, der prädiktive Analysen und proaktiven Support bietet, um den Betrieb von Storage-Systemen in der gesamten NetApp Hybrid Cloud zu optimieren. Siehe "NetApp Active IQ" Finden Sie weitere Informationen.

Die Ereignisse des Event Management-Systems sind

Das Event Management System (EMS) sammelt Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und bietet Mechanismen zur Ereignisweiterleitung. Diese ONTAP Ereignisse können im Unified Manager als EMS-Ereignisse gemeldet werden. Die zentralisierte Überwachung und Verwaltung erleichtert die Konfiguration kritischer EMS-Ereignisse und Alarmbenachrichtigungen auf der Grundlage dieser EMS-Ereignisse.

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

Für den Empfang von EMS-Ereignissen in Unified Manager gibt es zwei Methoden:

- Eine bestimmte Anzahl wichtiger EMS-Ereignisse wird automatisch gemeldet.
- Sie können sich für den Erhalt einzelner EMS-Events anmelden.

Die EMS-Ereignisse, die durch Unified Manager generiert werden, werden abhängig von der Methode, in der das Ereignis generiert wurde, unterschiedlich berichtet:

Funktionalität	Automatische EMS-Nachrichten	Abonnierte EMS-Nachrichten
Verfügbare EMS-Events	Teilmenge der EMS-Ereignisse	Alle EMS-Ereignisse
EMS-Nachrichtenname bei Auslösung	Unified Manager Ereignisname (aus EMS-Ereignisname konvertiert)	Nicht spezifisch im Format „Error EMS received“. Die detaillierte Meldung liefert das Punktnotationsformat des tatsächlichen EMS-Ereignisses
Empfangene Nachrichten	Sobald das Cluster erkannt wurde	Nach dem Hinzufügen jedes erforderlichen EMS-Ereignisses zu Unified Manager und nach dem nächsten 15-minütigen Abfragzyklus
Ereignislebenszyklus	Wie andere Unified Manager Ereignisse: Neuer, bestätigter, gelöster und überholter Status	Das EMS-Ereignis wird nach der Aktualisierung des Clusters nach 15 Minuten nach dem Erstellen des Ereignisses veraltet
Erfasst Ereignisse während Unified Manager-Downtime	Ja, wenn das System gestartet wird, kommuniziert es mit jedem Cluster, um fehlende Ereignisse zu erfassen	Nein
Veranstaltungsdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um konsistente Lösungen zu bieten	Korrekturmaßnahmen sind auf der Seite Ereignisdetails nicht verfügbar

Bei einigen der neuen automatischen EMS-Ereignisse handelt es sich um Informationsereignisse, die darauf hinweisen, dass ein vorheriges Ereignis behoben wurde. Beispielsweise zeigt das Informationsereignis „FlexGroup-Komponenten-Raumstatus alles OK“ an, dass das Fehlerereignis „FlexGroup-Komponenten haben Platzprobleme“ behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus verwaltet werden wie andere Arten von Schweregrad. Das Ereignis wird jedoch automatisch veraltet, wenn das gleiche Volume ein weiteres Fehlerereignis „`SPace Problems`“ erhält.

EMS-Ereignisse, die automatisch dem Unified Manager hinzugefügt werden

Die folgenden ONTAP EMS-Ereignisse werden dem Unified Manager automatisch hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf jedem Cluster ausgelöst werden, das Unified Manager überwacht.

Die folgenden EMS-Ereignisse stehen zur Verfügung, wenn Cluster mit ONTAP 9.5 oder höher überwacht werden:

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad von Unified Manager
Zugriff auf Cloud-Tier für Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Beim Storage Failover wurde der Zugriff auf Cloud-Tier für Aggregatverschiebung verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
Resync der FabricPool-Spiegelreplikation abgeschlossen	wafl.ca.resync.complete	Cluster	Fehler
FabricPool Speicherplatz fast voll	Fabricpool.Fast.full	Cluster	Fehler
Beginn des NVMe-of-Grace-Zeitraums	nvmf.graceperiod.start	Cluster	Warnung
NVMe-of-Grace-Zeitraum aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-of-Grace-Zeitraum abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN wurde zerstört	lun.destroy	LUN	Informationsdaten
Cloud AWS MetaDataConnFail	Cloud.aws.metadataConnFail	Knoten	Fehler
Cloud AWS IAMCredsExpired – Cloud	Cloud.aws.iamCredsExpired	Knoten	Fehler
Cloud AWS IAMCredsungültig	Cloud.aws.iamCredsungültig	Knoten	Fehler
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Knoten	Fehler
Cloud AWS IAMCredsNotinitialisiert	Cloud.aws.iamNotinitialisiert	Knoten	Informationsdaten
Cloud AWS IAMRoleInvalid	Cloud.AWS.iamRoleIngültig	Knoten	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad von Unified Manager
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Knoten	Fehler
Unlösbar Für Cloud Tier Host	Objstore.Host.unlösbar	Knoten	Fehler
Cloud Tier Intercluster-Netzwerkschnittstelle Nicht Aktiv	objstore.interclusterlifDown	Knoten	Fehler
Anforderung Einer Signatur Für Die Cloud-Ebene Mit Nicht Übereinstimmung	osc.signatureMismatch	Knoten	Fehler
Einer der NFSv4-Pools ist erschöpft	Nblade.nfsV4PoolAust	Knoten	Kritisch
QoS Monitor Memory-Besteuerung	qos.Monitor.Memory.maxed	Knoten	Fehler
QoS Monitor Memory nicht gespeichert	qos.Monitor.Memory.abgenutzt	Knoten	Informationsdaten
NVMeNS zerstören	NVMeNS.destroy	Namespace	Informationsdaten
NVMeNS Online	NVMeNS.offline	Namespace	Informationsdaten
NVMeNS Offline	NVMeNS.online	Namespace	Informationsdaten
NVMe Out of Space	NVMeNS.out.of.space	Namespace	Warnung
Synchrone Replizierung Aus Sync Heraus	sms.Status.out.of.Sync	SnapMirror Beziehung	Warnung
Synchrone Replizierung Wiederhergestellt	sms.status.in.sync	SnapMirror Beziehung	Informationsdaten
Fehler Bei Der Automatischen Synchronisierung Der Replikation	sms.Resync.Versuch.failed	SnapMirror Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad von Unified Manager
Max. CIFS-Verbindung überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS-Namenskonflikt	Nblade.cifsNbNameConflict	SVM	Fehler
Versucht, eine nicht existierende CIFS-Freigabe zu verbinden	Nblade.cifsNoPrivShare	SVM	Kritisch
Fehler beim CIFS Shadow Copy-Vorgang	cifs.shadowcopy.Failure	SVM	Fehler
Vom AV-Server gefundener Virus	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV-Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine reaktionsfähige AV-Server-Verbindung	Nblade.vscanConnInaktiv	SVM	Informationsdaten
AV-Server ist zu beschäftigt, um neue Scananforderung zu akzeptieren	Nblade.vscanConnBackPressure	SVM	Fehler
Nicht autorisierter Benutzer versucht, AV-Server zu verwenden	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup-Komponenten haben Platzprobleme	Flexgroup.debestandals.have.space.Issues	Datenmenge	Fehler
FlexGroup-Komponenten-Space-Status alles OK	Flexgroup.Komponenten.space.Status.all.ok	Datenmenge	Informationsdaten

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad von Unified Manager
FlexGroup-Komponenten haben Inodes-Probleme	flexgroup.constituents.have.inodes.issues	Datenmenge	Fehler
FlexGroup-Komponenten inodes Status Alle OK	flexgroup.constituents.inodes.status.all.ok	Datenmenge	Informationsdaten
Logischer Volume-Speicherplatz Fast Voll	monitor.vol.nearFull.inc.sav	Datenmenge	Warnung
Logischer Speicherplatz Des Volume Voll	monitor.vol.full.inc.sav	Datenmenge	Fehler
Logischer Speicherplatz Des Volume Ist Normal	monitor.vol.one.ok.inc.sav	Datenmenge	Informationsdaten
Fehler bei der automatischen WAFL-Volume-Größe	wafl.vol.autoSize.fail	Datenmenge	Fehler
Die automatische WAFL-Volume-Größe ist abgeschlossen	wafl.vol.autoSize.done	Datenmenge	Informationsdaten
Timeout für den Vorgang der WAFL-READDIR-Datei	wafl.readdir.exist	Datenmenge	Fehler

Abonnieren von ONTAP EMS-Veranstaltungen

Sie können EMS-Ereignisse (Event Management System) abonnieren, die von Systemen generiert werden, die mit ONTAP Software installiert sind. Eine Untermenge von EMS-Ereignissen wird automatisch an Unified Manager gemeldet. Weitere EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie sich für diese Ereignisse angemeldet haben.

Bevor Sie beginnen

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

Sie können eine beliebige Anzahl von EMS-Veranstaltungen abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert. Nur die validierten Ereignisse werden auf die in Unified Manager überwachten Cluster angewendet. Der *ONTAP 9 EMS Ereigniskatalog* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite ONTAP 9 Produktdokumentation die entsprechende Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Veranstaltungen zu finden.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die von Ihnen abonnierenden ONTAP EMS-Ereignisse konfigurieren und benutzerdefinierte Skripts für die Ausführung dieser Ereignisse erstellen.

> Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, kann es möglicherweise ein Problem mit der DNS-Konfiguration des Clusters geben, was verhindert, dass das Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Cluster-Administrator die DNS-Konfiguration des Clusters korrigieren und dann Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server gespült.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.
2. Klicken Sie auf der Seite Event Setup auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld EMS-Ereignisse abonnieren den Namen des EMS-Ereignisses von ONTAP ein, für das Sie abonnieren möchten.

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

   "So konfigurieren und erhalten Sie Benachrichtigungen von ONTAP EMS-Ereignisabonnement in Active IQ Unified Manager"

4. Klicken Sie Auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste der abonnierten EMS-Ereignisse hinzugefügt, aber in der Spalte „Cluster anwendbar“ wird für das hinzugefügte EMS-Ereignis der Status als „`Unbekannt`“ angezeigt.

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

   Der Status „`ja`“ wird in der Spalte „gilt für Cluster“ für das EMS-Ereignis, das Sie hinzugefügt haben, angezeigt.

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

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

Was passiert, wenn ein Ereignis empfangen wird

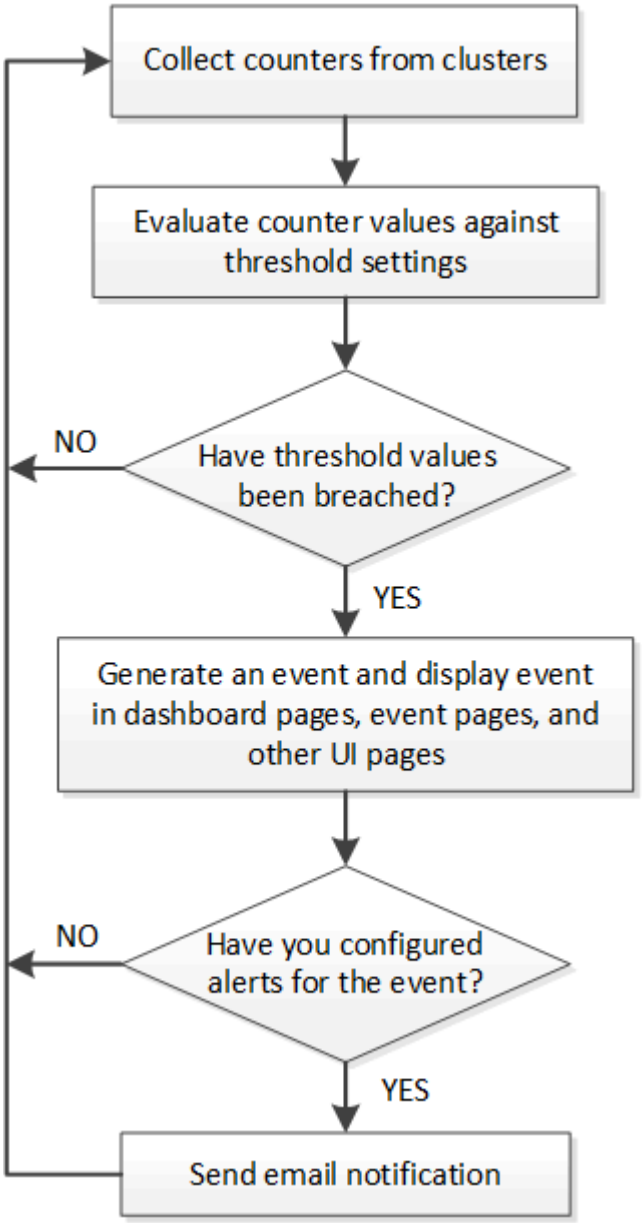
Wenn Unified Manager ein Ereignis empfängt, wird es auf der Seite Dashboard, auf der Seite Ereignismanagement-Inventar, auf den Registerkarten Zusammenfassung und Explorer der Seite Cluster/Performance und auf der objektspezifischen Bestandsseite (z. B. auf der Seite Volumes/Integritätsbestand) angezeigt.

Wenn Unified Manager mehrere kontinuierliche Vorkommnisse derselben Clusterkomponente erkennt, werden alle Vorkommnisse als einzelnes Ereignis behandelt und nicht als separate Ereignisse. Die Dauer des Ereignisses wird erhöht, um anzugeben, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie Einstellungen auf der Seite Alarmkonfiguration konfigurieren, können Sie andere Benutzer über diese Ereignisse benachrichtigen. Die Meldung bewirkt, dass folgende Aktionen ausgelöst werden:

- Eine E-Mail über das Ereignis kann an alle Unified Manager Administrator-Benutzer gesendet werden.
- Das Ereignis kann an weitere E-Mail-Empfänger gesendet werden.
- Ein SNMP-Trap kann an den Trap-Empfänger gesendet werden.
- Ein benutzerdefiniertes Skript kann ausgeführt werden, um eine Aktion auszuführen.

Dieser Workflow wird im folgenden Diagramm dargestellt.



Anzeigen von Ereignissen und Ereignisdetails

Sie können die Details zu einem Ereignis anzeigen, das von Unified Manager ausgelöst wird, um Korrekturmaßnahmen zu ergreifen. Wenn beispielsweise ein Systemzustandsereignis-Volume Offline vorhanden ist, können Sie auf dieses Ereignis klicken, um die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Die Ereignisdetails enthalten Informationen wie die Quelle des Ereignisses, die Ursache des Ereignisses und alle Notizen, die mit dem Ereignis zusammenhängen.

Schritte

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

   Standardmäßig werden in der Ansicht Alle aktiven Ereignisse die neuen und bestätigten (aktiven) Ereignisse angezeigt, die in den letzten 7 Tagen mit einem Level der Auswirkung von Vorfall oder Risiko generiert wurden.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen anzeigen möchten, z. B. Kapazitätsereignisse oder Performanceereignisse, klicken Sie auf **Ansicht** und wählen Sie im Menü der Ereignistypen aus.
3. Klicken Sie auf den Ereignisnamen, dessen Details angezeigt werden sollen.

   Die Ereignisdetails werden auf der Seite Ereignisdetails angezeigt.

Anzeigen nicht zugewiesener Ereignisse

Sie können nicht zugewiesene Ereignisse anzeigen und anschließend jedem Benutzer zuweisen, der diese auflösen kann.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritte

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

   Standardmäßig werden neue und bestätigte Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Fensterbereich **Filter** die Option **nicht zugewiesen** Filter im Bereich **zugewiesen zu** aus.

Bestätigen und Beheben von Ereignissen

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Bearbeitung des Problems beginnen, das das Ereignis verursacht hat, damit Sie keine wiederholten Warnmeldungen erhalten. Nachdem Sie die Korrekturmaßnahme für ein bestimmtes Ereignis durchgeführt haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können keine Informationsereignisse bestätigen.

Schritte

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

Ihr Ziel ist	Tun Sie das…
Bestätigen Sie ein einzelnes Ereignis und markieren Sie es als gelöst	a. Klicken Sie auf den Ereignisnamen. b. Bestimmen Sie auf der Seite Ereignisdetails die Ursache des Ereignisses. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.
Bestätigen und markieren Sie mehrere Ereignisse als erledigt	a. Bestimmen Sie die Ursache der Ereignisse auf der entsprechenden Seite „Ereignisdetails“. b. Wählen Sie die Ereignisse aus. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.

Nachdem das Ereignis als erledigt markiert wurde, wird das Ereignis in die Liste aufgelöster Ereignisse verschoben.

3. **Optional**: Fügen Sie im Bereich **Notizen und Updates** einen Hinweis dazu, wie Sie das Ereignis angesprochen haben, und klicken Sie dann auf **Post**.

Zuweisen von Ereignissen zu bestimmten Benutzern

Sie können nicht zugewiesene Ereignisse selbst oder anderen Benutzern, einschließlich Remote-Benutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer zuweisen. Wenn z. B. häufig Probleme an einem Storage-Objekt auftreten, können Sie den Benutzer, der das Objekt verwaltet, die Ereignisse für diese Probleme zuweisen.

Bevor Sie beginnen

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

Schritte

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

Wenn Sie das Ereignis zuweisen möchten…	Dann tun Sie das…
Sich Selbst.	Klicken Sie Auf **Zuweisen Zu** > **Mich**.
Einem anderen Benutzer	a. Klicken Sie auf **Zuweisen zu** > **anderer Benutzer**. b. Geben Sie im Dialogfeld Eigentümer zuweisen den Benutzernamen ein, oder wählen Sie einen Benutzer aus der Dropdown-Liste aus. c. Klicken Sie Auf **Zuweisen**. Der Benutzer erhält eine E-Mail-Benachrichtigung. Wenn Sie keinen Benutzernamen eingeben oder einen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt die Zuweisung des Ereignisses aufgehoben.

Deaktivieren unerwünschter Ereignisse

Standardmäßig sind alle Ereignisse aktiviert. Sie können Ereignisse global deaktivieren, um eine Generierung von Benachrichtigungen für in Ihrer Umgebung nicht wichtige Ereignisse zu verhindern. Sie können Ereignisse aktivieren, die deaktiviert sind, wenn Sie den Empfang von Benachrichtigungen für sie fortsetzen möchten.

Bevor Sie beginnen

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

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

Wenn Sie ein Ereignis für ein Objekt deaktivieren (z. B. das `vol offline` Ereignis), und später aktivieren Sie das Ereignis, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline geschaltet wurden, wenn das Ereignis im Status „deaktiviert“ war. Unified Manager generiert ein neues Ereignis nur, wenn nach der erneuten Aktivierung des Ereignisses eine Änderung im Objektstatus vorhanden ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.

2. Deaktivieren oder aktivieren Sie auf der Seite * Event Setup* Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	a. Klicken Sie Auf **Deaktivieren**. b. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad des Ereignisses aus. c. Wählen Sie in der Spalte „übereinstimmende Ereignisse“ die Ereignisse aus, die aufgrund des Schweregrads des Ereignisses deaktiviert werden sollen, und klicken Sie dann auf den Pfeil nach rechts, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und Schließen**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite Event Setup angezeigt werden.
Aktivieren von Ereignissen	a. Aktivieren Sie das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie aktivieren möchten. b. Klicken Sie Auf **Aktivieren**.

Behebung von Problemen mithilfe der automatischen Problembehebung in Unified Manager

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und eine einzige Lösung mit der Schaltfläche * Fix IT* bereitstellen kann. Wenn verfügbar, werden diese Auflösungen im Dashboard, auf der Seite Ereignisdetails und aus der Auswahl Workload Analysis im linken Navigationsmenü angezeigt.

Die meisten Ereignisse haben eine Vielzahl von möglichen Auflösungen, die auf der Seite Ereignisdetails angezeigt werden, so dass Sie die beste Lösung mit ONTAP System Manager oder der ONTAP CLI implementieren können. Eine Aktion **Beheben Sie es** ist verfügbar, wenn Unified Manager festgestellt hat, dass es eine einzige Lösung gibt, um das Problem zu beheben, und dass es mit einem ONTAP CLI-Befehl behoben werden kann.

Schritte

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

2. Um Probleme zu beheben, die Unified Manager beheben kann, klicken Sie auf die Schaltfläche **Fix IT**. Um ein Problem zu beheben, das auf mehreren Objekten vorhanden ist, klicken Sie auf die Schaltfläche * Alle beheben*.

Informationen zu Problemen, die durch automatische Problembehebung behoben werden können, finden Sie unter "Welche Probleme können mit Unified Manager behoben werden".

Aktivieren und Deaktivieren der Active IQ-Ereignisberichterstellung

Ereignisse auf der Active IQ-Plattform werden standardmäßig in der Benutzeroberfläche von Unified Manager generiert und angezeigt. Wenn diese Ereignisse zu „laut“ sind oder Sie diese Ereignisse nicht in Unified Manager anzeigen möchten, können Sie die Erzeugung dieser Ereignisse deaktivieren. Sie können sie zu einem späteren Zeitpunkt aktivieren, wenn Sie den Empfang dieser Benachrichtigungen fortsetzen möchten.

Bevor Sie beginnen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Wenn Sie diese Funktion deaktivieren, wird Active IQ-Plattformereignisse sofort von Unified Manager nicht mehr empfangen.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager gemäß der Zeitzone des Clusters kurz nach Mitternacht mit dem Empfang von Active IQ Plattformereignissen. Die Startzeit hängt ab, wenn Unified Manager AutoSupport Meldungen von jedem Cluster empfängt.

Schritte

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

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Active IQ-Plattformereignissen	Bewegen Sie im Fenster **Active IQ Portal Ereignisse** die Schieberegler-Taste nach links.
Aktivieren von Active IQ-Plattformereignissen	Bewegen Sie im Fenster **Active IQ Portal Ereignisse** die Schieberegler-Taste nach rechts.

Eine neue Datei für Active IQ-Regeln wird hochgeladen

Unified Manager prüft automatisch auf eine neue Active IQ-Datei (Events, Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln vorhanden sind. In Sites ohne externen Netzwerkzugriff müssen Sie die Regeldatei jedoch manuell hochladen.

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

Wenn Sie Unified Manager auf eine bestimmte Version an einem Standort ohne Netzwerkverbindung installieren oder aktualisieren, stehen die gebündelten Active IQ-Regeln automatisch für den Upload zur Verfügung. Wir empfehlen jedoch, etwa einmal pro Monat eine neue Regeldatei von der NetApp Support Site herunterzuladen, um sicherzustellen, dass aktualisierte Ereignisse generiert werden und Ihre Storage-Systeme weiterhin optimal funktionieren.

Bevor Sie beginnen

- Die Ereignisberichte für das Active IQ Portal müssen aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter "Aktivieren von Active IQ Portal-Ereignissen".
- Sie müssen die Regeldatei von der NetApp Support-Website herunterladen.

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

Schritte

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

   Das Paket der Paketregeln umfasst das regelRepository, die Datenquellen und einen NetApp KB-Artikel.

   > Auf Windows-Systemen wird der NetApp-KB-Artikel nicht standardmäßig mit dem Installer gebündelt, wenn er keine Netzwerkverbindung hat. Sie können die Datei *Secure_rules.zip* von der Support-Website herunterladen und hochladen, um den KB-Artikel für alle Regeln anzuzeigen.

2. Übertragen Sie die Regeldatei auf einige Medien, die Sie in den sicheren Bereich bringen können, und kopieren Sie sie dann in ein System im sicheren Bereich.
3. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.
4. Klicken Sie auf der Seite **Event Setup** auf die Schaltfläche **Regeln hochladen**.
5. Navigieren Sie im Dialogfeld **Regeln hochladen** zu den Regeln und wählen Sie diese aus `.zip` Datei, die Sie heruntergeladen haben, und klicken Sie auf **Upload**.

   Dieser Vorgang kann einige Minuten dauern.

Die Regeldatei wird auf dem Unified Manager-Server entpackt. Nachdem die gemanagten Cluster nach Mitternacht eine AutoSupport-Datei generiert haben, überprüft Unified Manager die Cluster anhand der Regeldatei und erzeugt bei Bedarf neue Risiken und Vorfälle.

Weitere Informationen finden Sie in diesem Artikel der Knowledge Base (KB): "Wie man AIQCASecure Regeln manuell in Active IQ Unified Manager aktualisiert".

Generieren von Active IQ-Plattformereignissen

Ereignisse und Risiken auf Active IQ Plattformen werden wie in der folgenden Abbildung dargestellt in Unified Manager Ereignisse konvertiert.

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

Ereignisse auf der Active IQ Plattform werden aufgelöst

Störungen und Risiken von Active IQ Plattformen ähneln anderen Ereignissen von Unified Manager, da sie anderen Benutzern zur Lösung zugewiesen werden können und

denselben verfügbaren Status aufweisen. Wenn Sie jedoch diese Art von Ereignissen mithilfe der Schaltfläche **Fix IT** lösen, können Sie die Auflösung innerhalb von Stunden überprüfen.

In dem folgenden Diagramm sind die Maßnahmen aufgeführt, die Sie ergreifen müssen (in Grün) und die Aktion, die Unified Manager beim Beheben von Ereignissen übernimmt, die über die Active IQ Plattform generiert wurden.

Wenn Sie eine manuelle Behebung des Problems durchführen, müssen Sie sich bei System Manager oder der Befehlszeilenschnittstelle von ONTAP anmelden, um das Problem zu beheben. Sie können das Problem nur überprüfen, nachdem das Cluster eine neue AutoSupport Meldung um Mitternacht generiert hat.

Wenn Sie eine halbautomatische Auflösung mit der **Fix IT**-Taste durchführen, können Sie überprüfen, ob die Fehlerbehebung innerhalb von Stunden erfolgreich war.

Konfigurieren von Einstellungen für die Ereignisaufbewahrung

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

Bevor Sie beginnen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Die Aufbewahrung von Ereignissen über 6 Monate kann die Serverleistung beeinträchtigen und wird nicht empfohlen.

Schritte

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

Was für ein Unified Manager-Wartungsfenster ist

Sie definieren ein Unified Manager Wartungsfenster, um Ereignisse und Warnmeldungen für einen bestimmten Zeitraum zu unterdrücken, wenn Sie für eine Cluster-Wartung geplant haben und keine unerwünschte Benachrichtigungen erhalten möchten.

Wenn das Wartungsfenster beginnt, wird ein Ereignis „Objektwartung gestartet“ auf der Seite „Ereignisverwaltung Bestand“ veröffentlicht. Dieses Ereignis wird automatisch veraltet, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden die Ereignisse, die sich auf alle Objekte im Cluster beziehen, weiterhin generiert, jedoch nicht in einer UI-Seite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet. Sie können jedoch die Ereignisse anzeigen, die während eines Wartungsfensters für alle Speicherobjekte generiert wurden, indem Sie auf der Seite „Ereignismanagement-Bestand“ eine der Optionen „Ansicht“ auswählen.

Sie können ein Wartungsfenster für die Zukunft planen, die Start- und Endzeit für ein geplantes

Wartungsfenster ändern und ein Wartungsfenster abbrechen.

Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen

Wenn Sie z. B. vor einer geplanten Ausfallzeit für ein Cluster stehen, um ein Cluster zu aktualisieren oder einen der Nodes zu verschieben, können Sie die Ereignisse und Warnungen unterdrücken, die normalerweise während dieses Zeitfensters generiert werden würden, indem Sie ein Unified Manager Wartungsfenster planen.

Bevor Sie beginnen

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

Während eines Wartungsfensters werden die Ereignisse, die mit allen Objekten auf dem Cluster zusammenhängen, weiterhin generiert, jedoch nicht auf der Ereignisseite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet.

Die Zeit, die Sie für das Wartungsfenster eingeben, basiert auf der Zeit im Unified Manager-Server.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie in der Spalte **Wartungsmodus** für den Cluster die Schieberegler-Schaltfläche aus, und verschieben Sie sie nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Wählen Sie das Start- und Enddatum und die Uhrzeit für das Wartungsfenster aus und klicken Sie auf **Anwenden**.

   Die Meldung „geplant“ wird neben dem Schieberegler angezeigt.

Wenn die Startzeit erreicht ist, wechselt das Cluster in den Wartungsmodus und ein Ereignis „Objektwartung gestartet“ wird generiert.

Ändern oder Abbrechen eines geplanten Wartungsfensters

Wenn Sie ein Wartungsfenster von Unified Manager für die Zukunft konfiguriert haben, können Sie die Start- und Endzeit ändern oder das Wartungsfenster nicht mehr ausführen.

Bevor Sie beginnen

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

Das Abbrechen eines derzeit ausgeführten Wartungsfensters ist hilfreich, wenn Sie die Cluster-Wartung vor dem Ende des geplanten Wartungsfensters abgeschlossen haben und Sie möchten Ereignisse und Warnmeldungen vom Cluster erneut empfangen.

Schritte

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

Ihr Ziel ist	Führen Sie diesen Schritt aus…
Ändern Sie den Zeitrahmen für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „geplant“. b. Ändern Sie das Start- und/oder Enddatum und die Uhrzeit, und klicken Sie auf **Anwenden**.
Verlängern Sie die Länge eines aktiven Wartungsfensters	a. Klicken Sie auf den Text „aktiv“ neben dem Schieberegler. b. Ändern Sie das Enddatum und die Endzeit, und klicken Sie auf **Anwenden**.
Abbrechen eines geplanten Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.
Abbrechen eines aktiven Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse werden nach Abschluss des Wartungsfensters im Status „veraltet“ angezeigt und alle Systemressourcen werden gesichert und ausgeführt.

Bevor Sie beginnen

Mindestens ein Wartungsfenster muss abgeschlossen sein, bevor Ereignisse verfügbar sind.

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

Schritte

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

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Fenster Ansicht die Option **Alle Ereignisse, die während der Wartung generiert wurden** aus.

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

3. Wenn mehrere Wartungsfenster für einen einzelnen Cluster vorhanden waren, können Sie auf das Kalendersymbol **ausgelöste Zeit** klicken und den Zeitraum für die Wartungsfenster-Ereignisse auswählen, die Sie interessieren.

Verwalten von Ressourcenereignissen des Host-Systems

Unified Manager umfasst einen Service zur Überwachung von Ressourcenproblemen auf dem Host-System, auf dem Unified Manager installiert ist. Probleme wie der fehlende Speicherplatz oder der fehlende Arbeitsspeicher auf dem Hostsystem können Ereignisse der Managementstation auslösen, die als Banner-Meldungen oben in der Benutzeroberfläche angezeigt werden.

Ereignisse der Managementstation zeigen ein Problem mit dem Hostsystem an, auf dem Unified Manager installiert ist. Beispiele für Probleme mit Management Station sind Festplattenspeicherplatz, der auf dem Host-System niedrig ist, Unified Manager fehlt einen regelmäßigen Datenerfassungszyklus, und Nichtabschluss oder späterer Abschluss der Statistikanalyse, da die nächste Erfassungsabfrage gestartet wurde.

Im Gegensatz zu allen anderen Unified Manager-Ereignismeldungen werden diese speziellen Warnmeldungen der Management Station sowie kritische Ereignisse in Bannermeldungen angezeigt.

Schritt

1. So zeigen Sie Ereignisinformationen der Management Station an:

Ihr Ziel ist	Tun Sie das…
Zeigen Sie Details der Veranstaltung an	Klicken Sie auf das Veranstaltungsbanner, um die Seite Veranstaltungsdetails mit Lösungsvorschlägen für das Problem anzuzeigen.
Alle Veranstaltungen der Management Station anzeigen	a. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**. b. Klicken Sie im Fensterbereich Filter auf der Seite „Inventar der Ereignisverwaltung“ in der Liste „Ausgangstyp“ auf das Feld für Management Station.

Allgemeines zu Ereignissen

Wenn Sie die Konzepte zu Ereignissen verstehen, können Sie Ihre Cluster und Cluster-Objekte effizient managen und Warnmeldungen entsprechend definieren.

Definition des Ereignisstatus

Der Status eines Ereignisses hilft Ihnen, zu identifizieren, ob eine geeignete Korrekturmaßnahme ergriffen werden muss. Ein Ereignis kann neu, bestätigt, aufgelöst oder veraltet sein. Beachten Sie, dass sowohl neue als auch bestätigte Ereignisse als aktive Ereignisse betrachtet werden.

Die Ereigniszustände sind wie folgt:

- * Neu*

Der Status eines neuen Ereignisses.

- * Bestätigt*

  Der Status eines Ereignisses, wenn Sie es bestätigt haben.

- * Gelöst*

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

- **Veraltet**

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

  Sie können ein überholetes Ereignis nicht bestätigen oder beheben.

Beispiel für unterschiedliche Zustände eines Ereignisses

Die folgenden Beispiele veranschaulichen manuelle und automatische Änderungen des Ereignisstatus.

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

Wenn das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls generiert wird, funktioniert das Cluster nach Wiederherstellung der Stromversorgung ohne ein Eingreifen des Administrators. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig, und im nächsten Überwachungszyklus wird der Ereignisstatus auf „veraltet“ geändert.

Unified Manager sendet eine Warnmeldung, wenn sich ein Ereignis im Status „veraltet“ oder „gelöst“ befindet. Die E-Mail-Betreffzeile und der E-Mail-Inhalt einer Meldung enthalten Informationen zum Ereignisstatus. Ein SNMP-Trap enthält auch Informationen zum Ereignisstatus.

Beschreibung der Ereignistypen

Jedes Ereignis ist mit einem Schweregrad verknüpft, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die eine unmittelbare Korrekturmaßnahme erfordern.

- * Kritisch*

  Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.

  Performance-kritische Ereignisse werden nur von benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

  Die Event-Quelle befindet sich noch in einer Performance. Zur Vermeidung von Serviceunterbrechungen sind jedoch Korrekturmaßnahmen erforderlich.

- **Warnung**

Bei der Event-Quelle kommt es zu einem Vorfall, den Sie beachten sollten, oder ein Performance-Zähler für ein Cluster-Objekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass der kritische Schweregrad nicht erreicht wurde. Ereignisse dieses Schweregrades führen nicht zu einer Serviceunterbrechung und unmittelbare Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

Ereignisse mit Performance-Warnmeldungen werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt wird oder wenn eine Benutzeraktion durchgeführt wird. Beispiel: Wenn ein Storage-Objekt gelöscht wird oder wenn Konfigurationsänderungen vorliegen, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

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

Beschreibung der Level der Ereignisauswirkungen

Jedes Ereignis ist mit einer Folgenabstufe (Vorfall, Risiko, Ereignis oder Upgrade) verbunden, die Ihnen dabei hilft, Ereignisse zu priorisieren, die umgehend Korrekturmaßnahmen erfordern.

- **Vorfall**

  Ein Vorfall ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster keine Daten mehr für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Auswirkungen auf den Vorfall sind am schwersten. Um Serviceunterbrechungen zu vermeiden, sollten sofortige Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster nicht mehr Daten für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Risikoeinwirkung können zu Serviceunterbrechungen führen. Möglicherweise ist eine Korrekturmaßnahme erforderlich.

- **Veranstaltung**

  Ein Ereignis ist eine Statusänderung von Storage-Objekten und ihren Attributen. Ereignisse mit Auswirkungen auf das Ereignis dienen zur Information und erfordern keine Korrekturmaßnahmen.

- **Upgrade**

  Upgrade-Ereignisse sind ein bestimmter Ereignistyp, der von der Active IQ Plattform gemeldet wird. Diese Ereignisse erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, Node-Firmware oder Betriebssystemsoftware erforderlich ist (für Sicherheitsempfehlungen). Möglicherweise möchten Sie für einige dieser Probleme sofortige Korrekturmaßnahmen durchführen, während andere Probleme möglicherweise bis zur nächsten geplanten Wartung warten können.

Beschreibung der Bereiche für Ereignisauswirkungen

Ereignisse werden in sechs Auswirkungsbereiche unterteilt (Verfügbarkeit, Kapazität, Konfiguration, Performance, Schutz, Und Sicherheit) damit Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse melden Sie, wenn ein Storage-Objekt offline geschaltet wird, wenn ein Protokollservice ausfällt, ein Problem mit dem Storage Failover auftritt oder wenn ein Problem mit der Hardware auftritt.

- * Kapazität*

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

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, das Löschen, das Hinzufügen, das Entfernen oder Umbenennen Ihrer Storage-Objekte. Konfigurationsereignisse haben eine Auswirkung auf das Ereignis und einen Schweregrad der Informationen.

- **Leistung**

  Bei Performance-Ereignissen werden Sie über Ressourcen, Konfigurationen oder Aktivitätsbedingungen auf dem Cluster informiert, die negative Auswirkungen auf die Geschwindigkeit der Eingabe oder den Abruf von Daten-Storage für Ihre überwachten Storage-Objekte haben können.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Vorfälle oder Risiken im Zusammenhang mit SnapMirror Beziehungen, Probleme mit Zielkapazität, Probleme mit SnapVault Beziehungen oder Probleme mit Sicherungsaufgaben. Alle ONTAP Objekte (insbesondere Aggregate, Volumes und SVMs), die sekundäre Volumes und Sicherungsbeziehungen hosten, werden im Bereich der Sicherungsauswirkungen kategorisiert.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP-Cluster, Storage Virtual Machines (SVMs) und Volumes auf den in definierten Parametern basieren "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9".

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

Wie der Objektstatus berechnet wird

Der Objektstatus wird durch das schwerste Ereignis bestimmt, das derzeit einen neuen oder bestätigten Status aufweist. Wenn z. B. der Objektstatus „Fehler“ lautet, weist eines der Ereignisse des Objekts den Schweregrad „Fehler“ auf. Wenn Korrekturmaßnahmen ergriffen wurden, wird der Ereignisstatus auf „gelöst“ verschoben.

Details des dynamischen Performance-Ereignidiagramms

Bei dynamischen Performance-Ereignissen werden auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ die wichtigsten Workloads mit der höchsten Latenz oder der höchsten Auslastung der Clusterkomponente angezeigt, die nicht besonders geeignet ist.

Die Performance-Statistiken basieren auf dem Zeitpunkt, zu dem das Performance-Ereignis bis zum letzten Mal erkannt wurde, als das Ereignis analysiert wurde. In den Diagrammen werden außerdem Verlaufsstatistiken zur Performance für die Cluster-Komponente angezeigt, die mit Konflikten in Konflikt sind.

Beispielsweise können Sie Workloads mit hoher Auslastung einer Komponente identifizieren, um zu ermitteln, welcher Workload in eine Komponente verschoben werden soll, die weniger genutzt wird. Durch ein Verschieben des Workloads würde der Arbeitsaufwand für die aktuelle Komponente verringert, sodass möglicherweise die Komponente nicht mehr unter Konflikten steht. Oben in diesem Abschnitt befindet sich der Zeit- und Datumsbereich, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird die zuletzt analysierte Zeit aktualisiert.

Die Latenz- und Aktivitätsdiagramme zeigen die Namen der wichtigsten Workloads an, wenn Sie den Mauszeiger über das Diagramm bewegen. Wenn Sie rechts im Diagramm auf das Menü „Workload Type“ klicken, können Sie die Workloads anhand ihrer Rolle beim Ereignis, einschließlich *Haie*, *bullies* oder *Opfern*, sortieren und Details zu ihrer Latenz und ihrer Verwendung für die Clusterkomponente anzeigen, deren Konflikte vorliegen. Sie können den tatsächlichen Wert mit dem erwarteten Wert vergleichen, um festzustellen, wann der Workload den erwarteten Latenzbereich oder die Auslastung betrug. Weitere Informationen finden Sie unter "Arten von Workloads, die von Unified Manager überwacht werden".

> Wenn Sie bei der Latenzspitze nach Abweichungen sortieren, werden systemdefinierte Workloads nicht in der Tabelle angezeigt, da sich die Latenz nur auf benutzerdefinierte Workloads bezieht. Workloads mit sehr niedrigen Latenzwerten werden in der Tabelle nicht angezeigt.

Weitere Informationen über die dynamischen Leistungsschwellenwerte finden Sie unter "Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten".

Informationen zum Sortieren der Workloads in Unified Manager und zum ermitteln der Sortierreihenfolge finden Sie unter "Wie Unified Manager die Auswirkungen auf die Performance eines Ereignisses ermittelt".

Die Daten in den Diagrammen zeigen 24 Stunden Performance-Statistiken vor dem letzten Mal, wenn das Ereignis analysiert wurde. Die tatsächlichen Werte und die erwarteten Werte für jeden Workload basieren auf der Zeit, an der der Workload am Ereignis beteiligt war. Beispielsweise kann ein Workload in ein Ereignis einbezogen werden, nachdem das Ereignis erkannt wurde. Die Performance-Statistiken entsprechen daher zum Zeitpunkt der Ereigniserkennung möglicherweise nicht den Werten. Standardmäßig werden die Workloads nach oberster (höchster) Abweichung der Latenz sortiert.

> Da Unified Manager maximal 30 Tage historische Performance- und Ereignisdaten von 5 Minuten speichert, werden keine Leistungsdaten angezeigt, wenn das Ereignis mehr als 30 Tage alt ist.

- * Spalte Workload Sortieren*
  - **Latenzdiagramm**

    Zeigt die Auswirkungen des Ereignisses auf die Latenz des Workloads während der letzten Analyse an.

- **Spalte Komponentenverwendung**

  Zeigt Details zur Workload-Nutzung der Clusterkomponente an, die mit einem Konflikt zu Konflikten führen ist. In den Diagrammen ist die tatsächliche Verwendung eine blaue Linie. Ein roter Balken markiert die Ereignisdauer von der Erkennungszeit bis zur letzten analysierten Zeit. Weitere Informationen finden Sie unter "Messwerte für die Workload-Performance".

  Da für die Netzwerkkomponente Statistiken zur Netzwerk-Performance aus dem Cluster stammen, wird diese Spalte nicht angezeigt.

- **Komponentenverwendung**

  Zeigt den Auslastungsverlauf in Prozent für die Netzwerkverarbeitung, Datenverarbeitung und Aggregatkomponenten oder den Verlauf des Vorgangs in Prozent für die Komponente der QoS-Richtliniengruppe an. Das Diagramm wird nicht für die Netzwerk- oder Verbindungskomponenten angezeigt. Sie können mit der Statistik zu einem bestimmten Zeitpunkt die Nutzungsstatistiken anzeigen.

- **Total Schreib MB/s Historie**

  Nur für die Komponente MetroCluster Ressourcen wird der gesamte Schreibdurchsatz in Megabyte pro Sekunde (MB/s) für alle Volume Workloads angezeigt, die in einer MetroCluster-Konfiguration dem Partner-Cluster gespiegelt werden.

- **Veranstaltungsverlauf**

  Zeigt in den rot schattierten Zeilen die historischen Ereignisse für die zu versagende Komponente an. Bei veralteten Ereignissen zeigt das Diagramm Ereignisse an, die vor dem Erkennen des ausgewählten Ereignisses aufgetreten sind und nach dessen Behebung behoben wurden.

Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen. So können Sie feststellen, ob eine Änderung zu einem Performance-Ereignis geführt oder beigetragen hat. Auf den Seiten des Performance Explorer wird ein Symbol für das Änderungsereignis (angezeigt) Zur Angabe des Datums und der Uhrzeit, zu der die Änderung erkannt wurde.

Sie können die Performance-Diagramme auf den Seiten des Performance Explorers und auf der Seite Workload Analysis überprüfen, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Cluster-Objekts auswirkt. Wenn die Änderung zu oder um die gleiche Zeit wie ein Performance-Ereignis erkannt wurde, hat die Änderung möglicherweise zum Problem beigetragen, was dazu führte, dass die Ereigniswarnung ausgelöst wurde.

Unified Manager erkennt die folgenden Änderungsereignisse, die als Informationsereignisse kategorisiert sind:

- Ein Volume wird zwischen Aggregaten verschoben.

  Unified Manager erkennt, wenn eine Verschiebung gerade ausgeführt, abgeschlossen oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume-Verschiebung ausfällt, erkennt er bei der Sicherung die Volume-Verschiebung und zeigt ein Änderungsereignis für ihn an.

- Der Durchsatz (MB/s oder IOPS) wird von einer QoS-Richtliniengruppe begrenzt, die eine oder mehrere überwachte Workload-Änderungen enthält.

  Das Ändern eines Richtliniengruppenlimits kann zu intermittierenden Latenzspitzen (Antwortzeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz kehrt nach und nach wieder in den Normalzustand zurück und alle Ereignisse, die durch diese Spitzen verursacht werden, werden obsolet.

- Ein Node in einem HA-Paar übernimmt den Storage seines Partner-Nodes oder gibt ihn zurück.

  Unified Manager erkennt, wann der Takeover-, Teil- oder Giveback-Vorgang abgeschlossen wurde. Wenn der Takeover durch einen Panik- Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein Upgrade oder Zurücksetzen von ONTAP wurde erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Liste von Ereignissen und Schweregraden

Sie können die Liste der Ereignisse verwenden, um mit Ereigniskategorien, Ereignisnamen und Schweregrad jedes Ereignisses, das Sie möglicherweise in Unified Manager sehen, vertraut zu werden. Die Ereignisse werden in alphabetischer Reihenfolge nach Objektkategorie aufgeführt.

Aggregieren von Ereignissen

Aggregierte Ereignisse liefern Ihnen Informationen zum Status von Aggregaten, sodass Sie bei potenziellen Problemen überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregate Offline(ocumEvtAggregateOffline)	Vorfall	Aggregat	Kritisch
Aggregat ist fehlgeschlagen (ocumEvtAggregateStateFailed)	Vorfall	Aggregat	Kritisch
Aggregat eingeschränkt(ocumEvtAggregateStateRestricted)	Dar	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat-Rekonstruktion (ocumEvtAggregateRaidStateRekonstruktion)	Dar	Aggregat	Warnung
Aggregat herabgestuft (ocumEvtAggregateRaidStateDegradiert)	Dar	Aggregat	Warnung
Cloud Tier teilweise erreichbar (ocumEventCloudTierPartiallyAbnehmbar)	Dar	Aggregat	Warnung
Cloud Tier nicht erreichbar (ocumEventCloudTiernicht erreichbar)	Dar	Aggregat	Fehler
Cloud-Tier-Zugriff für Aggregatverschiebung verweigert *(arlNetraCaCheckFailed)	Dar	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverschiebung während Storage Failover *(gbNetraCaCheckFailed) verweigert	Dar	Aggregat	Fehler
MetroCluster Aggregat links hinter(ocumEvtMetroClusterAggregateLeftBehind)	Dar	Aggregat	Fehler
MetroCluster Aggregatspiegelung mit herabgestufter(occumEvtMetroClusterAggregateMirrorDegradiert)	Dar	Aggregat	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat-Platz fast voll (ocumEvtAggregateNearFull)	Dar	Aggregat	Warnung
Aggregierter Platz voll (okumEvtAggregateFull)	Dar	Aggregat	Fehler
Aggregieren Sie Tage bis voll (ocumEvtAggregateTagenUntilFullSoon)	Dar	Aggregat	Fehler
Aggregat überengagiert (ocumEvtAggregateOverwockt)	Dar	Aggregat	Fehler
Aggregat fast überengagiert (ocumEvtAggregateAlmostOverengagiert)	Dar	Aggregat	Warnung
Aggregat-Snapshot-Reserve voll (ocumEvtaggregateSnapReserveFull)	Dar	Aggregat	Warnung
Aggregierte Wachstumsrate anormal (ocumEvtAggregateGrowthRateAbnormal)	Dar	Aggregat	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat entdeckt (nicht zutreffend)	Ereignis	Aggregat	Informationsdaten
Aggregat umbenannt(nicht zutreffend)	Ereignis	Aggregat	Informationsdaten
Aggregat gelöscht (nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster kritischer IOPS-Schwellenwert (okumAggregateIopsVorfall)	Vorfall	Aggregat	Kritisch
Unterschreitster Schwellenwert für die Aggregat-IOPS-Warnung (ocumAggregateIopsWarnung)	Dar	Aggregat	Warnung
Unterschreitster kritischer Schwellenwert für MB/s des Aggregats (ocumAggregateMbpsVorfall)	Vorfall	Aggregat	Kritisch
MB/s Aggregat Warnung: Unterschreitster Schwellenwert (ocumAggregateMbpsWarnung)	Dar	Aggregat	Warnung
Unterschreiten der kritischen Latenzzeit für das Aggregat (ocumAggregateLatencyVorfall)	Vorfall	Aggregat	Kritisch
Warnung: Aggregatlatenz - nicht erreichenem Schwellenwert (okumAggregateLatencyWarnung)	Dar	Aggregat	Warnung
Verwendete Aggregat-Performance-Kapazität, kritischer Schwellenwert verletzt (ocumAggregatePerfkapazitätVerwendungVorfall)	Vorfall	Aggregat	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Verwendete Aggregat-Performance-Kapazität, Warnschwellenwert nicht erreicht (ocumAggregatePerfkapazitätVerwendWarnung)	Dar	Aggregat	Warnung
Unterschreiten der Aggregatauslastung zum kritischen Schwellenwert (okumAggregateUtilizationVorfall)	Vorfall	Aggregat	Kritisch
Warnung vor nicht durchbrochenem Aggregat-Auslastungsschwellenwert (ocumAggregateUtilizationWarnung)	Dar	Aggregat	Warnung
Überlasteter Schwellenwert für Aggregat-Festplatten (ocumAggregateFestplattenOverUtilizedWarnung)	Dar	Aggregat	Warnung
Nicht durchbrochenes dynamisches Aggregat-Schwellenwert (okumAggregateDynamicEventWarnung)	Dar	Aggregat	Warnung

Cluster-Ereignisse

Cluster-Ereignisse bieten Informationen zum Status von Clustern. So können Sie das Cluster auf potenzielle Probleme überwachen. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cluster fehlt es an Spare Disks (ocumEvtDiscsNoSpares)	Dar	Cluster	Warnung
Cluster nicht erreichbar (ocumEvtClusternicht erreichbar)	Dar	Cluster	Fehler
Cluster-Überwachung fehlgeschlagen (ocumEvtClusterMonitoringFailed)	Dar	Cluster	Warnung
Kapazitätsbeschränkungen für Cluster-FabricPool-Lizenz, überschritten (OktEvtexterne KapazitätenTierSpaceFull)	Dar	Cluster	Warnung
NVMe-of Grace-Zeitraum gestartet *(nvmfGracePeriodStart)	Dar	Cluster	Warnung
NVMe-of Grace Period aktiv *(nvmfGracePeriodActive)	Dar	Cluster	Warnung
NVMe-of Grace-Zeitraum abgelaufen *(nvmfGracePeriodExpired)	Dar	Cluster	Warnung
Objekt-Wartungsfenster gestartet (ObjektPflege-Fenster gestartet)	Ereignis	Cluster	Kritisch
Objekt-Wartungsfenster beendet(ObjectWartungs-Fenster beendet)	Ereignis	Cluster	Informationsdaten
MetroCluster Ersatzfestplatten übrig (ocumEvtSpareDiskLeftBehind)	Dar	Cluster	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
MetroCluster Automatische ungeplante Umschaltung deaktiviert (ocumEvtMccAutomaticUnplanedSwitchOverdisabled)	Dar	Cluster	Warnung
Cluster-Benutzerpasswort geändert *(cluster.passwd.changed)	Ereignis	Cluster	Informationsdaten

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unausgeglichene Cluster-Kapazität – Schwellenwert überschritten (ocumConformanceNodeImbalanceWarnung)	Dar	Cluster	Warnung
Cluster-Cloud-Tier-Planung (ClusterCloudTierPlanningWarnung)	Dar	Cluster	Warnung
Resync der FabricPool-Spiegelreplikation abgeschlossen *(WaflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool-Bereich fast voll * (FabricPool Nearvoll)	Dar	Cluster	Fehler

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Node hinzugefügt (nicht zutreffend)	Ereignis	Cluster	Informationsdaten

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Node entfernt(nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Cluster entfernt (nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Cluster-Add fehlgeschlagen (nicht zutreffend)	Ereignis	Cluster	Fehler
Cluster-Name geändert(nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Notfallhilfe erhalten (nicht zutreffend)	Ereignis	Cluster	Kritisch
Erhalten von wichtigen EMS (nicht zutreffend)	Ereignis	Cluster	Kritisch
Alarm EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Fehler
Fehler EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung
Warnung EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung
Debug EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung
Hinweis erhalten EMS (nicht zutreffend)	Ereignis	Cluster	Warnung
Information EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS-Ereignisse sind in drei Schweregrade für Ereignisse von Unified Manager unterteilt.

Schweregrad für Unified Manager Ereignisse	Schweregrad des ONTAP EMS-Ereignisses-Ereignisses

Kritisch	Notfall Kritisch
Fehler	Alarm
Warnung	Fehler Warnung Debuggen Hinweis Informativ

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten Schwellenwert Für Das Lastwucht Des Clusters()	Dar	Cluster	Warnung
Unterschreitster Cluster-IOPS-Schwellenwert (OktumClusterIopsVorfall)	Vorfall	Cluster	Kritisch
Unterschreitster Cluster IOPS-Warnungsschwellenwert (ocumClusterIopsWarnung)	Dar	Cluster	Warnung
Cluster-MB/s – kritischer Schwellenwert überschritten (ocumClusterMbpsVorfall)	Vorfall	Cluster	Kritisch
Cluster MB/s Warnschwellenwert nicht erreicht (ocumClusterMbpsWarnung)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht verbundenes dynamischer Schwellenwert (ocumClusterDynamicEventWarnung)	Dar	Cluster	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfigurations deaktiviert)	Dar	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt (ocumClusterAuditLogunverschlüsselt)	Dar	Cluster	Warnung
Lokaler Admin-Standardbenutzer aktiviert (ocumClusterDefaultAdminaktiviert)	Dar	Cluster	Warnung
FIPS-Modus deaktiviert (ocumClusterFipsdeaktiviert)	Dar	Cluster	Warnung
Login Banner deaktiviert (ocumClusterLoginBannerdeaktiviert)	Dar	Cluster	Warnung
Login Banner geändert (ocumClusterLoginBannerChanged)	Dar	Cluster	Warnung
Log-Forwarding-Ziele geändert(ocumLogForwardDestinationsChanged)	Dar	Cluster	Warnung
NTP-Servernamen geändert(ocumNtpServerNamesChanged)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NTP-Server-Anzahl ist niedrig (securityConfigNTPServerCountLowRisk)	Dar	Cluster	Warnung
Cluster-Peer-Kommunikation nicht verschlüsselt (ocumClusterPeerVerschlüsselungdeaktiviert)	Dar	Cluster	Warnung
SSH verwendet unsichere Chiffren (ocumClusterSSHInSecure)	Dar	Cluster	Warnung
Telnet-Protokoll aktiviert (ocumClusterTelnetEnabled)	Dar	Cluster	Warnung
Passwörter einiger ONTAP-Benutzerkonten verwenden die weniger sichere MD5-Hash-Funktion (ocumClusterMD5PasswordHashUsed).	Dar	Cluster	Warnung
Cluster verwendet selbstsigniertes Zertifikat (ocumClusterSelfSignedZertifikat)	Dar	Cluster	Warnung
Cluster-Remote-Shell ist aktiviert (ocumClusterRshdeaktiviert)	Dar	Cluster	Warnung
Cluster Certificate About to Expire (ocumEvtClusterCertificateAboutToExpire)	Dar	Cluster	Warnung
Cluster-Zertifikat abgelaufen (ocumEvtClusterCertificateExpired)	Dar	Cluster	Fehler

Festplatten-Ereignisse

Festplatten-Events liefern Ihnen Informationen zum Status von Festplatten, sodass Sie Monitoring-Funktionen auf potenzielle Probleme ausführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Flash-Festplatten – Spare Blocks fast verbraucht (ocumEvtClusterFlashDiskFewerSpaeBlockError)	Dar	Cluster	Fehler
Flash-Festplatten – keine Spare-Blöcke (ocumEvtClusterFlashDiskNoSpareBlockkritisch)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Festplatten (ocumEvtClusterUnzuweisedDisksSome)	Dar	Cluster	Warnung
Einige ausgefallene Festplatten (ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Gehäuse-Ereignisse

Gehäuse-Events liefern Ihnen Informationen zum Status der Festplatten-Shelf-Gehäuse im Datacenter, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Platten-Shelf-Lüfter fehlgeschlagen(ocumEvtShelfFanFailed)	Vorfall	Storage Shelf	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Fehler bei der Festplatten-Shelf-Stromversorgung(ocumEvtShelfPowerSupplyFailed)	Vorfall	Storage Shelf	Kritisch
Platten-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	Dar	Knoten	Warnung
Festplatten-Shelf-Pfad-Ausfall(ocumDiskShelfConnectivitätPathFailure)	Dar	Storage Shelf	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Festplatten-Shelf erkannt (nicht zutreffend)	Ereignis	Knoten	Informationsdaten
Entfernte Festplatten-Shelfs (nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Fan-Events

Lüfterereignisse versorgen Sie mit Informationen zu den Statusventilatoren auf Nodes in Ihrem Datacenter, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Ein oder mehrere ausgefallene Lüfter(ocumEvtFansOneOrMoreFailed)	Vorfall	Knoten	Kritisch

Flash-Kartenereignisse

Flash-Karten-Events informieren Sie über den Status der auf Nodes in Ihrem Datacenter installierten Flash-Karten und überwachen mögliche Probleme. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Flash-Karten offline(ocumEvtFlashCardOffline)	Vorfall	Knoten	Kritisch

Inodes-Events

Inode-Ereignisse liefern Informationen, wenn die Inode voll oder fast voll ist, sodass Sie auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Inodes fast voll (ocumEvtInodesAlmostFull)	Dar	Datenmenge	Warnung
Inodes Full (ocumEvtInodesFull)	Dar	Datenmenge	Fehler

Ereignisse der Netzwerkschnittstelle (LIF)

Ereignisse an der Netzwerkschnittstelle liefern Informationen zum Status Ihrer

Netzwerkschnittstelle (LIFs), sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Status der Netzwerkschnittstelle aus (ocumEvtLifStatusDown)	Dar	Schnittstelle	Fehler
FC/FCoE-Netzwerkschnittstelle Status ausgefallen (occumEvtFCLifStatus aus)	Dar	Schnittstelle	Fehler
Network Interface Failover nicht möglich (ocumEvtLifFailoverNotMögliche)	Dar	Schnittstelle	Warnung
Netzwerkschnittstelle nicht am Home Port (ocumEvtLifNotAtHomePort)	Dar	Schnittstelle	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Network Interface Route nicht konfiguriert (nicht zutreffend)	Ereignis	Schnittstelle	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumNetworkLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(OccumNetworkLifMbpsWarnung)	Dar	Schnittstelle	Warnung
FC-Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumFcpLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
FC-Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(OccumFcpLifMbpsWarnung)	Dar	Schnittstelle	Warnung
NVMf FC-Netzwerkschnittstelle MB/s Critical Threshold Überlaufen(ocumNvmfcLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
NVMf FC-Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(ocumNvmfcLifMbpsWarnung)	Dar	Schnittstelle	Warnung

LUN-Ereignisse

LUN-Ereignisse liefern Ihnen Informationen zum Status Ihrer LUNs, sodass Sie ein Monitoring auf potenzielle Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN Offline(ocumEvtLunOffline)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN zerstört * (lunDestroy)	Ereignis	LUN	Informationsdaten
LUN zugeordnet mit nicht unterstütztem Betriebssystem in igroup(igroupUnsupportedOsType)	Vorfall	LUN	Warnung
Einzel aktiv Pfad für den Zugriff auf LUN(occumEvtLunSingleActivePath)	Dar	LUN	Warnung
Keine aktiven Pfade zum Zugriff auf die LUN (occumEvtLunNoteAbable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade zum Zugriff auf LUN(ocumEvtLunOptimizedPathInaktiv)	Dar	LUN	Warnung
Keine Pfade zum LUN vom HA Partner(ocumEvtLunHaPathInaktiv)	Dar	LUN	Warnung
Kein Pfad zum LUN-Zugriff von einem Knoten im HA-Paar (ocumEvtLunNodePathStatusDown)	Dar	LUN	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unzureichender Speicherplatz für LUN Snapshot Kopie (ocumEvtLunSnapshotmöglich)	Dar	Datenmenge	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN zugeordnet mit nicht unterstütztem Betriebssystem in igroup(igroupUnsupportedOsType)	Dar	LUN	Warnung

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten kritischer Schwellenwert für LUN-IOPS (OktumLunIopsVorfall)	Vorfall	LUN	Kritisch
Unterschreitr. LUN IOPS-Warnungsschwellenwert (ocumLunIopsWarnung)	Dar	LUN	Warnung
LUN MB/s Critical Threshold unchoccumLunMbpsIncident (ocumLunMbpsIncident)	Vorfall	LUN	Kritisch
LUN MB/s Warnschwellenwert nicht eingehalten(ocumLunMbpsWarnung)	Dar	LUN	Warnung
LUN-Latenz ms/op Critical Threshold undurchbrochen (ocumLunenzIncident)	Vorfall	LUN	Kritisch
LUN-Latenz ms/op Warnschwellenwert nicht eingehalten (ocumLunLatenzWarnung)	Dar	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und IOPS – kritischer Schwellenwert – nicht erreicht (ocumLunLatenzenIopsVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und IOPS - Überschreitung des Warnungsschwellenwerts (ocumLunLatenzIopsWarnung)	Dar	LUN	Warnung
LUN-Latenz und MB/s kritischer Schwellenwert überschritten (ocumLunLatenzMbpsVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und MB/s Warnschwellenwert nicht eingehalten(ocumLunenzMbpsWarnung)	Dar	LUN	Warnung
LUN-Latenz und Aggregat-Performance-Kapazität verwendet kritische Schwellenwert verletzt(ocumLunenzaggregatPerformance-AggregatePerformance-KapazitätenUsedVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und verwendete Aggregat-Performance-Kapazität Warnschwellenwert nicht erreicht (ocumLunenzAggregatePerformance-KapazitätenUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und aggregierte Auslastung kritischer Schwellenwert überschritten (ocumLunenzAggregateUtilizationVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und Aggregat-Auslastung Warnschwellenwert nicht erreicht (ocumLunenzAggregateUtilizationWarnung)	Dar	LUN	Warnung
LUN-Latenz und Node-Performance-Kapazität verwendet kritischen Schwellenwert überschritten (ocumLunLatenzenNodePerformance-kapazitätBenutzerfall)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node-Performance-Kapazität – Warnschwellenwert nicht erreicht (ocumLunLatencyNodePerformance-kapazitätUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und verwendete Node-Performance-Kapazität – Takeover Critical Threshold Rected (ocumLunenzyAggregatePerfkapazitätUseTakeoverIncident)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node-Performance-Kapazität - Überschreiten Warnungsschwellenwert (ocumLunenzAggregatePerfkapazitätUseTakeoverWarning)	Dar	LUN	Warnung
LUN-Latenz und Node-Auslastung – kritischer Schwellenwert – nicht erreicht (ocumLunLatenzenNodeUtilizationVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und Node-Auslastung Warnung nicht erreichender Schwellenwert (ocumLunenzNodeUtilizationWarnung)	Dar	LUN	Warnung
QoS LUN Max. IOPS Warnschwellenwert nicht erreicht (ocumQosLunMaxIopsWarnung)	Dar	LUN	Warnung
QoS LUN Max. MB/s Warnschwellenwert verletzt(ocumQosLunMaxMbpsWarnung)	Dar	LUN	Warnung
Workload-LUN-Latenzschwellenwert, der gemäß Definition in der Performance-Service-Level-Richtlinie überschritten wird (ocumConformanceLatencyWarnung)	Dar	LUN	Warnung

Management Station-Events

Management Station-Ereignisse geben Ihnen Informationen über den Status des Servers, auf dem Unified Manager installiert ist, sodass Sie auf mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Management Server Disk Space Fast Full (ocumEvtUnifiedManagerDiskSpaceNearFast Full)	Dar	Management Station	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Freier Speicherplatz auf dem Verwaltungsserver voll (ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Management Station	Kritisch
Management Server, auf dem der Speicher gering ist (ocumEvtUnifiedManagerMemoryLow)	Dar	Management Station	Warnung
Management Server fast nicht genügend Arbeitsspeicher (ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Management Station	Kritisch
Größe der MySQL-Log-Datei erhöht; Neustart erforderlich (ocumEvtMystqlLogFileSizeWarnung)	Vorfall	Management Station	Warnung
Die Zuweisung der Größe des gesamten Prüfprotokolls ist „Jetzt voll“	Dar	Management Station	Warnung
Syslog-Server-Zertifikat – Informationen zum Ablauf	Dar	Management Station	Warnung
Syslog Server-Zertifikat Abgelaufen	Dar	Management Station	Fehler
Audit Log-Datei Manipuliert	Dar	Management Station	Warnung
Audit Log-Datei Gelöscht	Dar	Management Station	Warnung
Syslog-Server-Verbindungsfehler	Dar	Management Station	Fehler
Syslog Server-Konfiguration Geändert	Ereignis	Management Station	Warnung

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Performance Data Analysis is hited(ocumEvtUnifiedManagerDataMissingAnalyze)	Dar	Management Station	Warnung
Performance Data Collection ist betroffen(OktEvtUnifiedManagerDataMissingCollection)	Vorfall	Management Station	Kritisch

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

Veranstaltungen auf der MetroCluster Bridge

MetroCluster Bridge Events informieren Sie über den Status der Bridges. So können Sie auf potenzielle Probleme in einer MetroCluster-over-FC-Konfiguration überwachen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Brücke nicht erreichbar(OktEvtBridgeheUnerreichbar)	Vorfall	MetroCluster-Brücke	Kritisch
Brückentemperatur anormal (occumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster-Brücke	Kritisch

Veranstaltungen für MetroCluster-Konnektivität

Konnektivitätsereignisse bieten Informationen über die Konnektivität zwischen den Komponenten eines Clusters und zwischen den Clustern in MetroCluster über FC und MetroCluster über IP-Konfigurationen, sodass Sie Monitoring auf potenzielle Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

In beiden Konfigurationen übliche Ereignisse

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

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Alle Links zwischen MetroCluster Partnern ausgefallen(occumEvtMetroClusterAllLinksBetweenPartnerDown)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Partner nicht über Peering-Netzwerk erreichbar(ocumEvtMetroClusterPartnerNotErreichbarkeit oberhalb von Netzwerk)	Vorfall	MetroCluster Beziehung	Kritisch
Betroffene MetroCluster Disaster Recovery-Funktion (ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Kritisch
MetroCluster Konfiguration umgeschaltet(ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Warnung

Konfiguration von MetroCluster over FC

Diese Veranstaltungen beziehen sich auf MetroCluster über FC-Konfigurationen.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Alle Inter-Switch Links Down(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster-Inter-Switch-Verbindung	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
FC-SAS Bridge zu Storage Stack Link Down (ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster Konfiguration teilweise umgeschaltet(ocumEvtMetroClusterDRStatusPartially ImpACTED)	Dar	MetroCluster Beziehung	Fehler
Knoten zu FC Switch Alle FC-VI Interconnect Links Down (ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster-Node-Switch-Verbindung	Kritisch
Knoten zu FC Switch ein oder mehrere FC-Initiator Links nach unten(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Dar	MetroCluster-Node-Switch-Verbindung	Warnung
Knoten zu FC Switch Alle FC-Initiator Links nach unten (ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster-Node-Switch-Verbindung	Kritisch
Switch to FC-SAS Bridge FC Link Down (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	Verbindung mit der MetroCluster-Switch-Bridge	Kritisch
Inter Node All FC VI Interconnect Links Down (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen Knoten	Kritisch
Inter Node One oder More FC VI Interconnect Links Down (ocumEvtMccInterNodeLinksOneOrMoreDown)	Dar	Verbindung zwischen Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Knoten zu Brücke Link nach unten (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Node-Bridge-Verbindung	Kritisch
Node zu Storage Stack All SAS Links Down (ocumEvtMccNodeStackLinksDown)	Vorfall	Node-Stack-Verbindung	Kritisch
Knoten zu Storage-Stack eine oder mehrere SAS-Links nach unten (occumEvtMccNodeStackLinksOneOrMoreDown)	Dar	Node-Stack-Verbindung	Warnung

Konfiguration von MetroCluster over IP

Diese Ereignisse betreffen MetroCluster über IP-Konfigurationen.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
MetroCluster IP-Verbindungsstatus der intersite ist ausgefallen (mcIntersitectureityStatusDown)	Dar	MetroCluster Beziehung	Kritisch
MetroCluster-IP Node zu Switch-Offline-Verbindung (mcIpPortStatusOffline)	Dar	Knoten	Fehler

Ereignisse auf dem MetroCluster-Switch

MetroCluster Switch-Ereignisse für MetroCluster-over-FC-Konfigurationen bieten Ihnen Informationen zum Status der MetroCluster-Switches, damit Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Schalttemperatur anormal (OktEvtSwitchTemperaturAbnormal)	Vorfall	MetroCluster-Switch	Kritisch
Switch nicht erreichbar (ocumEvtSwitchnicht erreichbar)	Vorfall	MetroCluster-Switch	Kritisch
Switch-Lüfter fehlgeschlagen (ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster-Switch	Kritisch
Switch-Netzteile fehlgeschlagen (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster-Switch	Kritisch
Schalter Temperatursensoren fehlgeschlagen (OcumEvtSwitchTemperatursensordefekt) Dieses Ereignis gilt nur für Cisco Switches.	Vorfall	MetroCluster-Switch	Kritisch

NVMe Namespace-Ereignisse

NVMe Namespace Ereignisse liefern Ihnen Informationen zum Status Ihrer Namespaces, damit Sie ein Monitoring auf potenzielle Probleme ermöglichen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

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

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVMe Offline *(nvmeNamespaceStatus Offline)	Ereignis	Namespace	Informationsdaten
NVMe Online * (nvmeNamespaceStatus Online)	Ereignis	Namespace	Informationsdaten
NVMe außerhalb des Speicherplatzes * (nvmeNamespaceSpace OutOfSpace)	Dar	Namespace	Warnung
NVMeNS Destroy * (nvmeNamespaceDestroy)	Ereignis	Namespace	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten des kritischen Schwellenwerts für NVMe-Namespace-IOPS (ocumNvmeNamespaceIopsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace IOPS – Warnung nicht behebter Schwellenwert (ocumNvmeNamespaceIopsWarnung)	Dar	Namespace	Warnung
NVMe Namespace MB/s Critical Threshold Undurchbrochen (ocumNvmeNamespaceMbpsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace MB/s Warnschwellenwert nicht eingehalten (ocumNvmeNamespaceMbpsWarnung)	Dar	Namespace	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVMe Namespace-Latenz ms/op Critical Threshold Undurchbrochen (ocumNvmeNamespeaceLatenturVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz ms/op Warnschwellenwert nicht eingehalten (ocumNvmeNamespaceLatency – Warnung)	Dar	Namespace	Warnung
NVMe Namespace-Latenz und IOPS-kritischer Schwellenwert – nicht erreicht (ocumNvmeNamespaceLatenzenIopsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz und IOPS Warnschwellenwert nicht erreicht (ocumNvmeNamespaceLatentenzIopsWarnung)	Dar	Namespace	Warnung
NVMe Namespace-Latenz und MB/s kritischer Schwellenwert – nicht überschritten (ocumNvmeNamespaceLatenzenMbpsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz und MB/s Warnschwellenwert nicht eingehalten (ocumNvmeNamespaceLatentenzMbpsWarnung)	Dar	Namespace	Warnung

Node-Ereignisse

Node-Ereignisse bieten Ihnen Informationen zum Node-Status, sodass Sie Ihr System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp

und den Schweregrad.

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

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Node-Root-Volume-Speicherplatz fast voll (ocumEvtClusterNodeRootVolumeSpaceNearline)	Dar	Knoten	Warnung
Cloud AWS MetaDataConnFail * (ocumCloudAwsMetadataConnFail)	Dar	Knoten	Fehler
Cloud AWS IAMCredsExpired * (ocumCloudAwsIamCredsExpired)	Dar	Knoten	Fehler
Cloud AWS IAMCredsIngültig * (ocumCloudAwsIamCredsungültig)	Dar	Knoten	Fehler
Cloud AWS IAMCredsNotFound * (ocumCloudAwsIamCredsNotFound)	Dar	Knoten	Fehler
Cloud AWS IAMCredsNotinitialisiert * (ocumCloudAwsIamCredsNotinitialisiert)	Ereignis	Knoten	Informationsdaten
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Dar	Knoten	Fehler
Cloud AWS IAMRoleNotFound * (ocumCloudAwsIamRoleNotFound)	Dar	Knoten	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unlösbar für Cloud Tier Host * (ocumObjstoreHostUnlösbar)	Dar	Knoten	Fehler
Cloud Tiering Intercluster-Netzwerkschnittstelle * (ocumObjstoreInterClusterLifDown)	Dar	Knoten	Fehler
Einer der NFSv4 Pools erschöpft * (nbladeNfsv4PoolEXhaust)	Vorfall	Knoten	Kritisch
Unmatch Cloud Tier Signature *(osbosnatureMismatch) anfordern	Dar	Knoten	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
QoS Monitor Memory maxed * (ocumQosMonitorMemory)	Dar	Knoten	Fehler
QoS Monitor Memory abited *(ocumQosMonitorMemoryAbed)	Ereignis	Knoten	Informationsdaten

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Knoten umbenannt(nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht behebgter Node-IOPS-Schwellenwert (OktumNodeIopsVorfall)	Vorfall	Knoten	Kritisch
Nicht beIOPS-Warnungsschwellenwert (OktumNodeIopsWarnung)	Dar	Knoten	Warnung
Node-MB/s – kritischer Schwellenwert überschritten (ocumNodeMbpsVorfall)	Vorfall	Knoten	Kritisch
Knoten MB/s Warnschwellenwert überschritten(OccumNodeMbpsWarnung)	Dar	Knoten	Warnung
Node-Latenz ms/op Critical Threshold undurchbrochen (OktumNodeLatenzIncident)	Vorfall	Knoten	Kritisch
Node-Latenz ms/op Warnschwellenwert nicht überschritten (OktumNodeLatenWarnung)	Dar	Knoten	Warnung
Node-Performance-Kapazität verwendet kritischen Schwellenwert verletzt (OktumNodePerftätNutzungVorfall)	Vorfall	Knoten	Kritisch
Verwendete Node-Performance-Kapazität, Warnschwellenwert nicht erreicht (ocumNodePerfkapazitätUsedWarnung)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Verwendete Node-Performance-Kapazität – Übernahme durch kritischen Schwellenwert überschritten (OktumNodePerftätNutzungTakeoverVorfall)	Vorfall	Knoten	Kritisch
Verwendete Node-Performance-Kapazität – Überschreitung der Warnschwelle (nicht erreicht wegen Performance-Performance-Performance-Kapazitäts-UseTakeoverWarning)	Dar	Knoten	Warnung
Unterschreitem kritischen Schwellenwert für die Node-Auslastung (OkumNodeUtilizationVorfall)	Vorfall	Knoten	Kritisch
Unterschreitr. Schwellenwert für Node-Auslastung (OkumNodeUtilizationWarnung)	Dar	Knoten	Warnung
Überlasteter Schwellenwert für Node-HA-Paar (OktumNodeHaPairOverUtilizedInformation)	Ereignis	Knoten	Informationsdaten
Unterschreitender Schwellenwert für die Node-Festplattenfragmentierung (ocumNodeDiskFragmentationWarnung)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht genutzter Performance-Kapazitätsschwellenwert (OktumNodeÜberschreitung Warnung)	Dar	Knoten	Warnung
Nicht behebener dynamischer Knotenschwellenwert (ocumNodeDynamicEvent Warnung)	Dar	Knoten	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Advisory ID: NTAP-<__Advisory ID_>(ocumx)	Dar	Knoten	Kritisch

Ereignisse der NVRAM-Batterie

NVRAM-Batterieereignisse geben Ihnen Informationen zum Status Ihrer Akkus, sodass Sie auf mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVRAM-Batterie schwach(OktEvtNvraBatterienNiedrig)	Dar	Knoten	Warnung
Entladene NVRAM-Batterie (OktEvtNvramBatteryEntladung)	Dar	Knoten	Fehler
NVRAM-Batterie übermäßig geladen (OktEvtNvramBatteryÜberCharged)	Vorfall	Knoten	Kritisch

Port-Ereignisse

Port-Ereignisse bieten Ihnen den Status zu Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, z. B. ob der Port ausgefallen ist.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Port Status Down (ocumEvtPortStatusDown)	Vorfall	Knoten	Kritisch

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Port MB/s kritischer Schwellenwert überschritten (ocumNetworkPortMbpsVorfall)	Vorfall	Port	Kritisch
Netzwerk-Port MB/s Warnschwellenwert nicht eingehalten (ocumNetworkPortMbpsWarnung)	Dar	Port	Warnung
MB/s kritischer Schwellenwert für FCP-Port überschritten (ocumFcpPortMbpsVorfall)	Vorfall	Port	Kritisch
MB/s-Warnschwellenwert für FCP-Port überschritten(ocumFcpPortMbpsWarnung)	Dar	Port	Warnung
Auslastung des Netzwerkports – kritischer Schwellenwert – unterlaufen (NetzwerkPortUtilizationVorfall)	Vorfall	Port	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Warnung über Netzwerk-Port-Auslastung, nicht überschritten (OktumNetzwerkPortUtilizationWarnung)	Dar	Port	Warnung
Unterschreitender Schwellenwert für die FCP-Port-Auslastung (ocumFcpPortUtilizationVorfall)	Vorfall	Port	Kritisch
Warnung: Nicht gestauter Schwellenwert für die FCP-Port-Auslastung (ocumFcpPortUtilizationWarnung)	Dar	Port	Warnung

Netzteile

Netzteile liefern Ihnen Informationen über den Status Ihrer Hardware, sodass Sie Monitoring auf potenzielle Probleme ermöglichen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Ein oder mehrere ausgefallene Netzteile (ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Knoten	Kritisch

Schutzereignisse

Schutzereignisse geben an, ob ein Job ausgefallen ist oder abgebrochen wurde, damit Sie eine Überwachung auf Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Schutzjob fehlgeschlagen (ocumEvtProtectionJobTaskFailed)	Vorfall	Volume oder Storage-Service	Kritisch
Schutzauftrag abgebrochen(OktaVerkündungSchutzJobAbgebrochen)	Dar	Volume oder Storage-Service	Warnung

Qtree Ereignisse

Qtree Events liefern Ihnen Informationen zur qtree Kapazität sowie Datei- und Festplattengrenzwerte, damit Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Qtree Space nahezu vollständig (ocumEvtQtreeSpaceNearFull)	Dar	Qtree	Warnung
Qtree Space Full(ocumEvtQtreeSpaceFull)	Dar	Qtree	Fehler
Qtree Space normal(ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Informationsdaten
Harte Grenze für qtree Dateien erreicht(ocumEvtQtreeDateienHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree-Dateien Grenzverletzungen weichen(occumEvtQtreeDateienSoftLimitBreached)	Dar	Qtree	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Qtree Space Hard Limit erreicht(ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree Space Soft Limit Procted (ocumEvtQtreeSpaceSoftLimitBreached)	Dar	Qtree	Warnung

Ereignisse des Service-Prozessors

Bei Service-Prozessor-Ereignissen erhalten Sie Informationen über den Status Ihres Prozessors. Diese Informationen können Sie auf potenzielle Probleme überwachen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Service Processor nicht konfiguriert (ocumEvtServiceProcessorNotConfigured)	Dar	Knoten	Warnung
Service Processor Offline(ocumEvtServiceProcessorOffline)	Dar	Knoten	Fehler

SnapMirror Beziehungsereignisse

SnapMirror Beziehungsereignisse geben Ihnen Informationen zum Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie mögliche Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage VMs als auch für Volumes generiert, synchrone SnapMirror Beziehungsereignisse werden jedoch nur für Volume-Beziehungen erstellt. Es gibt keine Ereignisse für zusammengehörige Volumes, die Teil der Disaster-Recovery-Beziehungen für Storage VMs sind. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

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

Die Ereignisse der SnapMirror Beziehungen werden für Storage VMs generiert, die durch die Disaster Recovery von Storage VM gesichert sind, jedoch nicht für einzelne Objektbeziehungen.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Spiegelreplikation ungesund(occumEvtSnapmirrorRelationshipUnHealthy)	Dar	SnapMirror Beziehung	Warnung
Spiegelreplikation - broken-off(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation wird initialisiert fehlgeschlagen(OktEvtSnapmirrorRelationshipInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipUpdateFailed)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation – Fehler (occumEvtSnapMirrorRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation Verzögerung Warnung(occumEvtSnapMirrorRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung
Resync der Spiegelreplikation fehlgeschlagen(OccumEvtSnapmirrorRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler
Synchronous Replication Out of Sync * (syncSnapmirrorRelationshipOutofsync)	Dar	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Synchrone Replizierung wiederhergestellt * (syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror Beziehung	Informationsdaten
Synchronous Replication Auto Resync failed * (Synchronisieren von SnapmirrorRelationshipAutoSyncRetryFailed)	Dar	SnapMirror Beziehung	Fehler
ONTAP Mediator wird auf dem Cluster hinzugefügt (SnapmirrorMediatorHinzugefügt)	Ereignis	Cluster	Informationsdaten
ONTAP Mediator wird aus dem Cluster entfernt (SnapmirrorMediatorRemoved)	Ereignis	Cluster	Informationsdaten
ONTAP Mediator ist vom Cluster nicht erreichbar (SnapmirrorMediatornicht erreichbar)	Dar	Mediator	Warnung
Zugriff auf ONTAP Mediator ist über das Cluster nicht möglich (SnapmirrorMediatorMiskonfiguriert)	Dar	Mediator	Fehler
ONTAP Mediator Connectivity wurde neu eingerichtet, neu synchronisiert und bereit für SnapMirror Active Sync (snapmirrorMediatorInQuorum)	Ereignis	Mediator	Informationsdaten

Ereignisse für asynchrone Spiegelung und Vault Beziehungen

Die Beziehungsereignisse von Asynchronous Mirror und Vault liefern Ihnen Informationen zum Status Ihrer asynchronen SnapMirror- und Vault-Beziehungen, damit Sie das System auf potenzielle Probleme überwachen können. Ereignisse für asynchrone Mirror- und Vault-Beziehungen werden sowohl für Volume- als auch für Storage VM-

Sicherungsbeziehungen unterstützt. Aber für das Disaster Recovery von Storage VM werden nicht nur Vault-Beziehungen unterstützt. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Die Ereignisse zu SnapMirror und Vault Beziehungen werden auch für Storage VMs generiert, die durch die Disaster Recovery von Storage VM geschützt sind, jedoch nicht für einzelne Objektbeziehungen.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Asynchroner Spiegel und Vault ungesund (OktMirrorVaultRelationshipUngesund)	Dar	SnapMirror Beziehung	Warnung
Asynchrones Spiegeln und Vault broken-off(ocumEvtMirrorVaultRelationshipSteateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Asynchrone Spiegelung und Vault Initialisieren fehlgeschlagen (OktEvtMirrorVaultRelationshierInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Asynchrones Spiegeln und Vault-Update fehlgeschlagen (ocumEvtMirrorVaultRelationshipUpdatefehlgeschlagen)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Mirror und Vault lag Fehler (ocumEvtMirrorVaultRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Mirror und Vault lag Warnung(OccumEvtMirrorVaultRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Resync für asynchronen Spiegel und Vault fehlgeschlagen (OcumEvtMirrorVaultRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler

Das Ereignis „SnapMirror Update Failure“ wird vom Active IQ Portal (Config Advisor) angehoben.

Snapshot Ereignisse

Snapshot Ereignisse liefern Informationen zum Status von Snapshots, mit denen Sie die Snapshots auf potenzielle Probleme überwachen können. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Snapshot Auto-delete deaktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Löschung von Snapshot aktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Snapshot Auto-delete-Konfiguration geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

SnapVault Beziehungsereignisse

SnapVault Beziehungsveranstaltungen enthalten Informationen zum Status Ihrer SnapVault Beziehungen, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Asynchronous Vault ungesund(OcumEvtSnapVaultRelationshipUnHealthy)	Dar	SnapMirror Beziehung	Warnung
Asynchronous Vault broken-off (ocumEvtSnapVaultRelationshipStateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Asynchrone Vault-Initialisierung fehlgeschlagen (OktEvtSnapVaultRelationshierInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Asynchrones Vault Update fehlgeschlagen (OktEvtSnapVaultRelationshipUpdateFailed)	Dar	SnapMirror Beziehung	Fehler
Asynchroner Vault lag Fehler (ocumEvtSnapVaultRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Vault lag Warnung (ocumEvtSnapVaultRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung
Resync für asynchronen Tresor fehlgeschlagen (ocumEvtsnapvaultRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler

Ereignisse auf Storage-Failover-Einstellungen

Ereignisse im Rahmen der Storage-Failover-Einstellungen (SFO) informieren Sie darüber, ob Ihr Storage-Failover deaktiviert oder nicht konfiguriert ist, damit Sie das System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage Failover Interconnect eine oder mehrere Links nach unten (OktEvtSfoVerbindungsOneOrMehrLinksDown)	Dar	Knoten	Warnung
Storage Failover deaktiviert(ocumEvtSfoSettingsdeaktiviert)	Dar	Knoten	Fehler
Storage-Failover nicht konfiguriert(ocumEvtSfoSettingsNotConfigured)	Dar	Knoten	Fehler
Storage-Failover-Status – Übernahme (OktEvtSfoStateTakeover)	Dar	Knoten	Warnung
Storage Failover State - Partial GiveBack(ocumEvtSfoStatePartialGiveBack)	Dar	Knoten	Fehler
Storage Failover Node Status Down (ocumEvtSfoNodeStatusDown)	Dar	Knoten	Fehler
Storage-Failover-Übernahme nicht möglich (OktEvtSfoÜbernahmemöglich)	Dar	Knoten	Fehler

Ereignisse auf Storage-Services

Bei Storage-Services-Ereignissen erhalten Sie Informationen über die Erstellung und das Abonnement von Storage-Services, sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage-Service erstellt(nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten
Storage Service abonniert (nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten
Storage Service nicht abonniert (nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unerwartetes Löschen von Managed SnapMirror RelationshipokumEvtStorageServiceUnsupportedRelationshipDeltion	Dar	Storage-Service	Warnung
Unerwartetes Löschen von Storage Service Member Volume(occumEvtStorageServiceUnexpectedVolumeDeltion)	Vorfall	Storage-Service	Kritisch

Storage-Shelf-Ereignisse

Storage Shelf-Ereignisse geben an, ob Ihr Storage Shelf anormal ist, sodass Sie nach potenziellen Problemen überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Anormaler Spannungsbereich (ocumEvtShelfVoltageAbnormal)	Dar	Storage Shelf	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Anormaler Strombereich (ocumEvtShelfAktuellesAbnormal)	Dar	Storage Shelf	Warnung
Anormale Temperatur(OkumEvtShelfTemperatureAbnormal)	Dar	Storage Shelf	Warnung

Ereignisse von Storage-VM

Ereignisse der Storage-VM (Storage Virtual Machine, auch als SVM bekannt) bieten Ihnen Informationen zum Status Ihrer Storage-VMs (SVMs), sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

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

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage VM CIFS Service Down (ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
Versuche, nicht vorhandene CIFS Share zu verbinden *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch
CIFS NetBIOS Namenskonflikt * (nbladeCifsNbNameConflict)	Dar	SVM	Fehler
CIFS Shadow Copy Operation fehlgeschlagen *(cifsShadowCopyFailure)	Dar	SVM	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Viele CIFS-Verbindungen * (nbladeCifsManyAuths)	Dar	SVM	Fehler
Max. CIFS-Verbindung überschritten * (nbladeCifsMaxOpenSameFile)	Dar	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten *(nbladeCifsMaxSessPerusrConn)	Dar	SVM	Fehler
SVM FC/FCoE Service-Down (ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM iSCSI Service-Down(ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
Storage VM NFS Service Down(ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM FC/FCoE-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM iSCSI-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM NFS-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
Storage VM angehalten (ocumEvtVserverDown)	Dar	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
AV-Server zu beschäftigt, um neue Scananforderung zu akzeptieren *(nbladeVscanConnBackPressure)	Dar	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Dar	SVM	Fehler
Keine Responsive AV-Serververbindung *(nbladeVscanConnInaktiv)	Ereignis	SVM	Informationsdaten
Nicht autorisierter Benutzerversuch für AV-Server *(nbladeVscanBadUserPrivAccess)	Dar	SVM	Fehler
Virus von AV Server gefunden *(nbladeVscanVirusDetected)	Dar	SVM	Fehler

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM erkannt (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM gelöscht (nicht zutreffend)	Ereignis	Cluster	Informationsdaten
SVM umbenannt (nicht zutreffend)	Ereignis	SVM	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitkter SVM-IOPS-Schwellenwert (OktumSvmIopsVorfall)	Vorfall	SVM	Kritisch
Unterschreiten SVM-IOPS-Warnungsschwellenwert (ocumSvmIopsWarnung)	Dar	SVM	Warnung
SVM MB/s Critical Threshold ToctusctusSvmMbpsVorfall)	Vorfall	SVM	Kritisch
SVM MB/s Warnschwellenwert überschritten (ocumSvmMbpsWarnung)	Dar	SVM	Warnung
Unterschreiten kritischen Schwellenwert für SVM-Latenz (ocumSvmLatencyVorfall)	Vorfall	SVM	Kritisch
Unterschreitung – SVM-Latenzschwellenwert (ocumSvmLatencyWarnung)	Dar	SVM	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Audit Log deaktiviert(ocumVserverAuditLogdeaktiviert)	Dar	SVM	Warnung
Login Banner deaktiviert(ocumVserverLoginBannerdeaktiviert)	Dar	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SSH verwendet unsichere Chiffren (ocumVserverSSHInSecure)	Dar	SVM	Warnung
Login Banner geändert(ocumVserverLoginBannerChanged)	Dar	SVM	Warnung
Anti-Ransomware-Überwachung von Storage-VMs ist deaktiviert (antiErlöserSvmStatedeaktiviert)	Dar	SVM	Warnung
Das Anti-Ransomware-Monitoring für Storage VMs ist aktiviert (Learning Mode) (antiBefreiwareSvmStateDryrun).	Ereignis	SVM	Informationsdaten
Storage VM geeignet für die Ransomware-Überwachung (Learning Mode) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Informationsdaten

Ereignisse für Benutzer- und Gruppenkontingente

Benutzer- und Gruppenkontingente liefern Ihnen Informationen über die Kapazität des Benutzer- und Benutzergruppenkontingens sowie über die Datei- und Festplattenlimits, damit Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
User- oder Group Quota Disk Space Soft Limit Proceed (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Dar	Benutzer- oder Gruppenkontingente	Warnung
Hard Limit für User- oder Group Quota Disk Space (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingente	Kritisch
Anzahl der Benutzer- oder Gruppenkontingente-Dateien weiche Grenze überschritten (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Dar	Benutzer- oder Gruppenkontingente	Warnung
Benutzer- oder Gruppenkontingente Dateianzahl harte Grenze erreicht(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingente	Kritisch

Volume-Ereignisse

Volume-Ereignisse liefern Informationen zum Status von Volumes, mit denen Sie auf potenzielle Probleme überwachen können. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

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

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumenbeschränkungen (occumEvtVolumeRestricted)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume Offline(ocumEvtVolumeOffline)	Vorfall	Datenmenge	Kritisch
Datenträger teilweise verfügbar(occumEvtVolumePartiallyverfügbar)	Dar	Datenmenge	Fehler
Volumen abgehängt (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume angehängt(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume neu eingebunden (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume Junction Path Inaktiv (ocumEvtVolumeJunctionPathInaktiv)	Dar	Datenmenge	Warnung
Automatische Volumengröße aktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Volume-Größe deaktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Volumengröße maximale Kapazität geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Größe der automatischen Volume-Größe geändert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Speicherplatz mit Thin Provisioning (ozumThinProvisionVolumeSpaceAtFestplatten)	Dar	Datenmenge	Warnung
Volume Efficiency Operation Error(ocumEvtVolumeEfficiency OperationError)	Dar	Datenmenge	Fehler
Voll Volume-Speicherplatz(occumEvtVolumeFull)	Dar	Datenmenge	Fehler
Volume fast voll (ocumEvtVolumeNearline)	Dar	Datenmenge	Warnung
Logischer Speicherplatz des Volume voll * (VolumeLogicalSpaceFull)	Dar	Datenmenge	Fehler
Logischer Speicherplatz des Volume fast voll * (VolumeLogicalSpaceNearlyFull)	Dar	Datenmenge	Warnung
Logischer Speicherplatz des Volume normal *(VolumeLogicalSpaceAllOK)	Ereignis	Datenmenge	Informationsdaten
Volume Snapshot Reserve voll(ocumEvtSnapshotvoll)	Dar	Datenmenge	Warnung
Zu viele Snapshot-Kopien (ocumEvtSnapshotTooManche)	Dar	Datenmenge	Fehler
Volume Qtree Kontingent überengagiert (occumEvtVolumeQtreeQuotaÜberengagiert)	Dar	Datenmenge	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume Qtree Kontingent fast überengagiert (ocumEvtVolumeQtreeQuotaAlmostÜberengagiert)	Dar	Datenmenge	Warnung
Volumenwachstumsrate anormal (ocumEvtVolumeGrowth RowthRateAbnormal)	Dar	Datenmenge	Warnung
Volume-Tage bis voll (ocumEvtVolumeTagesUntilFullSoon)	Dar	Datenmenge	Fehler
Volume Space Guarantee deaktiviert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Space-Garantie Aktiviert (Nicht Zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Space-Garantie geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume Snapshot Reserve – Tage bis voll (ocumEvtVolumeSnapshotReserviertDaysUntilFullSoon)	Dar	Datenmenge	Fehler
FlexGroup-Komponenten haben Raumprobleme *(FlexGroupInhaltHaveSpaceIssues)	Dar	Datenmenge	Fehler
FlexGroup-Komponenten Raumstatus alles OK *(flexGruppeKonstitelenSpaceStatusAllOK)	Ereignis	Datenmenge	Informationsdaten
FlexGroup-Bestandteile haben Inodes-Probleme *(flexGroupKonstitutionenHaveInodesIssues)	Dar	Datenmenge	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
FlexGroup-Komponenten inodes Status alles OK *(flexGroupConstitutionenInodesStatusAllOK)	Ereignis	Datenmenge	Informationsdaten
Fehler bei der WAFL-Volume-AutoSize * (WaflVolAutoSizeFail)	Dar	Datenmenge	Fehler
Automatische WAFL-Volume-Größe abgeschlossen * (WaflVolAutoSizeDone)	Ereignis	Datenmenge	Informationsdaten
FlexGroup Volumen ist über 80% ausgelastet*	Vorfall	Datenmenge	Fehler
FlexGroup Volumen ist über 90% ausgelastet*	Vorfall	Datenmenge	Kritisch
Volume Storage-Effizienz-Anomalie (ocumVolumeAbnormalStorageEffizienzWarnung)	Dar	Datenmenge	Warnung
Volume Snapshot-Reserve wird nicht genutzt (VolumeSnaphotReserveUnderutilizedWarnung)	Ereignis	Datenmenge	Warnung
Volume Snapshot Reserve wird nicht genutzt (VolumeSnaphotReserveUnderutilizedCleared)	Ereignis	Datenmenge	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumen umbenannt(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Ermittelte Volumes (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume gelöscht (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
QoS Volume Max. IOPS Warnschwellenwert nicht erreicht (ocumQosVolumeMaxIopsWarnung)	Dar	Datenmenge	Warnung
QoS-Volume max. MB/s Warnschwellenwert überschritten(ocumQosVolumeMaxMbpsWarnung)	Dar	Datenmenge	Warnung
QoS Volume Max. IOPS/TB Warnschwellenwert nicht erreicht (ocumQosVolumeMaxIopsPerTbWarnung)	Dar	Datenmenge	Warnung
Überschreitung des Workload-Volume-Latenzschwellenwerts gemäß Definition der Performance-Service-Level-Richtlinie (ocumConformanceLatency Warning)	Dar	Datenmenge	Warnung
Unterschreiten des kritischen Schwellenwerts für Volume-IOPS (OktumVolumeIopsVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitr. Volume IOPS-Warnungsschwellenwert (ocumVolumeIopsWarnung)	Dar	Datenmenge	Warnung
Unterschreiten kritischen Schwellenwert für Volume-MB/s (ocumVolumeMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Volume MB/s Warnschwellenwert überschritten(OccumVolumeMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz – kritischer Schwellenwert überschritten (ocumVolumeLatenzIncident)	Vorfall	Datenmenge	Kritisch
Schwellenwert für Volume-Latenzwarnung überschritten (ocumVolumeLatencyWarnung)	Dar	Datenmenge	Warnung
Volume Cache Miss-Verhältnis – kritischer Schwellenwert überschritten (ocumVolumeCacheMissRatioVorfall)	Vorfall	Datenmenge	Kritisch
Volume Cache Miss Ratio Warnung nicht überschritten (ocumVolumeCacheMissRatioWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und IOPS – kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyIopsVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht erreichender Volume-Latenz und IOPS -Warnungsschwellenwert (ocumVolumeLatencyIops Warnung)	Dar	Datenmenge	Warnung
Volume-Latenz und MB/s kritischer Schwellenwert – nicht überschritten (ocumVolumeLatencyMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und MB/s Warnschwellenwert nicht eingehalten (ocumVolumeLatencyMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und Aggregat-Performance-Kapazität eingesetzt. Kritischer Schwellenwert ist nicht erreicht (ocumVolumeLatencyAggregatePerformance-KapazitätenUsedVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und verwendete Aggregat-Performance-Kapazität Warnschwellenwert nicht erreicht (ocumVolumeLatencyAggregatePerformance-KapazitätenUsedWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und aggregierte Auslastung kritischer Schwellenwert überschritten (ocumVolumeLatenAggregateUtilizationVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Latenz und Aggregatauslastung Warnschwellenwert nicht erreicht (ocumVolumeLatenAggregateUtilizationWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und Node-Performance-Kapazität verwendet kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyNodePerformance-kapazitätBenutzerfall)	Vorfall	Datenmenge	Kritisch
Verwendete Volume-Latenz und Node-Performance-Kapazität – Warnschwellenwert nicht erreicht (ocumVolumeLatencyNodePerformance-kapazitätUsedWarnung)	Dar	Datenmenge	Warnung
Verwendete Volume-Latenz und Node-Performance-Kapazität – Überschreiten kritischer Schwellenwert (ocumVolumeLatencyAggregatePerfkapazitätUseTakeoverIncident)	Vorfall	Datenmenge	Kritisch
Verwendete Volume-Latenz und Node-Performance-Kapazität – Überschreitung der Schwellenwertverletzungen (ocumVolumeLatencyAggregatePerfkapazitätUseTakeoverWarning)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Latenz und Node-Auslastung – kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyNotilationVorfall)	Vorfall	Datenmenge	Kritisch
Nicht erreichender Schwellenwert für Volume-Latenz und Node-Auslastung (ocumVolumeLatencyNodeUtilizationWarnung)	Dar	Datenmenge	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Anti-Ransomware-Überwachung ist aktiviert (aktiv-Modus) (antiBefreieVolumeaktiviert)	Ereignis	Datenmenge	Informationsdaten
Volume-Anti-Ransomware-Überwachung ist deaktiviert (antiBefreieVolumeSpeicherdeaktiviert)	Dar	Datenmenge	Warnung
Volume-Anti-Ransomware-Überwachung ist aktiviert (Learning Mode) (antiBefreieVolumeStateDryrun)	Ereignis	Datenmenge	Informationsdaten
Volume Anti-Ransomware Monitoring ist angehalten (Learning Mode) (antiBefreiwareVolumeStateDryrunPen)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Anti-Ransomware-Überwachung ist angehalten (aktiver Modus) (antiBefreieVolumeSpeicherErd)	Dar	Datenmenge	Warnung
Anti-Ransomware-Monitoring auf Volume wird deaktiviert (AntiErlöserVolumeSpeicherErsternInProgress)	Dar	Datenmenge	Warnung
Aktivitäten durch Ransomware (CallHomeBefreiwareActivitySeen)	Vorfall	Datenmenge	Kritisch
Volume geeignet für die Anti-Ransomware-Überwachung (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Datenmenge	Informationsdaten
Volume geeignet für die Anti-Ransomware-Überwachung (aktiver Modus) (ocumVolumeSuitedForActiveAntiBefreiwareDetection)	Dar	Datenmenge	Warnung
Volume weist eine laute Anti-Ransomware-Warnung auf (antiBefreiwareFeatureNoisyVolume)	Dar	Datenmenge	Warnung

Impact-Bereich: Datensicherung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (VolumeLackLocalProtectionWarnung)	Dar	Datenmenge	Warnung
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (VolumeLackLocalProtectionCleared)	Dar	Datenmenge	Warnung

Statusereignisse für Volume-Verschiebung

Status-Events zur Volume-Verschiebung informieren Sie über den Status Ihrer Volume-Verschiebung, sodass Sie Ihr System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Status der Volume-Verschiebung: In Bearbeitung (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Status der Volume-Verschiebung – fehlgeschlagen (OktEvtVolumeMoveFailed)	Dar	Datenmenge	Fehler
Status der Volume-Verschiebung: Abgeschlossen (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Verschiebung - zurückgeschobener Umstieg (OktEvtVolumeMoveCustoverDeferred)	Dar	Datenmenge	Warnung

Beschreibung der Ereignisfenster und Dialogfelder

Ereignisse informieren Sie über Probleme in Ihrer Umgebung. Sie können die Seite „Lagerbestand für das Ereignismanagement“ und die Seite „Ereignisdetails“ verwenden, um alle Ereignisse zu überwachen. Über das Dialogfeld „Benachrichtigungseinstellungen“ können Sie Benachrichtigungen konfigurieren. Mithilfe der Seite Event Setup können Sie Ereignisse deaktivieren bzw. aktivieren.

Benachrichtigungsseite

Sie können den Unified Manager-Server so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder wenn es einem Benutzer zugewiesen ist. Sie können auch die Benachrichtigungsmechanismen konfigurieren. Benachrichtigungen können beispielsweise als E-Mails oder SNMP-Traps gesendet werden.

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

E-Mail

In diesem Bereich können Sie die folgenden E-Mail-Einstellungen für die Benachrichtigung von Warnmeldungen konfigurieren:

- * Von Adresse*

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

SMTP-Server

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

- **Hostname oder IP-Adresse**

  Gibt den Hostnamen Ihres SMTP-Hostservers an, der dazu verwendet wird, die Benachrichtigung an die angegebenen Empfänger zu senden.

- **Benutzername**

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

- **Passwort**

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

- **Port**

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

Der Standardwert ist 25.

- **Start/TLS verwenden**

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

- * Verwenden Sie SSL*

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

SNMP

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

- **Version**

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

- **Trap Destination Host**

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

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

- * Ausgebundener Trap Port*

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

  Der Standardwert ist 162.

- **Gemeinschaft**

  Die Community-Zeichenfolge für den Zugriff auf den Host.

- **Motor-ID**

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

- **Benutzername**

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

- **Authentifizierungsprotokoll**

  Gibt das Protokoll an, das zur Authentifizierung eines Benutzers verwendet wird. Die Protokolloptionen umfassen MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist verfügbar mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung.

- **Authentifizierungskennwort**

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

- **Datenschutzprotokoll**

  Gibt das Datenschutzprotokoll an, das zur Verschlüsselung von SNMP-Nachrichten verwendet wird. Die Protokolloptionen umfassen AES 128 und DES. Der Standardwert ist AES 128. Das Datenschutzprotokoll ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzkennwort**

  Gibt das Passwort an, wenn das Datenschutzprotokoll verwendet wird. Das Passwort für den Datenschutz ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Für weitere Informationen über SNMP-Objekte und Traps können Sie die herunterladen "Active IQ Unified Manager MIB" Von der NetApp Support Site aus.

Inventarseite des Ereignismanagements

Auf der Seite „Ereignismanagement-Bestand“ können Sie eine Liste aktueller Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie Quittieren, Auflösen und Zuweisen von Ereignissen durchführen. Sie können auch eine Meldung für bestimmte Ereignisse hinzufügen.

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

Komponenten filtern

Hier können Sie die in der Ereignisliste angezeigten Informationen anpassen. Sie können die Liste der Ereignisse, die mit den folgenden Komponenten angezeigt werden, verfeinern:

- Menü Ansicht zur Auswahl aus einer vordefinierten Liste von Filterauswahlen.

  Dazu gehören beispielsweise alle aktiven (neuen und bestätigten) Ereignisse, aktive Performanceereignisse, mir zugewiesene Ereignisse (der angemeldete Benutzer) und alle während aller Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Liste der Ereignisse durch Eingabe vollständiger oder teilweiser Begriffe.
- Die Filterschaltfläche öffnet den Fensterbereich Filter, sodass Sie aus jedem verfügbaren Feld und Feldattribut auswählen können, um die Ereignisliste zu verfeinern.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zuweisen Zu**

  Hiermit können Sie den Benutzer auswählen, dem das Ereignis zugeordnet ist. Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der Sie das Ereignis zugewiesen haben, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  - Ich

    Weist das Ereignis dem derzeit angemeldeten Benutzer zu.

  - Einem anderen Benutzer

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

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der 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.

  Sie können keine Informationsereignisse bestätigen.

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

  Wenn Sie ein Ereignis auflösen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis aufgelöst haben, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Alarm Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie Warnmeldungen für die ausgewählten Ereignisse hinzufügen können.

- **Berichte**

  Ermöglicht das Exportieren von Details der aktuellen Ereignisansicht in eine kommagetrennte Datei (.csv) oder ein PDF-Dokument.

- **Spaltenauswahl Ein-/Ausblenden**

  Hier können Sie die Spalten auswählen, die auf der Seite angezeigt werden, und die Reihenfolge auswählen, in der sie angezeigt werden.

Ereignisliste

Zeigt Details zu allen Ereignissen an, die nach ausgelöster Zeit geordnet sind.

Standardmäßig wird die Ansicht Alle aktiven Ereignisse angezeigt, um die neuen und bestätigten Ereignisse für die letzten sieben Tage mit einem Level der Auswirkung von Vorfall oder Risiko anzuzeigen.

- **Auslösezeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Severity**

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

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Impact Level**

  Die Auswirkungen auf das Ereignis: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Ereigniswirkungsbereich: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration, Oder Sicherheit.

- **Name**

  Der Ereignisname. Sie können den Namen auswählen, um die Seite Ereignisdetails für dieses Ereignis anzuzeigen.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis aufgetreten ist. Sie können den Namen auswählen, um die Seite mit den Angaben zu Systemzustand und Performance für das Objekt anzuzeigen.

  Wenn eine Richtlinienverletzung bei Shared QoS auftritt, 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 Ereignisdetails angezeigt.

- **Quelltyp**

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

- * Zugewiesen Zu*

  Der Name des Benutzers, dem das Ereignis zugeordnet ist.

- **Event Ursprung**

  Ob das Ereignis aus dem "Active IQ Portal" oder direkt aus "Active IQ Unified Manager" stammt.

- **Anmerkungsname**

Der Name der Anmerkung, die dem Speicherobjekt zugewiesen ist.

- **Hinweise**

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

- **Tage Herausragend**

  Die Anzahl der Tage seit der ersten Erzeugung des Ereignisses.

- **Zugewiesene Zeit**

  Die Zeit, die seit der Zuweisung des Ereignisses an einen Benutzer verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis einem Benutzer zugewiesen wurde.

- * Bestätigt Durch*

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

- * Quittierte Zeit*

  Die Zeit, die seit dem Ereignis vergangen ist, wurde bestätigt. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis bestätigt wurde.

- * Gelöst Von*

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

- * Zeit Gelöst*

  Die Zeit, die seit der Behebung des Ereignisses abgelaufen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis aufgelöst wurde.

- **Veraltete Zeit**

  Die Zeit, in der der Zustand des Ereignisses obsolet wurde.

Seite mit den Veranstaltungsdetails

Auf der Seite Ereignisdetails können Sie die Details eines ausgewählten Ereignisses anzeigen, z. B. den Schweregrad des Ereignisses, den Aufprallwert, den Aufprallbereich und die Ereignisquelle. Weitere Informationen zu möglichen Korrekturmaßnahmen können Sie zur Behebung des Problems einsehen.

- **Name Des Events**

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

  Bei Ereignissen ohne Leistungseinfall, während sich das Ereignis im Status „Neu“ oder „bestätigt“ befindet, sind die zuletzt erkannten Informationen nicht bekannt und daher verborgen.

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung der Veranstaltung.

  In manchen Fällen wird in der Ereignisbeschreibung ein Grund für das ausgelöste Ereignis angegeben.

- **Komponente in Konflikt**

  Für dynamische Performance-Ereignisse werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente einen Konflikt hat, ist ihr Symbol eingekreist und rot markiert.

  Eine Beschreibung der hier angezeigten Komponenten finden Sie unter *Cluster-Komponenten und darüber, warum sie sich in Konflikt befinden können*.

Die Abschnitte Ereignisinformationen, Systemdiagnose und vorgeschlagene Maßnahmen werden in anderen Themen beschrieben.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizen-Symbol**

  Ermöglicht Ihnen das Hinzufügen oder Aktualisieren von Notizen zum Ereignis und die Überprüfung aller von anderen Benutzern verbleibenden Notizen.

Aktionen Menü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

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

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der das Ereignis zugewiesen wurde, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

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

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse, damit Sie keine Wiederholungsbenachrichtigungen erhalten.

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

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

Wenn Sie ein Ereignis auflösen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis aufgelöst haben, in der Ereignisliste (aufgelöst von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Alarm Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Das wird im Abschnitt „Ereignisinformationen“ angezeigt

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

Felder, die nicht auf den Ereignistyp anwendbar sind, werden ausgeblendet. Sie können folgende Veranstaltungsdetails anzeigen:

- **Ereignis Trigger Zeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Veraltete Ursache**

  Die Aktionen, durch die das Ereignis veraltet war, z. B. wurde das Problem behoben.

- **Veranstaltungsdauer**

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

  Dieses Feld wird für alle Performanceereignisse und für andere Ereignistypen angezeigt, nachdem sie aufgelöst oder veraltet sind.

- **Zuletzt Gesehen**

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

  Bei Performanceereignissen kann dieser Wert höher sein als die Ereignis-Trigger-Zeit, da dieses Feld nach jeder neuen Sammlung von Performancedaten aktualisiert wird, solange das Ereignis aktiv ist. Bei anderen Arten von Ereignissen, wenn sich der Status Neu oder bestätigt befindet, wird dieser Inhalt nicht aktualisiert und das Feld wird daher ausgeblendet.

- **Severity**

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

- **Impact Level**

  Die Auswirkungen auf das Ereignis: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Ereigniswirkungsbereich: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration, Oder Sicherheit.

- **Quelle**

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

  Wenn sich die Details zu einem Ereignis für eine Shared QoS-Richtlinie anzeigen lassen, werden in diesem Feld bis zu drei Workload-Objekte aufgeführt, die die meisten IOPS oder MB/s verbrauchen.

  Sie können auf den Link des Quellnamens klicken, um die Seite mit den Angaben zu Systemzustand oder Performance für das Objekt anzuzeigen.

- **Quellanmerkungen**

  Zeigt den Anmerkungsnamen und -Wert für das Objekt an, dem das Ereignis zugeordnet ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, deren Mitglied das betroffene Objekt ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quelltyp**

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

- * Auf Cluster*

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

  Sie können auf den Cluster-Link klicken, um die Seite mit den Angaben zu Systemzustand und Performance für das Cluster anzuzeigen.

- **Betroffene Objekte Zählen**

  Die Anzahl der vom Ereignis betroffenen Objekte.

  Sie können auf den Objektlink klicken, um die Bestandsseite anzuzeigen, die mit den Objekten ausgefüllt wird, die aktuell von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Betroffene Volumen*

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

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

- * Ausgelöste Richtlinie*

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgegeben hat.

Sie können den Mauszeiger über den Richtliniennamen bewegen, um Details zur Schwellenwertrichtlinie anzuzeigen. Für anpassungsfähige QoS-Richtlinien werden die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener Speicherplatz oder genutzter Speicherplatz) angezeigt.

Dieses Feld wird nur für Performanceereignisse angezeigt.

- **Regel-Id**

  Bei Active IQ-Plattformereignissen ist dies die Anzahl der Regel, die zur Generierung des Ereignisses ausgelöst wurde.

- * Bestätigt durch*

  Der Name der Person, die das Ereignis bestätigt hat und die Zeit, zu der das Ereignis bestätigt wurde.

- * Gelöst von*

  Der Name der Person, die das Ereignis gelöst hat, und die Zeit, zu der das Ereignis gelöst wurde.

- * Zugewiesen zu*

  Der Name der Person, die der Arbeit an dem Ereignis zugeordnet ist.

- **Warnmeldungseinstellungen**

  Die folgenden Informationen über Meldungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnmeldungen zugeordnet sind, wird ein Link **Alarm hinzufügen** angezeigt.

    Sie können das Dialogfeld Alarm hinzufügen öffnen, indem Sie auf den Link klicken.

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

    Sie können das Dialogfeld Alarm bearbeiten öffnen, indem Sie auf den Link klicken.

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

    Sie können die Seite „Alarmkonfiguration“ öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Warnmeldungen anzuzeigen.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung Gesendet**

  Das Datum und die Uhrzeit, zu der die letzte Benachrichtigung gesendet wurde.

- **Senden nach**

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

- **Vorheriger Skriptlauf**

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

Der Abschnitt „Empfohlene Maßnahmen“ wird angezeigt

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite „Veranstaltungsdetails“ enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu lösen. Die vorgeschlagenen Maßnahmen werden auf Grundlage der Art des Ereignisses oder des Schwellenwerts, die nicht eingehalten wurden, angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen gibt es **Hilfe** Links auf der Seite, die zusätzliche Informationen für viele empfohlene Aktionen, einschließlich Anweisungen für die Durchführung einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools umfassen.

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

Wenn Sie das Objekt und das Ereignis genauer analysieren möchten, klicken Sie auf die Schaltfläche **Workload analysieren**, um die Seite Workload Analysis anzuzeigen.

Es gibt bestimmte Ereignisse, die Unified Manager sorgfältig diagnostizieren und eine einzige Lösung anbieten kann. Wenn verfügbar, werden diese Auflösungen mit der Schaltfläche **Fix IT** angezeigt. Klicken Sie auf diese Schaltfläche, damit Unified Manager das Problem, das das Ereignis verursacht, behebt.

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

Anzeigen des Abschnitts Systemdiagnose

Im Abschnitt Systemdiagnose der Seite Ereignisdetails finden Sie Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur für bestimmte Ereignisse angezeigt.

Einige Performanceereignisse bieten Diagramme, die für das Ereignis relevant sind, das ausgelöst wurde. Dies beinhaltet in der Regel ein IOPS- oder MB/s-Diagramm und ein Latenzdiagramm für die vorherigen zehn Tage. Nach Absprache sehen Sie, welche Storage-Komponenten die Latenz am meisten beeinträchtigen oder von der Latenz beeinträchtigt werden, wenn das Ereignis aktiv ist.

Für dynamische Performance-Ereignisse werden die folgenden Diagramme angezeigt:

- Workload-Latenz: Zeigt den Verlauf der Latenz für die Top-Opfer, -Bully oder -Hai-Workloads bei den zu versagenden Komponenten an.
- Workload-Aktivität: Zeigt Details zur Workload-Nutzung der Cluster-Komponente an, die durch Konflikte verursacht wird.
- Resource Activity: Zeigt historische Performance-Statistiken für eine Clusterkomponente an, die mit einem Konflikt in der Cluster-Komponente Konflikt ist.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten mit einem Konflikt zu belegen sind.

Andere Ereignisse liefern eine kurze Beschreibung der Analysetyp, die das System auf dem Storage-Objekt durchführt. In manchen Fällen gibt es eine oder mehrere Zeilen; eine für jede analysierte Komponente, für systemdefinierte Performance-Richtlinien, die mehrere Performance-Zähler analysieren. In diesem Szenario wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob ein Problem in dieser speziellen Diagnose gefunden wurde oder nicht.

Seite „Ereignis-Einrichtung“

Auf der Seite Event Setup werden die Liste der deaktivierten Ereignisse angezeigt und Informationen wie den zugehörigen Objekttyp und den Schweregrad des Ereignisses bereitgestellt. Sie können auch Aufgaben wie Deaktivieren oder Aktivieren von Ereignissen global ausführen.

Sie können diese Seite nur aufrufen, wenn Sie die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ besitzen.

Befehlsschaltflächen

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

- **Deaktivieren**

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

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **Regeln Hochladen**

  Startet das Dialogfeld „Regeln hochladen“, in dem Sites ohne externen Netzwerkzugriff die Datei „Active IQ-Regeln“ manuell auf Unified Manager hochladen können. Die Regeln werden auf Cluster AutoSupport Meldungen ausgeführt, um Ereignisse für die Systemkonfiguration, Verkabelung, Best Practice und Verfügbarkeit zu generieren, die von der Active IQ Plattform definiert wurden.

- **EMS Events abonnieren**

  Öffnet das Dialogfeld „EMS-Ereignisse abonnieren“, in dem Sie spezielle EMS-Ereignisse (Event Management System) aus den von Ihnen überwachten Clustern abonnieren können. Das EMS sammelt Informationen über Ereignisse, die auf dem Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis erhalten wird, wird ein Unified Manager-Ereignis mit dem entsprechenden Schweregrad generiert.

Listenansicht

In der Listenansicht werden Informationen zu deaktivierten Ereignissen (im Tabellenformat) angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Veranstaltung**

  Zeigt den Namen des Ereignisses an, das deaktiviert ist.

- **Severity**

  Zeigt den Schweregrad des Ereignisses an. Der Schweregrad kann kritisch, Fehler, Warnung oder Informationen sein.

- **Quelltyp**

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

Dialogfeld „Ereignisse deaktivieren“

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

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

Bereich Ereigniseigenschaften

Im Bereich Ereigniseigenschaften werden die folgenden Ereigniseigenschaften angegeben:

- **Ereignis Severity**

  Ermöglicht die Auswahl von Ereignissen auf der Grundlage des Schweregrads, der kritisch sein kann, Fehler, Warnung oder Informationen.

- **Ereignisname Enthält**

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

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem Schweregrad des Ereignisses und dem angegebenen Textstring entsprechen.

- **Ereignisse deaktivieren**

  Zeigt die Liste der Ereignisse an, die Sie zur Deaktivierung ausgewählt haben.

  Der Schweregrad des Ereignisses wird auch zusammen mit dem Event-Namen angezeigt.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für die ausgewählten Ereignisse ausführen:

- * Speichern und schließen*

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Abbrechen**

Die Änderungen werden diskCards und das Dialogfeld geschlossen.

Copyright-Informationen

Copyright © 2025 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.