Beschreibung der Ereignisfenster und Dialogfelder

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

This PDF was generated from https://docs.netapp.com/de-de/oncommand-unified-manager-95/online-help/reference-event-retention-settings-dialog-box.html on October 23, 2024. Always check docs.netapp.com for the latest.

Inhalt

Beschreibung der Ereignisfenster und Dialogfelder 1
Dialogfeld „Einstellungen für die Ereignisaufbewahrung“ 1
Setup-/Benachrichtigungsseite 2
Seite „Ereignisinventar“ 4
Seite mit den Veranstaltungsdetails 7
Seite „Ereignisse konfigurieren/managen“ 13
Dialogfeld „Ereignisse deaktivieren“ 14

Beschreibung der Ereignisfenster und Dialogfelder

Ereignisse informieren Sie über Probleme in Ihrer Umgebung. Sie können die Seite „Ereignisinventar“ und die Seite „Ereignisdetails“ verwenden, um alle Ereignisse zu überwachen. Über das Dialogfeld „Benachrichtigungseinstellungen“ können Sie Benachrichtigungen konfigurieren. Über die Seite „Ereignisse konfigurieren/managen“ können Ereignisse deaktiviert oder aktiviert werden.

Dialogfeld „Einstellungen für die Ereignisaufbewahrung“

Sie können die Ereigniseinstellungen so konfigurieren, dass Ereignisse (Informationen, aufgelöst oder veraltet) nach einer bestimmten Zeit und zu einer bestimmten Frequenz automatisch gelöscht werden. Sie können diese Ereignisse auch manuell löschen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereigniseinstellungen

Sie können die folgenden Optionen konfigurieren:

- **Löschen von Informationen, gelösten und veralteten Ereignissen, die älter sind als**

  Hiermit können Sie den Aufbewahrungszeitraum festlegen, nach dem Ereignisse, die als Information, Lösung oder veraltet markiert sind, vom Verwaltungsserver entfernt werden.

  Der Standardwert ist 180 Tage. Die Aufbewahrung der Ereignisse über mehr als 180 Tage wirkt sich auf die Leistung aus und wird nicht empfohlen. Die untere Grenze für die Ereignisaufbewahrungsdauer beträgt 7 Tage, obwohl es keine Obergrenze gibt.

- **Zeitplan Löschen**

  Hiermit können Sie festlegen, wie oft alle Ereignisse, die als Information, Lösung oder veraltet markiert sind und deren Altersgrenze überschritten wurde, automatisch vom Verwaltungsserver gelöscht werden. Die möglichen Werte sind „Daily“, „Weekly“ oder „Monthly“.

  Der Standardwert ist Daily.

- **Jetzt Löschen**

  Ermöglicht Ihnen das manuelle Löschen aller Informationen, gelösten und veralteten Ereignisse, die den angegebenen Aufbewahrungszeitraum überschritten haben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die Setup-Optionen speichern oder abbrechen:

- **Speichern und Schließen**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option und schließt das Dialogfeld.

- **Abbrechen**

  Bricht die letzten Änderungen ab und schließt das Dialogfeld.

Setup-/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 „OnCommand Administrator“ 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 „`OnCommand@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.

- **Verwenden Sie STARTTLS**

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.

- * 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.

Seite „Ereignisinventar“

Auf der Seite „Ereignisinventar“ können Sie eine Liste der aktuellen Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie Quittieren, Auflösen und Zuweisen von Ereignissen durchführen. Sie können auch eine Warnung zu bestimmten Ereignissen hinzufügen.

Standardmäßig werden die Informationen auf dieser Seite alle 5 Minuten automatisch 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.
- Zeitauswahl zur Verfeinerung der Ereignisliste um den Zeitpunkt, an dem das Ereignis ausgelöst wurde.

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.

- **Export**

  Ermöglicht das Exportieren von Details aller Ereignisse in kommagetrennte Werte (`.csv`) Datei.

- **Spaltenauswahl**

  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 werden neue und bestätigte Ereignisse für die letzten sieben Tage des Schweregrads kritisch, Fehler und Warnung angezeigt.

- **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 Ereigniseinwirkung: Vorfall, Risiko oder Ereignis.

- **Aufprallbereich**

  Die Auswirkung auf das Ereignis: Verfügbarkeit, Kapazität, Performance, Schutz oder Konfiguration.

- **Name**

  Der Ereignisname.

  Sie können den Ereignisnamen auswählen, um die Seite Ereignisdetails anzuzeigen.

- **Quelle**

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

  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.

  Sie können den Quellnamen auswählen, um die Seite für den Systemzustand oder die Performance-Details für das Objekt anzuzeigen.

- **Quelltyp**

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

- * Zugewiesen Zu*

  Der Name des Benutzers, dem das Ereignis zugeordnet 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.

  Die folgenden Komponenten können angezeigt werden:

  - **Netzwerk**

    Zeigt die Wartezeit von I/O-Anfragen durch iSCSI-Protokolle oder Fibre Channel-Protokollen (FC) des Clusters an. Die Wartezeit liegt darin, auf die Transaktionen „iSCSI Ready to Transfer“ (R2T) oder „FCP Transfer Ready“ (XFER_RDY) zu warten, bis der Cluster auf eine I/O-Anforderung antworten kann. Wenn die Netzwerkkomponente unter einem Konflikt steht, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene des Blocks die Latenz eines oder mehrerer Workloads

beeinflussen.

- * Netzwerkverarbeitung*

  Repräsentiert die Softwarekomponente in dem Cluster, die mit I/O-Verarbeitung zwischen Protokollebene und Cluster beteiligt ist Der Knoten, der die Netzwerkverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses möglicherweise geändert. Wenn die Netzwerkverarbeitungskomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **QoS-Richtlinie**

  Steht für die Storage-Richtliniengruppe für Quality of Service (QoS), der Mitglied des Workloads ist Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * Cluster Interconnect*

  Stellt die Kabel und Adapter dar, mit denen die physischen Nodes des Clustern verbunden sind. Wenn die Cluster-Interconnect-Komponente einen Konflikt verursacht, bedeutet dies hohe Wartezeiten bei I/O-Anfragen am Cluster Interconnect, die sich auf die Latenz eines oder mehrerer Workloads auswirken.

- **Datenverarbeitung**

  Zeigt die Softwarekomponente in dem Cluster an, die mit I/O-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat, das den Workload enthält. Der Node, der die Datenverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses geändert. Wenn die Datenverarbeitungkomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung am Datenverarbeitungs-Node die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **MetroCluster Ressourcen**

  Repräsentiert die MetroCluster-Ressourcen, einschließlich NVRAM und Interswitch Links (ISLs), die zur Spiegelung von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn die MetroCluster Komponente Konflikte verursacht, bedeutet dies einen hohen Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Systemzustandsproblem Auswirkungen auf die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster. Wenn das Cluster nicht in einer MetroCluster-Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate oder SSD Aggregate Ops**

  Repräsentiert das Storage-Aggregat, auf dem die Workloads ausgeführt werden Wenn die Aggregat-Komponente Konflikte verursacht, bedeutet dies, dass eine hohe Auslastung des Aggregats sich auf die Latenz eines oder mehrerer Workloads auswirkt. Ein Aggregat besteht aus rein HDDs oder einer Kombination aus HDDs und SSDs (einem Flash Pool Aggregat). Ein „`SSD Aggregat`“ besteht aus allen SSDs (ein All-Flash-Aggregat) oder einer Kombination aus SSDs und einer Cloud Tier (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente in dem Cluster dar, die mit I/O-Verarbeitung zwischen dem Cluster und dem Cloud-Tier beschäftigt ist, auf dem Benutzerdaten gespeichert werden Wenn die Komponente für

die Cloud-Latenz aufgrund von Konflikten vorliegen, bedeutet dies, dass sich ein großer Anteil der in der Cloud-Ebene gehosteten Lesevorgänge auf die Latenz eines oder mehrerer Workloads auswirkt.

- **Sync SnapMirror**

  Repräsentiert die Software-Komponente in dem Cluster, die mit der Replizierung von Benutzerdaten vom primären Volume auf das sekundäre Volume in einer SnapMirror Synchronous-Beziehung beteiligt ist Wenn die synchrone SnapMirror Komponente Konflikte verursacht, bedeutet dies, dass die Aktivitäten des synchronen Betriebs von SnapMirror sich auf die Latenz eines oder mehrerer Workloads auswirken.

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 Ereigniseinwirkung: Vorfall, Risiko oder Ereignis.

- **Aufprallbereich**

Die Auswirkung auf das Ereignis: Verfügbarkeit, Kapazität, Performance, Schutz oder Konfiguration.

- **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.

- * 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 Konfiguration/Warnmeldungen 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.

- **Gesendet Über**

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

- **Vorherige Skriptausführung**

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

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.

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, OnCommand System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools umfassen.

In diesem Hilfethema werden auch einige Links angezeigt.

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.

Seite „Ereignisse konfigurieren/managen“

Auf der Seite „Ereignisse konfigurieren/managen“ wird die Liste der deaktivierten Ereignisse angezeigt, und es werden Informationen wie der zugehörige Objekttyp und der Schweregrad des Ereignisses angezeigt. Sie können auch Aufgaben wie Deaktivieren oder Aktivieren von Ereignissen global ausführen.

Sie können diese Seite nur aufrufen, wenn Sie die Rolle „OnCommand-Administrator“ oder „Storage-Administrator“ 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.

- **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.

- **Einstellungen Für Die Ereignisaufbewahrung**

  Öffnet das Dialogfeld „Ereignisaufbewahrungseinstellungen“, in dem Sie den Aufbewahrungszeitraum festlegen können, nach dem die Informationen, aufgelösten und veralteten Ereignisse vom Verwaltungsserver entfernt werden. Der Standardwert für die Aufbewahrung ist 180 Tage.

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 „OnCommand Administrator“ 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 © 2024 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.