Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte

Active IQ Unified Manager

NetApp
November 13, 2026

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

Inhalt

Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte . . . 1
- Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten in Active IQ Unified Manager . . . 1
- Betroffene Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager identifizieren . . . 1
- Identifizierung überlastender Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager . . . 1
- Shark-Workloads in einem dynamischen Performance-Ereignis in Active IQ Unified Manager identifizieren . . . 2
- Performance Ereignisanalyse für eine MetroCluster Konfiguration . . . 2
  - Analyse von MetroCluster Leistungsereignissen mit Active IQ Unified Manager . . . 3
  - Analyse eines MetroCluster Leistungsereignisses auf einem Cluster in Active IQ Unified Manager . . . 3
  - Analyse eines MetroCluster Leistungsereignisses auf einem Remote Cluster in Active IQ Unified Manager . . . 4
- Reaktion auf ein dynamisches QoS-Drosselungsereignis in Active IQ Unified Manager . . . 5
- Reaktion auf ein Leistungsereignis, das durch einen Festplattenausfall in Active IQ Unified Manager verursacht wird . . . 7
- Reaktion auf ein Leistungsereignis, das durch eine HA Übernahme in Active IQ Unified Manager verursacht wurde . . . 8

Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten in Active IQ Unified Manager

Ereignisse, die durch dynamische Schwellenwerte generiert werden, weisen darauf hin, dass die tatsächliche Antwortzeit (Latenz) einer Arbeitslast im Vergleich zum erwarteten Antwortzeitbereich zu hoch oder zu niedrig ist. Sie verwenden die Seite „Ereignisdetails“, um das Performance-Ereignis zu analysieren und bei Bedarf eine Korrekturmaßnahme zu ergreifen, damit die Performance wieder den Normalzustand erreicht.

Dynamische Performance-Schwellenwerte sind auf Cloud Volumes ONTAP, ONTAP Edge oder ONTAP Select Systemen nicht aktiviert.

Betroffene Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager identifizieren

Im Unified Manager können Sie ermitteln, welche Volume-Workloads die größte Abweichung bei der Antwortzeit (Latenz) aufweisen, die durch eine Storage-Komponente in Contention verursacht wird. Die Identifizierung dieser Workloads hilft Ihnen zu verstehen, warum die darauf zugreifenden Clientanwendungen langsamer als üblich arbeiten.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es müssen neue, bestätigte oder veraltete dynamische Performance-Ereignisse vorliegen.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads an, sortiert nach der größten Abweichung bei Aktivität oder Nutzung auf der Komponente oder danach, wie stark sie vom Ereignis betroffen sind. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ erfolgt die Auswahl der Option **Victim Workloads**.
3. Wenn Sie den Mauszeiger über die Diagramme bewegen, sehen Sie die wichtigsten benutzerdefinierten Workloads, die sich auf die Komponente auswirken, sowie den Namen des betroffenen Workloads.

Identifizierung überlastender Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager

Im Unified Manager können Sie ermitteln, welche Workloads für eine Clusterkomponente

mit Ressourcenkonflikt die größte Nutzungsabweichung aufweisen. Die Identifizierung dieser Workloads hilft Ihnen zu verstehen, warum bestimmte Volumes im Cluster langsame Antwortzeiten (Latenz) aufweisen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es müssen neue, bestätigte oder veraltete dynamische Performance-Ereignisse vorliegen.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads, sortiert nach der höchsten Auslastung der Komponente oder der größten Beeinträchtigung durch das Ereignis. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Auf der Seite „Ereignisdetails“ können Informationen über das Ereignis angezeigt werden.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ erfolgt die Auswahl von **Bully Workloads**.
3. Wenn Sie den Mauszeiger über die Diagramme bewegen, werden die wichtigsten benutzerdefinierten Bully Workloads angezeigt, die sich auf die Komponente auswirken.

Shark-Workloads in einem dynamischen Performance-Ereignis in Active IQ Unified Manager identifizieren

Im Unified Manager können Sie die Workloads identifizieren, die bei einer Storage Komponente mit Ressourcenkonflikt die größte Nutzungsabweichung aufweisen. Die Identifizierung dieser Workloads hilft Ihnen bei der Entscheidung, ob diese Workloads in einen weniger ausgelasteten Cluster verschoben werden sollten.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es gibt neue, bestätigte oder veraltete dynamische Performance-Ereignisse.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads, sortiert nach der höchsten Auslastung der Komponente oder der größten Beeinträchtigung durch das Ereignis. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ können Sie **Shark Workloads** auswählen.
3. Wenn Sie den Mauszeiger über die Diagramme bewegen, werden die wichtigsten benutzerdefinierten Workloads angezeigt, die sich auf die Komponente auswirken, sowie der Name des Shark Workloads.

Performance Ereignisanalyse für eine MetroCluster Konfiguration

Analyse von MetroCluster Leistungsereignissen mit Active IQ Unified Manager

Mit Unified Manager können Sie ein Performance-Ereignis für eine MetroCluster Konfiguration analysieren. Sie können die an dem Ereignis beteiligten Workloads identifizieren und die vorgeschlagenen Maßnahmen zur Behebung des Problems überprüfen.

MetroCluster Performance Ereignisse können auf *bully* Workloads zurückzuführen sein, die die Interswitch-Verbindungen (ISLs) zwischen den Clustern übermäßig beanspruchen, oder auf Probleme mit dem Systemstatus der Verbindungen. Unified Manager überwacht jeden Cluster in einer MetroCluster Konfiguration unabhängig, ohne Performance Ereignisse auf einem Partnercluster zu berücksichtigen.

Performance Ereignisse beider Cluster in der MetroCluster Konfiguration werden ebenfalls auf der Unified Manager Dashboard Seite angezeigt. Außerdem können die Systemstatus-Seiten von Unified Manager angezeigt werden, um den Systemstatus der einzelnen Cluster zu überprüfen und deren Beziehung anzuzeigen.

Analyse eines MetroCluster Leistungsereignisses auf einem Cluster in Active IQ Unified Manager

Mit Unified Manager lässt sich der Cluster in einer MetroCluster Konfiguration analysieren, auf dem ein Performance Ereignis erkannt wurde. Dabei lassen sich der Cluster-Name, der Zeitpunkt der Ereigniserkennung sowie die beteiligten *bully* und *victim* Workloads identifizieren.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Für eine MetroCluster Konfiguration müssen neue, bestätigte oder veraltete Performance Ereignisse vorliegen.
- Beide Cluster in der MetroCluster Konfiguration müssen von derselben Instanz des Unified Manager überwacht werden.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die Ereignisbeschreibung enthält die Namen der beteiligten Workloads und deren Anzahl.

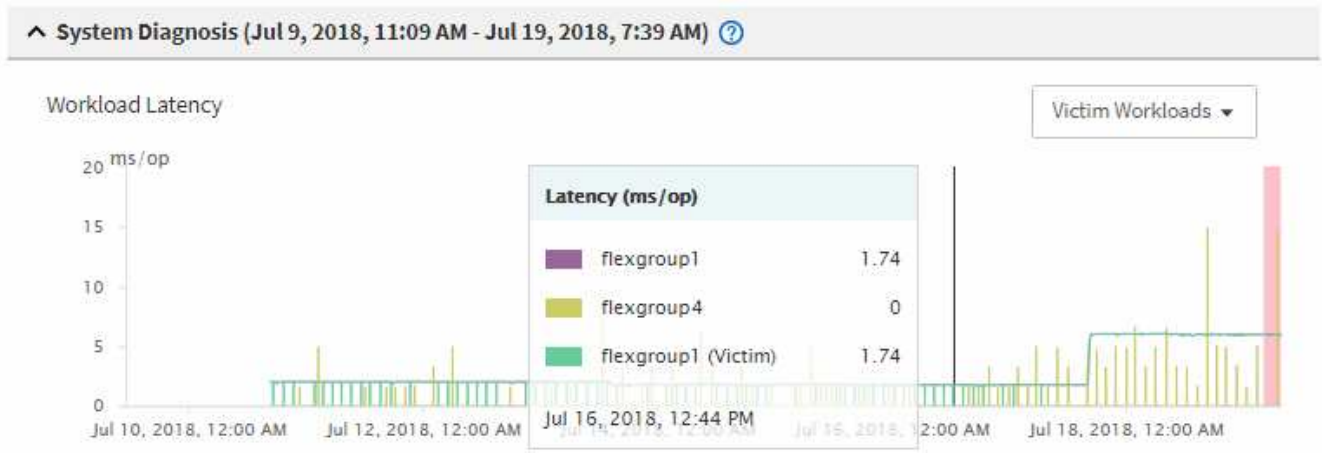
   In diesem Beispiel ist das Symbol MetroCluster Resources rot, was darauf hinweist, dass die MetroCluster Ressourcen umkämpft sind. Wenn sich der Mauszeiger über dem Symbol befindet, wird eine Beschreibung des Symbols angezeigt.



3. Der Clustername und der Zeitpunkt der Ereigniserkennung können zur Analyse von Performance Ereignissen auf dem Partnercluster verwendet werden.

4. In den Diagrammen ist zu prüfen, ob die Antwortzeiten der *victim*-Workloads über dem Performance-Schwellenwert liegen.

   In diesem Beispiel wird die betroffene Arbeitslast im Hover-Text angezeigt. Die Latenzdiagramme zeigen auf hoher Ebene ein konsistentes Latenzmuster für die betroffenen Arbeitslasten. Obwohl die anormale Latenz der betroffenen Arbeitslasten das Ereignis ausgelöst hat, könnte ein konsistentes Latenzmuster darauf hindeuten, dass die Arbeitslasten innerhalb ihres erwarteten Bereichs arbeiten, ein I/O-Spitzenwert jedoch die Latenz erhöht und das Ereignis ausgelöst hat.



   Wenn Sie kürzlich eine Applikation auf einem Client installiert haben, die auf diese Volume Workloads zugreift und diese Applikation eine hohe Anzahl von E/A-Operationen an sie sendet, ist möglicherweise mit einem Anstieg ihrer Latenzzeiten zu rechnen. Wenn die Latenz für die Workloads wieder in den erwarteten Bereich zurückkehrt, der Ereignisstatus in „veraltet“ wechselt und länger als 30 Minuten in diesem Status verbleibt, kann das Ereignis wahrscheinlich ignoriert werden. Wenn das Ereignis weiterhin besteht und im neuen Status verbleibt, kann es weiter untersucht werden, um festzustellen, ob andere Probleme das Ereignis verursacht haben.

5. Im Diagramm „Workload Throughput“ wird mit der Auswahl der Option **Bully Workloads** die Anzeige der Bully Workloads aktiviert.

   Das Vorhandensein von besonders ressourcenintensiven Workloads deutet darauf hin, dass das Ereignis möglicherweise durch einen oder mehrere Workloads im lokalen Cluster verursacht wurde, die die MetroCluster Ressourcen übermäßig beanspruchten. Diese Workloads weisen eine hohe Abweichung im Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm zeigt auf hoher Ebene das Schreibdurchsatzmuster (MB/s) für die Workloads. Anhand des Schreibdurchsatzmusters in MB/s lassen sich ungewöhnliche Durchsatzraten erkennen, die darauf hindeuten können, dass ein Workload die MetroCluster Ressourcen übermäßig nutzt.

   Wenn keine rechenintensiven Workloads an dem Ereignis beteiligt sind, könnte die Ursache ein Systemstatusproblem mit der Verbindung zwischen den Clustern oder ein Performance Problem auf dem Partnercluster sein. Mit Unified Manager kann der Systemstatus beider Cluster in einer MetroCluster Konfiguration überprüft werden. Außerdem kann Unified Manager verwendet werden, um Performance Ereignisse auf dem Partnercluster zu prüfen und zu analysieren.

Analyse eines MetroCluster Leistungsereignisses auf einem Remote Cluster in Active IQ Unified Manager

Mit Unified Manager können Sie dynamische Performance-Ereignisse auf einem Remote-Cluster in einer MetroCluster Konfiguration analysieren. Die Analyse hilft Ihnen

festzustellen, ob ein Ereignis auf dem Remote-Cluster ein Ereignis auf dem Partner-Cluster verursacht hat.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen ein Performance-Ereignis auf einem lokalen Cluster in einer MetroCluster Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Systemstatus des lokalen Clusters und des Partner-Clusters, das an dem Performance-Ereignis beteiligt ist, überprüft sowie den Namen des Partner-Clusters ermittelt haben.

Schritte

1. Bei der Unified Manager Instanz, die den Partnercluster überwacht, ist eine Anmeldung erforderlich.
2. Im linken Navigationsbereich lässt sich durch Klicken auf **Ereignisse** die Ereignisliste anzeigen.
3. Im Selektor **Time Range** erfolgt die Auswahl von **Last Hour**; anschließend folgt ein Klick auf **Apply Range**.
4. Im Selektor **Filter** wird im linken Dropdown-Menü **Cluster** ausgewählt, der Name des Partnerclusters in das Textfeld eingegeben und anschließend auf **Filter anwenden** geklickt.

   Wenn für den ausgewählten Cluster in der letzten Stunde keine Ereignisse verzeichnet wurden, bedeutet dies, dass der Cluster in dem Zeitraum, in dem das Ereignis auf seinem Partner erkannt wurde, keine Performance-Probleme hatte.

5. Wenn im ausgewählten Cluster in der letzten Stunde Ereignisse erkannt wurden, ist die Ereigniserkennungszeit mit der Ereigniserkennungszeit des Ereignisses im lokalen Cluster zu vergleichen.

   Wenn diese Ereignisse ressourcenintensive Workloads betreffen, die zu Ressourcenkonflikten auf der Datenverarbeitungskomponente führen, könnten einer oder mehrere dieser Workloads das Ereignis im lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Maßnahmen zu seiner Behebung auf der Seite mit den Ereignisdetails einzusehen.

   Falls diese Ereignisse keine Bully-Workloads betreffen, haben sie das Performance-Ereignis auf dem lokalen Cluster nicht verursacht.

Reaktion auf ein dynamisches QoS-Drosselungsereignis in Active IQ Unified Manager

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch eine QoS-Richtliniengruppe verursacht wurde, die den Workload-Durchsatz (MB/s) drosselt. Die Drosselung erhöhte die Antwortzeiten (Latenz) von Volume Workloads in der Richtliniengruppe. Anhand der Ereignisinformationen können Sie feststellen, ob neue Grenzwerte für die Richtliniengruppen erforderlich sind, um die Drosselung zu stoppen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.

2. Unter **Beschreibung** werden die Namen der von der Drosselung betroffenen Workloads angezeigt.

   Die Beschreibung kann für Opfer und Verursacher dieselbe Workload anzeigen, da die Drosselung die Workload zu ihrem eigenen Opfer macht.

3. Der Name des Volume wird mithilfe einer Applikation wie beispielsweise einem Texteditor notiert.

   Sie können anhand des Volume-Namens suchen, um ihn später wiederzufinden.

4. In den Diagrammen „Workload-Latenz“ und „Workload-Auslastung“ wird **Bully Workloads** ausgewählt.
5. Beim Bewegen des Mauszeigers über die Diagramme werden die wichtigsten benutzerdefinierten Workloads angezeigt, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast an oberster Stelle der Liste weist die größte Abweichung auf und hat die Drosselung verursacht. Die Aktivität gibt den prozentualen Anteil des von jeder Arbeitslast genutzten Limits der Richtliniengruppe an.

6. Im Bereich **Suggested Actions** lässt sich für die oberste Workload die Schaltfläche **Analyze Workload** auswählen.
7. Auf der Seite „Workload Analysis“ ist das Latenzdiagramm auf die Ansicht aller Cluster Components und das Durchsatzdiagramm auf Breakdown eingestellt.

   Die Aufschlüsselungsdiagramme werden unterhalb des Latenzdiagramms und des IOPS-Diagramms angezeigt.

8. Im **Latenz**-Diagramm lässt sich anhand der QoS-Grenzwerte erkennen, in welchem Ausmaß die Drosselung die Latenz zum Zeitpunkt des Ereignisses beeinflusst hat.

   Die QoS Richtliniengruppe hat einen maximalen Durchsatz von 1.000 Operationen pro Sekunde (op/sec), den die darin enthaltenen Workloads gemeinsam nicht überschreiten können. Zum Zeitpunkt des Ereignisses hatten die Workloads in der Richtliniengruppe einen kombinierten Durchsatz von über 1.200 op/sec, wodurch die Richtliniengruppe ihre Aktivität auf 1.000 op/sec drosselte.

9. Zum Vergleich dienen die Werte für die **Lese-/Schreiblatenz** und die Werte für **Lese-/Schreib-/Sonstiges**.

   Beide Diagramme zeigen eine hohe Anzahl von Leseanfragen mit hoher Latenz, während die Anzahl der Anfragen und die Latenz bei Schreibanfragen gering sind. Anhand dieser Werte lässt sich feststellen, ob ein hoher Durchsatz oder eine hohe Anzahl von Operationen die Latenz erhöht hat. Diese Werte können bei der Entscheidung verwendet werden, eine Richtliniengruppenbegrenzung für den Durchsatz oder die Operationen festzulegen.

10. Mit ONTAP System Manager kann das aktuelle Limit der Richtliniengruppe auf 1.300 Operationen/Sek. erhöht werden.
11. Nach einem Tag können Sie zu Unified Manager zurückkehren und auf der Seite **Workload Analysis** die in Schritt 3 erfasste Workload eingeben.
12. Auswahl des Diagramms „Durchsatzaufschlüsselung“.

    Das Diagramm „Lesen/Schreiben/Sonstiges“ wird angezeigt.

13. Oben auf der Seite wird der Mauszeiger auf das Symbol für das Änderungsereignis ( ) für die Änderung der Richtliniengruppenbegrenzung bewegt.
14. Vergleich zwischen dem Diagramm **Lesen/Schreiben/Sonstiges** und dem Diagramm **Latenz**.

Die Lese- und Schreibanfragen sind gleich, aber die Drosselung hat aufgehört und die Latenz hat sich verringert.

Reaktion auf ein Leistungsereignis, das durch einen Festplattenausfall in Active IQ Unified Manager verursacht wird

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch Workloads verursacht wurde, die ein Aggregat übermäßig auslasten. Mit Unified Manager können Sie außerdem den Systemstatus des Aggregats prüfen, um festzustellen, ob kürzlich auf dem Aggregat erkannte Systemstatusereignisse zu dem Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die **Beschreibung** enthält die am Ereignis beteiligten Workloads und die betroffene Clusterkomponente.

   Es gibt mehrere betroffene Volumes, deren Latenz durch die Clusterkomponente mit Konfliktpotenzial beeinträchtigt wurde. Das Aggregat, das sich mitten in einer RAID Rekonstruktion befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die Clusterkomponente mit Konfliktpotenzial. Unter Component in Contention ist das Aggregatssymbol rot hervorgehoben, und der Name des Aggregats wird in Klammern angezeigt.

3. Im Diagramm zur Workload Auslastung erfolgt die Auswahl von **Bully Workloads**.
4. Wenn sich der Mauszeiger über dem Diagramm befindet, werden die wichtigsten Bully-Workloads angezeigt, die sich auf die Komponente auswirken.

   Die Workloads mit der höchsten Spitzenauslastung seit Erkennung des Ereignisses werden oben im Diagramm angezeigt. Einer der wichtigsten Workloads ist der systemdefinierte Workload Disk Health, der auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess zum Wiederaufbau des Aggregats mit der Ersatzfestplatte. Der Workload Disk Health hat zusammen mit anderen Workloads auf dem Aggregat wahrscheinlich die Auslastungskonkurrenz auf dem Aggregat und das zugehörige Ereignis verursacht.

5. Nachdem bestätigt wurde, dass die Aktivität der Arbeitslast „Disk Health“ das Ereignis verursacht hat, ist etwa 30 Minuten zu warten, bis die Rekonstruktion abgeschlossen ist und Unified Manager das Ereignis analysiert hat und erkennt, ob das Aggregat noch in Konflikt steht.
6. Aktualisierung der **Event details**.

   Nach Abschluss der RAID-Rekonstruktion sollte der State „obsolete“ sein; daran ist erkennbar, dass das Ereignis behoben ist.

7. Im Diagramm zur Workload Auslastung werden bei Auswahl von **Bully Workloads** die Workloads auf dem Aggregat nach Spitzenauslastung angezeigt.
8. Im Bereich **Suggested Actions** lässt sich für die oberste Workload die Schaltfläche **Analyze Workload**

auswählen.

9. Auf der Seite **Workload Analysis** ist der Zeitbereich auf die letzten 24 Stunden (1 Tag) festgelegt, sodass die Daten für das ausgewählte Volume angezeigt werden.

   In der Ereigniszeitleiste zeigt ein roter Punkt (🔴) an, wann der Festplattenausfall aufgetreten ist.

10. Im Diagramm „Knoten- und Aggregatauslastung“ bleibt nach dem Ausblenden der Linie für die Knotenstatistiken nur die Aggregatlinie sichtbar.
11. Hier erfolgt der Vergleich der Daten in diesem Diagramm mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latency**.

    Zum Zeitpunkt des Ereignisses wies die Aggregatauslastung eine hohe Lese- und Schreibaktivität auf, verursacht durch die RAID-Rekonstruktionsprozesse, was die Latenz des ausgewählten Volumes erhöhte. Wenige Stunden nach dem Auftreten des Ereignisses waren sowohl die Lese- und Schreibvorgänge als auch die Latenz gesunken, was bestätigt, dass beim Aggregat kein Ressourcenkonflikt mehr besteht.

Reaktion auf ein Leistungsereignis, das durch eine HA Übernahme in Active IQ Unified Manager verursacht wurde

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch hohe Data Processing auf einem Cluster-Knoten verursacht wurde, der sich in einem Hochverfügbarkeitspaar (HA) befindet. Mit Unified Manager können Sie außerdem den Systemstatus der Knoten prüfen, um festzustellen, ob kürzlich auf den Knoten erkannte Systemstatusereignisse zu dem Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die **Beschreibung** enthält die am Ereignis beteiligten Workloads und die betroffene Clusterkomponente.

   Es gibt ein betroffenes Volume, dessen Latenz durch die Clusterkomponente in Konflikt beeinträchtigt wurde. Der Data Processing Knoten, der alle Workloads von seinem Partnerknoten übernommen hat, ist die Clusterkomponente in Konflikt. Unter „Component in Contention“ ist das Data Processing Symbol rot hervorgehoben, und der Name des Knotens, der zum Zeitpunkt des Ereignisses die Data Processing verarbeitete, wird in Klammern angezeigt.

3. In der **Beschreibung** wählen Sie den Namen des Volumes aus.

   Die Seite „Volume Performance Explorer“ wird angezeigt. Oben auf der Seite zeigt in der Zeitleiste der Ereignisse ein Symbol für ein Änderungsereignis (🔵) den Zeitpunkt an, zu dem Unified Manager den Beginn der HA-Übernahme erkannt hat.

4. Wenn der Cursor auf das Änderungsereignissymbol für die HA-Übernahme zeigt, werden Details zur HA-Übernahme als Hover-Text angezeigt.

   Im Latenzdiagramm zeigt ein Ereignis an, dass das ausgewählte Volume aufgrund hoher Latenz etwa zur gleichen Zeit wie die HA-Übernahme den Performance-Schwellenwert überschritten hat.

5. Mit **Zoom View** wird das Latenzdiagramm auf einer neuen Seite angezeigt.
6. Im Menü „Ansicht“ dient **Cluster Components** zur Anzeige der Gesamtlatenz nach Clusterkomponente.
7. Wenn Sie den Mauszeiger auf das Änderungsereignissymbol für den Beginn der HA Übernahme richten, lässt sich die Latenz für Data Processing mit der Gesamtlatenz vergleichen.

   Zum Zeitpunkt der HA-Übernahme kam es aufgrund der erhöhten Workload-Anforderung auf dem Data Processing Knoten zu einem sprunghaften Anstieg der Data Processing. Die erhöhte CPU-Auslastung führte zu einer höheren Latenz und löste das Ereignis aus.

8. Nach der Reparatur des ausgefallenen Knotens erfolgt die Durchführung einer HA-Rückführung in ONTAP System Manager, wodurch die Workloads vom Partnerknoten auf den reparierten Knoten verschoben werden.
9. Nach Abschluss des HA Giveback und nach der nächsten Konfigurationserkennung in Unified Manager (ca. 15 Minuten) lassen sich auf der Inventarseite **Event Management** das Ereignis und die Workload finden, die durch das HA Takeover ausgelöst wurden.

   Das durch die HA-Übernahme ausgelöste Ereignis hat nun den Status „veraltet“, was darauf hinweist, dass das Ereignis behoben ist. Die Latenz der Data Processing-Komponente hat sich verringert, wodurch die Gesamtlatenz gesunken ist. Der Knoten, den das ausgewählte Volume nun für Data Processing verwendet, hat das Ereignis behoben.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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