Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten

Active IQ Unified Manager 9.8

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-98/performance-checker/task-identifying-victim-workloads-involved-in-a-performance-event.html on January 31, 2025. Always check docs.netapp.com for the latest.

Inhalt

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten . . . 1
Identifizierung der Opfer-Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind . . . 1
Identifizierung problematischer Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind . . . 1
Erkennen von Haifischlasten, die an einem dynamischen Performance-Ereignis beteiligt sind . . . 2
Performance-Ereignisanalyse für eine MetroCluster-Konfiguration . . . 3
Er reagiert auf ein dynamisches Performance-Ereignis, das durch die QoS-Richtliniengruppendrosselung verursacht wird . . . 5
Reaktion auf ein dynamisches Performance-Ereignis aufgrund eines Festplattenausfalls . . . 7
Er reagiert auf ein dynamisches Performance-Ereignis, das durch HA Takeover verursacht wird . . . 8

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten

Ereignisse, die aus dynamischen Schwellenwerten generiert werden, geben an, dass die tatsächliche Reaktionszeit (Latenz) für einen Workload zu hoch oder zu niedrig ist im Vergleich zum erwarteten Reaktionszeitbereich. Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

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

Identifizierung der Opfer-Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Volume Workloads die höchste Abweichung der Reaktionszeit (Latenz) aufweisen, die durch eine Storage-Komponente verursacht wurde. Anhand der Identifizierung dieser Workloads können Sie nachvollziehen, warum die Client-Applikationen, auf die sie zugreifen, langsamer als normal ausgeführt wurden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Abweichung von Aktivität oder Auslastung der Komponente oder am stärksten vom Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Opfer-Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Workloads mit dem Opfer anzuzeigen.

Identifizierung problematischer Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste

Nutzungsabweichung einer Clusterkomponente aufweisen. Anhand der Ermittlung dieser Workloads können Sie nachvollziehen, warum bestimmte Volumes des Clusters über langsame Reaktionszeiten (Latenz) verfügen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Bully Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten problematischer Workloads anzuzeigen, die sich auf die Komponente auswirken.

Erkennen von Haifischlasten, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste Nutzungsabweichung einer Storage-Komponente aufweisen. Anhand der Identifizierung dieser Workloads können Sie ermitteln, ob diese Workloads in ein weniger ausgelasttes Cluster verschoben werden sollen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es gibt ein neues, anerkanntes oder überholes dynamisches Ereignis für die Leistung.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Shark-Workloads** aus.

3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Haifischarbeitslasts.

Performance-Ereignisanalyse für eine MetroCluster-Konfiguration

Sie können mit Unified Manager ein Performance-Ereignis für eine MetroCluster-Konfiguration analysieren. Sie können die an dem Ereignis beteiligten Workloads ermitteln und die vorgeschlagenen Maßnahmen zur Lösung prüfen.

MetroCluster-Performance-Ereignisse können auf *bully* Workloads zurückzuführen sein, die die Interswitch-Links (ISLs) zwischen den Clustern überlasten oder aufgrund von Systemzustandsproblemen. Unified Manager überwacht jedes Cluster in einer MetroCluster-Konfiguration unabhängig und berücksichtigt dabei nicht die Performance-Ereignisse in einem Partner-Cluster.

Außerdem werden auf der Seite „Unified ManagerDashboard“ Performancereignisse beider Cluster in der MetroCluster-Konfiguration angezeigt. Sie können auch die Systemzustandsseiten von Unified Manager anzeigen, um den Zustand der einzelnen Cluster zu überprüfen und ihre Beziehung anzuzeigen.

Analyse eines dynamischen Performance-Ereignisses auf einem Cluster in einer MetroCluster Konfiguration

Sie können Unified Manager verwenden, um das Cluster in einer MetroCluster-Konfiguration zu analysieren, bei der ein Performance-Ereignis erkannt wurde. Sie können den Cluster-Namen, die Ereigniserkennungszeit und die damit verbundenen Workloads *bully* und *victim* identifizieren.

Bevor Sie beginnen

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

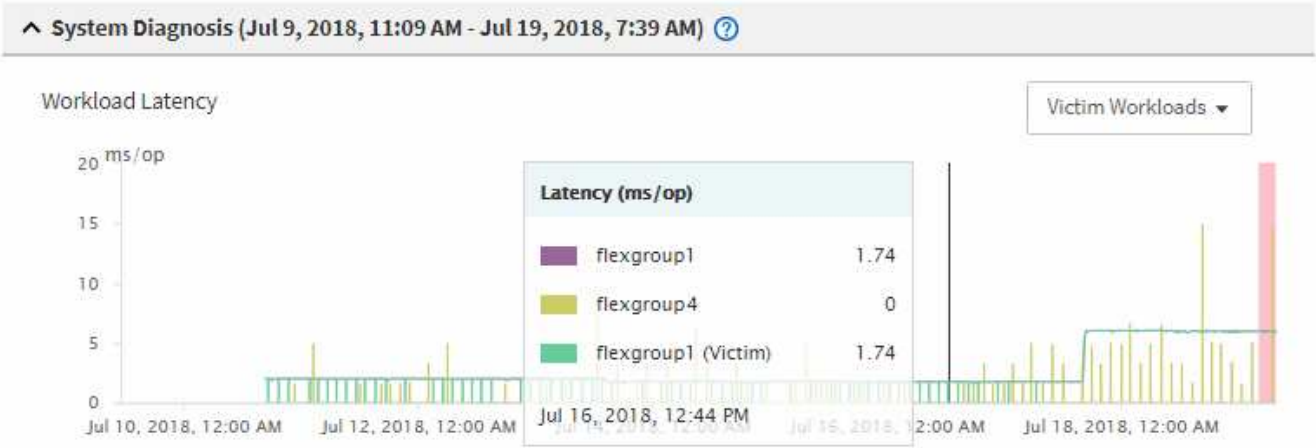
Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Die Ereignisbeschreibung enthält Namen der betroffenen Workloads sowie die Anzahl der betroffenen Workloads.

   In diesem Beispiel ist das Symbol für MetroCluster-Ressourcen rot dargestellt, was bedeutet, dass die MetroCluster-Ressourcen über Konflikte verfügen. Sie positionieren den Cursor über das Symbol, um eine Beschreibung des Symbols anzuzeigen.

3. Notieren Sie sich den Cluster-Namen und die Ereignis-Erkennungszeit, mit der Sie Performance-Ereignisse im Partner-Cluster analysieren können.
4. Überprüfen Sie in den Diagrammen die „_victim_Workloads“, um zu bestätigen, dass ihre Antwortzeiten höher sind als der Performance-Schwellenwert.

   In diesem Beispiel wird der Workload des Opfers im Hover-Text angezeigt. Die Latenzdiagramme werden auf hoher Ebene angezeigt, ein konsistentes Latenzmuster für die betroffenen Opfer-Workloads. Obwohl die anormale Latenz der betroffenen Workloads das Ereignis ausgelöst hat, kann ein konsistentes Latenzmuster darauf hindeuten, dass die Workloads innerhalb des erwarteten Bereichs liegen. Durch einen Spitzen bei den I/O wurde die Latenz erhöht und das Ereignis ausgelöst.



   Falls Sie vor Kurzem eine Applikation auf einem Client installiert haben, der auf diese Volume-Workloads zugreift und die Applikation eine hohe Anzahl an I/O-Vorgängen sendet, kann die Verzögerungen bereits vorwegnehmen. Wenn die Latenz für die Workloads innerhalb des erwarteten Bereichs zurückkehrt, ändert sich der Ereignisstatus zu veraltet und bleibt mehr als 30 Minuten in diesem Status, können Sie das Ereignis wahrscheinlich ignorieren. Wenn das Ereignis andauernde und im neuen Status verbleibt, können Sie es weiter untersuchen, um festzustellen, ob andere Probleme das Ereignis verursacht haben.

5. Wählen Sie im Workload-Durchsatzdiagramm die Option **problematische Workloads** aus, um die problematische Workloads anzuzeigen.

   Die Anwesenheit von problematischer Workloads zeigt an, dass ein Ereignis möglicherweise durch eine oder mehrere Workloads auf dem lokalen Cluster verursacht wurde, bei denen die MetroCluster-Ressourcen überlastet sind. Die problematische Workloads weisen eine hohe Abweichung beim Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm zeigt auf hoher Ebene das Muster für den Schreibdurchsatz (MB/s) für die Workloads an. Sie können das MB/s-Muster für Schreibvorgänge überprüfen, um einen anormalen Durchsatz zu identifizieren, der darauf hindeutet, dass ein Workload die MetroCluster-Ressourcen überausgelastet ist.

   Wenn an diesem Ereignis keine problematische Workloads beteiligt sind, wurde dieses Ereignis möglicherweise durch ein Systemzustandsproblem mit der Verbindung zwischen den Clustern oder durch

ein Performance-Problem auf dem Partner-Cluster verursacht. Sie können Unified Manager verwenden, um den Systemzustand beider Cluster in einer MetroCluster Konfiguration zu überprüfen. Außerdem können Sie mit Unified Manager Performance-Ereignisse im Partner-Cluster überprüfen und analysieren.

Analyse eines dynamischen Performance-Ereignisses für ein Remote-Cluster auf einer MetroCluster-Konfiguration

Mit Unified Manager können Sie dynamische Performance-Ereignisse auf einem Remote-Cluster in einer MetroCluster-Konfiguration analysieren. Mit der Analyse können Sie ermitteln, ob ein Ereignis im Remote-Cluster ein Ereignis auf seinem Partner-Cluster verursacht hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen ein Performance-Ereignis auf einem lokalen Cluster in einer MetroCluster Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Zustand des lokalen Clusters und dessen am Performance-Ereignis beteiligten Partner-Clusters überprüft und den Namen des Partner-Clusters erhalten haben.

Schritte

1. Loggen Sie sich bei der Unified Manager-Instanz ein, die das Partner-Cluster überwacht.
2. Klicken Sie im linken Navigationsbereich auf **Events**, um die Ereignisliste anzuzeigen.
3. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte Stunde** aus und klicken Sie dann auf **Bereich anwenden**.
4. Wählen Sie im Auswahlfeld **Filterung** im linken Dropdown-Menü die Option **Cluster** aus, geben Sie den Namen des Partner Clusters in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

   Wenn während der letzten Stunde keine Ereignisse für das ausgewählte Cluster vorhanden sind, zeigt dies an, dass es während des Ereignisses beim Partner keine Performance-Probleme aufgetreten sind.

5. Wenn im ausgewählten Cluster Ereignisse über die letzte Stunde erkannt wurden, vergleichen Sie die Ereignis-Erkennungszeit mit der Ereignis-Erkennungszeit für das Ereignis auf dem lokalen Cluster.

   Wenn diese Ereignisse problematische Workloads verursachen, die zu Konflikten bei der Datenverarbeitungskomponente führen, könnte ein oder mehrere dieser Punkte das Ereignis auf dem lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Aktionen für die Lösung auf der Seite Ereignisdetails zu prüfen.

   Wenn diese Ereignisse keine problematische Workloads betreffen, wurden sie nicht zum Performance-Ereignis auf dem lokalen Cluster verursacht.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch die QoS-Richtliniengruppendrosselung verursacht wird

Sie können mit Unified Manager ein Performance-Ereignis untersuchen, das durch eine

QoS-Richtliniengruppe (Quality of Service) verursacht wird, die den Workload-Durchsatz (MB/s) drosselt. Die Drosselung hat die Reaktionszeiten (Latenz) von Volume-Workloads in der Richtliniengruppe erhöht. Anhand der Ereignisinformationen können Sie bestimmen, ob neue Grenzen für die Richtliniengruppen erforderlich sind, um die Drosselung zu stoppen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, die den Namen der von der Drosselung betroffenen Workloads anzeigt.

   Die Beschreibung kann dieselbe Arbeitslast für das Opfer und den Täter anzeigen, da die Drosselung den Workload zum Opfer selbst macht.

3. Notieren Sie den Namen des Volumes mit einer Anwendung wie einem Texteditor.

   Sie können den Volume-Namen suchen, um ihn später zu finden.

4. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Auslastung **Bully Workloads** aus.
5. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast oben in der Liste hat die höchste Abweichung und verursacht die Drosselung. Die Aktivität entspricht dem Prozentsatz des von den einzelnen Workloads verwendeten Richtliniengruppenlimits.

6. Klicken Sie im Bereich **Suggested Actions** auf die Schaltfläche **Analyze Workload** für den oberen Workload.
7. Legen Sie auf der Seite **Workload Analysis** das Latenzdiagramm fest, um alle Cluster-Komponenten und das Durchsatzdiagramm zur Anzeige von Aufschlüsselung anzuzeigen.

   Die Aufschlüsselung werden unter dem Latenzdiagramm und dem IOPS-Diagramm angezeigt.

8. Vergleichen Sie die QoS-Limits im Diagramm * Latenz*, um zu sehen, welche Drosselung sich zum Zeitpunkt des Ereignisses auf die Latenz ausgewirkt hat.

   Die QoS-Richtliniengruppe weist einen maximalen Durchsatz von 1,000 Operationen pro Sekunde (in op/s) auf, die die Workloads in ihrer Gruppe nicht gemeinsam übersteigen können. Zum Zeitpunkt des Ereignisses führten die Workloads in der Richtliniengruppe einen Gesamtdurchsatz von über 1,200 Op/s durch, sodass die Richtliniengruppe ihre Aktivität wieder auf 1,000 Op/Sek. ausbremsen konnte

9. Vergleichen Sie die **Lese/Schreib Latenz** Werte mit den **Lese-/Schreibvorgängen/anderen** Werten.

   Beide Diagramme zeigen eine hohe Anzahl von Leseanforderungen mit einer hohen Latenz, jedoch ist die Anzahl der Anfragen und die Menge der Latenz für Schreibanforderungen niedrig. Anhand dieser Werte können Sie ermitteln, ob ein hoher Durchsatz oder eine höhere Anzahl an Operationen die Latenz erhöht. Sie können diese Werte verwenden, wenn Sie sich entscheiden, ein Richtliniengruppenlimit auf den

Durchsatz oder die Operationen zu legen.

10. Verwenden Sie ONTAP System Manager, um die aktuelle Obergrenze für die Richtliniengruppe auf 1,300 Op/Sek. zu erhöhen
11. Kehren Sie nach einem Tag zu Unified Manager zurück und geben Sie den Workload ein, den Sie in Schritt 3 auf der Seite * Workload Analysis* aufgezeichnet haben.
12. Wählen Sie das Diagramm zum Durchsatz aus.

    Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird angezeigt.

13. Zeigen Sie oben auf der Seite mit dem Cursor auf das Symbol Ereignis ändern ( ) Für die Änderung der Policy-Gruppengrenzen.
14. Vergleichen Sie das Diagramm **Lese/Schreibvorgänge/Sonstiges** mit dem Diagramm **Latenz**.

    Die Lese- und Schreibanfragen sind dieselben, aber die Drosselung hat gestoppt und die Latenz ist gesunken.

Reaktion auf ein dynamisches Performance-Ereignis aufgrund eines Festplattenausfalls

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch die Überprovisionierung eines Aggregats verursacht wird. Sie können auch Unified Manager verwenden, um den Systemzustand des Aggregats zu überprüfen, um zu ermitteln, ob kürzlich auf dem Aggregat erkannte Systemzustandsereignisse zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

    Es gibt mehrere Opfer-Volumes, deren Latenz von der Cluster-Komponente mit Konflikten beeinträchtigt wurde. Das Aggregat, das sich in der Mitte eines RAID-Rekonstruktionss befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die Clusterkomponente. Unter „Komponente in Konflikt“ ist das Aggregat-Symbol rot hervorgehoben und der Name des Aggregats wird in Klammern angezeigt.

3. Wählen Sie im Diagramm Workload-Auslastung die Option **Bully Workloads** aus.
4. Bewegen Sie den Mauszeiger über das Diagramm, um die obersten Workloads anzuzeigen, die sich auf die Komponente auswirken.

    Die wichtigsten Workloads mit der höchsten Spitzenauslastung seit dem Erkennen des Ereignisses werden oben in der Tabelle angezeigt. Einer der wichtigsten Workloads ist der durch das System definierte

Workload Disk Health, der auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess zur Wiederherstellung des Aggregats mit der freien Platte. Der Disk Health Workload und die anderen Workloads im Aggregat verursachten wahrscheinlich die Konflikte im Aggregat und das zugehörige Ereignis.

5. Nachdem Sie bestätigt haben, dass die Aktivitäten des Festplatten-Status-Workloads das Ereignis verursacht haben, warten Sie ca. 30 Minuten, bis die Rekonstruktion abgeschlossen ist, und warten Sie, bis Unified Manager das Ereignis analysiert und erkennt, ob es noch im Aggregat zu Konflikten kommt.
6. Aktualisieren Sie die **Veranstaltungsdetails**.

   Überprüfen Sie nach Abschluss der RAID-Rekonstruktion, ob der Status veraltet ist, und geben Sie an, dass das Ereignis behoben ist.

7. Wählen Sie im Workload-Auslastungsdiagramm **Bully Workloads** aus, um die Workloads auf dem Aggregat nach Spitzenauslastung zu sehen.
8. Klicken Sie im Bereich **Suggested Actions** auf die Schaltfläche **Analyze Workload** für den oberen Workload.
9. Legen Sie auf der Seite **Workload Analysis** den Zeitbereich fest, um die letzten 24 Stunden (1 Tag) der Daten für das ausgewählte Volumen anzuzeigen.

   In der Ereigniszeitleiste ist ein roter Punkt (🔴) Gibt an, wann das Ereignis des Festplattenfehlers aufgetreten ist.

10. Verbergen Sie im Diagramm für die Knotenauslastung und Aggregat die Zeile für die Knoten-Statistiken, so dass nur die Aggregat-Zeile bleibt.
11. Vergleichen Sie die Daten in diesem Diagramm mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latenz**.

    Zum Zeitpunkt des Ereignisses zeigt die aggregierte Auslastung einen hohen Anteil an Lese- und Schreibvorgängen durch die RAID-Rekonstruktionsprozesse an, wodurch die Latenz des ausgewählten Volumes erhöht wurde. Einige Stunden nach dem Ereignis waren sowohl die Lese- als auch die Schreibvorgänge sowie die Latenz gesunken, sodass die Konflikte zwischen dem Aggregat nicht mehr bestehen.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch HA Takeover verursacht wird

Mit Unified Manager können Sie ein Performance-Ereignis anhand hoher Datenverarbeitung auf einem Cluster Node in einem Hochverfügbarkeitspaar (HA-Paar) untersuchen. Sie können auch Unified Manager verwenden, um den Systemzustand der Nodes zu überprüfen, ob kürzlich entdeckte Systemzustandsereignisse auf den Nodes, die zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

   Es gibt ein Opfer-Volume, dessen Latenz von der Cluster-Komponente im Konflikt beeinträchtigt wurde. Der Datenverarbeitungs-Node, der alle Workloads vom Partner-Node übernommen hat, ist die Cluster-Komponente im Konflikt. Unter Komponente in Konflikt wird das Symbol für die Datenverarbeitung rot markiert und der Name des Node, der zum Zeitpunkt des Ereignisses die Datenverarbeitung verarbeitet hat, wird in Klammern angezeigt.

3. Klicken Sie in der **Beschreibung** auf den Namen des Volumes.

   Die Seite Volume Performance Explorer wird angezeigt. Oben auf der Seite, in der Zeile Ereignisse Zeit, ein Symbol für das Ereignis ändern ( ) Gibt die Zeit an, zu der Unified Manager den Start der HA-Übernahme erkannt hat.

4. Zeigen Sie den Mauszeiger auf das Änderungsereignis-Symbol für die HA-Übernahme und Details zur HA-Übernahme werden in Hover-Text angezeigt.

   Im Latenzdiagramm zeigt ein Ereignis an, dass das ausgewählte Volume aufgrund einer hohen Latenz um die gleiche Zeit wie das HA-Takeover den Performance-Schwellenwert überschritten hat.

5. Klicken Sie auf **Zoom View**, um das Latenzdiagramm auf einer neuen Seite anzuzeigen.
6. Wählen Sie im Menü Ansicht die Option **Cluster Components** aus, um die gesamte Latenz nach Clusterkomponente anzuzeigen.
7. Zeigen Sie mit der Maus auf das Änderungssymbol für den Start des HA-Takeover und vergleichen Sie die Latenz für die Datenverarbeitung mit der gesamten Latenz.

   Zum Zeitpunkt der HA-Übernahme betrug die Datenverarbeitung aufgrund der steigenden Workload-Anforderungen am Datenverarbeitungs-Node eine Spitze. Die höhere CPU-Auslastung steigerte die Latenz und löste das Ereignis aus.

8. Nach der Behebung des fehlerhaften Knotens führt ONTAP System Manager ein HA-Giveback durch, wodurch die Workloads vom Partner-Node zum festgelegten Node verschoben werden.
9. Nach Abschluss des HA-Giveback. Ermitteln Sie nach der nächsten Konfigurationsermittlung im Unified Manager (ca. 15 Minuten) das Ereignis und den Workload, das durch den HA-Takeover auf der Seite **Event Management** Inventory ausgelöst wurde.

   Das durch die HA Übernahme ausgelöste Ereignis weist jetzt einen Status als veraltet auf, sodass das Ereignis gelöst werden kann. Die Latenz der Komponente für die Datenverarbeitung wurde herabgesetzt, wodurch die gesamte Latenz verringert wurde. Der Node, den das ausgewählte Volume jetzt zur Datenverarbeitung verwendet, hat das Ereignis aufgelöst.

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.