Performance Ereignisanalyse für eine MetroCluster Konfiguration

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_performance_incident_analysis_for_metrocluster_configuration.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Performance Ereignisanalyse für eine MetroCluster Konfiguration 1
Analyse von MetroCluster Leistungsereignissen mit Active IQ Unified Manager 1
Analyse eines MetroCluster Leistungsereignisses auf einem Cluster in Active IQ Unified Manager 1
Analyse eines MetroCluster Leistungsereignisses auf einem Remote Cluster in Active IQ Unified Manager 3

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

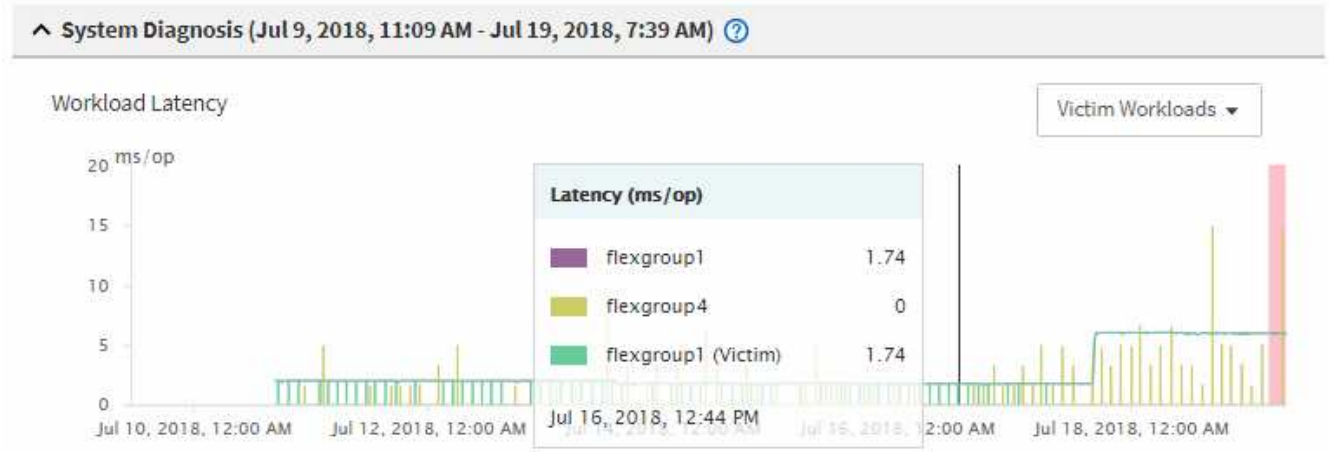
1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die Ereignisbeschreibung enthält die Namen der beteiligten Workloads und deren Anzahl.

   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.

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.