Monitoring der Performance

ONTAP 9

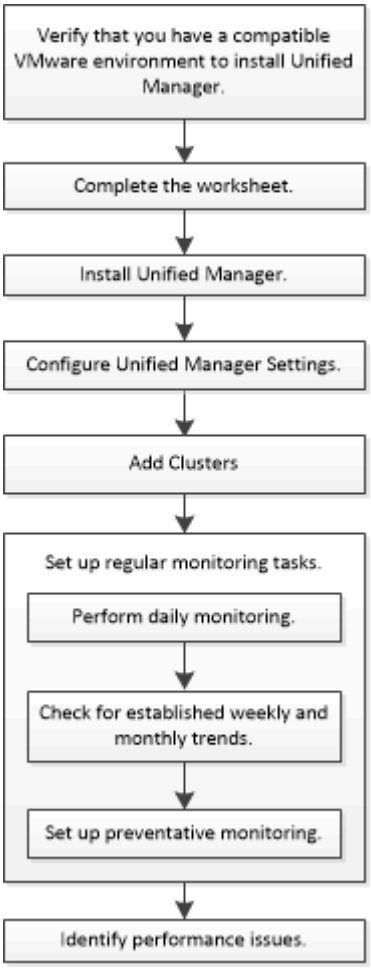
NetApp
September 12, 2024

Inhalt

Monitoring der Performance

Workflow-Übersicht zur Performance-Überwachung und Wartung

Zur Überwachung und Aufrechterhaltung der Cluster-Performance müssen die Active IQ Unified Manager Software installiert, grundlegende Monitoring-Aufgaben eingerichtet, Performance-Probleme erkannt und nach Bedarf Anpassungen vorgenommen werden.



Stellen Sie sicher, dass Ihre VMware-Umgebung unterstützt wird

Für eine erfolgreiche Installation von Active IQ Unified Manager müssen Sie überprüfen, ob Ihre VMware Umgebung die erforderlichen Anforderungen erfüllt.

Schritte

1. Vergewissern Sie sich, dass Ihre VMware Infrastruktur den Größenanforderungen für die Installation von Unified Manager entspricht.
2. Wechseln Sie zum "Interoperabilitätsmatrix" Um zu überprüfen, ob Sie eine unterstützte Kombination der folgenden Komponenten haben:

- ONTAP-Version
- ESXi-Betriebssystemversion
- VMware vCenter Server-Version
- VMware Tools-Version
- Browsertyp und -Version

```
http://mysupport.netapp.com/matrix["Interoperabilitätsmatrix"
^]In sind die für Unified Manager unterstützten
Konfigurationen aufgeführt.
```

3. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

   Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.

4. Überprüfen Sie die Informationen auf den folgenden Registerkarten:
   - Hinweise

     Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

   - Richtlinien und Richtlinien

     Allgemeine Richtlinien für alle Konfigurationen

Active IQ Unified Manager-Arbeitsblatt

Vor Installation, Konfiguration und Verbindung von Active IQ Unified Manager sollten spezifische Informationen zur Systemumgebung sofort verfügbar sein. Sie können die Informationen im Arbeitsblatt aufzeichnen.

Informationen zur Installation von Unified Manager

Virtual Machine, auf der Software bereitgestellt wird	Ihr Wert
IP-Adresse des ESXi-Servers	
Vollständig qualifizierter Domain-Name des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	

Sekundäre DNS-Adresse	
Domänen durchsuchen	
Wartungs-Benutzername	
Wartungs-Benutzer-Passwort	

Informationen zur Unified Manager-Konfiguration

Einstellung	Ihr Wert
Wartungs-Benutzer-E-Mail-Adresse	
NTP-Server	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Standardport	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	
LDAP Bind Distinguished Name	
LDAP-Bindekennwort	
Name des Active Directory-Administrators	
Active Directory-Kennwort	
Authentifizierungsserverbasis mit Distinguished Name	
Hostname oder IP-Adresse des Authentifizierungsservers	

Cluster-Informationen

Erfassen Sie die folgenden Informationen für jedes Cluster auf Unified Manager.

Cluster 1 von N	Ihr Wert

Host-Name oder Cluster-Management-IP-Adresse	
Benutzername des ONTAP-Administrators Dem Administrator muss die Rolle „admin“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll (HTTP oder HTTPS)	

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

Installation von Active IQ Unified Manager

Active IQ Unified Manager herunterladen und implementieren

Um die Software zu installieren, müssen Sie die Installationsdatei für die virtuelle Appliance (VA) herunterladen und dann einen VMware vSphere Client verwenden, um die Datei auf einem VMware ESXi-Server bereitzustellen. Die VA ist in einer OVA-Datei verfügbar.

Schritte

1. Gehen Sie auf die Seite **NetApp Support Site zum Software-Download** und suchen Sie nach Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Wählen Sie im Dropdown-Menü **Plattform auswählen** * VMware vSphere* aus und klicken Sie auf **Go!**
3. Speichern Sie die Datei „`OVA`“ in einem lokalen oder Netzwerkspeicherort, auf den Ihr VMware vSphere Client zugreifen kann.
4. Klicken Sie in VMware vSphere Client auf **Datei** > **OVF-Vorlage bereitstellen**.
5. Suchen Sie die Datei „`OVA`“ und stellen Sie die virtuelle Appliance mithilfe des Assistenten auf dem ESXi-Server bereit.

   Sie können die Registerkarte **Eigenschaften** im Assistenten verwenden, um Ihre statischen Konfigurationsdaten einzugeben.

6. Schalten Sie die VM ein.
7. Klicken Sie auf die Registerkarte **Konsole**, um den Startvorgang anzuzeigen.
8. Folgen Sie der Eingabeaufforderung, um VMware Tools auf der VM zu installieren.
9. Zeitzone konfigurieren.
10. Geben Sie einen Wartungs-Benutzernamen und ein Passwort ein.
11. Wechseln Sie zur URL, die von der VM-Konsole angezeigt wird.

Konfigurieren Sie die anfänglichen Active IQ Unified Manager-Einstellungen

Das Dialogfeld Active IQ Unified Manager Initial Setup wird angezeigt, wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen. Dadurch können Sie einige Anfangseinstellungen konfigurieren und Cluster hinzufügen.

Schritte

1. Akzeptieren Sie die Standardeinstellung AutoSupport Enabled.
2. Geben Sie die NTP-Serverdetails, die E-Mail-Adresse des Wartungsbenutzers, den SMTP-Servernamen und weitere SMTP-Optionen ein, und klicken Sie dann auf **Speichern**.

Nachdem Sie fertig sind

Nach Abschluss der Ersteinrichtung wird die Seite „Cluster-Datenquellen“ angezeigt, auf der Sie die Cluster-Details hinzufügen können.

Geben Sie die zu überwachenden Cluster an

Sie müssen einem Active IQ Unified Manager-Server ein Cluster hinzufügen, um das Cluster zu überwachen, den Status der Cluster-Erkennung anzuzeigen und die Performance zu überwachen.

Was Sie benötigen

- Sie müssen die folgenden Informationen haben:
  - Host-Name oder Cluster-Management-IP-Adresse

    Der Hostname ist der vollständig qualifizierte Domänenname (FQDN) oder der Kurzname, den Unified Manager zur Verbindung mit dem Cluster verwendet. Dieser Hostname muss mit der Cluster-Management-IP-Adresse aufgelöst werden.

  Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.

  - Benutzername und Passwort für den ONTAP-Administrator
  - Typ des Protokolls (HTTP oder HTTPS), der für das Cluster und die Portnummer des Clusters konfiguriert werden kann
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Der ONTAP-Administrator muss über die ONTAPI- und SSH-Administratorrollen verfügen.
- Der FQDN des Unified Managers muss ONTAP pingen können.

  Dies können Sie mit dem ONTAP-Befehl überprüfen `ping -node node_name -destination Unified_Manager_FQDN`.

Über diese Aufgabe

Für eine MetroCluster Konfiguration müssen Sie sowohl die lokalen als auch die Remote-Cluster hinzufügen, und die Cluster müssen korrekt konfiguriert sein.

Schritte

1. Klicken Sie Auf **Konfiguration** > **Cluster-Datenquellen**.
2. Klicken Sie auf der Seite Cluster auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cluster hinzufügen** die erforderlichen Werte an, z. B. den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Clusters, Benutzernamen, Passwort, Protokoll zur Kommunikation und Portnummer.

   Standardmäßig ist das HTTPS-Protokoll ausgewählt.

   Sie können die Cluster-Management-IP-Adresse von IPv6 zu IPv4 oder von IPv4 zu IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Cluster-Raster und die Seite zur Cluster-Konfiguration angezeigt.
4. Klicken Sie Auf **Hinzufügen**.
5. Wenn HTTPS ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie im Dialogfeld **Autorisieren Host** auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.

   b. Klicken Sie Auf **Ja**.

      Unified Manager überprüft das Zertifikat nur, wenn das Cluster erstmalig hinzugefügt wird, überprüft es aber nicht für jeden API-Aufruf an ONTAP.

   Wenn das Zertifikat abgelaufen ist, können Sie das Cluster nicht hinzufügen. Sie müssen das SSL-Zertifikat erneuern und dann den Cluster hinzufügen.
6. **Optional**: Anzeigen des Clusterermittlungsstatus:

   a. Überprüfen Sie den Cluster-Erkennungsstatus auf der Seite **Cluster Setup**.

   Das Cluster wird der Unified Manager-Datenbank nach dem Standard-Monitoring-Intervall von ca. 15 Minuten hinzugefügt.

Einrichten grundlegender Überwachungsaufgaben

Tägliche Überwachung

Sie können eine tägliche Überwachung durchführen, um sicherzustellen, dass keine unmittelbaren Performance-Probleme auftreten, die Aufmerksamkeit erfordern.

Schritte

1. Rufen Sie in der Active IQ Unified Manager-Benutzeroberfläche die Seite **Ereignisbestand** auf, um alle aktuellen und veralteten Ereignisse anzuzeigen.
2. Wählen Sie aus der Option **Ansicht** die Option `Active Performance Events` Und zu ermitteln, welche Maßnahmen erforderlich sind.

Ermitteln Sie Performance-Probleme anhand von wöchentlichen und monatlichen Performance-Trends

Anhand des Aufspüren von Performance-Trends können Sie erkennen, ob der Cluster überlastet ist oder nicht optimal genutzt wird, indem Sie die Latenz von Volumes

analysieren. Anhand ähnlicher Schritte können Sie CPU-, Netzwerk- oder andere Systemengpässe identifizieren.

Schritte

1. Suchen Sie das Volumen, das Sie vermutlich nicht optimal nutzen oder zu wenig nutzen.
2. Klicken Sie auf der Registerkarte **Volume Details** auf **30 d**, um die historischen Daten anzuzeigen.
3. Wählen Sie im Dropdown-Menü „Data by aufbrechen“ die Option **Latenz** aus und klicken Sie dann auf **Senden**.
4. Heben Sie die Auswahl von * Aggregat* im Vergleichstabelle der Cluster-Komponenten auf und vergleichen Sie dann die Cluster-Latenz mit dem Latenzdiagramm für das Volume.
5. Wählen Sie * Aggregat* aus und deaktivieren Sie die Auswahl aller anderen Komponenten im Vergleichstabelle der Cluster-Komponenten, und vergleichen Sie dann die aggregierte Latenz mit dem Latenzdiagramm für das Volume.
6. Vergleichen Sie das Diagramm für die Latenz bei Lese-/Schreibvorgängen mit dem Latenzdiagramm für das Volume.
7. Ermitteln, ob die Client-Applikationslasten einen Workload-Konflikt verursacht haben und Workloads nach Bedarf wieder ausgleichen.
8. Ermitteln Sie, ob das Aggregat zu stark beansprucht ist, und verursachen Sie Konflikte, und gleichen Sie Workloads je nach Bedarf aus.

Verwenden Sie Performance-Schwellenwerte zur Ereignisbenachrichtigung

Ereignisse sind Benachrichtigungen, die die Active IQ Unified Manager automatisch generiert, wenn eine vordefinierte Bedingung eintritt, oder wenn ein Performance-Zählerwert einen Schwellenwert überschreitet. Ereignisse helfen Ihnen bei der Ermittlung von Performance-Problemen in den von Ihnen überwachten Clustern. Sie können Benachrichtigungen so konfigurieren, dass automatisch E-Mail-Benachrichtigungen gesendet werden, wenn Ereignisse bestimmter Schweregrade auftreten.

Festlegen von Performance-Schwellenwerten

Sie können Performance-Schwellenwerte festlegen, um kritische Performance-Probleme zu überwachen. Benutzerdefinierte Schwellenwerte lösen eine Warnung oder eine wichtige Ereignisbenachrichtigung aus, wenn das System den definierten Schwellenwert erreicht oder überschreitet.

Schritte

1. Erstellen der Schwellenwerte für Warnung und kritisches Ereignis:
   a. Wählen Sie **Konfiguration** > **Leistungsschwellenwerte**.
   b. Klicken Sie Auf **Erstellen**.
   c. Wählen Sie den Objekttyp aus, und geben Sie einen Namen und eine Beschreibung der Richtlinie an.
   d. Wählen Sie die Zählerbedingung des Objekts aus, und geben Sie die Grenzwerte an, die Warnungs- und kritische Ereignisse definieren.
   e. Wählen Sie die Dauer aus, für die die Grenzwerte für ein zu sendes Ereignis überschritten werden müssen, und klicken Sie dann auf **Speichern**.

2. Weisen Sie die Schwellenwertrichtlinie dem Storage-Objekt zu.
    a. Wechseln Sie zur Seite „Inventar“ für denselben Cluster-Objekttyp, den Sie zuvor ausgewählt haben, und wählen Sie aus der Option „Ansicht“ die Option „**Performance**“ aus.
    b. Wählen Sie das Objekt aus, dem Sie die Schwellenwertrichtlinie zuweisen möchten, und klicken Sie dann auf **Grenzwertrichtlinie zuweisen**.
    c. Wählen Sie die zuvor erstellte Richtlinie aus und klicken Sie dann auf **Richtlinie zuweisen**.

Beispiel

Es können benutzerdefinierte Schwellenwerte festgelegt werden, die Informationen zu kritischen Performance-Problemen enthalten. Wenn Sie zum Beispiel einen Microsoft Exchange Server haben und Sie wissen, dass es abstürzt, wenn die Volume-Latenz 20 Millisekunden überschreitet, können Sie einen Warnschwellenwert mit 12 Millisekunden und einen kritischen Schwellenwert mit 15 Millisekunden setzen. Mit dieser Schwellenwerteinstellung können Sie Benachrichtigungen erhalten, wenn die Volume-Latenz die Obergrenze überschreitet.

Warnmeldungen hinzufügen

Sie können Benachrichtigungen konfigurieren, um Sie über die Erzeugung eines bestimmten Ereignisses zu benachrichtigen. Sie können Meldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse mit einem bestimmten Schweregrad konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und ein Skript der Warnmeldung zuordnen.

Was Sie benötigen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript auf der Grundlage des Ereignisses ausführen möchten, müssen Sie das Skript mithilfe der Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite „Alarmkonfiguration“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.

4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

   Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name "abc" enthält und schließt alle Volumes aus, deren Name "xyz" enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält "sample@domain.com", ein "Test"-Skript, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name "abc" enthält.
   b. Wählen Sie **<<All Volumes whose name contains 'abc'>>** aus dem Bereich Verfügbare Ressourcen und in den Bereich Ausgewählte Ressourcen verschieben.

c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.

3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test**-Skript aus.
8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie die Einstellungen für Warnmeldungen

Sie können festlegen, welche Ereignisse aus Active IQ Unified Manager-Trigger-Warnmeldungen, die E-Mail-Empfänger für diese Meldungen und die Häufigkeit der Meldungen betreffen.

Was Sie benötigen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Über diese Aufgabe

Sie können eindeutige Alarmeinstellungen für die folgenden Arten von Performance-Ereignissen konfigurieren:

- Kritische Ereignisse, die durch Verstöße gegen benutzerdefinierte Schwellenwerte ausgelöst werden
- Warnereignisse, die durch Verstöße gegen benutzerdefinierte Schwellenwerte, systemdefinierte Schwellenwerte oder dynamische Schwellenwerte ausgelöst werden

Standardmäßig werden E-Mail-Alarme für alle neuen Ereignisse an Unified Manager Admin-Benutzer gesendet. Sie können E-Mail-Benachrichtigungen an andere Benutzer senden, indem Sie die E-Mail-Adressen dieser Benutzer hinzufügen.

> Um das Senden von Warnmeldungen für bestimmte Ereignistypen zu deaktivieren, müssen Sie alle Kontrollkästchen in einer Ereigniskategorie löschen. Durch diese Aktion werden Ereignisse nicht in der Benutzeroberfläche angezeigt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Storage-Management** > **Alarm-Setup** aus.

   Die Seite „Alarm-Setup“ wird angezeigt.

2. Klicken Sie auf **Hinzufügen** und konfigurieren Sie die entsprechenden Einstellungen für jeden Ereignistypen.

   Um E-Mail-Benachrichtigungen an mehrere Benutzer zu senden, geben Sie ein Komma zwischen den einzelnen E-Mail-Adressen ein.

3. Klicken Sie Auf **Speichern**.

Performance-Probleme in Active IQ Unified Manager ermitteln

Wenn ein Performance-Ereignis eintritt, können Sie die Ursache des Problems in Active IQ Unified Manager lokalisieren und diese mithilfe anderer Tools beheben. Unter Umständen erhalten Sie während der täglichen Überwachung eine E-Mail-Benachrichtigung über ein Ereignis oder eine Benachrichtigung über das Ereignis.

Schritte

1. Klicken Sie in der E-Mail-Benachrichtigung auf den Link, der Sie mit einem Performance-Ereignis direkt zum Storage-Objekt bringt.

Sie suchen…	Dann…
Sie erhalten eine E-Mail-Benachrichtigung über ein Ereignis	Klicken Sie auf den Link, um direkt zur Seite mit den Veranstaltungsdetails zu gelangen.
Beachten Sie das Ereignis während der Analyse der Seite „Ereignisbestand“	Wählen Sie das Ereignis aus, um direkt zur Seite mit den Veranstaltungsdetails zu gelangen.

2. Wenn das Ereignis einen systemdefinierten Schwellenwert überschritten hat, befolgen Sie die vorgeschlagenen Aktionen in der UI, um das Problem zu beheben.
3. Wenn das Ereignis einen benutzerdefinierten Schwellenwert überschritten hat, analysieren Sie das Ereignis, um zu bestimmen, ob Sie Maßnahmen ergreifen müssen.
4. Wenn das Problem weiterhin besteht, überprüfen Sie die folgenden Einstellungen:
   - Protokolleinstellungen auf dem Storage-System
   - Netzwerkeinstellungen auf jedem Ethernet oder Fabric Switches
   - Netzwerkeinstellungen auf dem Storage-System
   - Das Festplattenlayout und die aggregierte Kennzahlen im Storage-System
5. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.