Monitore und Alarme

Data Infrastructure Insights

NetApp
September 09, 2025

Inhalt

Monitore und Alarme

Warnfunktionen mit Monitoren

Konfigurieren Sie Monitore, um Leistungsschwellenwerte, Protokollereignisse und Anomalien in Ihren Infrastrukturressourcen zu verfolgen. Erstellen Sie benutzerdefinierte Warnungen für Kennzahlen wie Schreiblatenz des Knotens, Speicherkapazität oder Anwendungsleistung und erhalten Sie Benachrichtigungen, wenn diese Bedingungen erfüllt sind.

Über Monitore können Sie Schwellenwerte auf Metriken festlegen, die von „Infrastruktur“-Objekten wie Storage, VM, EC2 und Ports generiert werden. Außerdem können Sie Daten zur „Integration“ verwenden, beispielsweise die für Kubernetes gesammelt wurden, erweiterte ONTAP Metriken und Telegraf Plug-ins. Diese *metrische* Überwachung warnt Sie, wenn Warnmeldungen oder kritische Schwellenwerte überschritten werden.

Sie können auch Monitore erstellen, um Warnmeldungen auf Warn-, kritischen oder informationellen Ebene auszulösen, wenn bestimmte *log-Ereignisse* erkannt werden.

Dateninfrastruktur Insights bietet ebenfalls eine Vielzahl an Funktionen"Systemdefinierte Monitore", je nach Umgebung.

Best Practice Für Sicherheit

Warnmeldungen zu Data Infrastructure Insights wurden entwickelt, um Datenpunkte und Trends für Ihren Mandanten hervorzuheben, und mit Data Infrastructure Insights können Sie jede gültige E-Mail-Adresse als Benachrichtigungsempfänger eingeben. Wenn Sie in einer sicheren Umgebung arbeiten, achten Sie besonders darauf, wer die Benachrichtigung erhält oder anderweitig Zugriff auf die Warnmeldung hat.

Metrik oder Protokollmonitor?

1. Klicken Sie im Menü Data Infrastructure Insights auf **Alerts > Manage Monitors**

   Die Listenseite Monitore wird angezeigt und zeigt die derzeit konfigurierten Monitore an.

2. Um einen vorhandenen Monitor zu ändern, klicken Sie in der Liste auf den Monitornamen.
3. Um einen Monitor hinzuzufügen, klicken Sie auf **+ Monitor**.

Wenn Sie einen neuen Monitor hinzufügen, werden Sie aufgefordert, einen Metric Monitor oder einen Protokollmonitor zu erstellen.

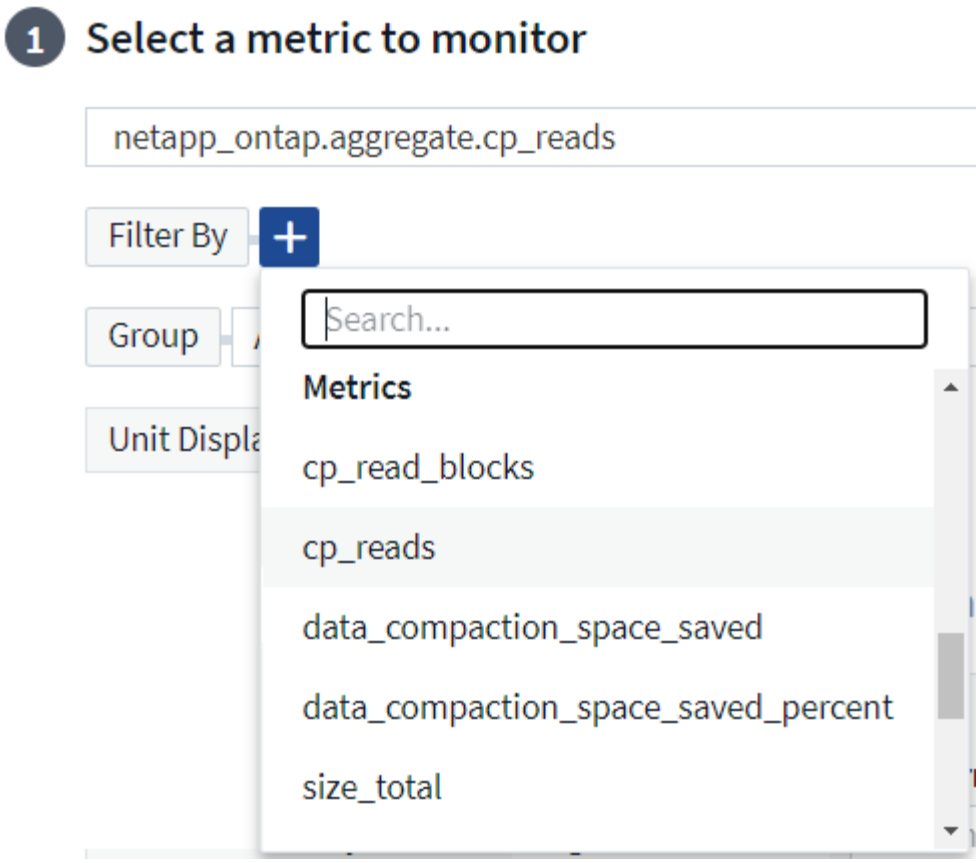
- *Metric* überwacht Warnmeldungen zu Infrastruktur- oder Performance-bezogenen Triggern
- *Log* überwacht die Warnung bei protokollbezogenen Aktivitäten

Nachdem Sie den Monitortyp ausgewählt haben, wird das Dialogfeld Monitorkonfiguration angezeigt. Die Konfiguration hängt davon ab, welche Art von Monitor Sie erstellen.

Metrischer Monitor

1. Suchen Sie im Dropdown-Menü nach einem Objekttyp und einer Metrik, die überwacht werden soll, und wählen Sie diesen aus.

Filter können eingesetzt werden, um festzulegen, welche Objektattribute oder Metriken überwacht werden sollen.



Beim Arbeiten mit Integrationsdaten (Kubernetes, erweiterte ONTAP Daten usw.) werden durch Metrikfilterung die einzelnen/nicht Punkte der aufgezeichneten Datenreihe entfernt, im Gegensatz zu Infrastrukturdaten (Storage, VM, Ports usw.). Dort arbeiten Filter am aggregierten Wert der Datenserie und entfernen das gesamte Objekt aus dem Diagramm.

Um einen Monitor mit mehreren Bedingungen zu erstellen (z. B. IOPS > X und Latenz > Y), definieren Sie die erste Bedingung als Schwellenwert und die zweite Bedingung als Filter.

Definieren Sie die Bedingungen des Monitors.

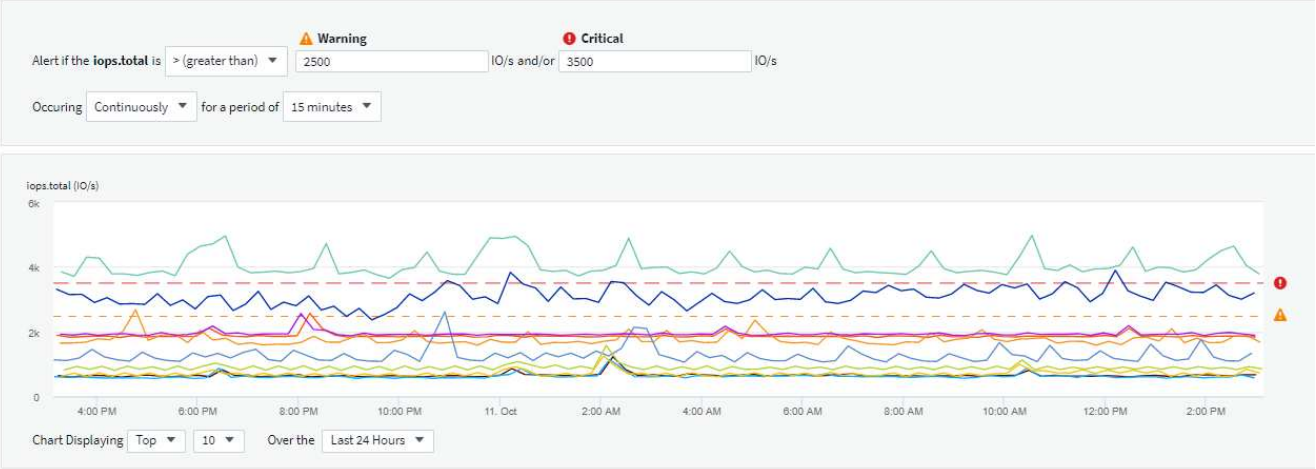
1. Nachdem Sie das zu überwachende Objekt und die Kennzahl ausgewählt haben, legen Sie die Schwellenwerte für Warnstufe und/oder kritische Stufe fest.
2. Geben Sie für die Stufe *Warnung* 200 für unser Beispiel ein. Die gestrichelte Linie, die diese Warnstufe angibt, wird im Beispieldiagramm angezeigt.
3. Geben Sie für die Stufe *Critical* 400 ein. Die gestrichelte Linie, die diesen kritischen Level angibt, wird im Beispieldiagramm angezeigt.

   Im Diagramm werden Verlaufsdaten angezeigt. Die Zeilen Warnung und kritische Ebene im Diagramm sind eine visuelle Darstellung des Monitors, sodass Sie leicht sehen können, wann der Monitor in jedem Fall eine Warnmeldung auslöst.

4. Wählen Sie für das Auftreten des Intervalls *kontinuierlich* für einen Zeitraum von *15 Minuten* aus.

   Sie können eine Warnung auslösen, sobald ein Schwellenwert überschritten wird, oder warten, bis der Schwellenwert für einen bestimmten Zeitraum kontinuierlich verletzt wurde. In unserem Beispiel möchten wir nicht jedes Mal benachrichtigt werden, wenn die IOPS-Punkte insgesamt über dem Warnungs- oder kritischen Level liegen, sondern nur, wenn ein überwachtes Objekt mindestens 15 Minuten lang einen

dieser Werte überschreitet.



Definieren Sie das Verhalten für die Alarmauflösung

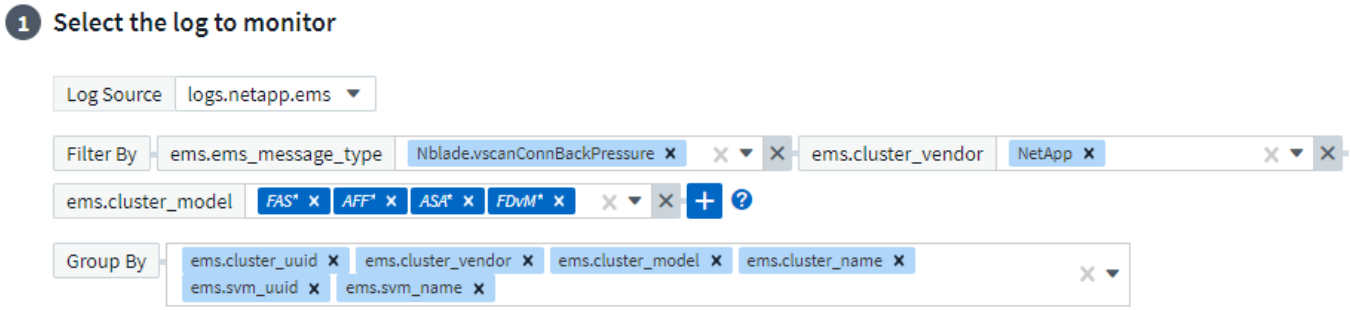
Sie können festlegen, wie eine Kennzahlüberwachung behoben werden soll. Ihnen stehen zwei Möglichkeiten zur Verfügung:

- Beheben Sie, wenn die Metrik wieder in den zulässigen Bereich zurückkehrt.
- Beheben Sie, wenn die Kennzahl für einen bestimmten Zeitraum innerhalb des zulässigen Bereichs liegt, von 1 Minute bis 7 Tage.

Protokollüberwachung

Beim Erstellen eines **Protokollmonitors** wählen Sie zunächst aus der verfügbaren Protokollliste aus, welches Protokoll überwacht werden soll. Sie können dann nach den verfügbaren Attributen wie oben filtern. Sie können auch ein oder mehrere Attribute „Gruppieren nach“ auswählen.

Der Filter Protokollmonitor darf nicht leer sein.



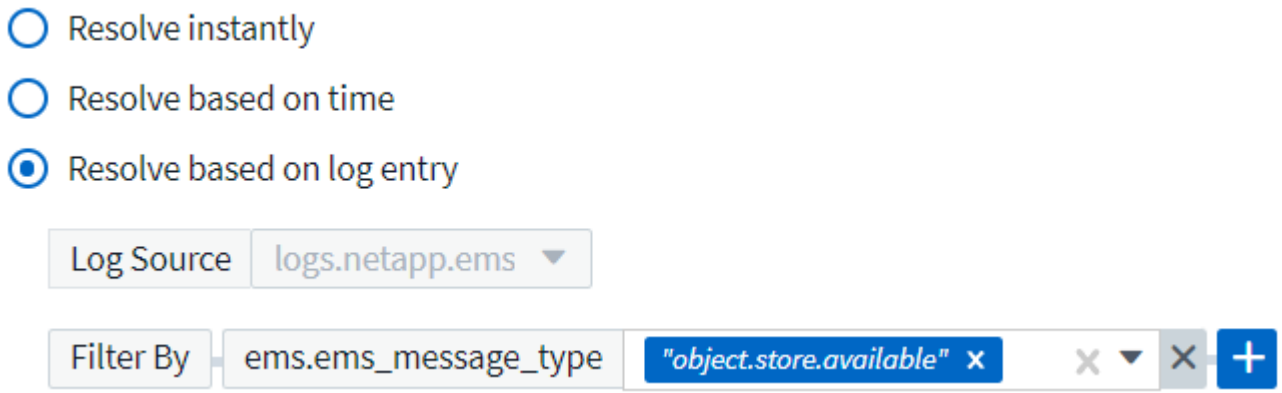
Definieren Sie das Alarmverhalten

Sie können den Monitor so erstellen, dass er mit dem Schweregrad „*kritisch*“, „*Warnung*“ oder „*informationell*“ benachrichtigt wird, wenn die oben definierten Bedingungen einmal (d. h. sofort) auftreten, oder warten, bis die Bedingungen mindestens 2 Mal auftreten.

Definieren Sie das Verhalten für die Alarmauflösung

Sie können festlegen, wie eine Protokollüberwachung behoben werden soll. Sie erhalten drei Möglichkeiten:

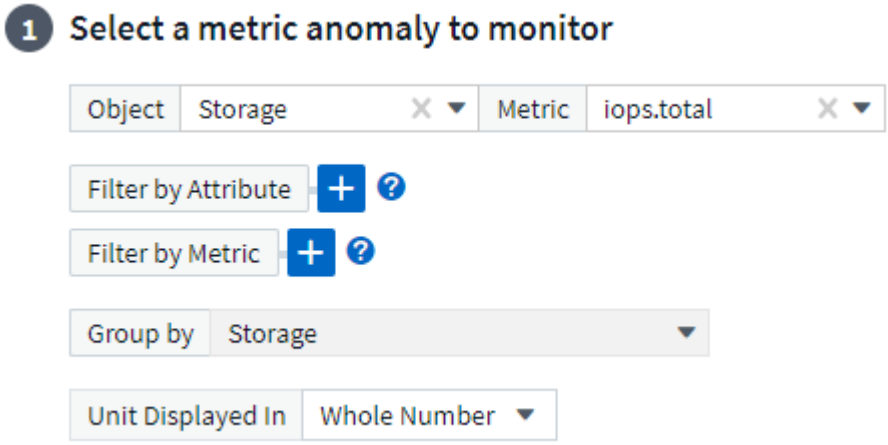
- **Sofort beheben**: Der Alarm wird sofort behoben, ohne dass weitere Maßnahmen erforderlich sind
- **Auflösung basierend auf Zeit**: Der Alarm wird nach Ablauf der angegebenen Zeit gelöst
- **Auflösung basierend auf Protokolleintrag**: Der Alarm wird aufgelöst, wenn eine nachfolgende Log-Aktivität stattgefunden hat. Beispiel: Wenn ein Objekt als „verfügbar“ protokolliert wird.



Überwachung Der Anomalieerkennung

1. Suchen Sie im Dropdown-Menü nach einem Objekttyp und einer Metrik, die überwacht werden soll, und wählen Sie diesen aus.

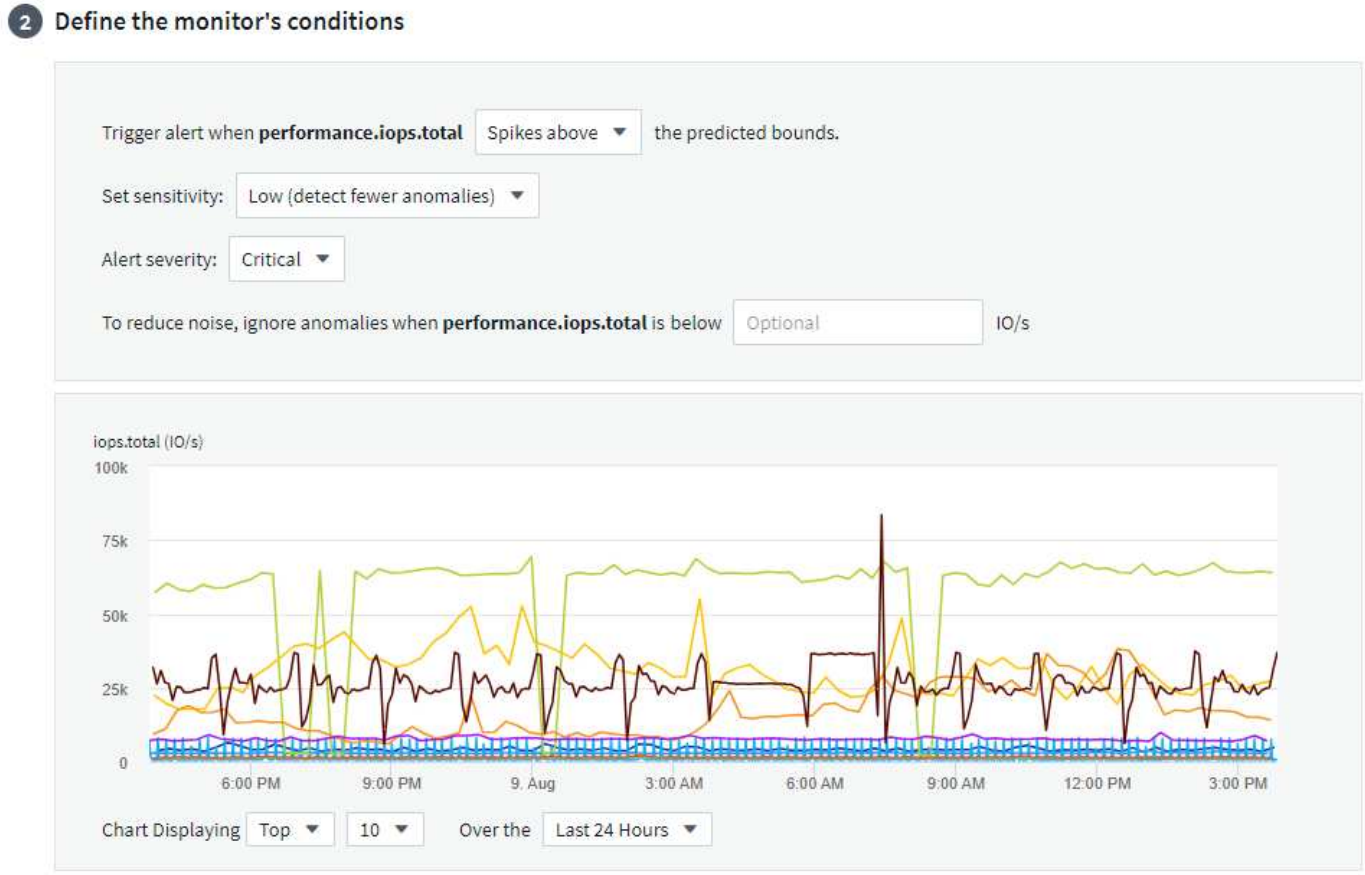
Filter können eingesetzt werden, um festzulegen, welche Objektattribute oder Metriken überwacht werden sollen.



Definieren Sie die Bedingungen des Monitors.

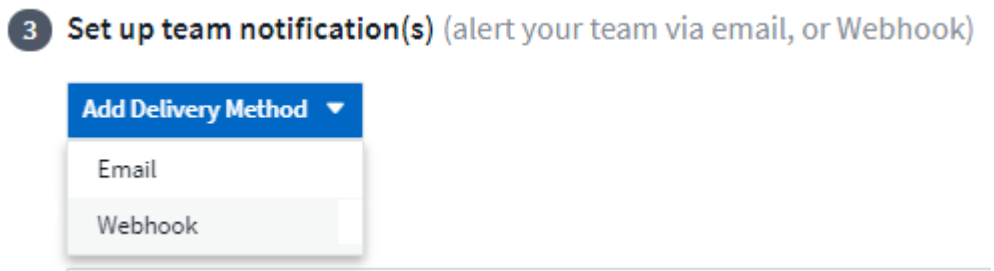
1. Nachdem Sie das zu überwachende Objekt und die zu überwachende Metrik ausgewählt haben, legen Sie die Bedingungen fest, unter denen eine Anomalie erkannt wird.
    - Wählen Sie aus, ob eine Anomalie erkannt werden soll, wenn die gewählte Metrik **über** die vorhergesagten Grenzen spikt, **unter** diese Grenzen fällt oder **Spikes über oder unter** die Grenzen fällt.

- Stellen Sie die **Empfindlichkeit** der Erkennung ein. **Niedrig** (weniger Anomalien werden entfernt), **Mittel** oder **hoch** (es werden mehr Anomalien entdeckt).
- Stellen Sie die Alarme auf verdorren **Warnung** oder **kritisch** ein.
- Bei Bedarf können Sie das Rauschen reduzieren und Anomalien ignorieren, wenn die gewählte Metrik unter einem von Ihnen festgelegten Schwellenwert liegt.



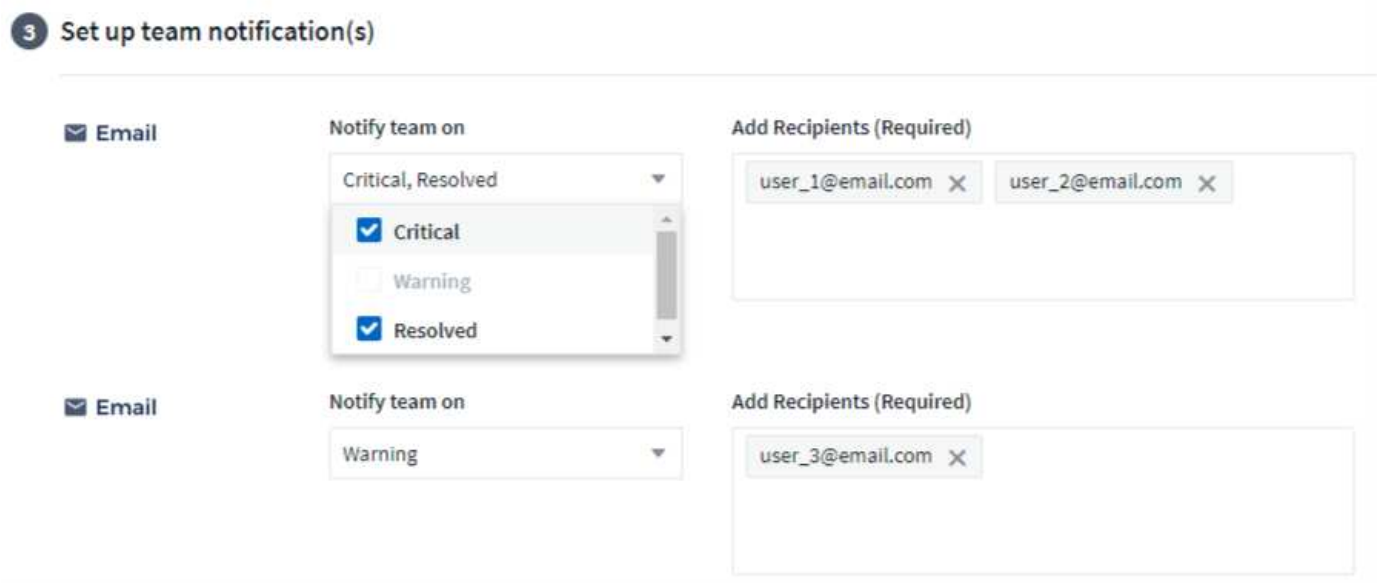
Wählen Sie Benachrichtigungstyp und Empfänger aus

Im Abschnitt „ Team Notification(s)_ einrichten“ können Sie auswählen, ob Sie Ihr Team per E-Mail oder Webhook benachrichtigen möchten.



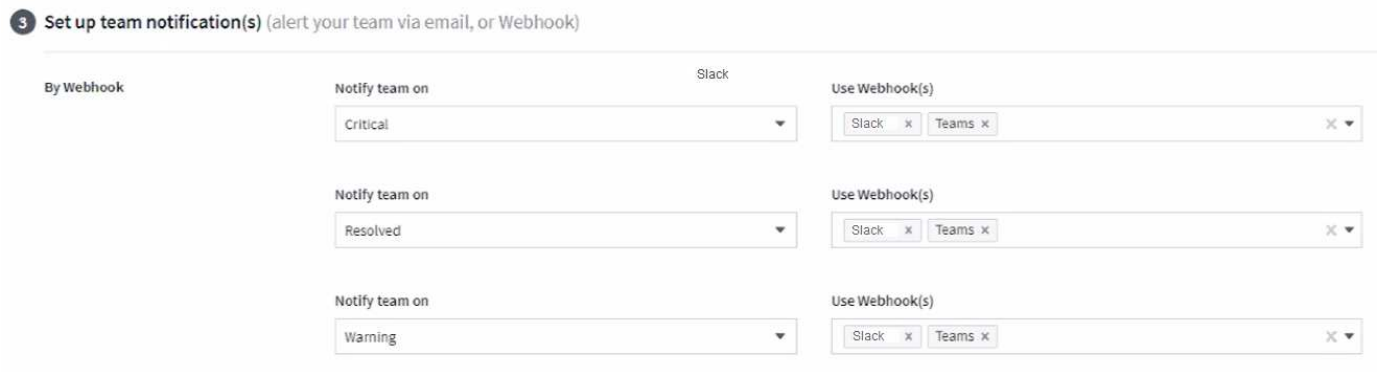
Alerting via Email:

Geben Sie die E-Mail-Empfänger für Benachrichtigungen an. Bei Bedarf können Sie verschiedene Empfänger für Warnungen oder kritische Warnungen auswählen.



Alerting via Webhook:

Legen Sie die Webhook(s) für Benachrichtigungen für Warnmeldungen fest. Bei Bedarf können Sie verschiedene Webhooks für Warnung oder kritische Alarme auswählen.



ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen zur Datenerfassung vorhanden sind, werden die von Monitor erzeugten Warnmeldungen an bestimmte Überwachungsempfänger gesendet.

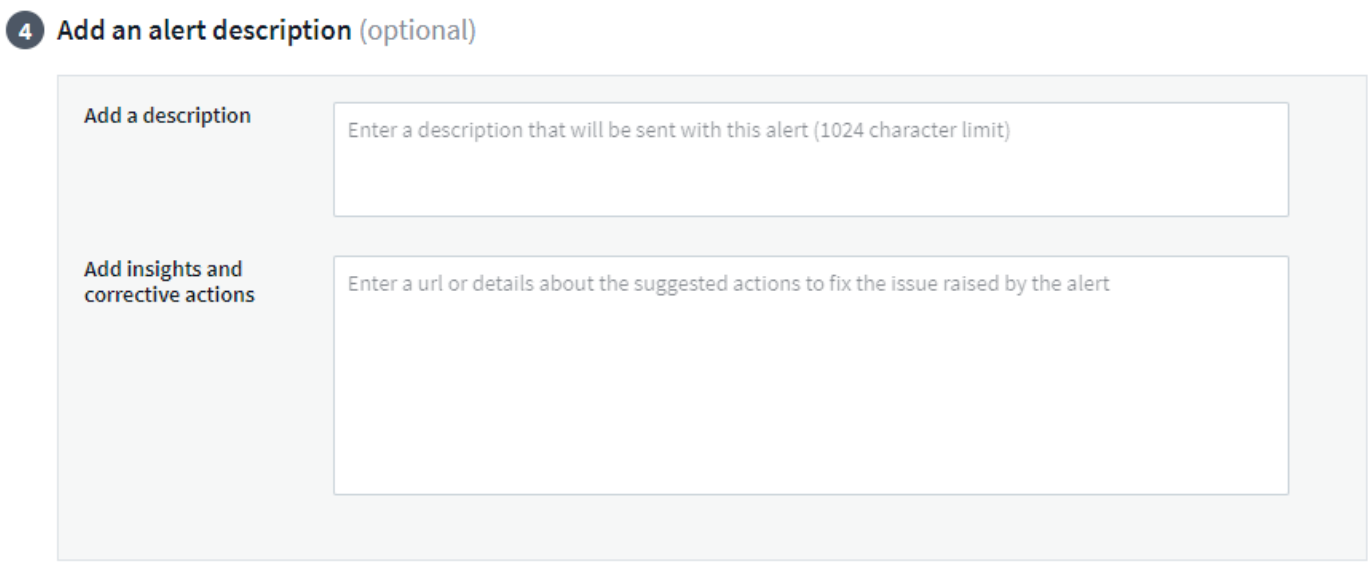
Einstellen von Korrekturmaßnahmen oder zusätzlichen Informationen

Sie können eine optionale Beschreibung sowie zusätzliche Erkenntnisse und/oder Korrekturmaßnahmen hinzufügen, indem Sie den Abschnitt **Alarm hinzufügen Beschreibung** ausfüllen. Die Beschreibung kann bis zu 1024 Zeichen lang sein und wird mit der Warnmeldung gesendet. Das Feld „Insights/Korrekturmaßnahmen“ kann bis zu 67,000 Zeichen lang sein und wird im Übersichtsbereich der Landing Page für die Warnmeldung angezeigt.

In diesen Feldern können Sie Hinweise, Links oder Schritte angeben, die Sie zur Korrektur oder anderweitigen Adresse der Warnmeldung ergreifen können.

Sie können ein beliebiges Objektattribut (z. B. Speichername) als Parameter zu einer Warnmeldungsbeschreibung hinzufügen. Beispielsweise können Sie Parameter für den Volume-Namen und

den Speichernamen in einer Beschreibung wie „hohe Latenz für Volume: *%%relatedObject.volume.name%%*, Storage: *%%relatedObject.storage.name%%*"“ festlegen.



Speichern Sie den Monitor

1. Auf Wunsch können Sie eine Beschreibung des Monitors hinzufügen.
2. Geben Sie dem Monitor einen aussagekräftigen Namen und klicken Sie auf **Speichern**.

   Ihr neuer Monitor wird zur Liste der aktiven Monitore hinzugefügt.

Monitorliste

Auf der Seite „Monitor“ werden die derzeit konfigurierten Monitore angezeigt, die Folgendes anzeigen:

- Monitorname
- Status
- Objekt/Metrik, die überwacht wird
- Bedingungen des Monitors

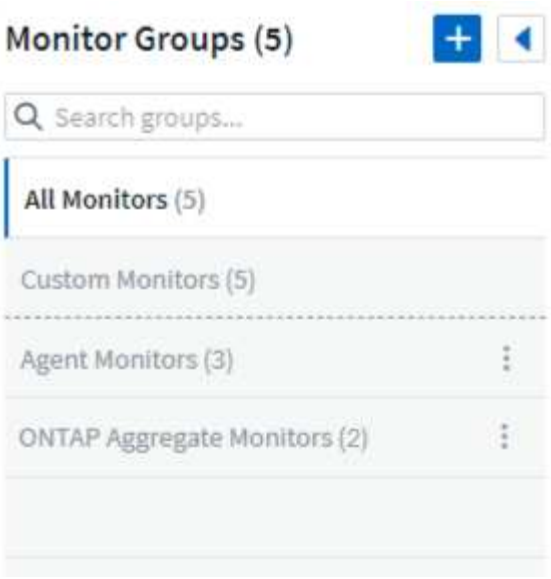
Sie können die Überwachung eines Objekttyps vorübergehend anhalten, indem Sie auf das Menü rechts neben dem Monitor klicken und **Pause** wählen. Wenn Sie bereit sind, die Überwachung fortzusetzen, klicken Sie auf **Fortsetzen**.

Sie können einen Monitor kopieren, indem Sie im Menü * Duplizieren* wählen. Anschließend können Sie den neuen Monitor ändern und das Objekt/die Metrik, den Filter, die Bedingungen, E-Mail-Empfänger usw. ändern

Wenn ein Monitor nicht mehr benötigt wird, können Sie ihn löschen, indem Sie im Menü **Löschen** wählen.

Gruppen Überwachen

Durch Gruppierung können Sie zugehörige Monitore anzeigen und verwalten. Sie können beispielsweise eine Überwachungsgruppe für den Speicher Ihres Mandanten festlegen oder für eine bestimmte Empfängerliste relevante Überwachungsgruppen überwachen.



Die folgenden Monitorgruppen werden angezeigt. Neben dem Gruppennamen wird die Anzahl der in einer Gruppe enthaltenen Monitore angezeigt.

- * Alle Monitore* listet alle Monitore auf.
- **Benutzerdefinierte Monitore** listet alle vom Benutzer erstellten Monitore auf.
- **Suspended Monitors** listet alle Systemmonitore auf, die von Data Infrastructure Insights ausgesetzt wurden.
- Data Infrastructure Insights zeigt auch eine Reihe von **Systemüberwachungsgruppen**, die eine oder mehrere Gruppen von auflisten"Systemdefinierte Monitore", einschließlich ONTAP Infrastruktur und Workload-Monitore.

Benutzerdefinierte Monitore können angehalten, fortgesetzt, gelöscht oder in eine andere Gruppe verschoben werden. Systemdefinierte Monitore können angehalten und fortgesetzt werden, können aber nicht gelöscht oder verschoben werden.

Suspendierte Monitore

Diese Gruppe wird nur angezeigt, wenn Data Infrastructure Insights einen oder mehrere Monitore ausgesetzt hat. Ein Monitor kann ausgesetzt werden, wenn er übermäßige oder kontinuierliche Alarme erzeugt. Wenn es sich bei dem Monitor um einen benutzerdefinierten Monitor handelt, ändern Sie die Bedingungen, um eine kontinuierliche Warnung zu verhindern, und setzen Sie den Monitor dann fort. Der Monitor wird aus der Gruppe der suspendierten Monitore entfernt, wenn das Problem, das die Aussetzung verursacht, behoben wird.

Systemdefinierte Monitore

In diesen Gruppen werden Monitore angezeigt, die von Data Infrastructure Insights bereitgestellt werden, sofern Ihre Umgebung die Geräte und/oder die Protokollverfügbarkeit enthält, die von den Monitoren benötigt werden.

Systemdefinierte Monitore können nicht geändert, in eine andere Gruppe verschoben oder gelöscht werden. Sie können jedoch ein Systemmonitor duplizieren und das Duplikat ändern oder verschieben.

Systemmonitore können auch Monitoring für ONTAP-Infrastruktur (Storage, Volume usw.) oder Workloads (Protokollmonitore) oder andere Gruppen umfassen. NetApp prüft die Anforderungen und Produktfunktionen von Kunden fortlaufend. Zudem werden Systemmonitore und -Gruppen nach Bedarf aktualisiert oder ergänzt.

Benutzerdefinierte Monitorgruppen

Sie können Ihre eigenen Gruppen erstellen, die Monitore auf der Grundlage Ihrer Anforderungen enthalten. Sie möchten beispielsweise eine Gruppe für alle speicherbezogenen Monitore.

Um eine neue benutzerdefinierte Monitorgruppe zu erstellen, klicken Sie auf die Schaltfläche **"+" Neue Monitorgruppe erstellen**. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **Gruppe erstellen**. Eine leere Gruppe mit diesem Namen wird erstellt.

Um Monitore zur Gruppe hinzuzufügen, gehen Sie zur Gruppe *Alle Monitore* (empfohlen) und führen Sie einen der folgenden Schritte aus:

- Um einen einzelnen Monitor hinzuzufügen, klicken Sie auf das Menü rechts neben dem Monitor und wählen Sie *zu Gruppe hinzufügen*. Wählen Sie die Gruppe aus, der der Monitor hinzugefügt werden soll.
- Klicken Sie auf den Monitornamen, um die Bearbeitungsansicht des Monitors zu öffnen, und wählen Sie im Abschnitt „_mit einer Monitorgruppe verknüpfen“ eine Gruppe aus.

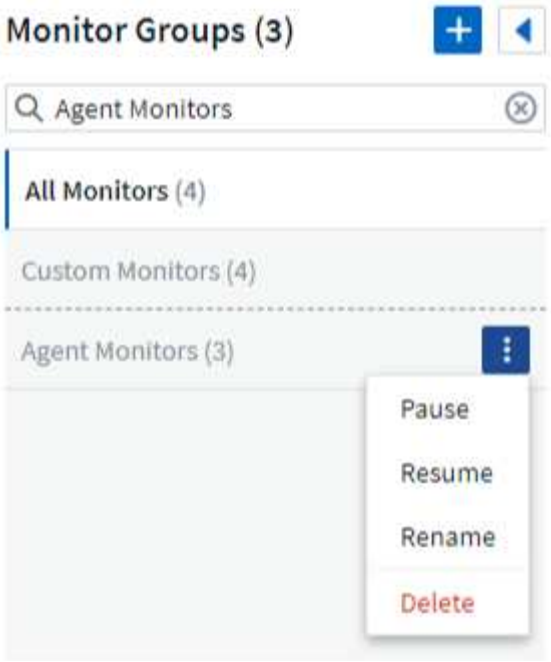
Entfernen Sie Monitore, indem Sie auf eine Gruppe klicken und im Menü *aus Gruppe* entfernen auswählen. Sie können keine Monitore aus der Gruppe „*Alle Monitore*“ oder „ Benutzerdefinierte Monitore_“ entfernen. Um einen Monitor aus diesen Gruppen zu löschen, müssen Sie den Monitor selbst löschen.

Durch das Entfernen eines Monitors aus einer Gruppe wird der Monitor nicht aus Data Infrastructure Insights gelöscht. Um einen Monitor vollständig zu entfernen, wählen Sie den Monitor aus, und klicken Sie auf *Löschen*. Dadurch wird sie auch aus der Gruppe entfernt, zu der sie gehört hat und für keinen Benutzer mehr verfügbar ist.

Sie können einen Monitor auf dieselbe Weise in eine andere Gruppe verschieben und dabei *zu Gruppe* verschieben.

Um alle Monitore in einer Gruppe gleichzeitig anzuhalten oder wieder aufzunehmen, wählen Sie das Menü für die Gruppe aus und klicken Sie auf *Pause* oder *Fortsetzen*.

Verwenden Sie dasselbe Menü, um eine Gruppe umzubenennen oder zu löschen. Beim Löschen einer Gruppe werden die Monitore nicht aus Data Infrastructure Insights gelöscht, sondern sind weiterhin in *Alle Monitore* verfügbar.



Systemdefinierte Monitore

Data Infrastructure Insights umfasst eine Reihe von systemdefinierten Monitoring-Funktionen für Kennzahlen und Protokolle. Die verfügbaren Systemmonitore hängen von den Datensammlern ab, die auf Ihrem Mandanten vorhanden sind. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Auf der "Systemdefinierte Monitore" Seite finden Sie Beschreibungen der in Data Infrastructure Insights enthaltenen Monitore.

Weitere Informationen

- "Anzeigen und Fehlstellen von Warnungen"

Anzeigen und Verwalten von Warnmeldungen von Monitoren

Data Infrastructure Insights zeigt Warnmeldungen an, wenn "Überwachte Schwellenwerte" diese überschritten werden.

Monitore und Alarmfunktionen sind ab Data Infrastructure Insights Standard Edition verfügbar.

Anzeigen und Verwalten von Warnungen

Gehen Sie wie folgt vor, um Meldungen anzuzeigen und zu verwalten.

1. Navigieren Sie zur Seite **Alerts > All Alerts**.
2. Eine Liste der letzten 1,000 Meldungen wird angezeigt. Sie können diese Liste in einem beliebigen Feld sortieren, indem Sie auf die Spaltenüberschrift für das Feld klicken. In der Liste werden die folgenden Informationen angezeigt. Beachten Sie, dass standardmäßig nicht alle dieser Spalten angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnradsymbol klicken:

- **Alarm-ID**: Vom System generierte eindeutige Alarm-ID
- **Auslösezeit**: Der Zeitpunkt, zu dem der betreffende Monitor den Alarm ausgelöst hat
- **Aktueller Schweregrad** (Registerkarte Aktive Warnmeldungen): Der aktuelle Schweregrad der aktiven Warnmeldung
- **Oberer Schweregrad** (Registerkarte „Erledigte Warnmeldungen“); der maximale Schweregrad der Warnmeldung, bevor sie behoben wurde
- **Monitor**: Der Monitor ist so konfiguriert, dass der Alarm ausgelöst wird
- **Ausgelöst an**: Das Objekt, auf dem die überwachte Schwelle überschritten wurde
- **Status**: Aktueller Alarmstatus, *Neu* oder *in Prozess*
- **Aktiver Status**: *Aktiv* oder *aufgelöst*
- **Bedingung**: Die Schwellwertbedingung, die die Warnung ausgelöst hat
- **Metrisch**: Die Objektmetrik, auf der der überwachte Schwellenwert überschritten wurde
- **Überwachungsstatus**: Aktueller Status des Monitors, der die Warnung ausgelöst hat
- **Hat Korrekturmaßnahmen**: Der Alarm hat Korrekturmaßnahmen vorgeschlagen. Öffnen Sie die Alarmseite, um diese anzuzeigen.

Sie können eine Warnmeldung verwalten, indem Sie auf das Menü rechts neben der Warnmeldung klicken und eine der folgenden Optionen auswählen:

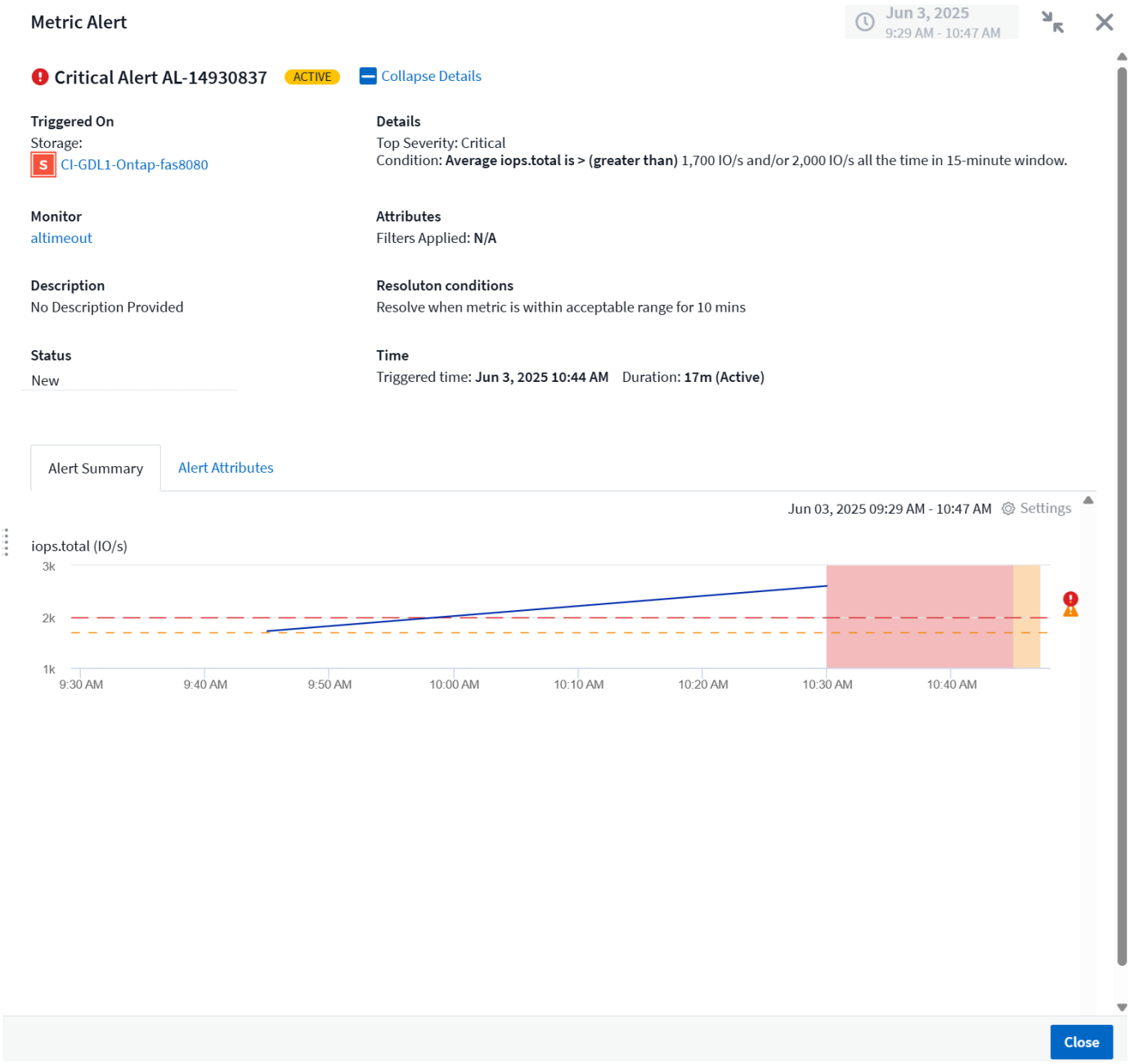
- **In Bearbeitung** um anzuzeigen, dass der Alarm untersucht wird oder anderweitig offen gehalten werden muss
- **Abweisen**, um die Warnung aus der Liste der aktiven Warnungen zu entfernen.

Sie können mehrere Warnungen verwalten, indem Sie das Kontrollkästchen links neben jeder Warnung aktivieren und auf „*Ausgewählte Warnungen ändern Status*“ klicken.

Wenn Sie auf eine Alarm-ID klicken, wird die Seite mit den Alarmdetails geöffnet.

Alarmdetailbereich

Wählen Sie eine beliebige Alarmzeile aus, um das Detailfenster des Alarms zu öffnen. Das Detailfenster bietet zusätzliche Informationen zum Alarm, darunter eine Zusammenfassung, eine Expertenansicht mit Diagrammen zu den Objektdaten, alle zugehörigen Assets und Kommentare der Alarmermittler.



Benachrichtigt, Wenn Daten Fehlen

In einem Echtzeit-System wie Data Infrastructure Insights, um die Analyse eines Monitors auszulösen, um zu entscheiden, ob ein Alarm generiert werden soll, setzen wir auf eines von zwei Dingen:

- Der nächste Datenpunkt zu kommen
- Ein Timer zum Feuer, wenn es keinen Datenpunkt gibt und Sie lange genug gewartet haben

Wie bei langsamen Dateneintreffen – oder gar keinem Dateneintreffen – muss der Timer-Mechanismus übernommen werden, da die Dateneingangsrate nicht ausreicht, um Warnungen in „Echtzeit“ auszulösen. Daher lautet die Frage in der Regel „wie lange warte ich, bevor ich das Analysefenster schließe und sehe, was ich habe?“ Wenn Sie zu lange warten, generieren Sie die Warnungen nicht schnell genug, um nützlich zu sein.

Wenn Sie einen Monitor mit einem 30-Minuten-Fenster haben, das bemerkt, dass eine Bedingung durch den letzten Datenpunkt vor einem langfristigen Datenverlust verletzt wird, Es wird eine Warnung generiert, da der

Monitor keine weiteren Informationen erhalten hat, die zur Bestätigung der Wiederherstellung der Metrik verwendet werden müssen, oder dass die Bedingung weiterhin besteht.

„Dauerhaft Aktiv“-Warnungen

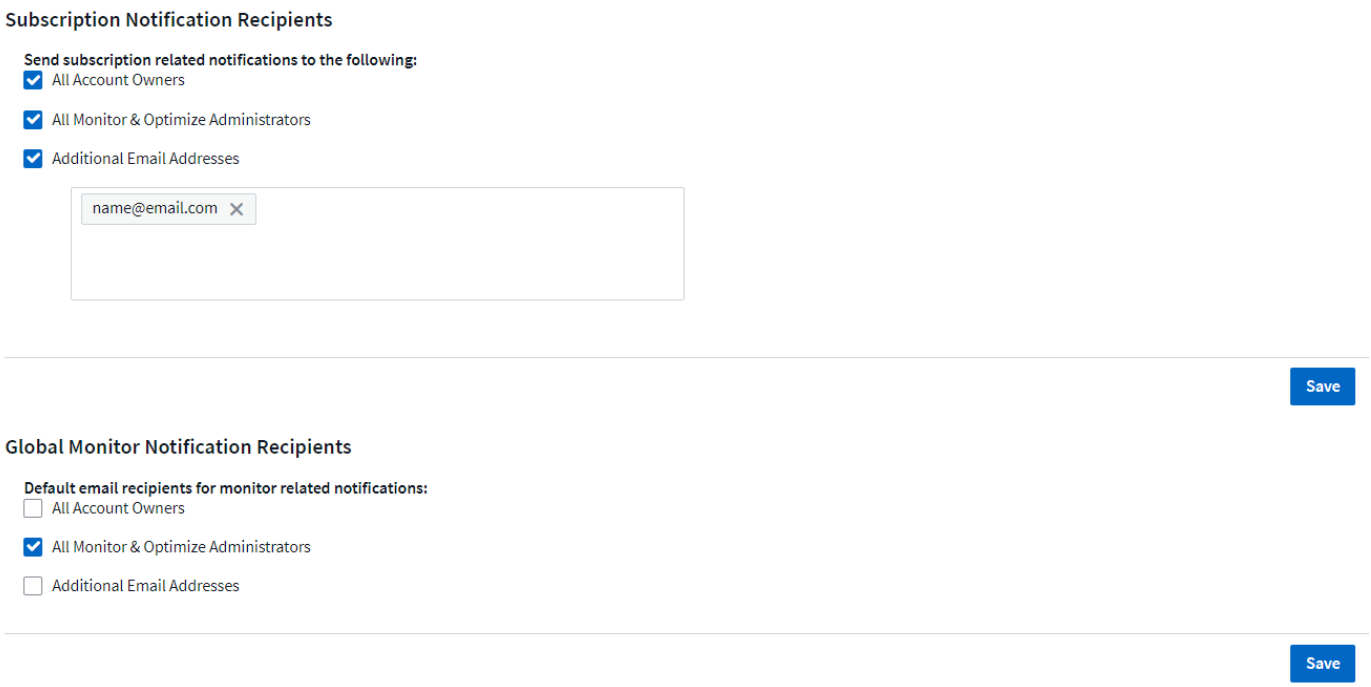
Es ist möglich, einen Monitor so zu konfigurieren, dass die Bedingung **immer** auf dem überwachten Objekt vorhanden ist, z. B. IOPS > 1 oder Latenz > 0. Diese werden oft als „Test“-Monitore erzeugt und dann vergessen. Solche Monitore erzeugen Warnmeldungen, die dauerhaft an den einzelnen Objekten offen bleiben. Dies kann zu Problemen mit der Systemspannung und Stabilität im Laufe der Zeit führen.

Um dies zu verhindern, schließt Data Infrastructure Insights automatisch alle „permanent aktiv“-Warnmeldungen nach 7 Tagen. Beachten Sie, dass die zugrunde liegenden Monitorbedingungen (wahrscheinlich) weiterhin existieren, wodurch fast sofort eine neue Warnung ausgegeben wird, aber durch das Schließen von „immer aktiven“ Warnungen werden einige der sonst auftretenden Systembelastungen verringert.

E-Mail-Benachrichtigungen Werden Konfiguriert

Sie können eine E-Mail-Liste für abonnementbezogene Benachrichtigungen sowie eine globale E-Mail-Liste mit Empfängern für die Benachrichtigung über Schwellenverletzungen für Leistungsrichtlinien konfigurieren.

Um die Einstellungen für Benachrichtigungen-E-Mail-Empfänger zu konfigurieren, gehen Sie zur Seite **Admin > Benachrichtigungen** und wählen Sie die Registerkarte *E-Mail* aus.



Empfänger Für Abonnementbenachrichtigung

Um Empfänger für abonnementbezogene Ereignisbenachrichtigungen zu konfigurieren, gehen Sie zum Abschnitt „Empfänger für Abonnementbenachrichtigungen“. Sie können wählen, dass E-Mail-Benachrichtigungen für abonnierte Ereignisse an einen oder alle der folgenden Empfänger gesendet werden:

- Alle Account-Inhaber
- Alle *Monitor & Optimize* Administratoren
- Zusätzliche E-Mail-Adressen, die Sie angeben

Im Folgenden finden Sie Beispiele für die Art von Benachrichtigungen, die gesendet werden können, und Benutzeraktionen, die Sie durchführen können.

Hinweis:	**Benutzeraktion:**
Testversion oder Abonnement wurde aktualisiert	Lesen Sie die Abonnementdetails auf der "Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab das Abonnement läuft in 30 Tagen ab	Bei Aktivierung von „Automatische Verlängerung“ sind keine Maßnahmen erforderlich. Wenden Sie sich an den NetApp Vertrieb, um das Abonnement zu verlängern
Die Testversion endet in 2 Tagen	Testversion von der Seite erneuern"Abonnement". Sie können eine einmalige Testversion erneuern. Wenden Sie sich an den NetApp Vertrieb, um ein Abonnement zu erwerben
Testversion oder Abonnement abgelaufen Konto wird das Sammeln von Daten in 48 Stunden beendet Konto wird nach 48 Stunden gelöscht	Wenden Sie sich an den NetApp Vertrieb, um ein Abonnement zu erwerben

Um sicherzustellen, dass Ihre Empfänger Benachrichtigungen von Data Infrastructure Insights erhalten, fügen Sie die folgenden E-Mail-Adressen zu beliebigen „Zulassen“-Listen hinzu:

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Globale Empfängerliste für Warnungen

Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an die Benachrichtigungsliste gesendet. Sie können Benachrichtigungen an eine globale Empfängerliste senden.

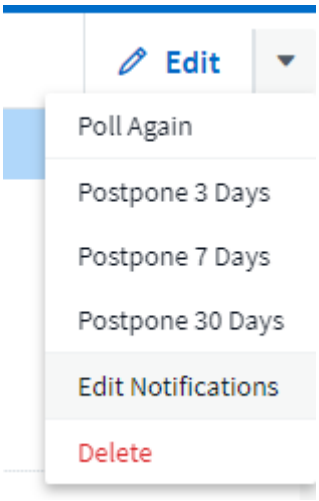
Wählen Sie zum Konfigurieren von Empfängern für globale Warnmeldungen die gewünschten Empfänger im Abschnitt **Empfänger für globale Monitorbenachrichtigungen** aus.

Sie können die globale Empfängerliste für einen einzelnen Monitor immer überschreiben, wenn Sie den Monitor erstellen oder ändern.

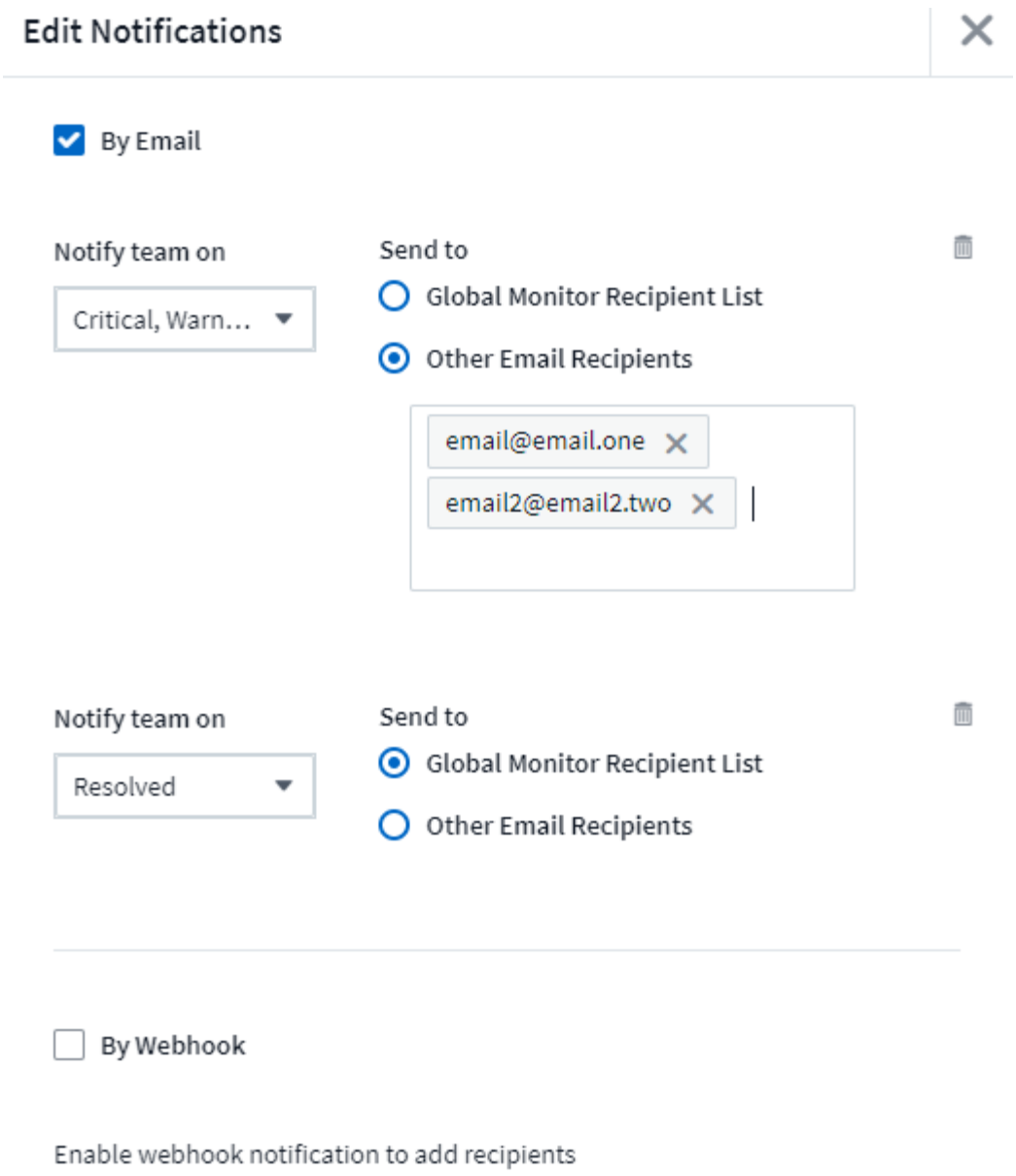
ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen zur Datenerfassung vorhanden sind, werden die von Monitor erzeugten Warnmeldungen an bestimmte Überwachungsempfänger gesendet.

Bearbeiten von Benachrichtigungen für ONTAP

Sie können Benachrichtigungen für ONTAP-Cluster ändern, indem Sie in der oberen rechten Dropdown-Liste auf einer Storage-Landing-Page „_Benachrichtigungen bearbeiten“ auswählen.



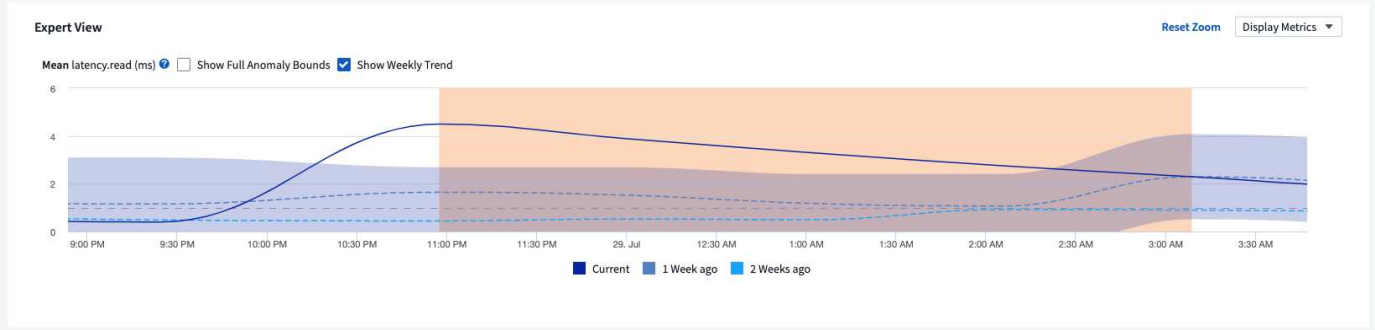
Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder gelöste Warnmeldungen festlegen. Jedes Szenario kann die Liste der globalen Empfänger oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Überwachung Der Anomalieerkennung

Anomalieerkennung bietet Einblicke in unerwartete Änderungen in den Datenmustern auf Ihrem Mandanten. Eine Anomalie tritt auf, wenn sich das Muster des Objektes ändert, z. B. wenn ein Objekt mittwochs zu einer bestimmten Zeit eine bestimmte Latenz erfährt, jedoch am folgenden Mittwoch eine Latenzspitze über diesem Niveau liegt, die dann als Anomalie angesehen würde. Data Infrastructure Insights ermöglicht die Erstellung von Monitoren, die bei solchen Anomalien entsprechende Alarme ausgeben.

Die Anomalieerkennung ist für Objektmetriken geeignet, die ein wiederkehrendes, vorhersehbares Muster aufweisen. Wenn diese Objektkennzahlen über oder unter dem erwarteten Niveau liegen, kann Data Infrastructure Insights eine Warnmeldung zur schnellen Untersuchung generieren.



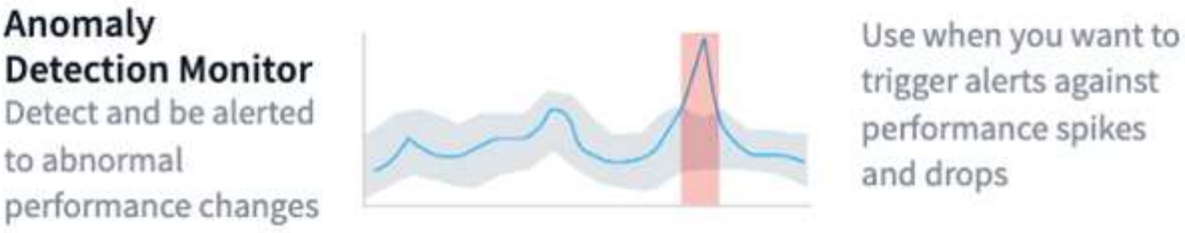
Was ist die Anomaly-Erkennung?

Eine Anomalie tritt auf, wenn der Mittelwert einer Metrik eine Reihe von Standardabweichungen außerhalb des gewichteten Mittelwerts dieser Metrik für die letzten Wochen ist, wobei die letzten Wochen mehr Gewicht als die letzten Wochen haben. Data Infrastructure Insights bietet die Möglichkeit, Daten zu überwachen und bei Anomalien entsprechende Warnmeldungen zu ausgeben. Sie haben die Wahl, die Erkennungsstufen für die „Empfindlichkeit“ einzustellen. Eine höhere Sensitivität wäre beispielsweise dann gegeben, wenn der Mittelwert weniger Standardabweichungen vom Mittelwert ist, wodurch mehr Warnungen generiert werden. Umgekehrt: Niedrigere Empfindlichkeit = mehr Standardabweichungen vom Mittelwert = weniger Alarme.

Die Überwachung der Anomalieerkennung unterscheidet sich von der Schwellenwertüberwachung.

- **Schwellenwertbasierte Überwachung** funktioniert, wenn Sie vordefinierte Schwellenwerte für bestimmte Metriken haben. Mit anderen Worten, wenn Sie ein klares Verständnis davon haben, was erwartet wird (d.h. innerhalb eines normalen Bereichs).

- **Anomaly Detection Monitoring** verwendet Machine Learning Algorithmen, um Ausreißer zu identifizieren, die von der Norm abweichen, wenn die Definition von "normal" nicht klar ist.



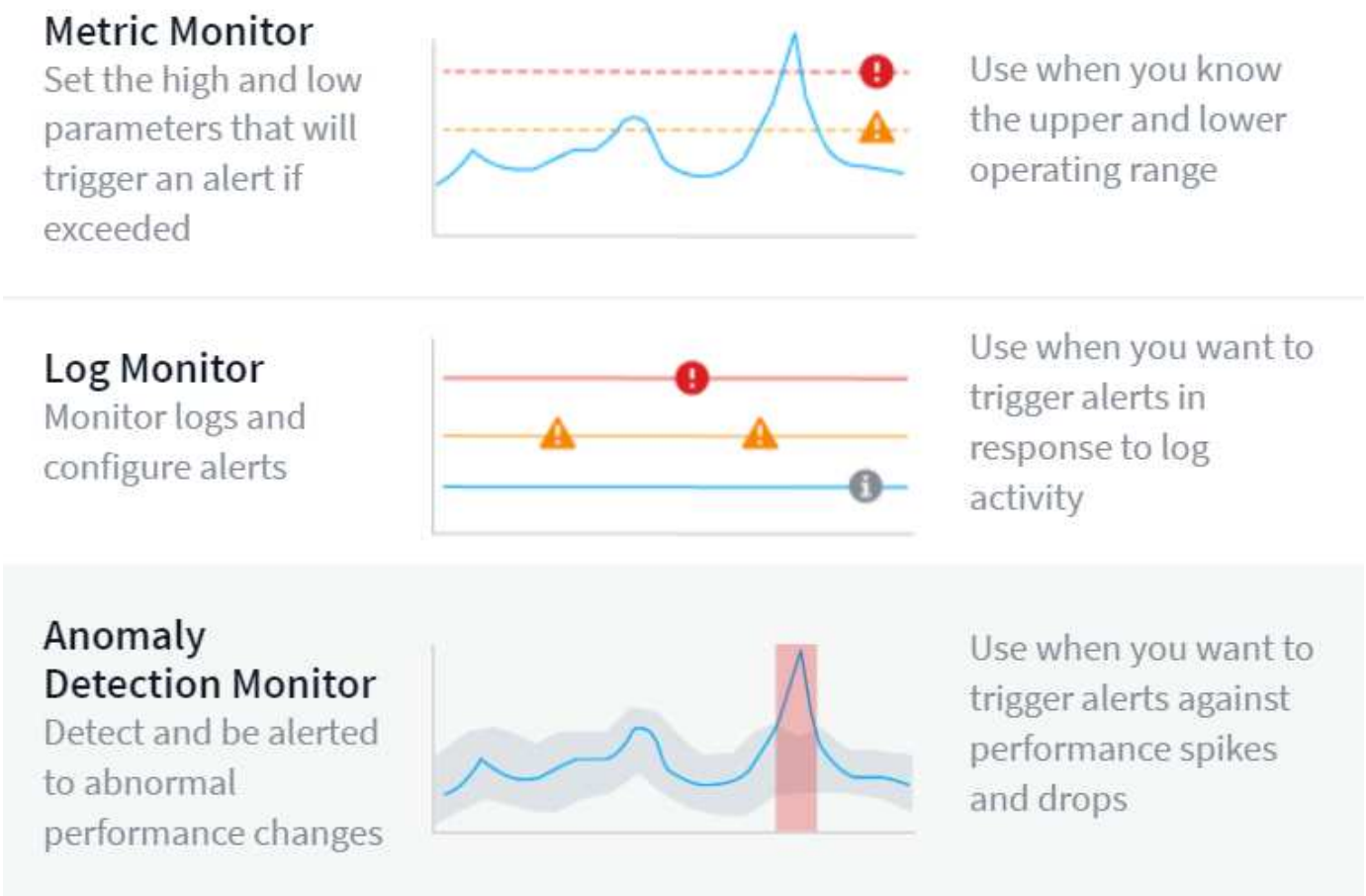
Wann benötige ich die Anomaly Detection?

Das Monitoring der Anomalieerkennung bietet in vielen Situationen hilfreiche Warnmeldungen, darunter:

- Wenn die Definition von *normal* unklar ist. Beispielsweise können SAN-Fehlerraten je nach Port unterschiedlich hoch sein. Die Alarmierung bei einem Fehler ist laut und unnötig, aber eine plötzliche oder signifikante Steigerung kann auf ein weit verbreitetes Problem hinweisen.
- Wo es Veränderungen im Laufe der Zeit gibt. Workloads mit saisonalen Schwankungen (d. h. zu bestimmten Zeiten sind sie beschäftigt oder still). Dies kann unerwartete Ruhezeiten sein, die auf einen Batch-Stillstand hindeuten können.
- Die Arbeit mit großen Datenmengen, bei denen die manuelle Festlegung und Anpassung von Schwellenwerten unpraktisch ist. Beispielsweise ein Mandant mit einer großen Anzahl von Hosts und/oder Volumes mit unterschiedlichen Workloads. Für jeden kann es unterschiedliche SLAs geben. Daher ist es wichtig, diejenigen zu verstehen, die die Norm überschreiten.

Erstellen eines Anomaly Detection Monitors

Um bei Anomalien zu warnen, erstellen Sie einen Monitor, indem Sie zu **Observability > Alerts > +Monitor** navigieren. Wählen Sie *Anomaly Detection Monitor* als Monitortyp.



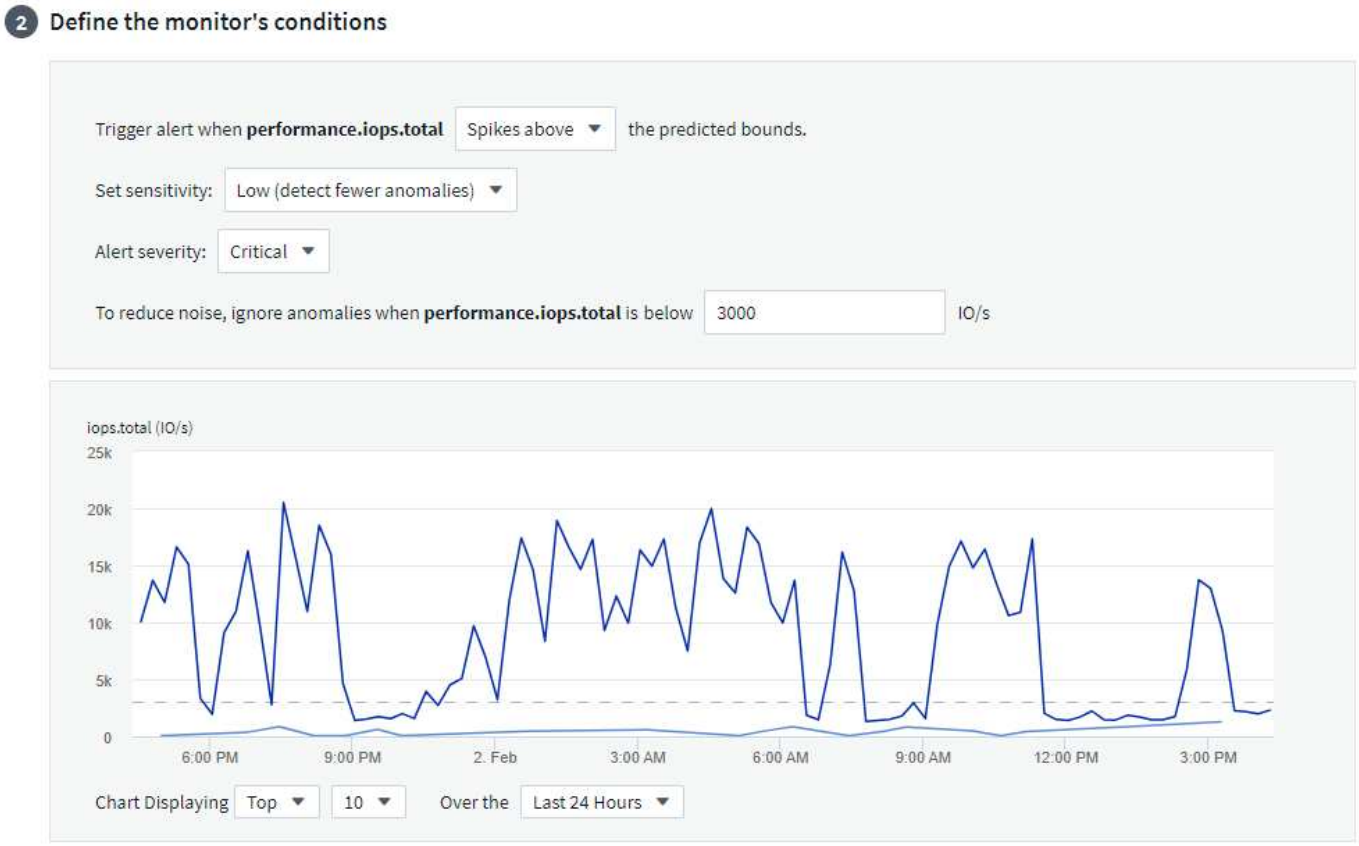
Wählen Sie das Objekt und die Metrik aus, die Sie überwachen möchten. Sie können Filter und Gruppierung wie bei anderen Monitortypen festlegen.

Legen Sie als Nächstes die Bedingungen für den Monitor fest.

- Lösen Sie eine Warnung aus, wenn die ausgewählte Metrik entweder *Spikes über* die vorhergesagten Grenzen, *Drops unter* diese Grenzen oder beides hat.
- Stellen Sie die Empfindlichkeit auf *Medium*, *Low* (weniger Anomalien werden erkannt) oder *High* (es

werden weitere Anomalien erkannt).

- Bestimmen Sie, ob die Alarmstufe „*Critical*“ oder „*Warning*“ ist.
- Legen Sie optional einen Wert fest, unter dem die Anomalien *ignoriert* sind. Dies kann zur Reduzierung von Geräuschen beitragen. Dieser Wert wird als gestrichelte Linie im Beispieldiagramm angezeigt.



Schließlich können Sie eine Bereitstellungsmethode für die Warnungen (E-Mail, Webhook oder beides) konfigurieren, dem Monitor eine optionale Beschreibung oder Korrekturmaßnahmen geben und den Monitor bei Bedarf einer benutzerdefinierten Gruppe hinzufügen.

Speichern Sie den Monitor mit einem aussagekräftigen Namen, und schon ist alles erledigt.

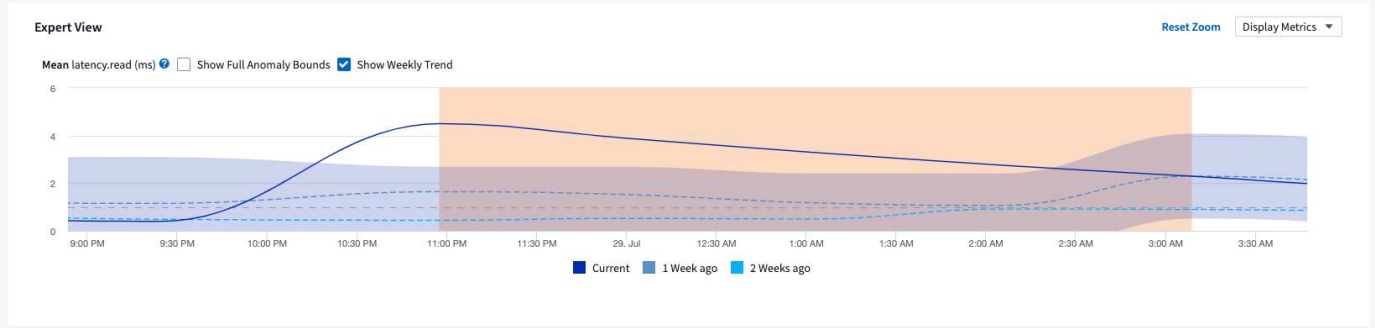
Nach der Erstellung analysiert der Monitor die Daten der Vorwoche, um eine erste Baseline zu erstellen. Die Anomalieerkennung wird genauer, wenn die Zeit vergeht und mehr Geschichte auftritt.

Bei der Erstellung eines Monitors prüft DII alle vorhandenen Daten der Vorwoche auf signifikante Datenspitzen oder -einbrüche; diese gelten als Anomalien. In der ersten Woche nach der Monitorerstellung (der Lernphase) kann es zu verstärktem Rauschen in den Warnmeldungen kommen. Um dieses Rauschen zu minimieren, werden nur Spitzen oder Einbrüche, die länger als 30 Minuten dauern, als Anomalien gewertet und lösen Warnmeldungen aus. Wenn in der darauffolgenden Woche weitere Daten analysiert werden, nimmt das Rauschen normalerweise ab und ein signifikanter Anstieg oder Abfall, der länger anhält, wird als Anomalie betrachtet.

Anzeigen der Anomalien

Auf einer Landing Page für Warnmeldungen, die ausgelöst werden, wenn Anomalien erkannt werden, wird im Diagramm ein markiertes Band angezeigt, von dem Zeitpunkt, zu dem die Metrik außerhalb der

vorhergesagten Grenzen stachelte, bis zu dem Zeitpunkt, zu dem sie sich innerhalb dieser Grenzen zurückbewegte.



Beim Anzeigen eines Anomaliediagramms auf einer Landing Page für Warnmeldungen können Sie die folgenden Optionen auswählen:

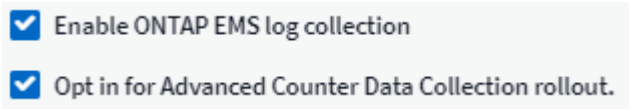
- Wöchentlicher Trend: vergleichen sie die Werte mit der gleichen Zeit, am gleichen Tag in den Vorwochen, für bis zu 5 vorherige Wochen.
- Vollständige Anomaly-Grenzen: Standardmäßig konzentriert sich die Grafik auf den metrischen Wert, damit Sie das metrische Verhalten besser analysieren können. Auswählen, um vollständige Grenzen für Anomalien anzuzeigen (Maximalwert usw.)

Sie können auch Objekte anzeigen, die zu der Anomalie beigetragen haben, indem Sie diese in der Expertenansicht der Landing Page auswählen. Das Diagramm zeigt das Verhalten der ausgewählten Objekte an.

Systemmonitore

Data Infrastructure Insights umfasst eine Reihe von systemdefinierten Monitoring-Funktionen für Kennzahlen und Protokolle. Die verfügbaren Systemmonitore hängen von den Datensammlern ab, die auf Ihrem Mandanten vorhanden sind. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Viele Systemmonitore befinden sich standardmäßig im Status „*Paused*“. Sie können einen Systemmonitor aktivieren, indem Sie die Option „*Fortsetzen*“ für den Monitor auswählen. Stellen Sie sicher, dass *Advanced Counter Data Collection* und *enable ONTAP EMS Log Collection* im Data Collector aktiviert sind. Diese Optionen finden Sie im ONTAP Data Collector unter *Erweiterte Konfiguration*:



inhaltsverzeichnis:[]

Monitorbeschreibungen

Systemdefinierte Monitore bestehen aus vordefinierten Metriken und Bedingungen sowie aus Standardbeschreibungen und Korrekturmaßnahmen, die nicht geändert werden können. Sie können die BenachrichtigungsEmpfängerliste für systemdefinierte Monitore ändern. Um die Metriken, Bedingungen, Beschreibungen und Korrekturmaßnahmen anzuzeigen oder die Empfängerliste zu ändern, öffnen Sie eine systemdefinierte Monitorgruppe, und klicken Sie in der Liste auf den Monitornamen.

Systemdefinierte Monitorgruppen können nicht geändert oder entfernt werden.

Die folgenden systemdefinierten Monitore sind in den genannten Gruppen verfügbar.

- **Die ONTAP-Infrastruktur** umfasst Monitore für Probleme mit der Infrastruktur in ONTAP-Clustern.
- **Beispiele für ONTAP-Workloads** enthält Monitore für Workload-Probleme.
- Monitore in beiden Gruppen sind standardmäßig in den Status *Paused* eingestellt.

Im Folgenden sind die Systemmonitore aufgeführt, die derzeit in Data Infrastructure Insights enthalten sind:

Metrische Monitore

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme

Auslastung Des Fibre Channel Ports Hoch	KRITISCH	Über die Fibre Channel Protocol-Ports wird der SAN-Datenverkehr zwischen dem Host-System des Kunden und den ONTAP-LUNs empfangen und übertragen. Bei hoher Port-Auslastung Dann wird es zu einem Engpass und es wird letztlich die Leistung von sensiblen Fibre-Channel-Protokoll-Workloads beeinträchtigen.…Eine Warnung zeigt an, dass geplante Maßnahmen getroffen werden sollten, um den Netzwerkverkehr auszugleichen.…eine kritische Warnung zeigt an, dass Serviceunterbrechungen unmittelbar bevorstehen und Notfallmaßnahmen ergriffen werden sollten, um das Netzwerk auszugleichen Traffic, um Servicekontinuität zu gewährleisten.	Bei Verstößen gegen kritische Schwellenwerte sind unmittelbare Maßnahmen zur Minimierung von Serviceunterbrechungen zu berücksichtigen: 1. Verschieben Sie Workloads auf einen anderen weniger ausgelasteten FCP-Port. 2. Begrenzen Sie den Verkehr bestimmter LUNs auf wesentliche Arbeit, entweder über QoS-Richtlinien in ONTAP oder Host-seitige Konfiguration, um die Auslastung der FCP-Ports zu erleichtern.… Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Konfigurieren Sie mehr FCP-Ports, um den Datenverkehr zu behandeln, damit die Port-Auslastung auf mehr Ports verteilt wird. 2. Verschieben Sie Workloads auf einen anderen weniger ausgelasteten FCP-Port. 3. Begrenzen Sie den Datenverkehr bestimmter LUNs auf wesentliche Arbeit, entweder mittels QoS-Richtlinien in ONTAP oder Host-seitiger Konfiguration, um die Auslastung der FCP-Ports zu erleichtern.

Lun-Latenz Hoch	KRITISCH	LUNs sind Objekte, die den I/O-Verkehr bedienen, der häufig von Performance-abhängigen Applikationen wie Datenbanken angetrieben wird. Hohe LUN-Latenzen bedeuten, dass Applikationen selbst unter Umständen darunter leiden und ihre Aufgaben nicht ausführen können.…eine Warnmeldung gibt an, dass bestimmte Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Node oder Aggregat zu verschieben.…Eine wichtige Warnmeldung gibt an, dass eine Serviceunterbrechung bevorsteht und Notfallmaßnahmen ergriffen werden sollten Sicherstellen von Servicekontinuität Die folgenden Latenzzeiten sind auf Grundlage des Medientyps zu erwarten – SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden	Bei einer Verletzung kritischer Schwellenwerte sollten Sie die folgenden Maßnahmen zur Minimierung der Serviceunterbrechung erwägen: Wenn der LUN oder ihrem Volume eine QoS-Richtlinie zugeordnet ist, bewerten Sie ihre Schwellenwerte und überprüfen Sie, ob sie die Drosselung des LUN-Workloads verursachen.… Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn zudem ein Node hohe Auslastung erzielt, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den gesamten Workload des Node. 3. Wenn der LUN oder ihrem Volume eine QoS-Richtlinie zugeordnet ist, bewerten Sie ihre Schwellenwerte und überprüfen Sie, ob sie eine Drosselung des LUN-Workloads verursachen.

Auslastung Des Netzwerkports Hoch	KRITISCH	Netzwerkports werden verwendet, um den Protokollverkehr zwischen den Host-Systemen des Kunden und den ONTAP Volumes zu empfangen und zu übertragen. Wenn die Port-Auslastung hoch ist, wird er zu einem Engpass, der letztlich die Performance von NFS beeinträchtigt CIFS- und iSCSI-Workloads.…Eine Warnmeldung gibt an, dass geplante Maßnahmen ergriffen werden sollten, um den Netzwerkverkehr auszugleichen.…ein kritischer Alarm zeigt an, dass Serviceunterbrechungen unmittelbar bevorstehen und Notfallmaßnahmen ergriffen werden sollten, um den Netzwerkverkehr auszugleichen, um die Servicekontinuität zu gewährleisten.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Begrenzen Sie den Datenverkehr bestimmter Volumes nur auf notwendige Aufgaben, entweder über QoS-Richtlinien in ONTAP oder mittels Host-seitiger Analysen, um die Auslastung der Netzwerk-Ports zu verringern. 2. Konfigurieren Sie ein oder mehrere Volumes, um einen anderen weniger ausgelasteten Netzwerkport zu verwenden.… Bei Überschreitung der Warnungsschwelle sollten folgende unmittelbare Maßnahmen berücksichtigt werden: 1. Konfigurieren Sie mehr Netzwerk-Ports, um den Datenverkehr zu verarbeiten, so dass die Port-Auslastung auf mehrere Ports verteilt wird. 2. Konfigurieren Sie ein oder mehrere Volumes, um einen anderen weniger ausgelasteten Netzwerkport zu verwenden.

NVMe Namespace-Latenz hoch	KRITISCH	NVMe Namesaces sind Objekte, die den I/O-Datenverkehr verarbeiten, der von Performance-abhängigen Applikationen wie Datenbanken gesteuert wird. Hohe NVMe Namesaces Latenz bedeutet, dass Applikationen selbst möglicherweise darunter leiden und ihre Aufgaben nicht ausführen können.…eine Warnmeldung gibt an, dass bestimmte geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Node oder Aggregat zu verschieben.…ein wichtiger Alarm zeigt, dass eine Serviceunterbrechung bevorsteht und Notfallmaßnahmen ergriffen werden sollten Für Servicekontinuität sorgen.	Bei Verstößen gegen kritische Schwellenwerte sollten Sie sofortige Maßnahmen zur Minimierung der Serviceunterbrechung in Erwägung ziehen: Wenn Ihnen der NVMe Namespace oder sein Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie seine Grenzschwellenwerte, falls sie eine Drosselung des NVMe-Namespace-Workloads verursachen.… Wenn der Warnungsschwellenwert überschritten wird, sollten die folgenden Maßnahmen ergriffen werden: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn zudem ein Node hohe Auslastung erzielt, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den gesamten Workload des Node. 3. Wenn Ihnen im NVMe Namespace oder seinem Volume eine QoS-Richtlinie zugewiesen wurde, bewerten Sie ihre Schwellenwerte für den Fall, dass der NVMe-Namespace-Workload gedrosselt wird.

Qtree-Kapazität voll	KRITISCH	Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines Volumes vorhanden sein kann. Jeder qtree verfügt über ein Standard-Speicherplatzkontingent oder eine durch eine Kontingentrichtlinie definierte Quote, um die Menge der im Baum gespeicherten Daten innerhalb der Volume-Kapazität zu begrenzen.…Eine Warnmeldung gibt an, dass geplante Maßnahmen zur Erhöhung des Speicherplatzes ergriffen werden sollten.…eine wichtige Warnmeldung gibt an, dass eine Serviceunterbrechung bevorsteht und Es sollten Notfallmaßnahmen ergriffen werden, um Speicherplatz freizugeben, um die Kontinuität der Wartung zu gewährleisten.	Bei Verstößen gegen kritische Schwellenwerte sind unmittelbare Maßnahmen zur Minimierung von Serviceunterbrechungen zu berücksichtigen: 1. Vergrößern Sie den Platz des qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie unerwünschte Daten, um Speicherplatz freizugeben.… Wenn der Warnschwellenwert nicht erreicht wird, sollten folgende Maßnahmen ergriffen werden: 1. Vergrößern Sie den Platz des qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie unerwünschte Daten, um Speicherplatz freizugeben.

Harte Grenze der qtree-Kapazität	KRITISCH	Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines Volumes vorhanden sein kann. Jeder qtree verfügt über eine in KByte gemessene Speicherquote, die zum Speichern von Daten verwendet wird, um das Wachstum der Benutzerdaten im Volumen zu kontrollieren und nicht die gesamte Kapazität zu überschreiten.…Ein qtree hält eine weiche Speicherkapazitätsquote bereit, die dem Anwender proaktiv eine Warnung gibt, bevor die Gesamtsumme erreicht wird Begrenzung der Kapazitätskontingente im qtree und keine Möglichkeit mehr Daten zu speichern Durch das Monitoring der in einem qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Erhöhen Sie die Baumspeicherquote, um dem Wachstum gerecht zu werden 2. Weisen Sie den Benutzer an, unerwünschte Daten im Baum zu löschen, um Speicherplatz freizugeben

Qtree Kapazitätsgrenze	WARNUNG	Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines Volumes vorhanden sein kann. Jeder qtree verfügt über eine in KByte gemessene Speicherquote, die dazu dient, Daten zu speichern, um das Wachstum von Benutzerdaten im Volumen zu steuern und nicht die gesamte Kapazität zu überschreiten.…Ein qtree hält ein weiches Speicherkapazitätskontingent an, das vor Erreichen des proaktiv eine Warnung für den Benutzer gibt Die Gesamtmenge an Kapazitätskontingenten im qtree und die nicht mehr Daten speichern können. Durch das Monitoring der in einem qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Bei Überschreitung der Warnungsschwelle sollten folgende unmittelbare Maßnahmen berücksichtigt werden: 1. Erhöhen Sie die Baumspeicherkontingente , um dem Wachstum gerecht zu werden. 2. Weisen Sie den Benutzer an, unerwünschte Daten in der Baumstruktur zu löschen, um Speicherplatz freizugeben.

Harte Grenze für qtree Dateien	KRITISCH	Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines Volumes vorhanden sein kann. Jeder qtree hat ein Kontingent an der Anzahl der Dateien, die er enthalten kann, um eine einfach zu verwaltende Dateisystemgröße innerhalb des Volumes zu erhalten.…Ein qtree behält eine harte Dateianzahl über das hinaus neue Dateien im Baum verweigert werden. Durch das Monitoring der Dateianzahl innerhalb eines qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Bei Verstößen gegen kritische Schwellenwerte sind unmittelbare Maßnahmen zur Minimierung von Serviceunterbrechungen zu berücksichtigen: 1. Erhöhen Sie das Kontingent der Dateien für den qtree. 2. Löschen Sie unerwünschte Dateien aus dem qtree-Dateisystem.

Qtree Files Soft Limit	WARNUNG	Ein qtree ist ein logisch definiertes File-System, das als spezielles Unterverzeichnis des Root-Verzeichnisses innerhalb eines Volumes vorhanden sein kann. Jeder qtree verfügt über eine Quote der Anzahl der enthaltenen Dateien, um eine einfach zu verwaltende Dateisystemgröße innerhalb des Volumes zu halten.…Ein qtree behält eine weiche Dateianzahl, um dem Benutzer proaktiv eine Warnung zu geben, bevor er die Dateigrenze im qtree erreicht und Keine zusätzlichen Dateien speichern. Durch das Monitoring der Dateianzahl innerhalb eines qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Wenn der Warnschwellenwert nicht erreicht wird, sollten folgende Maßnahmen ergriffen werden: 1. Erhöhen Sie das Kontingent der Dateien für den qtree. 2. Löschen Sie unerwünschte Dateien aus dem qtree-Dateisystem.

Speicherplatz Der Snapshot-Reserve Voll	KRITISCH	Die Storage-Kapazität eines Volumes ist erforderlich, um Applikations- und Kundendaten zu speichern. Ein Teil dieses Speicherplatzes, der als reservierter Snapshot-Speicherplatz bezeichnet wird, wird zum Speichern von Snapshots verwendet, mit denen Daten lokal gesichert werden können. Je mehr neue und aktualisierte Daten in dem ONTAP Volume gespeichert sind, desto mehr Snapshot-Kapazität wird benötigt und weniger Snapshot Storage-Kapazität ist für zukünftige neue oder aktualisierte Daten verfügbar. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reserve-Speicherplatz erreicht, kann dies dazu führen, dass der Kunde nicht in der Lage ist, neue Snapshot-Daten zu speichern und den Schutz der Daten im Volume zu verringern. Durch das Monitoring der verwendeten Snapshot-Kapazität des Volumes wird die Kontinuität der Datendienste gewährleistet.	Bei Verstößen gegen kritische Schwellenwerte sind unmittelbare Maßnahmen zur Minimierung von Serviceunterbrechungen zu berücksichtigen: 1. Konfigurieren Sie Snapshots so, dass der Datenplatz im Volume genutzt wird, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere unerwünschte Snapshots, um Speicherplatz freizugeben.… Wenn der Warnschwellenwert nicht erreicht wird, sollten folgende Maßnahmen ergriffen werden: 1. Erhöhen Sie den Speicherplatz der Snapshot Reserve innerhalb des Volumes, um dem Wachstum gerecht zu werden. 2. Konfigurieren Sie Snapshots so, dass der Datenplatz im Volume genutzt wird, wenn die Snapshot-Reserve voll ist.

Begrenzung Der Storage-Kapazität	KRITISCH	Wenn ein Storage Pool (Aggregat) gefüllt ist, werden I/O-Vorgänge verlangsamt und beenden schließlich das Ergebnis von Störungen bei Storage-Ausfällen. Eine Warnmeldung gibt an, dass geplante Maßnahmen zur Wiederherstellung des minimalen freien Speicherplatzes in Kürze getroffen werden sollten. Eine kritische Warnmeldung zeigt an, dass eine Serviceunterbrechung bevorsteht und Notmaßnahmen ergriffen werden sollten, um Speicherplatz freizugeben, um die Servicekontinuität sicherzustellen.	Bei Verstößen gegen kritische Schwellenwerte sind sofort folgende Maßnahmen zu ergreifen, um die Serviceunterbrechung zu minimieren: 1. Löschen von Snapshots auf nicht kritischen Volumes 2. Löschen Sie Volumes oder LUNs, die keine wesentlichen Workloads darstellen und die aus anderen Storage-Kopien wiederhergestellt werden können.……Wenn ein Warnschwellenwert verletzt wird, planen Sie die folgenden Sofortmaßnahmen ein: 1. Verschieben Sie ein oder mehrere Volumes an einen anderen Storage-Speicherort. 2. Hinzufügen von mehr Storage-Kapazität 3. Ändern Sie Einstellungen zur Storage-Effizienz oder verschieben Sie inaktive Daten in den Cloud-Storage.

Limit Der Storage-Performance	KRITISCH	Wenn ein Storage-System die Performance-Grenzen erreicht, werden Betriebsabläufe verlangsamt, die Latenz steigt und Workloads und Applikationen können ausfallen. ONTAP bewertet die Storage Pool-Auslastung für Workloads und schätzt den Prozentsatz der Performance, die tatsächlich verbraucht wurde.…eine Warnmeldung gibt an, dass Maßnahmen zur Senkung der Storage Pool-Auslastung ergriffen werden sollten, um sicherzustellen, dass genügend Performance für den Storage Pool zur Verfügung steht, um Workload-Spitzen zu bewältigen.…Ein wichtiger Alarm zeigt das Eine mögliche Performance-Konnektivitätsausfälle steht bevor und zur Reduzierung der Storage-Pool-Last sollten Notfallmaßnahmen ergriffen werden, um Service Continuity zu gewährleisten.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Unterbrechen Sie geplante Aufgaben wie Snapshots oder SnapMirror Replizierung. 2. Ungenutzte, nicht wichtige Workloads.… Wenn der Warnungsschwellenwert überschritten wird, ergreifen Sie sofort die folgenden Maßnahmen: 1. Verschieben Sie eine oder mehrere Workloads an einen anderen Storage-Standort. 2. Hinzufügen weiterer Storage Nodes (AFF) oder Festplatten-Shelfs (FAS) und Neuverteilung von Workloads 3 Ändern von Workload-Merkmalen (Blockgröße, Applikations-Caching)

Harte Grenze Der Kapazität Der Benutzerkontingente	KRITISCH	ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte verfügen, auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes zuzugreifen. Daher können Kunden mit ONTAP Storage-Kapazität für ihre Benutzer oder Benutzergruppen in ihren Linux- oder Windows-Systemen konfigurieren. Die Benutzer- oder Gruppenrichtlinien-Quote begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann.…ein hartes Kontingent ermöglicht eine Benachrichtigung des Benutzers, wenn die im Volume genutzte Kapazität richtig ist, bevor die gesamte Kapazitätsquote erreicht wird. Durch die Überwachung der Datenmenge, die innerhalb eines Benutzer- oder Gruppenkontingents gespeichert ist, wird sichergestellt, dass der Benutzer einen ununterbrochenen Datendienst erhält.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Vergrößern Sie den Platz des Benutzers oder der Gruppenquote, um dem Wachstum gerecht zu werden. 2. Weisen Sie den Benutzer oder die Gruppe an, unerwünschte Daten zu löschen, um Speicherplatz freizugeben.

Soft-Limit Für Benutzerkontingenenkapazität	WARNUNG	ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte verfügen, auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes zuzugreifen. Daher können Kunden mit ONTAP Storage-Kapazität für ihre Benutzer oder Benutzergruppen in ihren Linux- oder Windows-Systemen konfigurieren. Die Benutzer- oder Gruppenrichtlinien-Quote begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann.…ein softer Grenzwert für diese Quote ermöglicht eine proaktive Benachrichtigung an den Benutzer, wenn die innerhalb des Volumes genutzte Kapazität die gesamte Kapazitätsquote erreicht. Durch die Überwachung der Datenmenge, die innerhalb eines Benutzer- oder Gruppenkontingents gespeichert ist, wird sichergestellt, dass der Benutzer einen ununterbrochenen Datendienst erhält.	Wenn der Warnschwellenwert nicht erreicht wird, sollten folgende Maßnahmen ergriffen werden: 1. Vergrößern Sie den Platz des Benutzers oder der Gruppenquote, um dem Wachstum gerecht zu werden. 2. Löschen Sie unerwünschte Daten, um Speicherplatz freizugeben.

Volume-Kapazität Voll	KRITISCH	Die Storage-Kapazität eines Volumes ist erforderlich, um Applikations- und Kundendaten zu speichern. Je mehr Daten im ONTAP-Volume gespeichert werden, desto geringer ist die Storage-Verfügbarkeit für künftige Daten. Wenn die Datenspeicherkapazität innerhalb eines Volumes die gesamte Storage-Kapazität erreicht, kann der Kunde aufgrund des Fehlens der entsprechenden Storage-Kapazität möglicherweise nicht in der Lage sein, Daten zu speichern. Durch das Monitoring der verwendeten Storage-Kapazität wird die Kontinuität der Datendienste gewährleistet.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Erhöhen Sie den Platz des Volumes, um dem Wachstum gerecht zu werden. 2. Löschen Sie unerwünschte Daten, um Speicherplatz freizugeben. 3. Wenn Snapshot-Kopien mehr Speicherplatz belegen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie Volume Snapshot-Autodelete.…Wenn der Warnungsschwellenwert verletzt wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen: 1. Vergrößern Sie den Platzbedarf des Volumes, um dem Wachstum gerecht zu werden 2. Wenn Snapshot-Kopien mehr Speicherplatz beanspruchen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume Snapshot.……

Volume-Inodes-Limit	KRITISCH	Volumes, in denen Dateien gespeichert werden, verwenden Index-Nodes (Inode) zum Speichern von Dateimetadaten. Wenn ein Volumen seine Inode-Zuordnung entlüstet, Es können keine weiteren Dateien hinzugefügt werden.…eine Warnmeldung gibt an, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen.…eine kritische Warnung zeigt an, dass die Dateilimits unmittelbar erschöpft sind und Notmaßnahmen ergriffen werden sollten, um Inodes freizumachen, um die Kontinuität der Services zu gewährleisten.	Bei Verstößen gegen kritische Schwellenwerte sind folgende unmittelbare Maßnahmen zu ergreifen, um Service-Unterbrechungen zu minimieren: 1. Erhöhen Sie den Inodes-Wert für das Volumen. Wenn der Wert für Inodes bereits den Maximalwert überschreitet, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe gewachsen ist. 2. Verwenden Sie FlexGroup als Unterstützung bei der Aufnahme großer Dateisysteme.… Wenn der Warnschwellenwert nicht erreicht wird, sollten folgende Maßnahmen ergriffen werden: 1. Erhöhen Sie den Inodes-Wert für das Volumen. Wenn der Inodes-Wert bereits auf dem Maximum liegt, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe gewachsen ist. 2. Nutzen Sie FlexGroup als Unterstützung bei der Aufnahme großer File-Systeme

Volume-Latenz Hoch	KRITISCH	Volumes sind Objekte, die den I/O-Datenverkehr verarbeiten, der durch Performance-kritische Applikationen wie DevOps-Applikationen, Home Directorys und Datenbanken häufig geleitet wird. Latenzen bei hohen Mengen bedeuten, dass die Applikationen selbst unter Umständen darunter leiden und ihre Aufgaben nicht ausführen können. Das Monitoring von Volume-Latenzzeiten ist von entscheidender Bedeutung, um eine applikationskonsistente Performance zu gewährleisten. Die folgenden Latenzzeiten sind auf Grundlage des Medientyps zu erwarten – SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden.	Bei Verstößen gegen kritische Grenzwerte sind sofortige Maßnahmen zur Minimierung der Serviceunterbrechung zu beachten: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie die Schwellenwerte für den Fall, dass die Volume-Workload gedrosselt wird.… Bei Überschreitung der Warnungsschwelle sollten folgende unmittelbare Maßnahmen berücksichtigt werden: 1. Wenn zudem ein Aggregat eine hohe Auslastung erzielt, verschieben Sie das Volume zu einem anderen Aggregat. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie seine Grenzwerte, falls der Volume-Workload gedrosselt wird. 3. Wenn zudem ein Node hohe Auslastung erzielt, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den gesamten Workload des Node.
Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme

Hohe Node-Latenz	WARNUNG/KRITISCH	Die Node-Latenz hat die Werte erreicht, die möglicherweise die Performance der Applikationen auf dem Node beeinträchtigen könnten. Eine niedrigere Node-Latenz sorgt für eine konsistente Performance der Applikationen. Zu den erwarteten Latenzzeiten auf Grundlage des Medientyps zählen SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden.	Wenn kritische Schwellenwerte nicht eingehalten werden, sind sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen zu ergreifen: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder SnapMirror Replikation 2. Weniger Bedarf an Workloads mit niedriger Priorität über QoS-Limits 3 Nichtaktivierung von nicht wichtigen Workloads Verachten Sie sofortige Maßnahmen bei Überschreitung eines Warnschwellenwerts: 1. Verschieben Sie eine oder mehrere Workloads an einen anderen Storage-Standort 2. Weniger Bedarf an Workloads mit niedriger Priorität über QoS-Limits 3 Hinzufügen von weiteren Storage-Nodes (AFF) oder Festplatten-Shelfs (FAS) und Neuverteilung von Workloads 4 Änderung der Workload-Merkmale (Blockgröße, Applikations-Caching usw.)

Node-Performance-Limit	WARNUNG/KRITISCH	Die Performance-Auslastung der Nodes hat die Werte erreicht, in denen sie die Performance der I/O-Vorgänge und der vom Node unterstützten Applikationen beeinträchtigen könnten. Eine geringe Auslastung der Node-Performance stellt eine konsistente Performance der Applikationen sicher.	Zur Minimierung von Serviceunterbrechungen bei Überschreitung kritischer Schwellwerte sind sofortige Maßnahmen zu ergreifen: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder SnapMirror Replikation 2. Weniger Bedarf an Workloads mit niedriger Priorität über QoS-Limits 3 Bei der Nichtaktivierung von nicht wichtigen Workloads sollten folgende Maßnahmen ergriffen werden, wenn Warnschwellenwert überschritten wird: 1. Verschieben Sie eine oder mehrere Workloads an einen anderen Storage-Standort 2. Weniger Bedarf an Workloads mit niedriger Priorität über QoS-Limits 3 Hinzufügen von weiteren Storage-Nodes (AFF) oder Festplatten-Shelfs (FAS) und Neuverteilung von Workloads 4 Änderung der Workload-Merkmale (Blockgröße, Applikations-Caching usw.)

Storage-VM hohe Latenz	WARNUNG/KRITISCH	Die Latenz von Storage-VM (SVM) hat die Werte erreicht, die sich auf die Performance der Applikationen auf der Storage-VM auswirken könnten. Eine geringere Storage-VM-Latenz sorgt für eine konsistente Performance der Applikationen. Zu den erwarteten Latenzzeiten auf Grundlage des Medientyps zählen SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden.	Falls der kritische Schwellenwert nicht erreicht wird, bewerten Sie sofort die Grenzwerte für Volumes der Storage-VM mit einer zugewiesenen QoS-Richtlinie. So überprüfen Sie, ob die Volume-Workloads gedrosselt werden, und berücksichtigen Sie folgende unmittelbare Maßnahmen, wenn der Warnschwellenwert nicht erreicht wird: 1. Wenn zudem ein Aggregat eine hohe Auslastung erzielt, verschieben Sie einige Volumes der Storage VM zu einem anderen Aggregat. 2. Bewerten Sie bei Volumes der Storage-VM mit einer zugewiesenen QoS-Richtlinie die Schwellenwerte, wenn sie dazu führen, dass die Volume-Workloads gedrosselt werden 3. Falls der Node eine hohe Auslastung erzielt, verschieben Sie einige Volumes der Storage-VM auf einen anderen Node oder verringern Sie den Gesamtarbeitsbedarf des Node

Harte Grenze Für Benutzer-Quota-Dateien	KRITISCH	Die Anzahl der innerhalb des Volumes erstellten Dateien hat das kritische Limit erreicht, und es können keine zusätzlichen Dateien erstellt werden. Durch die Überwachung der Anzahl der gespeicherten Dateien wird sichergestellt, dass der Benutzer einen ununterbrochenen Datendienst erhält.	Sofortige Maßnahmen sind zur Minimierung von Service-Unterbrechungen nötig, wenn kritische Grenzwerte nicht eingehalten werden.…Ermöglichen Sie Maßnahmen: 1. Erhöhen Sie die Dateianzahl für den spezifischen Benutzer 2. Löschen Sie unerwünschte Dateien, um den Druck auf die Dateiquote für den spezifischen Benutzer zu verringern
Soft Limit Für Benutzerkontingendateien	WARNUNG	Die Anzahl der innerhalb des Volumes erstellten Dateien hat den Grenzwert der Quote erreicht und befindet sich nahe dem kritischen Limit. Sie können keine zusätzlichen Dateien erstellen, wenn die Quote die kritische Grenze erreicht. Durch die Überwachung der Anzahl der von einem Benutzer gespeicherten Dateien wird sichergestellt, dass der Benutzer einen ununterbrochenen Datendienst erhält.	Unmittelbare Maßnahmen sollten bei Überschreitung der Warnschwelle ergriffen werden: 1. Erhöhen Sie die Dateianzahl für das spezifische Benutzerkontingent 2. Löschen Sie unerwünschte Dateien, um den Druck auf die Dateiquote für den spezifischen Benutzer zu verringern

Miss-Verhältnis Von Volume Cache	WARNUNG/KRITISCH	Das Miss-Verhältnis des Volume Cache ist der Prozentsatz von Leseanforderungen der Client-Applikationen, die von der Festplatte zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden. Das bedeutet, dass das Volumen den eingestellten Schwellenwert erreicht hat.	Wenn kritische Schwellenwerte nicht eingehalten werden, sind sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen zu ergreifen: 1. Verschieben Sie einige Workloads vom Node des Volumes, um die I/O-Last zu reduzieren 2. Wenn Sie dies noch nicht auf dem Node des Volume getan haben, erhöhen Sie den WAFL Cache durch den Kauf und das Hinzufügen eines Flash Cache 3. Weniger Workloads mit niedriger Priorität auf demselben Node über QoS-Grenzen für sofortige Maßnahmen ergreifen, wenn ein Warnschwellenwert nicht erreicht wird: 1 Verschieben Sie einige Workloads vom Node des Volumes, um die I/O-Last zu reduzieren 2. Wenn Sie dies noch nicht auf dem Node des Volume getan haben, erhöhen Sie den WAFL Cache durch den Kauf und das Hinzufügen eines Flash Cache 3. Durch QoS-Limits sinken die Anforderungen von Workloads mit niedriger Priorität auf demselben Node 4. Änderung der Workload-Merkmale (Blockgröße, Applikations-Caching usw.)

Überprovisionierungsquote Bei Volume Qtree	WARNUNG/KRITISCH	Bei der Überprovisionierung von Volume-qtree wird der Prozentsatz angegeben, bei dem ein Volume durch die qtree Kontingente überengagiert wird. Der festgelegte Schwellenwert für die qtree-Quote wird für den Volumen erreicht. Durch Monitoring der Überprovisionierung von Volume-qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Wenn kritische Schwellenwerte nicht eingehalten werden, sind sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen zu ergreifen: 1. Vergrößern Sie den Speicherplatz des Volumens 2. Löschen Sie unerwünschte Daten, wenn ein Warnschwellenwert nicht erreicht wird. Dies empfiehlt sich, den Speicherplatz des Volume zu erhöhen.

Zurück nach oben

Protokollmonitore

Monitorname	Schweregrad	Beschreibung	Korrekturmaßnahme
Die AWS Zugangsdaten wurden nicht initialisiert	INFO	Dieses Ereignis tritt auf, wenn ein Modul versucht, über den Cloud-Anmeldedaten-Thread auf rollenbasierte IAM-Anmeldedaten (Identity and Access Management) von Amazon Web Services (AWS) zuzugreifen, bevor sie initialisiert werden.	Warten Sie, bis der Cloud-Anmeldedaten-Thread sowie das System vollständig initialisiert wurden.

Cloud-Tier Nicht Erreichbar	KRITISCH	Ein Storage-Node kann keine Verbindung mit der Objekt-Storage-API der Cloud-Ebene herstellen. Auf einige Daten kann nicht zugegriffen werden.	Wenn Sie Produkte vor Ort verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: …Überprüfen Sie mit dem Befehl „Network Interface show“, ob Ihre Intercluster-LIF online und funktionsfähig ist.…Überprüfen Sie die Netzwerkverbindung zum Objektspeicher-Server mithilfe des Befehls „ping“ über das Intercluster LIF des Ziel-Knotens.…Stellen Sie sicher, dass Folgendes vorliegt:…die Konfiguration Ihres Objektspeichers hat sich nicht geändert.…die Login- und Konnektivitätsinformationen sind Gültig weiterhin.…Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht. Wenn Sie Cloud Volumes ONTAP verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: …Stellen Sie sicher, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat.… Stellen Sie sicher, dass die Anmelde- und Verbindungsinformationen weiterhin gültig sind.…Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.

Disk außer Service	INFO	Dieses Ereignis tritt auf, wenn eine Festplatte aus dem Dienst entfernt wird, weil sie als fehlgeschlagen markiert, desinfiziert oder das Maintenance Center aufgerufen wurde.	Keine.
FlexGroup Konstituierend voll	KRITISCH	Ein Teil eines FlexGroup Volume ist voll, was zu einer potenziellen Serviceunterbrechung führen kann. Sie können weiterhin Dateien auf dem FlexGroup Volume erstellen oder erweitern. Allerdings kann keine der auf der Komponente gespeicherten Dateien geändert werden. Folglich werden möglicherweise zufällige Fehler angezeigt, wenn Sie versuchen, Schreibvorgänge auf dem FlexGroup Volume durchzuführen.	Es wird empfohlen, dass Sie dem FlexGroup-Volume Kapazität hinzufügen, indem Sie den Befehl „Volume modify -files +X“ verwenden.…Alternativ können Sie auch Dateien vom FlexGroup-Volume löschen. Allerdings ist es schwierig zu bestimmen, welche Akten auf dem Konstituierenden gelandet sind.
FlexGroup Konstituierend Fast Voll	WARNUNG	Ein Teil eines FlexGroup Volume ist beinahe nicht mehr genügend Speicherplatz, was zu einer potenziellen Serviceunterbrechung führen kann. Dateien können erstellt und erweitert werden. Wenn jedoch der Speicherplatz für die Komponente knapp ist, können Sie die Dateien auf der Komponente möglicherweise nicht anfügen oder ändern.	Es wird empfohlen, dass Sie dem FlexGroup-Volume Kapazität hinzufügen, indem Sie den Befehl „Volume modify -files +X“ verwenden.…Alternativ können Sie auch Dateien vom FlexGroup-Volume löschen. Allerdings ist es schwierig zu bestimmen, welche Akten auf dem Konstituierenden gelandet sind.

FlexGroup konstituierend fast aus Inodes	WARNUNG	Ein Teil eines FlexGroup Volume befindet sich nahezu außerhalb von Inodes, was zu einer potenziellen Serviceunterbrechung führen kann. Die Komponente erhält weniger Anfragen zur Erstellung als durchschnittlich. Dadurch kann sich unter Umständen die gesamte Performance des FlexGroup Volume auswirken, da die Anforderungen an Komponenten mit mehr Inodes weitergeleitet werden.	Es wird empfohlen, dass Sie dem FlexGroup-Volume Kapazität hinzufügen, indem Sie den Befehl „Volume modify -files +X“ verwenden.…Alternativ können Sie auch Dateien vom FlexGroup-Volume löschen. Allerdings ist es schwierig zu bestimmen, welche Akten auf dem Konstituierenden gelandet sind.
FlexGroup konstituierend aus Inodes	KRITISCH	Bei einem FlexGroup Volume sind nicht mehr Inodes vorhanden, was zu einer potenziellen Serviceunterbrechung führen kann. Sie können keine neuen Dateien auf dieser Komponente erstellen. Dies könnte zu einer insgesamt unausgeglichenen Verteilung von Inhalten über das FlexGroup-Volume führen.	Es wird empfohlen, dass Sie dem FlexGroup-Volume Kapazität hinzufügen, indem Sie den Befehl „Volume modify -files +X“ verwenden.…Alternativ können Sie auch Dateien vom FlexGroup-Volume löschen. Allerdings ist es schwierig zu bestimmen, welche Akten auf dem Konstituierenden gelandet sind.
LUN Offline	INFO	Dieses Ereignis tritt auf, wenn eine LUN manuell in den Offline-Modus versetzt wird.	Versetzen Sie die LUN wieder in den Online-Modus.
Hauptlüfter Fehlgeschlagen	WARNUNG	Mindestens ein Lüfter der Haupteinheit ist ausgefallen. Das System bleibt in Betrieb.…Wenn der Zustand jedoch zu lange andauert, kann die Übertemperatur ein automatisches Herunterfahren auslösen.	Setzen Sie die fehlerhaften Lüfter neu ein. Wenn der Fehler weiterhin besteht, ersetzen Sie ihn.
Hauptlüfter im Warnstatus	INFO	Dieses Ereignis tritt auf, wenn sich ein oder mehrere Hauptlüfter im Warnstatus befinden.	Ersetzen Sie die angezeigten Lüfter, um eine Überhitzung zu vermeiden.

NVRAM-Akku schwach	WARNUNG	Die Kapazität der NVRAM-Batterie ist kritisch niedrig. Es kann zu einem potenziellen Datenverlust kommen, wenn der Akku knapp wird.…das System generiert und sendet eine AutoSupport- oder „Call Home“-Meldung an den technischen Support von NetApp und die konfigurierten Ziele, sofern sie so konfiguriert sind. Die erfolgreiche Bereitstellung einer AutoSupport-Botschaft verbessert die Problembestimmung und -Lösung erheblich.	Führen Sie folgende Korrekturmaßnahmen durch:…Anzeigen des aktuellen Status, der Kapazität und des Ladezustands der Batterie mit dem Befehl „System Node Environment Sensors show“.…Wenn die Batterie kürzlich ausgetauscht wurde oder das System längere Zeit nicht betriebsbereit war, Überwachen Sie die Batterie, um zu überprüfen, ob sie ordnungsgemäß geladen wird.…wenden Sie sich an den technischen Support von NetApp, wenn die Akkulaufzeit unter den kritischen Wert nachlässt und das Speichersystem automatisch heruntergefahren wird.
Der Service-Prozessor Ist Nicht Konfiguriert	WARNUNG	Dieses Event findet wöchentlich statt, um Sie daran zu erinnern, den Service-Prozessor (SP) zu konfigurieren. Der SP ist ein physisches Gerät, das in Ihr System integriert ist und Remote-Zugriff sowie Remote Management-Funktionen bietet. Sie sollten den SP so konfigurieren, dass seine vollständige Funktionalität verwendet wird.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Konfigurieren Sie den SP mithilfe des Befehls „System Service-Processor Network modify“.…optional Rufen Sie die MAC-Adresse des SP mit dem Befehl „System Service-Processor Network show“ ab.…Überprüfen Sie die SP-Netzwerkkonfiguration mithilfe des Befehls „System Service-Processor Network show“.…Überprüfen Sie, ob der SP mit dem Befehl „System Service-Processor AutoSupport Invoke“ eine AutoSupport E-Mail senden kann. HINWEIS: AutoSupport-E-Mail-Hosts und -Empfänger sollten in ONTAP konfiguriert werden, bevor Sie diesen Befehl ausführen.

Service-Prozessor Offline	KRITISCH	Der ONTAP empfängt keine Heartbeats mehr vom Service-Prozessor (SP), obwohl alle SP-Wiederherstellungsaktionen durchgeführt wurden. Ohne SP kann ONTAP den Zustand der Hardware nicht überwachen.…das System wird heruntergefahren, um Hardware-Schäden und Datenverlust zu vermeiden. Richten Sie eine Panikwarnung ein, die unmittelbar benachrichtigt werden soll, wenn der SP offline geht.	Schalten Sie das System aus und wieder ein, indem Sie folgende Aktionen ausführen:…Ziehen Sie den Controller aus dem Gehäuse heraus.…Drücken Sie den Controller wieder ein.…Drehen Sie den Controller wieder ein.…Wenn das Problem weiterhin besteht, ersetzen Sie das Controller-Modul.
Fehler Bei Den Shelf-Lüftern	KRITISCH	Der angegebene Lüfter- oder Lüftermodul des Shelf ist ausgefallen. Die Festplatten im Shelf erhalten möglicherweise nicht genügend Luftstrom zur Kühlung, was zu einem Festplattenausfall führen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie, ob das Lüftermodul richtig eingesetzt und gesichert ist. HINWEIS: Der Lüfter ist in einige Platten-Shelves in das Netzteil-Modul integriert.…sollte das Problem weiterhin bestehen, ersetzen Sie das Lüftermodul.…sollte das Problem weiterhin bestehen, wenden Sie sich an den technischen Support von NetApp.
Das System kann aufgrund eines Ausfalls des Hauptlüfters nicht betrieben werden	KRITISCH	Ein oder mehrere Lüfter der Haupteinheit sind ausgefallen und der Systembetrieb wird unterbrochen. Dies kann zu einem potenziellen Datenverlust führen.	Ersetzen Sie die fehlerhaften Lüfter.

Nicht Zugewiesene Festplatten	INFO	System verfügt über nicht zugewiesene Festplatten – Kapazität wird verschwendet. Möglicherweise ist bei Ihrem System eine fehlerhafte Konfiguration oder ein Teil der Konfigurationsänderungen zu finden.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Bestimmen Sie, welche Festplatten durch den Befehl „Disk show -n“ nicht zugewiesen werden.…Zuweisen der Festplatten zu einem System mit dem Befehl „Disk assign“.
Antivirus-Server Belegt	WARNUNG	Der Antivirus-Server ist zu beschäftigt, um neue Scananforderungen zu akzeptieren.	Wenn diese Meldung häufig angezeigt wird, stellen Sie sicher, dass genügend Virenschutz-Server vorhanden sind, um die von der SVM erzeugte Virus-Scan-Last zu bewältigen.
Die AWS Zugangsdaten für die IAM-Rolle sind abgelaufen	KRITISCH	Cloud Volume ONTAP ist inzwischen nicht mehr zugänglich. Die rollenbasierten Anmeldedaten für Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) sind abgelaufen. Die Zugangsdaten werden über die IAM-Rolle vom Metadatenserver Amazon Web Services (AWS) erworben und werden zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet.	Führen Sie Folgendes aus:…Melden Sie sich an der AWS EC2 Management Console an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Funktionszustand.…Über prüfen Sie, ob die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und der Instanz entsprechende Berechtigungen erteilt wurde.

Die AWS Zugangsdaten für die IAM-Rolle wurden nicht gefunden	KRITISCH	Der Thread für die Cloud-Anmeldedaten kann die rollenbasierten Zugangsdaten für das IAM (Identity and Access Management) von Amazon Web Services (AWS) nicht vom AWS Metadatenserver abrufen. Mit den Zugangsdaten werden API-Anfragen an Amazon Simple Storage Service (Amazon S3) signieren. Cloud Volume ONTAP ist nicht mehr zugänglich.…	Führen Sie Folgendes aus:…Melden Sie sich an der AWS EC2 Management Console an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Funktionszustand.…Über prüfen Sie, ob die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und der Instanz entsprechende Berechtigungen erteilt wurde.
Die AWS Zugangsdaten für die IAM-Rolle sind nicht gültig	KRITISCH	Die rollenbasierten Zugangsdaten für das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) sind ungültig. Die Zugangsdaten werden über die IAM-Rolle vom Metadatenserver Amazon Web Services (AWS) erworben und werden zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet. Cloud Volume ONTAP ist inzwischen nicht mehr zugänglich.	Führen Sie Folgendes aus:…Melden Sie sich an der AWS EC2 Management Console an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Funktionszustand.…Über prüfen Sie, ob die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und der Instanz entsprechende Berechtigungen erteilt wurde.
Die AWS IAM-Rolle wurde nicht gefunden	KRITISCH	Der IAM-Thread (Identitäts- und Zugriffsmanagement) kann eine IAM-Rolle von Amazon Web Services (AWS) nicht auf dem AWS Metadatenserver finden. Die IAM-Rolle muss rollenbasierte Zugangsdaten erfassen, mit denen API-Anfragen an Amazon Simple Storage Service (Amazon S3) signieren. Cloud Volume ONTAP ist nicht mehr zugänglich.…	Führen Sie Folgendes durch:…Melden Sie sich an der AWS EC2-Verwaltungskonsole an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Zustand.…Überprüfen Sie, ob die mit der Instanz verknüpfte AWS-IAM-Rolle gültig ist.

Die AWS IAM-Rolle ist nicht gültig	KRITISCH	Die Amazon Web Services (AWS) Funktion für Identitäts- und Zugriffsmanagement (IAM) auf dem AWS Metadatenserver ist ungültig. Das Cloud Volume ONTAP ist unzugänglich geworden.…	Führen Sie Folgendes aus:…Melden Sie sich an der AWS EC2 Management Console an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Funktionszustand.…Überprüfen Sie, ob die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und der Instanz entsprechende Berechtigungen erteilt wurde.
Verbindung zum AWS Metadatenserver schlägt fehl	KRITISCH	Der IAM-Thread (Identity and Access Management) kann keine Kommunikationsverbindung zum Metadatenserver von Amazon Web Services (AWS) herstellen. Die Kommunikation sollte eingerichtet werden, um die erforderlichen rollenbasierten AWS IAM-Zugangsdaten zu erhalten, die zum Signieren von API-Anforderungen an Amazon Simple Storage Service (Amazon S3) verwendet werden. Cloud Volume ONTAP ist nicht mehr zugänglich.…	Führen Sie Folgendes durch:…Melden Sie sich an der AWS EC2 Management Console an.…Navigieren Sie zur Seite Instanzen.…Finden Sie die Instanz für die Cloud Volumes ONTAP-Bereitstellung und überprüfen Sie deren Zustand.…

Die zulässige Nutzung von FabricPool-Speicherplatz wurde nahezu erreicht	WARNUNG	Der gesamte Cluster-weite FabricPool-Platzbedarf von Objektspeichern von kapazitätslizenzierten Anbietern hat fast das lizenzierte Limit erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie den Prozentsatz der von den einzelnen FabricPool Storage-Klassen verwendeten lizenzierten Kapazität mithilfe des Befehls „Storage Aggregate Object-Store show-space“.…Löschen Sie Snapshot Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „Volume Snapshot delete“ zum Löschen von Speicherplatz verwenden.…Installieren Sie eine neue Lizenz Auf dem Cluster zur Erhöhung der lizenzierten Kapazität.
Grenzwert für die FabricPool-Speicherplatznutzung erreicht	KRITISCH	Die gesamte Nutzung des Cluster-weiten FabricPool-Speicherplatzes von Objektspeichern von kapazitätslizenzierten Anbietern hat die Lizenzgrenze erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie den Prozentsatz der von den einzelnen FabricPool Storage-Klassen verwendeten lizenzierten Kapazität mithilfe des Befehls „Storage Aggregate Object-Store show-space“.…Löschen Sie Snapshot Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „Volume Snapshot delete“ zum Löschen von Speicherplatz verwenden.…Installieren Sie eine neue Lizenz Auf dem Cluster zur Erhöhung der lizenzierten Kapazität.

GiveBack des Aggregats fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Storage Failover (SFO)-Rückgabe auf, wenn der Ziel-Node nicht auf die Objektspeicher zugreifen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie mithilfe des Befehls „Network Interface show“, ob Ihre Intercluster-LIF online und funktionsfähig ist.…Überprüfen Sie die Netzwerkverbindung mit dem Objektspeicher-Server mithilfe des Befehls „ping“ über das Intercluster LIF im Zielknoten. …Überprüfen Sie, ob sich die Konfiguration Ihres Objektspeichers nicht geändert hat und ob die Login- und Konnektivitätsinformationen durch den Befehl „Aggregate object-Store config show“ noch korrekt sind.…Alternativ, Sie können den Fehler überschreiben, indem Sie „false“ für den Parameter „waiting-Partner-waiting“ des Befehls „Giveback“ angeben.…Kontaktieren Sie den technischen Support von NetApp, um weitere Informationen oder Hilfe zu erhalten.

HA Interconnect herunter	WARNUNG	Der HA Interconnect ist ausgefallen. Risiko eines Serviceausfalls, wenn ein Failover nicht verfügbar ist.	Korrekturmaßnahmen hängen von der Anzahl und der Art der von der Plattform unterstützten HA Interconnect Links ab sowie vom Grund für einen Ausfall des Interconnect. …Wenn die Verbindungen ausgefallen sind:…Überprüfen Sie, dass beide Controller im HA-Paar betriebsbereit sind.…bei extern verbundenen Verbindungen stellen Sie sicher, dass die Verbindungskabel ordnungsgemäß angeschlossen sind und dass die Small Form-Factor Plugables (SFPs), falls zutreffend, ordnungsgemäß auf beiden Controllern eingesetzt werden.…für intern verbundene Links, deaktivieren und wieder aktivieren Sie die Links, Eines nach dem anderen, durch die Verwendung der "ic Link off" und "c Link on" Befehle. …Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl "ic Link on". …Wenn ein Peer nicht verbunden ist, deaktivieren Sie die Links nacheinander und aktivieren Sie sie erneut, indem Sie den Befehl „ic Link off“ und „ic Link on“ verwenden.…Kontaktieren Sie den technischen Support von NetApp, wenn das Problem weiterhin besteht.

Max. Sitzungen Pro Benutzer Überschritten	WARNUNG	Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anforderung zum Errichten einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden. …	Führen Sie die folgenden Korrekturmaßnahmen durch: …Überprüfen Sie alle Anwendungen, die auf dem Client ausgeführt werden, und beenden Sie alle, die nicht ordnungsgemäß funktionieren.…Booten Sie den Client neu.…Überprüfen Sie, ob das Problem durch eine neue oder bestehende Anwendung verursacht wird:…Wenn die Anwendung neu ist, legen Sie einen höheren Schwellenwert für den Client fest, indem Sie den Befehl „cifs Option modify -max-opens-same-file-per -Tree“ verwenden. In einigen Fällen arbeiten Clients wie erwartet, erfordern jedoch einen höheren Schwellenwert. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. …Wenn das Problem durch eine vorhandene Anwendung verursacht wird, kann es zu einem Problem mit dem Client kommen. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

Max Times Open Per File Überschritten	WARNUNG	Sie haben die maximale Anzahl von Zeiten überschritten, die Sie über eine TCP-Verbindung öffnen können. Alle Anfragen zum Öffnen dieser Datei werden abgelehnt, bis Sie einige offene Instanzen der Datei schließen. Dies weist in der Regel auf ein anormales Anwendungsverhalten hin.…	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie die Anwendungen, die auf dem Client mithilfe dieser TCP-Verbindung ausgeführt werden. Der Client arbeitet möglicherweise falsch, weil die auf ihm ausgeführte Anwendung ausgeführt wird.…Client neu starten.…Überprüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird:…Wenn die Anwendung neu ist, legen Sie einen höheren Schwellenwert für den Client fest, indem Sie den Befehl „cifs Option modify -max-opens-same-file-per -Tree“ verwenden. In einigen Fällen arbeiten Clients wie erwartet, erfordern jedoch einen höheren Schwellenwert. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. …Wenn das Problem durch eine vorhandene Anwendung verursacht wird, kann es zu einem Problem mit dem Client kommen. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

NetBIOS-Namenskonflikt	KRITISCH	Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Anfrage zur Namensregistrierung erhalten. Dies wird typischerweise durch einen Konflikt mit dem NetBIOS-Namen oder einem Alias verursacht. Infolgedessen können Clients möglicherweise nicht auf Daten zugreifen oder eine Verbindung mit dem richtigen Datenservice-Node im Cluster herstellen.	Führen Sie eine der folgenden Korrekturmaßnahmen durch:…Wenn es einen Konflikt im NetBIOS-Namen oder einem Alias gibt, Führen Sie einen der folgenden Schritte aus:…Löschen Sie den doppelten NetBIOS-Alias mit dem Befehl „vserver cifs delete -aliases alias -vserver vserver“.…Benennen Sie einen NetBIOS-Alias, indem Sie den doppelten Namen löschen und einen Alias mit einem neuen Namen hinzufügen, indem Sie den Befehl „vserver cifs create -aliases alias -vserver vServer“ verwenden. …Wenn keine Aliase konfiguriert sind und es einen Konflikt im NetBIOS-Namen gibt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -Server netbiosname“ um. HINWEIS: Das Löschen eines CIFS-Servers kann auf Daten zugreifen. …Entfernen Sie den NetBIOS-Namen, oder benennen Sie das NetBIOS auf dem Remotecomputer um.
NFSv4 Store Pool nicht vorhanden	KRITISCH	Ein NFSv4-Speicherpool wurde erschöpft.	Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht mehr reagiert, wenden Sie sich an den technischen Support von NetApp.

Keine Registrierte Scan Engine	KRITISCH	Der Antivirus-Anschluss hat ONTAP darüber informiert, dass es keine registrierte Scan-Engine hat. Dies kann zur Nichtverfügbarkeit von Daten führen, wenn die Option „Scannen obligatorisch“ aktiviert ist.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Stellen Sie sicher, dass die auf dem Virenschutz-Server installierte Scan-Engine-Software mit ONTAP kompatibel ist.…Stellen Sie sicher, dass die Scan-Engine-Software ausgeführt wird und konfiguriert ist, um eine Verbindung zum Antivirus-Anschluss über lokales Loopback herzustellen.
Keine Vscan-Verbindung	KRITISCH	ONTAP verfügt über keine Vscan-Verbindung zur Wartung von Virenabtastanforderungen . Dies kann zur Nichtverfügbarkeit von Daten führen, wenn die Option „Scannen obligatorisch“ aktiviert ist.	Stellen Sie sicher, dass der Scannerpool ordnungsgemäß konfiguriert ist und die Virenschutz-Server aktiv sind und mit ONTAP verbunden sind.
Node-Root-Volume-Speicherplatz Niedrig	KRITISCH	Das System hat festgestellt, dass das Root-Volumen über einen gefährlich niedrigen Speicherplatz verfügt. Der Node ist nicht vollständig betriebsbereit. Daten-LIFs sind möglicherweise ein Failover innerhalb des Clusters durchgeführt, da der NFS- und CIFS-Zugriff auf den Node begrenzt ist. Die administrative Funktion ist auf lokale Recovery-Verfahren beschränkt, um Speicherplatz auf dem Root-Volume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Löschen Sie Speicherplatz auf dem Root-Volume, indem Sie alte Snapshot-Kopien löschen, Dateien löschen, die nicht mehr im /mroot-Verzeichnis benötigt werden, oder erweitern Sie die Root-Volume-Kapazität.…Booten Sie den Controller neu.…wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Hilfe zu erhalten.
Keine Admin-Freigabe Vorhanden	KRITISCH	Vscan-Problem: Ein Kunde hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN-Freigabe zu herstellen.	Stellen Sie sicher, dass Vscan für die erwähnte SVM-ID aktiviert ist. Wenn Sie Vscan auf einer SVM aktivieren, wird die Dateifreigabe von ONTAP_ADMIN automatisch für die SVM erstellt.

Nicht mehr Speicherplatz für NVMe Namespace	KRITISCH	Ein NVMe-Namespace wurde aufgrund eines Schreibfehlers aufgrund von mangelndem Speicherplatz offline geschaltet.	Fügen Sie Speicherplatz zum Volume hinzu, und schalten Sie den NVMe Namespace dann online. Verwenden Sie dazu den Befehl „vserver nvme Namespace modify“.
NVMe-of-Grace-Zeitraum aktiv	WARNUNG	Diese Störung tritt täglich auf, wenn das NVMe over Fabrics-Protokoll (NVMe-of) verwendet wird und der Gnadenzeitraum der Lizenz aktiv ist. Für die NVMe-of Funktion ist nach Ablauf der Gnadenfrist der Lizenz eine Lizenz erforderlich. Die NVMe-of Funktion ist bei Ablauf der Gnadenfrist der Lizenz deaktiviert.	Wenden Sie sich an Ihren Ansprechpartner, um eine NVMe-of-Lizenz zu erhalten, fügen Sie sie dem Cluster hinzu oder entfernen Sie alle Instanzen der NVMe-of Konfiguration vom Cluster.
NVMe-of-Grace-Zeitraum abgelaufen	WARNUNG	Die Gnadenfrist für die NVMe over Fabrics (NVMe-of) Lizenz ist vorbei und die NVMe-of Funktion ist deaktiviert.	Wenden Sie sich an Ihren Ansprechpartner, um eine NVMe-of-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
Beginn des NVMe-of-Grace-Zeitraums	WARNUNG	Während des Upgrades auf die ONTAP 9.5 Software wurde die NVMe-of-Konfiguration (NVMe over Fabrics) erkannt. Für die NVMe-of Funktionalität ist nach Ablauf der Gnadenfrist der Lizenz eine Lizenz erforderlich.	Wenden Sie sich an Ihren Ansprechpartner, um eine NVMe-of-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
Objektspeicherhost Nicht Lösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicher-Client kann nicht mit dem Objektspeicher-Server kommunizieren, ohne sich auf eine IP-Adresse zu lösen. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Überprüfen Sie die DNS-Konfiguration, um zu überprüfen, ob der Hostname mit einer IP-Adresse korrekt konfiguriert ist.

Objektspeicher Intercluster LIF ausgefallen	KRITISCH	Der Objektspeicher-Client kann keine funktionsfähige LIF finden, die mit dem Objektspeicher-Server kommunizieren kann. Der Node ermöglicht dem Client-Datenverkehr zwischen Objekten erst dann, wenn die Intercluster LIF funktionsfähig ist. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie den Status der Intercluster-LIF mit dem Befehl „Network Interface show -role intercluster“.…Überprüfen Sie, ob die Intercluster LIF korrekt und betriebsbereit konfiguriert ist.…Wenn eine Intercluster-LIF nicht konfiguriert ist, fügen Sie sie mithilfe des Befehls „Network Interface create -role intercluster“ hinzu.
Unübereinkommen Bei Objektspeichersignatur	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Vergewissern Sie sich, dass der Schlüssel für den geheimen Zugriff richtig konfiguriert ist. Wenn er korrekt konfiguriert ist, wenden Sie sich an den technischen Support von NetApp, um Hilfe zu erhalten.

ZEITÜBERSCHREITUNG FÜR LESDIR	KRITISCH	Ein VORGANG DER READDIR-Datei hat die Zeitüberschreitung überschritten, die in WAFL ausgeführt werden darf. Dies kann wegen sehr großer oder spärlicher Verzeichnisse erfolgen. Eine Korrekturmaßnahme wird empfohlen.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Suchen Sie Informationen, die für aktuelle Verzeichnisse spezifisch sind, bei denen READDIR-Dateivorgänge ablaufen, indem Sie den folgenden Befehl 'diag' Privilege nodeshell CLI verwenden: WAFL readdir notice show.…Prüfen Sie, ob Verzeichnisse als wenig angezeigt werden oder nicht:…Wenn ein Verzeichnis als spärlich gekennzeichnet ist, empfiehlt es sich, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die Sparheit der Verzeichnisdatei zu entfernen. …Wenn ein Verzeichnis nicht als wenig angegeben wird und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem die Anzahl der Dateieinträge im Verzeichnis verringert wird.

Verschiebung des Aggregats fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Ziel-Node nicht die Objektspeicher erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Überprüfen Sie mithilfe des Befehls „Network Interface show“, ob Ihre Intercluster-LIF online und funktionsfähig ist.…Überprüfen Sie die Netzwerkverbindung mit dem Objektspeicher-Server mithilfe des Befehls „ping“ über das Intercluster LIF im Zielknoten. …Überprüfen Sie, ob sich die Konfiguration Ihres Objektspeicher nicht geändert hat und dass die Login- und Konnektivitätsinformationen noch korrekt sind, indem Sie den Befehl „Aggregate object-Store config show“ verwenden.…Alternativ können Sie den Fehler über den Parameter „override-Destination-checks“ des Befehls ocation überschreiben.…Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Hilfe zu erhalten.

Shadow Copy Fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Backup- und Wiederherstellungsdienst für Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie Folgendes anhand der in der Ereignismeldung angegebenen Informationen:…ist die Konfiguration der Schattenkopie aktiviert?…sind die entsprechenden Lizenzen installiert? …Auf welchen Shares wird die Schattenkopie-Operation durchgeführt?…ist der Freigabenname korrekt?…existiert der Freigabepfad?…welche Zustände gibt es für den Schattenkopie-Satz und seine Schattenkopien?
Stromversorgung Des Speicherschalters Fehlgeschlagen	WARNUNG	Im Cluster-Switch fehlt ein Netzteil. Die Redundanz wird reduziert, das Ausfallrisiko bei weiteren Stromausfällen.	Führen Sie die folgenden Korrekturmaßnahmen durch:…Stellen Sie sicher, dass das Netzteil, das den Cluster-Switch mit Strom versorgt, eingeschaltet ist.…Stellen Sie sicher, dass das Netzkabel an das Netzteil angeschlossen ist.…Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.
Zu viele CIFS-Authentisierung	WARNUNG	Viele Authentifizierungsverhandlungen sind gleichzeitig aufgetreten. Es gibt 256 unvollständige neue Sitzungsanfragen dieses Kunden.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanfragen erstellt hat. Möglicherweise müssen Sie den Anbieter des Clients oder der Anwendung kontaktieren, um festzustellen, warum der Fehler aufgetreten ist.

Nicht autorisierter Benutzerzugriff auf die Administratorfreigabe	WARNUNG	Ein Kunde hat versucht, eine Verbindung zu der privilegierten Version von ONTAP_ADMIN herzustellen, obwohl der angemeldete Benutzer kein berechtigter Benutzer ist.	Führen Sie folgende Korrekturmaßnahmen durch:…Stellen Sie sicher, dass der angegebene Benutzername und die IP-Adresse in einem der aktiven Vscan-Scannerpools konfiguriert sind.…Überprüfen Sie die Konfiguration des Scannerpools, die derzeit aktiv ist, indem Sie den Befehl „vserver vscan-Pool show-Active“ verwenden.
Virus Erkannt	WARNUNG	Ein Vscan-Server hat einen Fehler an das Speichersystem gemeldet. Dies bedeutet in der Regel, dass ein Virus gefunden wurde. Andere Fehler auf dem Vscan-Server können jedoch dieses Ereignis verursachen.…der Client-Zugriff auf die Datei wird verweigert. Der Vscan-Server kann je nach Einstellungen und Konfiguration die Datei bereinigen, in Quarantäne stellen oder löschen.	Prüfen Sie das Protokoll des Vscan-Servers, der im Ereignis „syslog“ gemeldet wurde, um zu sehen, ob die infizierte Datei erfolgreich bereinigt, isoliert oder gelöscht werden konnte. Wenn dies nicht möglich war, muss der Systemadministrator die Datei möglicherweise manuell löschen.
Volume Offline	INFO	Diese Meldung gibt an, dass ein Volume offline geschaltet wird.	Versetzen Sie das Volume wieder in den Online-Modus.
Volume-Beschränkungen	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volume eingeschränkt wird.	Versetzen Sie das Volume wieder in den Online-Modus.
Stopp der Storage-VM erfolgreich	INFO	Diese Meldung tritt auf, wenn eine Operation „vserver stop“ erfolgreich ist.	Verwenden Sie den Befehl „vserver Start“, um den Datenzugriff auf einer Storage-VM zu starten.
Knoten Panik	WARNUNG	Dieses Ereignis wird ausgegeben, wenn ein Panikzustand eintritt	Wenden Sie sich an den NetApp Kundensupport.

Zurück nach oben

Anti-Ransomware-Protokollmonitore

Monitorname	Schweregrad	Beschreibung	Korrekturmaßnahme
Anti-Ransomware-Monitoring für Storage VM ist deaktiviert	WARNUNG	Das Anti-Ransomware-Monitoring für die Storage-VM ist deaktiviert. Anti-Ransomware schützen die Storage-VM.	Keine
Anti-Ransomware-Monitoring von Storage VMs aktiviert (Learning Mode)	INFO	Im Learning-Modus ist die Anti-Ransomware-Überwachung für die Storage-VM aktiviert.	Keine
Volume-Anti-Ransomware-Monitoring ist aktiviert	INFO	Das Anti-Ransomware-Monitoring für das Volume ist aktiviert.	Keine
Volume-Anti-Ransomware-Überwachung deaktiviert	WARNUNG	Die Anti-Ransomware-Überwachung für das Volume ist deaktiviert. Anti-Ransomware-Angriffe können das Volume schützen.	Keine
Volume Anti-Ransomware Monitoring aktiviert (Learning-Modus)	INFO	Die Anti-Ransomware-Überwachung für das Volume ist im Lernmodus aktiviert.	Keine
Volume Anti-Ransomware Monitoring PaUsed (Learning Mode)	WARNUNG	Die Anti-Ransomware-Überwachung für das Volume wird im Lernmodus angehalten.	Keine
Volume Anti-Ransomware Monitoring angehalten	WARNUNG	Die Anti-Ransomware-Überwachung für das Volume wird angehalten.	Keine
Volume Anti-Ransomware Monitoring deaktiviert	WARNUNG	Die Anti-Ransomware-Überwachung für das Volume ist deaktiviert.	Keine

Ransomware-Aktivität Erkannt	KRITISCH	Zur Sicherung der Daten gegen erkannte Ransomware wurde eine Snapshot Kopie erstellt, die zur Wiederherstellung der Originaldaten eingesetzt werden kann. Das System generiert und überträgt eine AutoSupport- oder „Call Home“-Nachricht an den technischen Support von NetApp und alle konfigurierten Ziele. AutoSupport Message verbessert die Problembestimmung und -Lösung.	Korrekturmaßnahmen bei Ransomware-Aktivitäten sind mit dem Namen DES FINALEN DOKUMENTS zu beachten.

Zurück nach oben

FSX für NetApp ONTAP-Monitore

Monitorname	Schwellenwerte	Beschreibung Des Monitors	Korrekturmaßnahme
Die Kapazität der FSX-Volumes ist voll	Warnung @ > 85 %…Kritisch @ > 95 %	Die Storage-Kapazität eines Volumes ist erforderlich, um Applikations- und Kundendaten zu speichern. Je mehr Daten im ONTAP-Volume gespeichert werden, desto geringer ist die Storage-Verfügbarkeit für künftige Daten. Wenn die Datenspeicherkapazität innerhalb eines Volumes die gesamte Storage-Kapazität erreicht, kann der Kunde aufgrund des Fehlens der entsprechenden Storage-Kapazität möglicherweise nicht in der Lage sein, Daten zu speichern. Durch das Monitoring der verwendeten Storage-Kapazität wird die Kontinuität der Datendienste gewährleistet.	Zur Minimierung von Serviceunterbrechungen sind sofortige Maßnahmen erforderlich, wenn kritische Schwellenwerte nicht eingehalten werden:…1. Gehen Sie beispielsweise davon aus, Daten zu löschen, die nicht mehr benötigt werden, um Speicherplatz freizugeben

FSX Volume mit hoher Latenz	Warnung @ > 1000 µs…kritisch @ > 2000 µs	Volumes sind Objekte, die den I/O-Verkehr bedienen. Dabei werden häufig Performance-kritische Applikationen wie DevOps-Applikationen, Home Directorys und Datenbanken verwendet. Latenzen bei hohen Mengen bedeuten, dass die Applikationen selbst unter Umständen darunter leiden und ihre Aufgaben nicht ausführen können. Das Monitoring von Volume-Latenzzeiten ist von entscheidender Bedeutung, um eine applikationskonsistente Performance zu gewährleisten.	Zur Minimierung von Serviceunterbrechungen sind sofortige Maßnahmen erforderlich, wenn kritische Schwellenwerte nicht eingehalten werden:…1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzwerte für den Fall, dass der Volume-Workload gedrosselt wird……Bitte ergreifen Sie bei Überschreitung des Warnungsschwellenwerts die folgenden Aktionen…1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzwerte für den Fall, dass der Volume-Workload gedrosselt wird.…2. Wenn zudem ein Node hohe Auslastung erzielt, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den gesamten Workload des Node.

Limit für FSX-Volume-Inoden	Warnung @ > 85 %…Kritisch @ > 95 %	Volumes, in denen Dateien gespeichert werden, verwenden Index-Nodes (Inode) zum Speichern von Dateimetadaten. Wenn ein Volumen seine Inode-Zuordnung erschöpft, können keine Dateien mehr hinzugefügt werden. Eine Warnmeldung gibt an, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen. Eine kritische Warnung zeigt an, dass die Erschöpfung des Dateilimits unmittelbar bevorsteht und Notmaßnahmen ergriffen werden müssen, um Inodes freizumachen, um die Servicekontinuität sicherzustellen	Zur Minimierung von Serviceunterbrechungen sind sofortige Maßnahmen erforderlich, wenn kritische Schwellenwerte nicht eingehalten werden:…1. Ziehen Sie in Betracht, den Inodes-Wert für das Volumen zu erhöhen. Wenn der Inodes-Wert bereits auf dem Maximum liegt, ziehen Sie in Erwägung, das Volume in zwei oder mehr Volumes aufzuteilen, da das Dateisystem über die Maximalgröße gewachsen ist……Planen Sie bald die folgenden Aktionen, wenn der Warnschwellenwert überschritten wird:…1. Ziehen Sie in Betracht, den Inodes-Wert für das Volumen zu erhöhen. Wenn der Wert für Inodes bereits auf dem Maximum liegt, erüberlegen Sie sich, das Volume in zwei oder mehr Volumes aufzuteilen, da das Dateisystem über die maximale Größe gewachsen ist
Überprovisionierung der qtree Kontingente von FSX	Warnung @ > 95 %…Kritisch @ > 100 %	Bei der Überprovisionierung von Volume-qtree wird der Prozentsatz angegeben, bei dem ein Volume durch die qtree Kontingente überengagiert wird. Der festgelegte Schwellenwert für die qtree-Quote wird für den Volumen erreicht. Durch Monitoring der Überprovisionierung von Volume-qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datenservice erhält.	Wenn kritische Schwellenwerte nicht eingehalten werden, sind sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen zu ergreifen: 1. Löschen unerwünschter Daten…bei Überschreitung der Warnungsschwellenwerte sollten Sie den Speicherplatz des Volume erhöhen.

FSX-Snapshot-Reserve ist voll	Warnung @ > 90 %…Kritisch @ > 95 %	Die Storage-Kapazität eines Volumes ist erforderlich, um Applikations- und Kundendaten zu speichern. Ein Teil dieses Speicherplatzes, der als reservierter Snapshot-Speicherplatz bezeichnet wird, wird zum Speichern von Snapshots verwendet, mit denen Daten lokal gesichert werden können. Je mehr neue und aktualisierte Daten in dem ONTAP Volume gespeichert sind, desto mehr Snapshot-Kapazität wird benötigt und weniger Snapshot Storage-Kapazität wird für zukünftige neue oder aktualisierte Daten zur Verfügung stehen. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reserveplatz erreicht, kann dies dazu führen, dass der Kunde nicht in der Lage ist, neue Snapshot-Daten zu speichern und den Schutz der Daten im Volume zu verringern. Durch das Monitoring der verwendeten Snapshot-Kapazität des Volumes wird die Kontinuität der Datendienste gewährleistet.	Zur Minimierung von Serviceunterbrechungen sind sofortige Maßnahmen erforderlich, wenn kritische Schwellenwerte nicht eingehalten werden:…1. Erwägen Sie die Konfiguration von Snapshots, um Platz im Volumen zu nutzen, wenn die Snapshot-Reserve voll ist…2. Erwägen Sie das Löschen älterer Snapshots, die möglicherweise nicht mehr benötigt werden, um Speicherplatz freizugeben.……Planen Sie, bei Überschreitung eines Warnungsschwellenwerts die folgenden Maßnahmen zu ergreifen:…1. Erwägen Sie, den Speicherplatz innerhalb des Volumes zu erhöhen, um dem Wachstum gerecht zu werden…2. Es empfiehlt sich die Konfiguration von Snapshots, um den Platz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist

FSX Volume Cache Miss-Verhältnis	Warnung @ > 95 %…Kritisch @ > 100 %	Das Miss-Verhältnis des Volume Cache ist der Prozentsatz von Leseanforderungen der Client-Applikationen, die von der Festplatte zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden. Das bedeutet, dass das Volumen den eingestellten Schwellenwert erreicht hat.	Wenn kritische Schwellenwerte nicht eingehalten werden, sind sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen zu ergreifen: 1. Verschieben Sie einige Workloads vom Node des Volumes, um die I/O-Last zu reduzieren 2. Weniger Bedarf an Workloads mit niedriger Priorität auf demselben Node über QoS-Limits…sofortige Maßnahmen ergreifen, wenn Warnschwellenwert nicht erreicht wird: 1 Verschieben Sie einige Workloads vom Node des Volumes, um die I/O-Last zu reduzieren 2. Durch QoS-Limits sinken die Anforderungen von Workloads mit niedriger Priorität auf demselben Node 3. Änderung der Workload-Merkmale (Blockgröße, Applikations-Caching usw.)

Zurück nach oben

K8s-Monitore

Monitorname	Beschreibung	Korrekturmaßnahmen	Schweregrad/Schwellenwert

Hohe Persistent Volume Latency	Hohe persistente Volume-Latenzen bedeuten, dass die Applikationen selbst möglicherweise darunter leiden und ihre Aufgaben nicht ausführen können. Das Monitoring von Latenzen bei persistenten Volumes ist für eine applikationskonsistente Performance von entscheidender Bedeutung. Die folgenden Latenzzeiten sind auf Grundlage des Medientyps zu erwarten – SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden.	**Sofortige Maßnahmen** Wenn ein kritischer Schwellenwert überschritten wird, sollten sofortige Maßnahmen zur Minimierung der Service-Unterbrechung in Betracht gezogen werden: Wenn dem Volume eine QoS-Richtlinie zugewiesen wurde, sollten die Schwellenwerte für den Fall, dass die Volume-Workload gedrosselt wird, auswerten. **Maßnahmen, die bald zu tun sind** Wenn die Warnungsschwelle überschritten wird, planen Sie folgende Sofortmaßnahmen: 1. Wenn der Speicherpool auch eine hohe Auslastung erfährt, verschieben Sie das Volume in einen anderen Speicherpool. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie seine Grenzwerte, falls der Volume-Workload gedrosselt wird. 3. Wenn der Controller auch eine hohe Auslastung aufweist, verschieben Sie das Volume auf einen anderen Controller oder verringern Sie den gesamten Workload des Controllers.	Warnung @ > 6,000 µs kritisch @ > 12,000 µs
Cluster-Speichersättigung Hoch	Die zuteilbare Arbeitsspeichersättigung des Clusters ist hoch. Die Cluster-CPU-Sättigung wird als Summe der Arbeitsspeicherauslastung berechnet, geteilt durch die Summe des zuteilbaren Arbeitsspeichers aller K8s-Nodes.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von Speicher auf Nodes	Warnung @ > 80 % Kritisch @ > 90 %

POD-Anbindung fehlgeschlagen	Dieser Alarm tritt auf, wenn ein Volume-Anhang mit POD fehlgeschlagen ist.		Warnung
Hohe Wiederübertragungsrate	Hohe TCP-Übertragungsrate	Überprüfung auf Netzwerküberlastung – ermitteln von Workloads, die eine hohe Netzwerkbandbreite verbrauchen. Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks.	Warnung @ > 10 % Kritisch @ > 25 %
Kapazität Des Node-Dateisystems Hoch	Kapazität Des Node-Dateisystems Hoch	- Erhöhen Sie die Größe der Knotenplatten, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Verringern Sie die Verwendung von Anwendungsdateien.	Warnung @ > 80 % Kritisch @ > 90 %
Workload-Netzwerk-Jitter Hoch	Hoher TCP Jitter (hohe Latenz/Reaktionszeiten)	Prüfen Sie auf Netzwerküberlastung. Ermittlung von Workloads, die sehr viel Netzwerkbandbreite in Anspruch nehmen Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks	Warnung @ > 30 ms kritisch @ > 50 ms

Durchsatz Bei Persistenten Volumes	MBIT/S-Schwellenwerte auf persistenten Volumes können verwendet werden, um einen Administrator zu benachrichtigen, wenn persistente Volumes die vordefinierten Performance-Erwartungen übertreffen und möglicherweise andere persistente Volumes beeinträchtigen. Durch Aktivieren dieses Monitors werden Warnungen generiert, die für das typische Durchsatzprofil persistenter Volumes auf SSDs geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Monitoring-Zielen angepasst werden, indem dieser Monitor dupliziert und Grenzwerte für Ihre Storage-Klasse angepasst werden. Ein duplizierter Monitor kann zudem auf einen Teil der persistenten Volumes Ihres Mandanten ausgerichtet werden.	**Sofortige Maßnahmen** Wenn der kritische Schwellenwert überschritten wird, planen Sie sofort Maßnahmen, um die Serviceunterbrechung zu minimieren: 1. Einführung von QoS-MBIT/S-Limits für das Volume 2. Überprüfen Sie die Applikation, die für den Workload auf dem Volume verwendet wird, auf Anomalien. **Maßnahmen, die bald zu tun** Wenn Warnschwelle überschritten wird, planen Sie folgende unmittelbare Maßnahmen zu ergreifen: 1. Einführung von QoS-MBIT/S-Limits für das Volume 2. Überprüfen Sie die Applikation, die für den Workload auf dem Volume verwendet wird, auf Anomalien.	Warnung @ > 10,000 MB/s kritisch @ > 15,000 MB/s
Behälter, der Gefahr läuft, OOM zu töten	Die Speichergrenzen des Containers sind zu niedrig eingestellt. Der Container ist in Gefahr der Entfernung (Out of Memory Kill).	Erhöhen Sie die Speichergrenzen des Containers.	Warnung @ > 95 %
Workload-Ausfall	Workload enthält keine funktionstüchtigen Pods.		Kritisch @ < 1
Die Forderung Für Das Persistente Volume Konnte Nicht Verbindlich Sein	Dieser Alarm tritt auf, wenn eine Bindung an einem PVC fehlgeschlagen ist.		Warnung
ResourceQuota Mem Limits Überschreiten	Die Speichergrenzen für Namespace überschreiten ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %

ResourceQuota Mem Requests About to Exceed	Speicheranforderungen für Namespace überschreiten ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Fehler Beim Erstellen Des Node	Der Knoten konnte aufgrund eines Konfigurationsfehlers nicht geplant werden.	Prüfen Sie das Kubernetes-Ereignisprotokoll auf die Ursache des Konfigurationsfehlers.	Kritisch
Die Rückgewinnung Des Persistenten Volumes Ist Fehlgeschlagen	Die automatische Rückgewinnung des Volumes ist fehlgeschlagen.		Warnung @ > 0 B
Container-CPU-Drosselung	Die CPU-Grenzwerte des Containers sind zu niedrig eingestellt. Container-Prozesse werden verlangsamt.	Erhöhen Sie die CPU-Limits für Container.	Warnung @ > 95 % Kritisch @ > 98 %
Fehler beim Löschen des Service Load Balancer			Warnung
Persistente Volume-IOPS	IOPS-Schwellenwerte auf persistenten Volumes können verwendet werden, um einen Administrator zu benachrichtigen, wenn persistente Volumes die vordefinierten Performance-Erwartungen übertreffen. Durch die Aktivierung dieser Überwachung werden Warnungen generiert, die für das typische IOPS-Profil von persistenten Volumes geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Monitoring-Zielen angepasst werden, indem dieser Monitor dupliziert wird und Grenzwerte für Ihren Workload festgelegt werden.	**Sofortige Maßnahmen** Wenn kritische Schwelle überschritten wird, planen Sie sofortige Maßnahmen, um Serviceunterbrechungen zu minimieren : 1. Einführung von QoS-IOPS-Limits für das Volume 2. Überprüfen Sie die Applikation, die für den Workload auf dem Volume verwendet wird, auf Anomalien. **Maßnahmen, die bald zu tun sind** Wenn die Warnungsschwelle überschritten wird, planen Sie folgende Sofortmaßnahmen: 1. Einführung von QoS-IOPS-Limits für das Volume 2. Überprüfen Sie die Applikation, die für den Workload auf dem Volume verwendet wird, auf Anomalien.	Warnung @ > 20,000 IO/s kritisch @ > 25,000 IO/s

Fehler beim Aktualisieren des Service Load Balancer			Warnung
POD-Mount fehlgeschlagen	Diese Warnmeldung tritt auf, wenn ein Mount auf EINEM POD fehlgeschlagen ist.		Warnung
Knoten-PID-Druck	Die verfügbaren Prozesskennungen auf dem Knoten (Linux) sind unter einen Schwellenwert für die Entfernung gefallen.	Suchen und beheben Sie Pods, die viele Prozesse generieren und den Knoten der verfügbaren Prozess-IDs aushungern. Richten Sie PodPidsLimit ein, um Ihren Node vor Pods oder Containern zu schützen, die zu viele Prozesse hervorbringen.	Kritisch @ > 0
Fehler Beim Ziehen Des Pod-Image	Kubernetes konnte das Pod-Container-Image nicht abrufen.	- Stellen Sie sicher, dass das Bild des Pod korrekt in der Pod-Konfiguration geschrieben ist. - Check Image Tag existiert in Ihrer Registry. - Überprüfen Sie die Zugangsdaten für die Image Registry. - Überprüfen Sie auf Registry-Verbindungsprobleme. - Überprüfen Sie, dass Sie nicht die von öffentlichen Registrierungsanbietern auferlegten Ratenlimits erreichen.	Warnung
Job Wird Zu Lang Ausgeführt	Job wird zu lange ausgeführt		Warnung @ > 1 Std. Kritisch @ > 5 Std
Knotenspeicher Hoch	Die Speichernutzung der Nodes ist hoch	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von Speicher auf Nodes	Warnung @ > 85 % Kritisch @ > 90 %
ResourceQuota CPU-Limits Überschreiten	CPU-Limits für Namespace überschreiten ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Pod Crash Loop-Rückmeldung	Pod ist abgestürzt und versucht, es mehrmals neu zu starten.		Kritisch @ > 3

Knoten CPU hoch	CPU-Auslastung der Knoten ist hoch.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von CPU auf Nodes	Warnung @ > 80 % Kritisch @ > 90 %
Workload-Netzwerk-Latenz RTT hoch	Hohe TCP-RTT-Latenz (Round Trip Time)	Auf Netzwerküberlastung prüfen ▒ Workloads identifizieren, die eine hohe Netzwerkbandbreite verbrauchen. Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks.	Warnung @ > 150 ms kritisch @ > 300 ms
Job Fehlgeschlagen	Der Job wurde aufgrund eines Node-Absturzes oder Neubootens, Ressourcenerschöpfung, Job-Zeitüberschreitung oder Fehler bei der POD-Planung nicht erfolgreich abgeschlossen.	Prüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Warnung @ > 1
Persistentes Volume in wenigen Tagen vollständig	Dem persistenten Volume geht in wenigen Tagen der Speicherplatz aus	-Erhöhen Sie die Volumegröße, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. -Reduzieren Sie die Menge der in Anwendungen gespeicherten Daten.	Warnung @ < 8 Tage kritisch @ < 3 Tage
Speicherdruck Des Node	Dem Node geht der Speicher aus. Der verfügbare Speicher hat den Schwellenwert für die Entfernung erreicht.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von Speicher auf Nodes	Kritisch @ > 0
Knoten Nicht Bereit	Der Node war 5 Minuten lang nicht bereit	Überprüfen Sie, ob der Node über genügend CPU-, Arbeitsspeicher- und Festplattenressourcen verfügt. Prüfen Sie die Konnektivität des Node-Netzwerks. Prüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Kritisch @ < 1

Kapazität Des Persistenten Volumes Hoch	Die von einem persistenten Volume genutzte Back-End-Kapazität ist hoch.	- Erhöhen Sie die Volume-Größe, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Reduzierung der in Anwendungen gespeicherten Datenmenge.	Warnung @ > 80 % Kritisch @ > 90 %
Fehler beim Erstellen des Service Load Balancer	Erstellen Des Service Load Balancer Fehlgeschlagen		Kritisch
Workload-Replikatfehler	Einige Pods sind derzeit nicht für eine Bereitstellung oder ein DemonSet verfügbar.		Warnung @ > 1
ResourceQuota CPU Requests About to Exceed	CPU-Anforderungen für Namespace überschreiten ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Hohe Wiederübertragungsrate	Hohe TCP-Übertragungsrate	Überprüfung auf Netzwerküberlastung – ermitteln von Workloads, die eine hohe Netzwerkbandbreite verbrauchen. Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks.	Warnung @ > 10 % Kritisch @ > 25 %
Node-Festplattendruck	Verfügbarer Speicherplatz und Inodes auf dem Root-Dateisystem des Knotens oder dem Image-Dateisystem haben einen Schwellenwert für die Entfernung erreicht.	- Erhöhen Sie die Größe der Knotenplatten, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Verringern Sie die Verwendung von Anwendungsdateien.	Kritisch @ > 0
Cluster-CPU-Sättigung hoch	Cluster-zuteilbare CPU-Sättigung ist hoch. Die Cluster-CPU-Sättigung wird als Summe der CPU-Auslastung berechnet, geteilt durch die Summe der zuteilbaren CPU aller K8s-Nodes.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von CPU auf Nodes	Warnung @ > 80 % Kritisch @ > 90 %

Zurück nach oben

Protokollmonitore Ändern

Monitorname	Schweregrad	Beschreibung Des Monitors
Internes Volume Erkannt	Informativ	Diese Meldung tritt auf, wenn ein internes Volume erkannt wird.
Internes Volume Geändert	Informativ	Diese Meldung tritt auf, wenn ein internes Volume geändert wird.
Storage-Node Erkannt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknoten erkannt wird.
Speicherknoten Entfernt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknoten entfernt wird.
Speicherpool Erkannt	Informativ	Diese Meldung tritt auf, wenn ein Speicherpool erkannt wird.
Erkannte Storage Virtual Machine	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine erkannt wird.
Storage Virtual Machine Geändert	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine geändert wird.

Zurück nach oben

Datenerfassungsmonitore

Monitorname	Beschreibung	Korrekturmaßnahme
Herunterfahren Der Erfassungseinheit	Data Infrastructure Insights Acquisition Units werden regelmäßig im Rahmen von Upgrades neu gestartet, um neue Funktionen einzuführen. Dies geschieht einmal pro Monat oder weniger in einer typischen Umgebung. Eine Warnung, dass eine Erfassungseinheit heruntergefahren wurde, sollte bald darauf mit einer Auflösung folgen, die feststellt, dass die neu neu neu neu aufgestartete Erfassungseinheit eine Registrierung bei Data Infrastructure Insights abgeschlossen hat. In der Regel dauert dieser Vorgang beim Herunterfahren bis zur Registrierung 5 bis 15 Minuten.	Wenn der Alarm häufig auftritt oder länger als 15 Minuten dauert, überprüfen Sie den Betrieb des Systems, das die Erfassungseinheit, das Netzwerk und einen beliebigen Proxy hostet, der die AU mit dem Internet verbindet.

Collector Fehlgeschlagen	Bei der Abfrage eines Datensammlers ist eine unerwartete Fehlersituation aufgetreten.	Weitere Informationen zur Situation finden Sie auf der Seite Datensammler unter Data Infrastructure Insights.
Sammlerwarnung	Dieser Alarm kann in der Regel aufgrund einer fehlerhaften Konfiguration des Datensammlers oder des Zielsystems auftreten. Überprüfen Sie die Konfigurationen, um zukünftige Warnmeldungen zu vermeiden. Es kann auch durch einen Abruf von weniger als vollständigen Daten, wo der Datensammler alle Daten, die es konnte gesammelt werden. Dies kann vorkommen, wenn sich während der Datenerfassung Situationen ändern (z. B. wird während der Datenerfassung eine zu Beginn der Datenerfassung vorhandene virtuelle Maschine gelöscht und vor der Erfassung der Daten).	Überprüfen Sie die Konfiguration des Datensammlers oder Zielsystems. Beachten Sie, dass der Monitor für Collector-Warnung mehr Warnmeldungen als andere Monitortypen senden kann. Es wird daher empfohlen, keine Alarmempfänger festzulegen, es sei denn, Sie beheben die Fehlerbehebung.

Zurück nach oben

Sicherheitsmonitore

Monitorname	Schwellenwert	Beschreibung Des Monitors	Korrekturmaßnahme
AutoSupport HTTPS-Transport deaktiviert	Warnung @ < 1	AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.	Um HTTPS als Transportprotokoll für AutoSupport Meldungen festzulegen, führen Sie den folgenden ONTAP-Befehl aus:…System Node AutoSupport modify -Transport https
Cluster unsichere Chiffren für SSH	Warnung @ < 1	Gibt an, dass SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP-Befehl aus:…Security ssh remove -vserver <admin vserver> -Chiffers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc

Das Cluster-Anmelde-Banner Ist Deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer, die auf das ONTAP-System zugreifen, deaktiviert ist. Die Anzeige eines Anmeldebanners ist hilfreich, um die Erwartungen für den Zugriff und die Verwendung des Systems zu stellen.	Führen Sie zum Konfigurieren des Anmeldebanns für ein Cluster den folgenden ONTAP-Befehl aus:…Security Login Banner modify -vserver <admin svm> -message „Zugriff auf autorisierte Benutzer beschränkt“.
Cluster-Peer-Kommunikation Ist Nicht Verschlüsselt	Warnung @ < 1	Bei der Replizierung von Daten für Disaster Recovery, Caching oder Backup müssen die Daten während der Übertragung über das Netzwerk von einem ONTAP Cluster zum anderen gesichert werden. Die Verschlüsselung muss sowohl auf den Quell- als auch auf den Ziel-Clustern konfiguriert sein.	Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, muss das Quell- und Ziel-Cluster auf 9.6 aktualisiert werden. Verwenden Sie dann den Befehl „Cluster Peer modify“, um sowohl die Quell- als auch die Ziel-Cluster-Peering-Verschlüsselung zu ändern.…Details finden Sie im NetApp Security Hardening Guide for ONTAP 9.
Lokaler Admin-Standardbenutzer Aktiviert	Warnung @ > 0	NetApp empfiehlt, alle nicht benötigten Standard-Admin-Benutzer (integriert) mit dem Sperrbefehl zu sperren (zu deaktivieren). Es handelt sich dabei in erster Linie um Standardkonten, für die Passwörter nie aktualisiert oder geändert wurden.	Um das integrierte „admin“-Konto zu sperren, führen Sie den folgenden ONTAP-Befehl aus:…Security Login Lock -username admin
FIPS-Modus deaktiviert	Warnung @ < 1	Wenn die FIPS 140-2-Konformität aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn die FIPS 140-2-Compliance aktiviert ist.	Führen Sie zum Aktivieren der FIPS 140-2-Compliance auf einem Cluster den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security config modify -Interface SSL -is -fips-enabled true

Protokollweiterleitung Nicht Verschlüsselt	Warnung @ < 1	Das verlagern von Syslog-Informationen ist nötig, um den Umfang oder die Auswirkungen einer Sicherheitsverletzung auf ein einzelnes System oder eine einzelne Lösung zu beschränken. Daher empfiehlt NetApp, Syslog-Informationen sicher an einen sicheren Storage- oder Aufbewahrungsort zu verlagern.	Nach dem Erstellen eines Protokollweiterleitungsziel s kann sein Protokoll nicht mehr geändert werden. Wenn Sie zu einem verschlüsselten Protokoll wechseln möchten, löschen Sie das Ziel für die Protokollweiterleitung und erstellen Sie es mit dem folgenden ONTAP-Befehl:…Cluster log-fording create -Destination <Ziel-ip> -Protocol tcp-Encrypted
MD5-Kennwort gehasht	Warnung @ > 0	NetApp empfiehlt dringend, die sicherere SHA-512-Hash-Funktion für Passwörter für ONTAP-Benutzerkonten zu nutzen. Konten, die die weniger sichere MD5-Hash-Funktion verwenden, sollten auf die SHA-512-Hash-Funktion migriert werden.	NetApp empfiehlt Benutzerkonten, zur sichereren SHA-512-Lösung zu migrieren, indem Benutzer ihre Passwörter ändern.…um Konten mit Passwörtern zu sperren, die die MD5-Hash-Funktion verwenden, führen Sie den folgenden ONTAP-Befehl aus:…Security Login Lock -vserver * -username * -Hash -function md5
Es sind keine NTP-Server konfiguriert	Warnung @ < 1	Gibt an, dass auf dem Cluster keine konfigurierten NTP-Server vorhanden sind. Aus Gründen der Redundanz und des optimalen Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Um einen NTP-Server mit dem Cluster zu verknüpfen, führen Sie den folgenden ONTAP-Befehl aus: Cluster Time-Service ntp-Server create -Server <ntp-Server Host-Name oder ip-Adresse>
Die Anzahl der NTP-Server ist niedrig	Warnung @ < 3	Gibt an, dass auf dem Cluster weniger als 3 konfigurierte NTP-Server vorhanden sind. Aus Gründen der Redundanz und des optimalen Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Führen Sie den folgenden ONTAP-Befehl aus, um einen NTP-Server mit dem Cluster zu verknüpfen:…Cluster Time-Service ntp-Server create -Server <ntp-Server-Hostname oder ip-Adresse>

Remote Shell Aktiviert	Warnung @ > 0	Remote Shell ist keine sichere Methode zum Einrichten von Befehlszeilenzugriff auf die ONTAP Lösung. Die Remote-Shell sollte für einen sicheren Remote-Zugriff deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Remote-Zugriff.…um die Remote Shell auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security Protocol modify -Application rsh-enabled false
Überwachungsprotokoll für Storage VM ist deaktiviert	Warnung @ < 1	Gibt an, dass die Überwachungsprotokollierung für SVM deaktiviert ist.	Um das Überwachungsprotokoll für einen vserver zu konfigurieren, führen Sie den folgenden ONTAP-Befehl aus:…vserver Audit enable -vserver <svm>
Storage VM unsichere Chiffren für SSH	Warnung @ < 1	Gibt an, dass SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP-Befehl aus:…Security ssh remove -vserver <vserver> -Chiffers aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc
Anmeldebanner für Storage VM deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer, die auf SVMs auf dem System zugreifen, deaktiviert ist. Die Anzeige eines Anmeldebanners ist hilfreich, um die Erwartungen für den Zugriff und die Verwendung des Systems zu stellen.	Führen Sie zum Konfigurieren des Anmeldebanns für ein Cluster den folgenden ONTAP-Befehl aus:…Security Login Banner modify -vserver <svm> -message „Zugriff auf autorisierte Benutzer beschränkt“.

Telnet-Protokoll Aktiviert	Warnung @ > 0	Telnet ist keine sichere Methode zum Einrichten von Befehlszeilenzugriff auf die ONTAP-Lösung. Telnet sollte für den sicheren Remote-Zugriff deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff. Um Telnet auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security Protocol modify -Application telnet -enabled false

Zurück nach oben

Datensicherung Überwacht

Monitorname	Schwellenwerte	Beschreibung Des Monitors	Korrekturmaßnahme

Nicht genügend Speicherplatz für LUN Snapshot Kopie	(Filter contains_luns = ja) Warnung @ > 95 %…kritisch @ > 100 %	Die Storage-Kapazität eines Volumes ist erforderlich, um Applikations- und Kundendaten zu speichern. Ein Teil dieses Speicherplatzes, der als reservierter Snapshot-Speicherplatz bezeichnet wird, wird zum Speichern von Snapshots verwendet, mit denen Daten lokal gesichert werden können. Je mehr neue und aktualisierte Daten in dem ONTAP Volume gespeichert sind, desto mehr Snapshot-Kapazität wird benötigt und weniger Snapshot Storage-Kapazität wird für zukünftige neue oder aktualisierte Daten zur Verfügung stehen. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reserveplatz erreicht, kann dies dazu führen, dass der Kunde nicht in der Lage ist, neue Snapshot-Daten zu speichern und den Schutz der Daten in den LUNs im Volume zu verringern. Durch das Monitoring der verwendeten Snapshot-Kapazität des Volumes wird die Kontinuität der Datendienste gewährleistet.	**Sofortmaßnahmen** bei Überschreitung kritischer Schwelle sollten sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen in Betracht gezogen werden: 1. Konfigurieren Sie Snapshots so, dass der Datenplatz im Volume genutzt wird, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere unerwünschte Snapshots, um Speicherplatz freizugeben. **Maßnahmen, die bald zu tun** Wenn Warnschwelle überschritten wird, planen Sie folgende unmittelbare Maßnahmen zu ergreifen: 1. Erhöhen Sie den Speicherplatz der Snapshot Reserve innerhalb des Volumes, um dem Wachstum gerecht zu werden. 2. Konfigurieren Sie Snapshots so, dass der Datenplatz im Volume genutzt wird, wenn die Snapshot-Reserve voll ist.

SnapMirror BeziehungsVerzögerungen	Warnung @ > 150 %…Kritisch @ > 300 %	Die SnapMirror Beziehungsverzögerung ist der Unterschied zwischen dem Snapshot-Zeitstempel und der Zeit auf dem Zielsystem. Die lag_time_percent ist das Verhältnis der Verzögerungszeit zum Zeitplan-Intervall der SnapMirror Richtlinie. Wenn die Verzögerungszeit dem Zeitungsintervall entspricht, ist lag_time_percent 100 %. Wenn die SnapMirror-Richtlinie keinen Zeitplan enthält, wird lag_time_percent nicht berechnet.	Überwachen Sie den SnapMirror-Status mit dem Befehl „snapmirror show“. Überprüfen Sie den SnapMirror Übertragungsverlauf mithilfe des Befehls „snapmirror show-history“

Zurück nach oben

Cloud Volume (CVO) – Überwachung

Monitorname	Severity	Beschreibung Des Monitors	Korrekturmaßnahme
CVO Disk out of Service	INFO	Dieses Ereignis tritt auf, wenn eine Festplatte aus dem Dienst entfernt wird, weil sie als fehlgeschlagen markiert, desinfiziert oder das Maintenance Center aufgerufen wurde.	Keine

CVO Giveback vom Speicherpool fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Storage Failover (SFO)-Rückgabe auf, wenn der Ziel-Node nicht auf die Objektspeicher zugreifen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Vergewissern Sie sich, dass Ihre Intercluster LIF online und funktionsfähig ist, indem Sie den Befehl „Network Interface show“ verwenden. Überprüfen Sie die Netzwerkverbindung mit dem Objektspeicher-Server mithilfe des „Ping“-Befehls über das Ziel-Node Intercluster LIF. Überprüfen Sie, ob sich die Konfiguration Ihres Objektspeichers nicht geändert hat und ob die Login- und Konnektivitätsinformationen noch korrekt sind, indem Sie den Befehl „Aggregate object-Store config show“ verwenden. Alternativ können Sie den Fehler überschreiben, indem Sie beim Giveback-Befehl „false-Partner-waiting“-Parameter angeben. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

CVO HA Interconnect herunter	WARNUNG	Der HA Interconnect ist ausgefallen. Risiko eines Serviceausfalls, wenn ein Failover nicht verfügbar ist.	Korrekturmaßnahmen hängen von der Anzahl und der Art der von der Plattform unterstützten HA Interconnect Links ab sowie vom Grund für einen Ausfall des Interconnect. Wenn die Links ausgefallen sind: Vergewissern Sie sich, dass beide Controller im HA-Paar betriebsbereit sind. Stellen Sie bei extern angeschlossenen Verbindungen sicher, dass die Verbindungskabel ordnungsgemäß angeschlossen sind und dass die Small Form-Factor Pluggables (SFPs), falls zutreffend, ordnungsgemäß auf beiden Controllern eingesetzt werden. Deaktivieren und aktivieren Sie bei intern verbundenen Verbindungen die Links nacheinander, indem Sie die Befehle „IC Link off“ und „ic Link On“ verwenden. Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl „IC Link on“. Wenn ein Peer nicht verbunden ist, deaktivieren und aktivieren Sie die Links nacheinander, indem Sie die Befehle „IC Link off“ und „ic Link ON“ verwenden. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.

CVO max. Sitzungen pro Benutzer überschritten	WARNUNG	Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anforderung zum Errichten einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie alle Anwendungen, die auf dem Client ausgeführt werden, und beenden Sie alle, die nicht ordnungsgemäß funktionieren. Booten Sie den Client neu. Prüfen Sie, ob das Problem durch eine neue oder bestehende Anwendung verursacht wird: Wenn die Anwendung neu ist, legen Sie einen höheren Schwellenwert für den Client fest, indem Sie den Befehl „cifs Option modify -max-opens-same-file-per -tree“ verwenden. In einigen Fällen arbeiten Clients wie erwartet, erfordern jedoch einen höheren Schwellenwert. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. Wenn das Problem durch eine vorhandene Anwendung verursacht wird, kann es zu einem Problem mit dem Client kommen. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

CVO NetBIOS-Name-Konflikt	KRITISCH	Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Anfrage zur Namensregistrierung erhalten. Dies wird typischerweise durch einen Konflikt mit dem NetBIOS-Namen oder einem Alias verursacht. Infolgedessen können Clients möglicherweise nicht auf Daten zugreifen oder eine Verbindung mit dem richtigen Datenservice-Node im Cluster herstellen.	Führen Sie eine der folgenden Korrekturmaßnahmen durch: Falls ein Konflikt mit dem NetBIOS-Namen oder einem Alias besteht, führen Sie eine der folgenden Schritte aus: Löschen Sie den doppelten NetBIOS-Alias, indem Sie den Befehl "vserver cifs delete -aliases alias -vserver vServer" verwenden. Benennen Sie einen NetBIOS-Alias um, indem Sie den doppelten Namen löschen und einen Alias mit einem neuen Namen mit dem Befehl „vserver cifs create -aliases alias -vServer vServer“ hinzufügen. Wenn keine Aliase konfiguriert sind und es einen Konflikt im NetBIOS-Namen gibt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -Server netbiosname“ um. HINWEIS: Das Löschen eines CIFS-Servers kann auf Daten zugreifen. Entfernen Sie den NetBIOS-Namen, oder benennen Sie das NetBIOS auf dem Remotecomputer um.
CVO NFSv4 Store Pool ist nicht vorhanden	KRITISCH	Ein NFSv4-Speicherpool wurde erschöpft.	Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht mehr reagiert, wenden Sie sich an den technischen Support von NetApp.
Panik des CVO-Knotens	WARNUNG	Dieses Ereignis wird ausgegeben, wenn ein Panikzustand eintritt	Wenden Sie sich an den NetApp Kundensupport.

CVO Node Root-Volume-Speicherplatz niedrig	KRITISCH	Das System hat festgestellt, dass das Root-Volumen über einen gefährlich niedrigen Speicherplatz verfügt. Der Node ist nicht vollständig betriebsbereit. Daten-LIFs sind möglicherweise ein Failover innerhalb des Clusters durchgeführt, da der NFS- und CIFS-Zugriff auf den Node begrenzt ist. Die administrative Funktion ist auf lokale Recovery-Verfahren beschränkt, um Speicherplatz auf dem Root-Volume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch: Geben Sie Speicherplatz auf dem Root-Volume frei, indem Sie alte Snapshot-Kopien löschen, nicht mehr benötigte Dateien aus dem /mroot-Verzeichnis löschen oder die Root-Volume-Kapazität erweitern. Booten Sie den Controller neu. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.
CVO – nicht vorhandene Admin-Freigabe	KRITISCH	Vscan-Problem: Ein Kunde hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN-Freigabe zu herstellen.	Stellen Sie sicher, dass Vscan für die erwähnte SVM-ID aktiviert ist. Wenn Sie Vscan auf einer SVM aktivieren, wird die Dateifreigabe von ONTAP_ADMIN automatisch für die SVM erstellt.
CVO Object Store Host nicht lösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicher-Client kann nicht mit dem Objektspeicher-Server kommunizieren, ohne sich auf eine IP-Adresse zu lösen. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Überprüfen Sie die DNS-Konfiguration, um zu überprüfen, ob der Hostname mit einer IP-Adresse korrekt konfiguriert ist.

CVO Object Store Intercluster LIF ausgefallen	KRITISCH	Der Objektspeicher-Client kann keine funktionsfähige LIF finden, die mit dem Objektspeicher-Server kommunizieren kann. Der Node ermöglicht dem Client-Datenverkehr zwischen Objekten erst dann, wenn die Intercluster LIF funktionsfähig ist. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Führen Sie die folgenden Korrekturmaßnahmen durch: Prüfen Sie den LIF-Intercluster-Status mithilfe des Befehls „Network Interface show -role intercluster“. Überprüfen Sie, ob die Intercluster-LIF ordnungsgemäß konfiguriert und betriebsbereit ist. Wenn eine Intercluster-LIF nicht konfiguriert ist, fügen Sie sie mithilfe des Befehls „Network Interface create -role intercluster“ hinzu.
Signature des CVO-Objektspeichern stimmt nicht überein	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Aus diesem Grund ist der Zugriff auf Daten möglicherweise nicht möglich.	Vergewissern Sie sich, dass der Schlüssel für den geheimen Zugriff richtig konfiguriert ist. Wenn er korrekt konfiguriert ist, wenden Sie sich an den technischen Support von NetApp, um Hilfe zu erhalten.
Speicherzuordnung von CVO QoS Monitor	KRITISCH	Der dynamische Speicher des QoS-Subsystems hat die Grenze für die aktuelle Plattform-Hardware erreicht. Einige QoS-Funktionen können mit einer begrenzten Kapazität betrieben werden.	Löschen Sie einige aktive Workloads oder Streams, um Speicher freizumachen. Bestimmen Sie mithilfe des Befehls „Statistics show -object Workload -counter ops“, welche Workloads aktiv sind. Aktive Workloads weisen keine Vorgänge auf. Verwenden Sie dann mehrmals den Befehl „Workload delete <Workload_Name>“, um bestimmte Workloads zu entfernen. Alternativ können Sie mit dem Befehl „Stream delete -Workload <Workload Name> *“ die zugeordneten Streams aus dem aktiven Workload löschen.

Zeitüberschreitung FÜR CVO-LESEDIUM	KRITISCH	Ein VORGANG DER READDIR-Datei hat die Zeitüberschreitung überschritten, die in WAFL ausgeführt werden darf. Dies kann wegen sehr großer oder spärlicher Verzeichnisse erfolgen. Eine Korrekturmaßnahme wird empfohlen.	Führen Sie die folgenden Korrekturmaßnahmen durch: Suchen Sie Informationen, die für aktuelle Verzeichnisse spezifisch sind, bei denen READDIR-Dateivorgänge ablaufen, indem Sie den folgenden Befehl 'diag' Privilege nodeshell CLI verwenden: WAFL readdir notice show. Prüfen Sie, ob Verzeichnisse als wenig angezeigt werden oder nicht: Wenn ein Verzeichnis als wenig angegeben wird, wird empfohlen, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die Sparseness der Verzeichnisdatei zu entfernen. Wenn ein Verzeichnis nicht als dünn angegeben wird und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem die Anzahl der Dateieinträge im Verzeichnis verringert wird.

CVO-Verlagerung des Speicherpools fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Ziel-Node nicht die Objektspeicher erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Vergewissern Sie sich, dass Ihre Intercluster LIF online und funktionsfähig ist, indem Sie den Befehl „Network Interface show“ verwenden. Überprüfen Sie die Netzwerkverbindung mit dem Objektspeicher-Server mithilfe des „Ping“-Befehls über das Ziel-Node Intercluster LIF. Überprüfen Sie, ob sich die Konfiguration Ihres Objektspeichers nicht geändert hat und ob die Login- und Konnektivitätsinformationen noch korrekt sind, indem Sie den Befehl „Aggregate object-Store config show“ verwenden. Alternativ können Sie den Fehler über den Parameter „Override-Destination-Checks“ des Befehls „Relocation“ überschreiben. Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.

CVO Shadow Copy fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Backup- und Wiederherstellungsdienst für Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie Folgendes anhand der in der Ereignismeldung angegebenen Informationen: Ist die Konfiguration der Schattenkopie aktiviert? Sind die entsprechenden Lizenzen installiert? Auf welchen Freigaben wird der Schattenkopiervorgang durchgeführt? Ist der Share-Name korrekt? Gibt es den Share-Pfad? Wie lauten die Zustände des Schattenkopie-Satzes und seiner Schattenkopien?
CVO Storage VM Stop erfolgreich durchgeführt	INFO	Diese Meldung tritt auf, wenn eine Operation „vserver stop“ erfolgreich ist.	Verwenden Sie den Befehl „vserver Start“, um den Datenzugriff auf einer Storage-VM zu starten.
CVO zu viele CIFS-Authentifizierung	WARNUNG	Viele Authentifizierungsverhandlungen sind gleichzeitig aufgetreten. Es gibt 256 unvollständige neue Sitzungsanfragen dieses Kunden.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanfragen erstellt hat. Möglicherweise müssen Sie den Anbieter des Clients oder der Anwendung kontaktieren, um festzustellen, warum der Fehler aufgetreten ist.
Nicht zugewiesene CVO-Festplatten	INFO	System verfügt über nicht zugewiesene Festplatten – Kapazität wird verschwendet. Möglicherweise ist bei Ihrem System eine fehlerhafte Konfiguration oder ein Teil der Konfigurationsänderungen zu finden.	Führen Sie die folgenden Korrekturmaßnahmen durch: Bestimmen Sie mithilfe des Befehls „Disk show -n“, welche Festplatten nicht zugewiesen werden. Weisen Sie die Festplatten einem System über den Befehl „Disk assign“ zu.

CVO nicht autorisierter Benutzerzugriff auf die Administratorfreigabe	WARNUNG	Ein Kunde hat versucht, eine Verbindung zu der privilegierten Version von ONTAP_ADMIN herzustellen, obwohl der angemeldete Benutzer kein berechtigter Benutzer ist.	Führen Sie die folgenden Korrekturmaßnahmen durch: Stellen Sie sicher, dass der angegebene Benutzername und die IP-Adresse in einem der aktiven Vscan-Scannerpools konfiguriert sind. Überprüfen Sie die Konfiguration des Scannerpools, die derzeit aktiv ist, indem Sie den Befehl „vserver vscan Scanner Pool show-Active“ verwenden.
CVO-Virus erkannt	WARNUNG	Ein Vscan-Server hat einen Fehler an das Speichersystem gemeldet. Dies bedeutet in der Regel, dass ein Virus gefunden wurde. Andere Fehler auf dem Vscan-Server können jedoch dieses Ereignis verursachen. Der Client-Zugriff auf die Datei wird verweigert. Der Vscan-Server kann je nach Einstellungen und Konfiguration die Datei bereinigen, in Quarantäne stellen oder löschen.	Prüfen Sie das Protokoll des Vscan-Servers, der im Ereignis „syslog“ gemeldet wurde, um zu sehen, ob die infizierte Datei erfolgreich bereinigt, isoliert oder gelöscht werden konnte. Wenn dies nicht möglich war, muss der Systemadministrator die Datei möglicherweise manuell löschen.
CVO Volume offline	INFO	Diese Meldung gibt an, dass ein Volume offline geschaltet wird.	Versetzen Sie das Volume wieder in den Online-Modus.
CVO-Volume beschränkt	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volume eingeschränkt wird.	Versetzen Sie das Volume wieder in den Online-Modus.

Zurück nach oben

SnapMirror für Business Continuity (SMBC) Mediator Log Monitore

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
ONTAP Mediator hinzugefügt	INFO	Diese Meldung tritt auf, wenn ONTAP Mediator erfolgreich in einem Cluster hinzugefügt wurde.	Keine

Zugriff auf ONTAP Mediator nicht möglich	KRITISCH	Diese Meldung tritt auf, wenn entweder der ONTAP Mediator neu verwendet wird oder das Mediator-Paket nicht mehr auf dem Mediator-Server installiert ist. Daher ist ein SnapMirror Failover nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.
ONTAP Mediator entfernt	INFO	Diese Meldung tritt auf, wenn der ONTAP Mediator erfolgreich aus einem Cluster entfernt wurde.	Keine
ONTAP Mediator nicht erreichbar	WARNUNG	Diese Meldung tritt auf, wenn der ONTAP-Mediator auf einem Cluster nicht erreichbar ist. Daher ist ein SnapMirror Failover nicht möglich.	Überprüfen Sie die Netzwerkverbindung zum ONTAP Mediator mithilfe der Befehle „Netzwerk ping“ und „Network traceroute“. Wenn das Problem weiterhin besteht, entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.
SMBC CA-Zertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) abgelaufen ist. Dadurch wird eine weitere Kommunikation zum ONTAP Mediator nicht möglich sein.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Aktualisieren eines neuen CA-Zertifikats auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.

SMBC CA-Zertifikat läuft ab	WARNUNG	Diese Meldung erscheint, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) innerhalb der nächsten 30 Tage ausläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Aktualisieren eines neuen CA-Zertifikats auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.
SMBC-Clientzertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das Zertifikat des ONTAP Mediator-Clients abgelaufen ist. Dadurch wird eine weitere Kommunikation zum ONTAP Mediator nicht möglich sein.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.
SMBC-Clientzertifikat läuft ab	WARNUNG	Diese Meldung tritt auf, wenn das ONTAP Mediator-Clientzertifikat innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.

SMBC-Beziehung aus Sync Hinweis: UM hat diese nicht	KRITISCH	Diese Meldung erscheint, wenn eine SnapMirror for Business Continuity (SMBC)-Beziehung den Status „in-Sync“ zu „out-of-Sync“ ändert. Aufgrund dieser RPO=0 wird die Datensicherung unterbrochen.	Überprüfen Sie die Netzwerkverbindung zwischen Quell- und Ziel-Volumes. Überwachen Sie den SMBC-Beziehungsstatus mithilfe des Befehls „snapmirror show“ auf dem Ziel und unter Verwendung des Befehls „snapmirror list-destinations“ auf der Quelle. Die automatische Neusynchronisierung versucht, die Beziehung wieder auf den Status „im synchronen“ zu bringen. Falls die Resynchronisierung fehlschlägt, überprüfen Sie, ob alle Nodes im Cluster sich im Quorum befinden und sich in einem ordnungsgemäßen Zustand befinden.
SMBC-Serverzertifikat abgelaufen	KRITISCH	Diese Meldung tritt auf, wenn das Zertifikat des ONTAP Mediator-Servers abgelaufen ist. Dadurch wird eine weitere Kommunikation zum ONTAP Mediator nicht möglich sein.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Aktualisieren eines neuen Serverzertifikats auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.
SMBC-Serverzertifikat läuft ab	WARNUNG	Diese Meldung tritt auf, wenn das Zertifikat des ONTAP Mediator-Servers innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mithilfe des Befehls „snapmirror Mediator remove“. Aktualisieren eines neuen Serverzertifikats auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator mit dem Befehl „snapmirror Mediator add“ neu.

Zurück nach oben

Zusätzliche Monitore für Stromversorgung, Heartbeat und Sonstiges System

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
Erkannte Festplatten-Shelf-Stromversorgung	INFORMATIV	Diese Meldung tritt auf, wenn dem Festplatten-Shelf ein Netzteil hinzugefügt wird.	KEINE
Netzteil Der Platten-Shelfs Entfernt	INFORMATIV	Diese Meldung tritt auf, wenn ein Netzteil aus dem Festplatten-Shelf entfernt wird.	KEINE
MetroCluster Automatische ungeplante Umschaltung deaktiviert	KRITISCH	Diese Meldung tritt auf, wenn die Funktion zur automatischen ungeplanten Umschaltung deaktiviert ist.	Führen Sie den Befehl „MetroCluster modify -Node-Name <nodename> -automatic -Switchover-onFailure True“ für jeden Node im Cluster aus, um die automatische Umschaltung zu ermöglichen.
MetroCluster Speicherbrücke nicht erreichbar	KRITISCH	Die Speicherbrücke ist über das Managementnetzwerk nicht erreichbar	1) Wenn die Bridge durch SNMP überwacht wird, überprüfen Sie, ob die Knoten-Management-LIF über den Befehl „Network Interface show“ verfügt. Stellen Sie sicher, dass die Bridge aktiv ist, indem Sie den Befehl „Network ping“ verwenden. 2) Wenn die Bridge im Band überwacht wird, überprüfen Sie die Fabric-Verkabelung zur Bridge und stellen Sie dann sicher, dass die Bridge eingeschaltet ist.
MetroCluster-Brückentemperatur anormal - unter kritisch	KRITISCH	Der Sensor auf der Fibre Channel-Bridge meldet eine Temperatur, die unter dem kritischen Schwellenwert liegt.	1) Überprüfen Sie den Betriebsstatus der Lüfter auf der Speicherbrücke. 2) Überprüfen Sie, ob die Brücke unter den empfohlenen Temperaturbedingungen funktioniert.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
MetroCluster-Brückentemperatur anormal - über kritisch	KRITISCH	Der Sensor auf der Fibre Channel-Bridge meldet eine Temperatur, die über dem kritischen Schwellenwert liegt.	1) Überprüfen Sie den Betriebsstatus des Chassis-Temperatursensor auf der Storage Bridge mit dem Befehl „Storage Bridge show -cooling“. 2) Überprüfen Sie, ob die Speicherbrücke unter den empfohlenen Temperaturbedingungen funktioniert.
MetroCluster Aggregat links ab	WARNUNG	Das Aggregat wurde während des Umschalttaschens zurückgelassen.	1) Überprüfen Sie den Aggregatzustand mit dem Befehl „aggr show“. 2) Wenn das Aggregat online ist, geben Sie es mit dem Befehl „MetroCluster switchback“ an seinen ursprünglichen Eigentümer zurück.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
Alle Links zwischen MetroCluster-Partnern sind ausgefallen	KRITISCH	RDMA Interconnect-Adapter und Intercluster LIFs haben beschädigte Verbindungen mit dem Peering-Cluster bzw. der Peering-Cluster ist ausgefallen.	1) Stellen Sie sicher, dass die Intercluster LIFs betriebsbereit sind und ausgeführt werden. Reparieren Sie die Intercluster-LIFs, wenn sie ausgefallen sind. 2) Überprüfen Sie, ob der Peering-Cluster mit dem Befehl „Cluster Peer ping“ betriebsbereit ist und ausgeführt wird. Sollte das Peering Cluster ausfallen, sind Sie im MetroCluster Leitfaden für Disaster Recovery zu finden. 3) Überprüfen Sie bei Fabric MetroCluster, ob die ISLs der Back-End-Fabric-Strategie verfügbar sind. Reparieren Sie die ISLs des Back-End Fabric, wenn sie ausgefallen sind. 4) Überprüfen Sie bei nicht-Fabric-Konfigurationen mit MetroCluster, ob die Verkabelung zwischen den RDMA Interconnect Adaptern korrekt ist. Konfigurieren Sie die Verkabelung neu, wenn die Links ausgefallen sind.
MetroCluster Partner über Peering-Netzwerk nicht erreichbar	KRITISCH	Die Konnektivität zum Peer-Cluster ist unterbrochen.	1) Stellen Sie sicher, dass der Port mit dem richtigen Netzwerk/Switch verbunden ist. 2) Stellen Sie sicher, dass die Intercluster LIF mit dem Peering Cluster verbunden ist. 3) Stellen Sie sicher, dass der Peering-Cluster durch den Befehl „Cluster Peer ping“ betriebsbereit ist und ausgeführt wird. Sollte das Peering Cluster ausfallen, lesen Sie den MetroCluster Leitfaden für Disaster Recovery nach.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
MetroCluster Inter Schalten Sie alle Verbindungen ab	KRITISCH	Alle Inter-Switch Links (ISLs) auf dem Storage Switch sind ausgefallen.	1) Reparieren Sie die ISLs des Back-End Fabric auf dem Storage Switch. 2) sicherstellen dass der Partner-Switch an ist und seine ISLs betriebsbereit sind. 3) sicherstellen, dass Zwischengeräte, wie z.B. xWDM-Geräte, betriebsbereit sind.
Link zu MetroCluster-Knoten zu Storage-Stack SAS ausgefallen	WARNUNG	Der SAS-Adapter oder das angeschlossene Kabel befinden sich möglicherweise auf dem Fehler.	1. Vergewissern Sie sich, dass der SAS-Adapter online ist und ausgeführt wird. 2. Überprüfen Sie, ob die physische Kabelverbindung sicher und in Betrieb ist, und ersetzen Sie das Kabel ggf.. 3. Wenn der SAS-Adapter mit Festplatten-Shelfs verbunden ist, stellen Sie sicher, dass EAMs und Festplatten ordnungsgemäß eingesetzt sind.
MetroClusterFC Initiator Links ausgefallen	KRITISCH	Der FC-Initiator-Adapter befindet sich auf einem Fehler.	1. Stellen Sie sicher, dass der FC-Initiator-Link nicht manipuliert wurde. 2. Überprüfen Sie den Betriebsstatus des FC Initiator-Adapters mit dem Befehl „System Node run -Node local -command Storage show Adapter“.
FC-VI Interconnect-Link ausgefallen	KRITISCH	Die physische Verbindung auf dem FC-VI-Port ist offline.	1. Stellen Sie sicher, dass der FC-VI-Link nicht manipuliert wurde. 2. Überprüfen Sie mit dem Befehl „MetroCluster Interconnect Adapter show“, ob der physische Status des FC-VI-Adapters „up“ lautet. 3. Wenn die Konfiguration Fabric Switches umfasst, stellen Sie sicher, dass sie ordnungsgemäß verkabelt und konfiguriert sind.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
MetroCluster Spare-Festplatten übrig	WARNUNG	Die Ersatzfestplatte wurde während des Umschalttaschens zurückgelassen.	Wenn die Festplatte nicht ausgemustert wird, senden Sie sie mit dem Befehl „MetroCluster switchback“ an den ursprünglichen Eigentümer zurück.
Port der MetroCluster-Speicherbrücke unten	KRITISCH	Der Port auf der Speicherbrücke ist offline.	1) Überprüfen Sie den Betriebsstatus der Ports auf der Speicherbrücke mit dem Befehl „Storage Bridge show -Ports“. 2) Überprüfung der logischen und physischen Verbindung zum Port
Fehler bei den MetroCluster Storage-Switch-Lüftern	KRITISCH	Der Lüfter am Speicherschalter ist fehlgeschlagen.	1) Stellen Sie sicher, dass die Lüfter im Switch ordnungsgemäß funktionieren, indem Sie den Befehl „Storage Switch show -cooling“ verwenden. 2) Stellen Sie sicher, dass die Lüfter-FRUs ordnungsgemäß eingesetzt und betriebsbereit sind.
MetroCluster-Speicherschalter nicht erreichbar	KRITISCH	Der Storage-Switch ist über das Managementnetzwerk nicht erreichbar.	1) Stellen Sie sicher, dass die Node-Management-LIF über den Befehl „Network Interface show“ verfügt. 2) Stellen Sie sicher, dass der Switch aktiv ist, indem Sie den Befehl „Network ping“ verwenden. 3) Stellen Sie sicher, dass der Switch über SNMP erreichbar ist, indem Sie seine SNMP-Einstellungen nach der Anmeldung am Switch überprüfen.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
MetroCluster-Switch-Netzteile fehlgeschlagen	KRITISCH	Eine Netzteileinheit am Speicherschalter ist nicht funktionsfähig.	1) Überprüfen Sie die Fehlerdetails mit dem Befehl „Storage Switch show -error -Switch-Name <swtich name>“. 2) Identifizieren Sie das fehlerhafte Netzteil mit dem Befehl „Storage Switch show -Power -Switch-Name <switch name>“. 3) Stellen Sie sicher, dass das Netzteil ordnungsgemäß in das Gehäuse des Speicherschalters eingesetzt und voll funktionsfähig ist.
Fehler beim MetroCluster-Schalter der Temperatursensoren	KRITISCH	Der Sensor am Fibre Channel-Switch ist fehlgeschlagen.	1) Überprüfen Sie den Betriebsstatus der Temperatursensoren am Speicherschalter mit dem Befehl „Storage Switch show -cooling“. 2) Überprüfen Sie, ob der Schalter unter den empfohlenen Temperaturbedingungen funktioniert.
MetroCluster-Schalter Temperatur anormal	KRITISCH	Der Temperatursensor am Fibre Channel-Schalter meldet eine anormale Temperatur.	1) Überprüfen Sie den Betriebsstatus der Temperatursensoren am Speicherschalter mit dem Befehl „Storage Switch show -cooling“. 2) Überprüfen Sie, ob der Schalter unter den empfohlenen Temperaturbedingungen funktioniert.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
Heartbeat Des Service-Prozessors Nicht Erreicht	INFORMATIV	Diese Meldung tritt auf, wenn ONTAP kein erwartetes „Heartbeat“-Signal vom Service-Prozessor (SP) empfängt. Zusammen mit dieser Meldung werden Protokolldateien vom SP zum Debuggen ausgesendet. ONTAP setzt den SP zurück, um die Kommunikation wiederherzustellen. Der SP ist während eines Neustarts für bis zu zwei Minuten nicht verfügbar.	Wenden Sie sich an den technischen Support von NetApp.

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme
Der Heartbeat Des Service-Prozessors Wurde Angehalten	WARNUNG	Diese Meldung tritt auf, wenn ONTAP keine Heartbeats mehr vom Service-Prozessor (SP) empfängt. Je nach Hardwaredesign kann das System weiterhin Daten bereitstellen oder das Herunterfahren bestimmen, um Datenverluste oder Hardware-Schäden zu vermeiden. Das System stellt weiterhin Daten bereit, da der SP jedoch möglicherweise nicht funktioniert, kann das System keine Benachrichtigungen über heruntergekommen Appliances, Boot-Fehler oder Open Firmware (OFW) Power-On Self-Test (POST)-Fehler senden. Wenn Ihr System so konfiguriert ist, generiert und überträgt eine AutoSupport-Meldung (oder „Call Home“) an den technischen Support von NetApp und an die konfigurierten Ziele. Die erfolgreiche Bereitstellung einer AutoSupport-Botschaft verbessert die Problembestimmung und -Lösung erheblich.	Wenn das System heruntergefahren wurde, versuchen Sie ein schwieriges Ausschalten: Ziehen Sie den Controller aus dem Chassis heraus, drücken Sie ihn zurück, und schalten Sie das System ein. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem nach dem aus- und Wiedereinschalten oder andere möglicherweise Aufmerksamkeitsbedingungen weiterhin besteht.

Zurück nach oben

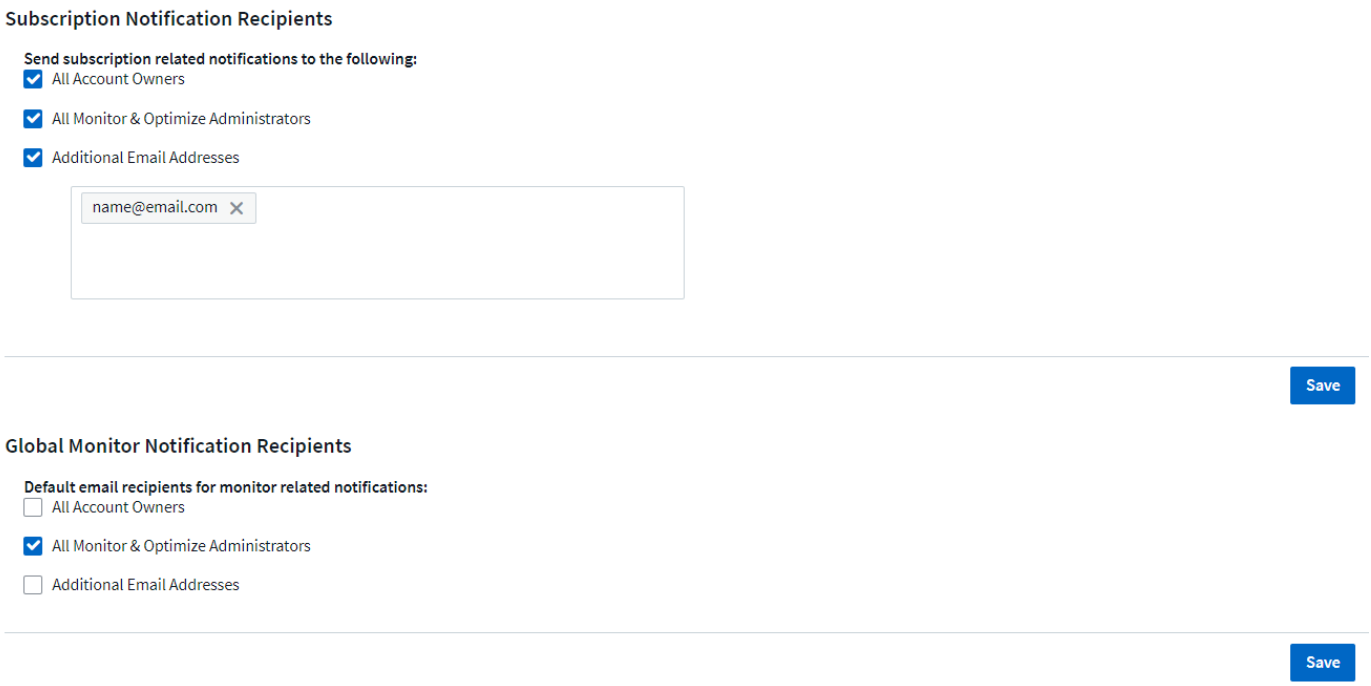
Weitere Informationen

- "Anzeigen und Fehlstellen von Warnungen"

E-Mail-Benachrichtigungen Werden Konfiguriert

Sie können eine E-Mail-Liste für abonnementbezogene Benachrichtigungen sowie eine globale E-Mail-Liste mit Empfängern für die Benachrichtigung über Schwellenverletzungen für Leistungsrichtlinien konfigurieren.

Um die Einstellungen für Benachrichtigungen-E-Mail-Empfänger zu konfigurieren, gehen Sie zur Seite **Admin > Benachrichtigungen** und wählen Sie die Registerkarte *E-Mail* aus.



Empfänger Für Abonnementbenachrichtigung

Um Empfänger für abonnementbezogene Ereignisbenachrichtigungen zu konfigurieren, gehen Sie zum Abschnitt „Empfänger für Abonnementbenachrichtigungen“. Sie können wählen, dass E-Mail-Benachrichtigungen für abonnierte Ereignisse an einen oder alle der folgenden Empfänger gesendet werden:

- Alle Account-Inhaber
- Alle *Monitor & Optimize* Administratoren
- Zusätzliche E-Mail-Adressen, die Sie angeben

Im Folgenden finden Sie Beispiele für die Art von Benachrichtigungen, die gesendet werden können, und Benutzeraktionen, die Sie durchführen können.

Hinweis:	**Benutzeraktion:**
Testversion oder Abonnement wurde aktualisiert	Lesen Sie die Abonnementdetails auf der "Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab das Abonnement läuft in 30 Tagen ab	Bei Aktivierung von „Automatische Verlängerung“ sind keine Maßnahmen erforderlich. Wenden Sie sich an den NetApp Vertrieb, um das Abonnement zu verlängern
Die Testversion endet in 2 Tagen	Testversion von der Seite erneuern"Abonnement". Sie können eine einmalige Testversion erneuern. Wenden Sie sich an den NetApp Vertrieb, um ein Abonnement zu erwerben

Testversion oder Abonnement abgelaufen Konto wird das Sammeln von Daten in 48 Stunden beendet Konto wird nach 48 Stunden gelöscht	Wenden Sie sich an den NetApp Vertrieb, um ein Abonnement zu erwerben

Um sicherzustellen, dass Ihre Empfänger Benachrichtigungen von Data Infrastructure Insights erhalten, fügen Sie die folgenden E-Mail-Adressen zu beliebigen „Zulassen“-Listen hinzu:

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Globale Empfängerliste für Warnungen

Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an die Benachrichtigungsliste gesendet. Sie können Benachrichtigungen an eine globale Empfängerliste senden.

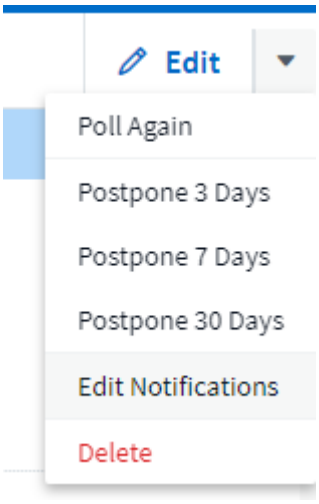
Wählen Sie zum Konfigurieren von Empfängern für globale Warnmeldungen die gewünschten Empfänger im Abschnitt **Empfänger für globale Monitorbenachrichtigungen** aus.

Sie können die globale Empfängerliste für einen einzelnen Monitor immer überschreiben, wenn Sie den Monitor erstellen oder ändern.

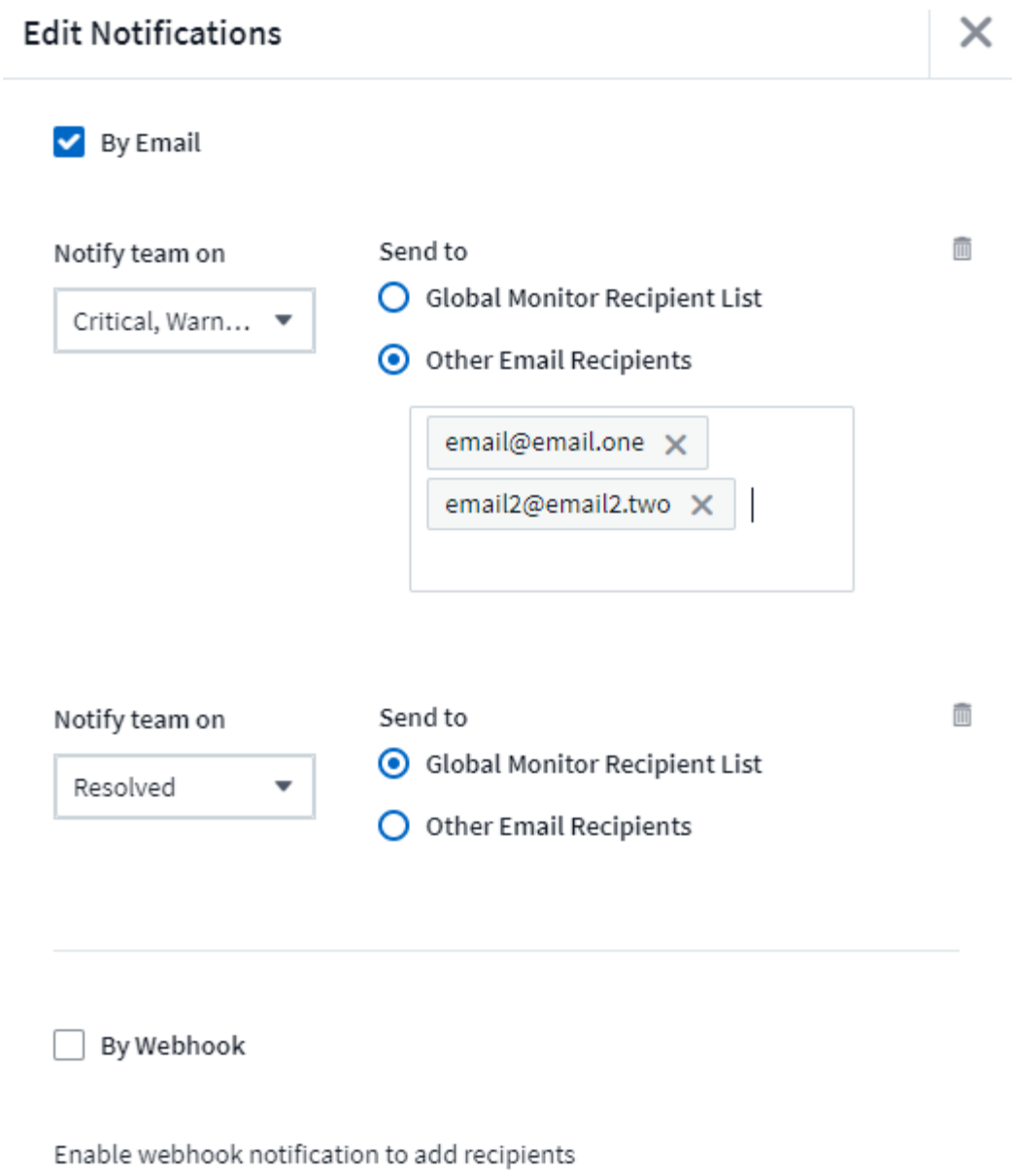
ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen zur Datenerfassung vorhanden sind, werden die von Monitor erzeugten Warnmeldungen an bestimmte Überwachungsempfänger gesendet.

Bearbeiten von Benachrichtigungen für ONTAP

Sie können Benachrichtigungen für ONTAP-Cluster ändern, indem Sie in der oberen rechten Dropdown-Liste auf einer Storage-Landing-Page „_Benachrichtigungen bearbeiten“ auswählen.



Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder gelöste Warnmeldungen festlegen. Jedes Szenario kann die Liste der globalen Empfänger oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Webhook-Benachrichtigungen

Benachrichtigung über Webhooks

Mit Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Benachrichtigungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standard-Input-Schnittstelle, zum Beispiel Slack, PagerDuty, Teams und Discord unterstützen Webhooks. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Data Infrastructure Insights viele dieser Bereitstellungskanäle unterstützen. Informationen zu Webhooks finden Sie auf diesen Anwendungs-Websites. Slack bietet zum Beispiel "Dieser Leitfaden ist hilfreich".

Sie können mehrere Webhook-Kanäle erstellen, jeden Kanal für einen anderen Zweck ausgerichtet; separate Anwendungen, verschiedene Empfänger, etc..

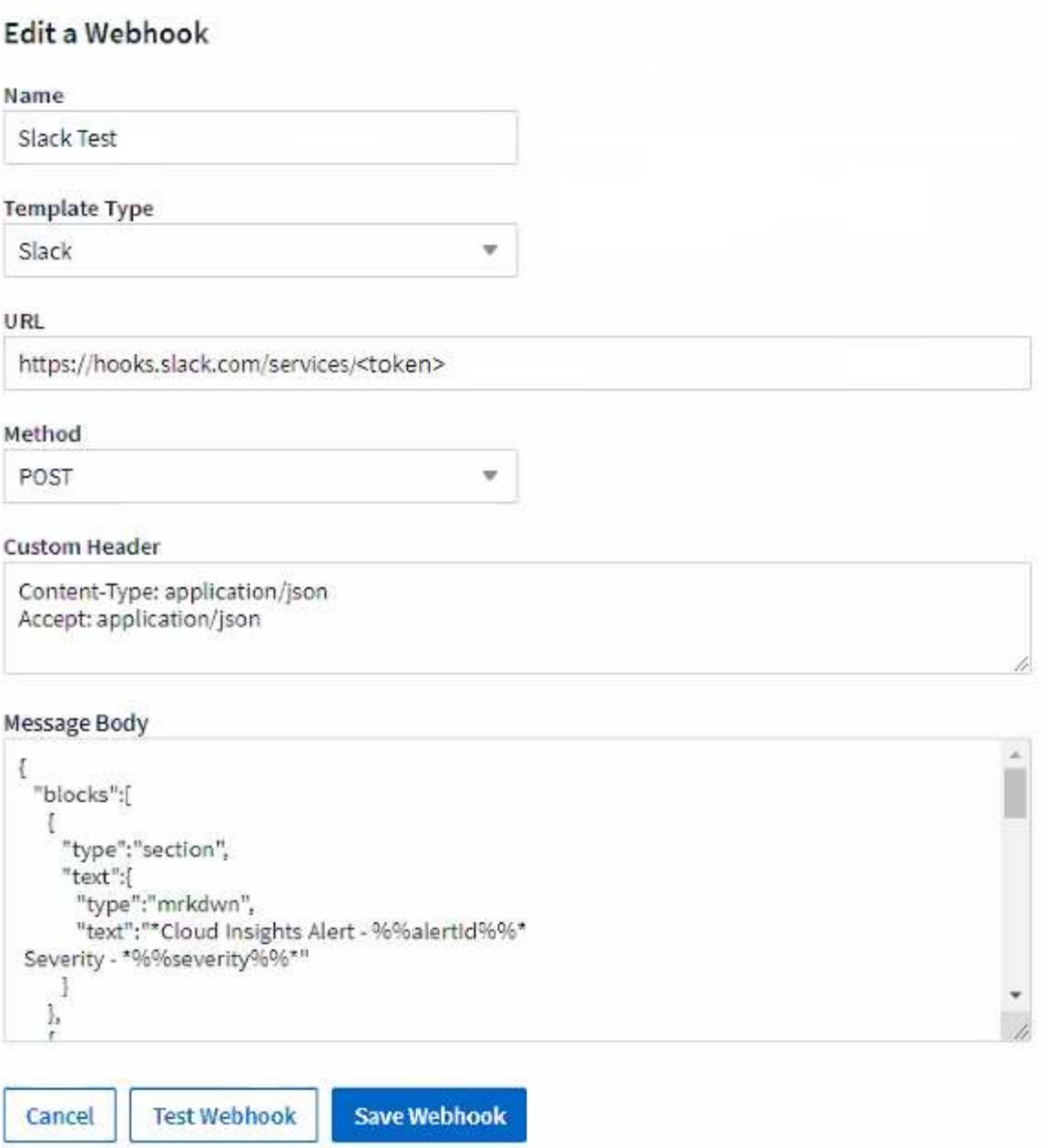
Die Instanz des Webhook-Kanals besteht aus folgenden Elementen:

Name	Eindeutiger Name
URL	Webhook-Ziel-URL, einschließlich der Präfix *http://* oder *https://* zusammen mit den url-Params
Methode	GET, POST - Standard ist POST
Benutzerdefinierte Kopfzeile	Geben Sie hier alle benutzerdefinierten Kopfzeilen an
Nachrichtentext	Setzen Sie den Text Ihrer Nachricht hier ein
Standardwarnparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen es Ihnen, eindeutige Parameter und sichere Elemente wie Passwörter hinzuzufügen

Erstellen eines Webhook

Um einen Data Infrastructure Insights Webhook zu erstellen, gehen Sie zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus.

Das folgende Bild zeigt einen Beispiel-Webhook, der für Slack konfiguriert ist:



Geben Sie die entsprechenden Informationen für die einzelnen Felder ein, und klicken Sie anschließend auf „Speichern“.

Sie können auch auf die Schaltfläche "Webhook testen" klicken, um die Verbindung zu testen. Beachten Sie, dass der Nachrichtentext (ohne Ersatz) entsprechend der ausgewählten Methode an die definierte URL gesendet wird.

Data Infrastructure Insights Webhooks umfassen eine Reihe von Standardparametern. Außerdem können Sie eigene benutzerdefinierte Parameter oder Geheimnisse erstellen.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parameter: Was sind sie und wie benutze ich sie?

Bei den Alarmparametern handelt es sich um dynamische Werte, die pro Meldung ausgefüllt werden. Beispielsweise wird der Parameter *%%TriggeredOn%%* durch das Objekt ersetzt, auf dem die Warnung ausgelöst wurde.

Sie können ein beliebiges Objektattribut (z. B. Speichername) als Parameter zu einem Webhook hinzufügen. Sie können beispielsweise Parameter für den Volume-Namen und den Speichernamen in einer Webhook-Beschreibung wie: „Hohe Latenz für Volume: *%%relatedObject.volume.name%%*, Speicher: *%%relatedObject.storage.name%%*".

Beachten Sie, dass in diesem Abschnitt beim Klicken auf die Schaltfläche „Webhook testen“ Substitutionen *Not* durchgeführt werden. Die Schaltfläche sendet eine Nutzlast, die die % Substitutionen anzeigt, sie jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

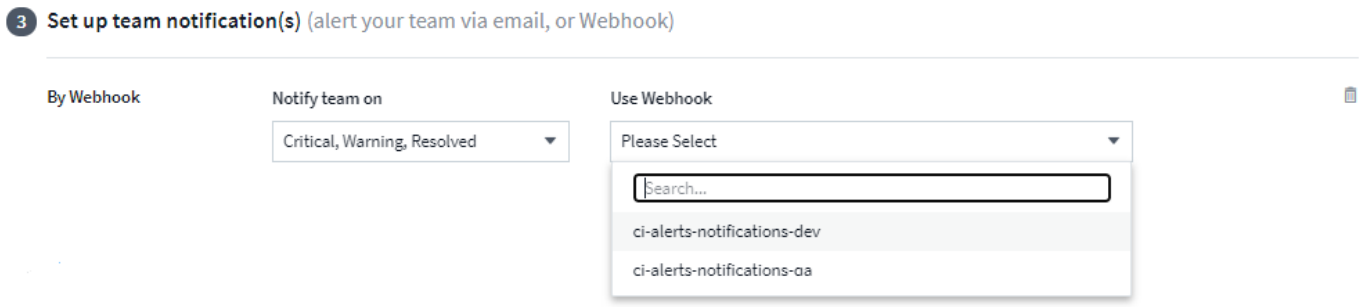
In diesem Abschnitt können Sie benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen, die Sie wünschen. Aus Sicherheitsgründen kann dieser Webhook-Kanal nur dann geändert werden, wenn ein Geheimnis definiert ist. Es ist schreibgeschützt für andere. Sie können Geheimnisse in URL/Headern als *%%<secret_Name>%* verwenden.

Seite „Webhooks List“

Auf der Listenseite Webhooks werden der Name, erstellt von, erstellt am, Status, sicher, und zuletzt gemeldete Felder.

Wählen Sie Webhook Notification in einem Monitor

Um die Webhook-Benachrichtigung in einem auszuwählen"Überwachen", gehen Sie zu **Alarme > Monitore verwalten** und wählen den gewünschten Monitor aus, oder fügen Sie einen neuen Monitor hinzu. Wählen Sie im Abschnitt „ Team notifications_ einrichten“ die Option „*Webhook*“ als Bereitstellungsmethode aus. Wählen Sie die Alarmstufen (kritisch, Warnung, gelöst), und wählen Sie dann den gewünschten Webhook.



Beispiele Für Webhook:

Webhooks für "Slack" Webhooks "PagerDuty"für Webhooks "Teams Aus""Abschnur"

Beispiel für den Webhook für die Kabeltrennleitung

Mit Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Benachrichtigungen an verschiedene Anwendungen senden. Diese Seite enthält ein Beispiel zum Einrichten von Webhooks für Discord.

Diese Seite bezieht sich auf Anweisungen von Dritten, die möglicherweise geändert werden können. Die aktuellsten Informationen finden Sie im"Dokumentation zum Auflösen von Kabel".

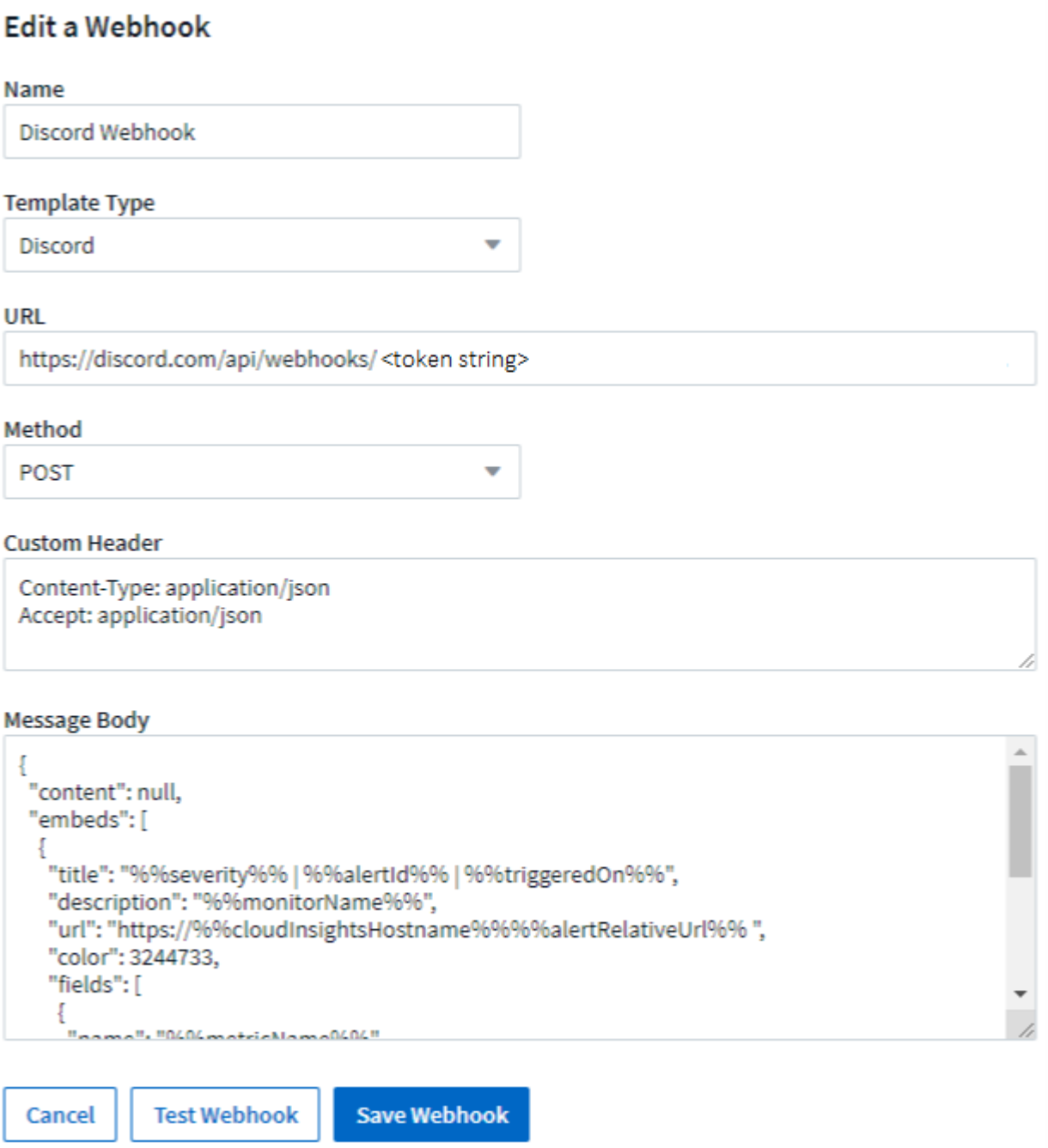
Kabelabschalt Einrichten:

- Wählen Sie in Discord den Server unter Textkanäle die Option Kanal bearbeiten (Zahnradsymbol) aus.
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**

- Kopieren Sie die Webhook-URL. Sie müssen diese in die Data Infrastructure Insights Webhook-Konfiguration einfügen.

Data Infrastructure Insights Webhook Erstellen:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Notifications** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, z. B. „Discord“.
3. Wählen Sie in der Dropdown-Liste *Template Type* die Option **Discord** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.

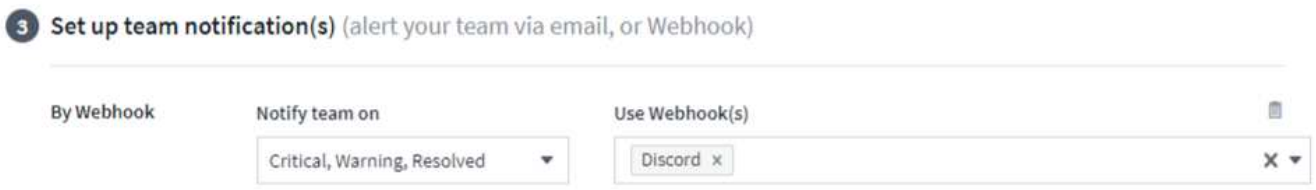


Um den Webhook zu testen, ersetzen Sie vorübergehend den url-Wert im Nachrichtentext durch eine beliebige gültige URL (z.B. *https://NetApp.com*) und klicken Sie dann auf den *Webhook* -Button testen. Stellen Sie den Nachrichtentext nach Abschluss des Tests wieder ein.

Benachrichtigungen über Webhook

Um Ereignisse über Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um eine neue zu erstellen"Überwachen".

- Wählen Sie eine Metrik aus, und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „ Team-Benachrichtigung(en) einrichten“ die Option „ **Webhook** Liefermethode“.
- Wählen Sie den Webhook „Discord“ für die gewünschten Ereignisse (kritisch, Warnung, gelöst).



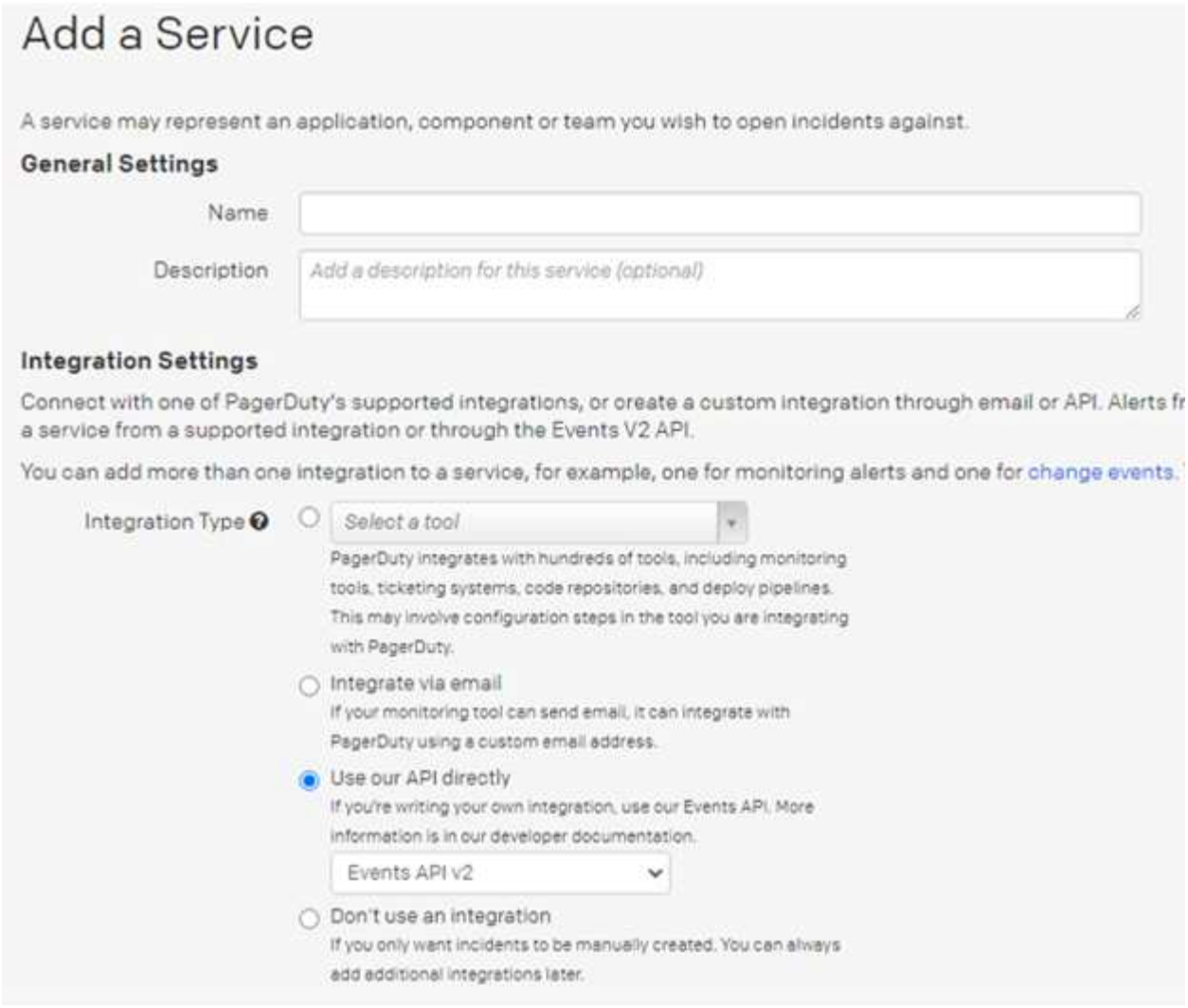
Webhook-Beispiel für PagerDuty

Mit Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Benachrichtigungen an verschiedene Anwendungen senden. Diese Seite enthält ein Beispiel zum Einrichten von Webhooks für PagerDuty.

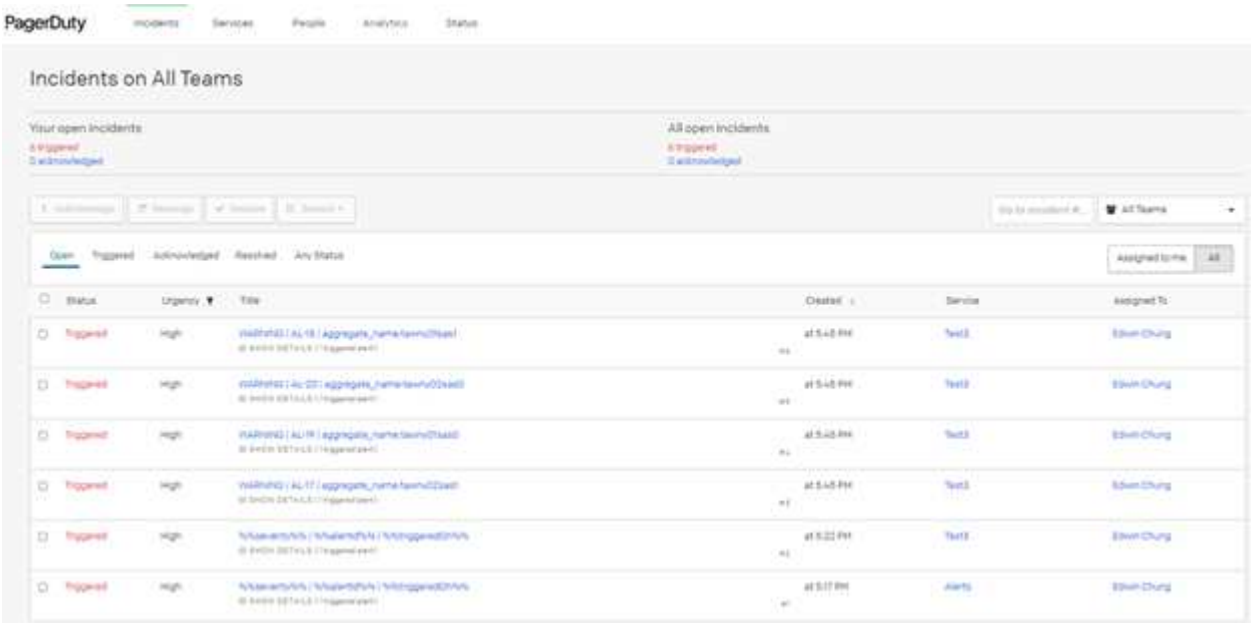
Diese Seite bezieht sich auf Anweisungen von Dritten, die möglicherweise geändert werden können. Die aktuellsten Informationen finden Sie im"PagerDuty-Dokumentation".

PagerDuty Setup:

1. Navigieren Sie in PagerDuty zu **Services > Service Directory** und klicken Sie auf **+New Service** button
2. Geben Sie einen *Name* ein, und wählen Sie *Use our API direkt* aus. Klicken Sie auf *Dienst hinzufügen*.

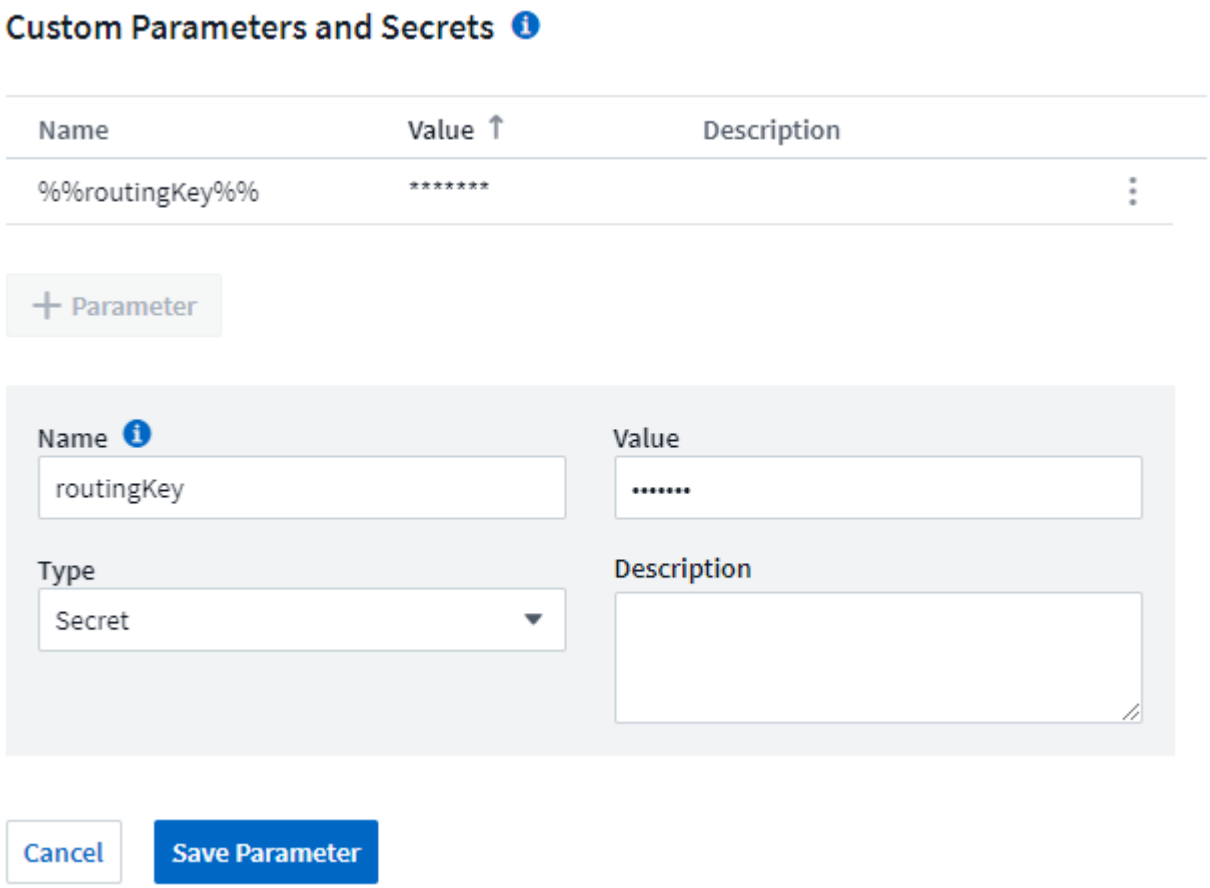


3. Klicken Sie auf die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie den Data Infrastructure Insights Webhook unten erstellen.
4. Gehen Sie zu **Incidents** oder **Services**, um Benachrichtigungen anzuzeigen.



Data Infrastructure Insights Webhook Erstellen:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Notifications** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, z. B. „PagerDuty Trigger“. Sie verwenden diesen Webhook für kritische und warning-Level-Ereignisse.
3. Wählen Sie in der Dropdown-Liste *Vorlagenart* die Option **PagerDuty** aus.
4. Erstellen Sie ein benutzerdefiniertes Parametergeheimnis namens *routingKey* und setzen Sie den Wert von oben auf den PagerDuty_Integration Key_-Wert.



Wiederholen Sie diese Schritte, um einen Webhook „PagerDuty Resolve“ für aufgelöste Ereignisse zu erstellen.

Feldzuordnung von PagerDuty zu Data Infrastructure Insights

Die folgende Tabelle und Abbildung zeigen die Zuordnung von Feldern zwischen PagerDuty und Data Infrastructure Insights:

PagerDuty	Einblicke In Die Dateninfrastruktur
Warntaste	Alarm-ID
Quelle	Ausgelöst Am
Komponente	Metrischer Name
Gruppieren	Objekttyp

PagerDuty	Einblicke In Die Dateninfrastruktur
Klasse	Monitorname

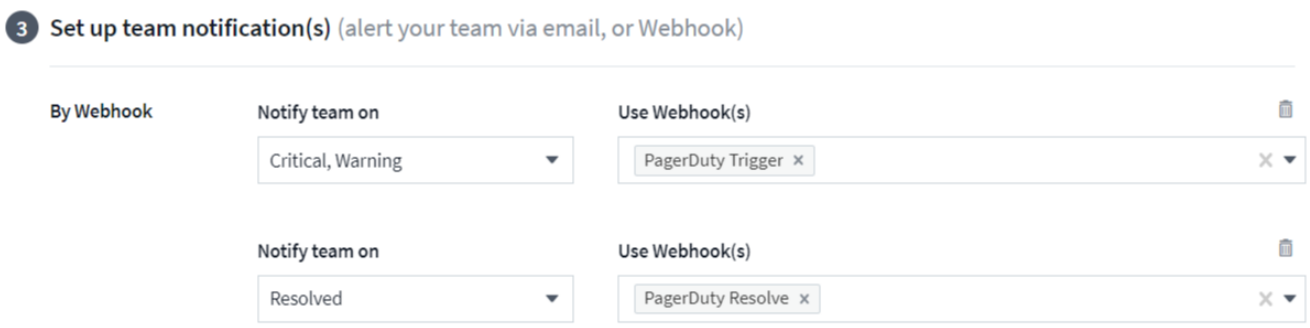
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Benachrichtigungen über Webhook

Um Ereignisse über Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um eine neue zu erstellen"Überwachen".

- Wählen Sie eine Metrik aus, und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „ Team-Benachrichtigung(en) einrichten“ die Option „ **Webhook** Liefermethode“.
- Wählen Sie den Webhook „PagerDuty Trigger“ für Ereignisse auf kritischen und Warnstufen.
- Wählen Sie „PagerDuty Resolve“ für aufgelöste Ereignisse.



Die Festlegung separater Benachrichtigungen für Trigger-Ereignisse und aufgelöste Ereignisse ist eine bewährte Vorgehensweise, da PagerDuty Trigger-Ereignisse anders als gelöste Ereignisse verarbeitet.

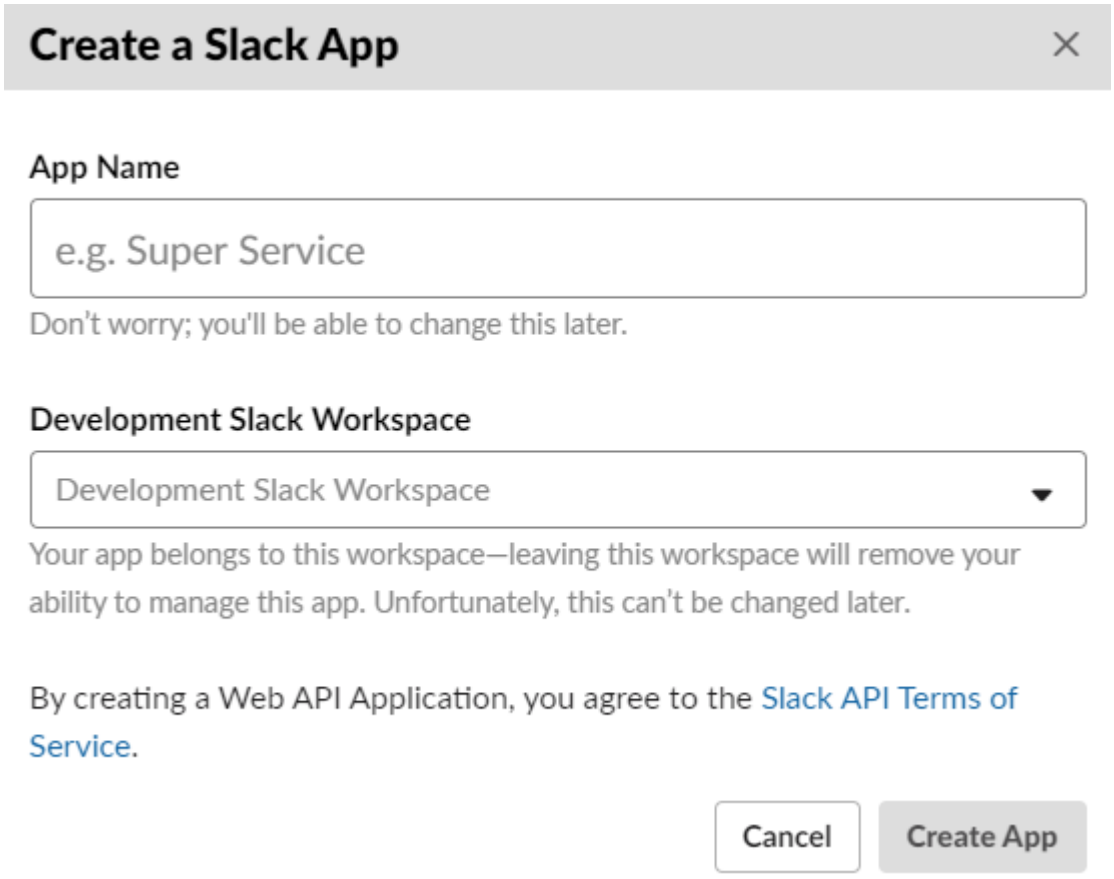
Webhook-Beispiel für Slack

Mit Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Benachrichtigungen an verschiedene Anwendungen senden. Diese Seite enthält ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite bezieht sich auf Anweisungen von Dritten, die möglicherweise geändert werden können. Die aktuellsten Informationen finden Sie im"Slack-Dokumentation".

Slack-Beispiel:

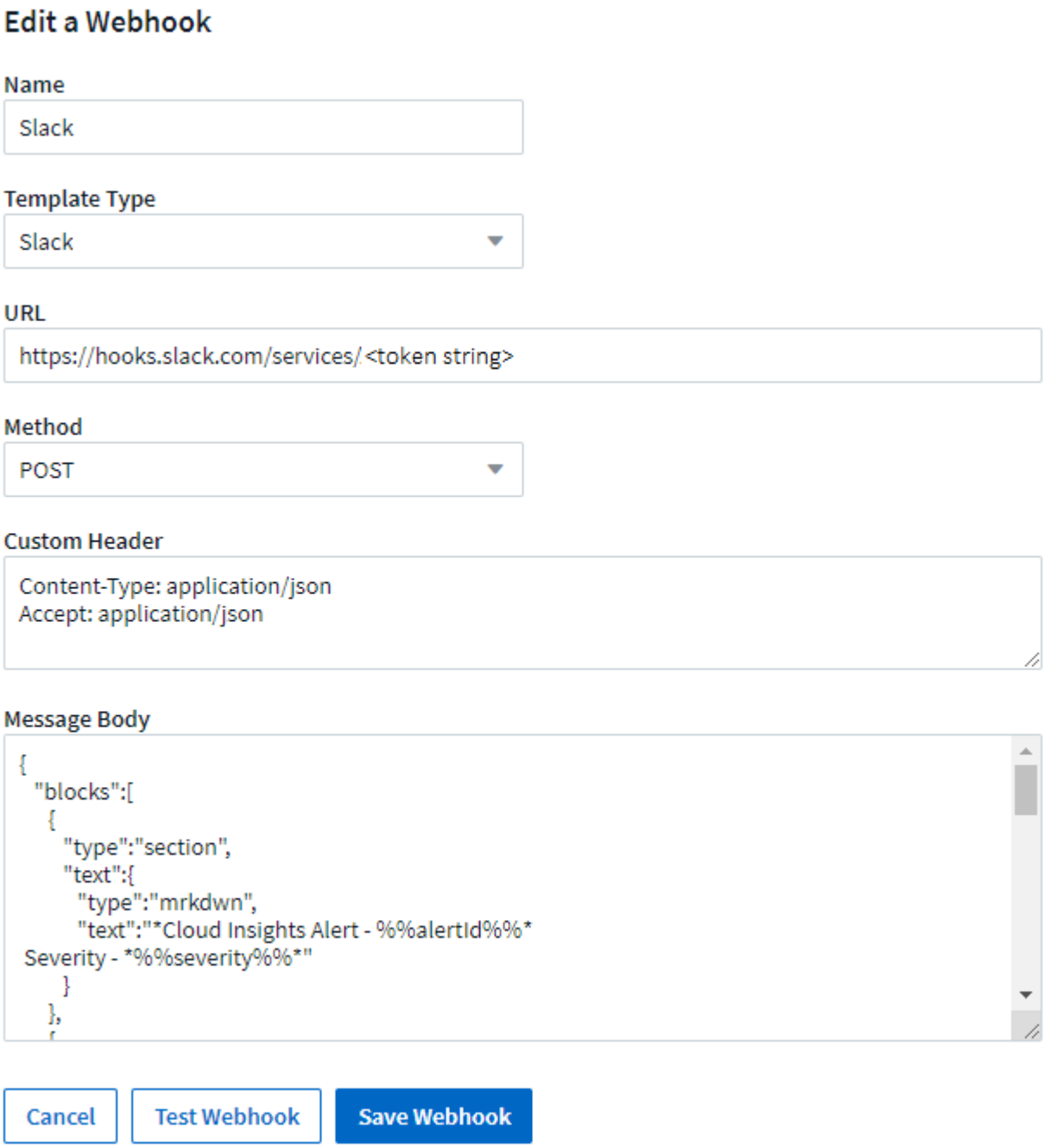
- Gehen Sie zu https://api.slack.com/apps und erstellen Sie eine neue App Gib ihm einen aussagekräftigen Namen und wähle den Slack Workspace aus.



- Gehen Sie zu eingehenden Webhooks, klicken Sie auf *eingehende Webhooks aktivieren*, Anforderung an *Neuen Webhook hinzufügen*, und wählen Sie den Kanal aus, auf dem Sie den Posten erhalten möchten.
- Kopieren Sie die Webhook-URL. Sie müssen diese in die Data Infrastructure Insights Webhook-Konfiguration einfügen.

Data Infrastructure Insights Webhook Erstellen:

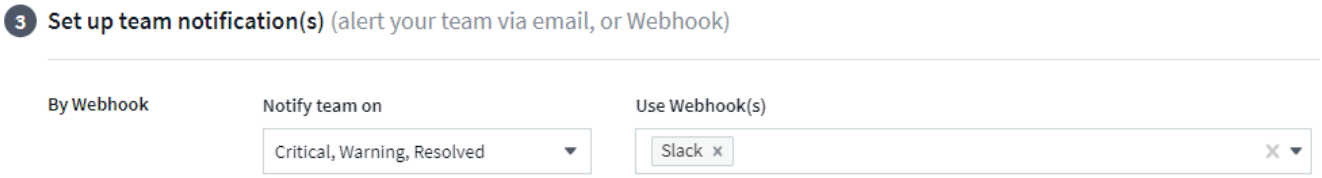
1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Notifications** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Gib dem Webhook einen aussagekräftigen Namen, wie "Slack Webhook".
3. Wählen Sie im Drop-down_Template Type_ **Slack** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.



Benachrichtigungen über Webhook

Um Ereignisse über Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um eine neue zu erstellen"Überwachen".

- Wählen Sie eine Metrik aus, und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „ Team-Benachrichtigung(en) einrichten“ die Option „ **Webhook** Liefermethode“.
- Wähle den Webhook „Slack“ für die gewünschten Ereignisse (kritisch, Warnung, gelöst)



Weitere Informationen:

- Informationen zum Ändern von Nachrichtenformat und -Layout finden Sie unter https://api.slack.com/messaging/composing
- Fehlerbehandlung: https://api.slack.com/messaging/webhooks#handling_errors

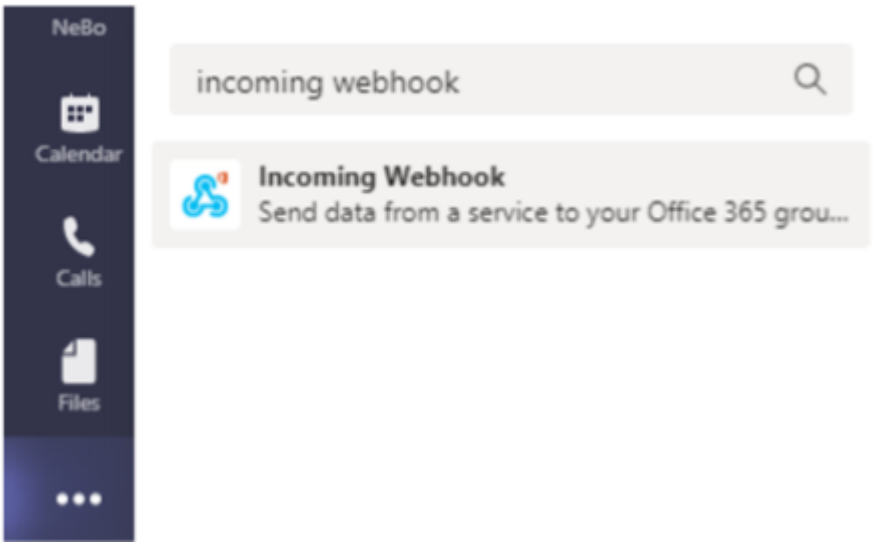
Webhook-Beispiel für Microsoft-Teams

Mit Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Benachrichtigungen an verschiedene Anwendungen senden. Diese Seite enthält ein Beispiel für das Einrichten von Webhooks für Teams.

Diese Seite bezieht sich auf Anweisungen von Dritten, die möglicherweise geändert werden können. Die aktuellsten Informationen finden Sie im"Die Dokumentation des Teams".

Teameinstellungen:

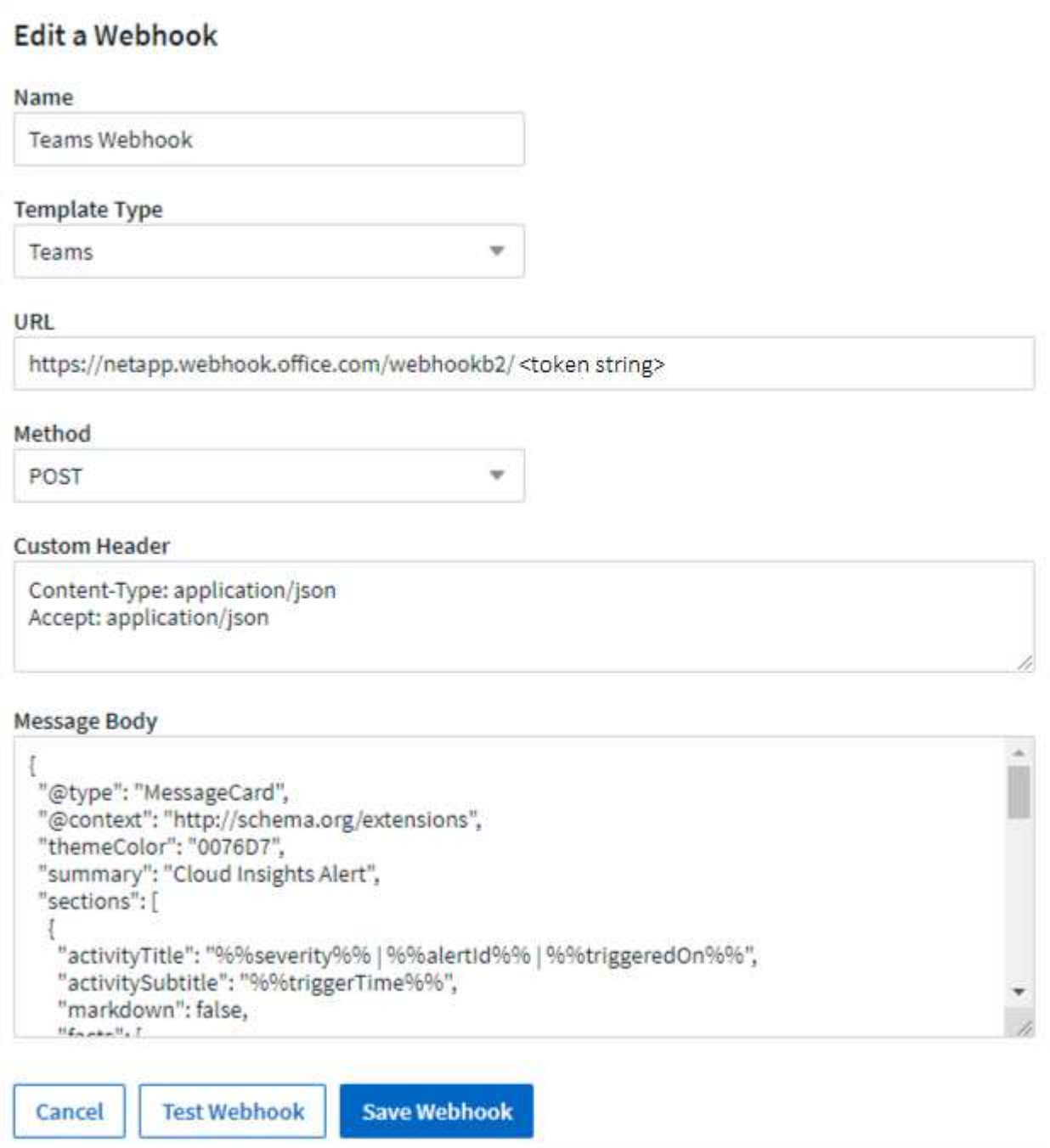
1. Wählen Sie in Teams den Kebab aus, und suchen Sie nach eingehender Webhook.



2. Wählen Sie **zu einem Team hinzufügen > Team auswählen > Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen diese in die Data Infrastructure Insights Webhook-Konfiguration einfügen.

Data Infrastructure Insights Webhook Erstellen:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Notifications** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, z. B. „Teams Webhook“.
3. Wählen Sie in der Dropdown-Liste *Template Type* die Option **Teams** aus.



1. Fügen Sie die URL von oben in das Feld *URL* ein.

Benachrichtigungen über Webhook

Um Ereignisse über Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um eine neue zu erstellen"Überwachen".

- Wählen Sie eine Metrik aus, und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „ Team-Benachrichtigung(en) einrichten“ die Option „ **Webhook** Liefermethode“.
- Wählen Sie den Webhook „Teams“ für die gewünschten Ereignisse (kritisch, Warnung, gelöst)