Beobachtbarkeit

Cloud Insights

NetApp
July 16, 2024

Inhalt

Beobachtbarkeit

Dashboards Werden Erstellt

Übersicht Über Dashboards

Cloud Insights bietet Benutzern die Flexibilität, Betriebsansichten von Infrastrukturdaten zu erstellen. So können Sie benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen, die jeweils eine umfangreiche Flexibilität bei der Anzeige und Dokumentation Ihrer Daten bieten.

> Die Beispiele in diesen Abschnitten dienen nur zu erklärenden Zwecken und decken nicht alle möglichen Szenarien ab. Die hierin enthaltenen Konzepte und Schritte können dazu verwendet werden, eigene Dashboards zu erstellen, um die Daten auf Ihre speziellen Bedürfnisse hin hervorzuheben.

Erstellen eines Dashboards

Sie erstellen ein neues Dashboard an einem von zwei Stellen:

- **Dashboards > [+Neues Dashboard]**
- **Dashboards > Alle Dashboards anzeigen >** Klicken Sie auf die Schaltfläche **[+Dashboard]**

Dashboard-Steuerelemente

Der Dashboard-Bildschirm verfügt über mehrere Bedienelemente:

- **Zeitauswahl**: Ermöglicht die Anzeige von Dashboard-Daten für einen Zeitraum von 15 Minuten bis zu den letzten 30 Tagen oder einen benutzerdefinierten Zeitbereich von bis zu 31 Tagen. Sie können diesen globalen Zeitbereich in einzelnen Widgets überschreiben.
- **Bearbeiten** Schaltfläche: Wenn Sie diese Option auswählen, wird der Bearbeitungsmodus aktiviert, sodass Sie Änderungen am Dashboard vornehmen können. Neue Dashboards werden standardmäßig im Bearbeitungsmodus geöffnet.
- **Speichern**-Taste: Ermöglicht das Speichern oder Löschen des Dashboards.

  Sie können das aktuelle Dashboard umbenennen, indem Sie einen neuen Namen eingeben, bevor Sie auf **Speichern** klicken.

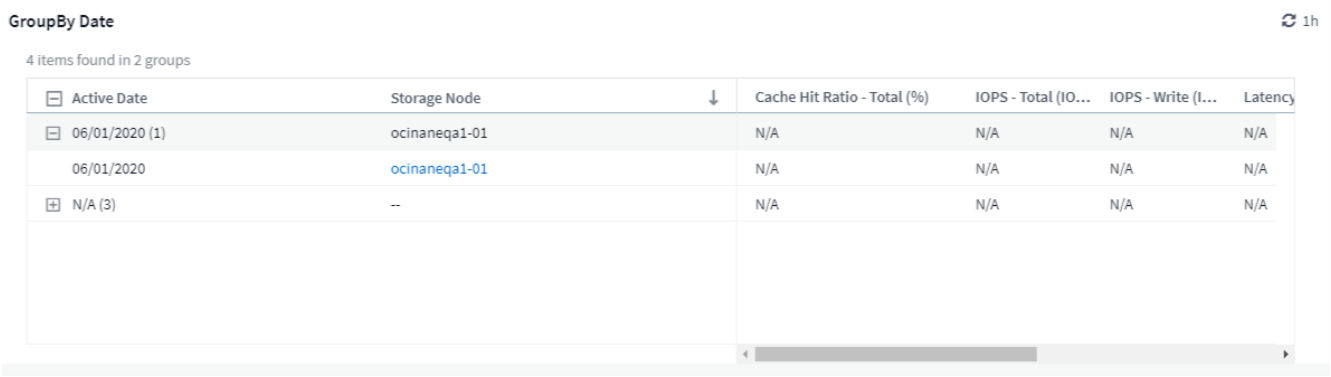
- **Widget**-Schaltfläche hinzufügen, mit der Sie eine beliebige Anzahl von Tabellen, Diagrammen oder anderen Widgets zum Dashboard hinzufügen können.

  Widgets können geändert und an verschiedene Positionen im Dashboard verschoben werden, um Ihnen die beste Ansicht Ihrer Daten entsprechend Ihren aktuellen Anforderungen zu geben.

Widget-Typen

Sie können aus den folgenden Widgets wählen:

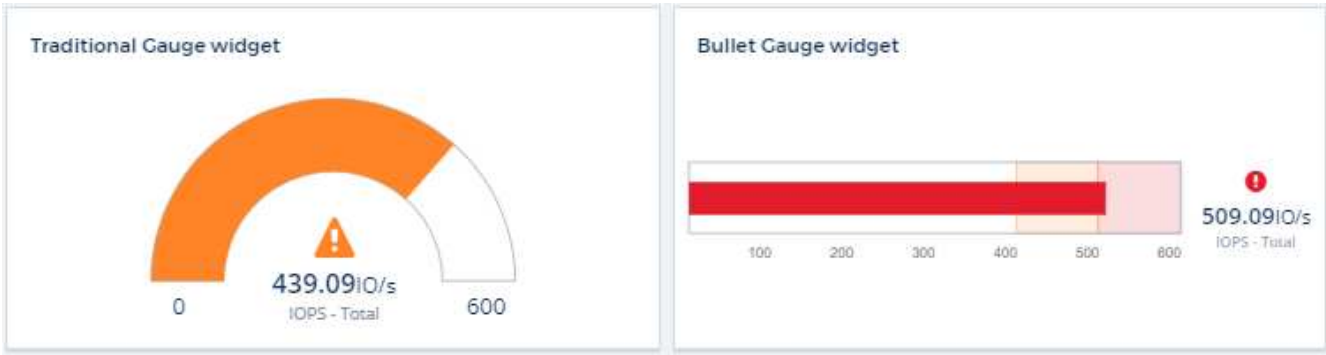
- **Tabelle Widget**: Eine Tabelle, die Daten nach den gewählten Filtern und Spalten anzeigt. Tabellendaten können in Gruppen zusammengefasst werden, die ausgeblendet und erweitert werden können.



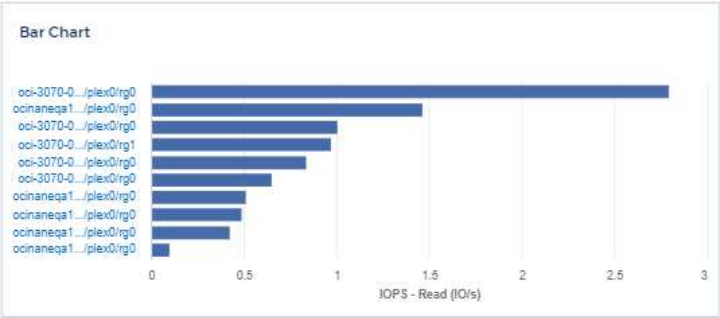
- **Linie, Spline, Bereich, gestapelte Flächendiagramme**: Dies sind Zeitreihenkarten-Widgets, auf denen Sie Leistung und andere Daten über die Zeit anzeigen können.

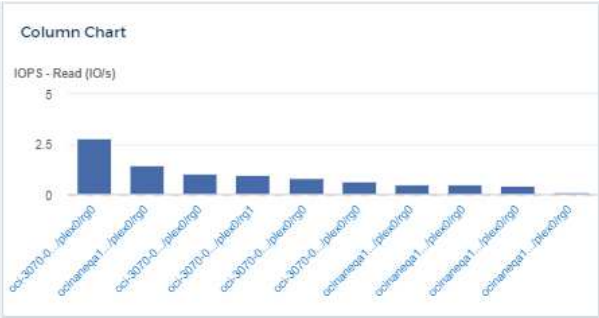
- **Single Value Widget**: Ein Widget, mit dem Sie einen einzelnen Wert anzeigen können, der entweder direkt von einem Zähler abgeleitet oder mithilfe einer Abfrage oder eines Ausdrucks berechnet werden kann. Sie können Schwellenwerte für die Farbformatierung definieren, um anzuzeigen, ob der Wert in „erwartet“, „Warnung“ oder „kritischer Bereich“ liegt.

- **Widget messen**: Zeigt Daten mit einem einzigen Wert in einem herkömmlichen (festen) Manometer oder einer Kugel an, mit Farben, die auf "Warnung" oder "kritische" Werte basieren "Anpassen".

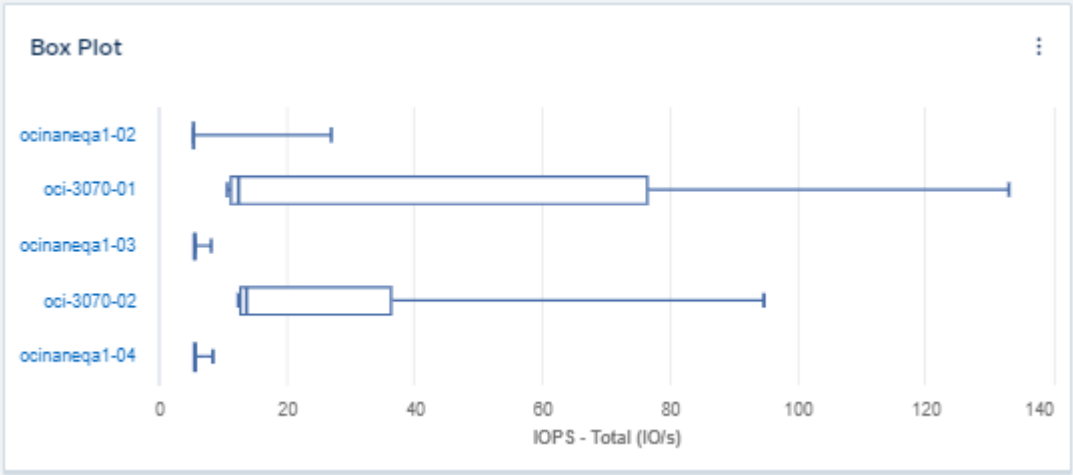


- **Balken, Spaltendiagramme**: Zeigt die oberen oder unteren N-Werte an, z. B. die Top 10-Storage nach Kapazität oder die unteren 5-Volumes nach IOPS.

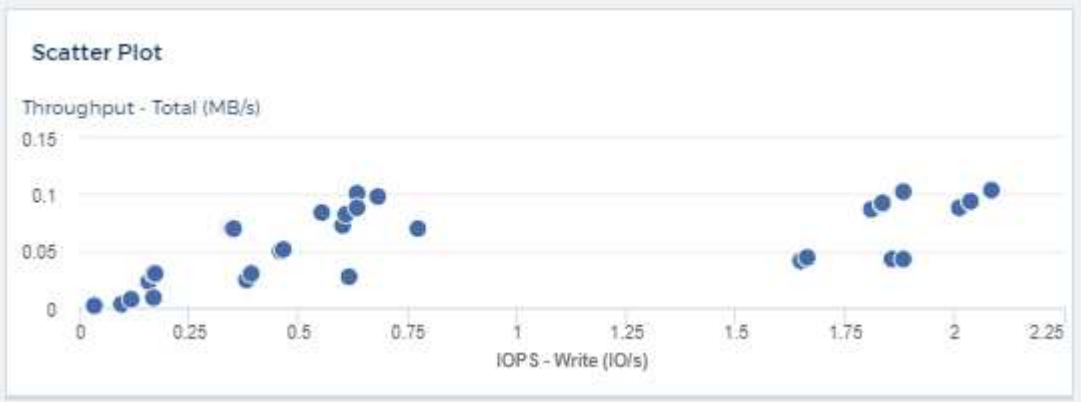




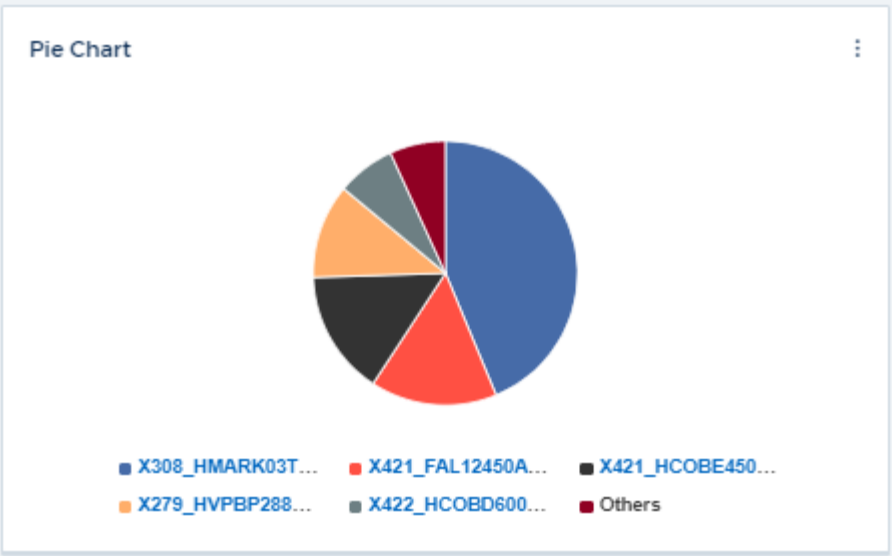
- **Box Plot Chart**: Eine Darstellung des min., max., Median und des Bereichs zwischen dem unteren und dem oberen Quartil der Daten in einem einzigen Diagramm.



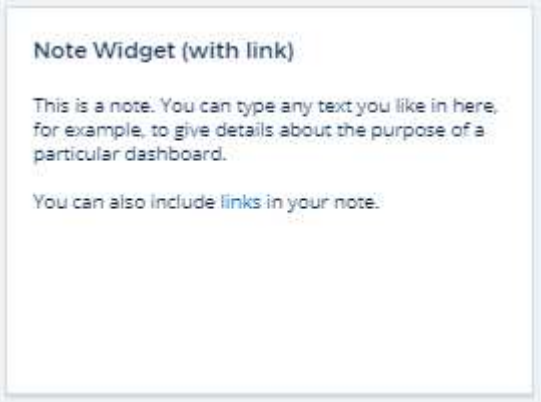
- **Scatter Plot Chart**: Zeichnet verwandte Daten als Punkte, zum Beispiel IOPS und Latenz. In diesem Beispiel sind Assets mit hohem Durchsatz und niedrigen IOPS schnell zu finden.



- **Pie Chart**: Ein traditionelles Kreisdiagramm, um Daten als Teil der Gesamtmenge anzuzeigen.



- **Widgets Anmerkung**: Bis zu 1000 Zeichen Freitext.



- **Warnungstabelle**: Zeigt bis zu den letzten 1,000 Warnungen an.

Ausführlichere Erläuterungen zu diesen und anderen Dashboard-Funktionen finden Sie "Klicken Sie hier".

Einrichten eines Dashboards als Startseite

Sie können wählen, welches Dashboard als **Startseite** Ihrer Umgebung eingestellt werden soll. Verwenden Sie dazu eine der folgenden Methoden:

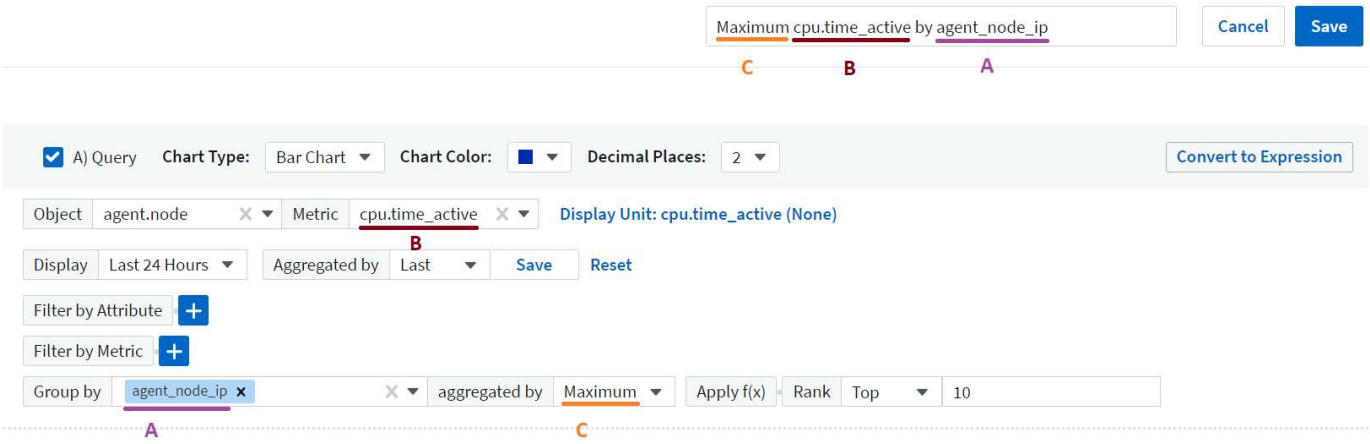
- Gehen Sie zu **Dashboards > Alle Dashboards anzeigen**, um die Liste der Dashboards in Ihrer Umgebung anzuzeigen. Klicken Sie auf das Optionsmenü rechts neben dem gewünschten Dashboard und wählen Sie **als Startseite festlegen**.
- Klicken Sie in der Liste auf ein Dashboard, um das Dashboard zu öffnen. Klicken Sie in der oberen Ecke auf das Dropdown-Menü und wählen Sie **als Startseite festlegen**.

Dashboard-Funktionen

Dashboards und Widgets ermöglichen eine große Flexibilität bei der Anzeige von Daten. Nachfolgend finden Sie einige Konzepte, mit denen Sie Ihre individuellen Dashboards optimal nutzen können.

Widget-Naming

Widgets werden automatisch auf der Grundlage des für die erste Widget-Abfrage ausgewählten Objekts, der Metrik oder des Attributs benannt. Wenn Sie auch eine Gruppierung für das Widget auswählen, werden die Attribute „Gruppieren nach“ in die automatische Benennung (Aggregationsmethode und Metrik) aufgenommen.



Durch Auswahl eines neuen Objekts oder Gruppierungsattributs wird der automatische Name aktualisiert.

Wenn Sie den automatischen Widget-Namen nicht verwenden möchten, können Sie einfach einen neuen Namen eingeben.

Widget-Platzierung und -Größe

Alle Dashboard-Widgets können entsprechend Ihren Anforderungen für jedes Dashboard positioniert und dimensioniert werden.

Duplizieren eines Widgets

Klicken Sie im Dashboard-Bearbeitungsmodus auf das Menü im Widget und wählen Sie **Duplizieren**. Der Widget-Editor wird gestartet, mit der ursprünglichen Widget-Konfiguration und mit einem "Kopie" Suffix im Widget-Namen ausgefüllt. Sie können ganz einfach alle erforderlichen Änderungen vornehmen und das neue Widget speichern. Das Widget wird am unteren Rand des Dashboards platziert und Sie können sie nach Bedarf positionieren. Denken Sie daran, Ihr Dashboard zu speichern, wenn alle Änderungen abgeschlossen sind.

Widget-Legenden Werden Angezeigt

Die meisten Widgets auf Dashboards können mit oder ohne Legenden angezeigt werden. Legenden in Widgets können auf einem Dashboard über eine der folgenden Methoden ein- oder ausgeschaltet werden:

- Klicken Sie beim Anzeigen des Dashboards auf die Schaltfläche **Optionen** im Widget und wählen Sie im Menü die Option **Legenden anzeigen** aus.

Wenn sich die im Widget angezeigten Daten ändern, wird die Legende für dieses Widget dynamisch aktualisiert.

Wenn Legenden angezeigt werden, wird die Legende als Link zu dieser Asset-Seite angezeigt, wenn die Landing-Page des von der Legende angegebenen Assets navigiert werden kann. Wenn die Legende „all“ anzeigt, wird durch Klicken auf den Link eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Neue Metriken

Cloud Insights bietet verschiedene **transform**-Optionen für bestimmte Metriken in Widgets (insbesondere die Metriken "Custom" oder Integration Metrics, wie etwa von Kubernetes, ONTAP Advanced Data, Telegraf Plugins, etc.), so dass Sie die Daten auf eine Reihe von Möglichkeiten anzuzeigen. Beim Hinzufügen transformbarer Metriken zu einem Widget werden Sie mit einem Dropdown-Menü mit den folgenden Optionen zur Transformation angezeigt:

Keine
: Die Daten werden ohne Manipulation als IS angezeigt.

Preis
: Aktueller Wert geteilt durch den Zeitbereich seit der vorherigen Beobachtung.

Kumulativ
: Die Akkumulation der Summe der vorherigen Werte und des aktuellen Werts.

Delta
: Die Differenz zwischen dem vorhergehenden Beobachtungswert und dem aktuellen Wert.

Delta-Preis
: Delta-Wert geteilt durch den Zeitraum seit der vorherigen Beobachtung.

Kumulierter Betrag
: Kumulativer Wert geteilt durch den Zeitraum seit der vorherigen Beobachtung.

Beachten Sie, dass bei der Transformation von Metriken nicht die zugrunde liegenden Daten selbst, sondern nur die Art und Weise geändert werden, wie Daten angezeigt werden.

Anfragen und Filter für das Dashboard-Widget

Abfragen

Die Abfrage in einem Dashboard-Widget ist ein leistungsstarkes Tool zur Verwaltung der Anzeige Ihrer Daten. Hier sind einige Dinge zu beachten über Widget-Abfragen.

Einige Widgets können bis zu fünf Abfragen haben. Jede Abfrage erstellt im Widget einen eigenen Satz von Linien oder Diagrammen. Das Einrichten von Rollup, Gruppierung, Ergebnissen von oben/unten usw. auf einer

Abfrage hat keine Auswirkungen auf andere Abfragen für das Widget.

Sie können auf das Augensymbol klicken, um eine Abfrage vorübergehend auszublenden. Das Widget wird automatisch aktualisiert, wenn Sie eine Abfrage ausblenden oder anzeigen. Auf diese Weise können Sie die angezeigten Daten auf einzelne Abfragen überprüfen, während Sie Ihr Widget erstellen.

Die folgenden Widget-Typen können mehrere Abfragen haben:

- Diagramm Bereich
- Stapelgebietskarte
- Liniendiagramm
- Spline-Diagramm
- Widget mit einem einzelnen Wert

Die übrigen Widget-Typen können nur eine einzige Abfrage haben:

- Tabelle
- Balkendiagramm
- Box-Darstellung
- Streudiagramm

Filtern in Dashboard-Widget-Abfragen

Hier sind einige Dinge, die Sie tun können, um das Beste aus Ihren Filtern.

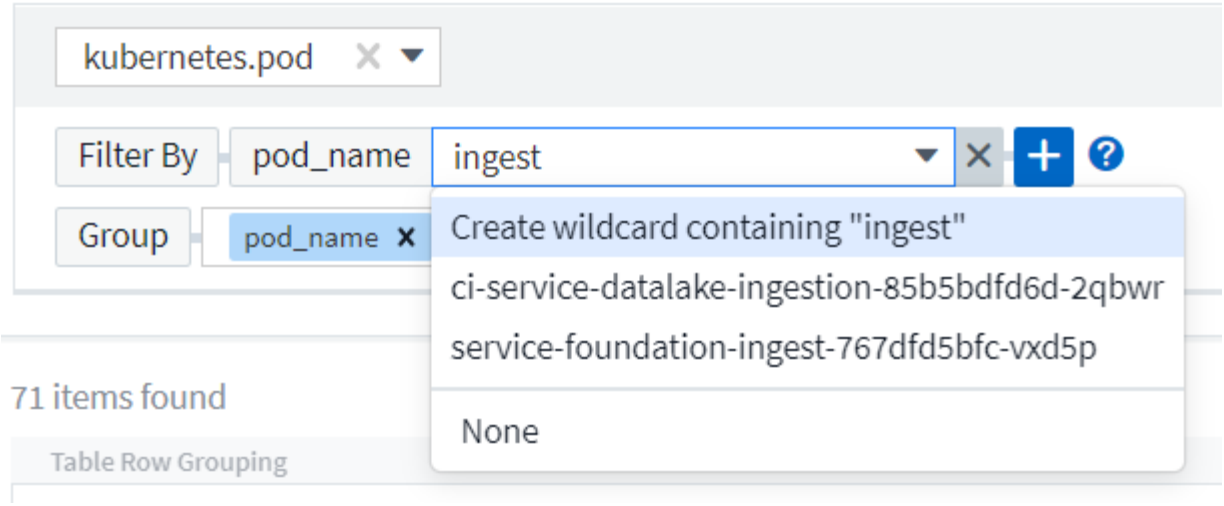
Filter Für Exakte Übereinstimmung

Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse, die ein wortwörtlicher Stern sind; das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren UND, OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in Doppelzitate eingeschlossen sind.

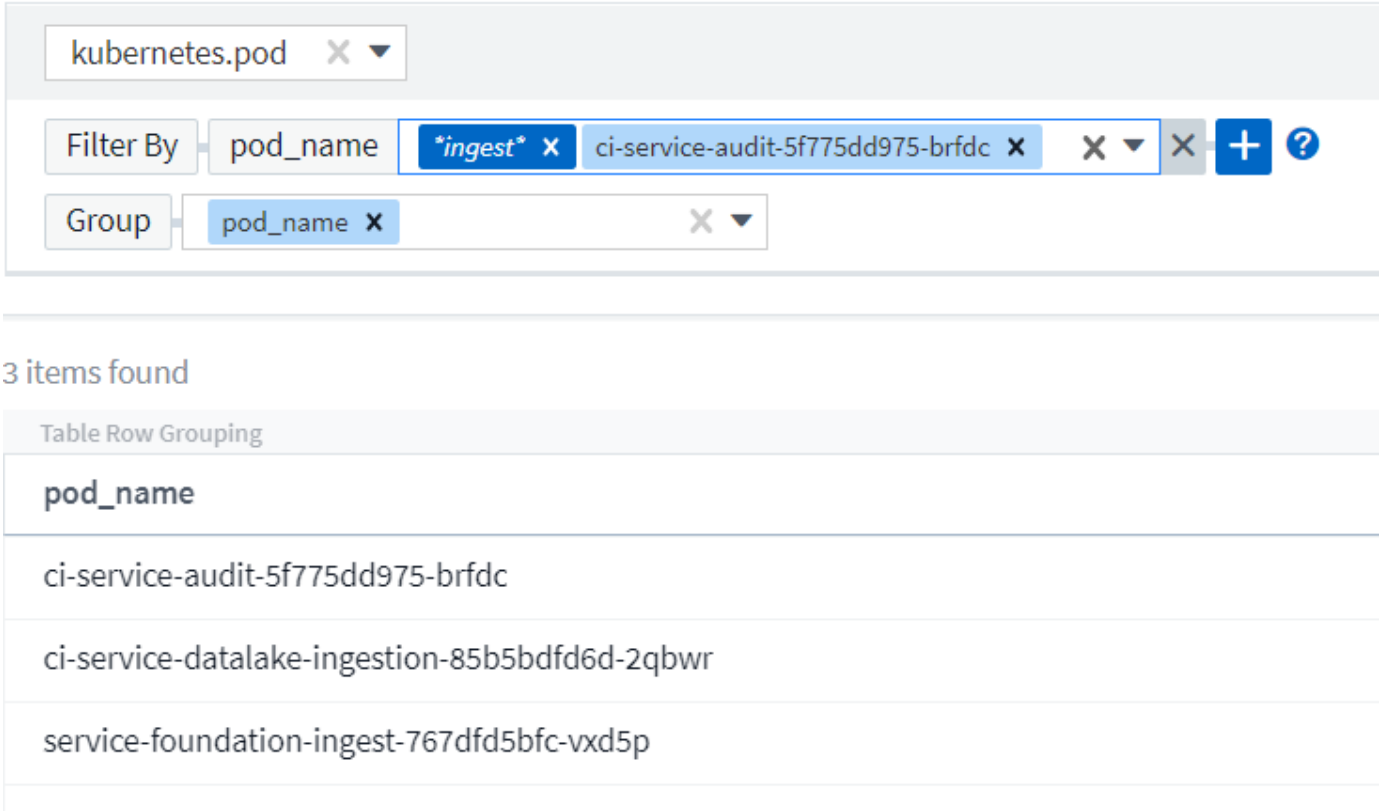
Sie können mithilfe von „Exact Match“-Filtern nach bestimmten Ressourcen suchen, z. B. nach Hostnamen. Wenn Sie nur den Hostnamen 'Marketing' finden möchten, aber 'Marketings-boston' ausschließen möchten, schließen Sie einfach den Namen "Marketing" in doppelte Anführungszeichen ein.

Platzhalter und Ausdrücke

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text- oder Listenwerten filtern, werden Sie beim Eingeben mit der Option angezeigt, basierend auf dem aktuellen Text einen **Platzhalter-Filter** zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse angezeigt, die dem Platzhalterausdruck entsprechen. Sie können auch **Expressions** mit NOT oder ODER erstellen, oder Sie können die Option "Keine" auswählen, um nach Null-Werten im Feld zu filtern.



Filter basierend auf Platzhalter oder Ausdrücken (z. B. NICHT, ODER, „Keine“ usw.) wird im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.



Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit numerischen Werten, Daten oder Booleanen.

Erweiterte Textfilterung mit Vorschlägen zum Kontexttyp

Filtern in Widget-Abfragen ist *contextal*. Wenn Sie einen Filterwert oder Werte für ein Feld auswählen, werden die anderen Filter für diese Abfrage Werte angezeigt, die für diesen Filter relevant sind. Wenn Sie beispielsweise einen Filter für ein bestimmtes Objekt *Name* festlegen, zeigt das Feld, das nach *Model* gefiltert werden soll, nur Werte an, die für diesen Objektnamen relevant sind.

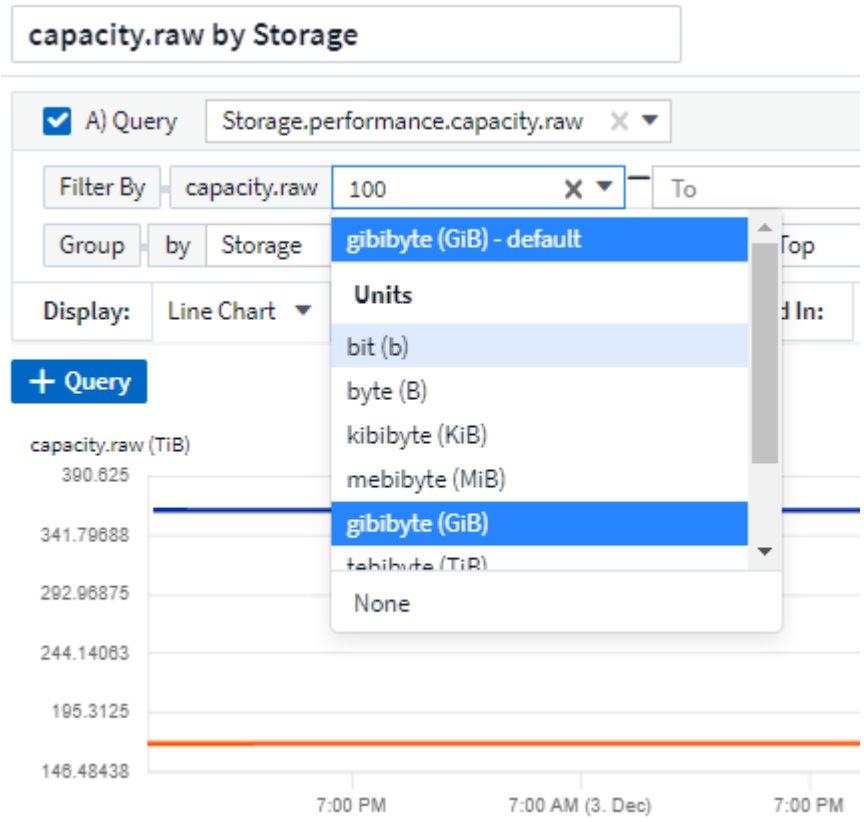
Kontextbezogene Filterung gilt auch für Dashboard-Seitenvariablen (nur Textattribute oder Anmerkungen). Wenn Sie einen Filer-Wert für eine Variable auswählen, werden bei allen anderen Variablen, die verwandte Objekte verwenden, nur mögliche Filterwerte auf der Grundlage dieser verwandten Variablen angezeigt.

Beachten Sie, dass nur Textfilter Kontextvorschläge anzeigen. Datum, Enum (Liste) usw. zeigt keine Vorschläge für den Voraus-Typ an. Das heißt, Sie können einen Filter auf ein Enum (d.h. Liste) Feld setzen und haben andere Textfelder im Kontext gefiltert. Wenn Sie z. B. einen Wert in einem Feld „Enum“ wie „Data Center“ auswählen, werden in anderen Filtern nur die Modelle/Namen in diesem Rechenzentrum angezeigt), nicht jedoch umgekehrt.

Der ausgewählte Zeitbereich stellt auch Kontext für die in Filtern angezeigten Daten bereit.

Auswählen der Filtereinheiten

Wenn Sie einen Wert in ein Filterfeld eingeben, können Sie die Einheiten auswählen, in denen die Werte auf dem Diagramm angezeigt werden sollen. Beispielsweise können Sie nach der Rohkapazität filtern und im deafult gib anzeigen, oder wählen Sie ein anderes Format wie tib aus. Dies ist nützlich, wenn auf dem Dashboard mehrere Diagramme angezeigt werden, die Werte in tib anzeigen, und Sie möchten, dass alle Diagramme konsistente Werte anzeigen.



Zusätzliche Filterveredlungen

Mit den folgenden Optionen können Sie Ihre Filter weiter verfeinern.

- Mit einem Sternchen können Sie nach allem suchen. Beispiel:

```
vol*rhel
```

Zeigt alle Ressourcen an, die mit „vol“ beginnen und mit „RHEL“ enden.

- Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Beispiel:

```
BOS-PRD??-S12
```

Zeigt *BOS-PRD12-S12*, *BOS-PRD13-S12* usw. an.

- Mit dem Operator ODER können Sie mehrere Einheiten angeben. Beispiel:

```
FAS2240 OR CX600 OR FAS3270
```

Findet mehrere Storage-Modelle

- Der NICHT-Operator ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen. Beispiel:

```
NOT EMC*
```

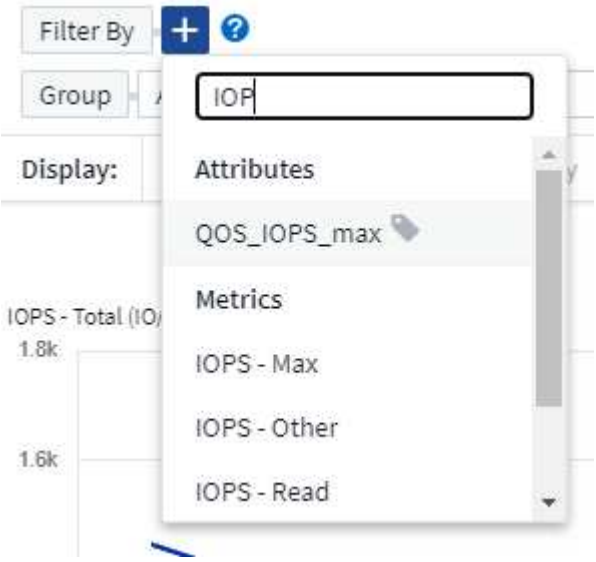
Findet alles, was nicht mit „EMC“ beginnt. Verwenden Sie können

```
NOT *
```

So zeigen Sie Felder an, die keinen Wert enthalten.

Identifizieren von Objekten, die von Abfragen und Filtern zurückgegeben werden

Die von Abfragen und Filtern zurückgegebenen Objekte sehen ähnlich aus wie in der folgenden Abbildung. Objekte, denen Tags zugewiesen sind, sind Annotationen, während die Objekte ohne Tags Performance-Zähler oder Objektattribute sind.



Gruppierung und Aggregation

Gruppierung (Rolling Up)

Die in einem Widget angezeigten Daten werden aus den zugrunde liegenden Datenpunkten, die während der Akquisition gesammelt wurden, gruppiert (manchmal als aufgerollt bezeichnet). Wenn Sie beispielsweise ein Liniendiagramm mit Storage-IOPS im Laufe der Zeit haben, kann es sinnvoll sein, eine separate Zeile für jedes Ihrer Datacenter zu sehen, um einen schnellen Vergleich zu erzielen. Sie haben verschiedene Möglichkeiten, diese Daten zu gruppieren:

- **Durchschnitt**: Zeigt jede Zeile als den *Mittelwert* der zugrunde liegenden Daten an.
- **Maximum**: Zeigt jede Zeile als *Maximum* der zugrunde liegenden Daten an.
- **Minimum**: Zeigt jede Zeile als *minimum* der zugrunde liegenden Daten an.
- **Sum**: Zeigt jede Zeile als die *Summe* der zugrunde liegenden Daten an.
- **Anzahl**: Zeigt eine *Anzahl* von Objekten an, die Daten innerhalb des angegebenen Zeitrahmens gemeldet haben. Sie können das *gesamte Zeitfenster* gemäß dem Zeitbereich des Dashboards auswählen.

Schritte

Gehen Sie wie folgt vor, um die Gruppierungsmethode festzulegen.

1. Wählen Sie in der Abfrage des Widgets einen Asset-Typ und eine Kennzahl (z. B. *Storage*) und eine Kennzahl (z. B. „ Performance IOPS Total_“) aus.
2. Wählen Sie für **Group** eine Roll-up-Methode (z. B. *Average*) aus, und wählen Sie die Attribute oder Metriken aus, mit denen die Daten (z. B. *Data Center*) angezeigt werden sollen.

   Das Widget wird automatisch aktualisiert und zeigt Daten für jedes Datacenter an.

Sie können auch auswählen, *all* der zugrunde liegenden Daten in das Diagramm oder die Tabelle zu gruppieren. In diesem Fall erhalten Sie für jede Abfrage im Widget eine einzelne Zeile, in der der Durchschnitt, das Minimum, das Maximum, die Summe oder die Anzahl der gewählten Metrik oder der Kennzahlen für alle zugrunde liegenden Assets angezeigt wird.

Durch Klicken auf die Legende für jedes Widget, dessen Daten nach „Alle“ gruppiert sind, wird eine Abfrageseite mit den Ergebnissen der ersten Abfrage geöffnet, die im Widget verwendet wird.

Wenn Sie einen Filter für die Abfrage festgelegt haben, werden die Daten basierend auf den gefilterten Daten gruppiert.

Beachten Sie, dass Sie, wenn Sie ein Widget nach einem beliebigen Feld gruppieren möchten (z. B. „*Model*“), trotzdem nach diesem Feld filtern müssen, um die Daten für dieses Feld auf dem Diagramm oder der Tabelle korrekt anzuzeigen.

Aggregation von Daten

Sie können Ihre Zeitreihendiagramme (Linien-, Bereich usw.) weiter abstimmen, indem Sie Datenpunkte in Minuten-, Stunden- oder Tages-Buckets aggregieren, bevor diese Daten anschließend nach Attribut gerollt werden (falls ausgewählt). Sie können Datenpunkte nach ihrem *Durchschnitt, Maximum, Minimum, Sum* oder *Count* aggregieren.

Ein kleines Intervall kombiniert mit einem langen Zeitbereich kann zu einem "Aggregation-Intervall führte zu zu zu vielen Datenpunkten." Warnung. Falls Sie in einem kleinen Intervall den Zeitrahmen für das Dashboard auf 7 Tage verkürzen möchten, werden Sie diesen vielleicht feststellen. In diesem Fall erhöht Insight

vorübergehend das Aggregationsintervall, bis Sie einen kleineren Zeitrahmen auswählen.

Sie können Daten auch im Balkendiagramm-Widget und im Widget mit Einzelwerten aggregieren.

Die meisten Asset-Zähler aggregieren standardmäßig auf *Average*. Einige Zähler aggregieren standardmäßig auf *Max, Min* oder *sum*. Beispielsweise aggregieren die Port-Fehler standardmäßig auf *sum*, wo Storage-IOPS-Aggregat zu *Average* lautet.

Anzeige Der Oberen/Unteren Ergebnisse

In einem Diagramm-Widget können Sie entweder die **Top**- oder **bottom**-Ergebnisse für gerollte Daten anzeigen und die Anzahl der Ergebnisse aus der angezeigten Dropdown-Liste auswählen. In einem TabellenWidget können Sie nach einer beliebigen Spalte sortieren.

Diagramm-Widget oben/unten

Wenn Sie in einem Diagramm-Widget Daten nach einem bestimmten Attribut einrollen möchten, haben Sie die Möglichkeit, entweder die oberen N- oder unteren N-Ergebnisse anzuzeigen. Beachten Sie, dass Sie die oberen oder unteren Ergebnisse nicht auswählen können, wenn Sie durch *all*-Attribute Rollen möchten.

Sie können wählen, welche Ergebnisse angezeigt werden sollen, indem Sie im Feld **Anzeigen** oder **unten** der Abfrage * einen Wert aus der Liste auswählen.

Tabelle Widget zeigt Einträge an

In einem TabellenWidget können Sie die Anzahl der in den Tabellenergebnissen angezeigten Ergebnisse auswählen. Sie haben nicht die Möglichkeit, obere oder untere Ergebnisse zu wählen, da Sie in der Tabelle nach Bedarf aufsteigend oder absteigend sortieren können.

Sie können die Anzahl der Ergebnisse auswählen, die in der Tabelle auf dem Dashboard angezeigt werden sollen, indem Sie einen Wert aus dem Feld **Einträge anzeigen** der Abfrage auswählen.

Gruppierung in TabellenWidget

Die Daten in einem TabellenWidget können nach allen verfügbaren Attributen gruppiert werden. So können Sie einen Überblick über Ihre Daten anzeigen und sie für mehr Details anzeigen. Metriken in der Tabelle werden für eine einfache Anzeige in jeder zusammenklappbaren Zeile aufgerollt.

Mit den Tabelle-Widgets können Sie Ihre Daten anhand der von Ihnen festgelegten Attribute gruppieren. Vielleicht soll in Ihrer Tabelle der gesamte Storage IOPS angezeigt werden, der nach Datacentern gruppiert ist, in denen diese Storages gespeichert sind. Oder Sie möchten eine Tabelle von virtuellen Maschinen anzeigen, die nach dem Hypervisor gruppiert sind, der sie hostet. In der Liste können Sie jede Gruppe erweitern, um die Assets in dieser Gruppe anzuzeigen.

Die Gruppierung ist nur im Widget-Typ Tabelle verfügbar.

Beispiel für Gruppierung (mit Rollup-Erklärung)

Mit den Tabelle-Widgets können Sie Daten gruppieren, um die Anzeige zu erleichtern.

In diesem Beispiel werden wir ein TabellenWidget erstellen, das alle VMs nach Datacenter gruppiert zeigt.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard, und fügen Sie ein Widget mit * Table* hinzu.

2. Wählen Sie *Virtual Machine* als Asset-Typ für dieses Widget aus.
3. Klicken Sie auf die Spaltenauswahl und wählen Sie *Hypervisor Name* und *IOPS - Total*.

   Diese Spalten werden jetzt in der Tabelle angezeigt.

4. Ignorieren Sie alle VMs ohne IOPS und schließen Sie nur VMs ein, die insgesamt IOPS mehr als 1 haben. Klicken Sie auf die Schaltfläche **Filter by [+]** und wählen Sie *IOPS - Total*. Klicken Sie auf *any*, und geben Sie im Feld **von 1** ein. Lassen Sie das Feld * to* leer. Klicken Sie auf Enter ot, und klicken Sie auf das Filterfeld, um den Filter anzuwenden.

   In der Tabelle werden jetzt alle VMs mit IOPS-Gesamtwerten größer oder gleich 1 angezeigt. Beachten Sie, dass es keine Gruppierung in der Tabelle gibt. Alle VMs werden angezeigt.

5. Klicken Sie auf die Schaltfläche **Group by [+]**.

   Sie können nach beliebigen Attributen oder Kommentaren gruppieren. Wählen Sie „ Alle_“, um alle VMs in einer einzelnen Gruppe anzuzeigen.

   In jedem Spaltenkopf für eine Leistungskennzahl wird ein Menü „drei Punkte“ mit einer Option **Roll Up** angezeigt. Die Standard-Rollup-Methode lautet *Average*. Das bedeutet, dass die für die Gruppe angezeigte Zahl der Durchschnitt aller gesamten IOPS ist, die für jede VM innerhalb der Gruppe gemeldet wurden. Sie können diese Spalte um *Durchschnitt, Summe, Minimum* oder *Maximum* nach oben Rollen. Alle angezeigten Spalten mit Performance-Metriken können individuell aufgerollt werden.

6. Klicken Sie auf *All* und wählen Sie *Hypervisor Name* aus.

   Die VM-Liste ist jetzt nach Hypervisor gruppiert. Sie können jeden Hypervisor erweitern, um die von ihm gehosteten VMs anzuzeigen.

7. Klicken Sie auf **Speichern**, um die Tabelle im Dashboard zu speichern. Sie können die Größe des Widgets ändern oder verschieben.
8. Klicken Sie auf **Speichern**, um das Dashboard zu speichern.

Aufkommen von Performance-Daten

Wenn Sie eine Spalte für Leistungsdaten (z. B. *IOPS - Total*) in ein TabellenWidget einfügen, können Sie bei Auswahl der Gruppierung der Daten eine Aufrollmethode für diese Spalte auswählen. Die Standard-Roll-up-Methode ist die Anzeige des Durchschnitts (*avg*) der zugrunde liegenden Daten in der Gruppenzeile. Sie können auch die Summe, das Minimum oder das Maximum der Daten anzeigen.

Dashboard-Zeitbereich – Auswahl

Sie können den Zeitbereich für Ihre Dashboard-Daten auswählen. Nur für den ausgewählten Zeitbereich relevante Daten werden in Widgets auf dem Dashboard angezeigt. Sie können aus folgenden Zeitbereichen auswählen:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Die Letzten 2 Stunden
- Die letzten 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

  Im benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinander folgende Tage auswählen. Sie können für diesen Bereich auch die Startzeit und die Endzeit des Tages festlegen. Die standardmäßige Startzeit ist 12:00 UHR am ersten ausgewählten Tag und die standardmäßige Endzeit ist am letzten ausgewählten Tag 11:59 Uhr. Durch Klicken auf **Anwenden** wird der benutzerdefinierte Zeitbereich auf das Dashboard angewendet.

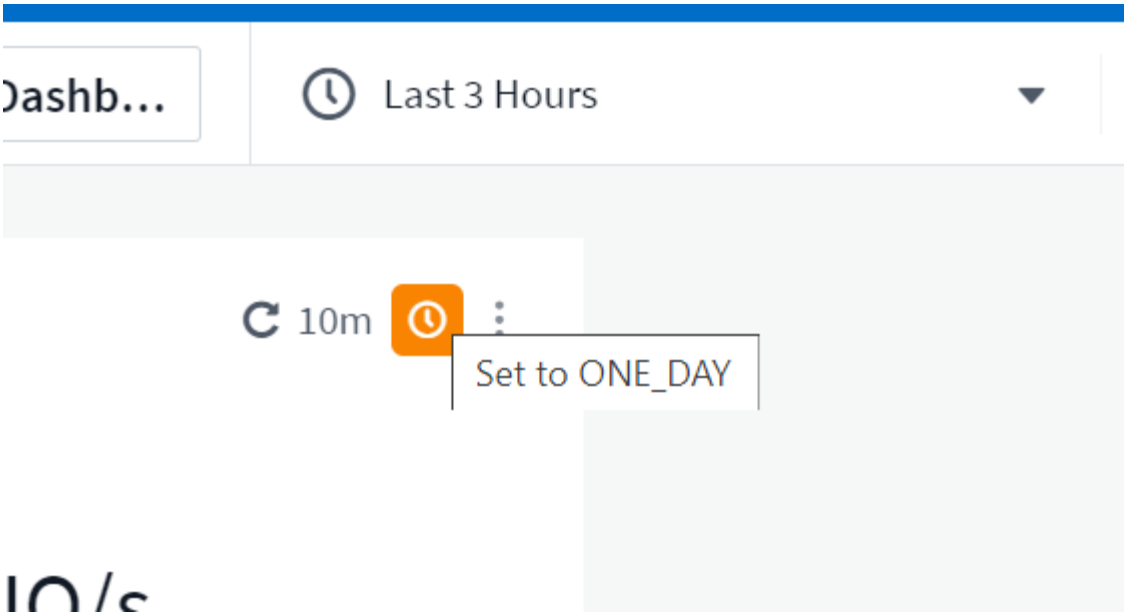
Dashboard-Zeit in einzelnen Widgets außer Kraft setzen

Sie können die Einstellung für den Hauptzeitbereich des Dashboards in den einzelnen Widgets überschreiben. Diese Widgets zeigen Daten basierend auf dem eingestellten Zeitrahmen an, nicht auf dem Zeitrahmen des Dashboards.

Um die Dashboard-Zeit außer Kraft zu setzen und ein Widget dazu zu zwingen, seinen eigenen Zeitrahmen zu verwenden, wählen Sie im Bearbeitungsmodus des Widgets den deisired Zeitbereich aus, und speichern Sie das Widget im Dashboard.

Das Widget zeigt seine Daten entsprechend dem dafür eingestellten Zeitrahmen an, unabhängig vom ausgewählten Zeitrahmen auf dem Dashboard selbst.

Der Zeitrahmen, den Sie für ein Widget festlegen, hat keine Auswirkungen auf andere Widgets auf dem Dashboard.



Primäre und sekundäre Achse

Verschiedene Metriken verwenden unterschiedliche Maßeinheiten für die Daten, die sie in einem Diagramm erfassen. Wenn wir beispielsweise IOPS betrachten, entspricht die Maßeinheit der Anzahl der I/O-Operationen pro Sekunde (I/O/s), während die Latenz lediglich ein Maß an Zeit ist (Millisekunden, Mikrosekunden, Sekunden usw.). Wenn Sie beide Metriken auf einem einzigen Liniendiagramm mit einem einzelnen Satz A-Werte für die Y-Achse angeben, werden die Latenzzahlen (normalerweise wenige Millisekunden) im selben Maßstab mit den IOPS (normalerweise sind Tausende) dargestellt und die Latenzzeile geht bei diesem Maßstab verloren.

Es ist jedoch möglich, beide Datensätze auf einem einzigen aussagekräftigen Diagramm zu grafisch zu gestalten, indem eine Maßeinheit auf der primären (linken) Y-Achse und die andere Maßeinheit auf der sekundären (rechten) Y-Achse eingestellt wird. Jede Metrik wird im eigenen Maßstab dokumentiert.

Schritte

Dieses Beispiel veranschaulicht das Konzept der primären und sekundären Achsen in einem Diagramm-Widget.

1. Erstellen oder Öffnen eines Dashboards. Fügen Sie dem Dashboard ein Liniendiagramm, ein Spline-Diagramm, ein Flächendiagramm oder ein Stacked Area Chart hinzu.
2. Wählen Sie einen Asset-Typ (z. B. *Storage*) aus, und wählen Sie für Ihre erste Metrik „*IOPS - Total*“ aus. Stellen Sie Ihre gewünschten Filter ein, und wählen Sie ggf. eine Roll-up-Methode aus.

   Die IOPS-Linie wird auf dem Diagramm angezeigt, wobei ihre Skalierung auf der linken Seite dargestellt ist.

3. Klicken Sie auf **[+Query]**, um eine zweite Zeile zum Diagramm hinzuzufügen. Wählen Sie für diese Zeile die Option *Latenz - Total* für die Kennzahl.

   Beachten Sie, dass die Linie flach am unteren Rand des Diagramms angezeigt wird. Der Grund dafür ist, dass sie *auf derselben Skala* wie die IOPS-Zeile gezeichnet wird.

4. Wählen Sie in der Latenzabfrage **Y-Achse: Sekundär** aus.

   Die Latenzlinie wird jetzt auf eigene Skala gezeichnet, die rechts im Diagramm angezeigt wird.

Ausdrücke in Widgets

In einem Dashboard können Sie mit einem Widget für Zeitreihen (Linie, Spline, Bereich, gestapelter Bereich), einem Balkendiagramm, einem Säulendiagramm, einem Kreisdiagramm oder einem Widget für Tabellen Ausdrücke aus von Ihnen ausgewählten Metriken erstellen und das Ergebnis dieser Ausdrücke in einem einzigen Diagramm (oder einer Spalte im Fall des) anzeigen Widget „Tabelle“). Die folgenden Beispiele verwenden Ausdrücke, um bestimmte Probleme zu lösen. Im ersten Beispiel möchten wir den IOPS-Wert für alle Storage Assets in unserer Umgebung als Prozentsatz von IOPS insgesamt darstellen. Das zweite Beispiel gibt Einblick in die in Ihrer Umgebung auftretenden IOPS des „Systems“ oder „Overhead“ - jene IOPS, die nicht direkt vom Lesen oder Schreiben von Daten stammen.

Sie können Variablen in Ausdrücken verwenden (z. B. _ € Var1 * 100_)

Ausdrücke Beispiel: Lese-IOPS in Prozent

In diesem Beispiel möchten wir den IOPS-Wert für Lesevorgänge als Prozentsatz des gesamten IOPS anzeigen. Sie können sich dies als folgende Formel vorstellen:

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Diese Daten können in einem Liniendiagramm auf Ihrem Dashboard angezeigt
werden. Um dies zu tun, führen Sie folgende Schritte aus:
```

Schritte

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im Bearbeitungsmodus.
2. Fügen Sie ein Widget zum Dashboard hinzu. Wählen Sie **Flächendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage mit *IOPS - Total* für *Storage* Assets angezeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Klicken Sie rechts auf den Link **in Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Beachten Sie, dass Sie den Asset-Typ im Expression-Modus nicht ändern können. Während Sie sich im Expression-Modus befinden, ändert sich der Link zu **revert to Query**. Klicken Sie auf diese Option, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass durch Umschalten zwischen den Modi die Felder auf ihre Standardeinstellungen zurückgesetzt werden.

   Bleiben Sie jetzt im Expression-Modus.

4. Die Metrik **IOPS - Total** befindet sich jetzt im alphabetischen Variablenfeld "**A**". Klicken Sie in der Variablen "**b**" auf **Auswählen** und wählen Sie **IOPS - Lesen**.

   Sie können insgesamt fünf alphabetische Variablen für Ihren Ausdruck hinzufügen, indem Sie auf die +-Schaltfläche nach den Variablenfeldern klicken. Für unser Beispiel in Bezug auf den Leseanteil benötigen wir lediglich Total IOPS ("**A**") und Lese-IOPS ("**b**").

5. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die jeder Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir wissen, dass Read prozentual = (Lese-IOPS / Gesamt-IOPS) x 100, also würden wir diesen Ausdruck schreiben als:

   ```
    (b / a) * 100
   . Das Feld *Beschriftung* kennzeichnet den Ausdruck. Ändern Sie die
   Bezeichnung in „Prozentsatz lesen‟ oder etwas, das für Sie gleichermaßen
   sinnvoll ist.
   . Ändern Sie das Feld *Einheiten* in „%‟ oder „Prozent‟.
   ```

   Das Diagramm zeigt den prozentualen IOPS-Leseanteil im Zeitverlauf für die ausgewählten Speichergeräte an. Auf Wunsch können Sie einen Filter einstellen oder eine andere Rollup-Methode auswählen. Beachten Sie, dass wenn Sie als Rollup-Methode Summe auswählen, alle Prozentwerte zusammen hinzugefügt werden, die möglicherweise über 100 % liegen können.

6. Klicken Sie auf **Speichern**, um das Diagramm auf Ihrem Dashboard zu speichern.

Ausdrücke Beispiel: "System" I/O

Beispiel 2: Zu den Kennzahlen, die von Datenquellen erfasst werden, zählen Lese-, Schreib- und IOPS-Gesamtwerte. Die Gesamtzahl der von einer Datenquelle gemeldeten IOPS umfasst jedoch manchmal „System“ IOPS, bei denen es sich um diese I/O-Vorgänge handelt, die nicht direkt zum Lesen oder Schreiben der Daten gehören. Dieser System-I/O kann auch als „Overhead“-I/O bezeichnet werden, der für einen ordnungsgemäßen Systembetrieb, aber nicht direkt mit Datenoperationen benötigt wird.

Zur Anzeige dieser System-I/OS können die Lese- und Schreib-IOPS von den insgesamt gemeldeten IOPS aus der Übernahme entfernt werden. Die Formel könnte wie folgt aussehen:

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Diese Daten können dann in einem Liniendiagramm auf Ihrem Dashboard
angezeigt werden. Um dies zu tun, führen Sie folgende Schritte aus:
```

Schritte

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im Bearbeitungsmodus.
2. Fügen Sie ein Widget zum Dashboard hinzu. Wählen Sie **Liniendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage mit *IOPS - Total* für *Storage* Assets angezeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Wählen Sie im Feld **Roll Up** die Option *sum* by *All*.

   Das Diagramm zeigt eine Zeile mit der Summe der IOPS-Gesamtwerte an.

4. Klicken Sie auf das Symbol *Diese Abfrage duplizieren* So erstellen Sie eine Kopie der Abfrage.

   Ein Duplikat der Abfrage wird unterhalb des Originals hinzugefügt.

5. Klicken Sie in der zweiten Abfrage auf die Schaltfläche **in Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Klicken Sie auf **Zurücksetzen auf Abfrage**, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass durch Umschalten zwischen den Modi die Felder auf ihre Standardeinstellungen zurückgesetzt werden.

   Bleiben Sie jetzt im Expression-Modus.

6. Die Metrik *IOPS - Total* befindet sich jetzt im alphabetischen Variablenfeld "**A**". Klicken Sie auf *IOPS - Total*, und ändern Sie ihn in *IOPS - Read*.
7. Klicken Sie in der Variablen "**b**" auf **Select** und wählen Sie *IOPS - Write*.
8. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die jeder Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir würden unseren Ausdruck einfach schreiben als:

   ```
   a + b
   ```

   Wählen Sie im Bereich Anzeige für diesen Ausdruck die Option **Flächendiagramm** aus.

9. Das Feld **Beschriftung** kennzeichnet den Ausdruck. Ändern Sie das Label in „System IOPS“ oder etwas, das für Sie gleichbedeutend ist.

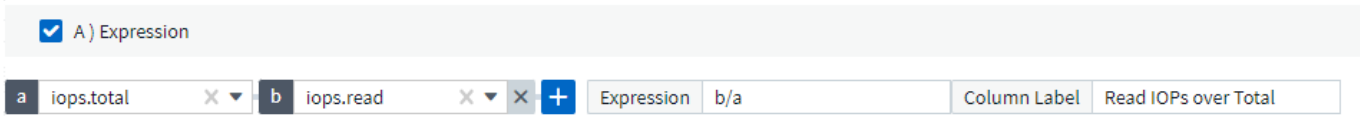
   Im Diagramm wird die IOPS insgesamt als Liniendiagramm angezeigt. In einem Flächendiagramm wird die Kombination aus Lese- und Schreib-IOPS unterhalb dieser Werte angezeigt. Die Lücke zwischen den beiden gibt die IOPS an, die nicht direkt mit Lese- oder Schreibvorgängen verbunden sind. Das sind Ihre „System“ IOPS.

10. Klicken Sie auf **Speichern**, um das Diagramm auf Ihrem Dashboard zu speichern.

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen ein, z. B. _ € var1 * 100_. Nur numerische Variablen können in Ausdrücken verwendet werden.

Ausdrücke in einem TabellenWidget

Tabellen-Widgets behandeln Ausdrücke etwas anders. Sie können bis zu fünf Ausdrücke in einem einzelnen Tabellen-Widget haben, von denen jeder als neue Spalte zur Tabelle hinzugefügt wird. Jeder Ausdruck kann bis zu fünf Werte enthalten, auf denen die Berechnung durchgeführt werden soll. Sie können die Spalte einfach etwas Sinnvolles benennen.



Variablen

Variablen ermöglichen es Ihnen, die in einigen oder allen Widgets auf einem Dashboard angezeigten Daten gleichzeitig zu ändern. Durch Festlegen eines oder mehrerer Widgets für die Verwendung einer allgemeinen Variable führen Änderungen an einem Ort dazu, dass die in jedem Widget angezeigten Daten automatisch

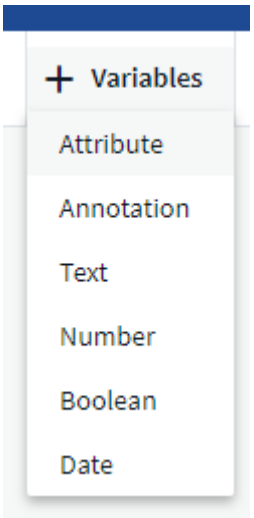
aktualisiert werden.

Dashboard-Variablen enthalten verschiedene Typen, können in verschiedenen Feldern verwendet werden und müssen Regeln für die Benennung befolgen. Diese Konzepte werden hier erläutert.

Variabentypen

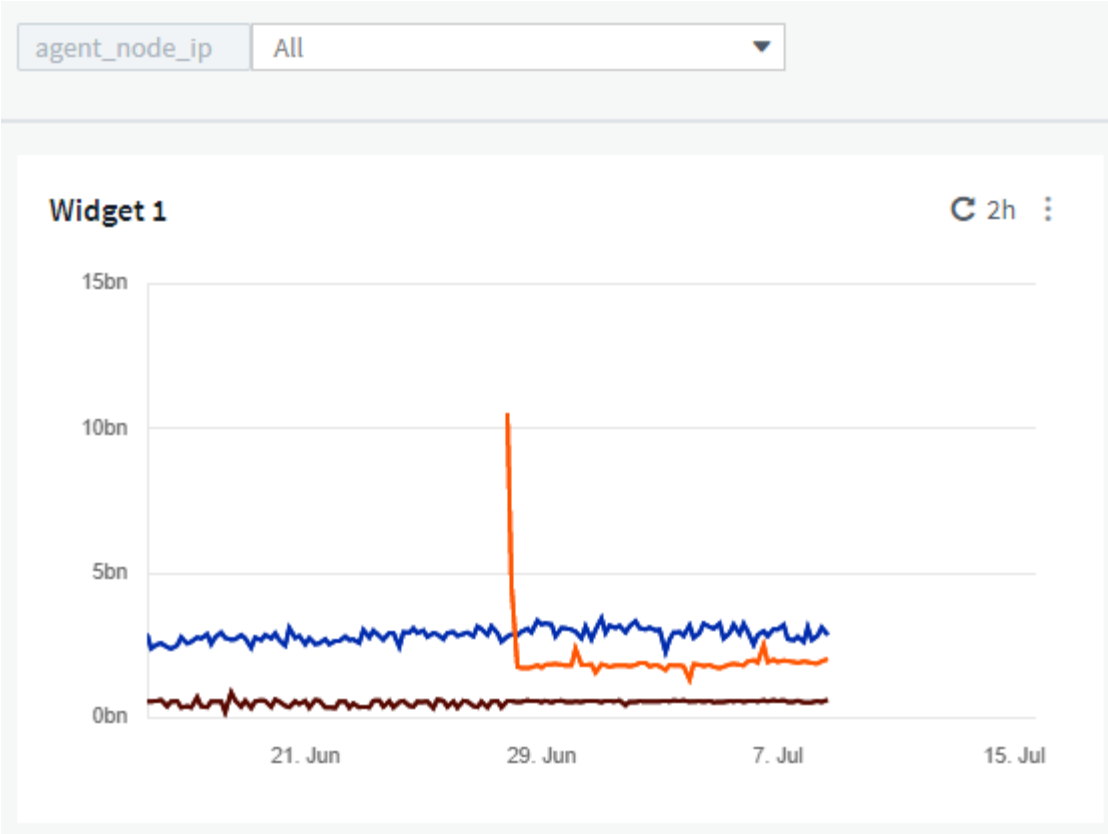
Eine Variable kann einen der folgenden Typen sein:

- **Attribut**: Verwenden Sie die Attribute oder Metriken eines Objekts, um sie zu filtern
- **Anmerkung**: Verwenden Sie eine vordefinierte "Anmerkung" Widget-Daten filtern.
- **Text**: Eine alphanumerische Zeichenfolge.
- **Numerisch**: Ein Zahlenwert. Sie können je nach Widget-Feld entweder selbst oder als „von“- oder „nach“-Wert verwenden.
- **Boolean**: Verwenden Sie für Felder mit Werten True/False, Yes/No, etc. Für die boolesche Variable stehen die Optionen Ja, Nein, Keine, Any.
- **Datum**: Ein Datumswert. Verwenden Sie je nach Konfiguration Ihres Widgets als „von“ oder „nach“-Wert.

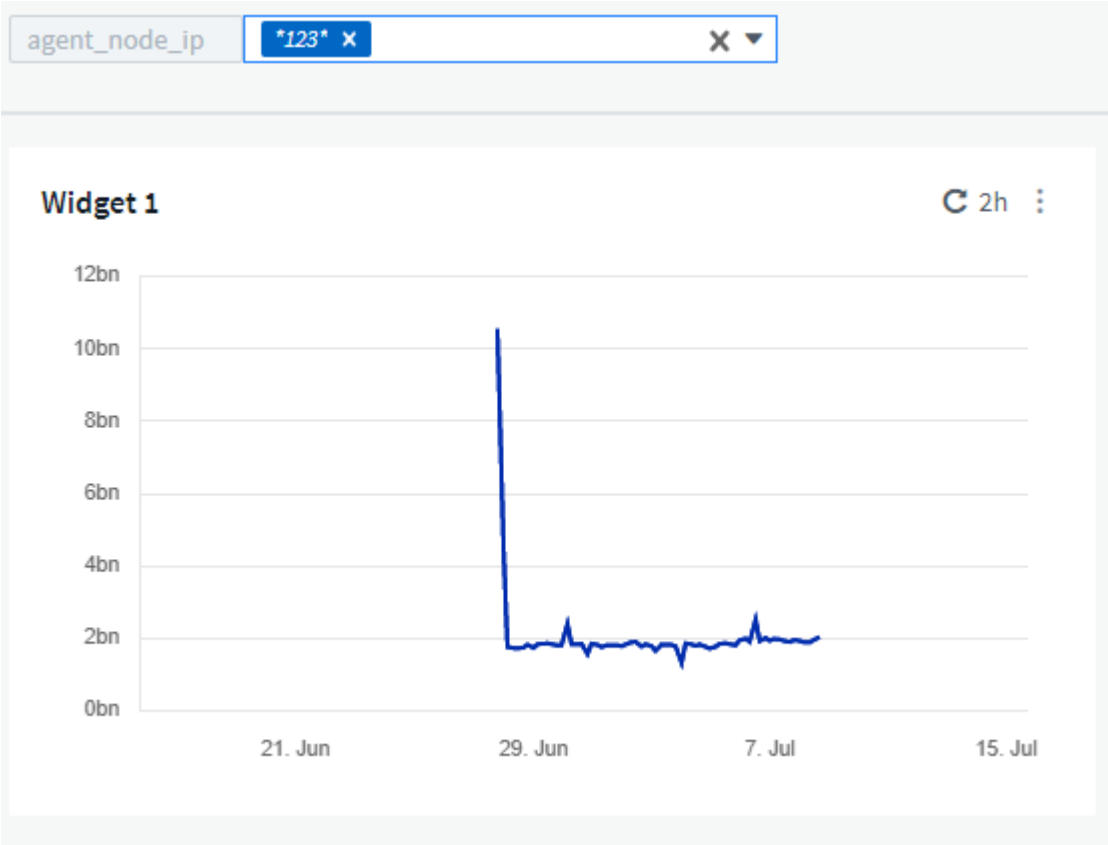


Attributvariablen

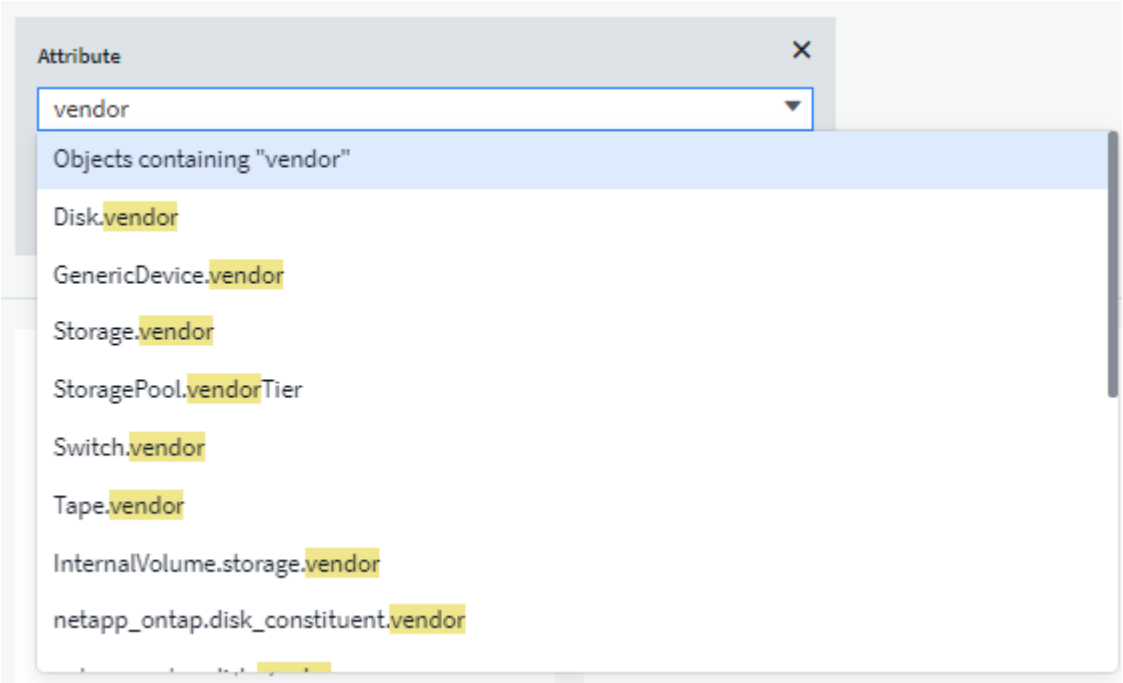
Durch die Auswahl einer Attributtypvariable können Sie nach Widget-Daten filtern, die den angegebenen Attributwert oder die angegebenen Werte enthalten. Das folgende Beispiel zeigt ein Line-Widget mit freien Speichertrends für Agent-Knoten. Wir haben eine Variable für Agent-Node-IPs erstellt, die derzeit auf die Anzeige aller IPs eingestellt ist:



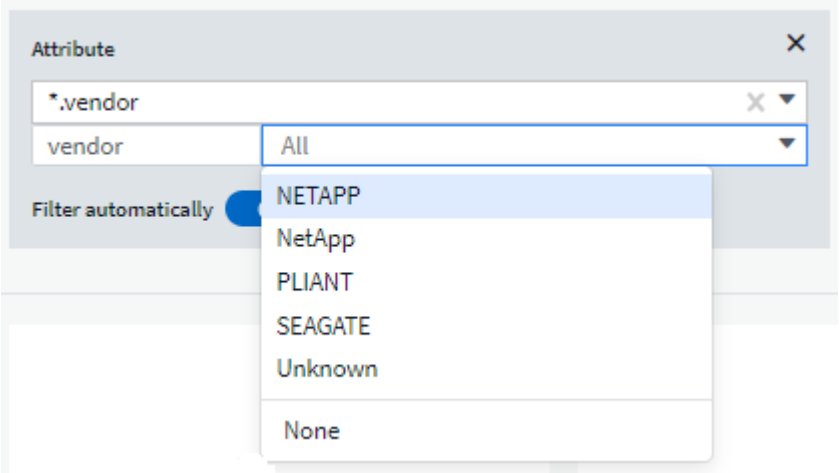
Wenn Sie jedoch vorübergehend nur Nodes in einzelnen Subnetzen in Ihrer Umgebung sehen möchten, können Sie die Variable in eine bestimmte Agent-Node-IP oder IPs einstellen oder ändern. Hier sehen wir nur die Knoten auf dem „123“ Subnetz:



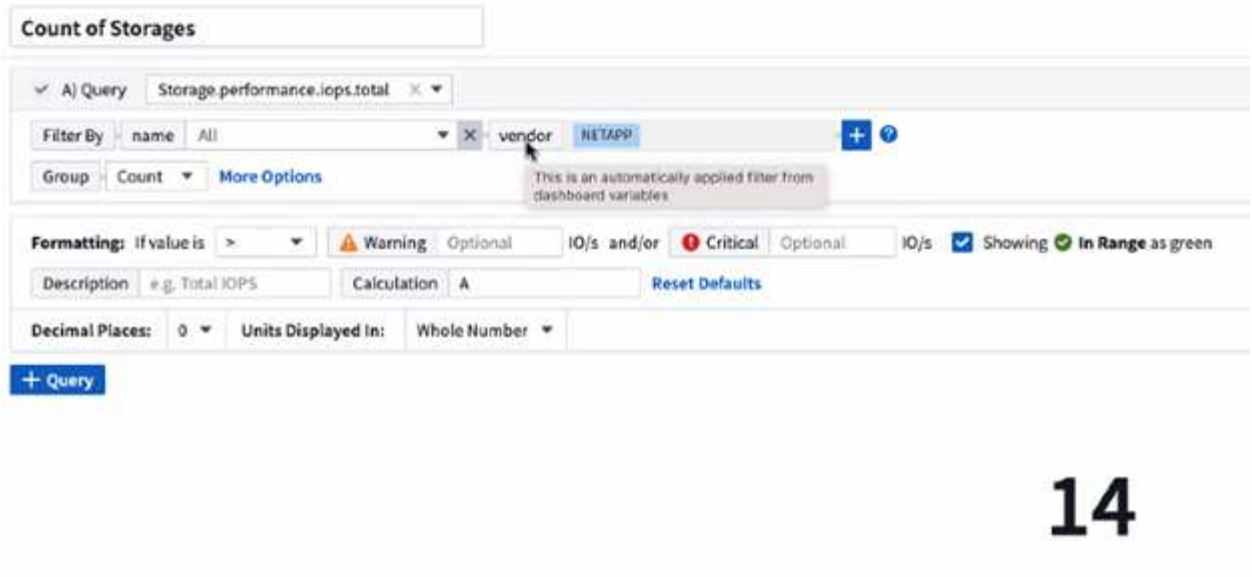
Sie können auch eine Variable festlegen, um unabhängig vom Objekttyp auf *all* Objekte mit einem bestimmten Attribut zu filtern, zum Beispiel Objekte mit einem Attribut "Anbieter", indem Sie **.Vendor* im Feld Variable angeben. Sie müssen nicht das "*." eingeben; Cloud Insights wird dies liefern, wenn Sie die Platzhalteroption auswählen.



Wenn Sie die Auswahlliste für den variablen Wert Dropdown, werden die Ergebnisse gefiltert, damit nur die verfügbaren Anbieter auf Basis der Objekte im Dashboard angezeigt werden.



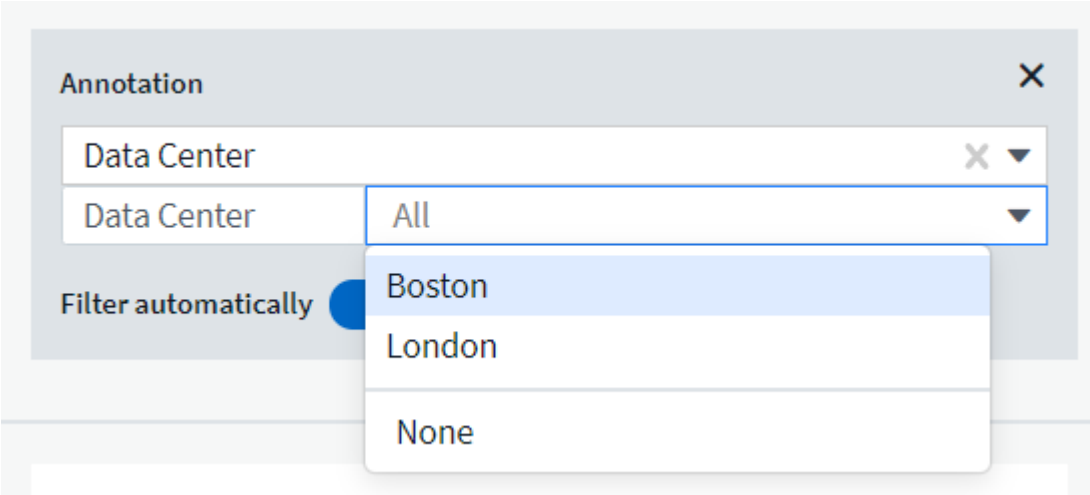
Wenn Sie ein Widget in Ihrem Dashboard bearbeiten, in dem der Attributfilter relevant ist (d. h. die Objekte des Widgets enthalten ein beliebiges **.Vendor-Attribut*), zeigt es Ihnen an, dass der Attributfilter automatisch angewendet wird.



Das Anwenden von Variablen ist genauso einfach wie das Ändern der Attributdaten Ihrer Wahl.

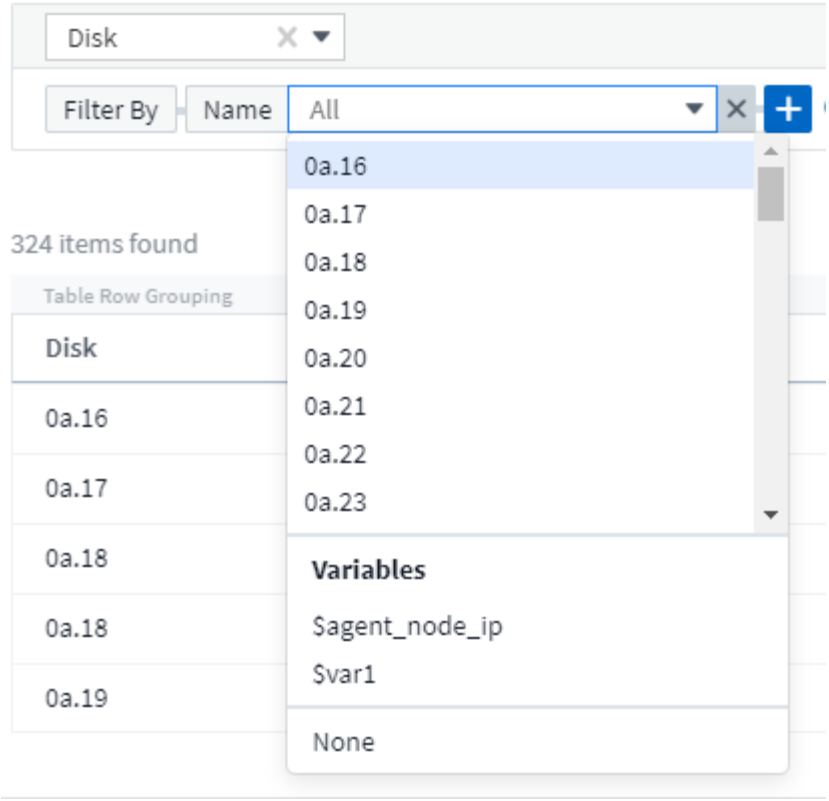
Anmerkungsvariablen

Durch Auswahl einer Anmerkungsvariable können Sie nach Objekten filtern, die mit dieser Anmerkung verknüpft sind, z. B. Objekten, die zum selben Rechenzentrum gehören.



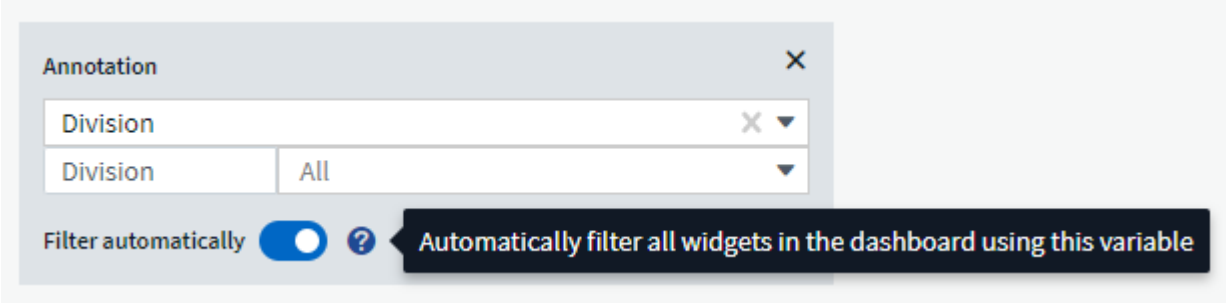
Text, Nummer, Datum oder Boolesche Variable

Sie können generische Variablen erstellen, die nicht mit einem bestimmten Attribut verknüpft sind, indem Sie einen Variablentyp von *Text*, *Number*, *Boolean* oder *Date* auswählen. Sobald die Variable erstellt wurde, können Sie sie in einem Widget-Filterfeld auswählen. Beim Festlegen eines Filters in einem Widget werden zusätzlich zu bestimmten Werten, die Sie für den Filter auswählen können, alle Variablen angezeigt, die für das Dashboard erstellt wurden. Diese werden im Dropdown-Menü unter dem Abschnitt „Variablen“ gruppiert und haben Namen, die mit „€“ beginnen. Wenn Sie eine Variable in diesem Filter auswählen, können Sie nach Werten suchen, die Sie im Feld Variable im Dashboard selbst eingeben. Alle Widgets, die diese Variable in einem Filter verwenden, werden dynamisch aktualisiert.



Bereich Für Variablenfilter

Wenn Sie Ihrem Dashboard eine Annotation- oder Attributvariable hinzufügen, kann die Variable auf *all* Widgets auf dem Dashboard angewendet werden. Das bedeutet, dass alle Widgets auf Ihrem Dashboard die Ergebnisse anzeigen, die entsprechend dem Wert gefiltert werden, den Sie in der Variable festgelegt haben.



Beachten Sie, dass nur Attribut- und Anmerkungsvariablen so automatisch gefiltert werden können. Variablen ohne Anmerkung oder -Attribut können nicht automatisch gefiltert werden. Die einzelnen Widgets müssen so konfiguriert werden, dass sie Variablen dieser Typen verwenden.

Um die automatische Filterung so zu deaktivieren, dass die Variable nur für die Widgets gilt, in denen Sie sie speziell eingestellt haben, klicken Sie auf den Schieberegler „automatisch filtern“, um sie zu deaktivieren.

Um eine Variable in einem einzelnen Widget zu setzen, öffnen Sie das Widget im Bearbeitungsmodus und wählen Sie die spezifische Anmerkung oder das Attribut im Feld *Filter by* aus. Bei einer Anmerkungsvariable können Sie einen oder mehrere bestimmte Werte auswählen oder den Variablennamen (angegeben durch die führende „€“) auswählen, um die Eingabe der Variable auf der Dashboard-Ebene zu ermöglichen. Das gleiche gilt für Attributvariablen. Nur die Widgets, für die Sie die Variable festlegen, werden die gefilterten Ergebnisse angezeigt.

Die Filterung in Variablen ist *contextal*; wenn Sie einen Filterwert oder Werte für eine Variable auswählen, werden die anderen Variablen auf Ihrer Seite nur für diesen Filter relevante Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf einen bestimmten Speicher *Model* setzen, werden alle Variablen, die für den Speicher *Name* gefiltert werden, nur für dieses Modell relevante Werte angezeigt.

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen als Teil des Ausdrucks ein, z. B. _ € var1 * 100_. Nur numerische Variablen können in Ausdrücken verwendet werden. In Ausdrücken können keine numerischen Anmerkungs- oder Attributvariablen verwendet werden.

Die Filterung in Variablen ist *contextal*; wenn Sie einen Filterwert oder Werte für eine Variable auswählen, werden die anderen Variablen auf Ihrer Seite nur für diesen Filter relevante Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf einen bestimmten Speicher *Model* setzen, werden alle Variablen, die für den Speicher *Name* gefiltert werden, nur für dieses Modell relevante Werte angezeigt.

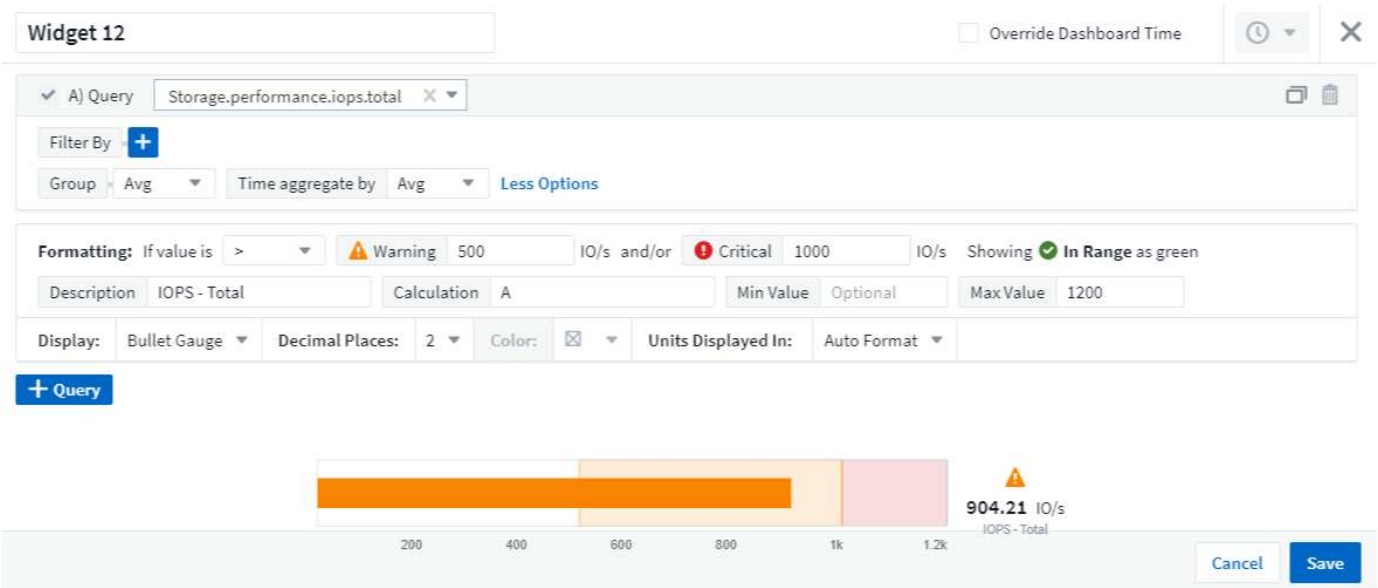
Variablenbenennung

Variablennamen:

- Darf nur die Buchstaben a-z, die Ziffern 0-9, Punkt (.), Unterstrich (_) und Leerzeichen ( ) enthalten.
- Darf nicht länger als 20 Zeichen sein.
- Achten Sie auf Groß- und Kleinschreibung: Cityname in Höhe von USD und Cityname sind verschiedene Variablen.
- Darf nicht mit einem vorhandenen Variablennamen identisch sein.
- Darf nicht leer sein.

Formatieren Von Messbreitewidgets

Mit den Widgets für Volumenanzeige und Glühlampen können Sie Schwellenwerte für die Stufen *Warnung* und/oder *kritisch* festlegen, um die angegebenen Daten klar zu darstellen.

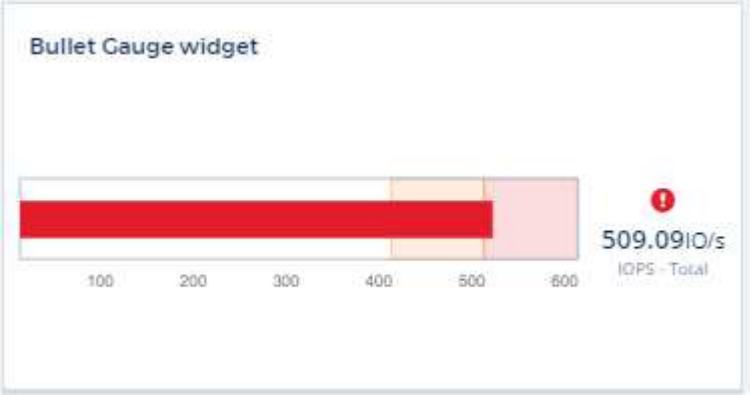


So legen Sie die Formatierung für diese Widgets fest:

1. Wählen Sie aus, ob Sie Werte größer als (>) oder kleiner als (<) Ihre Schwellenwerte markieren möchten. In diesem Beispiel werden Werte hervorgehoben, die größer sind als (>) die Schwellwerte.

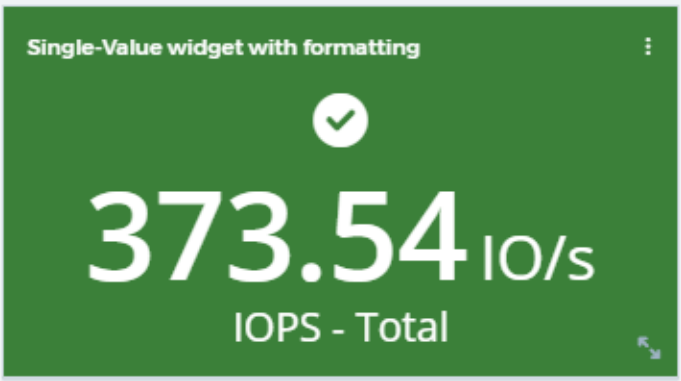
2. Wählen Sie einen Wert für den Schwellenwert „Warnung“ aus. Wenn im Widget Werte angezeigt werden, die größer als diese Stufe sind, wird die Anzeige orange angezeigt.
3. Wählen Sie einen Wert für den „kritischen“ Schwellenwert aus. Wenn die Werte größer sind als diese Stufe, wird das Messgerät rot angezeigt.

Sie können optional einen Mindest- und Maximalwert für die Messuhr auswählen. Die Werte unter dem Mindestwert werden nicht angezeigt. Werte über dem Maximum zeigen einen vollen Wert an. Wenn Sie keine Mindest- oder Höchstwerte auswählen, wählt das Widget basierend auf dem Wert des Widgets die optimale Min- und Höchstwert aus.



Formatieren Eines Single-Value-Widgets

Im Widget „Single-Value“ können Sie neben der Einstellung „Warning (orange)“ und „Critical (Red) schwellern die Werte im Bereich (die unterhalb der Warnstufe) mit grünem oder weißem Hintergrund anzeigen lassen.



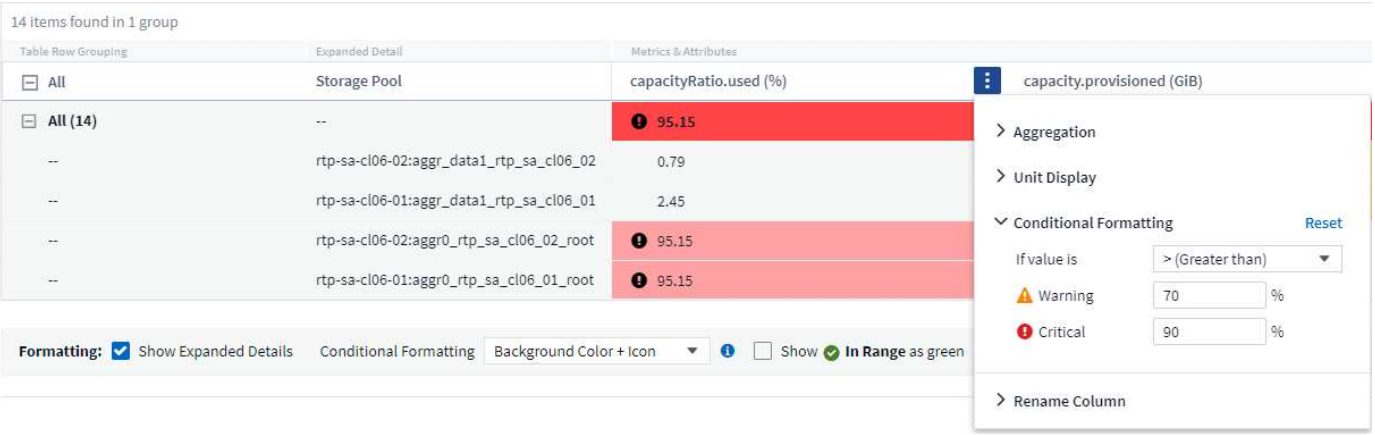
Wenn Sie auf den Link in einem Widget mit einem Wert oder einem Gauge-Widget klicken, wird eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Formatieren Von Tabellenwidgets

Wie Widgets mit einem Wert und einer Anzeige können Sie bedingte Formatierungen in TabellenWidgets festlegen, sodass Sie Daten mit Farben und/oder speziellen Symbolen hervorheben können.

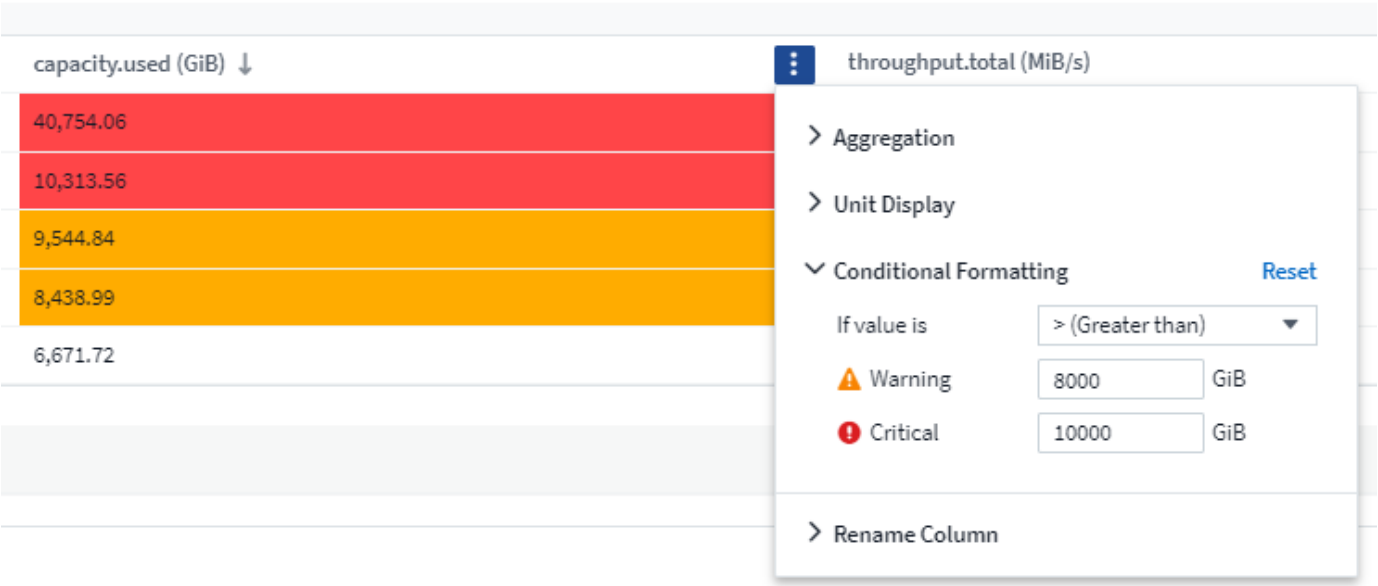
> Bedingte Formatierung ist derzeit in der Cloud Insights Bundesausgabe nicht verfügbar.

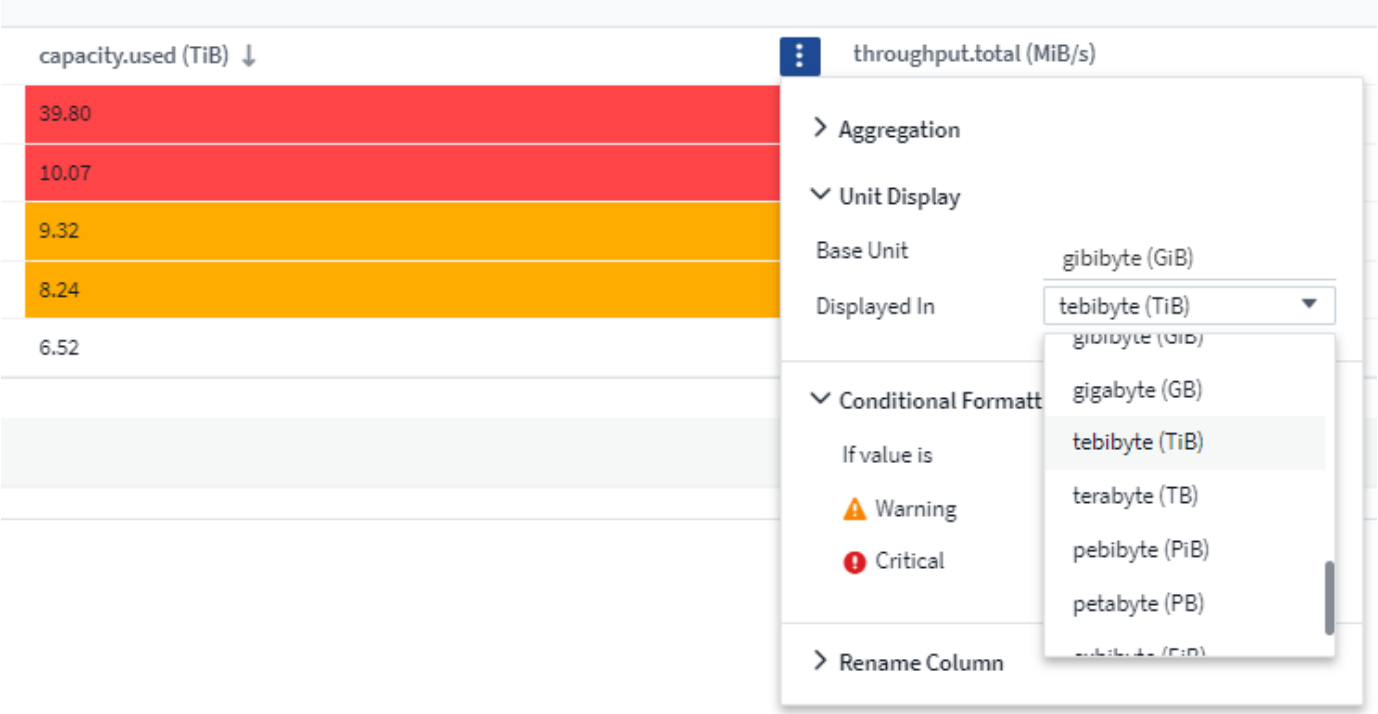
Mit Conditional Formatting können Sie Schwellenwerte auf Warnebene und kritische Ebene in den TabellenWidgets festlegen und hervorheben. Dadurch erhalten Sie sofortige Sichtbarkeit für Ausreißer und außergewöhnliche Datenpunkte.



Die bedingte Formatierung wird für jede Spalte in einer Tabelle separat festgelegt. Sie können beispielsweise einen Satz Schwellenwerte für eine Spalte Kapazität und einen weiteren Satz für eine Spalte Durchsatz auswählen.

Wenn Sie die Einheitenanzeige für eine Spalte ändern, bleibt die bedingte Formatierung erhalten und gibt die Änderung der Werte wieder. Die nachfolgenden Bilder zeigen die gleiche bedingte Formatierung, auch wenn die Anzeigeeinheit anders ist.



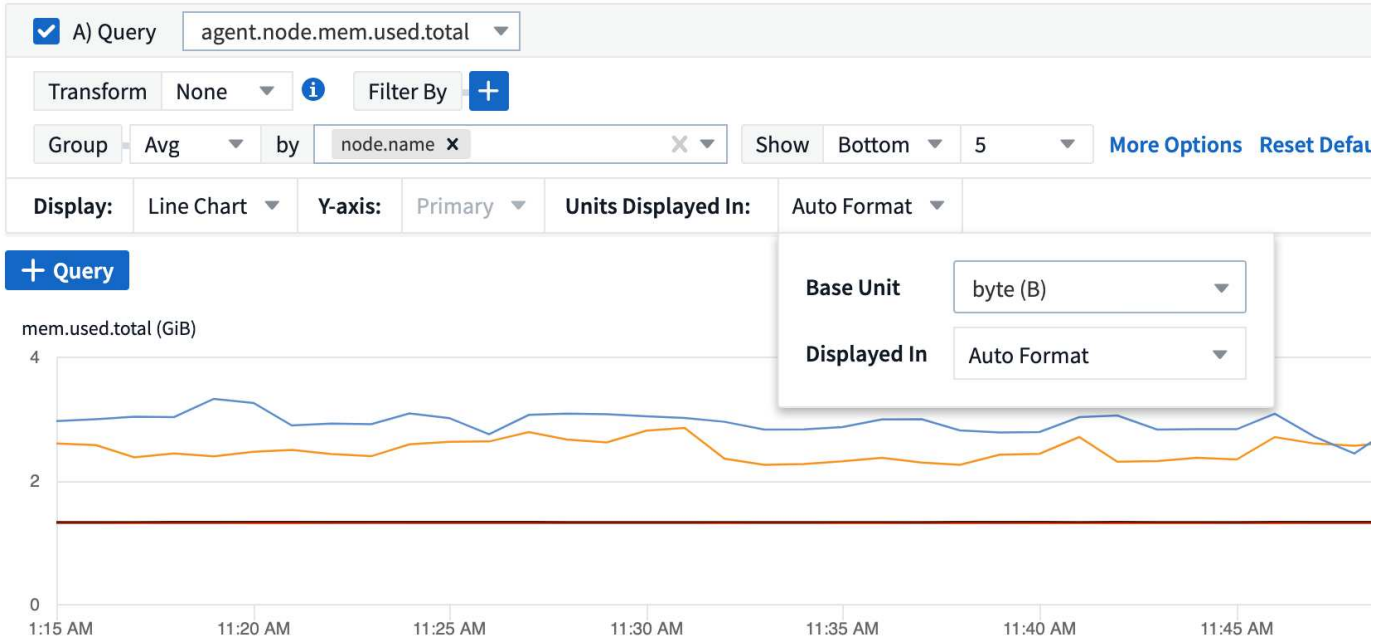


Sie können festlegen, ob die Zustandsformatierung als Farbe, Symbole oder beides angezeigt werden soll.

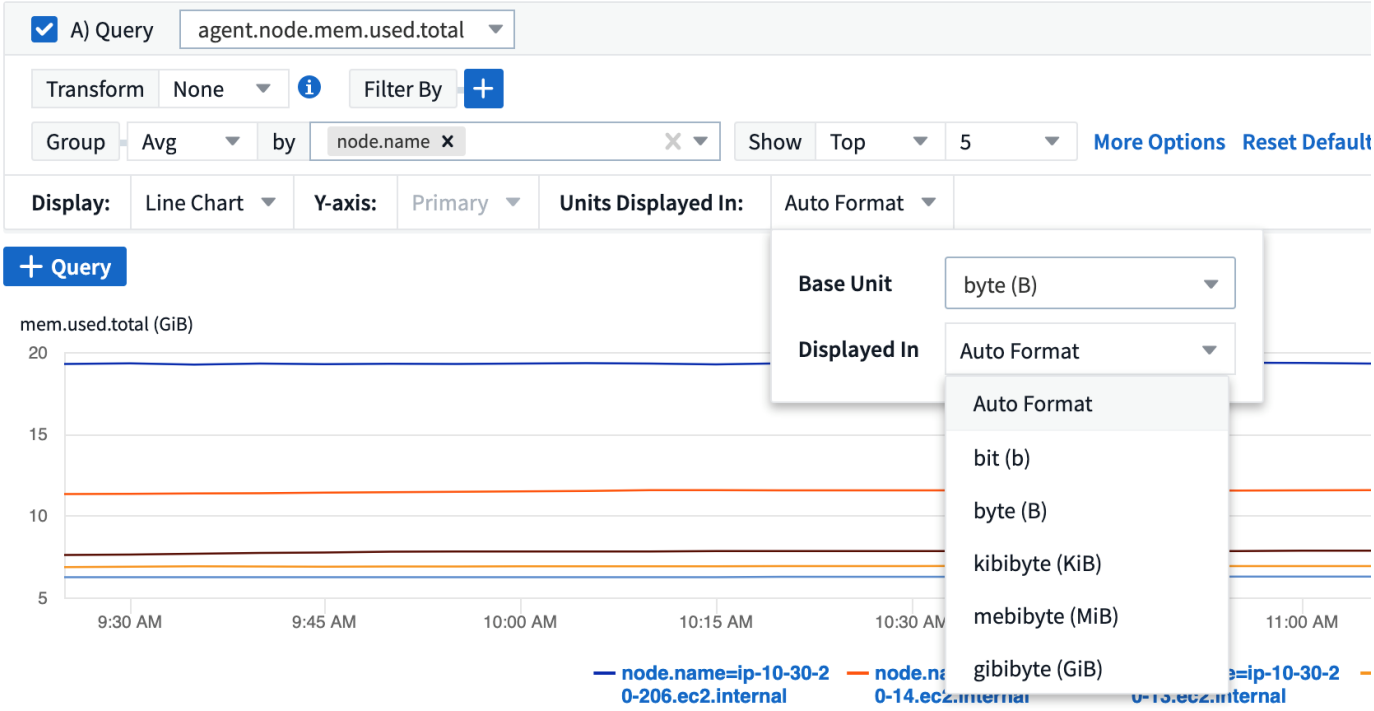
Auswählen des Geräts für die Datenanzeigen(Anzeige

Die meisten Widgets auf einem Dashboard ermöglichen die Angabe der Einheiten, in denen Werte angezeigt werden sollen, z. B. *Megabyte*, *Tausende*, *Prozentsatz*, *Millisekunden (ms)*, Etc. In vielen Fällen kennt Cloud Insights das beste Format für die zu erschaffenden Daten. Wenn das beste Format nicht bekannt ist, können Sie das gewünschte Format festlegen.

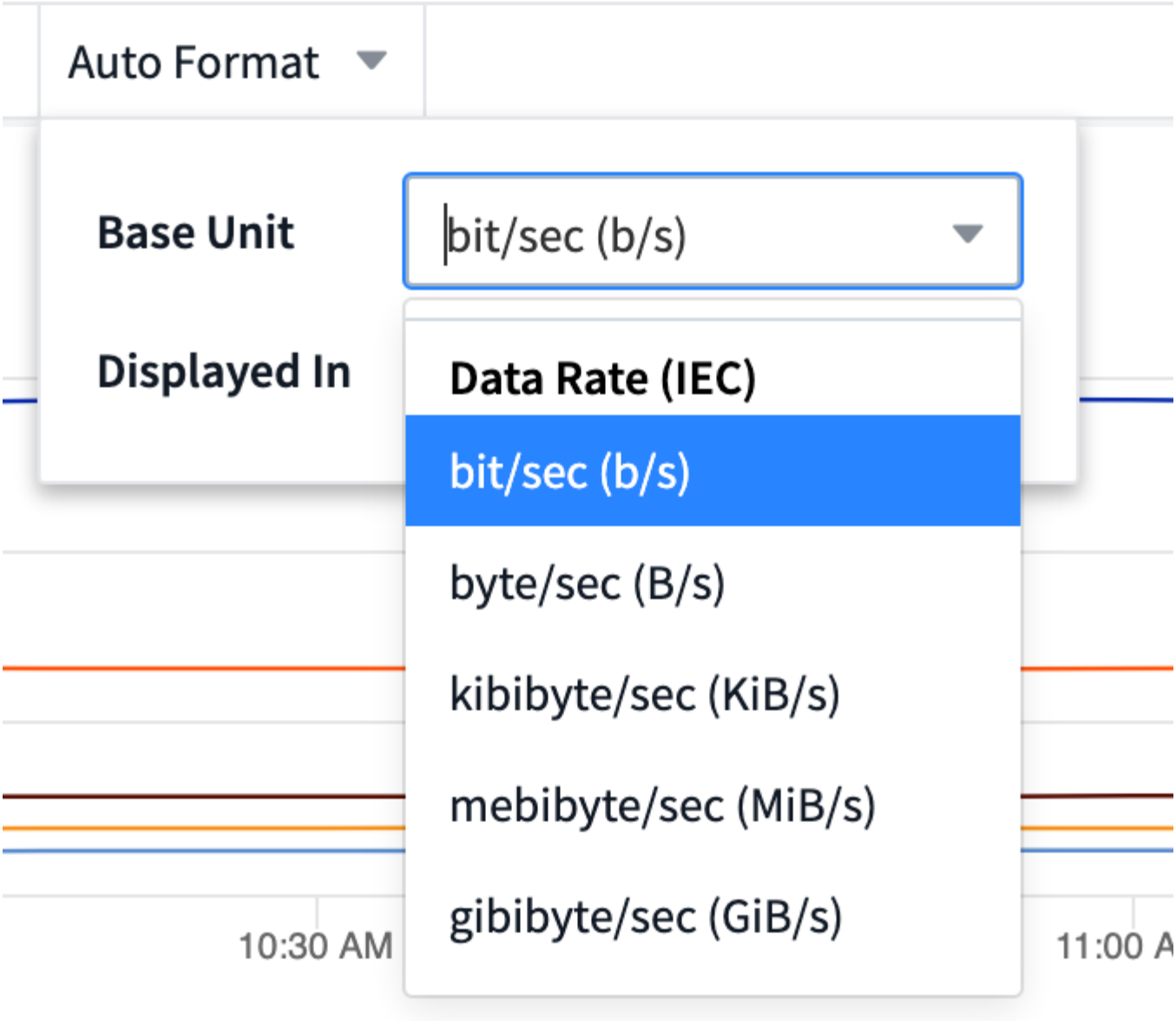
Im nachstehenden Liniendiagramm sind die für das Widget ausgewählten Daten in *Bytes* (die Basiseinheit IEC-Daten: Siehe Tabelle unten) angegeben, sodass die Basiseinheit automatisch als 'Byte (B)' ausgewählt wird. Die Datenwerte sind jedoch groß genug, um als Gibibyte (gib) präsentiert werden zu können, sodass Cloud Insights standardmäßig die Werte als gib automatisch formatiert. Auf der Y-Achse im Diagramm wird auf der Anzeigeeinheit „gib“ angezeigt, und alle Werte werden gemäß dieser Einheit angezeigt.



Wenn Sie das Diagramm in einer anderen Einheit anzeigen möchten, können Sie ein anderes Format auswählen, in dem die Werte angezeigt werden sollen. Da die Basiseinheit in diesem Beispiel *Byte* ist, können Sie zwischen den unterstützten „Byte-basierten“ Formaten wählen: Bit (b), Byte (B), Kibibyte (KiB), Mebibyte (MiB), Gibibyte (gib). Die Y-Achse und die Werte ändern sich je nach dem gewählten Format.



In Fällen, in denen die Basiseinheit nicht bekannt ist, können Sie eine Einheit aus dem zuweisen "Verfügbare Einheiten"Oder geben Sie Ihre eigene Eingabe ein. Sobald Sie eine Basiseinheit zugewiesen haben, können Sie auswählen, um die Daten in einem der entsprechenden unterstützten Formate anzuzeigen.



Um die Einstellungen zu löschen und wieder zu starten, klicken Sie auf **Standardeinstellungen zurücksetzen**.

Ein Wort zu Auto-Format

Die meisten Metriken werden von Datensammlern in der kleinsten Einheit berichtet, beispielsweise als ganze Zahl wie 1,234,567,890 Bytes. Standardmäßig formatiert Cloud Insights den Wert für die lesbare Anzeige automatisch. Beispielsweise würde ein Datenwert von 1,234,567,890 Byte automatisch auf 1.23 *Gibibyte* formatiert. Sie können wählen, ob Sie es in einem anderen Format anzeigen möchten, z. B. *Mebibyte*. Der Wert wird entsprechend angezeigt.

> Cloud Insights nutzt die Namensstandards für die Benennung amerikanischer Zahlen. Die amerikanische "Milliarde" entspricht "tausend Millionen".

Widgets mit mehreren Abfragen

Wenn Sie über ein Widget mit Zeitreihen verfügen (z. B. Linie, Spline, Bereich, gestapelter Bereich), das zwei Abfragen enthält, bei denen beide die primäre Y-Achse dargestellt werden, wird die Basiseinheit nicht oben auf

der Y-Achse angezeigt. Wenn Ihr Widget jedoch über eine Abfrage auf der primären Y-Achse und eine Abfrage auf der sekundären Y-Achse verfügt, werden die Basiseinheiten für jede einzelne Achse angezeigt.

Wenn Ihr Widget drei oder mehr Abfragen hat, werden Basiseinheiten auf der Y-Achse nicht angezeigt.

Verfügbare Einheiten

Die folgende Tabelle zeigt alle verfügbaren Einheiten nach Kategorie.

Kategorie	Einheiten
Währung	Cent-Dollar
Daten (IEC)	Bit-Byte-Kibibyte-Gibibyte-Tebibyte-Pebibyte-Exbibyte
Datenrate (IEC)	Bit/Sek.-Byte/Sek.-Kibibyte/Sek.-Mebibyte/Sek.-Gibibyte/Sek.-Tebibyte/Sek.-Pebibyte/Sek.
Daten (Metrisch)	kilobyte Megabyte Gigabyte Terabyte Petabyte Exabyte
Datenrate (metrisch)	kilobyte/s, Megabyte/s, Gigabyte/Sek. Terabyte/Sek., Exabyte/Sek.
IEC	kibi mebi gibi tebi pebi exbi
Dezimal	Ganze tausend Millionen Bilion Billionen
Prozentsatz	Prozentsatz
Zeit	Zweite Minute Stunde im Nanosekundenbereich im Mikrosekundenbereich
Temperatur	celsius fahrenheit
Frequenz	hertz Kilohertz Megahertz Gigahertz
CPU	Nanocores Mikrokerne Millicores Kerne kilocores megacores gigacores teracores petacores anspruchsvolle
Durchsatz	I/O OPs/s OPs/s gemäß s/s Lese-/Sek. Schreibzugriffe/s OPs/s OPs/Min. Lese-/Min. Schreib-/Min

TV-Modus und automatische Aktualisierung

Daten in Widgets auf Dashboards und Landing Pages von Assets werden automatisch aktualisiert, wenn ein Aktualisierungsintervall festgelegt wird, das vom ausgewählten Dashboard-Zeitbereich bestimmt wird. Das Aktualisierungsintervall hängt davon ab, ob es sich bei dem Widget um Zeitreihen (Linie, Spline, Bereich,

gestapelte Flächendiagramme) oder nicht-Zeitreihen (alle anderen Diagramme) handelt.

Dashboard-Zeitbereich	Zeit-Serie Aktualisierungsintervall	Nicht-Time-Series-Aktualisierungsintervall
Letzte 15 Minuten	10 Sekunden	1 Minute
Letzte 30 Minuten	15 Sekunden	1 Minute
Letzte 60 Minuten	15 Sekunden	1 Minute
Die Letzten 2 Stunden	30 Sekunden	5 Minuten
Letzte 3 Stunden	30 Sekunden	5 Minuten
Letzte 6 Stunden	1 Minute	5 Minuten
Letzte 12 Stunden	5 Minuten	10 Minuten
Letzte 24 Stunden	5 Minuten	10 Minuten
Letzte 2 Tage	10 Minuten	10 Minuten
Letzte 3 Tage	15 Minuten	15 Minuten
Letzte 7 Tage	1 Stunde	1 Stunde
Letzte 30 Tage	2 Stunden	2 Stunden

Jedes Widget zeigt sein Intervall für die automatische Aktualisierung in der oberen rechten Ecke des Widgets an.

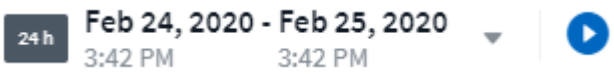
Die automatische Aktualisierung ist für den benutzerdefinierten Zeitbereich des Dashboards nicht verfügbar.

In Kombination mit **TV-Modus** ermöglicht die automatische Aktualisierung die Anzeige von Daten auf einem Dashboard oder einer Asset-Seite nahezu in Echtzeit. Der TV-Modus bietet ein übersichtliches Display. Das Navigationsmenü ist ausgeblendet und bietet so mehr Platz für Ihre Datenanzeige, wie die Schaltfläche Bearbeiten. Der TV-Modus ignoriert typische Cloud Insights-Timeouts und lässt das Display so lange in Betrieb, bis es manuell oder automatisch durch Autorisierungsprotokolle abgemeldet wird.

> Da NetApp BlueXP über eine eigene Zeitüberschreitung für die Benutzeranmeldung von 7 Tagen verfügt, muss sich Cloud Insights auch bei diesem Ereignis abmelden. Sie können sich einfach erneut anmelden und Ihr Dashboard wird weiterhin angezeigt.

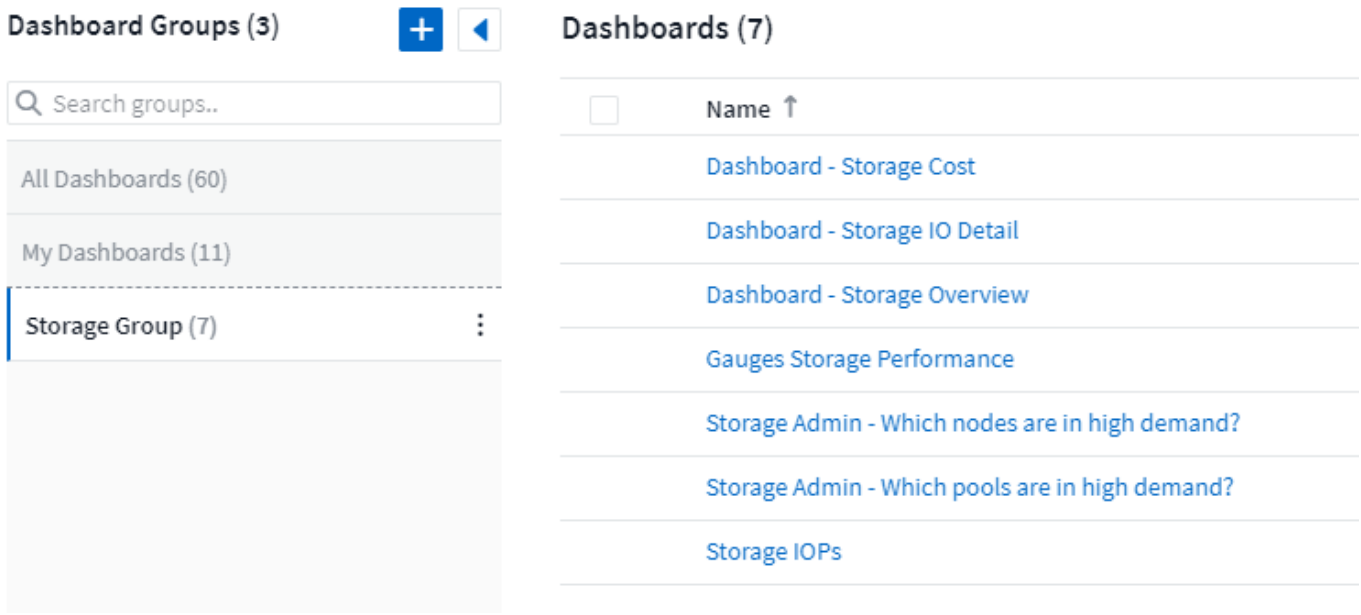
- Um den TV-Modus zu aktivieren, klicken Sie auf TV Mode Schaltfläche.
- Um den TV-Modus zu deaktivieren, klicken Sie oben links auf dem Bildschirm auf die Schaltfläche **Beenden**. Exit

Sie können die automatische Aktualisierung vorübergehend unterbrechen, indem Sie oben rechts auf die Schaltfläche „Pause“ klicken. Während der Pause wird im Feld Zeitbereich des Dashboards der aktive Zeitraum der angehaltenen Daten angezeigt. Ihre Daten werden weiterhin erfasst und aktualisiert, während die automatische Aktualisierung angehalten wird. Klicken Sie auf die Schaltfläche Fortsetzen, um mit der automatischen Aktualisierung von Daten fortzufahren.



Dashboard-Gruppen

Durch Gruppierung können Sie zugehörige Dashboards anzeigen und verwalten. Sie können beispielsweise eine Dashboard-Gruppe einrichten, die dem Storage in Ihrer Umgebung zugewiesen ist. Dashboard-Gruppen werden auf der Seite **Dashboards > Alle Dashboards anzeigen** verwaltet.



Standardmäßig werden zwei Gruppen angezeigt:

- **Alle Dashboards** listet alle Dashboards auf, die erstellt wurden, unabhängig vom Eigentümer.
- **Meine Dashboards** listet nur die Dashboards auf, die vom aktuellen Benutzer erstellt wurden.

Die Anzahl der Dashboards in jeder Gruppe wird neben dem Gruppennamen angezeigt.

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

Um Dashboards zur Gruppe hinzuzufügen, klicken Sie auf die Gruppe *Alle Dashboards*, um alle Dashboards in Ihrer Umgebung anzuzeigen, klicken Sie auf *eigene Dashboards*, wenn Sie nur die Dashboards sehen möchten, die Sie besitzen, und führen Sie eine der folgenden Aktionen durch:

- Um ein einzelnes Dashboard hinzuzufügen, klicken Sie auf das Menü rechts neben dem Dashboard und wählen Sie *zu Gruppe hinzufügen*.
- Um einer Gruppe mehrere Dashboards hinzuzufügen, wählen Sie diese aus, indem Sie auf das Kontrollkästchen neben jedem Dashboard klicken. Klicken Sie dann auf die Schaltfläche **Massenaktionen** und wählen Sie *zu Gruppe hinzufügen*.

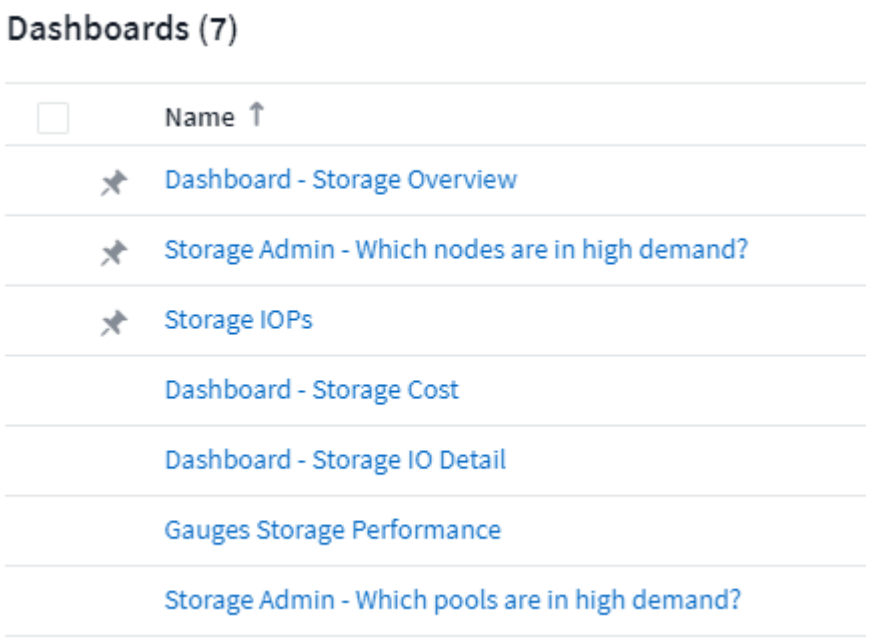
Entfernen Sie Dashboards auf dieselbe Weise aus der aktuellen Gruppe, indem Sie *aus Gruppe* entfernen auswählen. Sie können Dashboards nicht aus der Gruppe *Alle Dashboards* oder *Meine Dashboards* entfernen.

> Durch Entfernen eines Dashboards aus einer Gruppe wird das Dashboard nicht aus Cloud Insights gelöscht. Um ein Dashboard vollständig zu entfernen, wählen Sie das Dashboard aus, und klicken Sie auf *Löschen*. Dadurch wird er von allen Gruppen entfernt, zu denen er gehört hat und für keinen Benutzer mehr verfügbar ist.

PIN für Ihre Lieblings-Dashboards

Sie können Ihre Dashboards weiter verwalten, indem Sie Ihre Favoriten an der Spitze Ihrer Dashboard-Liste anheften. Um ein Dashboard anzuheften, klicken Sie einfach auf die Schaltfläche mit dem Daumenpack, die angezeigt wird, wenn Sie den Mauszeiger über ein Dashboard in einer beliebigen Liste bewegen.

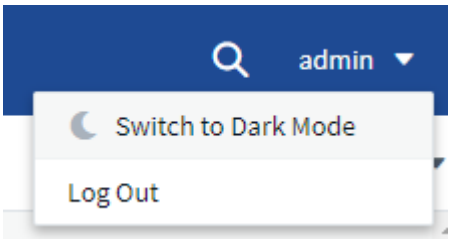
Dashboard PIN/Unpin ist eine individuelle Benutzerpräferenz und unabhängig von der Gruppe (oder Gruppen), zu der das Dashboard gehört.



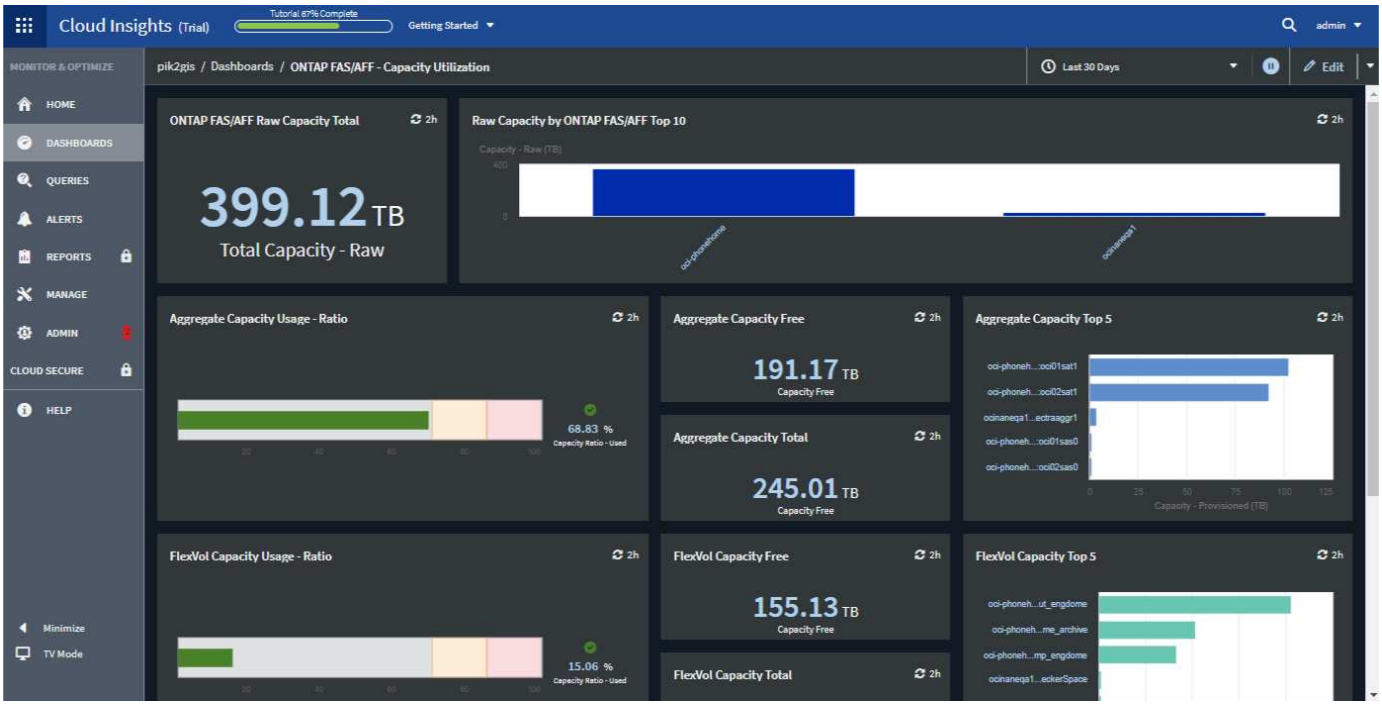
Dunkles Thema

Sie können wählen, Cloud Insights entweder mit einem hellen Thema (die Standardeinstellung), die die meisten Bildschirme mit einem hellen Hintergrund mit dunklem Text, oder ein dunkles Thema, das die meisten Bildschirme mit einem dunklen Hintergrund mit leichtem Text angezeigt.

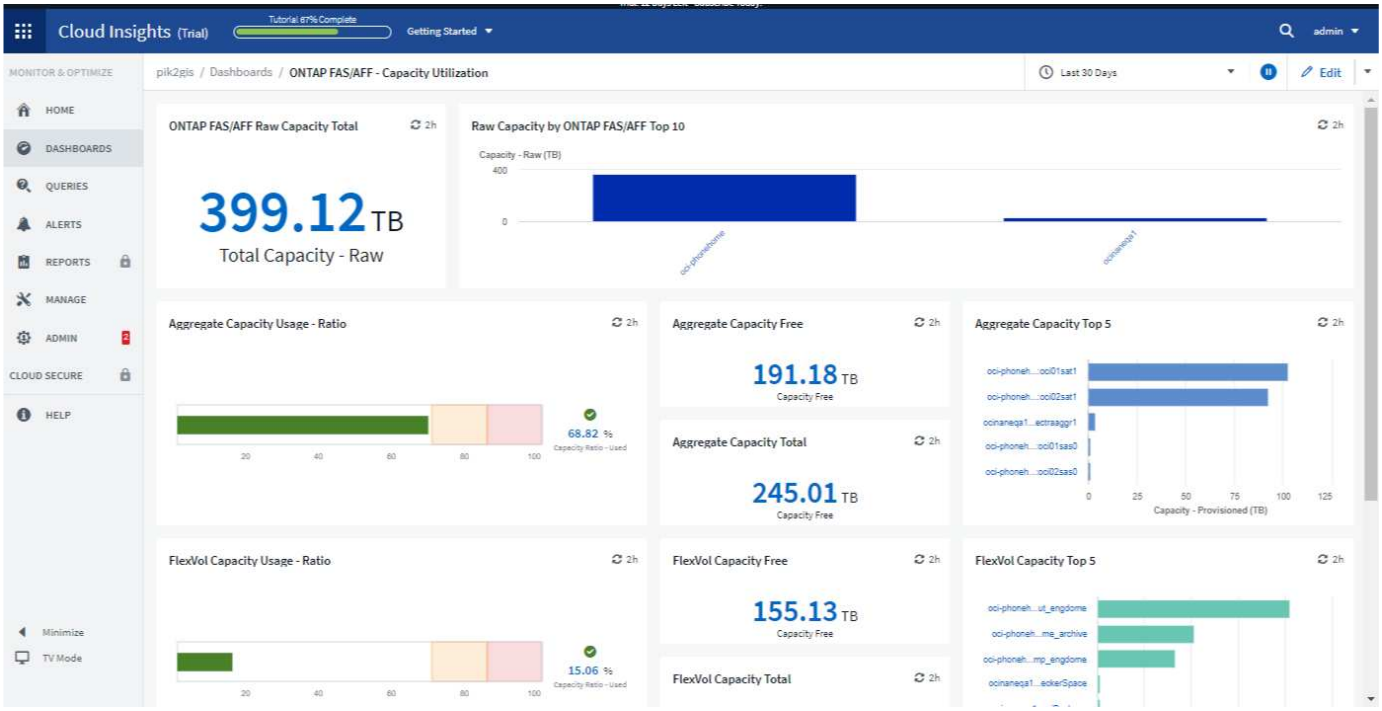
Um zwischen hellen und dunklen Themen zu wechseln, klicken Sie auf die Schaltfläche Benutzername in der oberen rechten Ecke des Bildschirms und wählen Sie das gewünschte Thema.



Dashboard-Ansicht „Dark Theme“:



Dashboard-Ansicht „Light Theme“:



Einige Bildschirmbereiche, wie bestimmte Widget-Diagramme, zeigen immer noch helle Hintergründe, auch wenn sie in dunklem Thema betrachtet.

Zeilendiagramm-Interpolation

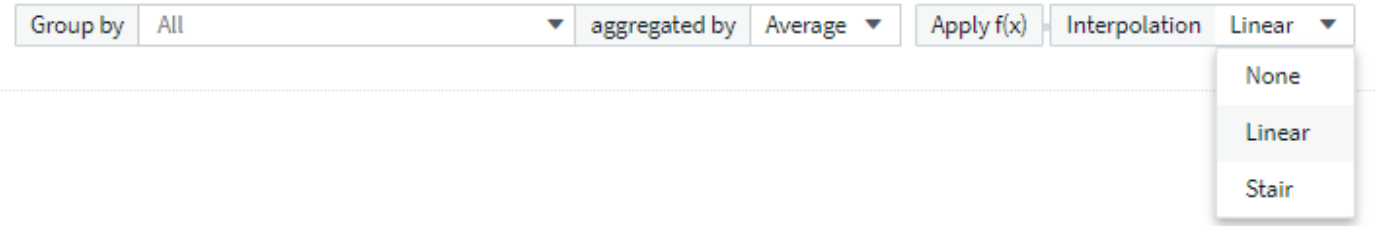
Unterschiedliche Datensammler stellen ihre Daten häufig in unterschiedlichen Intervallen in Frage. Zum Beispiel kann Datensammler A alle 15 Minuten abfragen, während Datensammler B alle fünf Minuten abfragt. Wenn ein Liniendiagramm-Widget (auch Spline-, Bereich- und gestapelte Flächendiagramme) diese Daten von mehreren Datensammlern in einer einzelnen Zeile zusammenfasst (z. B. wenn das Widget nach „all“ gruppiert

wird), Und die Aktualisierung der Linie alle fünf Minuten, können die Daten von Collector B korrekt angezeigt werden, während die Daten von Collector A Lücken haben können, so dass das Aggregat bis zum Sammler Eine erneute Abstimmungen.

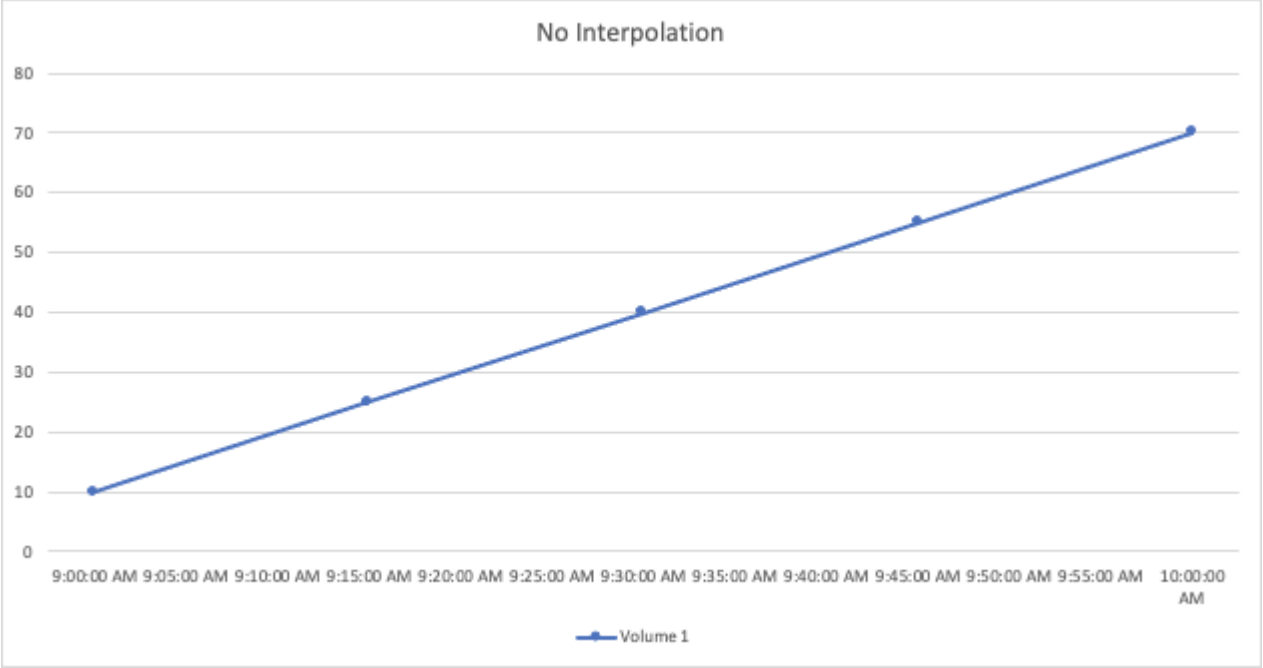
Um dies zu lindern, interpoliert Cloud Insights Daten bei der Aggregation, unter Verwendung der umgebenden Datenpunkte zu einem "besten Raten" an Daten bis Datensammler wieder abfragen. Sie können die Objektdaten jedes Datensammlers immer einzeln anzeigen, indem Sie die Gruppierung des Widgets anpassen.

Interpolationsmethoden

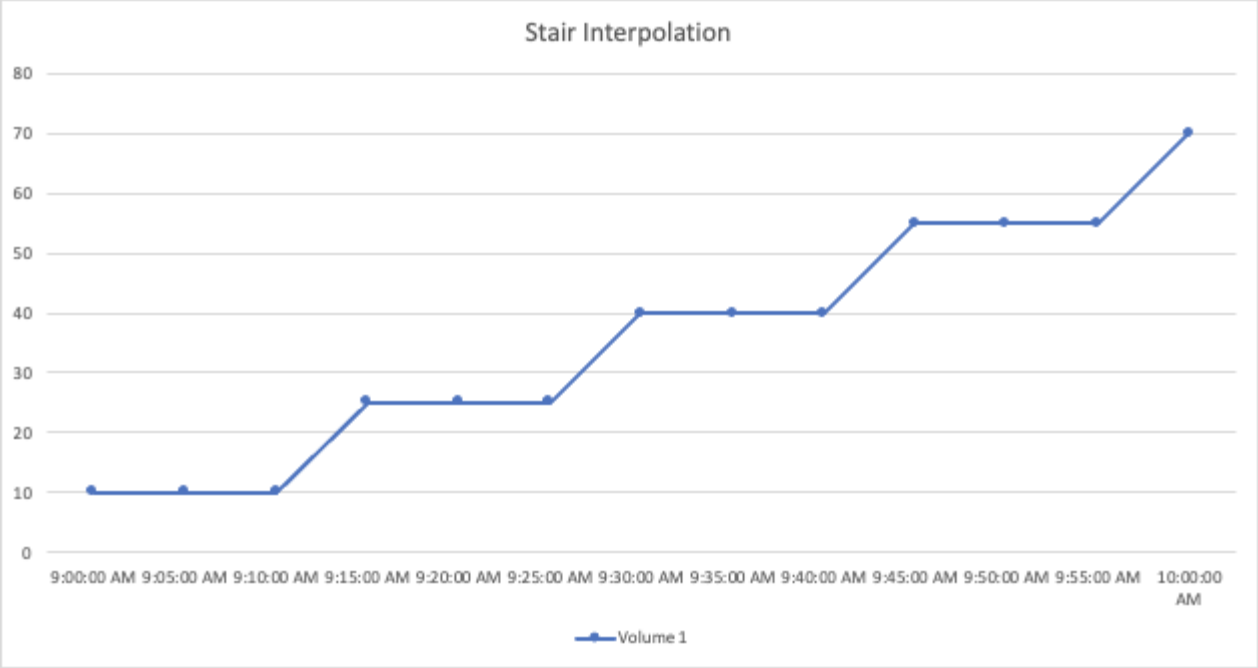
Wenn Sie ein Liniendiagramm (oder ein Spline-, Bereich- oder Stapeldiagramm) erstellen oder ändern, können Sie die Interpolationsmethode auf einen von drei Typen festlegen. Wählen Sie im Abschnitt „Gruppieren nach“ die gewünschte Interpolation aus.



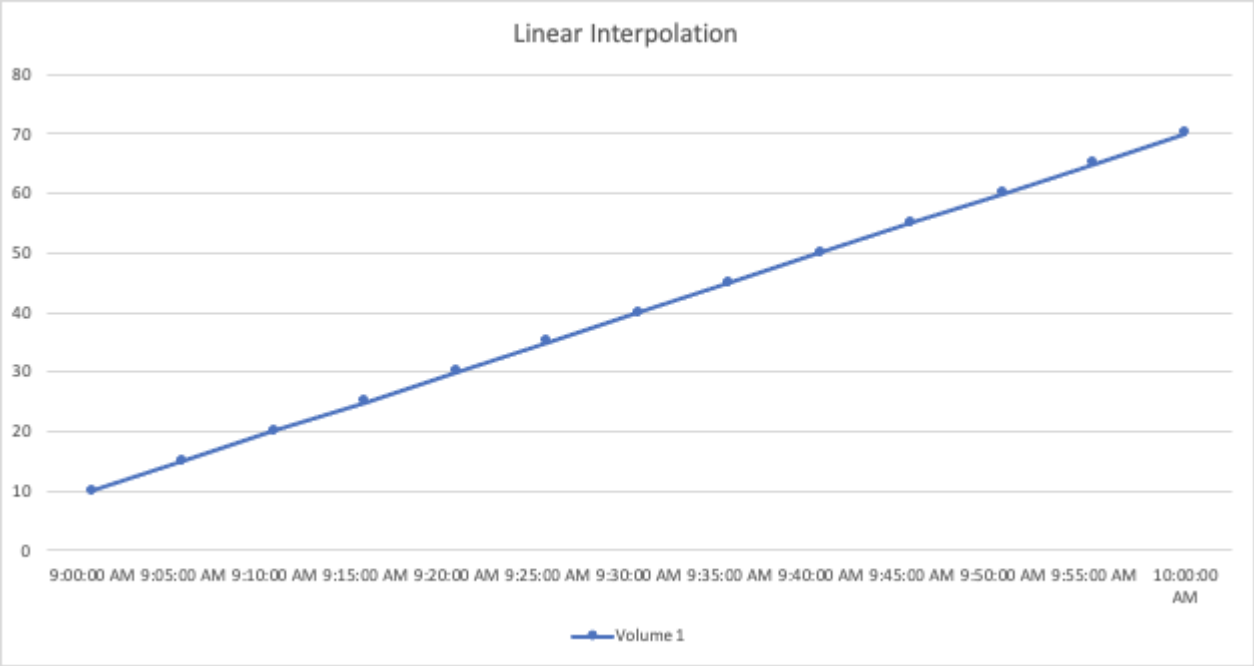
- **Keine**: Nichts tun, d.h. keine Punkte dazwischen erzeugen.



- **Stair**: Ein Punkt wird aus dem Wert des vorherigen Punktes generiert. In einer geraden Linie würde dies als typisches "Treppenhaus"-Layout angezeigt.



- **Linear**: Ein Punkt wird als Wert zwischen der Verbindung der beiden Punkte erzeugt. Erzeugt eine Linie, die wie die Linie aussieht, die die beiden Punkte verbindet, aber mit zusätzlichen (interpolierten) Datenpunkten.



Beispiele Für Dashboards

Dashboard-Beispiel: Virtual Machine Performance

IT-Abteilungen stehen heute vor zahlreichen Herausforderungen. Von Administratoren muss mit weniger Aufwand mehr erreicht werden, und eine vollständige Übersicht über dynamische Datacenter ist daher ein muss. In diesem Beispiel zeigen wir Ihnen, wie Sie ein Dashboard mit Widgets erstellen, die Ihnen betriebliche Einblicke in die Performance

der Virtual Machine (VM) in Ihrer Umgebung geben. Wenn Sie diesem Beispiel folgen und Widgets erstellen, um Ihre spezifischen Anforderungen zu erfüllen, können Sie beispielsweise die Performance von Back-End-Storage im Vergleich zur Frontend-Performance der Virtual Machines oder die Anzeige von VM-Latenz gegenüber I/O-Anforderungen visualisieren.

Über diese Aufgabe

Hier werden wir ein Dashboard für die Performance von virtuellen Maschinen erstellen, das Folgendes enthält:

- Eine Tabelle mit VM-Namen und Performance-Daten
- Ein Diagramm, das VM-Latenz mit Storage-Latenz vergleicht
- Ein Diagramm mit den Angaben zu Lese-, Schreib- und IOPS insgesamt für VMs
- Ein Diagramm zeigt den maximalen Durchsatz für Ihre VMs

Dies ist nur ein einfaches Beispiel. Sie können Ihr Dashboard so anpassen, dass Sie Ihre ausgewählten Performance-Daten hervorheben und vergleichen, um Ihre eigenen Best Practices im Betrieb zu berücksichtigen.

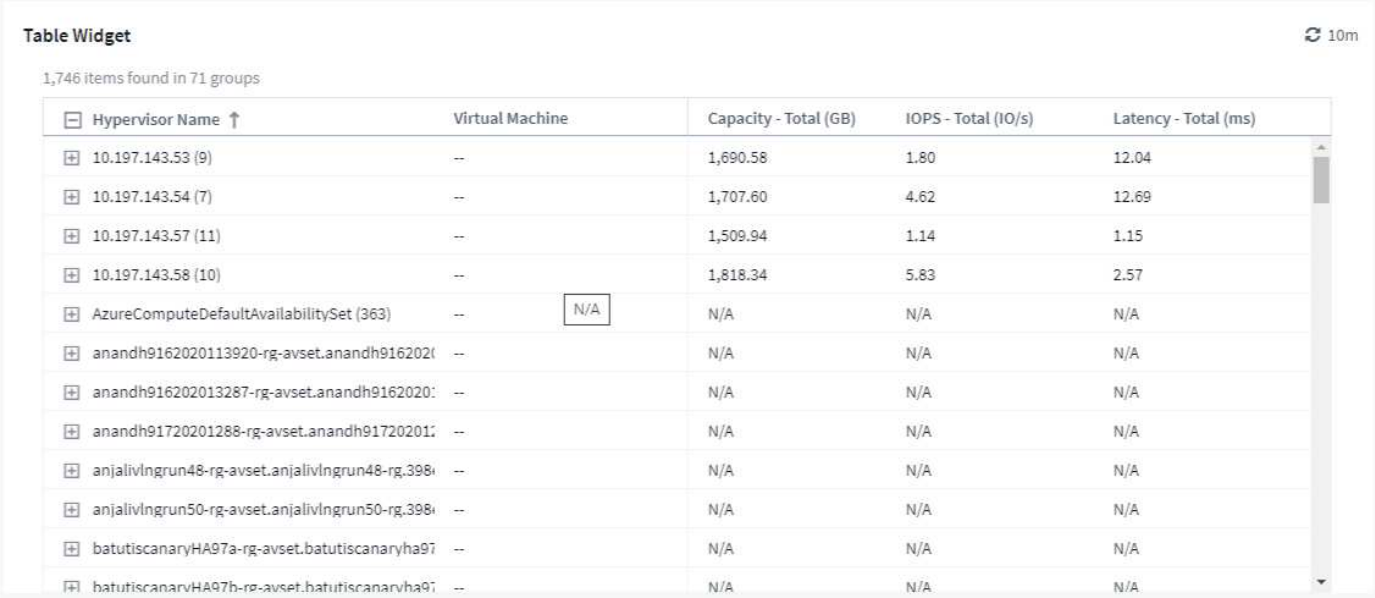
Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
2. Wählen Sie im Menü **Dashboards** * **[+Neues Dashboard]** aus.

   Die Seite **Neues Dashboard** wird geöffnet.

3. Geben Sie oben auf der Seite einen eindeutigen Namen für das Dashboard ein, zum Beispiel „VM Performance by Application“.
4. Klicken Sie auf **Speichern**, um das Dashboard mit dem neuen Namen zu speichern.
5. Beginnen wir mit dem Hinzufügen unserer Widgets. Klicken Sie bei Bedarf auf das Symbol **Bearbeiten**, um den Bearbeitungsmodus zu aktivieren.
6. Klicken Sie auf das Symbol * Widget hinzufügen* und wählen Sie **Tabelle**, um dem Dashboard ein neues TabellenWidget hinzuzufügen.

   Das Dialogfeld Widget bearbeiten wird geöffnet. Die angezeigten Standarddaten sind für alle Speicher in Ihrer Umgebung.



1. Wir können dieses Widget anpassen. Löschen Sie im Feld Name oben „Widget 1“ und geben Sie „Virtual Machine Performance table“ ein.
2. Klicken Sie auf das Dropdown-Menü Asset type und ändern Sie *Storage* zu *Virtual Machine*.

   Die Änderungen an den Tabellendaten werden angezeigt, wenn alle Virtual Machines in Ihrer Umgebung angezeigt werden.

3. Fügen wir der Tabelle einige Spalten hinzu. Klicken Sie rechts auf das Symbol „Gear“, und wählen Sie „*Hypervisor Name*, *IOPS - Total*, and *Latenz - Total*“ aus. Sie können auch versuchen, den Namen in die Suche einzugeben, um das gewünschte Feld schnell anzuzeigen.

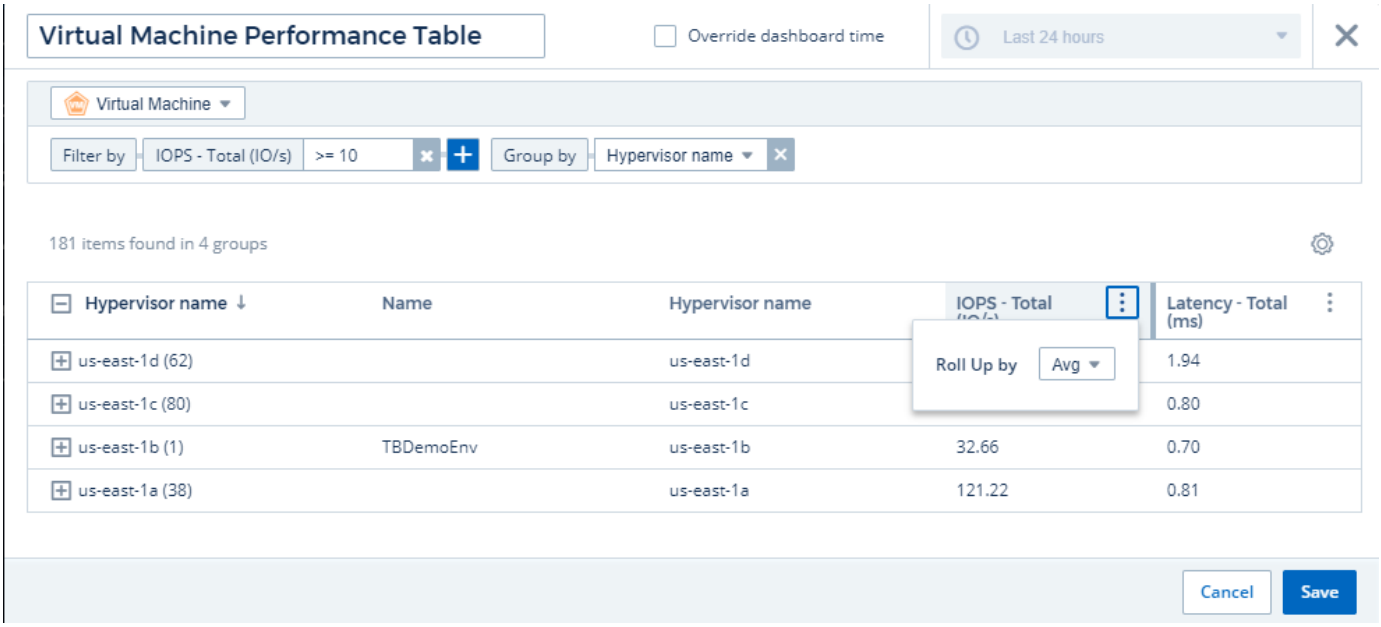
   Diese Spalten werden nun in der Tabelle angezeigt. Sie können die Tabelle nach einer dieser Spalten sortieren. Beachten Sie, dass die Spalten in der Reihenfolge angezeigt werden, in der sie dem Widget hinzugefügt wurden.

4. Bei dieser Übung werden wir VMs ausschließen, die nicht aktiv genutzt werden. Wir sollten also etwas mit weniger als 10 IOPS insgesamt herausfiltern. Klicken Sie auf die Schaltfläche **[+]** neben **Filtern nach** und wählen Sie *IOPS - Total*. Klicken Sie auf **Any** und geben Sie "10" in das Feld **von** ein. Lassen Sie das Feld * to* leer. Klicken Sie auf das Filterfeld auslassen, oder drücken Sie die Eingabetaste, um den Filter festzulegen.

   Die Tabelle zeigt jetzt nur VMs mit insgesamt 10 IOPS oder mehr.

5. Wir können die Tabelle weiter reduzieren, indem wir Ergebnisse gruppieren. Klicken Sie auf die Schaltfläche **[+]** neben **Group by** und wählen Sie ein Feld aus, nach dem Sie gruppieren möchten, z. B. *Application* oder *Hypervisor Name*. Gruppierung wird automatisch angewendet.

   Die Tabellenzeilen werden nun entsprechend Ihrer Einstellung gruppiert. Sie können die Gruppen nach Bedarf erweitern und reduzieren. Gruppierte Zeilen zeigen gerollte Daten für jede der Spalten an. In einigen Spalten können Sie die Aufrollmethode für diese Spalte auswählen.



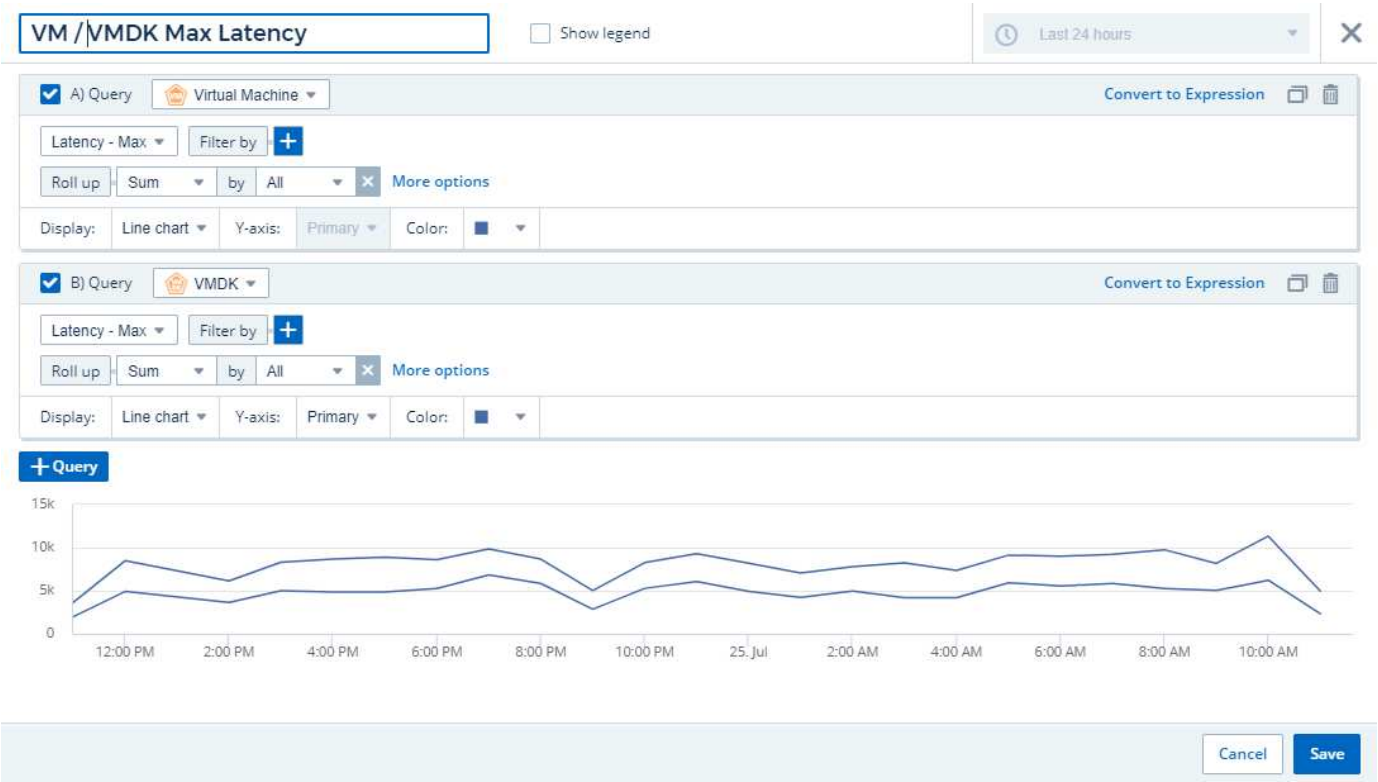
1. Wenn Sie das TabellenWidget auf Ihre Zufriedenheit angepasst haben, klicken Sie auf die Schaltfläche **[Save]**.

   Das TabellenWidget wird im Dashboard gespeichert.

Sie können die Größe des Widgets auf dem Dashboard ändern, indem Sie die untere rechte Ecke ziehen. Machen Sie das Widget breiter, um alle Spalten deutlich anzuzeigen. Klicken Sie auf **Speichern**, um das aktuelle Dashboard zu speichern.

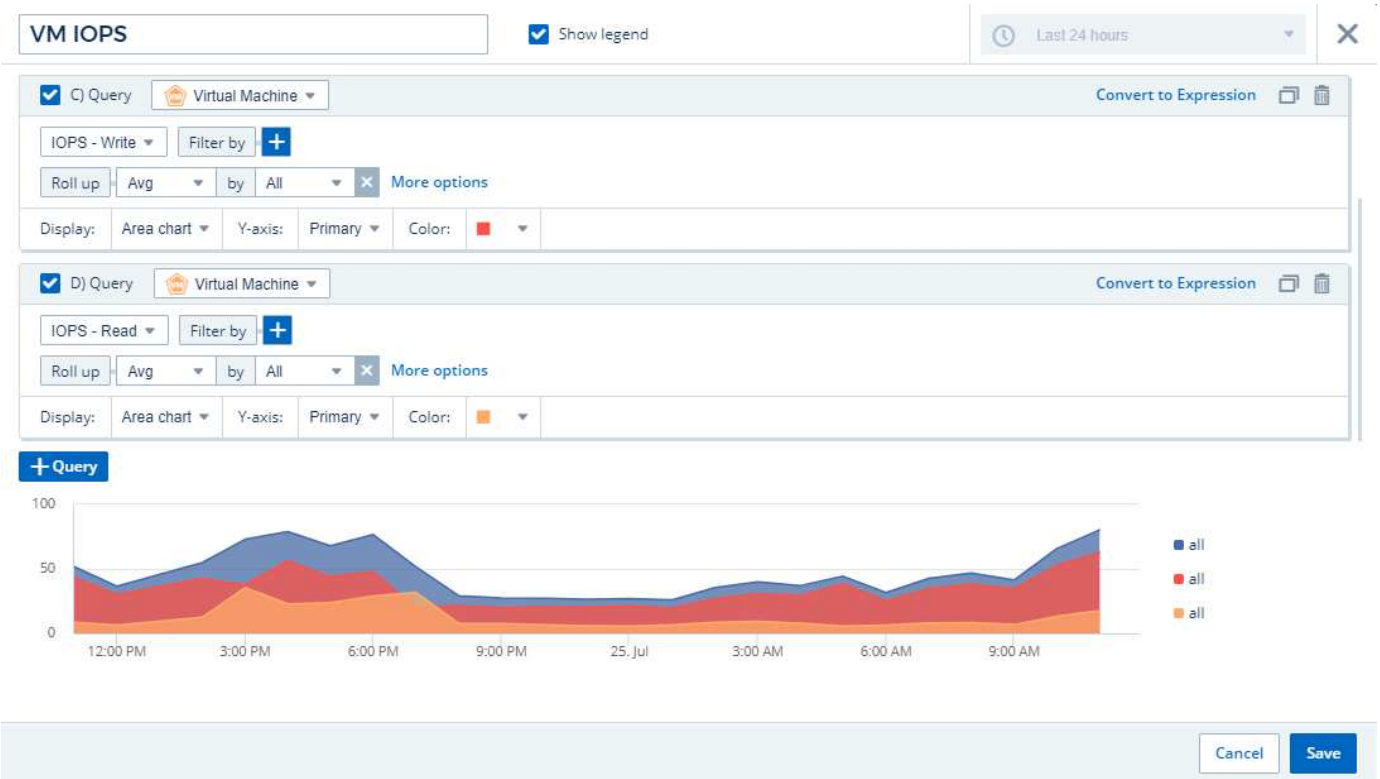
Als nächstes fügen wir einige Diagramme hinzu, um unsere VM-Performance anzuzeigen. Erstellen wir ein Liniendiagramm, in dem die VM-Latenz mit VMDK-Latenz verglichen wird.

1. Klicken Sie bei Bedarf auf das Symbol **Bearbeiten** auf dem Dashboard, um den Bearbeitungsmodus zu aktivieren.
2. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm*, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
3. Das Dialogfeld **Widget bearbeiten** wird geöffnet. Benennen Sie dieses Widget „VM/VMDK max Latency“ (max.
4. Wählen Sie **Virtual Machine** und wählen Sie *Latenz - Max*. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Für **Roll Up** wählen Sie *sum* by *All*. Diese Daten als *Liniendiagramm* anzeigen und *Y-Achse* als *Primär* verlassen.
5. Klicken Sie auf die Schaltfläche **[+Query]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie in dieser Zeile *VMDK* und *Latenz - Max* aus. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Für **Roll Up** wählen Sie *sum* by *All*. Diese Daten als *Liniendiagramm* anzeigen und *Y-Achse* als *Primär* verlassen.
6. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.



Als nächstes fügen wir ein Diagramm mit den IOPS „Lesen“, „Schreiben“ und „Gesamt“ in einem einzelnen Diagramm ein.

1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Flächendiagramm*, um dem Dashboard ein neues Widget mit einem Flächendiagramm hinzuzufügen.
2. Das Dialogfeld Widget bearbeiten wird geöffnet. Benennen Sie dieses Widget „VM IOPS“ (VM-IOPS).
3. Wählen Sie **Virtual Machine** und dann „*IOPS - Total*“. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Für **Roll Up** wählen Sie *sum* by *All*. Diese Daten als *Flächendiagramm* anzeigen und *Y-Achse* als *Primär* verlassen.
4. Klicken Sie auf die Schaltfläche **[+Query]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und dann *IOPS - Read*.
5. Klicken Sie auf die Schaltfläche **[+Query]**, um eine dritte Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** aus und wählen Sie *IOPS - Write*.
6. Klicken Sie auf **Legende anzeigen**, um eine Legende für dieses Widget auf dem Dashboard anzuzeigen.



1. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.

Danach fügen wir ein Diagramm hinzu, das den VM-Durchsatz für jede mit der VM verbundene Applikation anzeigt. Dafür nutzen wir die Roll-Up-Funktion.

1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm*, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
2. Das Dialogfeld Widget bearbeiten wird geöffnet. Benennen Sie dieses Widget „VM-Durchsatz nach Applikation“ (nach Applikation).
3. Wählen Sie Virtual Machine aus, und wählen Sie „Durchsatz – Gesamt“. Stellen Sie alle gewünschten Filter ein, oder lassen Sie den Filter leer. Wählen Sie bei Roll Up „Max“ und wählen Sie „Anwendung“ oder „Name“ aus. Zeigt die 10 besten Anwendungen an. Diese Daten als Liniendiagramm anzeigen und die Y-Achse als Primär belassen.
4. Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.

Sie können Widgets auf dem Dashboard verschieben, indem Sie die Maustaste an einer beliebigen Stelle im Widget gedrückt halten und an eine neue Position ziehen.

Sie können die Größe von Widgets ändern, indem Sie die untere rechte Ecke ziehen.

Achten Sie darauf, **[Speichern]** das Dashboard zu verwenden, nachdem Sie Ihre Änderungen vorgenommen haben.

Ihr letztes VM Performance Dashboard sieht so aus:

Best Practices für Dashboards und Widgets

Tipps und Tricks, damit Sie die leistungsstarken Funktionen von Dashboards und Widgets optimal nutzen können.

Suchen der richtigen Metrik

Cloud Insights erfasst Zähler und Kennzahlen unter Verwendung von Namen, die sich manchmal von der Datenerfassung zu Datensammler unterscheiden.

Bei der Suche nach der richtigen Metrik oder dem Zähler für Ihr Dashboard-Widget sollten Sie bedenken, dass die Metrik, die Sie benötigen, unter einem anderen Namen als der Metrik stehen kann, an die Sie denken. Während die Dropdown-Listen in Cloud Insights in der Regel alphabetisch sind, wird manchmal ein Begriff nicht in der Liste angezeigt, in der er Ihrer Meinung nach sein sollte. Beispielsweise werden Begriffe wie „Rohkapazität“ und „genutzte Kapazität“ in den meisten Listen nicht zusammen angezeigt.

Best Practice: Verwenden Sie die Suchfunktion in Feldern wie Filtern nach oder Orten wie der Spaltenauswahl, um das zu finden, was Sie suchen. Beispielsweise zeigt die Suche nach „Cap“ alle Metriken mit „Capacity“ in ihren Namen an, unabhängig davon, wo sie in der Liste auftreten. Sie können dann ganz einfach die gewünschten Metriken aus dieser kürzeren Liste auswählen.

Hier sind ein paar alternative Formulierungen, die Sie bei der Suche nach Metriken versuchen können:

Wann Sie suchen möchten:	Versuchen Sie auch die Suche nach:
CPU	Prozessor
Kapazität	Genutzte Kapazität Rohkapazität bereitgestellte Kapazität Storage Pools Kapazität <anderer Asset-Typ> geschriebene Kapazität
Festplattengeschwindigkeit	Niedrigste Festplattengeschwindigkeit, die am wenigsten geeignete Festplattenart ausführt
Host	Hypervisor-Hosts

Hypervisor	Host ist Hypervisor
Mikrocode	Firmware
Name	Alias Hypervisor Name Storage Name <other Asset type> Name Simple Name Resource Name Fabric Alias
Lesen/Schreiben	Teilweise Lese-/Lese-Schreib-IOPS – Schreiblatenz – Lese-Cache-Auslastung – Lesen
Virtual Machine	Die VM ist virtuell

Dies ist keine umfassende Liste. Dies sind nur Beispiele für mögliche Suchbegriffe.

Ermitteln der richtigen Ressourcen

Die Ressourcen, auf die Sie in Widget-Filtern und -Suchen verweisen können, variieren von Asset-Typ zu Asset-Typ.

In Dashboards und Asset-Seiten bestimmt der Asset-Typ, um den Sie Ihr Widget erstellen, die anderen Asset-Typen-Zähler, für die Sie eine Spalte filtern oder hinzufügen können. Beachten Sie beim Erstellen Ihres Widgets Folgendes:

Dieser Asset-Typ / Zähler:	Kann unter diesen Assets gefiltert werden:
Virtual Machine	VMDK
Datenspeicher(e)	Internes Volume VMDK Virtual Machine Volume
Hypervisor	Virtual Machine ist Hypervisor-Host
Host(s)	Host Virtual Machine Des Internen Volume Cluster
Fabric	Port

Dies ist keine umfassende Liste.

Best Practice: Wenn Sie nach einem bestimmten Asset-Typ filtern, der nicht in der Liste angezeigt wird, versuchen Sie, Ihre Anfrage um einen alternativen Asset-Typ zu erstellen.

Scatter-Plot Beispiel: Ihre Achse kennen

Durch Ändern der Zählerreihenfolge in einem Widget mit Streudiagramm werden die Achsen geändert, auf denen die Daten angezeigt werden.

Über diese Aufgabe

Dieses Beispiel erstellt ein Scatter-Diagramm, mit dem Sie leistungsschwache VMs sehen können, die eine hohe Latenz im Vergleich zu niedrigen IOPS haben.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard im Bearbeitungsmodus und fügen Sie ein Widget **Streudiagramm** hinzu.
2. Wählen Sie einen Asset-Typ aus, z. B. *Virtual Machine*.
3. Wählen Sie den ersten Zähler aus, den Sie zeichnen möchten. Wählen Sie in diesem Beispiel „*Latenz - Total*“ aus.

Latenz - Total wird entlang der X-Achse des Diagramms kartiert.

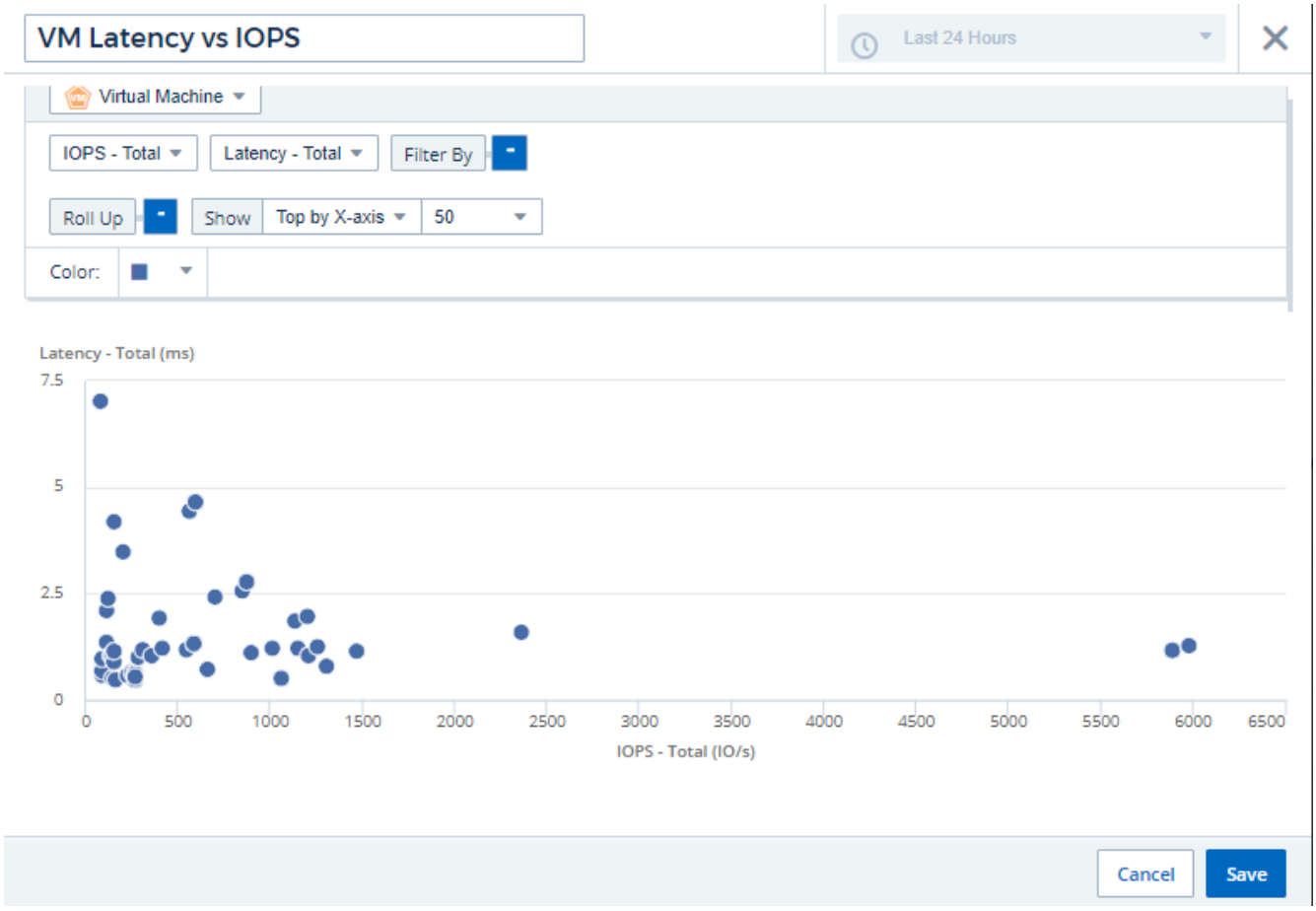
4. Wählen Sie den zweiten Zähler aus, den Sie zeichnen möchten. Wählen Sie in diesem Beispiel „*IOPS – Total*“ aus.

   IOPS - Total wird entlang der Y-Achse im Diagramm dargestellt. VMs mit höherer Latenz werden rechts im Diagramm angezeigt. Es werden nur die 100 VMs mit der höchsten Latenz angezeigt, da die Einstellung **Top by X-Axis** aktuell ist.

5. Nun die Reihenfolge der Zähler umkehren, indem der erste Zähler auf *IOPS - Total* und der zweite auf *Latenz - Total* eingestellt wird.

   Latenz- Total wird jetzt entlang der Y-Achse im Diagramm und *IOPS - Total* entlang der X-Achse kartiert. VMs mit höheren IOPS werden jetzt rechts im Diagramm angezeigt.

   Da wir die **Top by X-Axis**-Einstellung nicht geändert haben, zeigt das Widget jetzt die Top 100 VMs mit den höchsten IOPS an, da dies das ist, was derzeit entlang der X-Achse dargestellt wird.



Sie können wählen, dass das Diagramm die obere N nach X-Achse, die obere N nach Y-Achse, die untere N nach X-Achse oder die untere N nach Y-Achse anzeigt. In unserem letzten Beispiel werden die 100 wichtigsten VMs mit den höchsten IOPS insgesamt angezeigt. Wenn wir es in **Top by Y-Achse** ändern, zeigt das Diagramm wieder die Top 100 VMs mit der höchsten Gesamt-Latenz an.

Beachten Sie, dass Sie in einem Scatter-Diagramm auf einen Punkt klicken können, um die Asset-Seite für diese Ressource aufzurufen.

Arbeiten mit Abfragen

In Abfragen verwendete Ressourcen

Mit Abfragen können Sie Ihr Netzwerk überwachen und Fehler beheben, indem Sie die Assets und Metriken in Ihrer Umgebung auf granularer Ebene auf der Grundlage von vom Benutzer ausgewählten Kriterien (z. B. Anmerkungen) durchsuchen.

Beachten Sie, dass Anmerkungsregeln, die Assets automatisch Anmerkungen zuweisen, *eine Abfrage erfordern*.

Sie können die physischen oder virtuellen Inventarressourcen (und die zugehörigen Metriken) in Ihrer Umgebung abfragen oder die Metriken, die bei der Integration wie Kubernetes oder ONTAP Advanced Data bereitgestellt werden.

Lagerbestände

Die folgenden Asset-Typen können für Abfragen, Dashboard-Widgets und benutzerdefinierte Asset-Landing-Pages verwendet werden. Die für Filter, Ausdrücke und Anzeigen verfügbaren Felder und Zähler variieren je nach Asset-Typen. Nicht alle Assets können in allen Widgets verwendet werden.

- Applikation
- Datenspeicher
- Festplatte
- Fabric
- Generisches Gerät
- Host
- Internes Volumen
- ISCSI-Sitzung
- ISCSI-Netzwerkportal
- Pfad
- Port
- Qtree
- Kontingente
- Share
- Storage
- Storage-Node
- Storage-Pool
- Storage Virtual Machine (SVM)
- Switch
- Tape
- VMDK
- Virtual Machine
- Datenmenge
- Zone
- Zonenmitglied

Integrationsmetriken

Neben der Abfrage von Inventarressourcen und zugehörigen Performance-Metriken können Sie auch Metriken für **Integrationsdaten** abfragen, beispielsweise bei von Kubernetes oder Docker generierten oder mit ONTAP Advanced Metrics bereitgestellten Metriken.

Abfragen Werden Erstellt

Mit Abfragen können Sie die Assets in Ihrer Umgebung auf granularer Ebene durchsuchen und so nach den gewünschten Daten filtern und die Ergebnisse nach Ihren Wünschen sortieren.

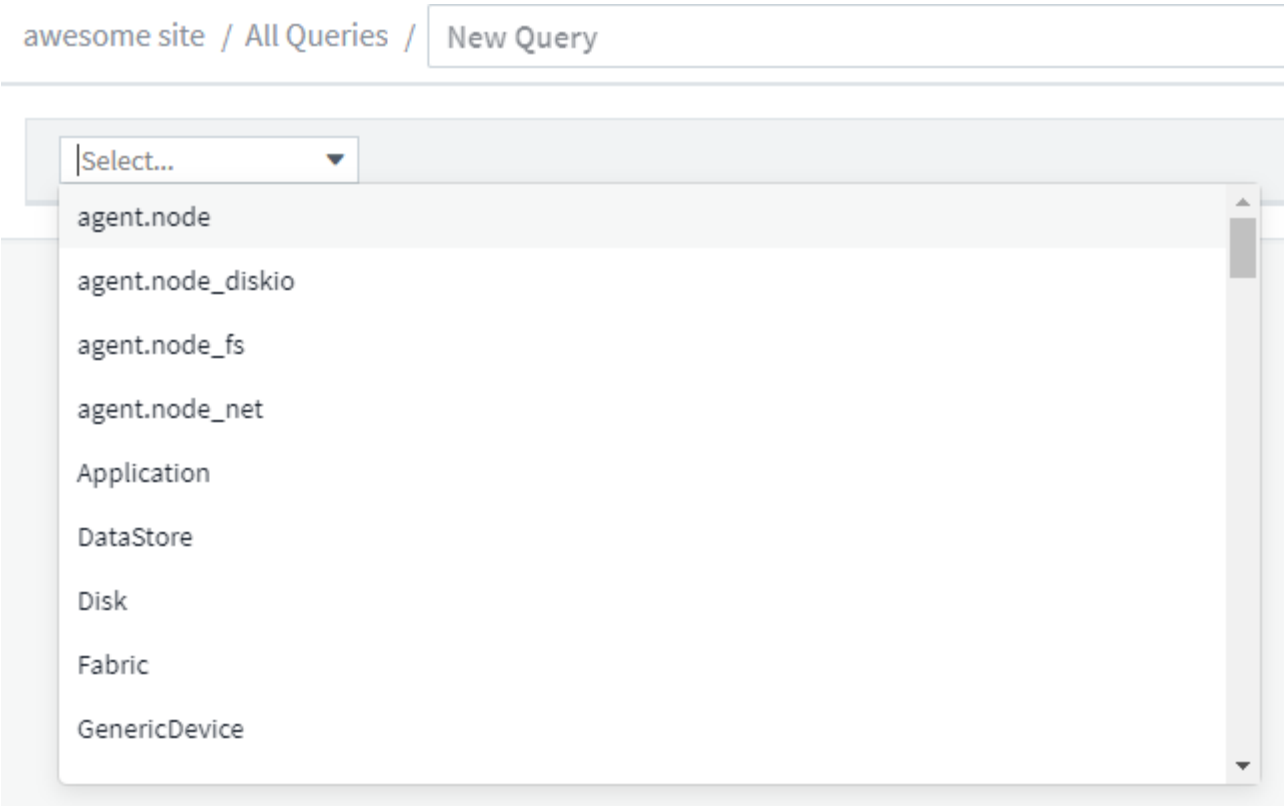
Sie können z. B. eine Abfrage für *Volumes* erstellen, einen Filter hinzufügen, um bestimmte *Storage* zu den ausgewählten Volumes zu finden, einen weiteren Filter hinzufügen, um eine bestimmte *Annotation* zu finden, z. B. „Tier 1“ auf den ausgewählten Speichern, Und schließlich noch einen Filter hinzufügen, um alle Speicher mit *IOPS - Read (IO/s)* größer als 25 zu finden. Wenn die Ergebnisse angezeigt werden, können Sie die mit der Abfrage verknüpften Datenspalten in aufsteigender oder absteigender Reihenfolge sortieren.

Hinweis: Wenn ein neuer Datensammler hinzugefügt wird, der Assets erfasst oder Anmerkungen oder Anwendungszuweisungen vorgenommen werden, können Sie diese neuen Assets, Anmerkungen oder Anwendungen erst nach der Indizierung der Abfragen abfragen. Die Indizierung erfolgt in regelmäßigen Abständen oder während bestimmter Ereignisse, z. B. bei der Ausführung von Anmerkungsregeln.

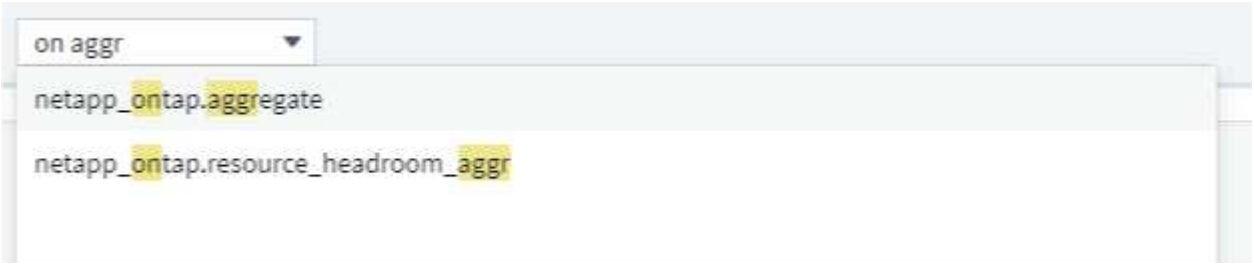
Das Erstellen einer Abfrage ist sehr einfach:

1. Navigieren Sie zu **Abfragen > *+Neue Abfrage**.
2. Wählen Sie in der Liste „Auswählen…“ den Objekttyp aus, nach dem Sie abfragen möchten. Sie können durch die Liste blättern oder Sie können mit der Eingabe beginnen, um schneller zu finden, wonach Sie suchen.

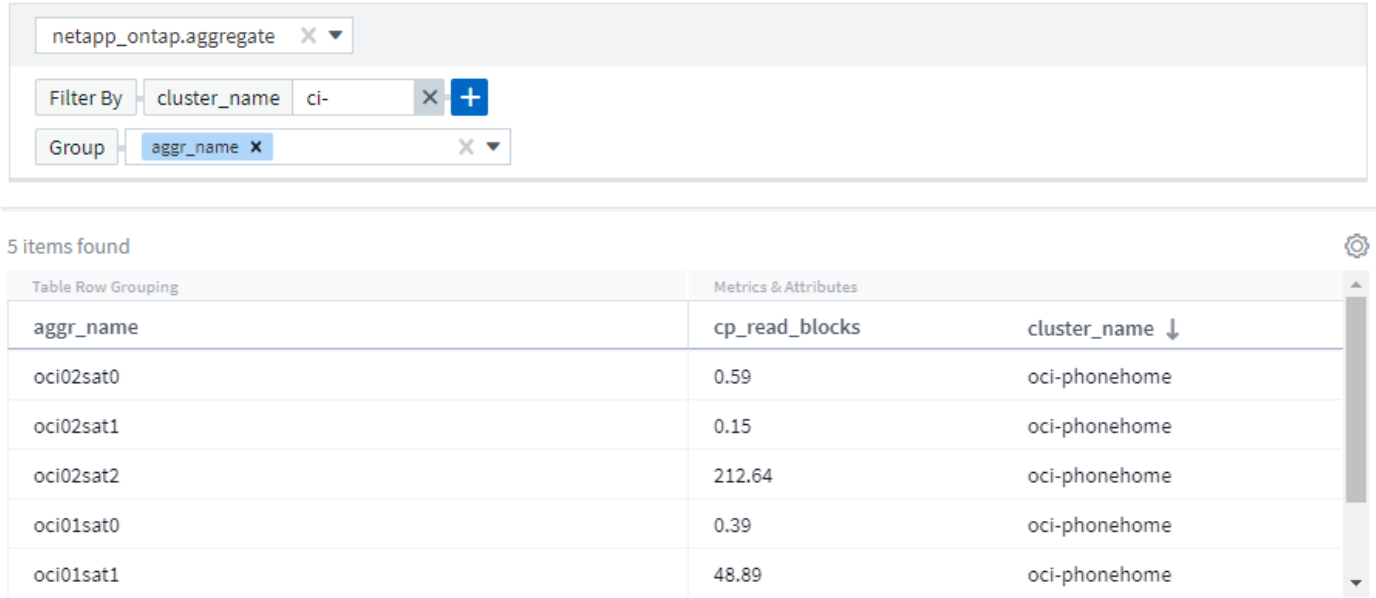
Bildlaufliste:



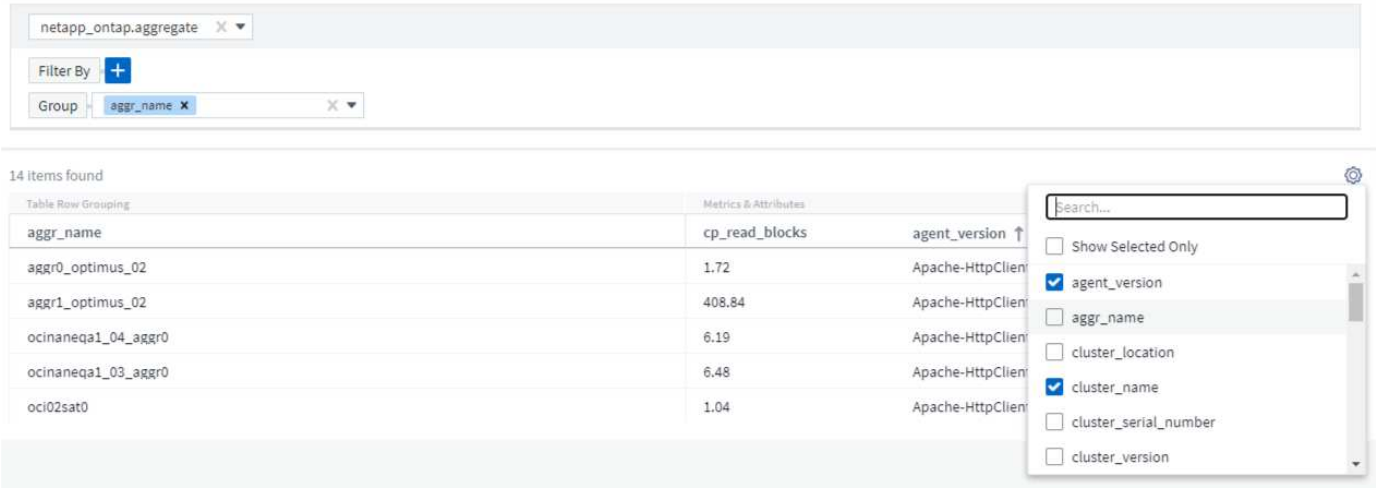
Typ-zu-Suche:



Sie können Filter hinzufügen, um Ihre Anfrage weiter einzuschränken, indem Sie im Feld **Filtern nach** auf die Schaltfläche **+** klicken. Zeilen nach Objekt oder Attribut gruppieren. Bei der Arbeit mit Integrationsdaten (Kubernetes, ONTAP Advanced Metrics usw.) können Sie, falls gewünscht, mehrere Attribute gruppieren.



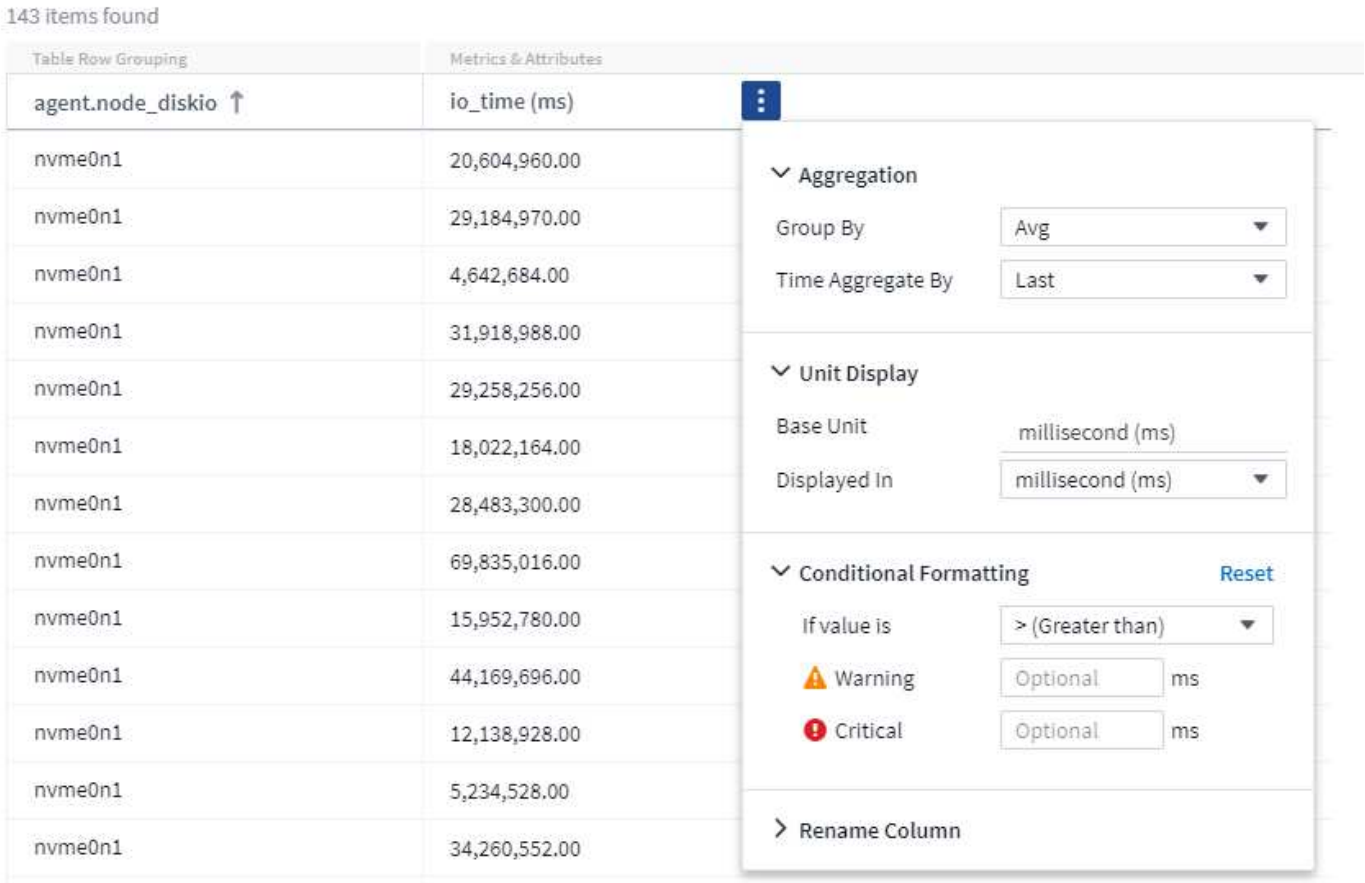
Die Liste der Abfrageergebnisse zeigt je nach dem gesuchten Objekttyp eine Reihe von Standardspalten an. Um die Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle. Die verfügbaren Spalten variieren je nach Asset/metrischem Typ.



Wählen Sie „Aggregation“, „Einheiten“, „Bedingte Formatierung“

Aggregation und Einheiten

Bei „Wert“-Spalten können Sie Ihre Abfrageergebnisse weiter verfeinern, indem Sie auswählen, wie die angezeigten Werte aggregiert werden, und die Einheiten auswählen, in denen diese Werte angezeigt werden. Diese Optionen finden Sie, indem Sie das Menü „drei Punkte“ in der oberen Ecke einer Spalte auswählen.



Einheiten

Sie können die Einheiten auswählen, in denen die Werte angezeigt werden sollen. Wenn z. B. in der Spalte „ausgewählt“ die Bruttokapazität angezeigt wird und die Werte in gib angezeigt werden, sie jedoch lieber als tib angezeigt werden, wählen Sie aus dem Dropdown-Menü „Geräteanzeige“ einfach „tib“ aus.

Aggregation

Wenn die angezeigten Werte aus den zugrunde liegenden Daten als „Durchschnitt“ aggregiert werden, Aber Sie möchten die Summe aller Werte anzeigen, wählen Sie "Summe" entweder aus der Dropdown-Liste *Group by* (wenn Sie die Summen in Gruppen anzeigen möchten) oder aus der Dropdown-Liste *time Aggregate by* (wenn die Zeilenwerte Summen der zugrunde liegenden Daten anzeigen sollen).

Sie können gruppierte Datenpunkte nach *AVG, Max, Min oder Sum* aggregieren.

Sie können einzelne Zeilendaten nach *Average, Last Data Point Acquired, Maximum, Minimum oder Sum* aggregieren.

Bedingte Formatierung

Mit der bedingten Formatierung können Sie in der Liste der Abfrageergebnisse Schwellenwerte für die Warn- und kritische Ebene hervorheben und so Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar machen.

Bedingte Formatierung wird für jede Spalte separat festgelegt. Sie können beispielsweise einen Satz Schwellenwerte für eine Spalte Kapazität und einen weiteren Satz für eine Spalte Durchsatz auswählen.

Spalte Umbenennen

Durch das Umbenennen einer Spalte wird der angezeigte Name in der Liste der Abfrageergebnisse geändert. Der neue Spaltenname wird auch in der resultierenden Datei angezeigt, wenn Sie die Abfrageliste in .CSV exportieren.

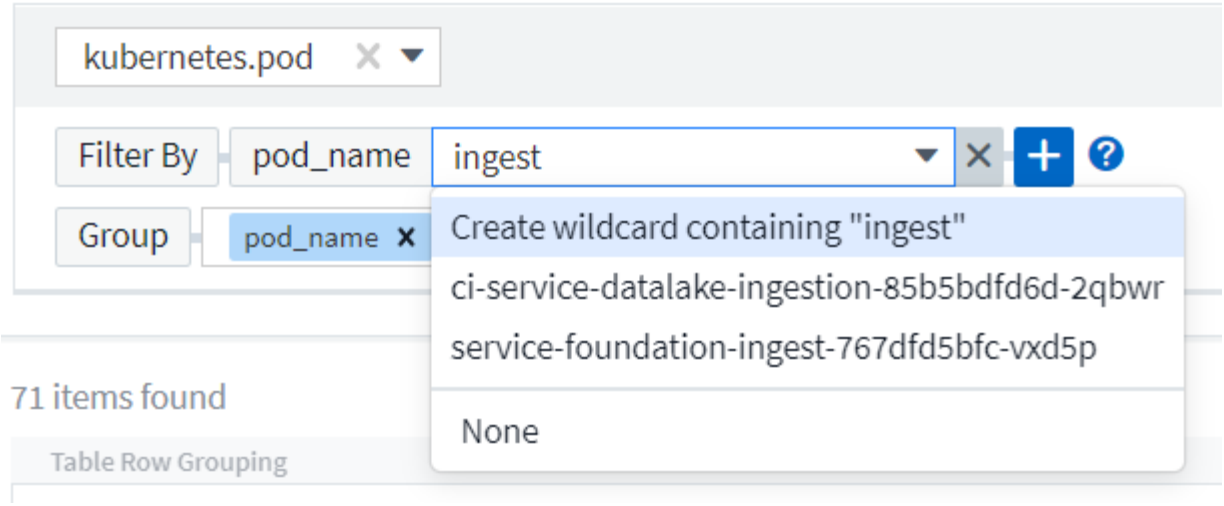
Speichern

Nachdem Sie Ihre Anfrage so konfiguriert haben, dass Sie die gewünschten Ergebnisse anzeigen, können Sie auf die Schaltfläche **Speichern** klicken, um die Abfrage für die zukünftige Verwendung zu speichern. Geben Sie ihm einen aussagekräftigen und eindeutigen Namen.

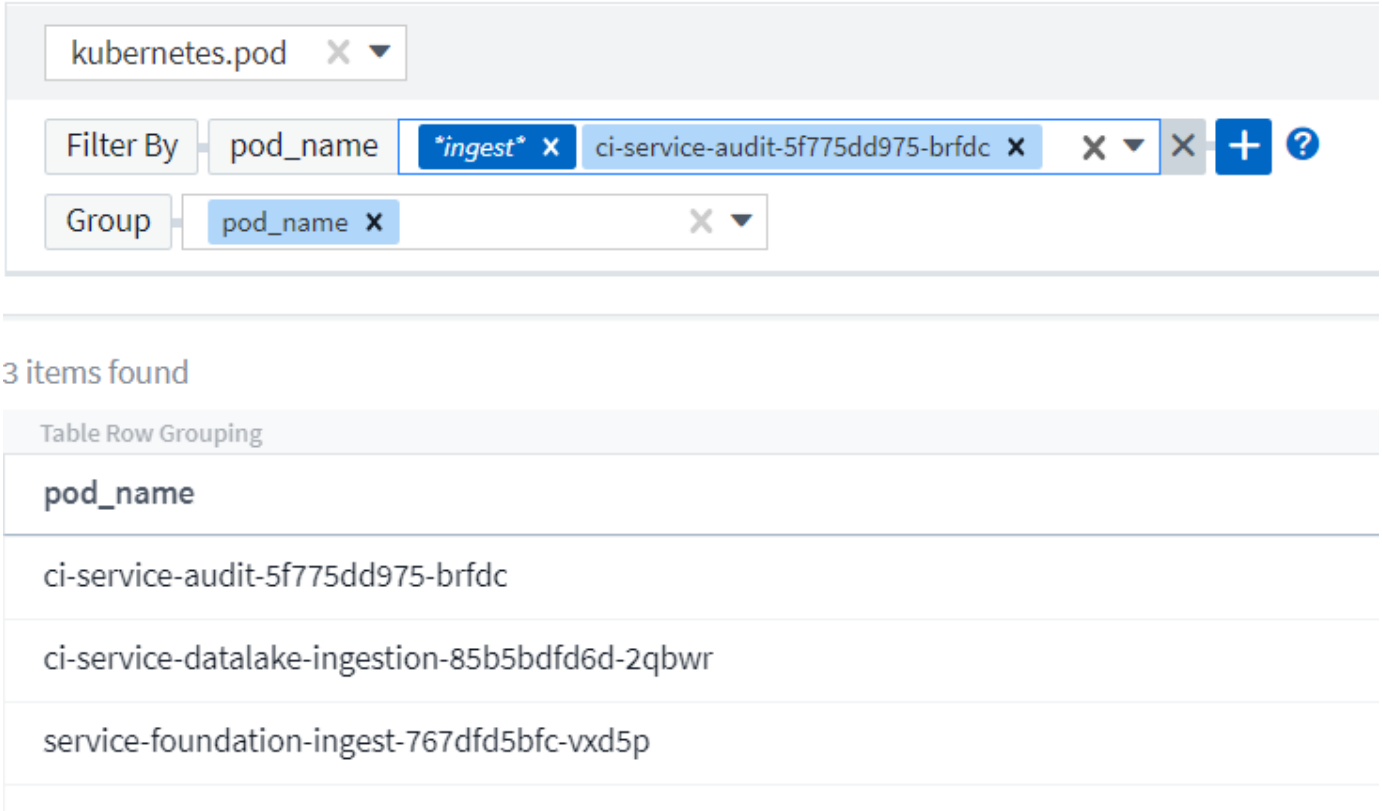
Mehr zum Filtern

Platzhalter und Ausdrücke

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text- oder Listenwerten filtern, werden Sie beim Eingeben mit der Option angezeigt, basierend auf dem aktuellen Text einen **Platzhalter-Filter** zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse angezeigt, die dem Platzhalterausdruck entsprechen. Sie können auch **Expressions** mit NOT oder ODER erstellen, oder Sie können die Option "Keine" auswählen, um nach Null-Werten im Feld zu filtern.



Filter basierend auf Platzhalter oder Ausdrücken (z. B. NICHT, ODER, „Keine“ usw.) wird im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.



Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit numerischen Werten, Daten oder Booleanen.

Verfeinern Von Filtern

Sie können den Filter wie folgt verfeinern:

Filtern	Das macht es	Beispiel	Ergebnis

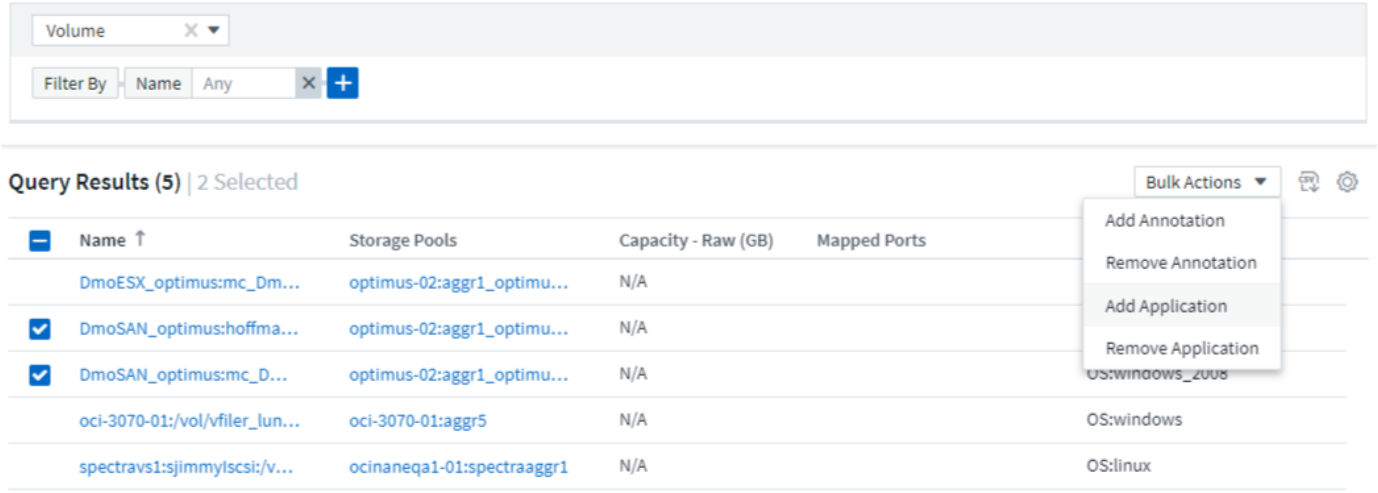
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	vol.	Gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „RHEL“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	Gibt BOS-PRD zurück***12_ -S12, BOS-PRD23_***-S12 und so weiter
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	FAS2240, CX600 ODER FAS3270	Gibt eine beliebige von FAS2440, CX600 oder FAS3270 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT EMC*	Liefert alles zurück, was nicht mit „EMC“ beginnt
Keine	Sucht in allen Feldern nach Null-Werten	*Keine*	Gibt Ergebnisse an, bei denen das Zielfeld leer ist
Nicht *	Sucht nach Null-Werten in Feldern *Text-only*	Nicht *	Gibt Ergebnisse an, bei denen das Zielfeld leer ist

Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse, die ein wortwörtlicher Stern sind; das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelten Anführungszeichen eingeschlossen sind.

Was mache ich jetzt, wenn ich Abfrageergebnisse habe?

Durch Abfragen können Sie einfach Anmerkungen hinzufügen oder Anwendungen zu Assets zuweisen. Beachten Sie, dass Sie Ihren Bestandsbeständen (Festplatte, Speicher usw.) nur Anwendungen oder Anmerkungen zuweisen können. Integrationsmetriken können keine Anmerkungen oder Anwendungszuweisungen übernehmen.

Um den Anlagen, die sich aus Ihrer Abfrage ergeben, eine Anmerkung oder Anwendung zuzuweisen, wählen Sie die Anlage(en) mithilfe der Checkbox-Spalte links in der Ergebnistabelle aus. Klicken Sie dann rechts auf die Schaltfläche **Massenaktionen**. Wählen Sie die gewünschte Aktion aus, die auf die ausgewählten Assets angewendet werden soll.



Abfrage zu Anmerkungsregeln erforderlich

Wenn Sie konfigurieren "Anmerkungsregeln", Jede Regel muss eine zugrunde liegende Abfrage haben, um mit zu arbeiten. Aber wie Sie oben gesehen haben, können Abfragen so breit oder so eng gemacht werden, wie Sie benötigen.

Anzeigen von Abfragen

Sie können Ihre Abfragen anzeigen, um Ihre Assets zu überwachen und zu ändern, wie Ihre Abfragen die Daten zu Ihren Assets anzeigen.

Schritte

1. Melden Sie sich bei Ihrem Cloud Insights-Mandanten an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**. Sie können die Anzeige von Abfragen mit einer der folgenden Methoden ändern:
3. Sie können Text in das Filterfeld eingeben, um nach bestimmten Abfragen zu suchen.
4. Sie können die Sortierreihenfolge der Spalten in der Tabelle der Abfragen durch Klicken auf den Pfeil in der Spaltenüberschrift auf aufsteigender (Aufwärtspfeil) oder absteigender (Abwärtspfeil) ändern.
5. Wenn Sie die Größe einer Spalte ändern möchten, bewegen Sie den Mauszeiger über die Spaltenüberschrift, bis ein blauer Balken angezeigt wird. Legen Sie die Maus über die Leiste, und ziehen Sie sie nach rechts oder links.
6. Um eine Spalte zu verschieben, klicken Sie auf die Spaltenüberschrift und ziehen Sie sie nach rechts oder links.

Beachten Sie beim Blättern durch die Abfrageergebnisse, dass sich die Ergebnisse ändern können, wenn Cloud Insights Ihre Datensammler automatisch abfragt. Dies kann dazu führen, dass einige Elemente fehlen oder einige Elemente in der Reihenfolge erscheinen, je nachdem, wie sie sortiert sind.

Abfrageergebnisse werden in eine CSV-Datei exportiert

Sie können die Ergebnisse einer beliebigen Abfrage in eine .CSV-Datei exportieren, die es Ihnen ermöglicht, die Daten zu analysieren oder in eine andere Anwendung zu importieren.

Schritte

1. Melden Sie sich bei Cloud Insights an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

3. Klicken Sie auf eine Abfrage.
4. Klicken Sie Auf So exportieren Sie die Abfrageergebnisse in eine CSV-Datei.

> Der Export nach .CSV ist auch im Menü „drei Punkte“ in den Dashboard-Tabellen Widgets sowie in den meisten Landing Page-Tabellen verfügbar.

Die exportierten Daten geben die aktuell angezeigten Filter-, Spalten- und Spaltennamen wieder.

Hinweis: Wenn ein Komma in einem Asset-Namen angezeigt wird, schließt der Export den Namen in Anführungszeichen ein, wobei der Asset-Name und das richtige .csv-Format beibehalten werden.

Wenn Sie eine exportierte CSV-Datei mit Excel öffnen, wenn Sie einen Objektnamen oder ein anderes Feld im Format NN:NN haben (zwei Ziffern gefolgt von einem Doppelpunkt gefolgt von zwei weiteren Ziffern), interpretiert Excel diesen Namen manchmal als Zeitformat, statt Textformat. Dies kann dazu führen, dass in Excel falsche Werte in diesen Spalten angezeigt werden. Ein Objekt mit dem Namen „81:45“ wird beispielsweise in Excel als „81:45:00“ angezeigt.

Um dies zu umgehen, importieren Sie die .CSV-Datei in Excel anhand der folgenden Schritte:

1. Öffnen Sie ein neues Blatt in Excel.
2. Wählen Sie auf der Registerkarte „Daten“ die Option „aus Text“.
3. Suchen Sie die gewünschte .CSV-Datei und klicken Sie auf „Importieren“.
4. Wählen Sie im Importassistenten die Option "getrennt" und klicken Sie auf Weiter.
5. Wählen Sie "Komma" für das Trennzeichen und klicken Sie auf Weiter.
6. Wählen Sie die gewünschten Spalten aus und wählen Sie „Text“ für das Spaltendatenformat.
7. Klicken Sie Auf Fertig Stellen.

   Ihre Objekte sollten in Excel im richtigen Format angezeigt werden.

Eine Abfrage ändern oder löschen

Sie können die Kriterien ändern, die einer Abfrage zugeordnet sind, wenn Sie die Suchkriterien für die abfragenden Assets ändern möchten.

Ändern einer Abfrage

Schritte

1. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage
3.

Um der Abfrage ein Kriterium hinzuzufügen, klicken Sie auf Wählen Sie in der Liste ein Kriterium aus.

4. Um einen Filter aus der Abfrage zu entfernen, klicken Sie auf das **X** neben dem zu entfernenden Filter.

Wenn Sie alle erforderlichen Änderungen vorgenommen haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Schaltfläche **Speichern**, um die Abfrage mit dem ursprünglich verwendeten Namen zu speichern.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Speichern unter**, um die Abfrage mit einem anderen Namen zu speichern. Die ursprüngliche Abfrage wird dadurch nicht überschrieben.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Umbenennen** aus, um den ursprünglich verwendeten Abfragenamen zu ändern. Dadurch wird die ursprüngliche Abfrage überschrieben.
- Klicken Sie auf das Dropdown-Menü neben der Schaltfläche **Speichern** und wählen Sie **Kartenänderungen** aus, um die Abfrage auf die zuletzt gespeicherten Änderungen zurückzusetzen.

Löschen einer Abfrage

Um eine Abfrage zu löschen, klicken Sie auf **Abfragen** und wählen Sie **Alle Abfragen anzeigen** aus, und führen Sie einen der folgenden Schritte aus:

1. Klicken Sie rechts neben der Abfrage auf das Menü "drei Punkte" und klicken Sie auf **Löschen**.
2. Klicken Sie auf den Namen der Abfrage und wählen Sie im Dropdown-Menü * Speichern* * die Option * Löschen.

Tabellenwerte werden kopiert

Sie können Werte in Tabellen zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopieren.

Über diese Aufgabe

Es gibt zwei Methoden, mit denen Sie Werte aus Tabellen kopieren oder Ergebnisse in die Zwischenablage abfragen können.

Schritte

1. Methode 1: Markieren Sie den gewünschten Text mit der Maus, kopieren Sie ihn und fügen Sie ihn in Suchfelder oder andere Anwendungen ein.
2. Methode 2: Bewegen Sie den Mauszeiger über das Feld, und klicken Sie auf das Clipboard-Symbol Das erscheint. Der Wert wird zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopiert.

   Beachten Sie, dass nur Werte, die Verknüpfungen zu Assets sind, mit dieser Methode kopiert werden können. Nur Felder, die einzelne Werte enthalten (d. h. nicht-Listen), haben das Kopiensymbol.

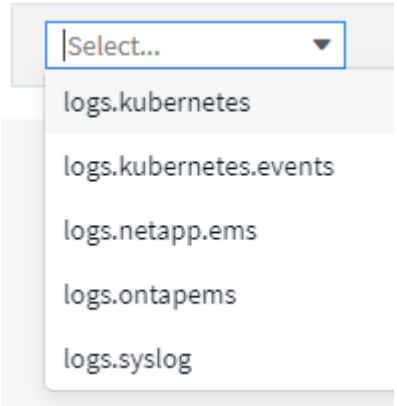
Log-Explorer

Der Cloud Insights Log Explorer ist ein leistungsstarkes Tool zum Abfragen von

Systemprotokollen. Zusätzlich zur Unterstützung bei Ermittlungen können Sie auch eine Protokollabfrage in einem Monitor speichern, um Warnmeldungen zu geben, wenn diese bestimmten Protokollauslöser aktiviert sind.

Klicken Sie auf **Log Queries > +New Log Query**, um mit der Suche nach Protokollen zu beginnen.

Wählen Sie ein verfügbares Protokoll aus der Liste aus.

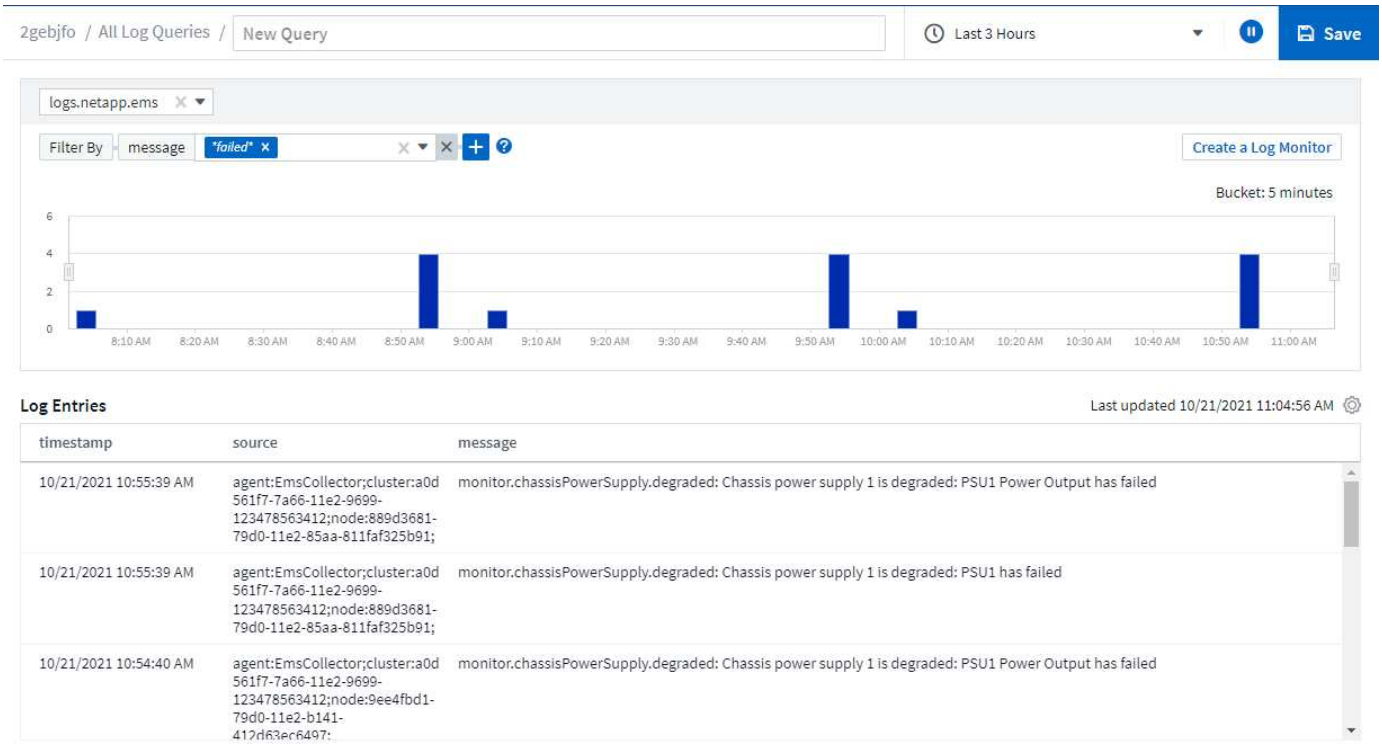


Die für das Abfragen verfügbaren Protokolltypen können je nach Umgebung variieren. Im Laufe der Zeit können weitere Protokolltypen hinzugefügt werden.

Sie können Filter festlegen, um die Ergebnisse der Abfrage weiter zu verfeinern. Um beispielsweise alle Protokollmeldungen zu finden, die einen Fehler anzeigen, setzen Sie einen Filter für *Messages*, der das Wort „Fehlgeschlagen“ enthält.

Sie können damit beginnen, den gewünschten Text in das Filterfeld einzugeben. Cloud Insights fordert Sie auf, eine Platzhaltersuche zu erstellen, die den String enthält, während Sie eingeben.

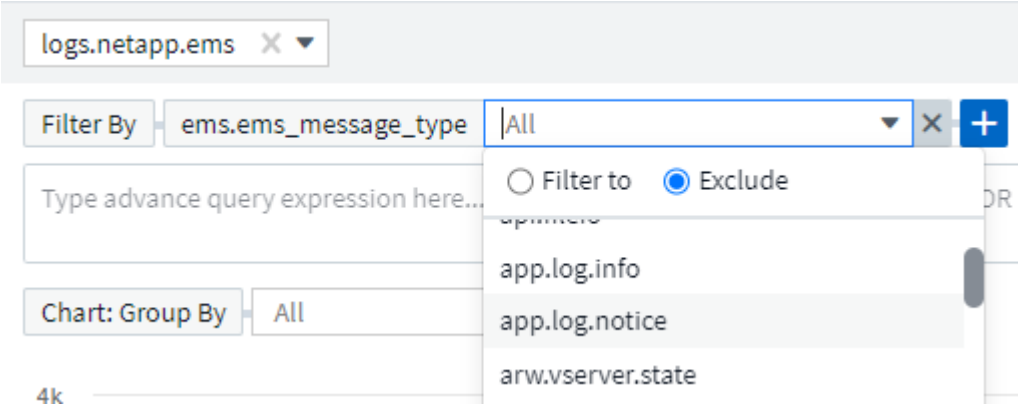
Die Ergebnisse werden in einem Diagramm angezeigt, in dem die Anzahl der Protokollinstanzen in jedem angezeigten Zeitraum angezeigt wird. Unter der Grafik sehen Sie die Protokolleinträge, die sich selbst bewegen. Das Diagramm und die Einträge werden automatisch auf der Grundlage des ausgewählten Zeitbereichs aktualisiert.



Filtern

Ein-/Ausschließen

Beim Filtern der Protokolle können Sie wählen, ob Sie **include** (d.h. "Filter to") oder **exclude** die von Ihnen eintippten Strings wählen. Ausgeschlossene Zeichenfolgen werden im abgeschlossenen Filter als „NICHT <string>“ angezeigt.



Filter basierend auf Platzhalter oder Ausdrücken (z. B. NICHT, ODER, „Keine“ usw.) wird im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.

> Sie können jederzeit auf *Protokollmonitor erstellen* klicken, um einen neuen Monitor basierend auf dem aktuellen Filter zu erstellen.

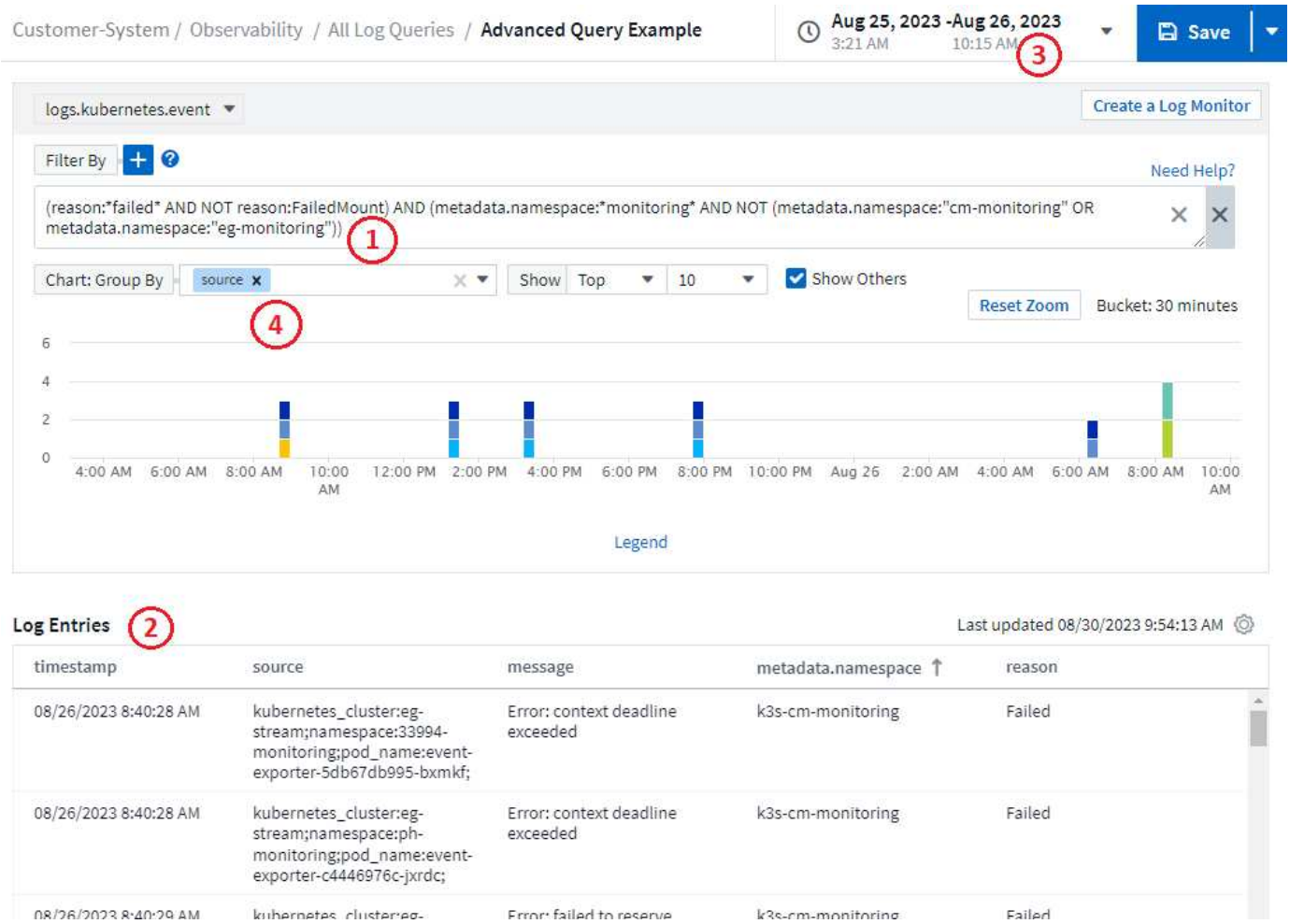
Erweiterte Filterung

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text- oder Listenwerten filtern, werden Sie beim Eingeben mit der Option angezeigt, basierend auf dem aktuellen Text einen **Platzhalter-Filter** zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse angezeigt, die dem Platzhalterausdruck

entsprechen. Sie können auch Ausdrücke mit NOT, AND, OR oder erstellen oder Sie können die Option „Keine“ auswählen, um nach Nullwerten zu filtern.

> Achten Sie darauf, Ihre Abfrage frühzeitig und häufig zu speichern, wenn Sie Ihre Filterung erstellen. Beim erweiterten Abfragen handelt es sich um einen „Freiform“-String-Eintrag, und beim Erstellen können Fehler beim Parsen auftreten.

Sehen Sie sich dieses Bildschirmbild an, das gefilterte Ergebnisse für eine erweiterte Abfrage des *logs.kubernetes.Event*-Protokolls zeigt. Auf dieser Seite ist viel los, was unter dem Bild erklärt wird:



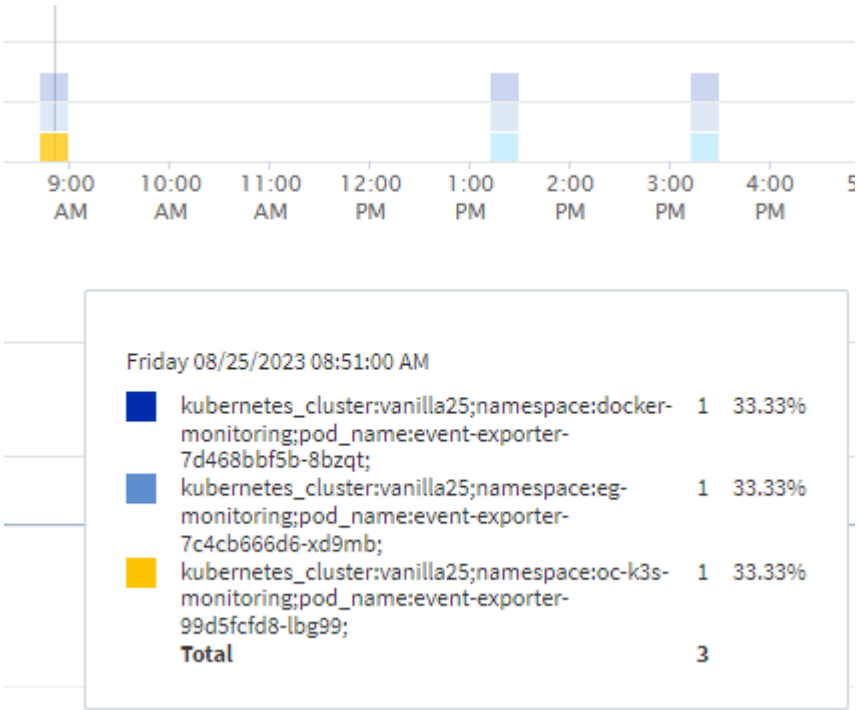
1. Diese erweiterte Abfragezeichenfolge filtert Folgendes:
   - Filtern Sie nach Protokolleinträgen mit einem *reason*, der das Wort "failed" enthält, aber nichts mit dem spezifischen Grund von "FailedMount".
   - Fügen Sie einen dieser Einträge mit *metadata.namespace* ein, einschließlich des Wortes "Monitoring", aber schließen Sie die spezifischen Namespaces von "cm-Monitoring" oder "EG-Monitoring" aus.

     Beachten Sie, dass im obigen Fall, da sowohl "cm-Monitoring" als auch "EG-Monitoring" einen Bindestrich ("-") enthalten, die Strings in doppelte Anführungszeichen eingefügt werden müssen, oder ein Parsing-Fehler angezeigt wird. Zeichenfolgen, die keine Bindestriche, Leerzeichen usw. enthalten, müssen nicht in Anführungszeichen eingeschlossen werden. Im Zweifelsfall versuchen Sie, die Zeichenfolge in Anführungszeichen zu setzen.

2. Die Ergebnisse des aktuellen Filters, einschließlich aller „Filtern nach“-Werte UND des erweiterten Abfragefilters, werden in der Ergebnisliste angezeigt. Die Liste kann nach allen angezeigten Spalten

sortiert werden. Um weitere Spalten anzuzeigen, wählen Sie das Zahnrad-Symbol.

3. Das Diagramm wurde vergrößert, um nur Protokollergebnisse anzuzeigen, die innerhalb eines bestimmten Zeitrahmens aufgetreten sind. Der hier angezeigte Zeitbereich entspricht dem aktuellen Zoomfaktor. Wählen Sie die Schaltfläche *Zoom zurücksetzen*, um den Zoom-Level auf den aktuellen Cloud Insights-Zeitbereich zurückzusetzen.
4. Die Diagrammergebnisse wurden nach dem Feld *source* gruppiert. Das Diagramm zeigt die Ergebnisse in jeder Spalte, die in Farben gruppiert sind. Wenn Sie den Mauszeiger über eine Spalte im Diagramm bewegen, werden einige Details zu den spezifischen Einträgen angezeigt.



Verfeinern Von Filtern

Sie können den Filter wie folgt verfeinern:

Filtern	Das macht es
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen
Keine	Sucht in allen Feldern nach Null-Werten
Nicht *	Sucht nach Null-Werten in Feldern *Text-only*

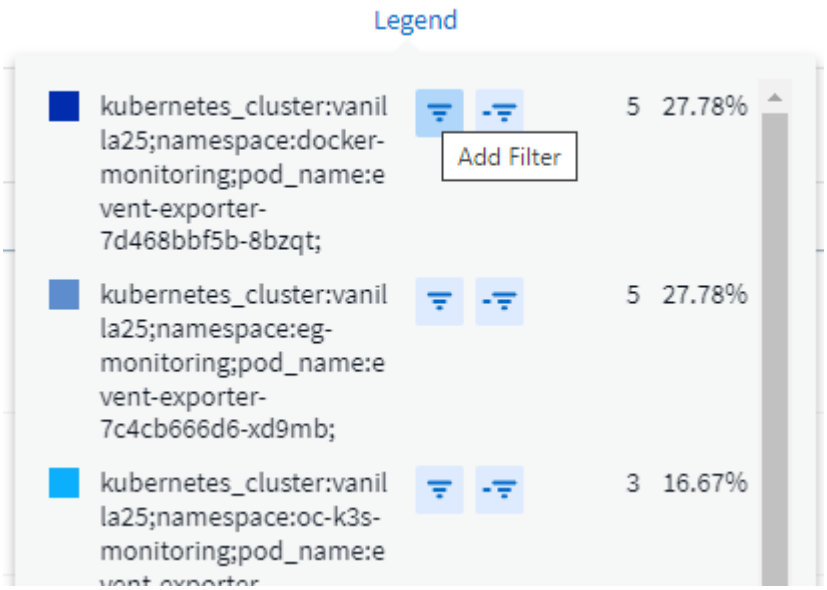
Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse, die ein wortwörtlicher Stern sind; das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelten

Anführungszeichen eingeschlossen sind.

Sie können einen einfachen Filter mit einem erweiterten Abfragefilter kombinieren; der resultierende Filter ist ein "UND" der beiden.

Die Diagrammlegende

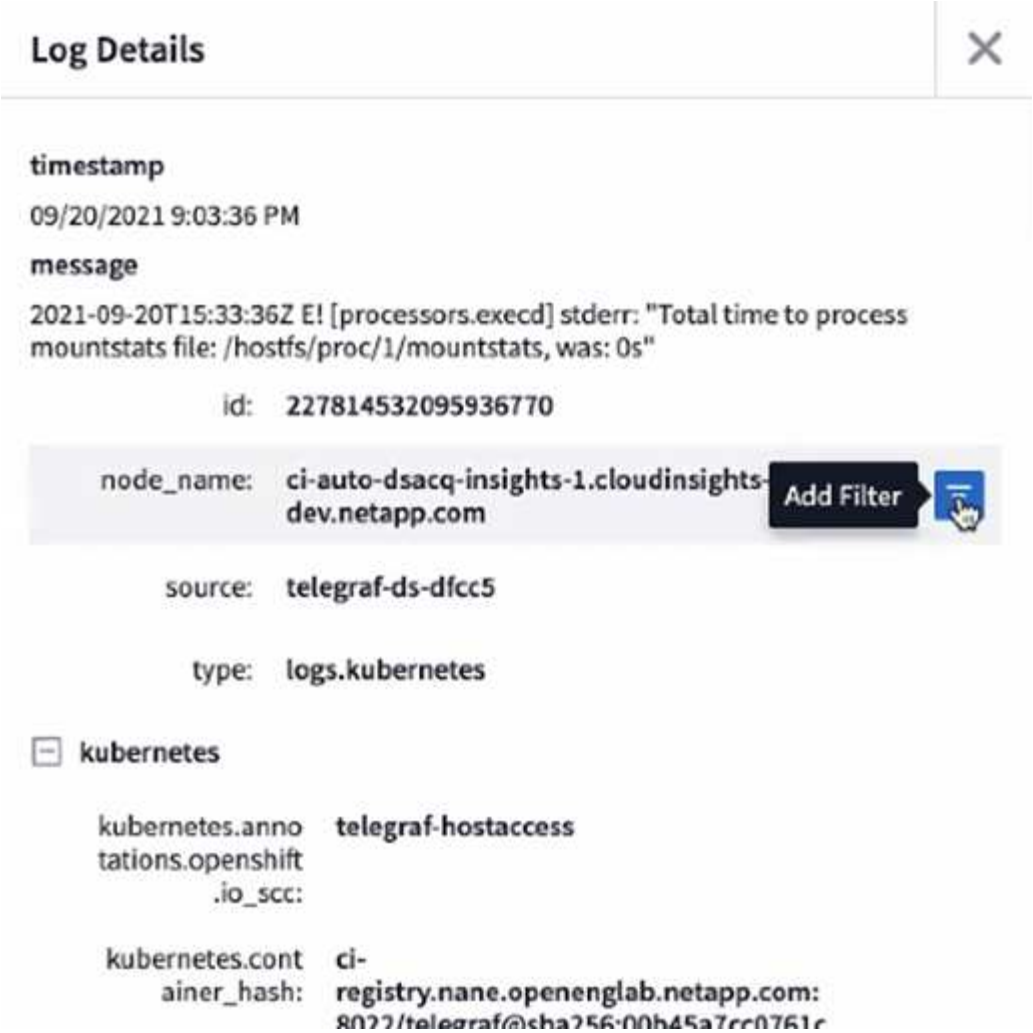
Die *Legend* unterhalb des Diagramms hat auch einige Überraschungen. Für jedes in der Legende angezeigte Ergebnis (basierend auf dem aktuellen Filter) haben Sie die Möglichkeit, nur Ergebnisse für diese Zeile anzuzeigen (Filter hinzufügen) oder Ergebnisse anzuzeigen, die NICHT für diese Zeile vorhanden sind (Filter hinzufügen). Das Diagramm und die Liste Protokolleinträge werden aktualisiert, um die Ergebnisse basierend auf Ihrer Auswahl anzuzeigen. Um diese Filterung zu entfernen, öffnen Sie die Legende erneut, und wählen Sie [X], um den Legendenfilter zu löschen.



Protokolldetails

Wenn Sie auf eine beliebige Stelle in einem Protokolleintrag in der Liste klicken, wird ein Detailfenster für diesen Eintrag geöffnet. Hier können Sie weitere Informationen zur Veranstaltung einsehen.

Klicken Sie auf „Filter hinzufügen“, um das ausgewählte Feld dem aktuellen Filter hinzuzufügen. Die Protokolleintragsliste wird basierend auf dem neuen Filter aktualisiert.



Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Protokollanfragen.

Problem:	Teste das:
Ich sehe keine „Debug“ Nachrichten in meiner Log-Abfrage	Debug-Protokollnachrichten werden nicht erfasst. Um die gewünschten Meldungen zu erfassen, ändern Sie den Schweregrad der betreffenden Nachricht in den Wert *„informative“, „Error“, „Alert“, „Emergency“ oder „Notice“*.

Einblick

Einblick

Einblicke ermöglichen es Ihnen, sich über Dinge wie die Ressourcennutzung und die Auswirkungen auf andere Ressourcen oder die Zeit-zu-volle Analyse zu informieren.

Eine Reihe von Einsichten stehen zur Verfügung. Navigieren Sie zu **Dashboards > Insights**, um mit dem Tauchen zu beginnen. Sie können aktive Insights (derzeit auftretende Einblicke) auf der Hauptregisterkarte oder inaktive Einblicke auf der Registerkarte „*Inaktive Insights*“ anzeigen. Inaktive Einblicke sind solche, die

zuvor aktiv waren, aber nicht mehr auftreten.

Insight Typen

Unter Stress Abbauen

Durch Workloads mit hohen Auswirkungen kann die Performance anderer Workloads in einer gemeinsamen Ressource reduziert werden. Dadurch wird die gemeinsam genutzte Ressource unter Druck. Cloud Insights bietet Tools, mit denen Sie die Sättigung von Ressourcen und Auswirkungen in Ihrer Umgebung analysieren können. "Weitere Informationen"

Kubernetes Namespaces sind nicht mehr platzsparend

Die Kubernetes Namesaces sind nicht mehr Teil des Space Insight. Sie erhalten einen Einblick in Workloads in Ihren Kubernetes-Namespaces, die Gefahr bestehen, dass der Speicherplatz zu knapp wird. Sie erhalten eine Schätzung für die Anzahl der verbleibenden Tage, bevor der Speicherplatz voll ist. "Weitere Informationen"

Rückgewinnung von ONTAP Cold Storage

Der *Reclaim ONTAP Cold Storage* Insight liefert Daten zur kalten Kapazität, zu potenziellen Kosten-/Energieeinsparungen sowie empfohlene Maßnahmen für Volumes auf ONTAP Systemen. "Weitere Informationen"

> Dies ist eine *Preview* Funktion und kann sich im Laufe der Zeit ändern, wenn Verbesserungen vorgenommen werden. "Weitere Informationen ." Informationen zu den Funktionen der Cloud Insights-Vorschau.

Einblicke: Shared Ressourcen Unter Stress

Durch Workloads mit hohen Auswirkungen kann die Performance anderer Workloads in einer gemeinsamen Ressource reduziert werden. Dadurch wird die gemeinsam genutzte Ressource unter Druck. Cloud Insights bietet Tools, mit denen Sie die Sättigung von Ressourcen und Auswirkungen in Ihrer Umgebung analysieren können.

Terminologie

Wenn wir über Workload- oder Ressourcenauswirkungen sprechen, sind die folgenden Definitionen hilfreich.

Ein **anspruchsvoller Workload** ist ein Workload, der derzeit als Auswirkungen auf andere Ressourcen im Shared Storage Pool identifiziert wird. Diese Workloads führen zu höheren IOPS (zum Beispiel) und reduzieren somit die IOPS für die betroffenen Workloads. Anspruchsvolle Workloads werden manchmal „*High-verbrauchende Workloads*“ genannt.

Ein **betroffener Workload** ist ein Workload, der von einer hohen Auslastung im Shared Storage Pool beeinflusst wird. Diese Workloads verzeichnen aufgrund anspruchsvoller Workloads einen geringeren IOPS-Wert und/oder eine höhere Latenz.

Zu beachten ist, dass das Volume oder das interne Volume selbst als Workload erkannt wird, falls Cloud Insights den führenden Computing-Workload nicht erkannt hat. Dies gilt sowohl für anspruchsvolle als auch für betroffene Workloads.

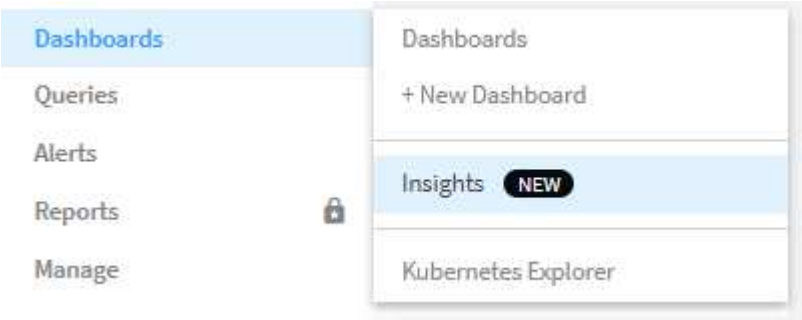
Shared Resource Sättigung ist das Verhältnis der IOPS-Auswirkung zu *Baseline*.

Baseline wird als der maximal gemeldete Datenpunkt für jeden Workload in der Stunde definiert, die unmittelbar vor der erkannten Sättigung liegt.

Ein **Konflikt** oder **Sättigung** tritt auf, wenn sich die IOPS auf andere Ressourcen oder Workloads im Shared Storage Pool auswirken.

Anspruchsvolle Workloads

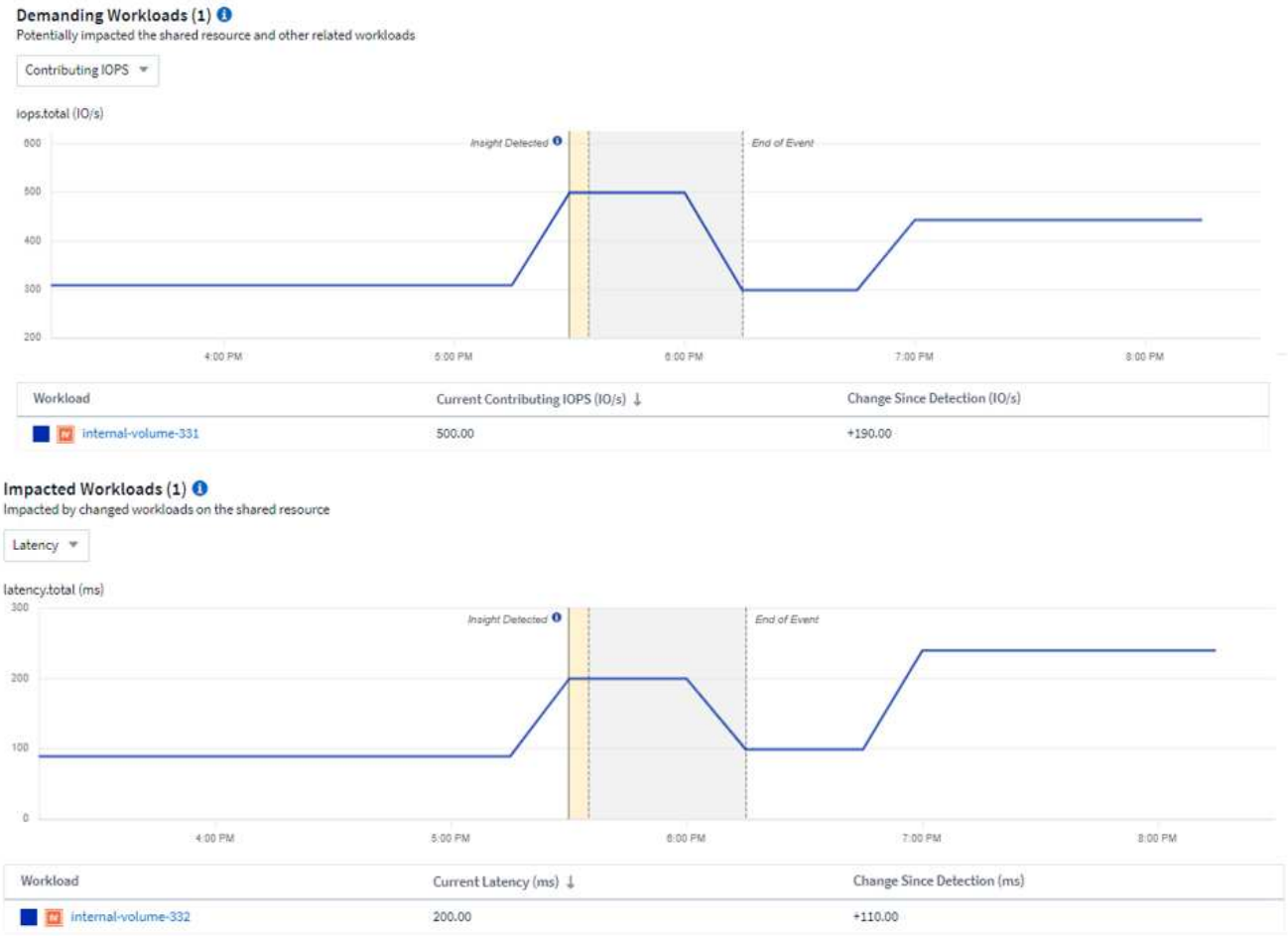
Wenn Sie sich mit anspruchsvollen und beeinträchtigten Workloads in Ihren gemeinsam genutzten Ressourcen vertraut machen möchten, klicken Sie auf **Dashboards > Insights** und wählen Sie die Option **Shared Resources under Stress** Insight aus.



Cloud Insights zeigt eine Liste aller Workloads an, bei denen eine Sättigung erkannt wurde. Beachten Sie, dass Cloud Insights Workloads zeigt, bei denen mindestens eine *anspruchsvolle Ressource* **oder** *betroffene Ressource* erkannt wurde.

Klicken Sie auf einen Workload, um die Detailseite anzuzeigen. Das obere Diagramm zeigt den Vorgang auf der gemeinsam genutzten Ressource (z. B. einen Storage-Pool), über den Konflikte/Sättigung stattfinden.

Im Folgenden werden die beiden Diagramme mit den *anspruchsvollen* Workloads und den Workloads angezeigt, die _durch diese anspruchsvollen Workloads beeinträchtigt sind.



Unter den einzelnen Tabellen finden Sie eine Liste mit Workloads und/oder Ressourcen, die von den Engpässen betroffen sind oder die von diesen Konflikten betroffen sind. Wenn Sie auf eine Ressource klicken (z. B. auf eine VM), wird eine Detailseite für diese Ressource geöffnet. Wenn Sie auf einen Workload klicken, wird eine Abfrageseite geöffnet, auf der die beteiligten Pods angezeigt werden. Beachten Sie, dass, wenn der Link eine leere Abfrage öffnet, es sein kann, dass der betroffene Pod nicht mehr Teil der aktiven Konflikte ist. Sie können den Zeitbereich der Abfrage ändern, um die Pod-Liste in einem größeren oder stärker fokussierten Zeitbereich anzuzeigen.

Was muss ich tun, um Sättigung zu lösen?

Es gibt eine Reihe von Schritten, die Sie ergreifen können, um die Wahrscheinlichkeit einer Sättigung in Ihrer Umgebung zu verringern oder zu beseitigen. Diese werden durch erweitern des Links **+Empfehlungen anzeigen** auf der Seite angezeigt. Hier sind ein paar Dinge, die Sie versuchen können.

- Kunden mit hohen IOPS-Werten bewegen

  Verschieben Sie die „gierigen“ Workloads in weniger gesättigte Storage-Pools. Es wird empfohlen, die Ebene und die Kapazität dieser Pools vor der Verschiebung der Workloads zu bewerten, um unnötige Kosten oder zusätzliche Konflikte zu vermeiden.

- Implementierung einer QoS-Richtlinie (Quality of Service

  Implementierung einer QoS-Richtlinie pro Workload, um sicherzustellen, dass genügend freie Ressourcen verfügbar sind, um die Sättigung des Storage-Pools zu verringern. Das ist eine langfristige Lösung.

- Fügen Sie weitere Ressourcen hinzu

Wenn die gemeinsam genutzte Ressource (zum Beispiel Storage Pool) den IOPS-Sättigungspunkt erreicht hat, stellt das Hinzufügen von mehr oder schnelleren Festplatten zum Pool sicher, dass genügend freie Ressourcen zur Verfügung stehen, um die Sättigung zu verringern.

Zum Schluss können Sie auf den **Insight-Link kopieren** klicken, um die Seiten-url in die Zwischenablage zu kopieren, um sie leichter mit Kollegen zu teilen.

Kubernetes-Namesaces: Der Speicherplatz wird nicht mehr durch den Platzbedarf bestimmt

Speicherplatzbelegung in Ihrer Umgebung ist nie eine gute Situation. Cloud Insights hilft Ihnen, den Zeitaufwand vorherzusagen, bevor die persistenten Volumes von Kubernetes voll werden.

Die _Kubernetes Namesaces sind nicht mehr genügend Speicherplatz für Insight. Sie erhalten eine Übersicht über Workloads auf Ihren Kubernetes-Namespaces, die Gefahr laufen, dass der Speicherplatz zu knapp wird. Eine Schätzung für die verbleibende Anzahl an Tagen, bevor jedes persistente Volume voll wird.

Sie können sich diese Insight anzeigen lassen, indem Sie zu **Dashboards > Einblicke** navigieren.

Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

Klicken Sie auf einen Workload, um eine Detailseite für die Insight zu öffnen. Auf dieser Seite sehen Sie ein Diagramm, das die Workload-Kapazitätstrends sowie eine Tabelle mit den folgenden Angaben zeigt:

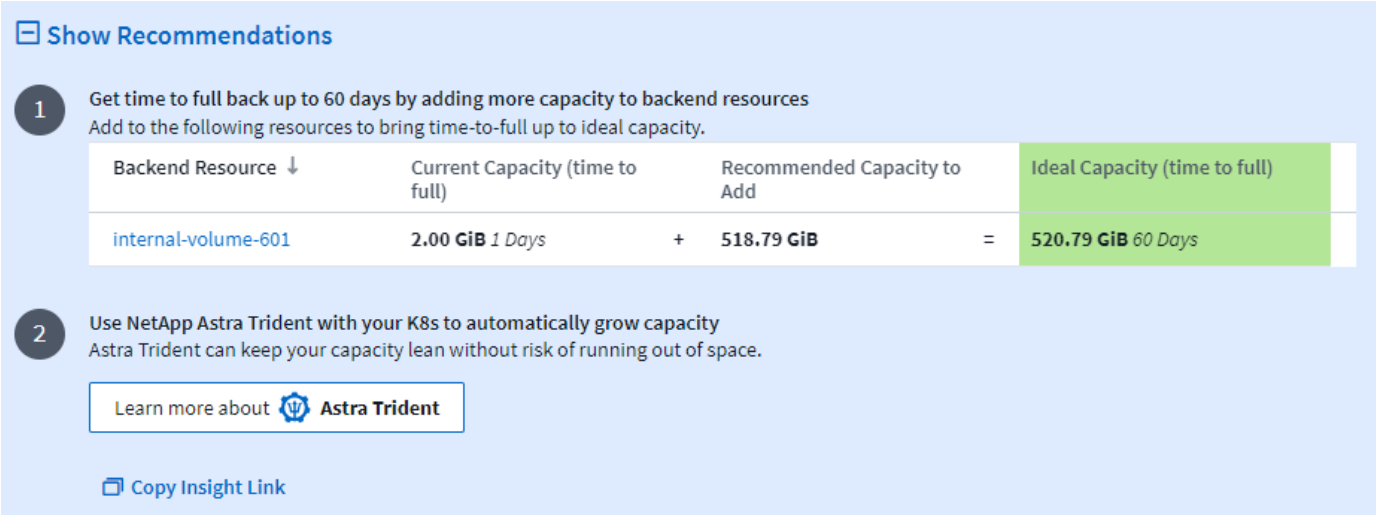
- Workload-Name
- Betroffene persistente Volumes
- Prognostizierte Zeitdauer innerhalb von Tagen
- Kapazität des persistenten Volumes
- Betroffen ist die Back-End Storage-Ressource, wobei die aktuelle Kapazität nicht mehr insgesamt belegt wird. Wenn Sie auf diesen Link klicken, wird die detaillierte Landing Page für das Backend-Volume geöffnet.

Workloads at risk (2)

Workloads	Persistant Volume (pvClaim)	Time to Full (Days) ↓	Persistant Volume Capacity (GiB)	Backend Storage Resource (Capacity Used)	
multi (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)
taskmanager (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)

Was kann ich tun, wenn mir der Platz knapp wird?

Klicken Sie auf der Insight Seite auf **+Empfehlungen anzeigen**, um mögliche Lösungen anzuzeigen. Die einfachste Option, wenn kein Speicherplatz mehr vorhanden ist, ist immer das Hinzufügen weiterer Kapazität. Cloud Insights zeigt Ihnen die optimale Kapazität, um die Zeit bis zur vollständigen 60-Tage-Vorhersage zu erhöhen. Weitere Empfehlungen sind ebenfalls aufgeführt.



Hier können Sie auch einen bequemen Link zu dieser Insight kopieren, die Seite als Lesezeichen hinzufügen oder sie ganz einfach mit Ihrem Team teilen.

Einblick: Rückgewinnung von ONTAP Cold Storage

Der *Reclaim ONTAP Cold Storage* Insight liefert Daten zur kalten Kapazität, zu potenziellen Kosten-/Energieeinsparungen sowie empfohlene Maßnahmen für Volumes auf ONTAP Systemen.

Um diese Einblicke anzuzeigen, navigieren Sie zu **Dashboards > Einblicke** und werfen Sie einen Blick auf den *Reclaim ONTAP Cold Storage* Insight. Beachten Sie, dass diese Insight nur betroffene Storage-Systeme auflistet, wenn Cloud Insights Cold Storage entdeckt hat. Andernfalls wird die Meldung „All clear“ angezeigt.

Beachten Sie, dass kalte Daten, die weniger als 30 Tage alt sind, nicht angezeigt werden.

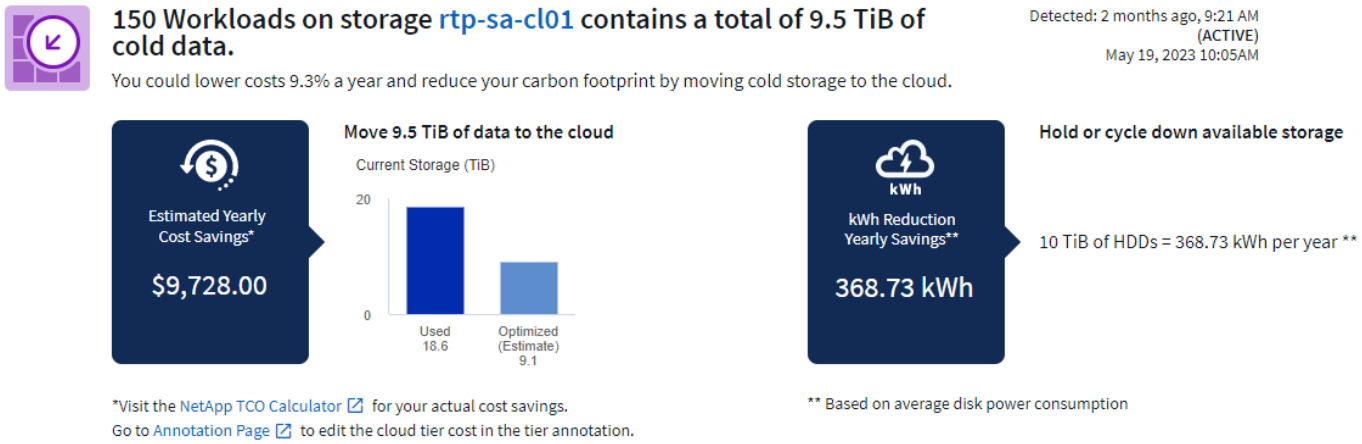
Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected ↓
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

Die Beschreibung von Insight gibt schnell Aufschluss über die erkannte Datenmenge, die als „kalt“ erkannt wird und auf welchem Storage sich die Daten befinden. Die Tabelle bietet auch die Anzahl der Workloads mit „kalten“ Daten.

Wenn Sie einen Insight aus der Liste auswählen, wird eine Seite mit weiteren Details geöffnet, darunter Empfehlungen zum Verschieben von Daten in die Cloud oder zum Herunterfahren von nicht verwendeten Festplatten sowie geschätzte Kosten- und Energieeinsparungen, die Sie durch die Implementierung dieser

Empfehlungen erzielen können. Die Seite bietet sogar einen praktischen Link zu "Der TCO-Rechner von NetApp" So können Sie mit den Zahlen experimentieren.



Empfehlungen

Erweitern Sie auf der Insight-Seite die Option **Empfehlungen**, um die folgenden Optionen zu untersuchen:

- Verschieben Sie ungenutzte Workloads (Zombies) auf kostengünstigeren Storage Tier (HDD).

  Mithilfe der Zombie-Flagge, des Cold Storage und der Anzahl der Tage, finden Sie die kälteste und größte Datenmenge und verschieben Sie den Workload auf eine kostengünstigere Storage-Ebene (z. B. einen Speicherpool, der Festplattenspeicher nutzt). Ein Workload wird als „Zombie“ betrachtet, wenn IS 30 Tage oder länger keine wesentlichen I/O-Anfragen erhalten hat.

- Löschen Sie ungenutzte Workloads

  Überprüfung, welche Workloads nicht verwendet werden, und Archivierung dieser Workloads erwägen oder Entfernen aus dem Storage-System.

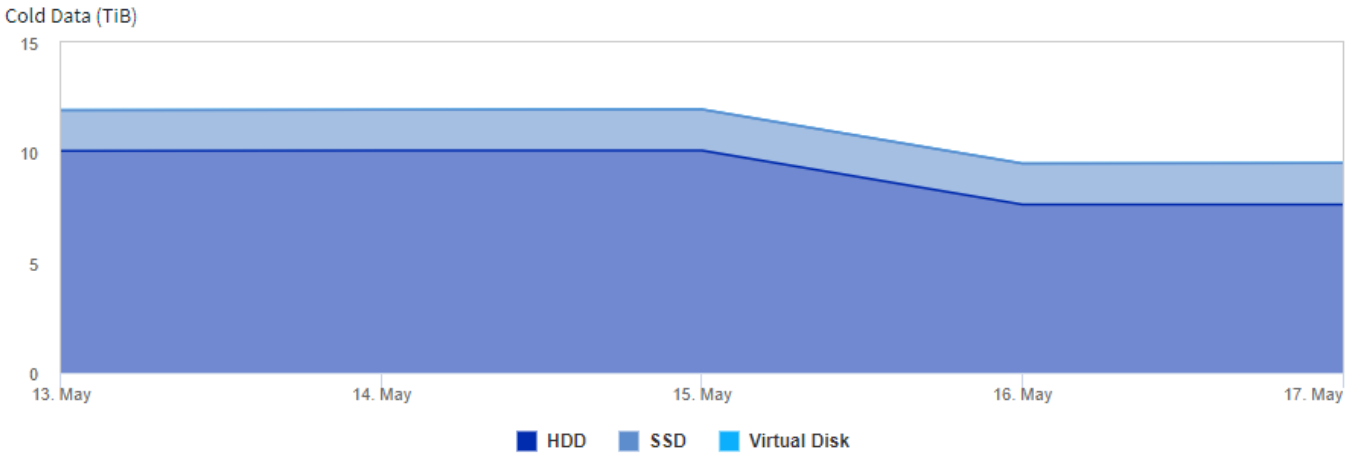
- Man betrachte die Fabric Pool Lösung von NetApp

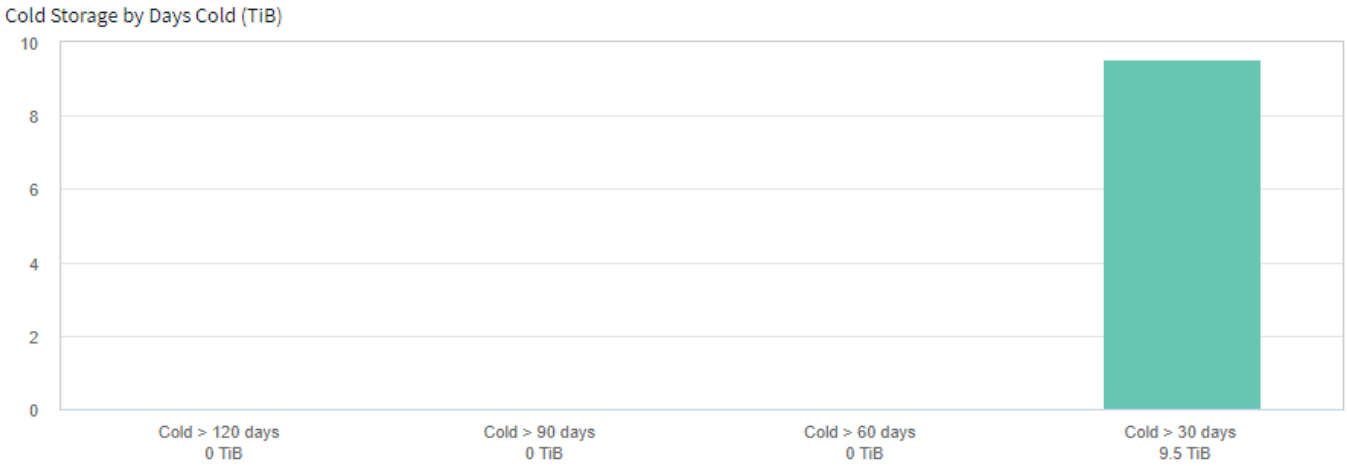
  NetApp "Fabric Pool Lösung" Verschiebt selten benötigte Daten automatisch in kostengünstigen Cloud-Storage, um so die Effizienz Ihrer Performance-Tiers zu steigern und Remote-Datensicherung zu ermöglichen.

Visualisieren und erkunden

Die Diagramme und die Tabelle bieten zusätzliche Trendinformationen sowie die Möglichkeit, detaillierte Informationen zu den einzelnen Workloads zu erhalten.

Cluster Cold Storage Trend Show Details





Workloads with cold data (150) View all workloads Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

Monitore und Alarme

Warnfunktionen mit Monitoren

Sie erstellen Monitore zum Festlegen von Schwellenwerten, die Alarme auslösen, um Sie über Probleme im Zusammenhang mit den Ressourcen im Netzwerk zu informieren. Beispielsweise können Sie einen Monitor erstellen, der für eine beliebige Vielzahl an Protokollen eine Warnung bezüglich „*Node Write Latency*“ ausgegeben wird.

> Monitore und Alarmfunktionen sind in allen Cloud Insights Editionen verfügbar. Die Basisversion unterliegt jedoch den folgenden Eigenschaften: * Sie können nur bis zu fünf benutzerdefinierte Monitore gleichzeitig aktiv haben. Alle Monitore jenseits von fünf werden im Status *Paused* erstellt oder in den Status verschoben. * Die metrischen Monitore VMDK, Virtual Machine, Host und Datenspeicher werden nicht unterstützt. Wenn für diese Metriken Monitore erstellt wurden, werden sie angehalten und können nicht wieder aufgenommen werden, wenn Sie auf Basic Edition heruntergestuft werden.

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.

Cloud Insights bietet eine Reihe von "Systemdefinierte Monitore" Außerdem zu integrieren.

Best Practice Für Sicherheit

Cloud Insights Warnmeldungen wurden entwickelt, um Datenpunkte und Trends in Ihrer Umgebung hervorzuheben. Mit Cloud Insights können Sie jede gültige E-Mail-Adresse als Warnungsempfänger angeben. 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 Cloud Insights auf **Alarme > Monitore verwalten**

   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.

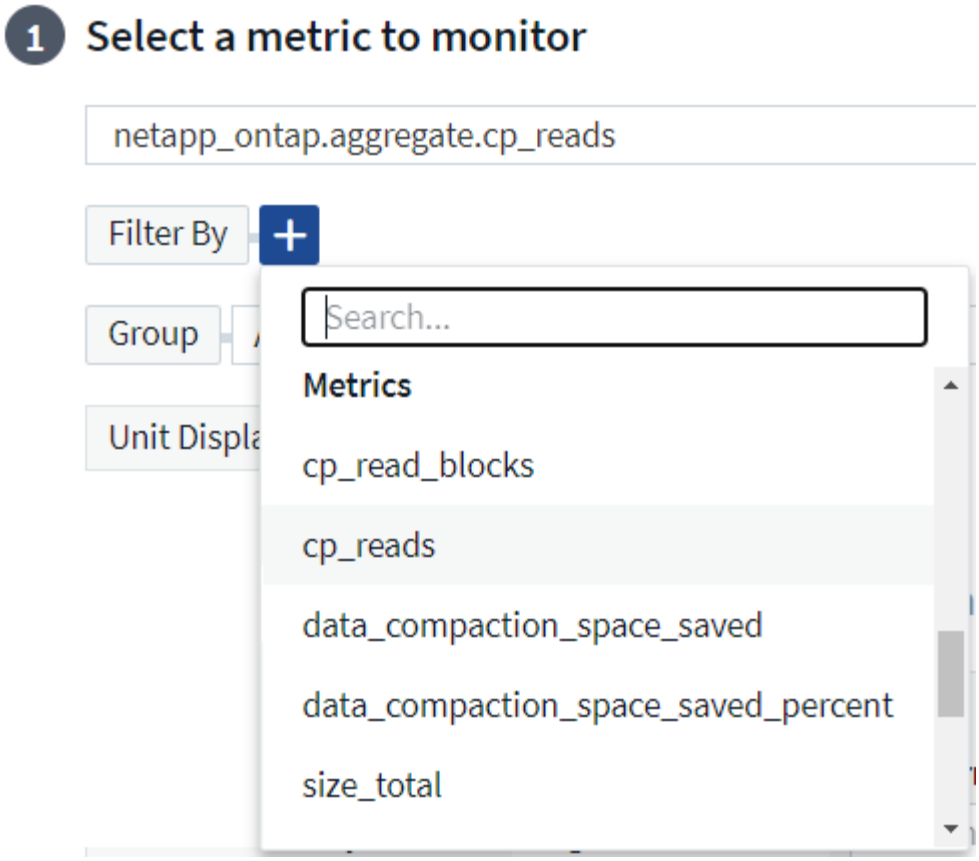
   - *Metric* überwacht Warnmeldungen zu Infrastruktur- oder Performance-bezogenen Triggern
   - *Log* überwacht die Warnung bei protokollbezogenen Aktivitäten

   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.

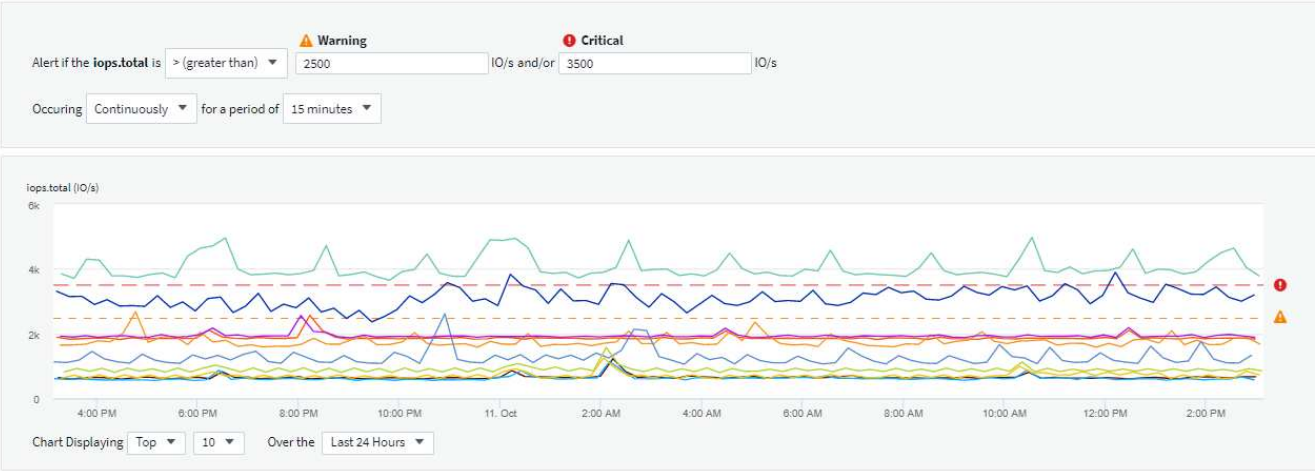
1. Nachdem Sie das zu überwachende Objekt und die Kennzahl ausgewählt haben, legen Sie die Schwellenwerte für Warnstufe und/oder kritische Stufe fest.
2. Geben Sie für die Stufe *Warnung* 200 für unser Beispiel ein. Die gestrichelte Linie, die diese Warnstufe angibt, wird im Beispieldiagramm angezeigt.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

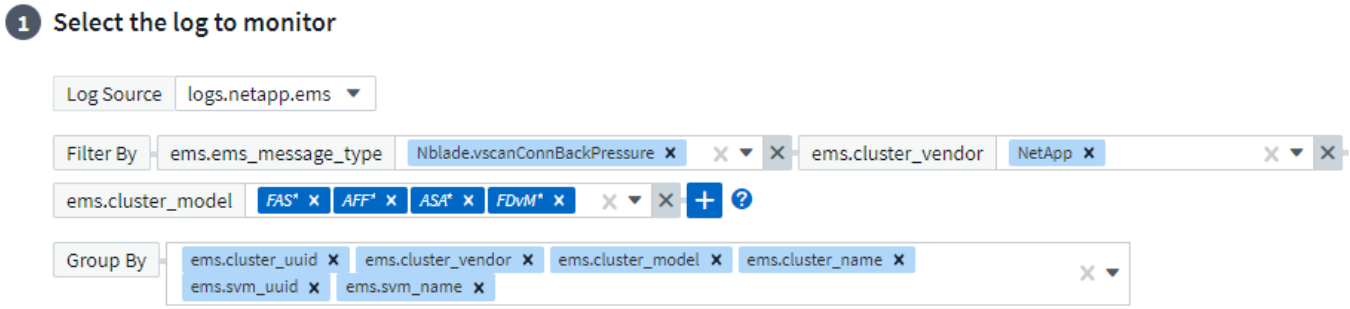
dieser Werte überschreitet.



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.



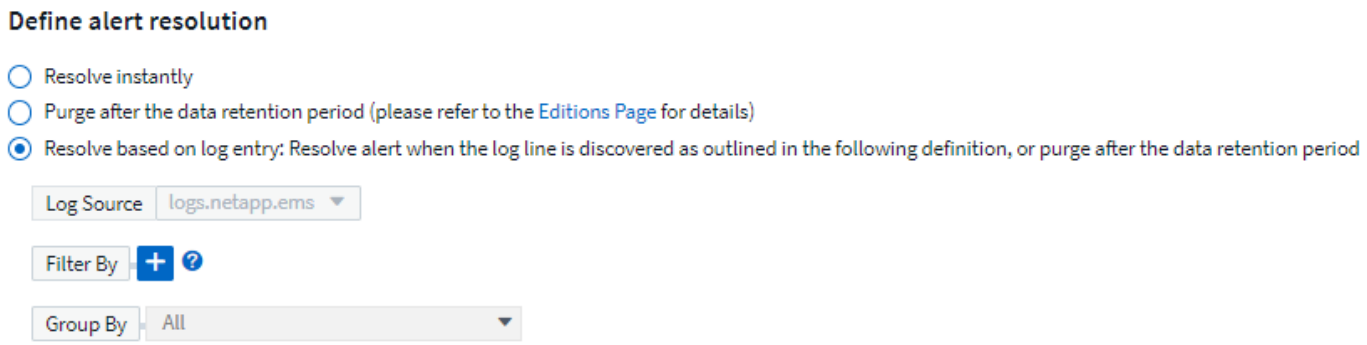
Definieren Sie das Alarmverhalten

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

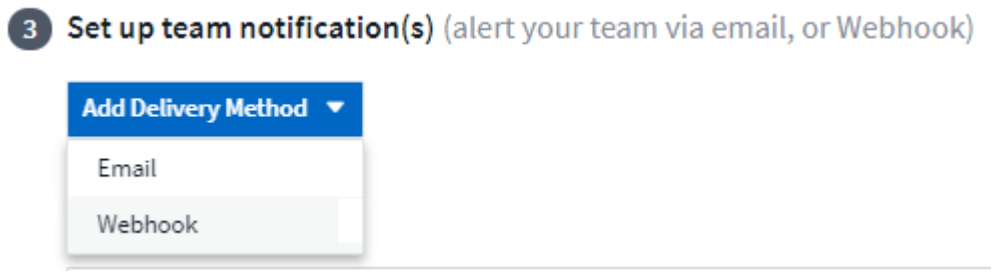
Sie können festlegen, wie eine Protokollüberwachung behoben werden soll. Sie erhalten drei Möglichkeiten:

- Sofort beheben
- Löschen Sie die Daten nach Ablauf der Aufbewahrungsfrist (Details finden Sie auf der Seite „Editionen“). Beachten Sie, dass der Monitor keine Auflösungsbedingung per Definition hat. Daher bleibt eine Warnung *aktiv* und unterdrückt alle nachfolgenden Warnungen mit übereinstimmenden *Group_by*, die von diesem Monitor erstellt wurden, bis die Aufbewahrungsfrist für Daten abgelaufen ist.
- Auflösen anhand von Protokolleingaben: Warnung auflösen, wenn die Protokollzeile wie in der folgenden Definition beschrieben erkannt wird, oder nach Ablauf der Aufbewahrungsfrist löschen.



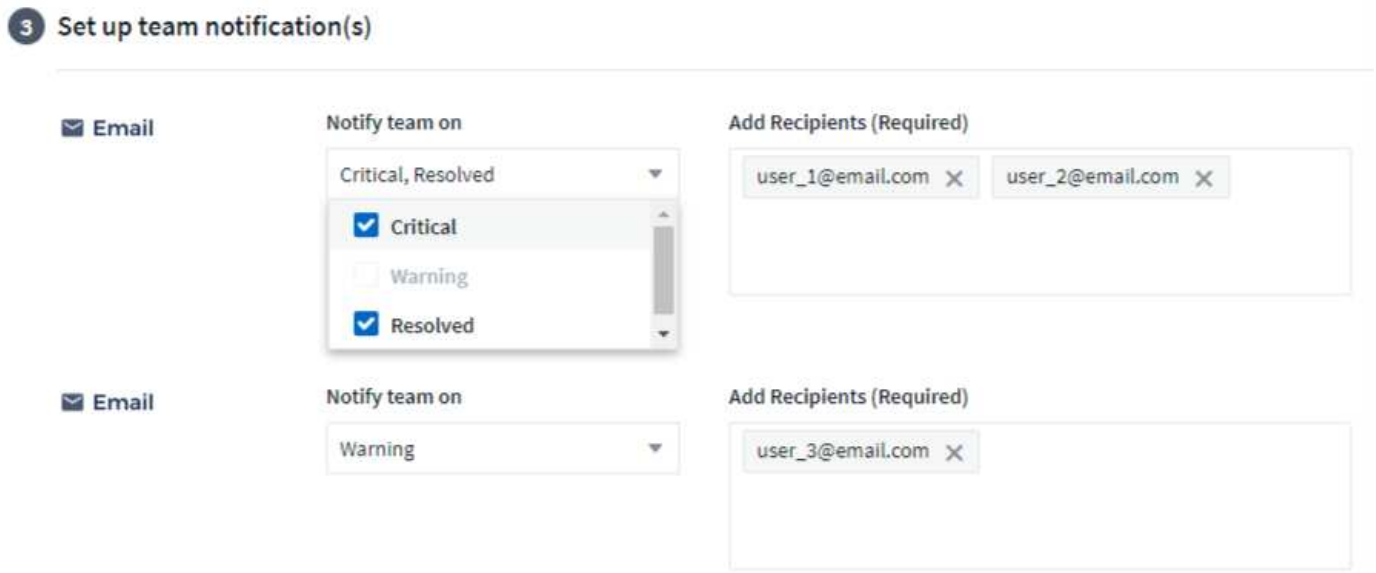
Wählen Sie Benachrichtigungstyp und Empfänger aus

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



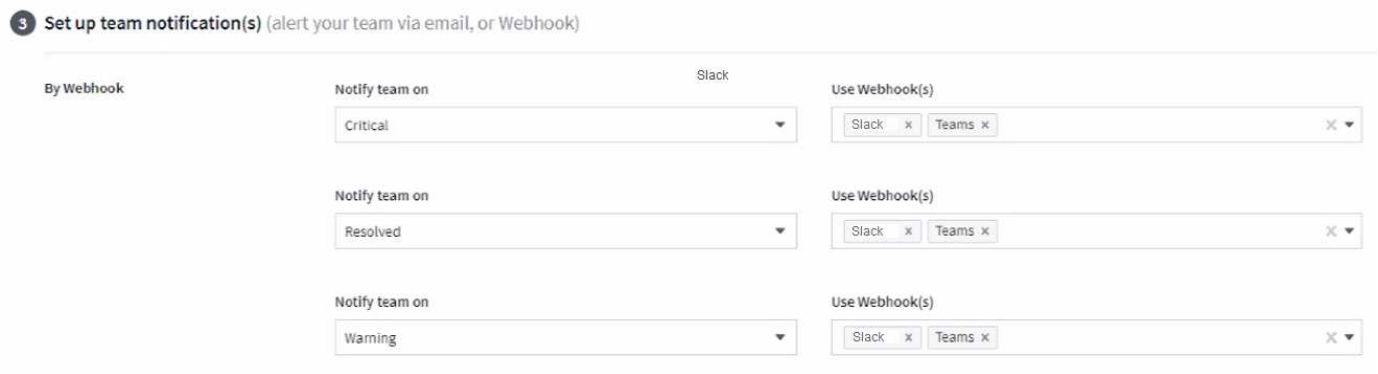
Alerting via Email:

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.

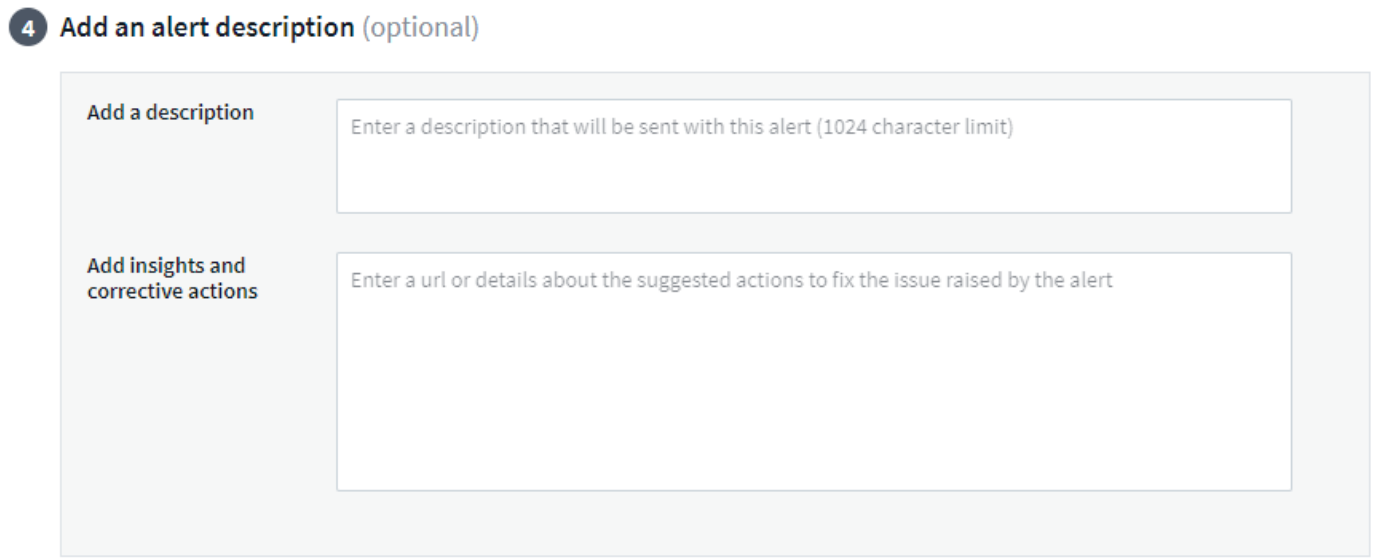


ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen 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.



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

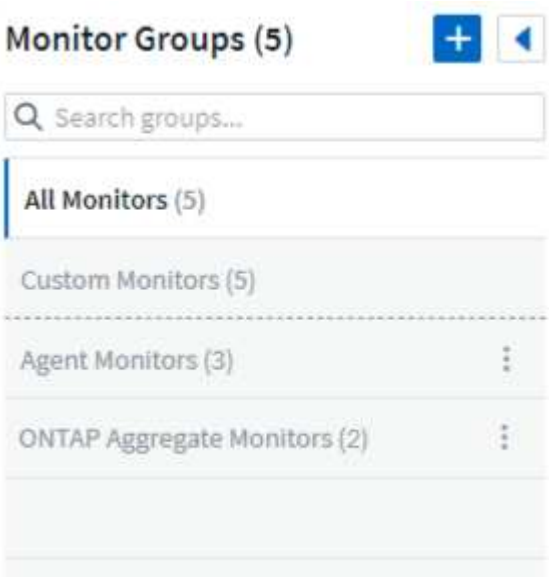
Sie können die Überwachung eines Objekttyps vorübergehend anhalten, indem Sie auf das Menü rechts neben dem Monitor klicken und **Pause** wählen. Wenn Sie bereit sind, die Überwachung fortzusetzen, klicken Sie auf **Fortsetzen**.

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 Monitorgruppe für den Speicher in Ihrer Umgebung einrichten oder überwachen, die für eine bestimmte Empfängerliste relevant ist.



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 Monitore** listet alle Systemmonitore auf, die von Cloud Insights ausgesetzt wurden.
- Cloud Insights zeigt auch eine Reihe von **Systemüberwachengruppen** an, in denen eine oder mehrere Gruppen von aufgelistet werden "Systemdefinierte Monitore", Einschließlich der ONTAP Infrastruktur und Workload-Überwachung.

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 Cloud 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

Diese Gruppen zeigen von Cloud Insights bereitgestellte Monitore an, sofern Ihre Umgebung die von den Monitoren benötigten Geräte und/oder Protokollverfügbarkeit enthält.

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.

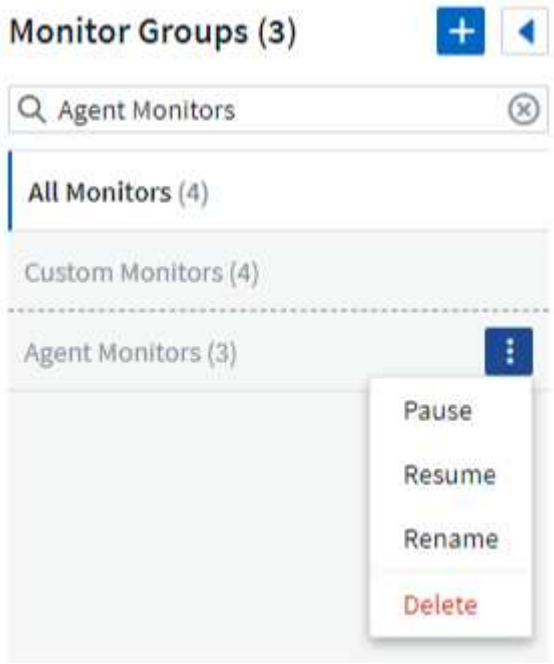
Entfernen Sie Monitore, indem Sie auf eine Gruppe klicken und im Menü *aus Gruppe* entfernen auswählen. Sie können keine Monitore aus der Gruppe „*Alle Monitore*“ oder „ Benutzerdefinierte Monitore_“ entfernen. Um einen Monitor aus diesen Gruppen zu löschen, müssen Sie den Monitor selbst löschen.

> Durch Entfernen eines Monitors aus einer Gruppe wird der Monitor nicht aus Cloud 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. Durch das Löschen einer Gruppe werden die Monitore nicht aus Cloud Insights gelöscht; sie sind weiterhin in *Alle Monitore* verfügbar.



Systemdefinierte Monitore

Cloud Insights umfasst eine Reihe von systemdefinierten Monitoren für Kennzahlen und Protokolle. Die verfügbaren Systemmonitore sind abhängig von den Datensammlern in Ihrer Umgebung. Aus diesem Grund können sich die in Cloud Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Sehen Sie sich die an "Systemdefinierte Monitore" Seite mit Beschreibungen der in Cloud Insights enthaltenen Monitore.

Weitere Informationen

- "Anzeigen und Fehlstellen von Warnungen"

Anzeigen und Verwalten von Warnmeldungen von Monitoren

Cloud Insights zeigt bei jedem dieser Meldungen an "Überwachte Schwellenwerte" Werden überschritten.

Monitore und Alarmfunktionen sind in der Cloud Insights Standard Edition und höher erhältlich.

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 Zahnrad-Symbol 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:

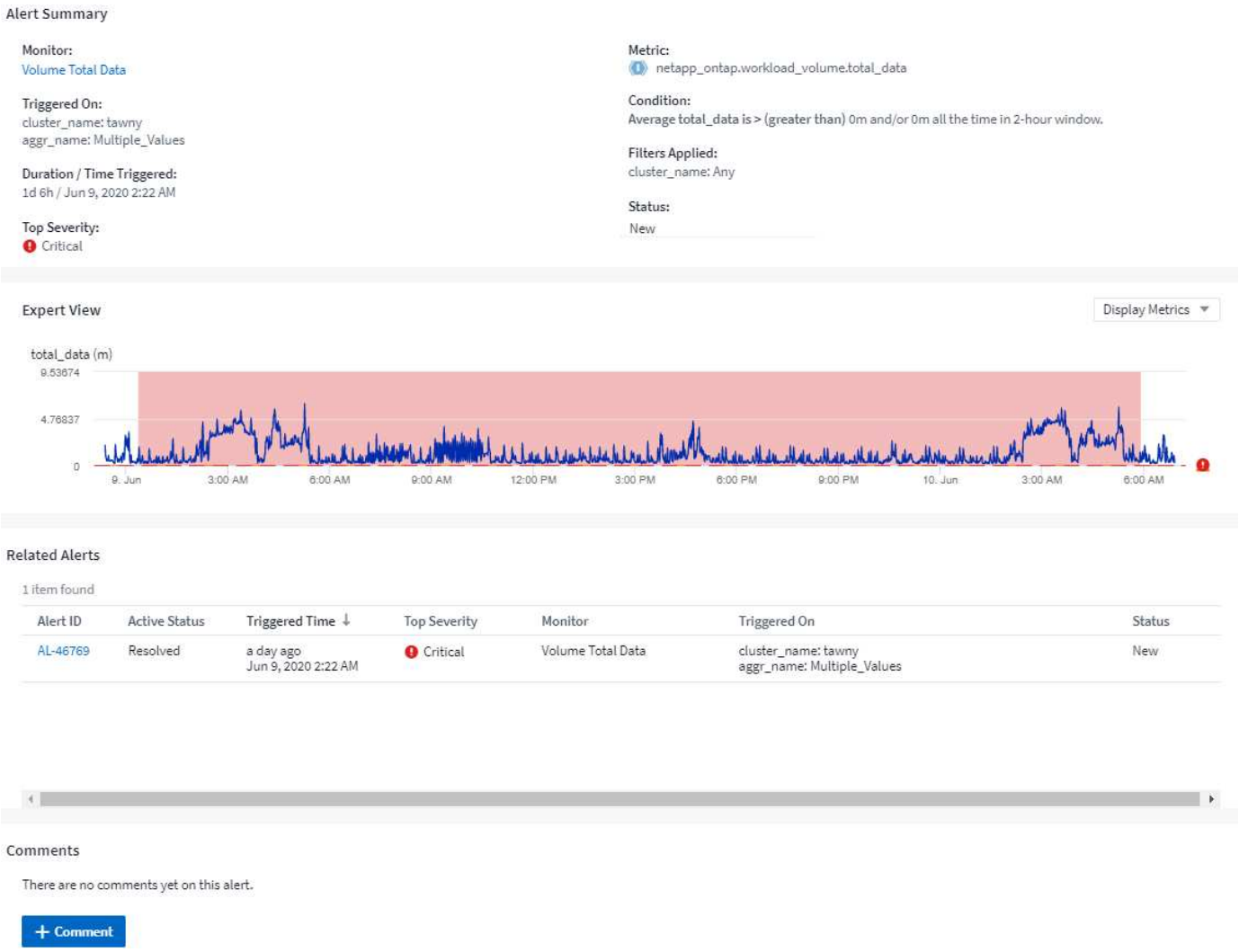
- **In Bearbeitung** um anzuzeigen, dass der Alarm untersucht wird oder anderweitig offen gehalten werden muss
- **Abweisen**, um die Warnung aus der Liste der aktiven Warnungen zu entfernen.

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.

Seite Mit Den Alarmdetails

Die Seite mit den Details für Warnmeldungen enthält weitere Details zu der Warnmeldung, darunter eine *Zusammenfassung*, eine *Expert View* mit Diagrammen zu den Objektdaten, beliebige *zugehörige Assets* und *Kommentare*, die von den Alarmforschern eingegeben wurden.



Benachrichtigt, Wenn Daten Fehlen

In einem Echtzeit-System wie Cloud Insights, um die Analyse eines Monitors anzustoßen, um zu entscheiden, ob ein Alarm generiert werden soll, verlassen wir uns 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 langsamer Datenankunft oder keiner Datenzukunft muss der Timer-Mechanismus übernehmen, da die Dateneineinzugsrate nicht ausreicht, um Alarme in „Echtzeit“ auszulösen. So wird die Frage gewöhnlich: „Wie lange warte ich, bevor ich das Analysenfenster schließe und mir die habe?“ Wenn Sie zu lange warten, dann 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

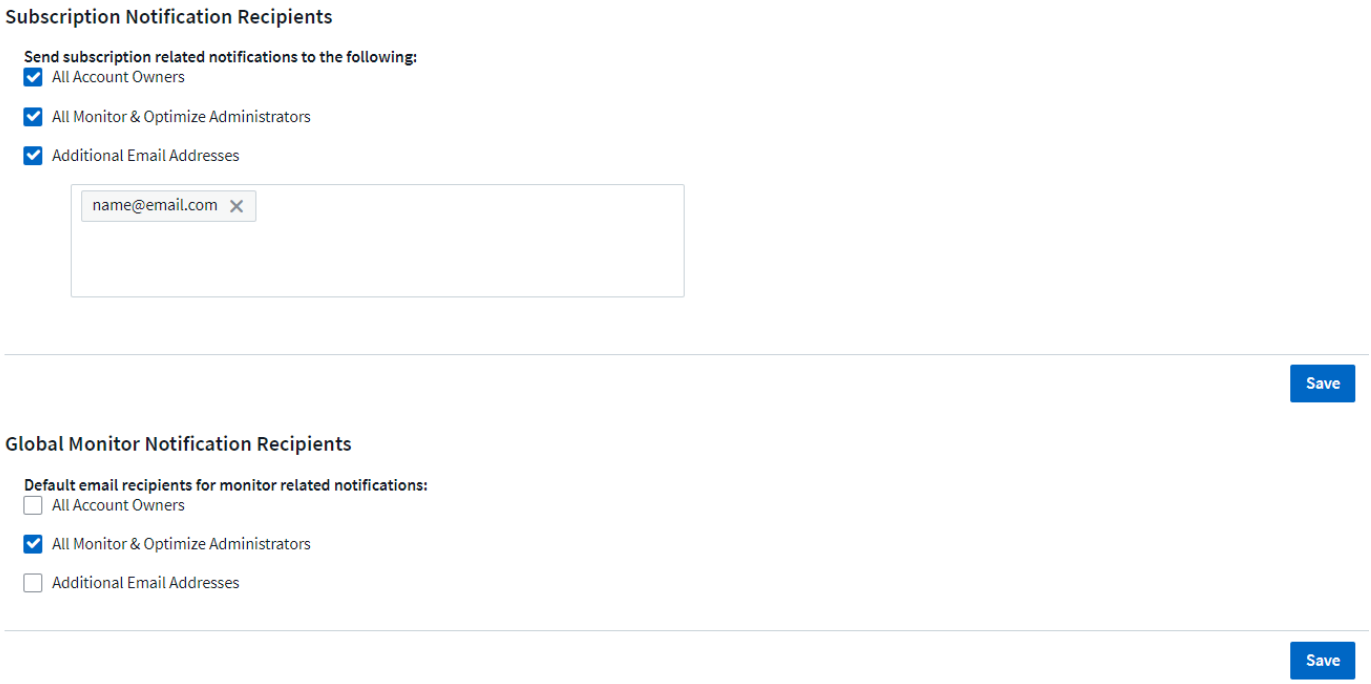
bleiben. Dies kann zu Problemen mit der Systemspannung und Stabilität im Laufe der Zeit führen.

Um dies zu verhindern, schließt Cloud Insights automatisch alle „dauerhaft aktiven“ Warnungen 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	Überprüfen Sie die Abonnementdetails auf der "Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab das Abonnement läuft in 30 Tagen ab	Keine Aktion erforderlich, wenn „Auto Renewal“ aktiviert ist Kontakt "NetApp Vertrieb" Um das Abonnement zu verlängern
Die Testversion endet in 2 Tagen	Verlängern Sie die Testversion vom "Abonnement" Seite. Sie können eine einmalige Testversion erneuern. Kontakt "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	Kontakt "NetApp Vertrieb" Um ein Abonnement zu erwerben

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.

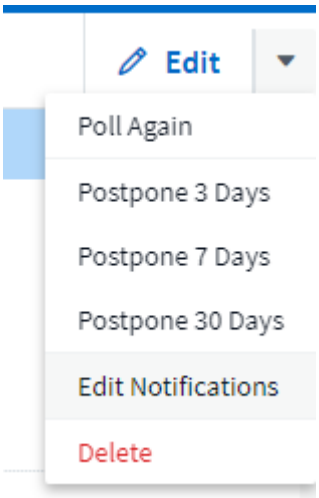
Wählen Sie zum Konfigurieren von Empfängern für globale Warnmeldungen die gewünschten Empfänger im Abschnitt **Empfänger für globale Monitorbenachrichtigungen** aus.

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.

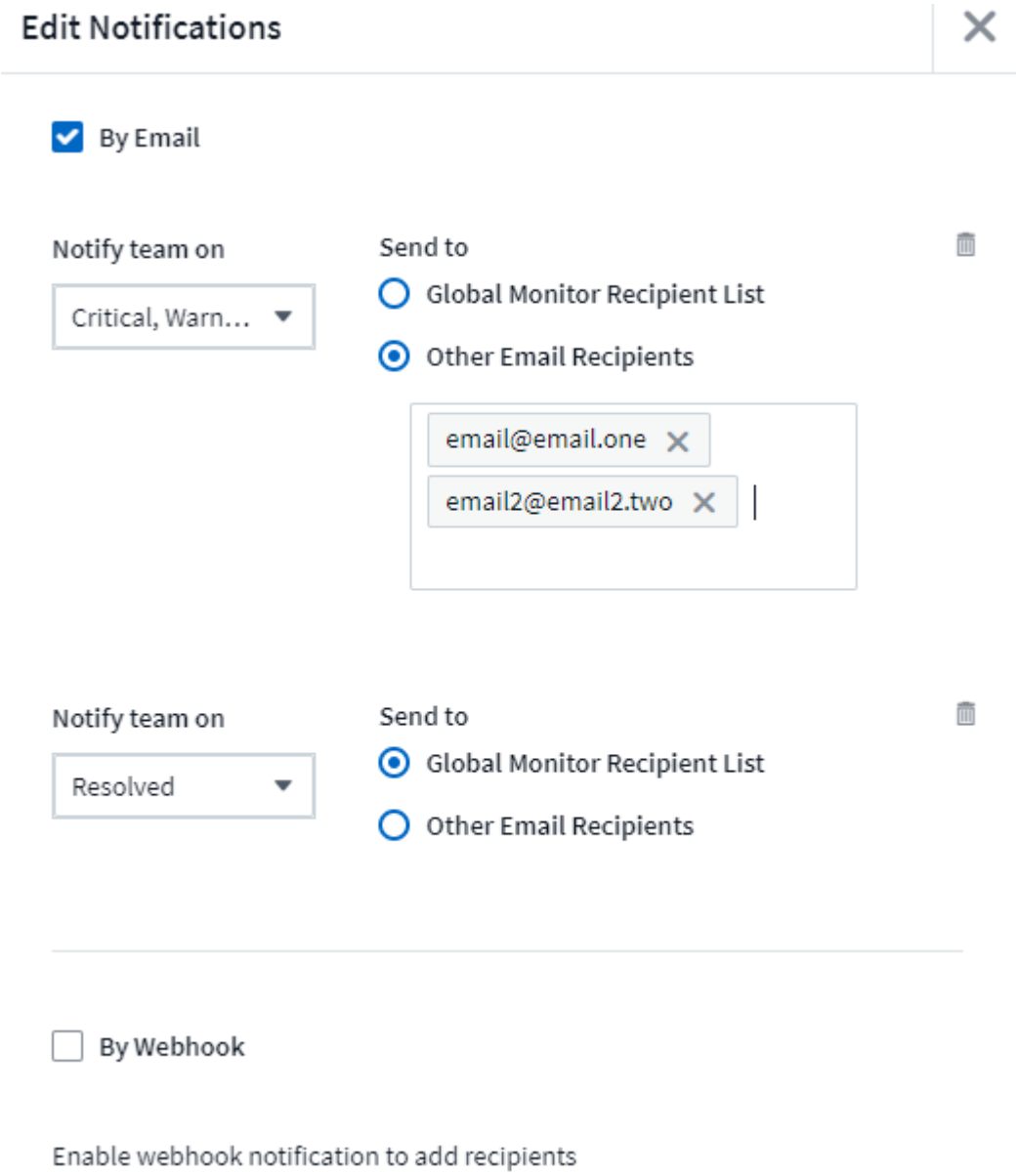
Bearbeiten von Benachrichtigungen für ONTAP

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

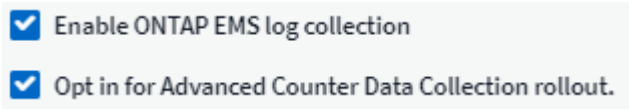
Warnmeldungen festlegen. Jedes Szenario kann die Liste der globalen Empfänger oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Systemmonitore

Cloud Insights umfasst eine Reihe von systemdefinierten Monitoren für Kennzahlen und Protokolle. Die verfügbaren Systemmonitore sind abhängig von den Datensammlern in Ihrer Umgebung. Aus diesem Grund können sich die in Cloud 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*:



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.

Nachfolgend sind die derzeit in Cloud Insights enthaltenen Systemmonitore aufgeführt:

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 nur auf wesentliche Arbeit, entweder über QoS-Richtlinien in ONTAP oder Host-seitige Konfiguration, um die Auslastung der FCP-Ports zu erleichtern.… Falls der Warnschwellenwert nicht erreicht wird, folgende Maßnahmen ergreifen: 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 Verkehr bestimmter LUNs nur auf wesentliche Arbeit, entweder über QoS-Richtlinien in ONTAP oder Host-seitige 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	Falls der kritische Schwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen zur Minimierung der Serviceunterbrechung berücksichtigen: Wenn der LUN oder seinem Volume eine entsprechende QoS-Richtlinie zugeordnet ist, bewerten Sie dann seine Schwellenwerte und überprüfen Sie, ob der LUN-Workload gedrosselt wird.… Falls der Warnschwellenwert nicht erreicht wird, folgende Maßnahmen ergreifen: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn der Node auch eine hohe Auslastung verzeichnet, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den Gesamtarbeitsbedarf des Node. 3. Wenn das LUN oder sein Volume eine QoS-Richtlinie damit verknüpft ist, bewerten Sie seine Schwellenwerte und validieren Sie, ob sie den LUN-Workload gedrosselt werden.

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 genutzten 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 genutzten 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.	Falls ein kritischer Schwellenwert nicht erreicht wird, sollten sofortige Maßnahmen zur Minimierung der Service-Unterbrechung in Betracht gezogen werden: Wenn dem NVMe Namespace oder seinem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzwerte dann, falls der NVMe Namespace Workload gedrosselt wird.… Wenn der Warnschwellenwert nicht erreicht wird, folgende Maßnahmen ergreifen: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn der Node auch eine hohe Auslastung verzeichnet, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den Gesamtarbeitsbedarf des Node. 3. Wenn ihnen der NVMe Namespace oder dessen Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzschwellenwerte, falls 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 im Baum 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, um Platz im Volumen zu nutzen, 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 wichtigen Workloads sind und aus anderen Storage-Kopien wiederhergestellt werden können.……Wenn Warnschwellenwert nicht erreicht wird, planen Sie folgende unmittelbare Aktionen: 1. Verschieben Sie ein oder mehrere Volumes an einen anderen Storage-Speicherort. 2. Mehr Speicherkapazität hinzufügen. 3. Ändern Sie Einstellungen für die Speichereffizienz oder Tiering inaktiver Daten in den Cloud-Speicher.

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. Nicht kritische Workloads im Leerlauf.… Wenn der Warnschwellenwert nicht erreicht wird, ergreifen Sie sofort folgende 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 Platz beanspruchen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume Snapshot.…Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Aktionen: 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, wie es hilft, große Dateisysteme unterzubringen.… 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. Verwenden Sie FlexGroup, da es hilft, große Dateisysteme unterzubringen

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.	Falls ein kritischer Schwellenwert überschritten wird, sollten folgende unmittelbare Maßnahmen zur Minimierung der Service-Unterbrechung ergriffen werden: Falls dem Volume eine QoS-Richtlinie zugewiesen ist, sollten dessen Grenzwerte für den Fall bewertet werden, dass der 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 ihre Grenzwerte für den Fall, dass sie den Volume-Workload dazu bringen, gedrosselt zu werden. 3. Wenn auch der Node eine hohe Auslastung verzeichnet, verschieben Sie das Volume auf einen anderen Node oder reduzieren Sie den Gesamtarbeitslastpunkt 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 für Volumes der Storage-VM mit einer zugewiesenen QoS-Richtlinie die Schwellenwertgrenzen, 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 Anmeldeinformationen und Konnektivitätsinformationen 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.…Über prüfen 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.	**Sofortmaßnahmen** Wenn kritische Grenzwerte überschritten werden, sollten sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen in Betracht gezogen werden: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie seine Grenzwerte, falls der Volume-Workload gedrosselt wird. **Maßnahmen, Die Bald Zu Tun Sind** Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Wenn der Speicherpool auch eine hohe Auslastung hat, verschieben Sie das Volume in einen anderen Speicherpool. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten sie ihre Grenzwerte für den Fall, dass sie den Volume-Workload dazu bringen, gedrosselt zu werden. 3. Wenn der Controller auch eine hohe Auslastung aufweist, verschieben Sie das Volume auf einen anderen Controller oder verringern Sie die Gesamtlast 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 in Ihrer Umgebung 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 in Ihrer Umgebung ausgerichtet werden.	**Sofortmaßnahmen** Wenn kritische Grenzwerte nicht eingehalten werden, sollten sofortige Maßnahmen geplant werden, um die Serviceunterbrechung zu minimieren: 1. Einführung QoS MBPS Grenzen für das Volume. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Volumen für Anomalien. **Maßnahmen, Die Bald Zu Tun Sind** Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Einführung QoS MBPS Grenzen für das Volume. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Volumen für 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 in Ihrer Umgebung 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.	**Sofortmaßnahmen** Wenn der kritische Schwellenwert überschritten wird, planen Sie sofortige Maßnahmen ein, um die Serviceunterbrechung zu minimieren: 1. Einführen von QoS-IOPS-Limits für das Volume 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Volumen für Anomalien. **Maßnahmen, Die Bald Zu Tun Sind** Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Einführen von QoS-IOPS-Limits für das Volume 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Volumen für 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	Die Cloud Insights Acquisition Units werden im Rahmen von Upgrades regelmäßig neu gestartet, um neue Funktionen einzuführen. Dies geschieht einmal pro Monat oder weniger in einer typischen Umgebung. Eine Warnung, dass eine Akquisitionseinheit kurz nach einer Resolution heruntergefahren wurde, die darauf hinweist, dass die neu neu neu gestartet wurde Akquisition mit Cloud Insights abgeschlossen ist. 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.	Besuchen Sie die Datensammlungsseite in Cloud Insights, um mehr über die Situation zu erfahren.
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, um Platz im Volumen zu nutzen, 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. Stellen Sie sicher, dass die physische Kabelverbindung sicher ist und funktioniert, und ersetzen Sie ggf. das Kabel. 3. Wenn der SAS-Adapter an die Platten-Shelves angeschlossen ist, stellen Sie sicher, dass die IOMs 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 die FC-VI-Verbindung nicht manipuliert wurde. 2. Überprüfen Sie, ob der physische Status des FC-VI-Adapters „up“ ist, indem Sie den Befehl „MetroCluster Interconnect Adapter show“ verwenden. 3. Wenn die Konfiguration umfasst Fabric Switches, 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"

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 allgemeinen, individuell anpassbaren Webhook-Kanals unterstützt Cloud Insights viele dieser Lieferkanäle. 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..

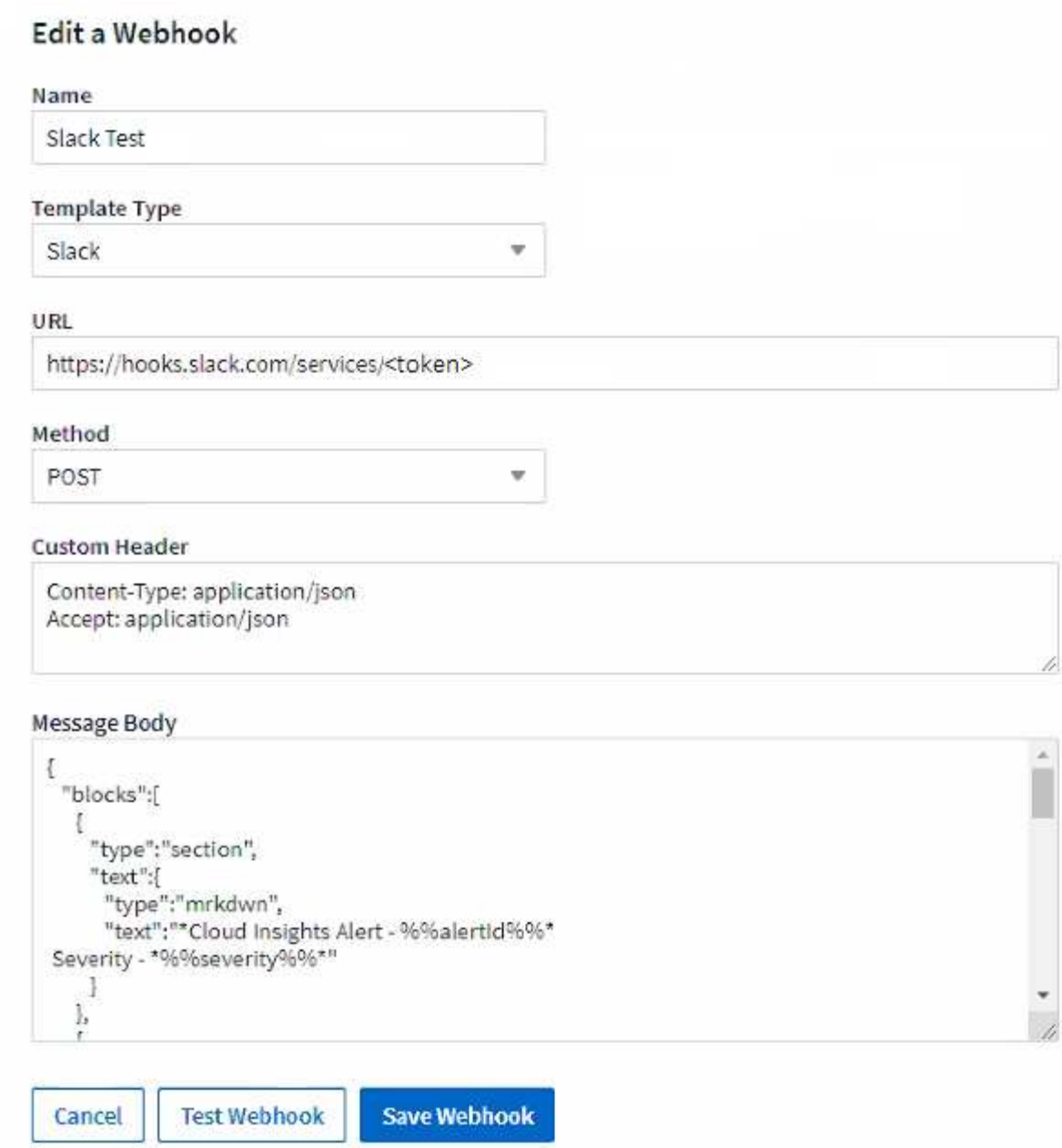
Die Instanz des Webhook-Kanals besteht aus folgenden Elementen:

Name	Eindeutiger Name
URL	Webhook-Ziel-URL, einschließlich dem 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 Cloud Insights Webhook zu erstellen, gehen Sie zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks**.

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.

Cloud Insights Webhooks enthalten 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.

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

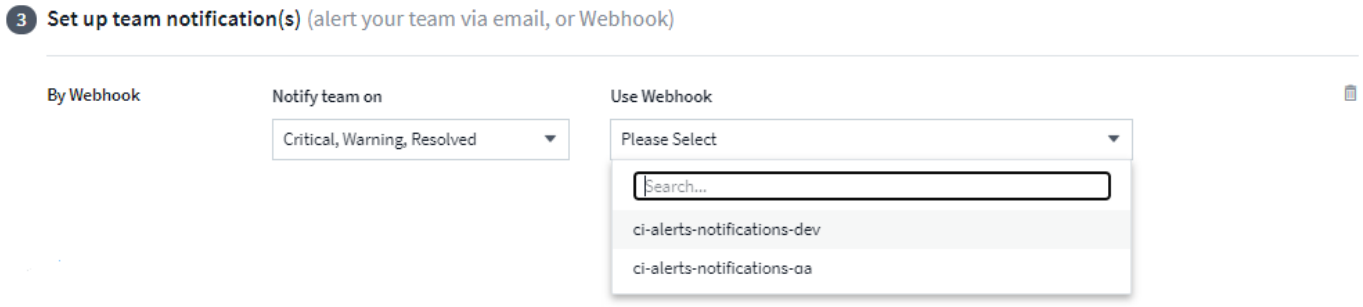
In diesem Abschnitt können Sie benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen, die Sie wünschen. Aus Sicherheitsgründen kann dieser Webhook-Kanal nur dann geändert werden, wenn ein Geheimnis definiert ist. Es ist schreibgeschützt für andere. Sie können Geheimnisse in URL/Headern als *%%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

So wählen Sie die Webhook-Benachrichtigung in a aus "Überwachen"Gehen Sie zu **Alerts > Monitor verwalten** und wählen Sie 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:

Webhaken für "Slack"Webhaken für "PagerDuty"Webhaken für "Teams Aus"Webhaken für "Abschnur"

Arbeiten mit Anmerkungen

Anmerkungen definieren

Wenn Sie Cloud Insights anpassen, um die Daten zur Nachverfolgung Ihrer Unternehmensanforderungen zu verfolgen, können Sie spezielle Notizen, die so genannten Anmerkungen, definieren und diese Ihrer Assets zuweisen.

Sie können Assets mit Informationen zum Ende des Lebenszyklus der Ressource, zum Datacenter, zum Standort, zum Storage-Tier oder zu einem Volume Service-Level Anmerkungen zuweisen.

Durch die Verwendung von Annotationen zum Monitoring Ihrer Umgebung werden die folgenden grundlegenden Aufgaben aufgeführt:

- Erstellen oder Bearbeiten von Definitionen für alle Anmerkungstypen.
- Anzeigen von Asset-Seiten und Verknüpfen jeder Anlage mit einer oder mehreren Anmerkungen.

  Wenn z. B. ein Asset geleast wird und der Mietvertrag innerhalb von zwei Monaten abläuft, können Sie

eine End-of-Life-Anmerkung auf das Asset anwenden. Dadurch wird verhindert, dass andere diese Ressource über einen längeren Zeitraum nutzen können.

- Erstellen von Regeln, um Anmerkungen automatisch auf mehrere Assets desselben Typs anzuwenden.
- Filtern Sie Assets nach ihren Anmerkungen.

Standard-Anmerkungstypen

Cloud Insights bietet einige Standard-Anmerkungstypen. Mit diesen Annotationen lassen sich Daten filtern oder gruppieren.

Sie können Assets mit Standardanmerkungstypen verknüpfen, z. B.:

- Lebenszyklus von Anlagen, z. B. Geburtstag, Sonnenuntergang oder Ende des Lebenszyklus
- Positionsinformationen zu einem Gerät wie z. B. Rechenzentren, Gebäude oder Etage
- Klassifizierung von Assets, z. B. nach Qualität (Tiers), nach angeschlossenen Geräten (Switch-Ebene) oder nach Service-Level
- Status, z. B. „heiß“ (hohe Auslastung)

In der folgenden Tabelle sind die von Cloud Insights bereitgestellten Anmerkungstypen aufgeführt.

Anmerkungstypen	Beschreibung	Typ
Alias	Benutzerfreundlicher Name für eine Ressource	Text
Rechnerressourcengruppe	Gruppenzuordnung, die vom Datensammler der Host- und VM-Dateisysteme verwendet wird	Liste
Rechenzentrum	Physischer Standort	Liste
Heiß	Geräte, die regelmäßig oder an der Kapazitätsgrenze unter hohem Verbrauch stehen	Boolesch
Hinweis	Kommentare, die einer Ressource zugeordnet sind	Test
Service-Level	Eine Reihe unterstützter Service-Level, die Sie Ressourcen zuweisen können. Zeigt eine Liste mit bestellten Optionen für interne Volumes, qtree und Volumes an. Bearbeiten Sie Service Levels, um Performance-Richtlinien für unterschiedliche Level festzulegen.	Liste
Sonnenuntergang	Schwellenwert, nach dem keine neuen Zuordnungen an das Gerät vorgenommen werden können. Nützlich für geplante Migrationen und andere ausstehende Netzwerkänderungen.	Datum
Switch-Ebene	Vordefinierte Optionen zum Einrichten von Kategorien für Schalter. In der Regel bleiben diese Bezeichnungen für die Lebensdauer des Geräts, Sie können sie jedoch bearbeiten. Nur für Switches verfügbar.	Liste

Ebene	Sie können darüber hinaus verwendet werden, um in Ihrer Umgebung verschiedene Service Levels zu definieren. Tiers können den Typ des Levels definieren, z. B. die erforderliche Geschwindigkeit (z. B. Gold oder Silber). Diese Funktion ist nur für interne Volumes, qtrees, Storage Arrays, Storage-Pools und Volumes verfügbar.	Liste
Schweregrad Der Verletzung	Rangfolge (z. B. Major) eines Verstoßes (z. B. fehlende Host-Ports oder fehlende Redundanz) in einer Hierarchie von höchster bis niedrigster Bedeutung.	Liste

Alias, Datacenter, Heiß, Service-Level, Sonnenuntergang, Switch-Ebene, Stufe und Verstoß Schweregrad sind Anmerkungen auf Systemebene, die Sie nicht löschen oder umbenennen können. Sie können nur deren zugewiesenen Werte ändern.

Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. Cloud Insights bietet eine Reihe von Standardanmerkungen, doch können Sie herausfinden, dass Sie Daten auf andere Weise anzeigen möchten. Die Daten in benutzerdefinierten Annotationen ergänzen bereits erfassten Gerätedaten, wie z. B. Speicherhersteller, Anzahl Volumen und Leistungsstatistiken. Die Daten, die Sie mit Annotationen hinzufügen, werden von Cloud Insights nicht erkannt.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anmerkungen**.

   Auf der Seite Anmerkungen wird die Liste der Anmerkungen angezeigt.

2. Klicken Sie Auf **+Hinzufügen**
3. Geben Sie einen **Name** und eine **Beschreibung** der Anmerkung ein.

   Sie können in diese Felder bis zu 255 Zeichen eingeben.

4. Klicken Sie auf **Typ** und wählen Sie dann eine der folgenden Optionen aus, die den in dieser Anmerkung zulässigen Datentyp darstellt:

Anmerkungstypen

Boolesch

Erstellt eine Dropdown-Liste mit den Optionen „Ja“ und „Nein“ Beispielsweise ist die Beschriftung „Direct Attached“ Boolesch.

Datum

Dadurch wird ein Feld erstellt, das ein Datum enthält. Wenn es sich bei der Anmerkung um ein Datum handelt, wählen Sie diese Option aus.

Liste

Erstellt eine der folgenden Optionen:

- Eine feste Dropdown-Liste

  Wenn andere diesem Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste keine weiteren Werte hinzufügen.

- Eine Liste mit flexiblen Dropdown-Menüs

  Wenn Sie beim Erstellen dieser Liste die Option Neue Werte hinzufügen auswählen, wenn andere diesen Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste weitere Werte hinzufügen.

Nummer

Erstellt ein Feld, in dem der Benutzer, der die Anmerkung zuweist, eine Zahl eingeben kann. Wenn der Anmerkungstyp beispielsweise „Stockwerk“ lautet, kann der Benutzer den Wert „number“ auswählen und die Bodennummer eingeben.

Text

Erstellt ein Feld, das Freiformtext zulässt. Sie können z. B. „Sprache“ als Anmerkungstyp eingeben, „Text“ als Wertetyp auswählen und eine Sprache als Wert eingeben.

> Nachdem Sie den Typ festgelegt und Ihre Änderungen gespeichert haben, können Sie den Typ der Anmerkung nicht ändern. Wenn Sie den Typ ändern müssen, müssen Sie die Anmerkung löschen und eine neue erstellen.

1. Wenn Sie Liste als Anmerkungstyp auswählen, gehen Sie folgendermaßen vor:
   a. Wählen Sie **Neue Werte hinzufügen auf der Fly** aus, wenn Sie der Anmerkung weitere Werte hinzufügen möchten, wenn Sie auf einer Asset-Seite, die eine flexible Liste erstellt.

      Angenommen, Sie befinden sich auf einer Asset-Seite und das Asset hat die City-Anmerkung mit den Werten Detroit, Tampa und Boston. Wenn Sie die Option **Neue Werte hinzufügen auf der Fly** ausgewählt haben, können Sie City wie San Francisco und Chicago direkt auf der Asset-Seite zusätzliche Werte hinzufügen, anstatt zur Seite Anmerkungen zu gehen, um sie hinzuzufügen. Wenn Sie diese Option nicht wählen, können Sie beim Anwenden der Anmerkung keine neuen Anmerkungswerte hinzufügen; dadurch wird eine feste Liste erstellt.

   b. Geben Sie einen Wert und eine Beschreibung in die Felder **Wert** und **Beschreibung** ein.
   c. Klicken Sie auf **Add**, um weitere Werte hinzuzufügen.
   d. Klicken Sie auf das Papierkorb-Symbol, um einen Wert zu löschen.
2. Klicken Sie Auf **Speichern**

   Ihre Anmerkungen werden in der Liste auf der Seite Anmerkungen angezeigt.

Nachdem Sie fertig sind

In der UI steht die Beschriftung sofort zur Verwendung zur Verfügung.

Mit Anmerkungen

Sie erstellen Anmerkungen und weisen diese den zu überwachten Assets zu. Anmerkungen sind Notizen, die Informationen zu einer Ressource wie zum Beispiel physischen Standort, Ende der Nutzungsdauer, Storage-Tier oder Volume Service Level enthalten.

Anmerkungen definieren

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. Cloud Insights bietet zwar eine Reihe von

Standardanmerkungen, z. B. den Lebenszyklus von Ressourcen (Geburtstag oder Ende der Nutzungsdauer), den Standort des Gebäudes oder Datacenters und das Tier, doch können Sie auch feststellen, dass Sie Daten auf andere Weise anzeigen möchten.

Die Daten in benutzerdefinierten Annotationen ergänzen die bereits erfassten Gerätedaten wie Switch-Hersteller, Anzahl Ports und Leistungsstatistiken. Die Daten, die Sie mit Annotationen hinzufügen, werden von Cloud Insights nicht erkannt.

Bevor Sie beginnen

- Geben Sie die Terminologie an, der die Umgebungsdaten zugeordnet werden müssen.
- Geben Sie die Terminologie des Unternehmens an, der die Umgebungsdaten zugeordnet werden müssen.
- Geben Sie alle standardmäßigen Anmerkungstypen an, die Sie verwenden können.
- Ermitteln Sie, welche benutzerdefinierten Anmerkungen Sie erstellen müssen. Sie müssen die Anmerkung erstellen, bevor sie einem Asset zugewiesen werden kann.

Führen Sie die folgenden Schritte aus, um eine Anmerkung zu erstellen.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anmerkungen**
2. Klicken Sie auf **+ Anmerkung**, um eine neue Anmerkung zu erstellen.
3. Geben Sie einen Namen, eine Beschreibung und einen Typ für die neue Anmerkung ein.

   Geben Sie beispielsweise Folgendes ein, um eine Textbeschriftung zu erstellen, die den physischen Speicherort eines Assets in Data Center 4 definiert:

   - Geben Sie einen Namen für die Anmerkung ein, z. B. „Standort“.
   - Geben Sie eine Beschreibung der Beschreibung der Anmerkung ein, z. B. „physischer Standort ist Datacenter 4“.
   - Geben Sie den 'Typ' der Anmerkung ein, wie z. B. „Text“.

Manuelles Zuweisen von Anmerkungen zu Assets

Durch das Zuweisen von Annotationen zu Assets können Sie Assets auf eine für Ihr Unternehmen relevante Weise sortieren, gruppieren und protokollieren. Sie können Assets eines bestimmten Typs automatisch mithilfe von Anmerkungsregeln Anmerkungen zuweisen. Sie können jedoch einem einzelnen Asset über die entsprechende Asset-Seite Anmerkungen zuweisen.

Bevor Sie beginnen

- Sie müssen die Anmerkung erstellt haben, die Sie zuweisen möchten.

Schritte

1. Melden Sie sich in Ihrer Cloud Insights Umgebung an.
2. Suchen Sie das Element, auf das Sie die Anmerkung anwenden möchten.
   - Sie können Assets suchen, indem Sie eine Abfrage durchführen, aus einem Dassoard-Widget auswählen oder suchen. Wenn Sie die gewünschte Ressource gefunden haben, klicken Sie auf den Link, um die Landing Page der Ressource zu öffnen.
3. Klicken Sie auf der Seite Asset im Abschnitt Benutzerdaten auf **+ Anmerkung**.
4. Das Dialogfeld Anmerkung hinzufügen wird angezeigt.

5. Wählen Sie eine Anmerkung aus der Liste aus.
6. Klicken Sie auf „Wert“ und führen Sie eine der folgenden Aktionen aus, je nachdem, welche Anmerkungstypen Sie ausgewählt haben:
   - Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   - Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
7. Klicken Sie Auf **Speichern**.

Wenn Sie den Wert der Anmerkung nach der Zuweisung ändern möchten, klicken Sie auf das Anmerkungsfeld, und wählen Sie einen anderen Wert aus. Wenn die Anmerkung vom Listentyp ist, für den die Option *neue Werte hinzufügen auf der Fly* ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

Anmerkungen mit Anmerkungsregeln zuweisen

Um Assets anhand von Kriterien, die Sie definieren, automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerkungsregeln. Cloud Insights weist anhand dieser Regeln Anmerkungen zu Assets zu. Cloud Insights bietet zudem zwei Standard-Anmerkungsregeln, die Sie je nach Bedarf ändern können oder entfernen können, wenn Sie sie nicht verwenden möchten.

Anmerkungsregeln werden erstellt

Alternativ zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Wenn Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Über diese Aufgabe

Sie können zwar die Anmerkungstypen bearbeiten, während Sie die Regeln erstellen, aber Sie sollten die Typen bereits im Voraus definiert haben.

Schritte

1. Klicken Sie auf **Verwalten > Anmerkungsregeln**

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

2. Klicken Sie Auf **+ Hinzufügen**.
3. Gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Dieser Name wird auf der Seite Anmerkungsregeln angezeigt.

   b. Klicken Sie auf **Query** und wählen Sie die Abfrage aus, mit der die Anmerkung auf Assets angewendet wird.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Beschriftung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise als Anmerkung Geburtstag auswählen, geben Sie ein Datum für den Wert an.

e. Klicken Sie Auf **Speichern**

f. Klicken Sie auf **Alle Regeln**, wenn Sie alle Regeln sofort ausführen möchten; andernfalls werden die Regeln in einem regelmäßigen geplanten Intervall ausgeführt.

Anmerkungsregeln werden erstellt

Mit Anmerkungsregeln können Sie Anmerkungen automatisch auf mehrere Assets anwenden, die auf den von Ihnen definierten Kriterien basieren. Cloud Insights weist anhand dieser Regeln Anmerkungen zu Assets zu. Wenn Cloud Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anmerkungsregeln**.
2. Klicken Sie auf **+ Regel**, um eine neue Anmerkungsregel hinzuzufügen.

   Das Dialogfeld Regel hinzufügen wird angezeigt.

3. Gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Der Name wird auf der Seite Anmerkungsregeln angezeigt.

   b. Klicken Sie auf **Query** und wählen Sie die Abfrage aus, die Cloud Insights verwendet, um die Assets zu identifizieren, für die die Anmerkung gilt.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Beschriftung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise als Anmerkung Geburtstag auswählen, geben Sie ein Datum für den Wert an.

   e. Klicken Sie Auf **Speichern**
   f. Klicken Sie auf **Alle Regeln**, wenn Sie alle Regeln sofort ausführen möchten; andernfalls werden die Regeln in einem regelmäßigen geplanten Intervall ausgeführt.

> In einer großen Cloud Insights-Umgebung fällt möglicherweise auf, dass das Ausführen von Anmerkungsregeln etwas Zeit in Anspruch nehmen scheint. Dies liegt daran, dass der Indexer zuerst ausgeführt wird und vor der Ausführung der Regeln abgeschlossen werden muss. Mit dem Indexer kann Cloud Insights nach neuen oder aktualisierten Objekten und Zählern in Ihren Daten suchen oder filtern. Die Regel-Engine wartet, bis der Indexer seine Aktualisierung abgeschlossen hat, bevor die Regeln angewendet werden.

Anmerkungsregeln ändern

Sie können eine Anmerkungsregel ändern, um den Namen der Regel, ihre Anmerkung, den Wert der Anmerkung oder die mit der Regel verknüpfte Abfrage zu ändern.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

2. Suchen Sie die Anmerkungsregel, die Sie ändern möchten.

   Sie können die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerkungsregeln nach Seite zu durchsuchen.

3. Klicken Sie auf das Menüsymbol für die Regel, die Sie ändern möchten.
4. Klicken Sie Auf **Bearbeiten**

   Das Dialogfeld Regel bearbeiten wird angezeigt.

5. Ändern Sie den Namen, die Anmerkungen, den Wert oder die Abfrage der Anmerkungsregel.

Die Reihenfolge der Regeln ändern

Anmerkungsregeln werden von oben in der Regelliste bis unten verarbeitet. Um die Reihenfolge zu ändern, in der eine Regel verarbeitet wird, gehen Sie wie folgt vor:

Schritte

1. Klicken Sie auf das Menüsymbol für die Regel, die Sie verschieben möchten.
2. Klicken Sie nach Bedarf auf **nach oben** oder **nach unten bewegen**, bis die Regel an dem gewünschten Ort angezeigt wird.

Beachten Sie, dass beim Ausführen mehrerer Regeln, die dieselbe Anmerkung für ein Asset aktualisieren, die erste Regel (wie von oben nach unten ausgeführt) die Anmerkung anwendet und das Asset aktualisiert, dann gilt die zweite Regel, ändert aber keine Beschriftung, die bereits durch die vorherige Regel festgelegt wurde.

Anmerkungsregeln werden gelöscht

Möglicherweise möchten Sie Anmerkungsregeln löschen, die nicht mehr verwendet werden.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

2. Suchen Sie die Anmerkungsregel, die gelöscht werden soll.

   Sie können die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerkungsregeln nach Seite zu durchsuchen.

3. Klicken Sie auf das Menüsymbol für die Regel, die Sie löschen möchten.
4. Klicken Sie Auf **Löschen**

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Regel löschen möchten.

5. Klicken Sie auf **OK**

Anmerkungen Werden Importiert

Cloud Insights enthält eine API zum Importieren von Anmerkungen oder Applikationen aus einer CSV-Datei und Zuweisen zu Objekten, die Sie angeben.

> Die Cloud Insights API ist in **Cloud Insights Premium Edition** erhältlich.

Importieren

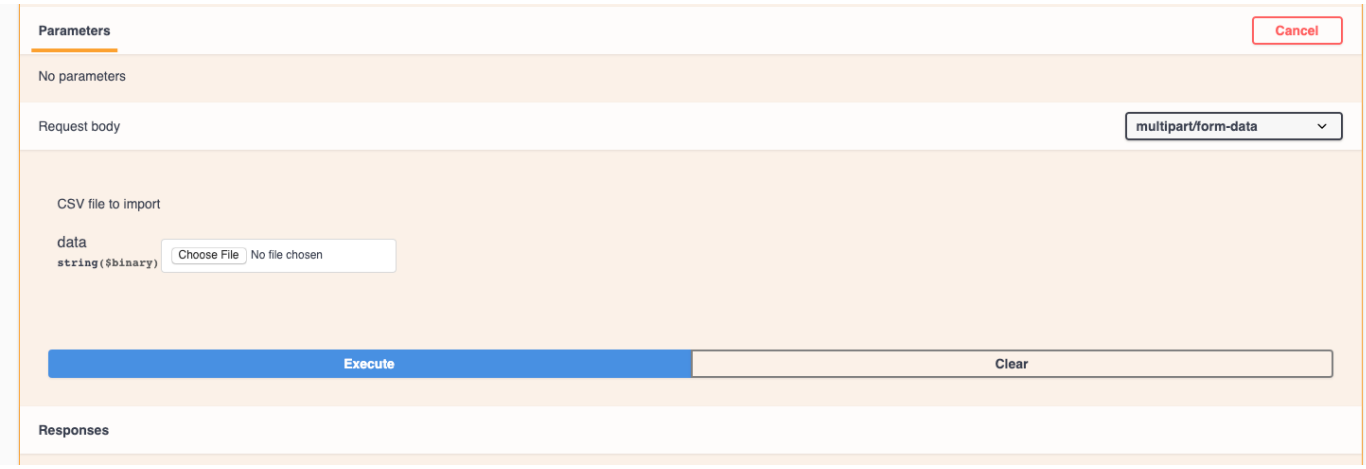
Die Links **Admin > API Access** enthalten "Dokumentation" Für die API **Assets/Import**. Diese Dokumentation enthält Informationen zum CSV-Dateiformat.

.CSV-Dateiformat

Das allgemeine Format der CSV-Datei ist wie folgt. Die erste Zeile der Datei definiert die Importfelder und gibt die Reihenfolge der Felder an. Danach folgen separate Zeilen für jede Anmerkung oder Anwendung. Sie müssen nicht jedes Feld definieren. Die nachfolgenden Anmerkungszeilen müssen jedoch der Reihenfolge der Definitionszeile entsprechen.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
In der API-Dokumentation finden Sie Beispiele für CSV-Dateien.
```

Sie können Anmerkungen aus einer .CSV-Datei innerhalb des API-Swagger selbst importieren und zuweisen. Wählen Sie einfach die zu verwendende Datei aus und klicken Sie auf die Schaltfläche *Execute*:



Importverhalten

Während des Importvorgangs werden je nach importierten Objekten und Objekttypen Daten hinzugefügt, zusammengeführt oder ersetzt. Beim Importieren sollten Sie die folgenden Verhaltensweisen beachten.

- Fügt eine Anmerkung oder Anwendung hinzu, wenn keine mit demselben Namen im Zielsystem vorhanden ist.
- Fügt eine Anmerkung zusammen, wenn der Anmerkungstyp eine Liste ist, und eine Anmerkung mit dem gleichen Namen existiert im Zielsystem.
- Ersetzt eine Anmerkung, wenn der Anmerkungstyp eine andere als eine Liste ist und eine Anmerkung mit dem gleichen Namen im Zielsystem vorhanden ist.

  Hinweis: Wenn im Zielsystem eine Anmerkung mit demselben Namen, aber mit einem anderen Typ vorhanden ist, schlägt der Import fehl. Wenn Objekte von der fehlgeschlagenen Annotation abhängen, können diese Objekte falsche oder unerwünschte Informationen anzeigen. Nach Abschluss des Importvorgangs müssen alle Anmerkungsabhängigkeiten geprüft werden.

- Wenn ein Anmerkungswert leer ist, wird diese Anmerkung aus dem Objekt entfernt. Übernommene Anmerkungen sind nicht betroffen.
- Anmerkungswerte für Datumstypen müssen als unix-Zeit in Millisekunden eingegeben werden.
- Beim Kommentieren von Volumes oder internen Volumes ist der Objektname eine Kombination aus Storage-Name und Volume-Name mithilfe des Trennzeichens „->“. Beispiel: *<Storage-Name>-><Volume-Name>*
- Wenn ein Objektname ein Komma enthält, muss der gesamte Name in doppelten Anführungszeichen sein. Beispiel: *„NetApp1,NetApp2“->023F*
- Beim Anfügen von Anmerkungen zu Speicher, Switches und Ports wird die Spalte „Anwendung“ ignoriert.
- Mandant, Line_of_Business, Business_Unit und/oder Projekt macht eine Geschäftseinheit. Wie bei allen Geschäftseinheiten können alle Werte leer sein.

Die folgenden Objekttypen können mit Anmerkungen versehen werden.

OBJEKTTYP	NAME ODER TASTE
Host	id-><id>, <Name> oder <IP>
VM	id-><id> oder <Name>
Storage Pool	id-><id> oder <Storage Name>-><Storage Pool Name>
InternalVolume	id-><id> oder <Storage Name>-><Name des internen Volumes>
Datenmenge	id-><id> oder <Storage Name>-><Volume Name>
Storage	id-><id>, <Name> oder <IP>
Switch	id-><id>, <Name> oder <IP>
Port	id-><id> oder <WWN>
Qtree	id-><id> oder <Storage Name>-><Name des internen Volumes>-><Qtree Name>

Share	id-><id> oder <Storage Name>-><Name des internen Volumes>-><Name der Freigabe>-><Protokoll>[-><Qtree-Name (optional im Fall von qtree Standard)>]

Arbeiten mit Anwendungen

Nachverfolgung der Asset-Nutzung nach Applikation

Bevor Sie Daten zu den in Ihrer Umgebung ausgeführten Applikationen nachverfolgen können, müssen Sie zunächst diese Applikationen definieren und sie den entsprechenden Assets zuordnen. Applikationen können folgenden Assets zugewiesen werden: Hosts, virtuelle Maschinen, Volumes, interne Volumes, qtrees, Freigaben und Hypervisoren:

Dieses Thema enthält ein Beispiel für die Verfolgung der Verwendung virtueller Maschinen, die das Marketingteam für seine Exchange-E-Mail verwendet.

Möglicherweise möchten Sie eine Tabelle ähnlich der folgenden erstellen, um die in Ihrer Umgebung verwendeten Applikationen zu identifizieren und die Gruppe oder Geschäftseinheit mit den jeweiligen Applikationen zu notieren.

Mandant	Geschäftsbereich	Geschäftsbereich	Projekt	Applikationen Unterstützt
NetApp	Datenspeicher	Legal	Patente	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Datenspeicher	Marketing	Verkaufsveranstaltungen	Exchange, gemeinsam genutzte Oracle-Datenbank, BlastOff Event Planner

Diese Tabelle zeigt, dass das Marketing Team die Exchange-Applikation verwendet. Wir möchten die Auslastung ihrer Virtual Machines in Exchange nachverfolgen, damit wir vorhersagen können, wann wir mehr Storage hinzufügen müssen. Wir können die Exchange-Anwendung mit allen virtuellen Maschinen des Marketings verknüpfen:

1. Erstellen Sie eine Anwendung mit dem Namen *Exchange*
2. Gehen Sie zu **Abfragen > +Neue Abfrage**, um eine neue Abfrage für virtuelle Maschinen zu erstellen (oder wählen Sie ggf. eine vorhandene VM-Abfrage aus).

   Wenn die VMs des Marketingteams alle einen Namen haben, der den String „**mkt**“ enthält, erstellen Sie Ihre Anfrage, um den VM-Namen für „mkt“ zu filtern.

3. Wählen Sie die VMs aus.
4. Verknüpfen Sie die VMs mit der Anwendung *Exchange* unter Verwendung von **Massenaktionen > Anwendungen hinzufügen**.
5. Wählen Sie die gewünschte Anwendung aus und klicken Sie auf **Speichern**.
6. Wenn Sie fertig sind, **Speichern** die Abfrage.

Anwendungen Werden Erstellt

Um die Daten zu verfolgen, die mit bestimmten Applikationen verknüpft sind, die in Ihrer Umgebung ausgeführt werden, können Sie die Applikationen in Cloud Insights definieren.

Bevor Sie beginnen

Wenn Sie die Anwendung einer Geschäftseinheit zuordnen möchten, müssen Sie die Geschäftseinheit erstellen, bevor Sie die Anwendung definieren.

Über diese Aufgabe

Mit Cloud Insights können Sie Daten von Ressourcen, die zu Applikationen zugeordnet sind, aus z. B. zu Nutzungsdaten oder zur Kostenberichterstellung nachverfolgen.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Verwalten > Anwendungen**.

   Das Dialogfeld Anwendung hinzufügen wird angezeigt.

2. Geben Sie einen eindeutigen Namen für die Anwendung ein.
3. Wählen Sie eine Priorität für die Anwendung aus.
4. Klicken Sie Auf **Speichern**.

Nach dem Definieren einer Anwendung kann sie Assets zugewiesen werden.

Zuweisen von Anwendungen zu Assets

Diese Prozedur weist die Anwendung einem Host als Beispiel zu. Sie können einer Applikation Host, Virtual Machine, Volume oder interne Volumes zuweisen.

Schritte

1. Suchen Sie das Asset, dem Sie der Anwendung zuweisen möchten:
2. Klicken Sie auf **Abfragen > +Neue Abfrage** und suchen Sie nach Host.
3. Klicken Sie auf das Kontrollkästchen links neben dem Host, den Sie der Anwendung zuordnen möchten.
4. Klicken Sie Auf **Massenaktionen > Anwendung Hinzufügen**.
5. Wählen Sie die Anwendung aus, der Sie die Anlage zuweisen.

Neue Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem anderen Asset abgeleitet wurden. Beispielsweise übernehmen Volumes Applikationen von Hosts, und wenn neuen Applikationen einem Volume zugewiesen werden, hat die neue Applikation Vorrang vor der abgeleiteten Applikation.

> In Umgebungen mit großen Mengen verwandter Assets kann die Vererbung von Applikationszuweisungen an diese Ressourcen mehrere Minuten dauern. Bitte geben Sie mehr Zeit für Vererbung, wenn Sie viele verwandte Vermögenswerte haben.

Nachdem Sie fertig sind

Nachdem Sie den Host der Anwendung zugewiesen haben, können Sie die verbleibenden Assets der Anwendung zuweisen. Um auf die Landing Page für die Anwendung zuzugreifen, klicken Sie auf **Verwalten > Anwendung** und wählen Sie die von Ihnen erstellte Anwendung aus.

Automatische Geräteauflösung

Überblick Über Die Automatische Geräteauflösung

Sie müssen alle Geräte identifizieren, die Sie mit Cloud Insights überwachen möchten. Für die genaue Nachverfolgung der Performance und des Inventars in Ihrer Umgebung ist eine Identifizierung erforderlich. In der Regel werden die meisten in Ihrer Umgebung erkannten Geräte durch *Automatische Geräteauflösung* identifiziert.

Nachdem Sie Datensammler konfiguriert haben, werden Geräte in Ihrer Umgebung einschließlich Switches, Storage-Arrays und Ihre virtuelle Infrastruktur von Hypervisoren und VMs identifiziert. Dies erkennt jedoch normalerweise nicht 100 % der Geräte in Ihrer Umgebung.

Nachdem Geräte vom Typ Data Collector konfiguriert wurden, empfiehlt es sich, Regeln zur Geräterauflösungsregelung zu nutzen, um die verbleibenden unbekannten Geräte in Ihrer Umgebung zu identifizieren. Die Geräteauflösung kann Ihnen dabei helfen, unbekannte Geräte als die folgenden Gerätetypen zu lösen:

- Physische Hosts
- Storage-Arrays durchführt
- Bänder

Geräte, die nach der Geräteauflösung als nicht bekannt sind, gelten als allgemeine Geräte, die Sie auch in Abfragen und auf Dashboards anzeigen können.

Die wiederum erstellten Regeln identifizieren automatisch neue Geräte mit ähnlichen Attributen, wie sie Ihrer Umgebung hinzugefügt werden. In manchen Fällen ermöglicht die Geräteauflösung auch eine manuelle Identifizierung, bei der die Geräterauflösungsregeln für nicht erkannte Geräte innerhalb von Cloud Insights nicht beachtet werden.

Eine unvollständige Identifizierung von Geräten kann zu folgenden Problemen führen:

- Unvollständige Pfade
- Nicht identifizierte Multipath-Verbindungen
- Applikationen können nicht gruppieren
- Ungenaue Topologieansichten
- Ungenaue Daten im Data Warehouse und Berichterstellung

Die Geräteauflösungsfunktion (Verwalten > Geräteauflösung) umfasst die folgenden Registerkarten, von denen jede eine Rolle bei der Planung der Geräteauflösung und der Anzeige der Ergebnisse spielt:

- **Fibre Channel Identify** enthält eine Liste WWNs und Port-Informationen von Fibre Channel-Geräten, die nicht durch automatische Geräteauflösung aufgelöst wurden. Auf der Registerkarte wird außerdem der Prozentsatz der erkannten Geräte angegeben.
- **IP Address Identify** enthält eine Liste von Geräten, die auf CIFS-Freigaben und NFS-Freigaben zugreifen, die nicht durch automatische Geräteauflösung identifiziert wurden. Auf der Registerkarte wird außerdem der Prozentsatz der erkannten Geräte angegeben.
- **Regeln zur automatischen Auflösung** enthält die Liste der Regeln, die bei der Durchführung der Auflösung eines Fibre-Channel-Geräts ausgeführt werden. Dies sind Regeln, die Sie erstellen, um nicht identifizierte Fibre Channel-Geräte zu lösen.

- **Einstellungen** enthält Konfigurationsoptionen, mit denen Sie die Geräteauflösung für Ihre Umgebung anpassen können.

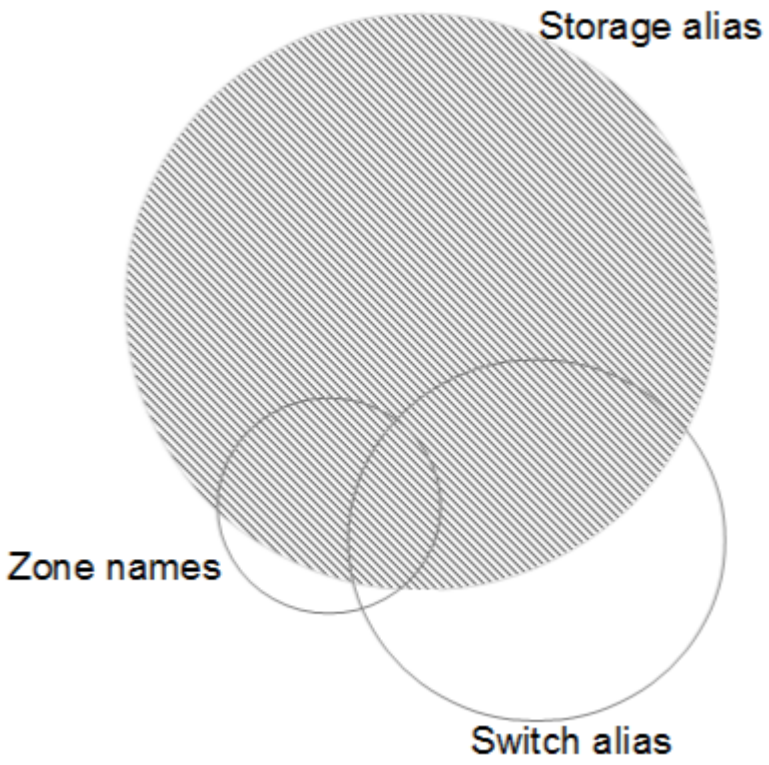
Bevor Sie Beginnen

Sie müssen wissen, wie Ihre Umgebung konfiguriert ist, bevor Sie die Regeln für die Identifizierung von Geräten definieren. Je mehr Sie über Ihre Umgebung wissen, desto einfacher ist es, Geräte zu identifizieren.

Sie müssen die folgenden Fragen beantworten, um genaue Regeln zu erstellen:

- Gibt es in Ihrer Umgebung Namensstandards für Zonen oder Hosts, und wie viel Prozent dieser Standards sind korrekt?
- Verwendet Ihre Umgebung einen Switch-Alias oder Storage-Alias und stimmt mit dem Host-Namen überein?
- Wie oft ändern sich Benennungsschemata in Ihrer Umgebung?
- Gab es Übernahmen oder Fusionen, bei denen verschiedene Benennungsschemata eingeführt wurden?

Nach der Analyse Ihrer Umgebung sollten Sie in der Lage sein, zu identifizieren, welche Benennungsstandards existieren, die Sie mit der Zuverlässigkeit rechnen können. Die gesammelten Informationen können grafisch in einer Abbildung dargestellt werden, die der folgenden ähnelt:



In diesem Beispiel wird die größte Anzahl von Geräten zuverlässig durch Speicheraliasen dargestellt. Regeln, die Hosts mit Speicheraliasen identifizieren, sollten zuerst geschrieben werden, Regeln mit Switch-Aliasen sollten als Nächstes geschrieben werden, und die letzten erstellten Regeln sollten Zonenaliasen verwenden. Aufgrund der Überlappung der Verwendung von Zonen-Aliasen und Switch-Aliasen können einige Speicher-Alias-Regeln zusätzliche Geräte identifizieren, so dass weniger Regeln für Zonen-Aliase und Switch-Aliase erforderlich sind.

Schritte zur Identifizierung von Geräten

In der Regel würden Sie einen Workflow verwenden, der dem folgenden ähnelt, um Geräte in Ihrer Umgebung zu identifizieren. Die Identifizierung ist ein iterativer Prozess und erfordert möglicherweise mehrere Schritte bei der Planung und Verfeinerung von Regeln.

- Forschungsumgebung
- Planregeln
- Regeln erstellen/überarbeiten
- Prüfen Sie die Ergebnisse
- Erstellen Sie zusätzliche Regeln oder identifizieren Sie Geräte manuell
- Fertig

> Wenn Sie in Ihrer Umgebung nicht identifizierte Geräte (sonst als unbekannte oder generische Geräte bekannt) haben und anschließend eine Datenquelle konfigurieren, die diese Geräte beim Abruf identifiziert, werden sie nicht mehr als generische Geräte angezeigt oder gezählt.

Verwandte Themen:"Geräterauflösungsregeln Werden Erstellt"
"Fibre Channel-Geräteauflösung"
"IP-Geräteauflösung"
"Einstellen Der Einstellungen Für Die Geräteauflösung"

Regeln zur Geräterauflösung

Sie erstellen Geräterauflösungsregeln, um Hosts, Storage und Tapes zu identifizieren, die derzeit nicht automatisch von Cloud Insights ermittelt werden. Die Regeln, die Sie erstellen, identifizieren Geräte, die sich derzeit in Ihrer Umgebung befinden, und identifizieren ähnliche Geräte, die Ihrer Umgebung hinzugefügt werden.

Geräterauflösungsregeln Werden Erstellt

Wenn Sie Regeln erstellen, müssen Sie zunächst die Informationsquelle identifizieren, auf die die Regel angewendet wird, die Methode, mit der Informationen extrahiert werden sollen, und ob DNS-Suche auf die Ergebnisse der Regel angewendet wird.

Quelle, mit der das Gerät identifiziert wird	* SRM Aliase für Hosts * Storage-Alias mit eingebettetem Host- oder Bandnamen * Switch-Alias, der einen eingebetteten Host- oder Bandnamen enthält * Zonennamen, die einen eingebetteten Hostnamen enthalten
Methode, die zum Extrahieren des Gerätenamens aus der Quelle verwendet wird	* AS (einen Namen aus einem SRM extrahieren) * Trennzeichen * reguläre Ausdrücke
DNS-Suche	Gibt an, ob Sie den Hostnamen mit DNS überprüfen

Sie erstellen Regeln auf der Registerkarte Regeln für die automatische Auflösung. Die folgenden Schritte beschreiben den Prozess zur Regelerstellung.

Verfahren

1. Klicken Sie Auf **Verwalten > Geräteauflösung**

2. Klicken Sie auf der Registerkarte **Regeln zur automatischen Auflösung** auf **+ Hostregel** oder **+ Bandregel**.

   Der Bildschirm **Auflösungsregel** wird angezeigt.

   > Klicken Sie auf den Link *Matching Criteria*, um Hilfe zu erhalten und Beispiele zum Erstellen von regulären Ausdrücken zu erhalten.

3. Wählen Sie in der Liste **Typ** das Gerät aus, das Sie identifizieren möchten.

   Sie können *Host* oder *Band* auswählen.

4. Wählen Sie in der Liste **Quelle** die Quelle aus, mit der Sie den Host identifizieren möchten.

   Je nach gewählter Quelle wird Cloud Insights die folgende Antwort angezeigt:

   a. **Zonen** listet die Zonen und WWN auf, die von Cloud Insights identifiziert werden müssen.
   b. **SRM** listet die nicht identifizierten Aliase auf, die von Cloud Insights identifiziert werden müssen
   c. **Storage Alias** listet Storage-Aliase und WWN auf, die von Cloud Insights identifiziert werden müssen
   d. **Alias wechseln** listet die Switch Aliase auf, die von Cloud Insights identifiziert werden müssen

5. Wählen Sie in der Liste **Methode** die Methode aus, die Sie verwenden möchten, um den Host zu identifizieren.

Quelle	Methode
SRM	Wie ist, Trennzeichen, reguläre Ausdrücke
Storage-Alias	Trennzeichen, reguläre Ausdrücke
Alias wechseln	Trennzeichen, reguläre Ausdrücke
Zonen	Trennzeichen, reguläre Ausdrücke

   - Für Regeln, die Trennzeichen verwenden, sind die Trennzeichen und die Mindestlänge des Hostnamens erforderlich. Die Mindestlänge des Host-Namens ist die Anzahl der Zeichen, die Cloud Insights zum Identifizieren eines Hosts verwenden sollte. Cloud Insights führt die DNS-Suche nur für Hostnamen durch, die so lange oder länger sind.

     Bei Regeln, die Trennzeichen verwenden, wird die Eingabeszeichenfolge durch das Trennzeichen getokenisiert, und eine Liste von Hostnamenkandidaten wird durch das Erstellen mehrerer Kombinationen des benachbarten Tokens erstellt. Die Liste wird dann sortiert, die größte bis die kleinste. Für einen Eingabeerring von *vipsnq03_hba3_emc3_12ep0* würde die Liste beispielsweise Folgendes ergeben:

     - Vipsnq03_hba3_emc3_12ep0
     - Vipsnq03_hba3_emc3
     - Hba3 emc3_12ep0
     - Vipsnq03_hba3
     - Emc3_12ep0
     - Hba3_emc3
     - Vipsnq03

        - 12ep0
        - Emc3
        - Hba3
    - Regeln, die reguläre Ausdrücke verwenden, erfordern einen regulären Ausdruck, das Format und die Empfindlichkeitsauswahl für Fälle.
6. Klicken Sie auf **Run AR**, um alle Regeln auszuführen, oder klicken Sie auf den Pfeil nach unten in der Schaltfläche, um die von Ihnen erstellte Regel (und alle anderen Regeln, die seit der letzten vollständigen Ausführung von AR erstellt wurden) auszuführen.

    Die Ergebnisse des Regellaufs werden auf der Registerkarte * FC Identify* angezeigt.

Starten einer automatischen Aktualisierung der Geräteauflösung

Ein Update zur Geräteauflösung setzt manuelle Änderungen fest, die seit der letzten vollständigen automatischen Gerätelaufauflösung hinzugefügt wurden. Das Ausführen eines Updates kann verwendet werden, um nur die neuen manuellen Einträge für die Konfiguration der Geräteauflösung zu übergeben und auszuführen. Es wird keine vollständige Gerätelaufauflösung durchgeführt.

Verfahren

1. Melden Sie sich in der Cloud Insights Web-UI an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Klicken Sie im Bildschirm **Geräteauflösung** auf den Pfeil nach unten in der Schaltfläche **Run AR**.
4. Klicken Sie auf **Aktualisieren**, um die Aktualisierung zu starten.

Regelgestützte manuelle Identifizierung

Diese Funktion wird für spezielle Fälle verwendet, in denen Sie eine bestimmte Regel oder eine Liste von Regeln (mit oder ohne einmalige Neuanordnung) ausführen möchten, um unbekannte Hosts, Speicher und Bandgeräte aufzulösen.

Bevor Sie beginnen

Sie verfügen über eine Reihe von Geräten, die nicht identifiziert wurden, und Sie haben auch mehrere Regeln, die andere Geräte erfolgreich identifiziert haben.

> Wenn Ihre Quelle nur einen Teil eines Host- oder Gerätenamens enthält, verwenden Sie eine Regel für reguläre Ausdrücke, und formatieren Sie sie, um den fehlenden Text hinzuzufügen.

Verfahren

1. Melden Sie sich in der Cloud Insights Web-UI an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte * Fibre Channel Identify*.

    Das System zeigt die Geräte zusammen mit ihrem Auflösungsstatus an.

4. Wählen Sie mehrere nicht identifizierte Geräte aus.
5. Klicken Sie auf **Massenaktionen** und wählen Sie **Hostauflösung festlegen** oder **Bandauflösung festlegen**.

Das System zeigt den Identify-Bildschirm an, der eine Liste aller Regeln enthält, die Geräte erfolgreich identifiziert haben.

6. Ändern Sie die Reihenfolge der Regeln in eine Bestellung, die Ihren Anforderungen entspricht.

   Die Reihenfolge der Regeln wird im Identify-Bildschirm geändert, aber nicht global geändert.

7. Wählen Sie die Methode aus, die Ihren Anforderungen entspricht.

Cloud Insights führt den Host-Auflösungsvorgang in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit den oben genannten.

Wenn geltende Regeln gefunden werden, werden in der Spalte Regeln Regelnamen angezeigt und als Handbuch identifiziert.

Verwandte Themen:"Fibre Channel-Geräteauflösung"
"IP-Geräteauflösung"
"Einstellen Der Einstellungen Für Die Geräteauflösung"

Fibre Channel-Geräteauflösung

Auf dem Bildschirm Fibre Channel Identify werden WWN und WWPN von Fibre Channel-Geräten angezeigt, deren Hosts nicht durch automatische Geräteauflösung identifiziert wurden. Auf dem Bildschirm werden auch alle Geräte angezeigt, die durch manuelle Geräteauflösung gelöst wurden.

Geräte, die durch manuelle Auflösung aufgelöst wurden, enthalten den Status *OK* und identifizieren die Regel, die zum Identifizieren des Geräts verwendet wird. Fehlende Geräte haben den Status *Unidentifiziert*. Geräte, die ausdrücklich von der Identifizierung ausgeschlossen sind, haben den Status *excluded*. Die Gesamtabdeckung für die Identifizierung von Geräten ist auf dieser Seite aufgeführt.

Sie führen Massenaktionen durch, indem Sie auf der linken Seite des Bildschirms Fibre Channel Identify mehrere Geräte auswählen. Aktionen können auf einem einzelnen Gerät ausgeführt werden, indem Sie den Mauszeiger über ein Gerät bewegen und die Schaltflächen *identifizieren* oder *Unidentifizieren* ganz rechts in der Liste auswählen.

Der Link „*Total Coverage*“ zeigt eine Liste der für Ihre Konfiguration verfügbaren Geräte an:

- SRM-Alias
- Storage-Alias
- Alias wechseln
- Zonen
- Benutzerdefiniert

Manuelles Hinzufügen eines Fibre-Channel-Geräts

Sie können Cloud Insights manuell ein Fibre Channel-Gerät hinzufügen, indem Sie die Funktion *Manual Add* verwenden, die auf der Registerkarte Fibre Channel Identify für Geräteauflösung verfügbar ist. Dieser Prozess kann für die Voridentifizierung eines Geräts verwendet werden, das in Zukunft entdeckt werden soll.

Bevor Sie beginnen

Zum erfolgreichen Hinzufügen einer Geräteidentifikation zum System müssen Sie die WWN- oder IP-Adresse

und den Gerätenamen kennen.

Über diese Aufgabe

Sie können Host, Speicher, Band oder Unbekanntes Fibre Channel-Gerät manuell hinzufügen.

Verfahren

1. Melden Sie sich in der Weboberfläche von Cloud Insights an
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte * Fibre Channel Identify*.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Dialogfeld **Gerät hinzufügen** wird angezeigt

5. Geben Sie die WWN- oder IP-Adresse, den Gerätenamen ein, und wählen Sie den Gerätetyp aus.

   Das Gerät, das Sie eingeben, wird der Geräteliste auf der Registerkarte Fibre Channel Identify hinzugefügt. Die Regel wird als *manuell* bezeichnet.

Importieren der Fibre-Channel-Gerätekennung aus einer CSV-Datei

Sie können die Identifikation von Fibre-Channel-Geräten mithilfe einer Geräteliste in einer CSV-Datei manuell in die Cloud Insights-Geräteauflösung importieren.

1. Bevor Sie beginnen

Sie benötigen eine korrekt formatierte CSV-Datei, um die Geräteidentifizierungen direkt in die Geräteauflösung importieren zu können. Die .CSV-Datei für Fibre Channel-Geräte erfordert folgende Informationen:

WWN	IP	Name	Typ

Die Datenfelder müssen in Anführungszeichen eingeschlossen werden, wie im folgenden Beispiel gezeigt.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

> Als Best Practice wird empfohlen, zunächst die Fibre Channel-Identify-Informationen in eine .CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in die Fibre Channel Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten in der richtigen Reihenfolge vorhanden sind.

Um Fibre Channel zu importieren, identifizieren Sie Informationen:

1. Melden Sie sich in der Cloud Insights Web-UI an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte * Fibre Channel Identify* aus.
4. Klicken Sie auf die Schaltfläche * Identifizieren > aus Datei identifizieren*.

5. Navigieren Sie zu dem Ordner, der Ihre .CSV-Dateien zum Importieren enthält, und wählen Sie die gewünschte Datei aus.

   Die von Ihnen eingegebenen Geräte werden der Geräteliste auf der Registerkarte Fibre Channel Identify hinzugefügt. Die „Regel“ wird als Handbuch bezeichnet.

Exportieren der Identifizierungen von Fibre Channel-Geräten in eine CSV-Datei

Sie können vorhandene Identifizierungen für Fibre Channel-Geräte von der Cloud Insights-Geräteauflösung in eine CSV-Datei exportieren. Sie können eine Geräteidentifikation exportieren, damit Sie sie ändern und dann wieder in Cloud Insights importieren können, wo sie dann verwendet wird, um Geräte zu identifizieren, die denen ähneln, die ursprünglich mit der exportierten Identifizierung übereinstimmen.

Über diese Aufgabe

Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die einfach in der .CSV-Datei bearbeitet und dann wieder in das System importiert werden können.

Wenn Sie eine Fibre-Channel-Gerätekennung in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

WWN	IP	Name	Typ

Verfahren

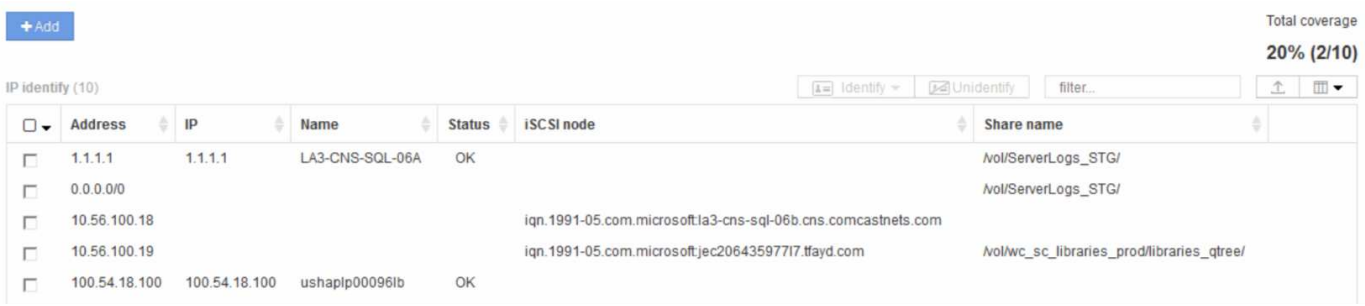
1. Melden Sie sich in der Cloud Insights Web-UI an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte * Fibre Channel Identify* aus.
4. Wählen Sie das Fibre-Channel-Gerät oder die Geräte aus, deren Kennung Sie exportieren möchten.
5. Klicken Sie auf die Option **Export** Schaltfläche.

   Wählen Sie aus, ob die .CSV-Datei geöffnet oder die Datei gespeichert werden soll.

Verwandte Themen:"IP-Geräteauflösung"
"Geräterauflösungsregeln Werden Erstellt"
"Einstellen Der Einstellungen Für Die Geräteauflösung"

IP-Geräteauflösung

Auf dem Bildschirm IP-Identifizierung werden alle iSCSI- und CIFS- oder NFS-Freigaben angezeigt, die durch die automatische Geräteauflösung oder durch manuelle Geräteauflösung identifiziert wurden. Auch nicht identifizierte Geräte werden angezeigt. Der Bildschirm enthält die IP-Adresse, den Namen, den Status, den iSCSI-Knoten und den Freigabenamen für Geräte. Der Prozentsatz der erfolgreich identifizierten Geräte wird ebenfalls angezeigt.



Manuelles Hinzufügen von IP-Geräten

Sie können Cloud Insights manuell ein IP-Gerät hinzufügen, indem Sie die im Bildschirm IP-Identifizierung verfügbare Funktion zum manuellen Hinzufügen verwenden.

Verfahren

1. Melden Sie sich in der Weboberfläche von Cloud Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte * IP-Adresse identifizieren*.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Dialogfeld Gerät hinzufügen wird angezeigt

5. Geben Sie die Adresse, die IP-Adresse und einen eindeutigen Gerätenamen ein.

Ergebnis

Das von Ihnen verwendete Gerät wird der Geräteliste auf der Registerkarte IP Address Identify hinzugefügt.

Importieren der IP-Geräteidentifizierung aus einer .CSV-Datei

Sie können die Identifikationen für IP-Geräte manuell über eine Liste der Geräteerkennungen in einer CSV-Datei in die Funktion „Geräteauflösung“ importieren.

1. Bevor Sie beginnen

Sie benötigen eine korrekt formatierte CSV-Datei, um die Geräteidentifizierungen direkt in die Funktion „Geräteauflösung“ importieren zu können. Die .CSV-Datei für IP-Geräte erfordert folgende Informationen:

Adresse	IP	Name

Die Datenfelder müssen in Anführungszeichen eingeschlossen werden, wie im folgenden Beispiel gezeigt.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

> Als Best Practice wird empfohlen, zunächst die IP-Adresse Identify-Informationen in eine .CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in die IP-Adresse Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten in der richtigen Reihenfolge vorhanden sind.

Exportieren der IP-Gerätekennung in eine CSV-Datei

Sie können vorhandene Identifizierungen für IP-Geräte von der Cloud Insights-Geräteauflösung in eine CSV-Datei exportieren. Sie können eine Geräteidentifikation exportieren, damit Sie sie ändern und dann wieder in Cloud Insights importieren können, wo sie dann verwendet wird, um Geräte zu identifizieren, die denen ähneln, die ursprünglich mit der exportierten Identifizierung übereinstimmen.

Über diese Aufgabe

1. Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die einfach in der .CSV-Datei bearbeitet und dann wieder in das System importiert werden können.

Wenn Sie eine IP-Geräte-ID in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

Adresse	IP	Name

Verfahren

1. Melden Sie sich in der Cloud Insights Web-UI an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte * IP Address Identify* aus.
4. Wählen Sie das IP-Gerät oder die Geräte aus, deren Kennung Sie exportieren möchten.
5. Klicken Sie auf die Option **Export** Schaltfläche.

   Wählen Sie aus, ob die .CSV-Datei geöffnet oder die Datei gespeichert werden soll.

Verwandte Themen:"Fibre Channel-Geräteauflösung"
"Geräterauflösungsregeln Werden Erstellt"
"Einstellen Der Einstellungen Für Die Geräteauflösung"

Einstellungen auf der Registerkarte Einstellungen

Auf der Registerkarte „Voreinstellungen für die Geräteauflösung“ können Sie einen Zeitplan für die automatische Auflösung erstellen, Speicher- und Bandanbieter angeben, die die Identifizierung einschließen oder ausschließen sollen, und DNS-Suchoptionen festlegen.

Zeitplan für die automatische Auflösung

Ein Zeitplan für die automatische Auflösung kann festlegen, wann die automatische Gerätelaufauflösung ausgeführt wird:

Option	Beschreibung

Alle	Verwenden Sie diese Option, um die automatische Geräteauflösung in Intervallen von Tagen, Stunden oder Minuten durchzuführen.
Jeden Tag	Verwenden Sie diese Option, um die automatische Geräteauflösung täglich zu einem bestimmten Zeitpunkt auszuführen.
Manuell	Verwenden Sie diese Option, um nur die automatische Geräteauflösung manuell auszuführen.
Bei jeder Umgebungsänderung	Verwenden Sie diese Option, um bei jeder Änderung der Umgebung eine automatische Geräteauflösung auszuführen.

Wenn Sie *manuell* angeben, wird die nächtliche automatische Geräteauflösung deaktiviert.

DNS-Verarbeitungsoptionen

Mit den DNS-Verarbeitungsoptionen können Sie die folgenden Funktionen auswählen:

- Wenn die Verarbeitung der DNS-Suchtresultat aktiviert ist, können Sie eine Liste von DNS-Namen hinzufügen, die an aufgelöste Geräte angehängt werden sollen.
- Sie können die Option Automatische Auflösung von IPs auswählen: Ermöglicht die automatische Hostauflösung für iSCSI-Initiatoren und Hosts, die über DNS-Lookup auf NFS-Freigaben zugreifen. Wenn dies nicht angegeben wird, wird nur FC-basierte Auflösung ausgeführt.
- Sie können Unterstriche in Hostnamen zulassen und anstelle des Standard-Port-Alias in Results einen Alias „Connected to“ verwenden.

Einschließlich oder mit Ausnahme bestimmter Storage- und Tape-Anbieter

Zur automatischen Lösung können Sie bestimmte Speicher- und Bandanbieter ein- oder ausschließen. Möglicherweise möchten Sie bestimmte Anbieter ausschließen, wenn Sie beispielsweise wissen, dass ein bestimmter Host zu einem veralteten Host wird und von Ihrer neuen Umgebung ausgeschlossen werden sollte. Sie können auch Anbieter, die Sie zuvor ausgeschlossen haben, erneut hinzufügen, möchten aber nicht mehr ausgeschlossen werden.

> Die Regeln zur Geräteauflösung für Bänder funktionieren nur für WWNs, bei denen der Hersteller für diesen WWN in den Anbietereinstellungen auf _nur als Band eingeschlossen eingestellt ist.

Siehe auch: "Beispiele Für Reguläre Ausdrücke"

Beispiele für reguläre Ausdrücke

Wenn Sie den regulären Ausdrucks-Ansatz als Ihre Ausgangs-Benennungsstrategie ausgewählt haben, können Sie die Beispiele für reguläre Ausdrücke als Leitfäden für Ihre eigenen Ausdrücke verwenden, die in den automatischen Auflösungsmethoden von Cloud Insights verwendet werden.

Formatieren von regulären Ausdrücken

Wenn Sie reguläre Ausdrücke für die automatische Auflösung von Cloud Insights erstellen, können Sie das Ausgabeformat konfigurieren, indem Sie Werte in ein Feld mit dem Namen *FORMAT* eingeben.

Die Standardeinstellung ist \1. Das bedeutet, dass ein Zonenname, der dem regulären Ausdruck entspricht, durch den Inhalt der ersten Variablen ersetzt wird, die durch den regulären Ausdruck erstellt wurde. In einem regelmäßigen Ausdruck werden variable Werte durch parteiliche Aussagen erzeugt. Wenn mehrere parenthetische Aussagen auftreten, werden die Variablen numerisch von links nach rechts referenziert. Die Variablen können in beliebiger Reihenfolge im Ausgabeformat verwendet werden. Konstanttext kann auch in die Ausgabe eingefügt werden, indem es dem FORMATFELD hinzugefügt wird.

Möglicherweise haben Sie beispielsweise die folgenden Zonennamen für diese Zonenbenennung:

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_Filer_FC1
* S14_Tampa_hostname2_Switch_FC4
* S3991_Boston_Hostname3_windows2K_FC0
* S44_Raleigh_Hostnamen 4_solaris_FC1
```

Möglicherweise soll die Ausgabe im folgenden Format vorliegen:

```
 [hostname]-[data center]-[device type]
Dazu müssen Sie die Felder Hostname, Rechenzentrum und Gerätetyp in
Variablen erfassen und in der Ausgabe verwenden. Der folgende reguläre
Ausdruck würde dies tun:
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Da es drei Gruppen von Klammern gibt, würden die Variablen \1, \2 und \3
ausgefüllt.
```

Sie können dann das folgende Format verwenden, um die Ausgabe in Ihrem bevorzugten Format zu empfangen:

```
 \2-\1-\3
Ihr Output wäre wie folgt:
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Die Bindestriche zwischen den Variablen liefern ein Beispiel für konstanten Text, der in die formatierte Ausgabe eingefügt wird.

Beispiele

Beispiel 1 mit Zonennamen

In diesem Beispiel verwenden Sie den regulären Ausdruck, um einen Hostnamen aus dem Zonennamen zu extrahieren. Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

Der reguläre Ausdruck, mit dem Sie den Hostnamen erfassen können, lautet:

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
Das Ergebnis ist eine Übereinstimmung aller Zonen, die mit S beginnen,
gefolgt von einer beliebigen Kombination von Ziffern, gefolgt von einem
Unterstrich, dem alphanumerischen Hostnamen (myComputer1Name), einem
Unterstrich oder Bindestrich, den Großbuchstaben HBA und einer einzelnen
Ziffer (0-9). Der Hostname allein ist in der Variablen *\1* gespeichert.
```

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- „S“ steht für den Zonennamen und beginnt den Ausdruck. Dies entspricht nur einem „S“ am Anfang des Zonennamens.
- Die Zeichen [0-9] in Klammern geben an, dass das folgende „S“ eine Ziffer zwischen 0 und 9, einschließlich sein muss.
- Das +-Zeichen gibt an, dass das Auftreten der Informationen in den vorhergehenden Klammern 1 oder mehr Mal bestehen muss.
- Der _ (Unterstrich) bedeutet, dass den Ziffern nach S sofort nur ein Unterstrich im Zonennamen folgen muss. In diesem Beispiel verwendet die Namenskonvention für die Zone den Unterstrich, um den Zonennamen vom Hostnamen zu trennen.
- Nach dem erforderlichen Unterstrich geben die Klammern an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Die in Klammern getierten Zeichen [A-ZA-Z0-9] geben an, dass es sich bei den Zeichen um alle Buchstaben (unabhängig von Groß- und Kleinschreibung) und Zahlen handelt.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die Klammern [_-] (Unterstrich und Strich) geben an, dass dem alphanumerischen Muster ein Unterstrich oder ein Strich folgen muss.
- Die Buchstaben HBA im regulären Ausdruck geben an, dass diese genaue Reihenfolge der Zeichen im Zonennamen erfolgen muss.
- Der letzte Satz mit Klammern [0-9] entspricht einer einstelligen Ziffer von 0 bis 9, inklusive.

Beispiel 2

überspringen Sie in diesem Beispiel den ersten Unterstrich "*", dann passen Sie E und alles danach bis zum zweiten "*"", und überspringen Sie danach alles.

ZONE: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

RegEXP: .**?*(E.*?)**.*?

Beispiel 3

Die Klammern "( )" um den letzten Abschnitt im regulären Ausdruck (unten) geben an, welcher Teil der Hostname ist. Wenn VSAN3 der Hostname sein soll, lautet dies: _([A-ZA-Z0-9]).*

ZONE: A_VSAN3_SR48KENT_A_CX2578_SPA0

Hostname: SR48KENT

RegExp: _[A-ZA-Z0-9]+_([A-ZA-Z0-9]).*

Beispiel 4 zeigt ein komplizierteren Benennungsmuster

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- MyComputerName123-HBA1_Symm1_FA3
- MyComputerName123-HBA2_Symm1_FA5
- MyComputerName123-HBA3_Symm1_FA7

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
 ([a-zA-Z0-9]*)_.*
Die Variable \1 enthält nach der Auswertung durch diesen Ausdruck nur
_myComputerName123_.
```

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Die Klammern [A-ZA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig vom Fall) oder jede Ziffer übereinstimmen wird.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Das Zeichen _ (Unterstrich) im regulären Ausdruck bedeutet, dass der Zonenname unmittelbar nach dem alphanumerischen String, der mit den vorangegangenen Klammern übereinstimmt, einen Unterstrich aufweisen muss.
- Der . (Periode) entspricht einem beliebigen Zeichen (ein Platzhalter).
- Das Sternchen * (Sternchen) zeigt an, dass der Platzhalter für den vorherigen Zeitraum 0 oder mehr Mal auftreten kann.

  Mit anderen Worten, die Kombination .* zeigt jedes Zeichen an, jede beliebige Anzahl von Zeiten.

Beispiel 5 zeigt Zonennamen ohne Muster an

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- MyComputerName_HBA1_Symm1_FA1
- MyComputerName123_HBA1_Symm1_FA1

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
 (.*?)_.*
Die Variable \1 enthält _MyComputerName_ (im Beispiel für den ersten
Zonennamen) oder _myComputerName123_ (im Beispiel für den zweiten
Zonennamen). Dieser reguläre Ausdruck würde somit alles vor dem ersten
Unterstrich entsprechen.
```

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die ? Charakter macht den Match nicht-gierig. Dies zwingt es, beim ersten Unterstrich nicht beim letzten zu stimmen.
- Die Zeichen _.* entsprechen dem ersten gefundenen Unterstrich und allen Zeichen, die ihm folgen.

Beispiel 6 zeigt Computernamen mit einem Muster an

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Da die Namenskonvention für die Zone mehr ein Muster hat, könnten wir den
obigen Ausdruck verwenden, der allen Instanzen eines Hostnamen
(MyComputerName im Beispiel) entspricht, der entweder mit Einer A, einem B
oder einem T endet und diesen Hostnamen in die \1-Variable setzt.
```

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.
- Die ? Charakter macht den Match nicht-gierig. Dies zwingt es, beim ersten Unterstrich nicht beim letzten zu stimmen.

- Das Unterstrich-Zeichen entspricht dem ersten Unterstrich im Zonennamen.
- Somit entspricht die erste Kombination .*?_ den Zeichen Storage1_ im Beispiel des ersten Zonennamens.
- Die zweite Kombination .*?_ verhält sich wie die erste, stimmt aber im Beispiel für den Namen der ersten Zone mit Switch1_ überein.
- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Die Klammern [A-ZA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig vom Fall) oder jede Ziffer übereinstimmen wird.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die Klammern im regulären Ausdruck [ABT] entsprechen einem einzelnen Zeichen im Zonennamen, das A, B oder T. sein muss
- Der _ (Unterstrich) nach den Klammern zeigt an, dass der [ABT]-Zeichenabgleiche einen Unterstrich nachgehen muss.
- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.

Das Ergebnis würde daher dazu führen, dass die Variable \1 alle alphanumerischen Zeichenfolgen enthält, die:

- Zuvor waren einige alphanumerische Zeichen und zwei Unterstriche
- Gefolgt von einem Unterstrich (und dann einer beliebigen Anzahl alphanumerischer Zeichen)
- Hatte vor dem dritten Unterstrich einen letzten Charakter von A, B oder T.

Beispiel 7

Zone: myComputerName123_HBA1_Symm1_FA1

Hostname: myComputerName123

RegExp: ([A-ZA-Z0-9]+)_.*

Beispiel 8

Dieses Beispiel findet alles vor dem ersten _.

Zone: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname: MyComputerName

Regexp: (.**?)_.**

Beispiel 9

Dieses Beispiel findet alles nach dem 1. _ Und bis zum zweiten _.

Zone: Z_MyComputerName_StorageName

Hostname: MyComputerName

RegEXP: .**?(.?)**.*?

Beispiel 10

Dieses Beispiel extrahiert „MyComputerName123“ aus den Zonenbeispielen.

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Hostname: MyComputerName123

RegExp: .**?.?**([A-ZA-Z0-9]+)**[ABT]_.**

Beispiel 11

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Hostname: MyComputerName123A

RegExp: .**?.?**([A-ZA-z0-9]+).*?

Beispiel 12

Die ^ (umgangen oder caret) **innen eckige Klammern** negiert den Ausdruck, zum Beispiel, [^FF] bedeutet alles außer Groß- oder Kleinbuchstaben F, und [^a-z] bedeutet alles außer Kleinbuchstaben a bis z, und im obigen Fall alles außer dem _. Die Formatanweisung fügt den Namen des Ausgabehosts in „-“ hinzu.

Zone: mhs_apps44_d_A_10a0_0429

Hostname: mhs-apps44-d

RegExp: ()_([ab]).*Format in Cloud Insights: \1-\2 ([^_])_ ()_([^_]).*Format in Cloud Insights: \1-\2-\3

Beispiel 13

In diesem Beispiel wird der Speicher-Alias durch "\" getrennt und der Ausdruck muss mit "\\" definieren, dass tatsächlich "\" in der Zeichenfolge verwendet wird und dass diese nicht Teil des Ausdrucks selbst sind.

Speicheralias: \Hosts\E2DOC01C1\E2DOC01N1

Hostname: E2DOC01N1

RegEXP: \\.**?\\.**?\\(.*?)

Beispiel 14

Dieses Beispiel extrahiert „PD-RV-W-AD-2“ aus den Zonenbeispielen.

ZONE: PD_D-PD-RV-W-AD-2_01

HOSTNAME: PD-RV-W-AD-2

RegExp: -(.*-\d).*

Beispiel 15

Die Formateinstellung in diesem Fall fügt dem Hostnamen die „US-BV-“ hinzu.

ZONE: SRV_USBVM11_F1

HOSTNAME: US-BV-M11

RegEXP: SRV_USBV([A-Za-z0-9]+)_F[12]

Format: US-BV-\1

Informationen Zur Asset-Seite

Übersicht Über Die Asset-Seite

Die Asset-Seiten fassen den aktuellen Status eines Assets zusammen und enthalten Links zu zusätzlichen Informationen über das Asset und die zugehörigen Assets.

Arten von Asset-Seiten

Cloud Insights bietet Asset-Seiten für die folgenden Materialien:

- Virtual Machine
- Storage Virtual Machine (SVM)
- Datenmenge
- Internes Volumen
- Host (einschließlich Hypervisor)
- Storage-Pool
- Storage
- Datenspeicher
- Applikation
- Storage-Node
- Qtree
- Festplatte
- VMDK
- Port
- Switch
- Fabric

Ändern des Zeitbereichs der angezeigten Daten

Standardmäßig werden auf einer Asset-Seite die letzten 24 Stunden an Daten angezeigt. Sie können jedoch das angezeigte Datensegment ändern, indem Sie einen anderen festen Zeitbereich oder einen benutzerdefinierten Zeitbereich auswählen, um immer weniger Daten anzuzeigen.

Sie können das Zeitsegment der angezeigten Daten ändern, indem Sie eine Option verwenden, die sich auf

jeder Asset-Seite befindet, unabhängig vom Asset-Typ. Um den Zeitbereich zu ändern, klicken Sie in der oberen Leiste auf den angezeigten Zeitbereich, und wählen Sie zwischen den folgenden Zeitsegmenten aus:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Die Letzten 2 Stunden
- Die letzten 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

Im benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinander folgende Tage auswählen. Sie können für diesen Bereich auch die Startzeit und die Endzeit des Tages festlegen. Die standardmäßige Startzeit ist 12:00 UHR am ersten ausgewählten Tag und die standardmäßige Endzeit ist am letzten ausgewählten Tag 11:59 Uhr. Wenn Sie auf Anwenden klicken, wird der benutzerdefinierte Zeitbereich auf die Asset-Seite angewendet.

Die Informationen in einer Zusammenfassung der Bestandsseite sowie in beliebigen Tabellen oder benutzerdefinierten Widgets auf der Seite werden automatisch basierend auf dem ausgewählten Zeitraum aktualisiert. Die aktuelle Aktualisierungsrate wird in der oberen rechten Ecke des Abschnitts Zusammenfassung sowie in allen relevanten Tabellen oder Widgets auf der Seite angezeigt.

Benutzerdefinierte Widgets Hinzufügen

Sie können Ihre eigenen Widgets zu jeder Asset-Seite hinzufügen. Widgets, die Sie hinzufügen, werden für alle Objekte dieses Typs auf den Asset-Seiten angezeigt. Wenn Sie beispielsweise ein benutzerdefiniertes Widget zu einer Speicherressource hinzufügen, wird dieses Widget auf den Asset-Seiten für alle Speicherressourcen angezeigt.

Filtern nach Objekten im Kontext

Wenn Sie ein Widget auf der Landing Page eines Assets konfigurieren, können Sie die Filter *in-Context* so einstellen, dass nur Objekte angezeigt werden, die direkt mit dem aktuellen Asset verknüpft sind. Wenn Sie ein Widget hinzufügen, werden standardmäßig *alle* Objekte des ausgewählten Typs in Ihrer Umgebung angezeigt. Mit in-Context-Filtern können Sie nur die Daten anzeigen, die für Ihre aktuelle Anlage relevant sind.

Auf den meisten Asset-Landing-Pages können Sie über Widgets nach Objekten filtern, die mit dem aktuellen Asset verknüpft sind. In den Dropdown-Menüs Filter werden Objekttypen angezeigt, die ein Verknüpfungssymbol anzeigen Kann im Kontext des aktuellen Assets gefiltert werden.

Beispielsweise können Sie auf einer Storage Asset-Seite ein Balkendiagramm-Widget hinzufügen, um die

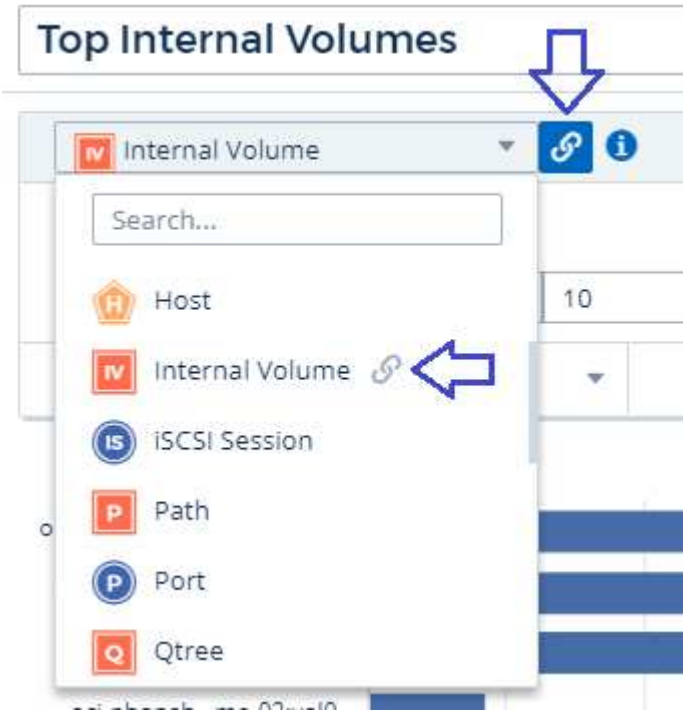
wichtigsten IOPS nur für interne Volumes auf diesem Storage anzuzeigen. Standardmäßig werden beim Hinzufügen eines Widgets *alle* interne Volumes in Ihrer Umgebung angezeigt.

So zeigen Sie nur interne Volumes der aktuellen Storage-Ressourcen an:

Schritte

1. Öffnen Sie eine Asset-Seite für jedes **Storage**-Asset.
2. Klicken Sie auf **Bearbeiten**, um die Asset-Seite im Bearbeitungsmodus zu öffnen.
3. Klicken Sie auf **Widget hinzufügen** und wählen Sie *Balkendiagramm*.
4. Wählen Sie **Internes Volumen** für den Objekttyp, der auf dem Balkendiagramm angezeigt werden soll.

   Beachten Sie, dass der Objekttyp des internen Volumes über ein Verknüpfungssymbol verfügt Daneben. Das Symbol „Verknüpfung“ ist standardmäßig aktiviert.



5. Wählen Sie „*IOPS – Total*“, und stellen Sie alle weiteren Filter ein, die Sie mögen.
6. Das Feld **Roll Up** können Sie ausblenden, indem Sie auf das [X] neben dem Feld klicken. Das Feld **Anzeigen** wird angezeigt.
7. Wählen Sie diese Option, um die Top 10 anzuzeigen.
8. Speichern Sie das Widget.

   Das Balkendiagramm zeigt nur die internen Volumes an, die sich auf der aktuellen Speicherressource befinden.

Das Widget wird auf den Asset-Seiten für alle Speicherobjekte angezeigt. Wenn der in-Context-Link im Widget aktiviert ist, zeigt das Balkendiagramm Daten für interne Volumes an, die sich nur auf die aktuell angezeigte Speicherressource beziehen.

Um die Verknüpfung der Objektdaten zu aufheben, bearbeiten Sie das Widget und klicken Sie auf das Link-Symbol Neben dem Objekttyp. Der Link wird deaktiviert Und das Diagramm zeigt Daten von *all*

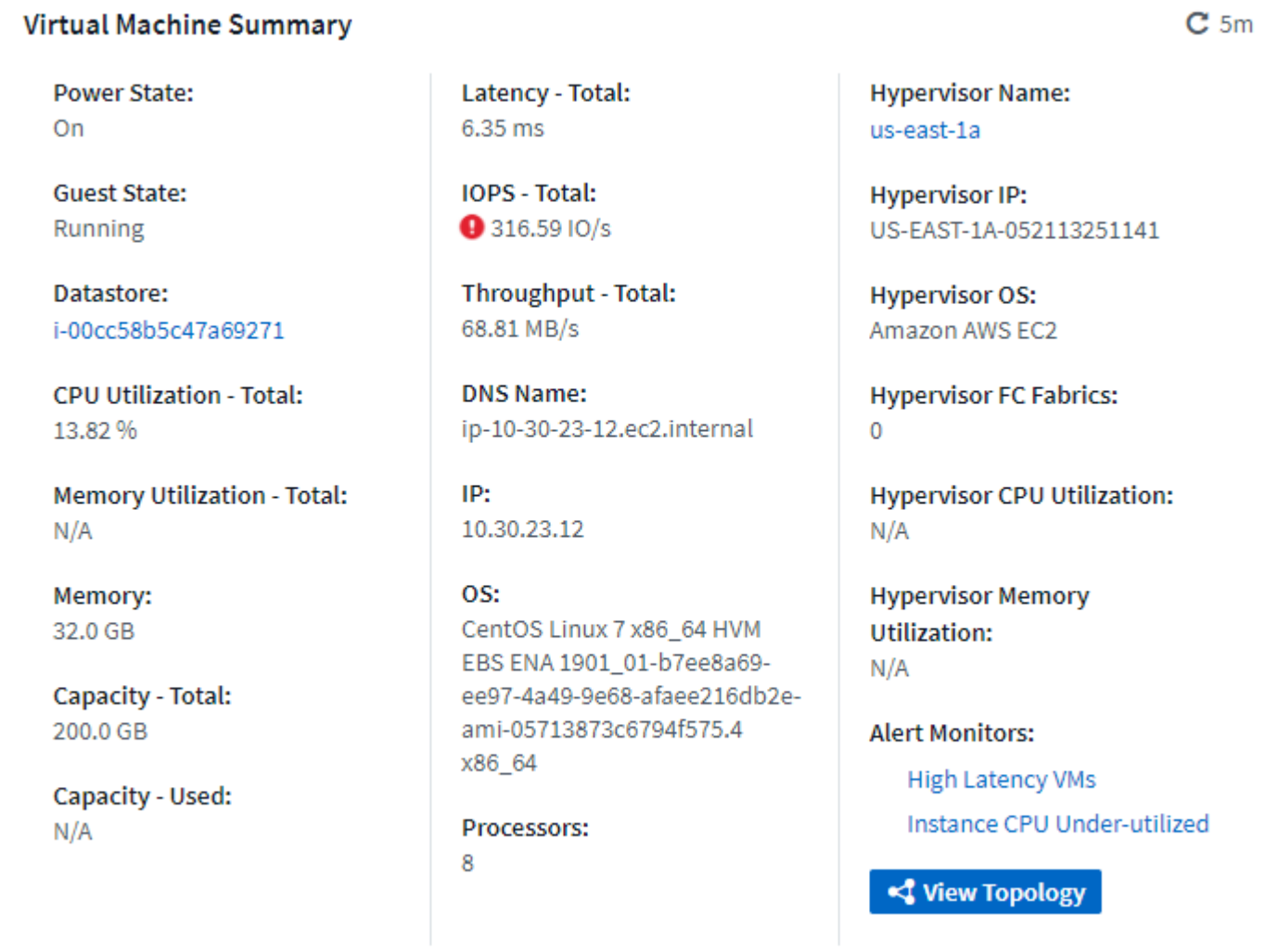
Objekten in Ihrer Umgebung an.

Sie können auch verwenden **"Sondervariablen in Widgets"** Um Asset-bezogene Informationen auf Landing Pages anzuzeigen.

Abschnitt „Ressourcen-Seite-Übersicht“

Im Abschnitt Zusammenfassung einer Asset-Seite werden allgemeine Informationen zu einem Asset angezeigt, einschließlich der Frage, ob Kennzahlen oder Leistungsrichtlinien für Bedenken sorgen. Potenzielle Problembereiche werden durch einen roten Kreis gekennzeichnet.

Die Informationen in der Zusammenfassung sowie in beliebigen Tabellen oder benutzerdefinierten Widgets auf der Bestandsseite werden automatisch auf Basis des ausgewählten Zeitbereichs aktualisiert. Sie können die aktuelle Aktualisierungsrate in der oberen rechten Ecke des Abschnitts Zusammenfassung, den Tabellen und beliebigen benutzerdefinierten Widgets anzeigen.



Hinweis: Die im Abschnitt Zusammenfassung angezeigten Informationen variieren je nach Art des anzuzeigenden Assets.

Sie können auf einen der Asset-Links klicken, um die Asset-Seiten anzuzeigen. Wenn Sie beispielsweise einen Speicherknoten anzeigen, können Sie auf einen Link klicken, um die Asset-Seite des zugehörigen Speichers

anzuzeigen.

Sie können die Metriken anzeigen, die mit der Ressource verknüpft sind. Ein roter Kreis neben einer Metrik zeigt an, dass Sie mögliche Probleme diagnostizieren und lösen müssen.

> Sie können feststellen, dass die Volume-Kapazität bei einigen Storage-Assets größer als 100 % sein kann. Das liegt an Metadaten, die sich auf die Kapazität des Volumes beziehen, die Teil der verbrauchten Kapazitätsdaten sind, die von der Ressource gemeldet wurden.

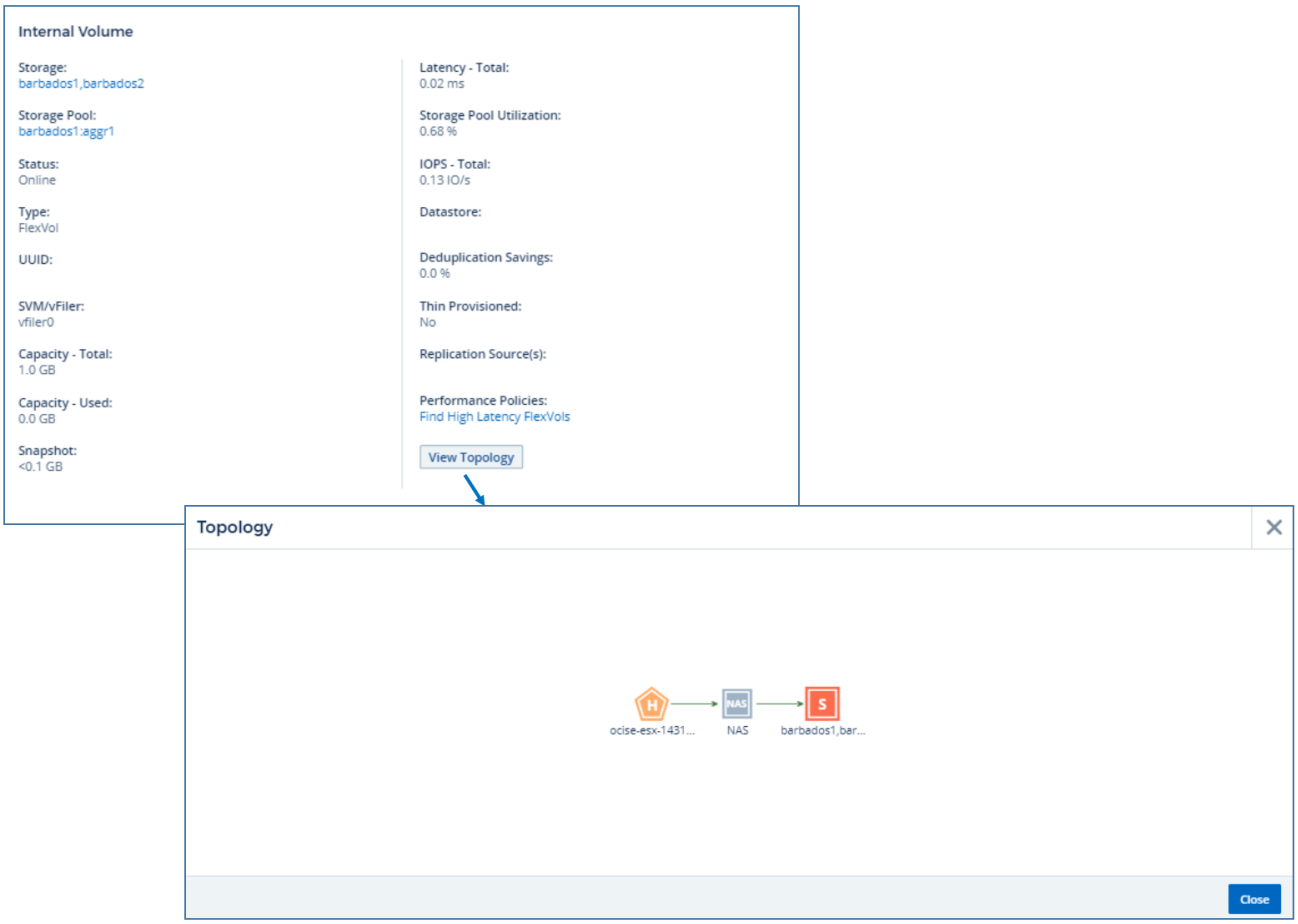
Falls zutreffend, können Sie auf einen Warnlink klicken, um die mit dem Gerät verknüpfte Warnung und den Monitor anzuzeigen.

Topologie

Auf bestimmten Asset-Seiten enthält der Abschnitt Zusammenfassung einen Link, um die Topologie des Assets und dessen Verbindungen anzuzeigen.

Die Topologie ist für die folgenden Asset-Typen verfügbar:

- Applikation
- Festplatte
- Fabric
- Host
- Internes Volumen
- Port
- Switch
- Virtual Machine
- VMDK
- Datenmenge

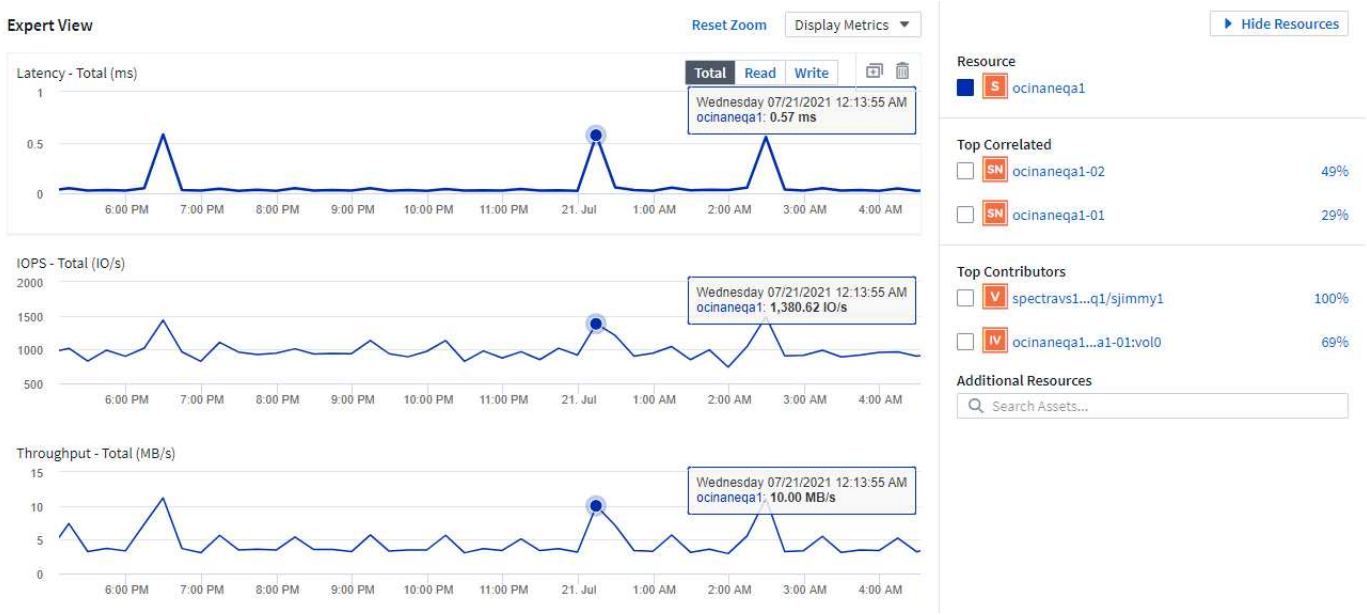


Expertensicht

Im Abschnitt „Expertenansicht“ auf der Seite „Anlage“ können Sie anhand einer beliebigen Anzahl anwendbarer Metriken im Kontext eines ausgewählten Zeitraums im Leistungsdiagramm und aller damit verbundenen Ressourcen eine Performance-Probe für das Basisressource anzeigen. Die Daten in den Diagrammen werden automatisch aktualisiert, wenn Datensammler abfragen und aktualisierte Daten erfasst werden.

Verwenden des Abschnitts „Expertenansicht“

Im Folgenden finden Sie ein Beispiel für den Abschnitt „Expert View“ auf einer Storage Asset-Seite:



Sie können die Metriken auswählen, die im Performance-Diagramm für den ausgewählten Zeitraum angezeigt werden sollen. Klicken Sie auf das Dropdown-Menü „ Metriken anzeigen “, und wählen Sie aus den aufgeführten Metriken aus.

Der Abschnitt **Ressourcen** zeigt den Namen des Basisinformers und die Farbe, die das Basisoutum im Leistungsdiagramm darstellt. Wenn der Abschnitt **Top Correlated** kein Asset enthält, das im Leistungsdiagramm angezeigt werden soll, können Sie das Feld **Assets suchen** im Abschnitt **zusätzliche Ressourcen** verwenden, um das Asset zu lokalisieren und zum Leistungsdiagramm hinzuzufügen. Beim Hinzufügen von Ressourcen werden diese im Abschnitt zusätzliche Ressourcen angezeigt.

Sind auch im Abschnitt Ressourcen aufgeführt, sofern zutreffend, alle Assets, die sich auf das Basivermögen in den folgenden Kategorien beziehen:

- Oben korreliert

  Zeigt die Assets, die eine hohe Korrelation (in Prozent) mit einem oder mehreren Performance-Kennzahlen zur Basisinressource haben.

- Top-Mitwirkende

  Zeigt die Assets an, die (in Prozent) zur Basisinressource beitragen.

- Workload-Konflikte

  Zeigt die Ressourcen an, die Auswirkungen auf andere gemeinsam genutzte Ressourcen wie Hosts, Netzwerke und Storage haben bzw. von diesen betroffen sind. Diese werden manchmal als *gierige* und *degradierte* Ressourcen bezeichnet.

Warnmeldungen in der Ansicht „Experten“

Warnmeldungen werden auch im Abschnitt „Expertenansicht“ einer Asset-Landing-Page angezeigt, auf der die Zeit und Dauer der Warnmeldung sowie die Monitorbedingung angezeigt werden, die diese ausgelöst hat.

Metrische Definitionen der Expertenansicht

Im Abschnitt „Expertenansicht“ einer Asset-Seite werden je nach dem für das Asset ausgewählten Zeitraum mehrere Metriken angezeigt. Jede Metrik wird in einem eigenen Performance-Diagramm angezeigt. Je nachdem, welche Daten angezeigt werden sollen, können Sie Metriken und zugehörige Assets in den Diagrammen hinzufügen oder entfernen. Die ausgewählten Metriken sind abhängig von dem Asset-Typ.

Metrisch	Beschreibung
BB Credit Null Rx, Tx	Die Anzahl der Empfangs-/Übertragungs-Buffer-zu-Buffer-Gutschriften wurde während des Probenzeitraums auf Null übertragen. Diese Metrik gibt an, wie oft der angeschlossene Port die Übertragung beenden musste, da dieser Port nicht mehr als Credits zur Verfügung stand.
BB Kredit Null Dauer Tx	Zeit in Millisekunden, während der der transmit BB-Guthaben während des Abtastintervalls null war.
Cache-Trefferrverhältnis (gesamt, Lesen, Schreiben) %	Prozentsatz von Anforderungen, die zu Cache-Treffern führen. Je höher die Anzahl der Treffer im Vergleich zum Volume ist, desto besser ist die Performance. Diese Spalte ist leer für Speicher-Arrays, die keine Cache-Trefferinformationen erfassen.
Cache-Auslastung (gesamt) %	Gesamtprozentsatz der Cacheanforderungen, die zu Cache-Treffern führen
Discards der Klasse 3	Anzahl der Rückwürfe für die Datenübertragung in der Fibre Channel-Klasse 3
CPU-Auslastung (gesamt) %	Menge der aktiv genutzten CPU-Ressourcen als Prozentsatz der insgesamt verfügbaren (über alle virtuellen CPUs)
CRC-Fehler	Anzahl der Frames mit ungültigen zyklischen Redundanzprüfungen (CRCs), die vom Port während des Probenahmezeitraums erkannt wurden
Frame-Rate	Bildrate in Bildern pro Sekunde übertragen (FPS)
Bildgröße durchschnittlich (Rx, Tx)	Verhältnis von Datenverkehr zu Bildgröße. Mit dieser Metrik können Sie feststellen, ob es Overhead Frames in der Fabric gibt.

Rahmengröße zu lang	Anzahl der zu langen Fibre Channel-Datenübertragungsrahmen
Rahmengröße zu kurz	Anzahl der zu kurzen Fibre Channel-Datenübertragungsrahmen
I/O-Dichte (gesamt, Lesen, Schreiben)	Anzahl der IOPS geteilt durch genutzte Kapazität (wie bei der letzten Inventarabfrage der Datenquelle erworben) für das Element Volume, Internal Volume oder Storage. Diese wird anhand der Anzahl der I/O-Vorgänge pro Sekunde pro TB gemessen.
IOPS (gesamt, Lesen, Schreiben)	Anzahl der Lese-/Schreib-I/O-Serviceanfragen, die den I/O-Kanal oder einen Teil dieses Kanals pro Zeiteinheit durchlaufen (gemessen in I/O pro Sekunde)
IP-Durchsatz (gesamt, Lesen, Schreiben)	Gesamt: Aggregierte Rate, bei der IP-Daten in Megabyte pro Sekunde übertragen und empfangen wurden.
Lesen: IP-Durchsatz (Empfangen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde empfangen wurden.
Schreiben: IP-Durchsatz (übertragen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde übertragen wurden.
Latenz (Gesamt, Lesen, Schreiben)	Latenz (R&W): Geschwindigkeit, mit der Daten in einem festgelegten Zeitraum gelesen oder auf die Virtual Machines geschrieben werden Der Wert wird in Megabyte pro Sekunde gemessen.
Latenz	Durchschnittliche Antwortzeit von den Virtual Machines in einem Datenspeicher.
Höchste Latenz:	Die höchste Reaktionszeit von den Virtual Machines in einem Datenspeicher.
Verbindungsfehler	Anzahl der Verbindungsfehler, die der Port während des Probenahmezeitraums entdeckt hat.
Link Reset Rx, Tx	Anzahl der Rücksetzungen von Empfangs- oder Übertragungsverbindung während des Probenzeitraums. Diese Metrik gibt die Anzahl der vom angeschlossenen Port an diesen Port ausgegebenen Link-Resets an.
Speicherauslastung (gesamt) %	Schwellenwert für den vom Host verwendeten Speicher.

Teilweise R/W (gesamt) %	Gesamtzahl der Male, die ein Lese-/Schreibvorgang einen Stripe-Grenzwert auf einem Festplattenmodul in RAID 5, RAID 1/0 oder RAID 0 LUN überschreitet, sind Stripe-Crossings in der Regel nicht von Vorteil, da jeder eine zusätzliche I/O-Operation erfordert Ein geringer Prozentsatz zeigt eine effiziente Stripe-Elementgröße an und gibt Aufschluss über eine nicht ordnungsgemäße Ausrichtung eines Volumes (oder einer NetApp LUN). Bei CLARiiON ist dieser Wert die Anzahl der Stripe-Crossings, geteilt durch die Gesamtzahl der IOPS.
Port-Fehler	Bericht über Port-Fehler über den Probenzeitraum/den angegebenen Zeitraum.
Signalverlust zählen	Anzahl der Signalverlustfehler. Wenn ein Signalverlustfehler auftritt, gibt es keine elektrische Verbindung und es besteht ein physikalisches Problem.
Swap-Rate (Gesamtrate, Rate, out-Rate)	Rate, mit welcher der Speicher während des Probenzeitraums in den aktiven Speicher des Laufwerks oder aus dem Datenträger in den aktiven Speicher eingetauscht wird. Dieser Zähler bezieht sich auf virtuelle Maschinen.
Synchrone Verlustzahl	Anzahl der Fehler bei Synchronisierungsverlust. Wenn ein Fehler bei der Synchronisierung auftritt, kann die Hardware den Datenverkehr nicht erkennen oder darauf sperren. Das gesamte Gerät verwendet möglicherweise nicht die gleiche Datenrate, oder die optischen oder physischen Verbindungen können von schlechter Qualität sein. Der Port muss nach jedem solchen Fehler erneut synchronisiert werden, was sich auf die Systemleistung auswirkt. Gemessen in KB/Sek.
Durchsatz (Gesamt, Lesen, Schreiben)	Geschwindigkeit, mit der Daten übertragen, empfangen oder in einem festen Zeitraum als Reaktion auf I/O-Serviceanfragen (gemessen in MB pro s) gesendet werden.
Timeout - Rahmen verwerfen - Tx	Anzahl der durch Timeout verursachten verworfenen Übertragungsrahmen.
Traffic-Rate (gesamt, Lesen, Schreiben)	Der während des Probenahmezeitraums übertragenen, empfangenen oder beide empfangenen Datenverkehr in Mebibyte pro Sekunde.
Traffic-Auslastung (gesamt, Lesen, Schreiben)	Verhältnis der empfangenen/übertragenen/gesamten Kapazität zu Empfangs-/Übertragungs-/Gesamtkapazität während des Probenzeitraums.
Auslastung (Gesamt, Lesen, Schreiben) %	Prozentsatz der verfügbaren Bandbreite für die Übertragung (Tx) und den Empfang (Rx).
Ausstehende Schreibvorgänge (Gesamt)	Anzahl der ausstehenden Schreib-I/O-Serviceanfragen.

Verwenden des Abschnitts „Expertenansicht“

In der Ansicht „Experten“ können Sie Leistungsdiagramme für ein Asset anzeigen, die auf einer beliebigen Anzahl von anwendbaren Metriken während eines ausgewählten Zeitraums basieren, und zugehörige Assets hinzufügen, um Asset- und Performance-Werte über verschiedene Zeiträume zu vergleichen und zu kontrastieren.

Schritte

1. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Suchen Sie nach einem bestimmten Asset, und wählen Sie es aus.
   - Wählen Sie in einem Dashboard-Widget einen Asset aus.
   - Fragen Sie nach einem Satz von Assets ab, und wählen Sie eines aus der Ergebnisliste aus.

     Die Seite Anlage wird angezeigt. Standardmäßig werden im Performance-Diagramm zwei Metriken für den Zeitraum angezeigt, der für die Seite Anlage ausgewählt wurde. Beispielsweise zeigt das Performance-Diagramm für einen Storage standardmäßig die Latenz und die IOPS insgesamt an. Im Abschnitt Ressourcen werden der Ressourcenname und der Abschnitt „zusätzliche Ressourcen“ angezeigt, in dem Sie nach Assets suchen können. Je nach Asset können Sie auch Assets in den Abschnitten „Top Correlated“, „Top Contributor“, „Greedy“ und „degradierte Werte“ sehen. Wenn für diese Abschnitte keine relevanten Assets vorhanden sind, werden sie nicht angezeigt.

2. Sie können ein Leistungsdiagramm für eine Metrik hinzufügen, indem Sie auf **Kennzahlen anzeigen** klicken und die gewünschten Metriken auswählen.

   Für jede ausgewählte Metrik wird ein separates Diagramm angezeigt. Das Diagramm zeigt die Daten für den ausgewählten Zeitraum an. Sie können den Zeitraum ändern, indem Sie auf einen anderen Zeitraum in der rechten oberen Ecke der Asset-Seite klicken oder ein beliebiges Diagramm vergrößern.

   Klicken Sie auf **Kennzahlen anzeigen**, um die Auswahl eines Diagramms zu dewählen. Das Performance-Diagramm für die Metrik wird aus Expert View entfernt.

3. Sie können den Cursor über das Diagramm positionieren und die für das Diagramm angezeigten metrischen Daten ändern, indem Sie je nach Anlage auf eine der folgenden Optionen klicken:
   - Lesen, Schreiben oder Gesamt
   - TX, Rx oder Total

     Die Gesamtsumme ist die Standardvorgabe.

   Sie können den Cursor über die Datenpunkte im Diagramm ziehen, um zu sehen, wie sich der Wert der Metrik im ausgewählten Zeitraum ändert.

4. Im Abschnitt Ressourcen können Sie den Leistungsdiagrammen alle zugehörigen Assets hinzufügen:
   - Sie können eine zugehörige Ressource in den Abschnitten **Top Correlated**, **Top Contributors**, **Greedy** und **degraded** auswählen, um Daten aus dieser Ressource in das Leistungsdiagramm für jede ausgewählte Metrik hinzuzufügen.

     Nachdem Sie das Element ausgewählt haben, wird neben dem Element ein Farbblock angezeigt, der die Farbe seiner Datenpunkte im Diagramm kennzeichnet.

5. Klicken Sie auf **Ressourcen ausblenden**, um das Fenster zusätzliche Ressourcen auszublenden. Klicken Sie auf **Ressourcen**, um das Fenster anzuzeigen.

- Für alle angezeigten Assets können Sie auf den Namen des Assets klicken, um die Seite des Assets anzuzeigen. Sie können auch auf den Prozentsatz klicken, der das Asset korreliert oder zum Basisspital beiträgt, um weitere Informationen über die Beziehung des Assets zum BasisinAsset anzuzeigen.

  Wenn Sie beispielsweise auf den verknüpften Prozentsatz neben einem Top-korrelierten Asset klicken, wird eine Informationsmeldung angezeigt, die den Typ der Korrelation zwischen der Anlage und der Basisinressource vergleicht.

- Wenn der Abschnitt „Top Correlated“ keine Anlage enthält, die in einem Leistungsdiagramm zum Vergleich angezeigt werden soll, können Sie im Abschnitt „zusätzliche Ressourcen“ das Feld „Assets suchen“ verwenden, um andere Assets zu finden.

Nachdem Sie ein Asset ausgewählt haben, wird es im Abschnitt zusätzliche Ressourcen angezeigt. Wenn Sie keine Informationen über das Asset mehr anzeigen möchten, klicken Sie auf 🗑.

Abschnitt „Benutzerdaten“

Der Abschnitt „Benutzerdaten“ einer Asset-Seite wird angezeigt und ermöglicht das Ändern benutzerdefinierter Daten wie Anwendungen und Anmerkungen.

Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anwendungen

Sie können Applikationen, die in Ihrer Umgebung ausgeführt werden, bestimmten Assets (Host, Virtual Machines, Volumes, interne Volumes, qtrees, Und Hypervisoren). Im Abschnitt „Benutzerdaten“ können Sie die Anwendungen hinzufügen, ändern oder entfernen, die einem Asset zugewiesen sind. Für alle diese Asset-Typen außer für Volumes können Sie mehr als eine Anwendung zuweisen.

Schritte

1. Suchen Sie eine Asset-Seite, indem Sie einen der folgenden Schritte ausführen:
   a. Abfrage nach einer Liste von Assets, und wählen Sie dann eine aus der Liste aus.
   b. Suchen Sie in einem Dashboard nach einem Asset-Namen, und klicken Sie darauf.
   c. Führen Sie eine Suche durch, und wählen Sie aus den Ergebnissen eine Anlage aus.

      Die Seite Anlage wird angezeigt. Im Abschnitt „Benutzerdaten“ auf der Seite werden aktuell zugewiesene Anwendungen oder Anmerkungen angezeigt.

Um die zugewiesene Anwendung zu ändern oder eine Anwendung oder weitere Anwendungen zuzuweisen, klicken Sie auf die Liste **Anwendung** und wählen Sie die Anwendung(en) aus, die Sie dem Asset zuweisen möchten. Sie können eingeben, um nach einer Anwendung zu suchen, oder eine aus der Liste auswählen.

Um eine Anwendung zu entfernen, legen Sie die Anwendungsliste herunter und deaktivieren Sie die Prüfung der Anwendung.

Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anmerkungen

Wenn Sie Cloud Insights anpassen, um die Daten zur Nachverfolgung Ihrer Unternehmensanforderungen zu verfolgen, können Sie spezielle Anmerkungen mit der Bezeichnung „Anmerkungen“ definieren und diese Ihren Assets zuweisen. Im Abschnitt „Benutzerdaten“ einer Asset-Seite werden Anmerkungen angezeigt, die einem Asset zugeordnet sind, und Sie können auch die Anmerkungen ändern, die diesem Asset zugewiesen sind.

Schritte

1. Um dem Asset eine Anmerkung hinzuzufügen, klicken Sie im Bereich Benutzerdaten auf der Asset-Seite auf **+Annotation**.
2. Wählen Sie eine Anmerkung aus der Liste aus.
3. Klicken Sie auf „Wert“ und führen Sie eine der folgenden Aktionen aus, je nachdem, welche Anmerkungstypen Sie ausgewählt haben:
   a. Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   b. Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
4. Klicken Sie auf Speichern .

Die Anmerkung wird dem Asset zugewiesen. Sie können Assets später mithilfe einer Abfrage nach Anmerkungen filtern.

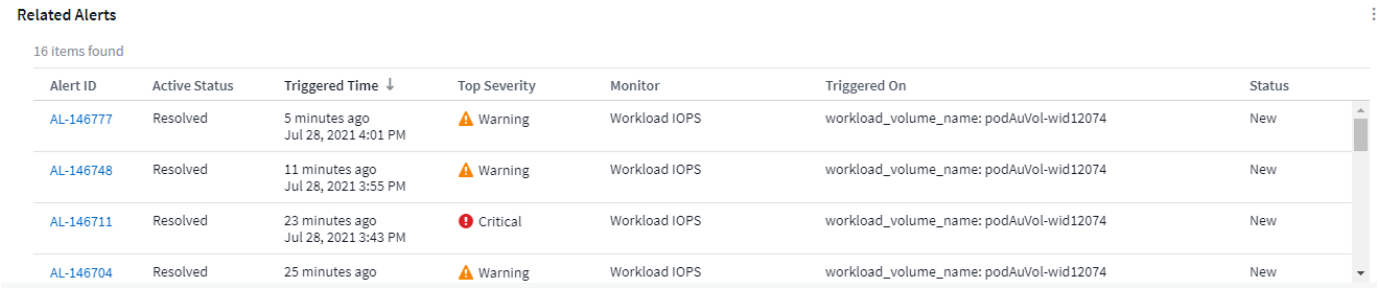
Wenn Sie den Wert der Anmerkung nach der Zuweisung ändern möchten, lassen Sie die Anmerkungsliste herunter und geben einen anderen Wert ein.

Wenn die Anmerkung vom Listentyp ist, für den die Option *neue Werte hinzufügen auf der Fly* ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Wertes einen neuen Wert hinzufügen.

Abschnitt „Hinweise auf der Seite „Ressourcen“

Sie können den Abschnitt „Verwandte Warnungen“ einer Asset-Seite verwenden, um alle Warnmeldungen anzuzeigen, die in Ihrer Umgebung als Ergebnis eines Monitors auftreten, der einem Asset zugewiesen ist. Monitore generieren Warnungen auf der Grundlage von festgelegten Bedingungen. So können Sie Implikationen identifizieren und die Auswirkungen und Ursache des Problems auf eine schnelle und effektive Korrektur analysieren.

Das folgende Beispiel zeigt einen typischen Abschnitt „Verwandte Warnungen“, der auf einer Asset-Seite angezeigt wird:



Im Abschnitt „Verwandte Warnungen“ können Sie die Warnmeldungen anzeigen und verwalten, die in Ihrem Netzwerk aufgrund von Überwachungsbedingungen auftreten, die einem Asset zugewiesen sind.

Schritte

- Suchen Sie eine Asset-Seite, indem Sie einen der folgenden Schritte ausführen:
  - Geben Sie den Namen des Assets im Suchbereich ein, und wählen Sie das Element aus der Liste aus.
  - Klicken Sie in einem Dashboard-Widget auf den Namen eines Assets.
  - Fragen Sie nach einem Satz von Assets ab, und wählen Sie in der Ergebnisliste ein aus.

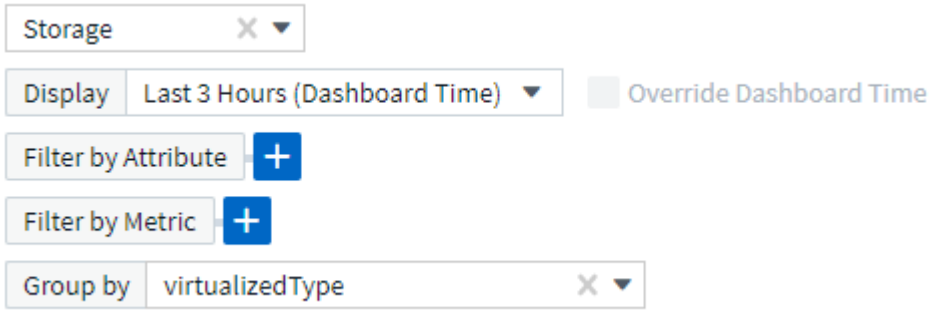
Die Seite Anlage wird angezeigt. Im Abschnitt „Verwandte Warnungen“ werden die Zeit angezeigt, zu der die Warnmeldung ausgelöst wurde, sowie der aktuelle Status der Warnmeldung und der Monitor, der sie ausgelöst hat. Sie können auf die Alarm-ID klicken, um die Landing Page für die Warnmeldung zur weiteren Untersuchung zu öffnen.

Storage-Virtualisierung

Cloud Insights kann zwischen einem Storage-Array mit lokalem Speicher oder der Virtualisierung anderer Storage-Arrays unterscheiden. So können Sie Kosten nachvollziehen und die Performance vom Front-End bis zum Back-End Ihrer Infrastruktur differenzieren.

Widget „Virtualisierung in einer Tabelle“

Eine der einfachsten Möglichkeiten zur Betrachtung Ihrer Storage-Virtualisierung ist die Erstellung eines Dashboard-Tabellen-Widgets mit virtualisierter Art. Wenn Sie die Abfrage für das Widget erstellen, fügen Sie einfach „virtualizedType“ zu Ihrer Gruppierung oder Ihrem Filter hinzu.



Das resultierende Tabellen-Widget zeigt Ihnen die *Standard*, *Backend* und *Virtual* Speicher in Ihrer Umgebung.

Storage by virtualizedType

50 items found in 4 groups

virtualizedType	Storage
Backend (5)	--
Backend	Sym-Perf
Backend	Sym-000050074300343
Backend	CX600_26_CK00351029326
Backend	VNX8000_46_CK00351029346
Backend	Sym-000050074300324
Standard (36)	--
Virtual (8)	--

Landing Pages zeigen virtualisierte Informationen an

Auf einer Storage-, Volume-, internen Volume- oder Disk-Landing Page können Sie die relevanten Virtualisierungsinformationen sehen. Wenn Sie beispielsweise auf der unten stehenden Storage-Landing Page sehen, sehen Sie, dass es sich um einen virtuellen Storage handelt und welches Back-End-Storage-System angewendet wird. Alle relevanten Tabellen auf Landing-Pages enthalten je nach Bedarf auch Virtualisierungsinformationen.

Storage Summary

Model: V-Series
Vendor: NetApp
Family: V-Series
Serial Number: 1306894
IP: 192.168.7.41

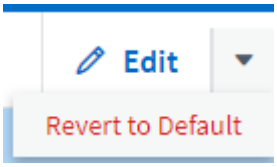
Virtualized Type: Virtual
Backend Storage: Sym-000050074300343
Microcode Version: 8.0.2 7-Mode
Raw Capacity: 0.0 GiB
Latency - Total: N/A

IOPS - Total: N/A
Throughput - Total: N/A
Management:
FC Fabrics Connected: 7
Alert Monitors:

Vorhandene Landing Pages und Dashboards

Beachten Sie, dass wenn Sie derzeit benutzerdefinierte Landing Pages oder Dashboards in Ihrer Umgebung haben, diese nicht automatisch alle Virtualisierungsinformationen standardmäßig anzeigen. Sie können jedoch jedes benutzerdefinierte Dashboard oder jede Landing Page *revert to Default* (Sie müssen Ihre Anpassungen neu implementieren) oder die relevanten Widgets so ändern, dass sie die gewünschten Virtualisierungsattribute oder Metriken enthalten.

Auf Standard zurücksetzen ist in der oberen rechten Ecke eines benutzerdefinierten Dashboard- oder Landing Page-Bildschirms verfügbar.



Tipps und Tricks für die Suche nach Ressourcen und Warnungen

Es können mehrere Suchmethoden verwendet werden, um in Ihrer überwachten Umgebung nach Daten oder Objekten zu suchen.

- **Platzhaltersuche**

  Sie können Platzhaltersuche für mehrere Zeichen mit dem * Zeichen durchführen. Zum Beispiel würde *Application*n__Application* zurückgeben.

- **Phrasen verwendet bei der Suche**

  Ein Begriff ist eine Gruppe von Wörtern, die von doppelten Anführungszeichen umgeben sind, z. B. „VNX LUN 5“. Sie können doppelte Anführungszeichen verwenden, um nach Dokumenten zu suchen, die Leerzeichen in ihren Namen oder Attributen enthalten.

- **Boolesche Operatoren**

  Mit Booleschen Operatoren ODER, UND, und, und NICHT können Sie mehrere Begriffe kombinieren, um eine komplexere Abfrage zu bilden.

  ODER

  Der OR-Operator ist der Standard-Konjunktion-Operator.

  Wenn zwischen zwei Begriffen kein Boolescher Operator vorhanden ist, wird der OPERATOR ODER verwendet.

  Der OR-Operator verknüpft zwei Begriffe und findet ein passendes Dokument, wenn einer der Termini in einem Dokument vorhanden ist.

  Beispielsweise sucht *Storage ODER netapp* nach Dokumenten, die entweder *Storage* oder *netapp* enthalten.

  Hohe Bewertungen werden an Dokumente vergeben, die den meisten Bedingungen entsprechen.

  UND

  Sie können den OPERATOR UND verwenden, um Dokumente zu suchen, in denen beide Suchbegriffe in einem einzigen Dokument vorhanden sind. Beispielsweise sucht *Storage UND netapp* nach Dokumenten, die *Storage* und *netapp* enthalten.

  Sie können anstelle des Wortes UND das Symbol **&** verwenden.

  NICHT

Wenn Sie den NICHT-Operator verwenden, werden alle Dokumente, die den Begriff nachher NICHT enthalten, von den Suchergebnissen ausgeschlossen. Beispiel: *Storage NOT netapp* sucht nach Dokumenten, die nur *Storage* und nicht *netapp* enthalten.

Anstelle des Wortes NOT können Sie das Symbol **!** verwenden.

Die Groß-/Kleinschreibung der Suche wird nicht berücksichtigt.

Suche mit indizierten Begriffen

Suchvorgänge, die mehr der indizierten Begriffe entsprechen, führen zu höheren Punktzahlen.

Der Suchstring wird in separate Suchbegriffe nach Leerzeichen aufgeteilt. Die Suchzeichenfolge „Storage aurora netapp“ ist beispielsweise in drei Schlagwörter unterteilt: „Storage“, „aurora“ und „netapp“. Die Suche wird unter Verwendung aller drei Begriffe durchgeführt. Die Dokumente, die den meisten dieser Begriffe entsprechen, haben die höchste Punktzahl. Je mehr Informationen Sie zur Verfügung stellen, desto besser sind die Suchergebnisse. Sie können zum Beispiel nach einem Storage mit dessen Namen und Modell suchen.

Die Benutzeroberfläche zeigt die Suchergebnisse für verschiedene Kategorien mit den drei besten Ergebnissen pro Kategorie an. Wenn Sie ein Objekt nicht gefunden haben, das Sie erwartet haben, können Sie weitere Termini in die Suchzeichenfolge eingeben, um die Suchergebnisse zu verbessern.

Die folgende Tabelle enthält eine Liste indizierter Begriffe, die der Suchzeichenfolge hinzugefügt werden können.

Kategorie	Indizierte Begriffe
Storage	Name des Anbieters „Storage“
Storage Pool	„storagepool“: Name der Storage-IP-Adressen der Storage-Seriennummer des Storage-Anbieters Namen von Storage-Modellen aller damit verbundenen internen Volumes-Namen aller zugehörigen Festplatten
Internes Volumen	Name des Storage IP-Adressen der Storage-Seriennummer des Storage-Anbieters Name des Storage-Modells: Namen des Storage-Pools aller damit verbundenen Shares Namen aller zugehörigen Applikationen
Datenmenge	„Volume“: Name aller internen Volumes Name des Storage-Pools Name der Storage-IP-Adressen der Storage-Seriennummer des Storage-Anbietermodells
Storage-Node	Name des Storage-IP-Adressen der Storage-Serialnummer des Storage-Anbieters, Name des Storage-Modells
Host	Name „Host“ IP-Adressen Namen aller zugehörigen Anwendungen
Datenspeicher	„Datastore“: Name der virtuellen Center-IP-Namen aller Volumes Namen aller internen Volumes

Kategorie	Indizierte Begriffe
Virtual Machines	„virtualmachine“ Name DNS Name IP-Adressen Name der Host-IP-Adressen der Hostnamen aller Datenspeicher Namen aller zugehörigen Anwendungen
Switches (normal und Kapitalwert)	„Switch“-IP-Adresse wwn-Name Seriennummer Modell Domain-ID-Name des Fabric-wwn der Fabric
Applikation	„Applikation“: Name des Mandantenbereichsprojekts der Geschäftseinheit
Tape	„Tape“-IP-Adresse Name Seriennummer Anbieter
Port	„Port“ wwn-Name
Fabric	„Fabric“ wwn-Name
Storage Virtual Machine (SVM)	Name UUID von „storagevirtualMachine“

Berichterstellung

Cloud Insights-Berichte: Überblick

Cloud Insights Berichte sind ein Business Intelligence Tool, mit dem Sie vordefinierte Berichte anzeigen oder individuelle Berichte erstellen können.

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Mit Cloud Insights Reporting können Sie die folgenden Aufgaben durchführen:

- Führen Sie einen vordefinierten Bericht aus
- Erstellen Sie einen benutzerdefinierten Bericht
- Passen Sie das Format und die Bereitstellungsmethode eines Berichts an
- Planen Sie die automatische Ausführung von Berichten
- E-Mail-Berichte
- Verwenden Sie Farben, um Schwellenwerte für Daten darzustellen

Cloud Insights-Berichte können benutzerdefinierte Berichte für Bereiche wie Chargeback, Verbrauchsanalysen und Prognosen erstellen. Darüber hinaus bieten sie Unterstützung bei der Beantwortung von Fragen wie folgenden:

- Welche Bestände habe ich?
- Wo ist mein Inventar?
- Wer nutzt unsere Ressourcen?
- Wie sieht die Rückberechnung von zugewiesenem Storage für einen Geschäftsbereich aus?
- Wie lange dauert es, bis ich zusätzliche Storage-Kapazität anschaffen muss?
- Werden die Geschäftseinheiten auf die entsprechenden Storage Tiers abgestimmt?
- Inwiefern ändert sich die Storage-Zuweisung über einen Monat, ein Quartal oder ein Jahr?

Zugriff Auf Cloud Insights-Berichte

Sie können auf Cloud Insights-Berichte zugreifen, indem Sie im Menü auf den Link **Berichte** klicken.

Sie werden zur Berichtsschnittstelle geleitet. Cloud Insights verwendet für seine Reporting Engine IBM Cognos Analytics.

Was ist ETL?

Bei der Arbeit mit Reporting hören Sie die Begriffe „Data Warehouse“ und „ETL“. ETL steht für „Extract, Transform, Load“. Der ETL-Prozess ruft in Cloud Insights gesammelte Daten ab und wandelt diese in ein Format um, das für die Berichterstellung verwendet werden kann. „Data Warehouse“ bezieht sich auf die gesammelten Daten, die für die Berichterstattung zur Verfügung stehen.

Der ETL-Prozess umfasst folgende Einzelprozesse:

- **Extrakt**: Nimmt Daten aus Cloud Insights.
- **Transform**: Wendet Geschäftslogik Regeln oder Funktionen auf die Daten an, wie sie aus Cloud Insights extrahiert werden.
- **Load**: Speichert die umgewandelten Daten in das Data Warehouse zur Verwendung in Reporting.

Benutzerrollen Für Cloud Insights-Berichte

Wenn Sie über Cloud Insights Premium Edition mit Reporting verfügen, verfügt jeder Cloud Insights-Benutzer in Ihrer Umgebung auch über eine SSO-Anmeldung bei der Reporting-Anwendung (d. h. Cognos). Klicken Sie einfach im Menü auf den Link **Berichte** und Sie werden automatisch bei Reporting angemeldet.

Ihre Benutzerrolle in Cloud Insights legt Ihre Rolle für die Berichterstellung fest:

Cloud Insights Rolle	Berichtsrolle	Reporting-Berechtigungen
Gast	Verbraucher	Es können Berichte angezeigt, geplant und erstellt sowie persönliche Einstellungen wie z. B. für Sprachen und Zeitzonen festgelegt werden. Verbraucher können keine Berichte erstellen oder administrative Aufgaben ausführen.
Benutzer	Autor	Kann alle Funktionen des Verbrauchers ausführen sowie Berichte und Dashboards erstellen und verwalten.
Verwalter	Verwalter	Kann alle Author-Funktionen sowie alle administrativen Aufgaben wie die Konfiguration von Berichten und das Herunterfahren und Neustarten von Reporting-Aufgaben ausführen.

Die folgende Tabelle zeigt die Funktionen, die den einzelnen Berichtsrollen zur Verfügung stehen.

Merkmal	Verbraucher	Autor	Verwalter
Anzeigen von Berichten auf der Registerkarte „Teaminhalt“	Ja.	Ja.	Ja.
Berichte erstellen	Ja.	Ja.	Ja.
Planen von Berichten	Ja.	Ja.	Ja.
Externe Dateien hochladen	Nein	Ja.	Ja.
Erstellen Von Jobs	Nein	Ja.	Ja.
Erstellen von Geschichten	Nein	Ja.	Ja.
Erstellen von Berichten	Nein	Ja.	Ja.
Erstellen von Paketen und Datenmodulen	Nein	Ja.	Ja.
Ausführung administrativer Aufgaben	Nein	Nein	Ja.
HTML-Element hinzufügen/bearbeiten	Nein	Nein	Ja.
Bericht mit HTML-Element ausführen	Ja.	Ja.	Ja.
Benutzerdefinierte SQL hinzufügen/bearbeiten	Nein	Nein	Ja.
Berichte mit benutzerdefiniertem SQL ausführen	Ja.	Ja.	Ja.

Festlegen der E-Mail-Einstellungen für Berichte (Cognos)

> Wenn Sie Ihre Benutzer-E-Mail-Einstellungen innerhalb von Cloud Insights Reporting ändern (d. h. die Cognos-Anwendung), sind diese Einstellungen aktiv_nur für die aktuelle Sitzung_. Wenn Sie sich bei Cognos und wieder zurück in anmelden, werden Ihre E-Mail-Einstellungen zurückgesetzt.

Wichtiger Hinweis für Bestandskunden

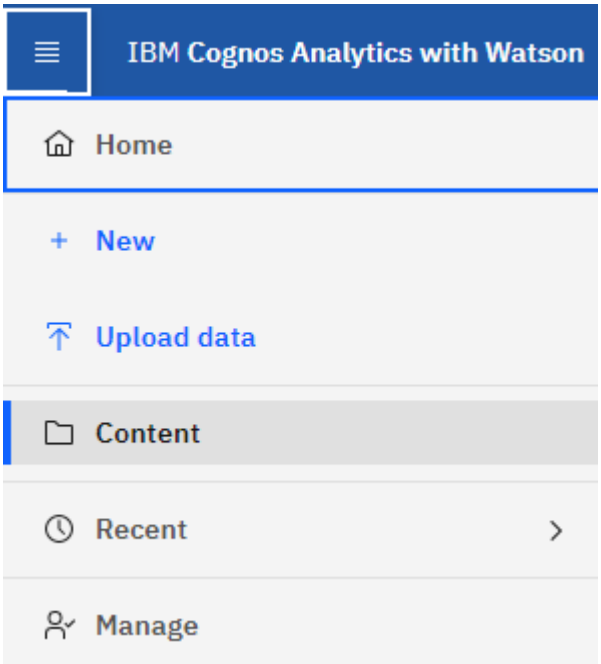
Neue Berichte bei Cloud Insights Es gibt nichts mehr, was Sie tun müssen, um die Berichterstattung zu genießen.

Wenn Sie bereits Premium Edition-Kunde sind, ist SSO für Ihre Umgebung nicht automatisch aktiviert. Wenn Sie SSO aktivieren, existiert der Administrator-Benutzer für das Berichtsportal (Cognos) nicht mehr. Das bedeutet, dass alle Berichte, die sich im Ordner *My Content* befinden, entfernt werden und in *Team Content* neu installiert oder neu erstellt werden müssen. Darüber hinaus müssen nach Aktivierung von SSO geplante Berichte konfiguriert werden.

Welche Schritte sollte ich Unternehmen, um meine vorhandene Umgebung auf die Aktivierung von SSO vorzubereiten?

Um sicherzustellen, dass Ihre Berichte erhalten bleiben, migrieren Sie alle Berichte von *My Content* zu *Team Content*. Gehen Sie dabei wie folgt vor. Vor der Aktivierung von SSO in Ihrer Umgebung sind folgende Schritte erforderlich:

1. Navigieren Sie zu **Menü > Inhalt**



1. Erstellen Sie einen neuen Ordner in ***Team Content***
   a. Wenn mehrere Benutzer erstellt wurden, erstellen Sie für jeden Benutzer einen separaten Ordner, um zu vermeiden, dass Berichte mit doppelten Namen überschrieben werden
2. Navigieren Sie zu *My Content*
3. Wählen Sie alle Berichte aus, die Sie beibehalten möchten.
4. Wählen Sie oben rechts im Menü die Option „Kopieren oder Verschieben“ aus.
5. Navigieren Sie zum neu erstellten Ordner in *Team Content*
6. Fügen Sie die Berichte mithilfe der Schaltflächen „Kopieren nach“ oder „Verschieben nach“ in den neu erstellten Ordner ein
7. Sobald SSO für Cognos aktiviert ist, melden Sie sich bei Cloud Insights an, wobei die E-Mail-Adresse zum Erstellen Ihres Kontos verwendet wird.
8. Navigieren Sie in Cognos zum Ordner „*Team Content*“, und kopieren oder verschieben Sie die zuvor gespeicherten Berichte zurück zu „*My Content*“.

Vordefinierte Berichte Leicht Gemacht

Cloud Insights Reporting enthält vordefinierte Berichte, die eine Reihe allgemeiner Berichtsanforderungen erfüllen und wichtige Einblicke bieten, die Stakeholder fundierte Entscheidungen bezüglich ihrer Storage-Infrastruktur treffen müssen.

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Sie können vordefinierte Berichte aus dem Cloud Insights-Berichtsportal generieren, sie per E-Mail an andere Benutzer senden und sogar ändern. Mithilfe mehrerer Berichte können Sie nach Gerät, Geschäftseinheit oder Tier filtern. Die Berichterstellungs-Tools verwenden IBM Cognos als Grundlage und bieten Ihnen viele Möglichkeiten zur Datenpräsentation.

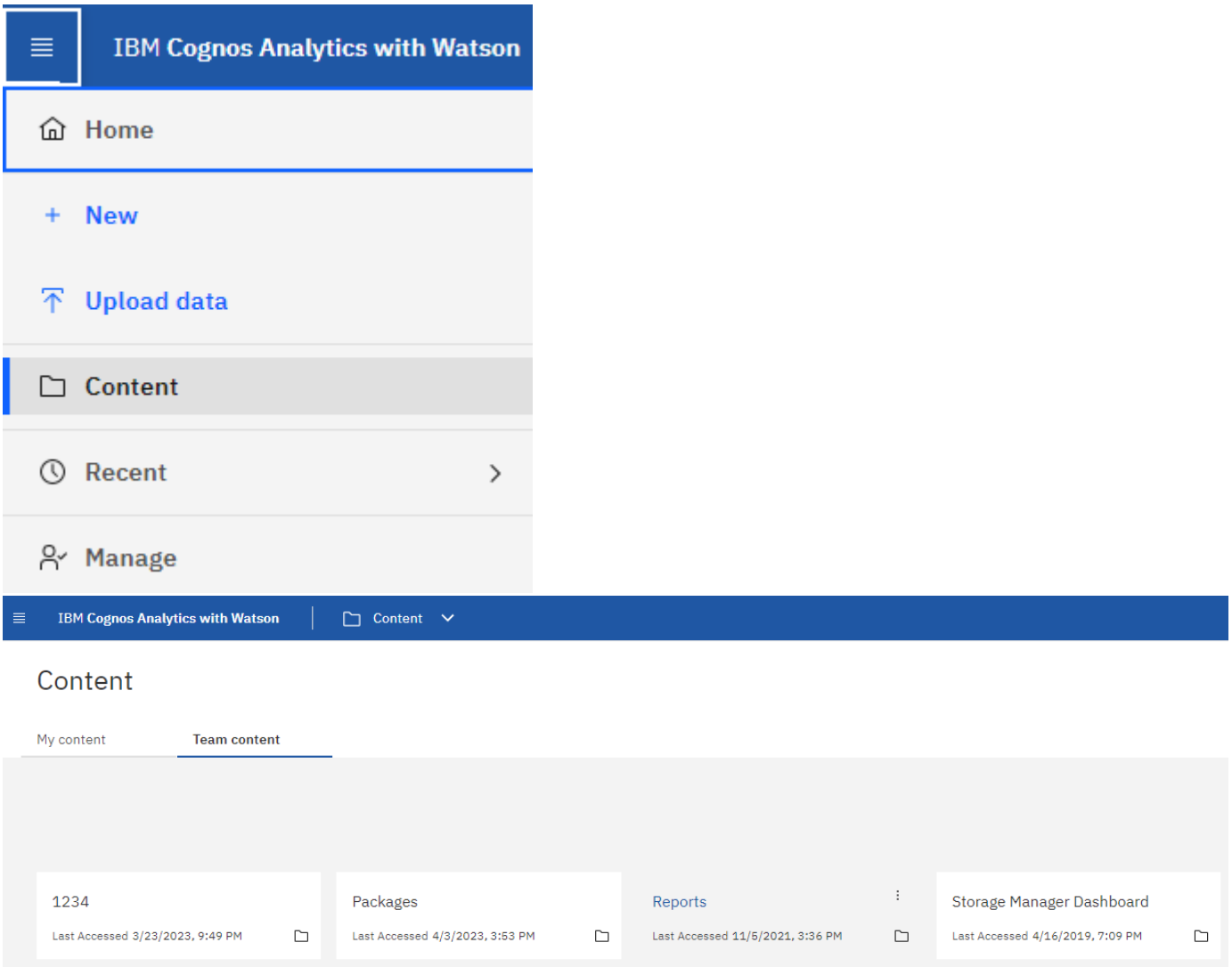
In den vordefinierten Berichten werden Ihr Inventar, Storage-Kapazität, Kostenzuordnung, Performance, Storage-Effizienz Und Cloud-kosten Daten. Sie können diese vordefinierten Berichte ändern und Ihre Änderungen speichern.

Sie können Berichte in verschiedenen Formaten generieren, darunter HTML, PDF, CSV, XML, Und Excel.

Navigieren zu vordefinierten Berichten

Wenn Sie das Berichtsportal öffnen, ist der Ordner „*Teaminhalt*“ der Ausgangspunkt, um die Informationen auszuwählen, die Sie in den Cloud Insights-Berichten benötigen.

1. Wählen Sie im linken Navigationsbereich **Inhalt > Teaminhalt**.
2. Wählen Sie **Reports**, um auf die vordefinierten Berichte zuzugreifen.



Verwenden von vordefinierten Berichten zur Beantwortung häufiger Fragen

Die folgenden vordefinierten Berichte stehen unter **Teaminhalt > Berichte** zur Verfügung.

Kapazität und Performance des Applikations-Service-Level

Der Bericht Application Service Level Capacity and Performance liefert einen allgemeinen Überblick über die Applikationen. Diese Informationen können für die Kapazitätsplanung oder für einen Migrationsplan verwendet werden.

Kostenverrechnung

Der Bericht Chargeback liefert Informationen zur Rückberechnung von Storage-Kapazitäten nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein.

Um zu verhindern, dass die Doppelzählung keine ESX Server beinhaltet, überwachen Sie nur die VMs.

Datenquellen

Der Bericht „Datenquellen“ zeigt alle Datenquellen an, die auf Ihrem Standort installiert sind, den Status der Datenquelle (Erfolg/Fehler) und Statusmeldungen. Der Bericht enthält Informationen darüber, wo mit der Fehlerbehebung von Datenquellen begonnen werden soll. Fehlerhafte Datenquellen wirken sich auf die Genauigkeit der Berichterstellung und die allgemeine Benutzerfreundlichkeit des Produkts aus.

ESX im Vergleich zur VM-Performance

Der Bericht ESX vs VM Performance zeigt einen Vergleich der ESX Server und VMs und zeigt die durchschnittliche und Spitzen-IOPS, den Durchsatz und die Latenz sowie die Auslastungen für ESX-Server und VMs an. Um eine Doppelzählung zu verhindern, schließen Sie die ESX Server aus; schließen Sie nur die VMs ein. Eine aktualisierte Version dieses Berichts finden Sie im NetApp Storage Automation Store.

Fabric – Zusammenfassung

Der Bericht Fabric Summary identifiziert Switches und Switch-Informationen, einschließlich der Anzahl von Ports, Firmware-Versionen und Lizenzstatus. Der Bericht enthält keine NPV Switch-Ports.

Host HBAs

Der Bericht Host HBAs bietet einen Überblick über die Hosts in der Umgebung und bietet die Hersteller-, Modell- und Firmware-Version von HBAs sowie die Firmware-Ebene der Switches, mit denen sie verbunden sind. Dieser Bericht kann zur Analyse der Firmware-Kompatibilität bei der Planung eines Firmware-Upgrades für einen Switch oder einen HBA verwendet werden.

Kapazität und Performance des Host Service Level

Der Bericht über Kapazität und Performance auf Host Service Level bietet einen Überblick über die Storage-Auslastung je Host für rein Block-beschränkte Applikationen.

Host-Zusammenfassung

Der Host Summary Report bietet einen Überblick über die Speichernutzung für jeden ausgewählten Host mit Informationen für Fibre Channel- und iSCSI-Hosts. Der Bericht ermöglicht den Vergleich von Ports und Pfaden, der Fibre Channel- und ISCSI-Kapazität und der Anzahl der Verstöße.

Lizenzdetails

Im Bericht Lizenzdetails wird die berechtigte Menge an Ressourcen angezeigt, die Sie für alle Standorte mit aktiven Lizenzen lizenziert haben. Der Bericht zeigt außerdem eine Zusammenfassung der tatsächlichen Menge an allen Standorten mit aktiven Lizenzen. Die Zusammenfassung kann Überschneidungen von Storage Arrays umfassen, die von mehreren Servern gemanagt werden.

Zugeordneten, aber nicht maskierten Volumes

Der Bericht zugeordnete, jedoch nicht maskierte Volumes enthält die Volumes, deren Logical Unit Number (LUN) von einem bestimmten Host zur Verwendung zugeordnet wurde, jedoch nicht für diesen Host maskiert ist. In einigen Fällen können diese LUNs deaktiviert werden, die nicht maskiert wurden. Auf nicht maskierte Volumes kann jeder Host zugegriffen werden, wodurch sie anfällig für Datenkorruption sind.

NetApp Kapazität und Performance

Der Bericht NetApp Capacity and Performance liefert globale Daten für zugewiesene, genutzte und zugeteilte Kapazitäten im Rahmen von Trend- und Performance-Daten zur NetApp Kapazität.

Scorecard

Der Scorecard-Bericht bietet eine Zusammenfassung und allgemeinen Status aller von Cloud Insights erworbenen Assets. Der Status wird mit grünen, gelben und roten Markierungen angezeigt:

- Grün zeigt den normalen Zustand an
- Gelb zeigt ein potenzielles Problem in der Umgebung an
- Rot weist auf ein Problem hin, das Aufmerksamkeit erfordert

Alle Felder im Bericht werden im Data Dictionary beschrieben, das mit dem Bericht bereitgestellt wird.

Zusammenfassung

Der Bericht „Storage Summary“ bietet eine vollständige Übersicht über genutzte und nicht genutzte Kapazitätsdaten für Brutto-, zugewiesene Storage-Pools und Volumes. Dieser Bericht bietet einen Überblick über den gesamten erkannten Storage.

VM-Kapazität und Performance

Beschreibt die VM-Umgebung (Virtual Machine) und ihre Kapazitätsauslastung. VM-Tools müssen aktiviert sein, um einige Daten anzuzeigen, z. B. wenn die VMs heruntergefahren wurden.

VM-Pfade

Der Bericht zu VM-Pfaden enthält Daten zur Storage-Kapazität und Performancemetriken, wobei Virtual Machines auf welchem Host ausgeführt werden, welche Hosts auf welche gemeinsam genutzten Volumes zugreifen, was der aktive Zugriffspfad ist und welche Kapazitätszuweisung und -Nutzung umfasst.

HDS-Kapazität durch Thin Pool

Der HDS Bericht zur Kapazität nach Thin Pool zeigt die Menge der nutzbaren Kapazität in einem Storage-Pool, der per Thin Provisioning bereitgestellt ist.

NetApp Kapazität nach Aggregat

Der Bericht NetApp-Kapazität nach Aggregaten zeigt die Gesamtmenge, die Gesamtzahl der genutzten, verfügbaren und den engagierten Speicherplatz von Aggregaten.

Symmetrix-Kapazität durch Thick Array

Der Bericht Symmetrix Capacity by Thick Array zeigt die Rohkapazität, nutzbare Kapazität, freie Kapazität, zugeordnet, maskiert, Und der gesamten freien Kapazität.

Symmetrix-Kapazität durch Thin Pool

Der Bericht Symmetrix Capacity by Thin Pool zeigt die Rohkapazität, nutzbare Kapazität, genutzte Kapazität, freie Kapazität, verwendeter Prozentsatz, Abonnierte Kapazitäten und Abonnementtarif.

XIV Kapazität nach Array

Der Bericht XIV Capacity by Array zeigt genutzte und ungenutzte Kapazität des Arrays an.

XIV Kapazität pro Pool

Der Bericht zur Nutzung der XIV-Kapazität anhand von Pools zeigt genutzte und nicht genutzte Kapazität für Storage Pools an.

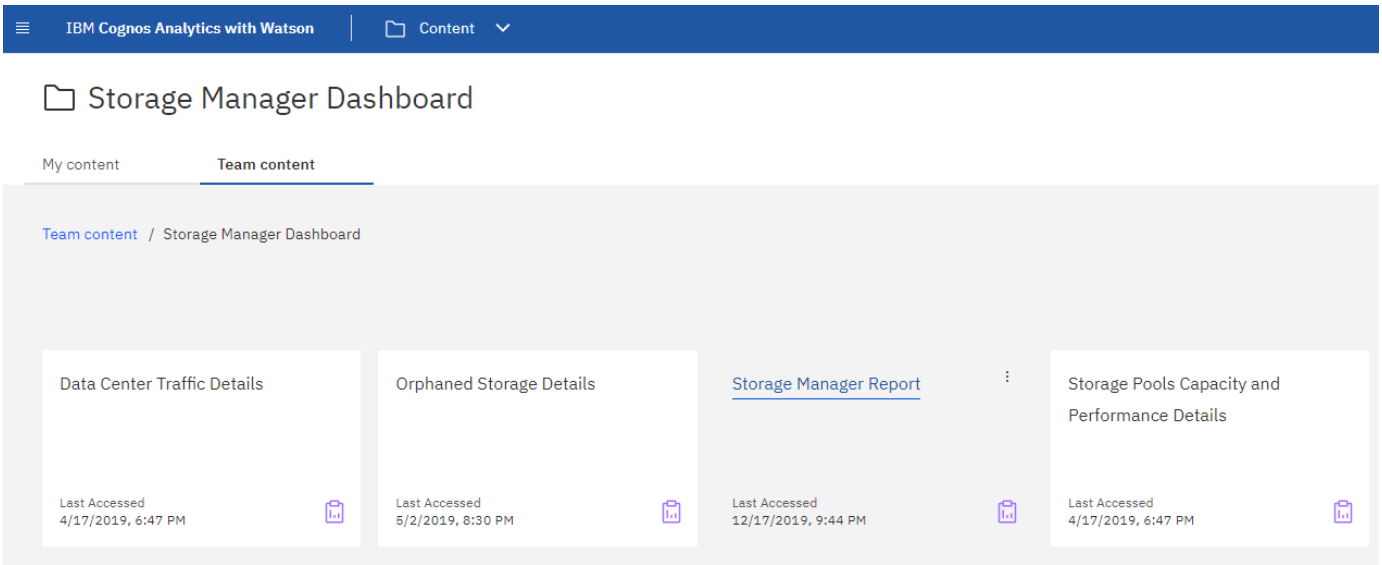
Storage Manager Dashboard

Das Storage Manager Dashboard bietet Ihnen eine zentrale Visualisierung, mit der Sie die Ressourcennutzung im Laufe der Zeit mit dem akzeptablen Bereich und den vorherigen Aktivitätstagen vergleichen und kontrastieren können. Wenn nur die wichtigsten Performance-Metriken für Ihre Storage-Services angezeigt werden, können Sie Entscheidungen zur Wartung Ihres Datacenters treffen.

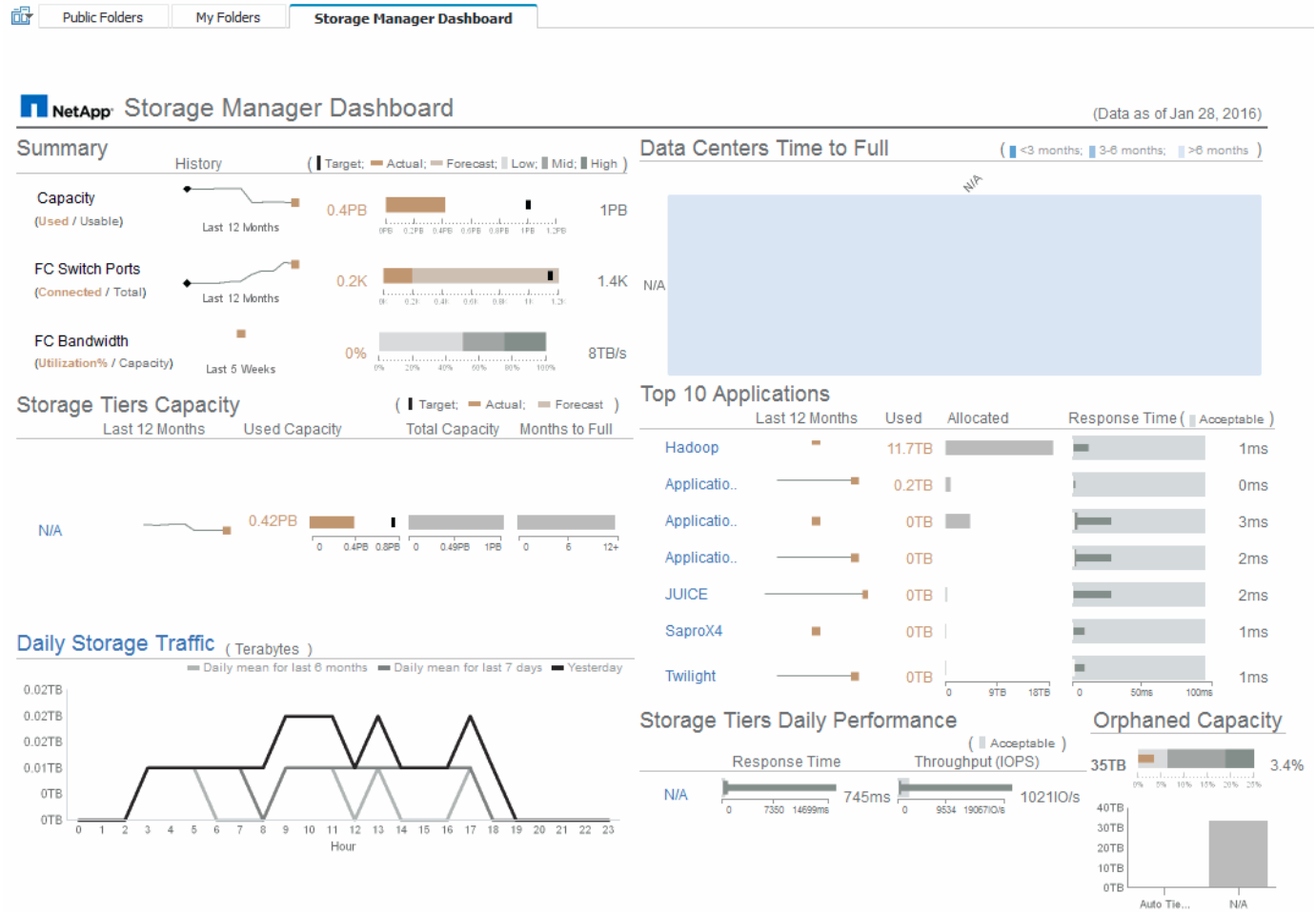
Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Zusammenfassung

Wenn Sie **Storage Manager Dashboard** aus Team Content auswählen, erhalten Sie mehrere Berichte, die Informationen über Ihren Datenverkehr und Ihren Speicher enthalten.



Der **Storage Manager Report** besteht aus sieben Komponenten, die Kontextinformationen zu vielen Aspekten Ihrer Speicherumgebung enthalten. Sie können die Aspekte Ihrer Storage-Services detailliert analysieren und einen Abschnitt, der für Sie am wichtigsten ist, analysieren.



Diese Komponente zeigt die genutzte im Vergleich zur nutzbaren Storage-Kapazität, die Switch-Ports insgesamt gegenüber der Anzahl der verbundenen Switch-Ports sowie die Gesamtauslastung des verbundenen Switch-Ports gegenüber der Bandbreite und die jeweiligen Trends im Laufe der Zeit an. Sie können die tatsächliche Auslastung im Vergleich zum niedrigen, mittleren und hohen Bereich anzeigen, sodass

Sie die Nutzung anhand eines Ziels vergleichen und einen Kontrast zwischen Projektionen und den gewünschten ist-Werten festlegen können. Für Kapazität und Switch Ports können Sie dieses Ziel konfigurieren. Die Prognose basiert auf einer Extrapolation der aktuellen Wachstumsrate und des festgelegten Datums. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, das Ziel überschreitet, wird neben der Kapazität eine Warnmeldung (roter Kreis) angezeigt.

Kapazität Des Storage-Tiers

Diese Komponente zeigt die genutzte Tier-Kapazität im Vergleich zur dem Tier zugewiesenen Kapazität. Dadurch wird angegeben, wie die genutzte Kapazität über einen Zeitraum von 12 Monaten erhöht oder verringert wird und wie viele Monate für die volle Kapazität übrig sind. Die Kapazitätsauslastung wird mit Werten für die tatsächliche Nutzung, die Nutzungsprognose und ein Ziel für die Kapazität angezeigt, die Sie konfigurieren können. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, die Zielkapazität überschreitet, wird neben einer Tier eine Warnmeldung (roter Kreis) angezeigt.

Sie können auf eine beliebige Ebene klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen, in dem freie Kapazitäten und nicht genutzte Kapazitäten, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier angezeigt werden. Sie können auch auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Täglicher Storage-Traffic

Diese Komponente zeigt die Performance der Umgebung, falls ein großes Wachstum, Änderungen oder potenzielle Probleme im Vergleich zu den vorangegangenen sechs Monaten auftreten. Es zeigt auch den durchschnittlichen Verkehr gegenüber dem Verkehr für die letzten sieben Tage, und für den Vortag. Sie können Anomalien in der Performance der Infrastruktur visualisieren, da sie Informationen liefert, die sowohl zyklische (vorherige sieben Tage) als auch saisonale Schwankungen (vorherige sechs Monate) hervorheben.

Sie können auf den Titel (täglicher Speicherverkehr) klicken, um den Bericht Speicherdatenverkehr anzuzeigen, der die Heatmap des stündlichen Speicherverkehrs für den Vortag für jedes Speichersystem anzeigt. Klicken Sie auf einen beliebigen Speichernamen in diesem Bericht, um die Seite „Anlage“ anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

Datacenter voll Zeit

Diese Komponente zeigt alle Datacenter im Vergleich zu allen Tiers und wie viel Kapazität für jeden Storage Tier verbleibt, basierend auf prognostizierten Wachstumsraten. Die Füllstandkapazität wird blau angezeigt. Je dunkler die Farbe ist, desto geringer ist die Zeit, die die Tier an der Position verlassen hat, bevor sie voll ist.

Sie können auf einen Abschnitt einer Ebene klicken, um den Bericht „Storage Pools Days to Full Details“ anzuzeigen. Dieser zeigt die Gesamtkapazität, die freie Kapazität und die Anzahl der Tage an, die für alle Pools in der ausgewählten Tier und im Datacenter voll werden sollen. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

Top 10 Applikationen

Diese Komponente zeigt die 10 wichtigsten Applikationen auf Grundlage der genutzten Kapazität an. Unabhängig davon, wie der Tier die Daten organisiert, werden in diesem Bereich die aktuelle Kapazität und der Anteil der Infrastruktur angezeigt. Sie können die Benutzerfreundlichkeit der letzten sieben Tage visualisieren, um zu sehen, ob der Verbraucher akzeptable (oder, was noch wichtiger ist, nicht akzeptable) Reaktionszeiten hat.

In diesem Bereich werden auch Trendanalysen angezeigt, die angeben, ob die Applikationen ihre Service Level Objectives (SLOs) hinsichtlich der Performance erfüllen. Sie können die Mindestreaktionszeit der letzten Woche, das erste Quartil, das dritte Quartil und die maximale Reaktionszeit anzeigen, wobei ein Median im Vergleich zu einer akzeptablen SLO angezeigt wird, die Sie konfigurieren können. Wenn die mittlere Antwortzeit für eine Applikation außerhalb des zulässigen SLO-Bereichs liegt, wird neben der Applikation ein Alarm (ein roter Kreis) angezeigt. Sie können auf eine Anwendung klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Storage Tiers Tägliche Performance

Diese Komponente zeigt eine Zusammenfassung der Performance der Tier für Reaktionszeit und IOPS für die letzten sieben Tage. Die Performance wird mit einer SLO verglichen, die Sie konfigurieren können. Dadurch sehen Sie, ob es Möglichkeiten gibt, die Storage Tiers zu konsolidieren, die von diesen Tiers bereitgestellten Workloads neu auszurichten oder Probleme mit bestimmten Tiers zu identifizieren. Wenn sich die mittlere Antwortzeit oder der mittlere IOPS außerhalb des akzeptablen SLO-Bereichs befindet, wird eine Warnmeldung (ein roter Kreis) neben einer Tier angezeigt.

Sie können auf einen Tier-Namen klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen. Er enthält Angaben zu freier und genutzter Kapazität, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

„Verlorene“ Kapazität

Diese Komponente zeigt die gesamte verwaiste Kapazität und verwaiste Kapazität je Tier. Sie wird verglichen mit einem akzeptablen Bereich für die gesamte nutzbare Kapazität und zeigt die tatsächliche verwaiste Kapazität an. Verwaiste Kapazität wird durch die Konfiguration und die Performance definiert. Der nach der Konfiguration verwaiste Storage beschreibt die Situation, in der einem Host Speicher zugewiesen ist. Die Konfiguration wurde jedoch nicht ordnungsgemäß ausgeführt, und der Host kann nicht auf den Speicher zugreifen. Diese Performance ist dann verwaist, wenn der Storage korrekt konfiguriert ist, damit ein Host auf sie zugreifen kann. Es gab jedoch keinen Lagerverkehr.

Der horizontale gestapelte Balken zeigt die zulässigen Bereiche an. Je dunkler das Grau ist, desto unannehmbarer ist die Situation. Die tatsächliche Situation wird mit dem schmalen Bronzebalken angezeigt, der die tatsächliche verwaiste Kapazität anzeigt.

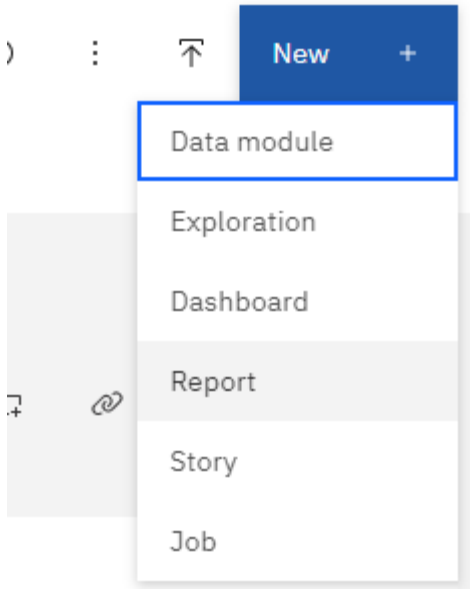
Sie können auf eine Tier klicken, um den Bericht „Verlorene Storage-Details“ anzuzeigen. In diesem Bericht werden alle Volumes angezeigt, die nach Konfiguration und Performance der ausgewählten Tier als „verwaist“ identifiziert wurden. Klicken Sie in diesem Bericht auf eine beliebige Ablage, einen Speicherpool oder ein beliebiges Volume, um die Seite „Asset“ anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Erstellen eines Berichts (Beispiel)

Erstellen Sie anhand der Schritte in diesem Beispiel einen einfachen Bericht zur physischen Kapazität von Storage- und Speicherpools in verschiedenen Datacentern.

Schritte

1. Navigieren Sie zu **Menü > Inhalt > Teaminhalt > Berichte**
2. Wählen Sie oben rechts im Bildschirm **[Neu +]** aus
3. Wählen Sie **Bericht**



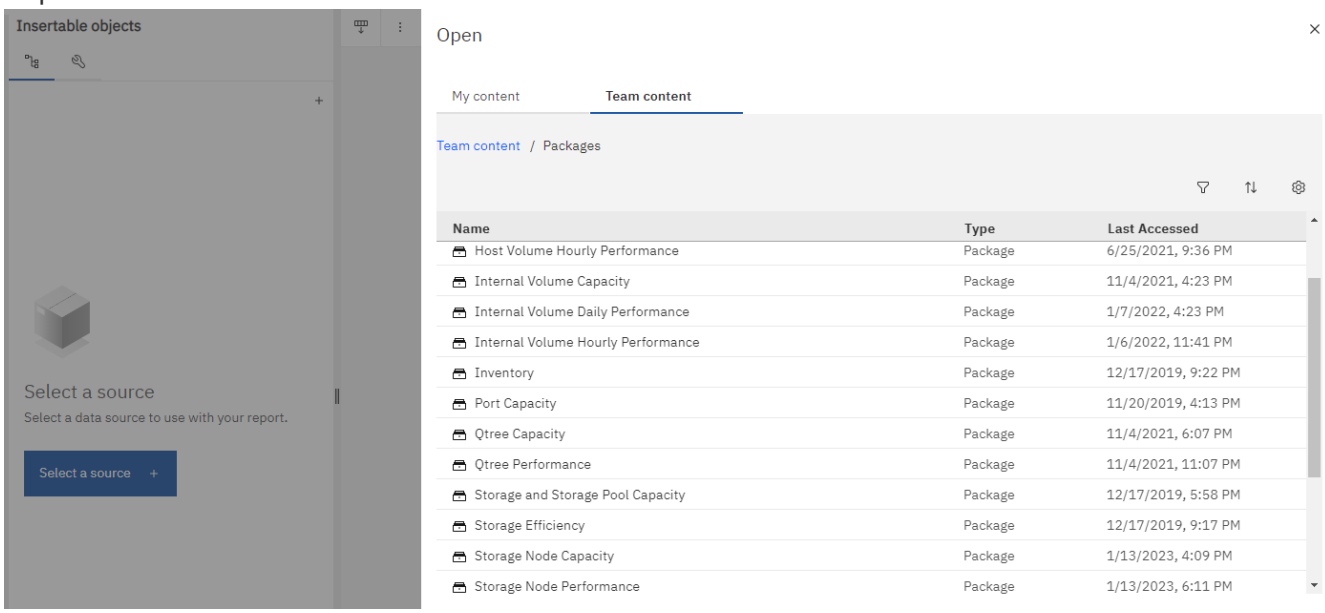
4. Wählen Sie auf der Registerkarte **Templates** die Option *leer*

   Die Registerkarte „Quelle und Daten“ wird angezeigt

5. Öffnen **Quelle auswählen +**
6. Öffnen Sie unter **Team content Packages**

   Eine Liste der verfügbaren Pakete wird angezeigt.

7. Wählen Sie *Speicher- und Speicherpool-Kapazität*



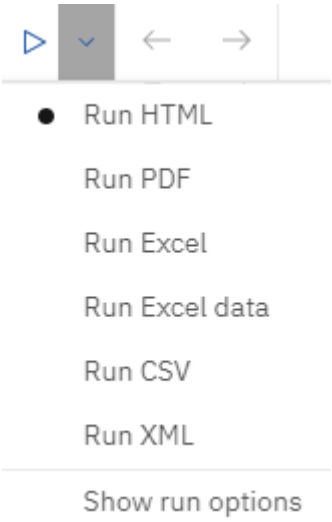
8. Wählen Sie * Öffnen*

   Die verfügbaren Stile für Ihren Bericht werden angezeigt.

9. Wählen Sie **Liste**

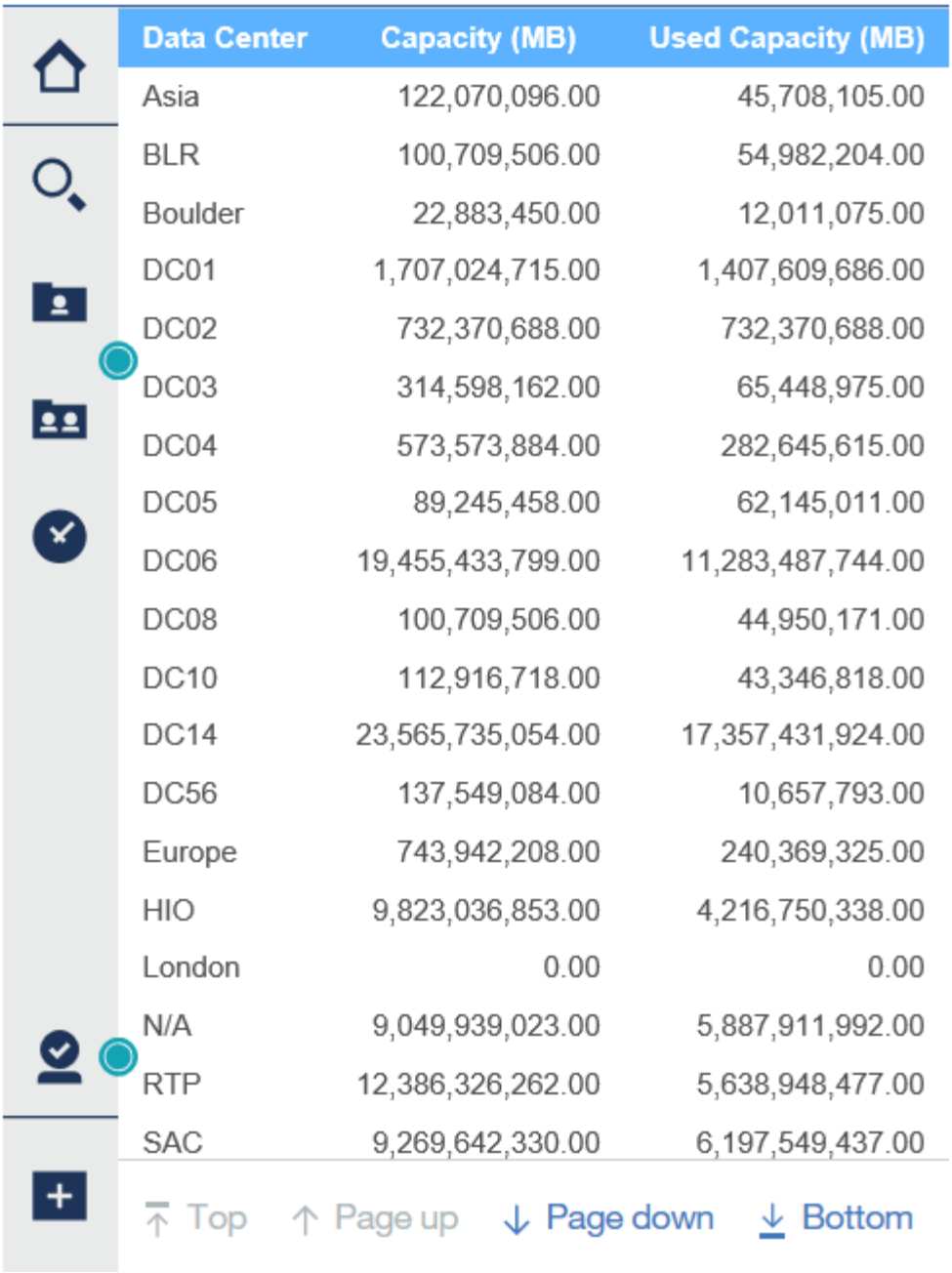
   Fügen Sie entsprechende Namen für Liste und Abfrage hinzu

10. Wählen Sie **OK**
11. Erweiterung_Physische Kapazität_
12. Erweitern Sie das System auf die unterste Ebene *Data Center*
13. Ziehen Sie *Data Center* zum Reporting-Gaumen.
14. Erweitern Sie *Capacity (MB)*
15. Ziehen Sie *Kapazität (MB)* zum Berichtspaue.
16. Ziehen Sie *genutzte Kapazität (MB)* zum Berichtsausgang.
17. Führen Sie den Bericht durch, indem Sie einen Ausgabetyp aus dem Menü **Ausführen** auswählen.



Ergebnis

Ein Bericht wie der folgende wird erstellt:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Verwalten Von Berichten

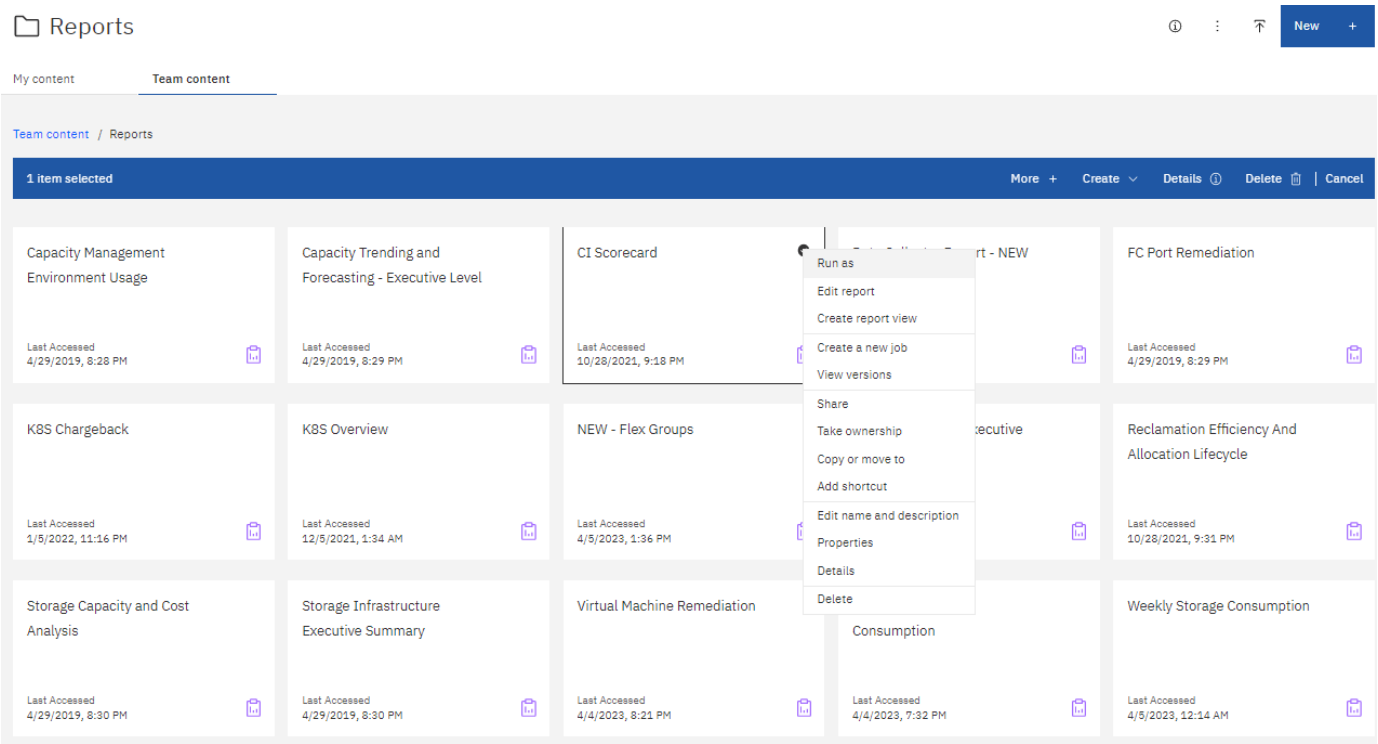
Sie können das Ausgabeformat und die Ausgabe eines Berichts anpassen, Berichteigenschaften oder Zeitpläne festlegen und E-Mail-Berichte erstellen.

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Anpassen des Ausgabeformats und der Bereitstellung eines Berichts

Sie können das Format und die Bereitstellungsmethode von Berichten anpassen.

1. Gehen Sie im Cloud Insights-Berichtsportal zu **Menü > Inhalt > eigene Inhalte/Teaminhalte**. Bewegen Sie die Maus über den Bericht, den Sie anpassen möchten, und öffnen Sie das Menü „drei Punkte“.

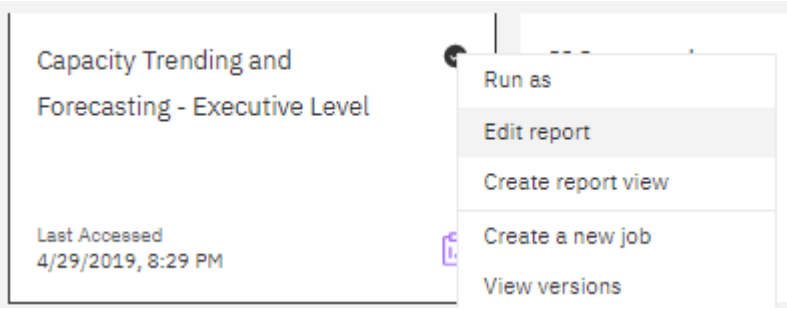


1. Klicken Sie Auf **Eigenschaften > Zeitplan**
2. Sie können folgende Optionen festlegen:
   - **Zeitplan**, wenn Sie Berichte ausführen möchten.
   - Wählen Sie **Optionen** für Berichtformat und -Zustellung (Speichern, Drucken, E-Mail) und Sprachen für den Bericht.
3. Klicken Sie auf **Speichern**, um den Bericht anhand der von Ihnen getroffenen Auswahl zu erstellen.

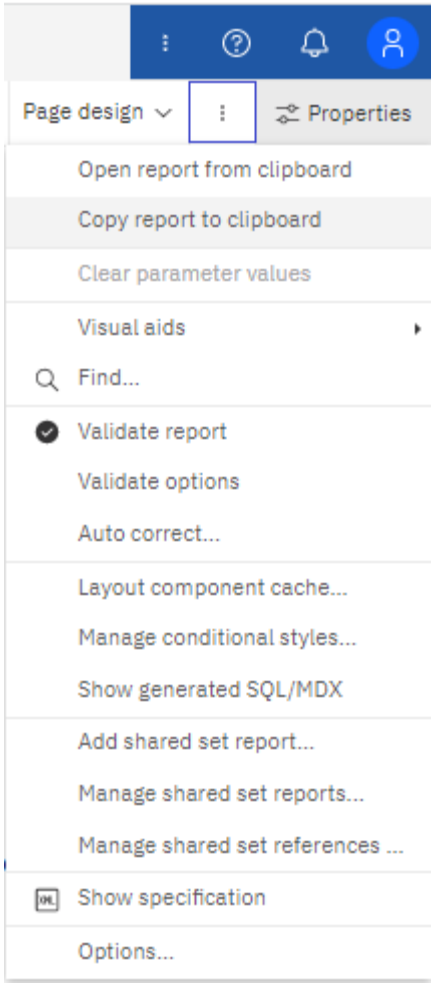
Kopieren eines Berichts in die Zwischenablage

Verwenden Sie diesen Vorgang, um einen Bericht in die Zwischenablage zu kopieren.

1. Wählen Sie einen zu kopierenden Bericht aus (**Menü > Inhalt > Mein Inhalt oder Teaminhalt**)
2. Wählen Sie im Dropdown-Menü des Berichts die Option *Report bearbeiten*



3. Öffnen Sie oben rechts auf dem Bildschirm das Menü „drei Punkte“ neben „Eigenschaften“.
4. Wählen Sie **Bericht in Zwischenablage kopieren**.

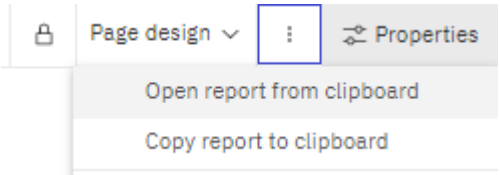


Öffnen von Berichten aus der Zwischenablage

Sie können eine Berichtsspezifikation öffnen, die zuvor in die Zwischenablage kopiert wurde.

Über diese Aufgabe Erstellen Sie zunächst einen neuen Bericht oder öffnen Sie einen vorhandenen Bericht, den Sie durch den kopierten Bericht ersetzen möchten. Die folgenden Schritte gelten für einen neuen Bericht.

1. Wählen Sie **Menü > +Neu > Bericht** und erstellen Sie einen leeren Bericht.
2. Öffnen Sie oben rechts auf dem Bildschirm das Menü „drei Punkte“ neben „Eigenschaften“.
3. Wählen Sie **Bericht aus Zwischenablage öffnen**.



1. Fügen Sie den kopierten Code in das Fenster ein und wählen Sie **OK**.
2. Wählen Sie das Diskettensymbol, um den Bericht zu speichern.
3. Wählen Sie, wo der Bericht gespeichert werden soll (*My Content*, *Team Content*, oder erstellen Sie einen neuen Ordner).
4. Geben Sie dem neuen Bericht einen aussagekräftigen Namen und wählen Sie **Speichern**.

Bearbeiten eines vorhandenen Berichts

Beachten Sie, dass die Bearbeitung von Dateien am Standardspeicherort das Risiko birgt, dass diese Berichte bei der nächsten Aktualisierung des Berichtkatalogs überschrieben werden. Es wird empfohlen, den bearbeiteten Bericht unter einem neuen Namen zu speichern oder an einem nicht standardmäßigen Speicherort zu speichern.

Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Problemen mit der Berichterstattung.

Problem:	Teste das:
Bei der Planung eines Berichts, der per E-Mail versendet werden soll, wird der Name des angemeldeten Benutzers im Feld „an“ der E-Mail vorausgefüllt. Der Name ist jedoch in der Form von "Vorname Nachname" (Vorname, Leerzeichen, Nachname). Da es sich hierbei nicht um eine gültige E-Mail-Adresse handelt, wird die E-Mail nicht gesendet, wenn der geplante Bericht ausgeführt wird.	Löschen Sie bei der Planung des zu sendenden Berichts per E-Mail den vorausgefüllten Namen und geben Sie eine gültige, korrekt formatierte E-Mail-Adresse in das Feld „To“ ein.

Erstellen Von Benutzerdefinierten Berichten

Sie können die Tools zur Erstellung benutzerdefinierter Berichte verwenden. Nachdem Sie Berichte erstellt haben, können Sie sie speichern und regelmäßig ausführen. Die Ergebnisse der Berichte können automatisch per E-Mail an sich selbst und andere gesendet werden.

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Die Beispiele in diesem Abschnitt veranschaulichen den folgenden Prozess, der für jedes der Cloud Insights-Berichtsdatenmodelle verwendet werden kann:

- Ermitteln einer Frage, die mit einem Bericht beantwortet werden soll
- Ermitteln der für die Ergebnisse erforderlichen Daten
- Auswählen von Datenelementen für den Bericht

Bevor Sie Ihren benutzerdefinierten Bericht erstellen, müssen Sie einige erforderliche Aufgaben ausführen. Wenn Sie diese nicht ausfüllen, können die Berichte ungenau oder unvollständig sein.

Wenn Sie beispielsweise den Gerätekennungsprozess nicht abschließen, sind die Kapazitätsberichte nicht korrekt. Oder, wenn Sie die Einrichtung von Annotationen (wie z. B. Tiers, Geschäftsbereiche und Datacenter) nicht abschließen, werden in Ihren individuellen Berichten möglicherweise keine Daten aus der gesamten Domäne genau gemeldet oder „N/A“ für einige Datenpunkte angezeigt.

Bevor Sie Ihre Berichte entwerfen, führen Sie die folgenden Aufgaben aus:

- Alle konfigurieren "Datensammler" Richtig.
- Geben Sie Annotationen (z. B. Tiers, Datacenter und Geschäftsbereiche) auf Geräten und Ressourcen in Ihrer Umgebung ein. Da Cloud Insights Reporting historische Daten erfasst, ist es vorteilhaft, Anmerkungen vor der Berichterstellung stabil zu lassen.

Berichtserstellung

Der Prozess der Erstellung benutzerdefinierter (auch als „Ad-hoc“ bezeichnet) Berichte umfasst mehrere Aufgaben:

- Planen Sie die Ergebnisse Ihres Berichts.
- Daten identifizieren, um Ergebnisse zu unterstützen
- Wählen Sie das Datenmodell aus (z. B. Chargeback-Datenmodell, Bestandsdatenmodell usw.), das die Daten enthält.
- Datenelemente für den Bericht auswählen.
- Optional können Sie Berichtsergebnisse formatieren, sortieren und filtern.

Planen der Ergebnisse Ihres benutzerdefinierten Berichts

Bevor Sie die Tools zur Erstellung von Berichten öffnen, sollten Sie die gewünschten Ergebnisse aus dem Bericht planen. Mit den Tools zur Erstellung von Berichten können Sie problemlos Berichte erstellen und benötigen möglicherweise keine umfangreiche Planung. Es ist jedoch sinnvoll, den Berichtsinfragesteller zu den Berichtanforderungen zu verstehen.

- Geben Sie die genaue Frage an, die Sie beantworten möchten. Beispiel:
  - Wie viel Kapazität habe ich noch übrig?
  - Wie hoch sind die Kosten für die Rückberechnung pro Geschäftsbereich?
  - Wie groß ist die Kapazität je Tier, um sicherzustellen, dass die Geschäftsbereiche auf die richtige Storage-Tier ausgerichtet sind?
  - Wie kann ich einen Strom- und Kühlungsbedarf vorhersagen? (Fügen Sie benutzerdefinierte Metadaten durch Hinzufügen von Annotationen zu Ressourcen hinzu.)
- Ermitteln Sie die Datenelemente, die Sie zur Unterstützung der Antwort benötigen.
- Identifizieren Sie die Beziehungen zwischen Daten, die in der Antwort angezeigt werden sollen. Nehmen Sie keine unlogischen Beziehungen in Ihre Frage auf, zum Beispiel: „Ich möchte die Ports sehen, die sich auf die Kapazität beziehen.“
- Ermitteln der für Daten erforderlichen Berechnungen
- Bestimmen Sie, welche Filtertypen erforderlich sind, um die Ergebnisse zu begrenzen.
- Bestimmen, ob aktuelle oder historische Daten verwendet werden müssen.
- Legen Sie fest, ob Sie Zugriffsberechtigungen für Berichte festlegen müssen, um die Daten auf bestimmte Zielgruppen zu beschränken.
- Ermitteln Sie, wie der Bericht verteilt werden soll. Sollte er beispielsweise per E-Mail an einen festgelegten Zeitplan gesendet oder im Bereich „Team Content Folder“ enthalten sein?
- Bestimmen Sie, wer den Bericht verwalten soll. Dies kann sich auf die Komplexität des Designs auswirken.
- Erstellen Sie ein Modell des Berichts.

Tipps für das Design von Berichten

Bei der Erstellung von Berichten sind einige Tipps hilfreich.

- Legen Sie fest, ob Sie aktuelle oder historische Daten verwenden müssen.

  Die meisten Berichte müssen nur über die neuesten Daten berichten, die in der Cloud Insights verfügbar

sind.

- Cloud Insights-Berichte liefern zwar Verlaufsdaten zu Kapazität und Performance, jedoch nicht zum Inventar.
- Jeder sieht alle Daten, aber möglicherweise müssen Sie die Daten auf bestimmte Zielgruppen beschränken.

  Um die Informationen für verschiedene Benutzer zu segmentieren, können Sie Berichte erstellen und Zugriffsberechtigungen für sie festlegen.

Reporting-Datenmodelle

Cloud Insights umfasst mehrere Datenmodelle, aus denen Sie entweder vordefinierte Berichte auswählen oder Ihren eigenen benutzerdefinierten Bericht erstellen können.

Jedes Datenmodell enthält einen einfachen Data Marts und einen erweiterten Data Marts:

- Der einfache Data Mart bietet schnellen Zugriff auf die am häufigsten verwendeten Datenelemente und enthält nur den letzten Snapshot der Data Warehouse-Daten, enthält keine Verlaufsdaten.
- Der erweiterte Data Marts stellt alle Werte und Details zur Verfügung, die über den einfachen Data Marts verfügbar sind, und bietet Zugriff auf historische Datenwerte.

Kapazitätsdatenmodelle

Mit können Sie Fragen zur Storage-Kapazität, Auslastung des Filesystems, zur internen Volume-Kapazität, Port-Kapazität, qtree-Kapazität, beantworten. Und Kapazität von Virtual Machines (VMs). Das Kapazitätsdatenmodell ist ein Container für mehrere Kapazitätsmodelle. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen beantworten:

Modell für Storage- und Storage-Pool-Kapazitätsdaten

Ermöglicht das Antworten auf Fragen zur Ressourcenplanung von Storage-Kapazitäten, einschließlich Storage- und Storage-Pools, und umfasst sowohl physische als auch virtuelle Storage-Pool-Daten. Dieses einfache Datenmodell unterstützt Sie bei der Beantwortung von Fragen hinsichtlich Kapazität im Boden und der Kapazitätsauslastung von Storage-Pools nach Tier und Datacenter im Laufe der Zeit. Neue Kapazitätsberichte sind die Basis für ein Datenmodell, da es sich um ein einfacheres, zielgerichtetes Datenmodell handelt. Sie können Fragen wie die folgenden beantworten, indem Sie dieses Datenmodell verwenden:

- Welches ist der voraussichtliche Termin für die Erreichung der Kapazitätsgrenze von 80 % meines physischen Storage?
- Wie hoch ist die physische Storage-Kapazität auf einem Array für eine bestimmte Tier?
- Wie groß ist meine Speicherkapazität nach Hersteller und Familie sowie nach Rechenzentrum?
- Welchen Trend geht zur Storage-Auslastung bei einem Array für alle Tiers?
- Welches sind meine 10 wichtigsten Storage-Systeme bei höchster Auslastung?
- Wie sieht der Trend zur Storage-Auslastung der Storage Pools aus?
- Wie viel Kapazität ist bereits zugewiesen?
- Welche Kapazität ist für die Zuweisung verfügbar?

Datenmodell für die Dateisystemauslastung

Dieses Datenmodell bietet eine Übersicht über die Kapazitätsauslastung durch Hosts auf Filesystem-Ebene. Administratoren können zugewiesene und genutzte Kapazität pro Filesystem ermitteln, den Typ des Filesystems festlegen und Trendstatistiken nach Filesystem-Typ ermitteln. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

- Wie groß ist das Filesystem?
- Wo sind die Daten aufbewahrt und wie wird auf sie zugegriffen, z. B. lokal oder SAN?
- Was sind historische Trends für die Kapazität des Filesystems? Und was können wir dann, basierend auf diesen, für zukünftige Anforderungen erwarten?

Internes Datenmodell für die Volume-Kapazität

Hier können Sie Fragen zur verwendeten Kapazität des internen Volume, zu der zugewiesenen Kapazität und zur Kapazitätsauslastung beantworten:

- Welche internen Volumes haben eine Auslastung über einem vordefinierten Schwellenwert?
- Welche internen Volumes besteht in der Gefahr, dass die Kapazität aufgrund von Trends nicht mehr verfügbar ist? 8 welche Kapazität wird genutzt im Vergleich zur zugewiesenen Kapazität bei unseren internen Volumes?

Datenmodell für Port-Kapazität

Mit dieser Option können Sie Fragen zu Switch-Port-Konnektivität, Portstatus und Portgeschwindigkeit im Laufe der Zeit beantworten. Sie können folgende Fragen beantworten, um Ihnen beim Kauf neuer Switches zu helfen: Wie kann ich eine Prognose zum Portverbrauch erstellen, die die Verfügbarkeit von Ressourcen (Ports) prognostiziert (je nach Rechenzentrum, Switch-Anbieter und Port-Geschwindigkeit)?

- Welche Ports werden wahrscheinlich zu Kapazitätsknapp, wenn es um Datengeschwindigkeit, Datacenter, Anbieter und Anzahl der Host- und Storage-Ports geht?
- Welche Trends haben die Switch-Port-Kapazität im Laufe der Zeit?
- Welche Port-Geschwindigkeiten werden verwendet?
- Welche Art von Port-Kapazität ist erforderlich und welches Unternehmen wird gerade dabei sein, einen bestimmten Port-Typ oder einen bestimmten Anbieter zu nutzen?
- Wie lange kann diese Kapazität optimal erworben und verfügbar gemacht werden?

Datenmodell für qtree Kapazität

Ermöglicht die Trend-Nutzung von qtree (mit Daten wie genutzter bzw. zugewiesener Kapazität) im Laufe der Zeit. Sie können die Informationen nach verschiedenen Dimensionen anzeigen, beispielsweise nach Geschäftseinheit, Applikation, Ebene und Service Level. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

- Wie hoch ist die genutzte Kapazität von qtrees im Vergleich zu den Limits, die pro Applikation oder Geschäftseinheit gesetzt werden?
- Welche Trends haben wir bei unserer genutzten und freien Kapazität, sodass wir Kapazitäten planen können?
- Welche Geschäftseinheiten nutzen die größte Kapazität?
- Welche Applikationen belegen die größte Kapazität?

Datenmodell für VM-Kapazität

Ermöglicht Ihnen, Berichte über Ihre virtuelle Umgebung und deren Kapazitätsauslastung zu erstellen. Mit diesem Datenmodell können Sie Änderungen des Kapazitätsverbrauchs über die Zeit für VMs und Datenspeicher berichten. Das Datenmodell bietet außerdem Thin Provisioning und Chargeback-Daten für Virtual Machines.

- Wie kann ich das Kapazitätszuordnungsberechnung basierend auf der Kapazität bestimmen, die für VMs und Datenspeicher bereitgestellt wird?
- Welche Kapazitäten werden nicht von VMs genutzt, und welcher Anteil ungenutzte Kapazitäten ist frei, verwaist oder anderer?
- Welche Anschaffungen müssen wir anhand von Verbrauchstrends erwerben?
- Wie hoch sind meine Storage-Effizienzeinsparungen durch Storage Thin Provisioning und Deduplizierungstechnologien?

Die Kapazitäten im VM-Kapazitätsdatenmodell werden von virtuellen Festplatten (VMDKs) genutzt. Das bedeutet, dass die bereitgestellte Größe einer VM mit dem VM-Kapazitätsdatenmodell die Größe der virtuellen Festplatten entspricht. Dies unterscheidet sich von der bereitgestellten Kapazität in der Ansicht Virtual Machines in Cloud Insights, die die bereitgestellte Größe für die VM selbst anzeigt.

Datenmodell für Volume-Kapazität

Ermöglicht die Analyse sämtlicher Volumes in Ihrer Umgebung und die Organisation von Daten nach Anbieter, Modell, Tier, Service Level und Datacenter.

Sie können die Kapazität für verwaiste Volumes, ungenutzte Volumes und Datensicherungs-Volumes (zur Replizierung genutzt) anzeigen. Außerdem können Sie unterschiedliche Volume-Technologien (iSCSI oder FC) sehen und virtuelle Volumes mit nicht-virtuellen Volumes vergleichen, um Probleme bei der Array-Virtualisierung zu beheben.

Sie können Fragen wie die folgenden mit diesem Datenmodell beantworten:

- Welche Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Welchen Trend geht in meinem Datacenter hinsichtlich verwaister Volume-Kapazität?
- Wie viel meiner Datacenter-Kapazität ist virtualisiert oder Thin Provisioning?
- Wie viel meiner Datacenter-Kapazität muss für die Replizierung reserviert werden?

Modell für die Kostenzuordnung

Ermöglicht das Antworten auf Fragen zur genutzten Kapazität und zugewiesenen Kapazität in Storage-Ressourcen (Volumes, interne Volumes und qtrees). Dieses Datenmodell liefert Informationen zur Kostenverrechnung und Transparenz der Storage-Kapazität nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein. Berichtsdaten können nach Service Level und Storage Tier kategorisiert werden.

Sie können dieses Datenmodell verwenden, um Berichte zur Rückberechnung zu erstellen, indem Sie die Menge an Kapazität ermitteln, die von einer Geschäftseinheit verwendet wird. Dieses Datenmodell ermöglicht Ihnen die Erstellung einheitlicher Berichte für verschiedene Protokolle (einschließlich NAS, SAN, FC und iSCSI).

- Bei Storage ohne interne Volumes werden Berichte zur Kostenverrechnung nach Volumes angezeigt.
- Zur Speicherung mit internen Volumes:

- Wenn den Volumes Geschäftseinheiten zugewiesen sind, werden Chargeback-Berichte nach Volumes angezeigt.
- Wenn Geschäftseinheiten nicht Volumes zugewiesen, aber qtrees zugewiesen sind, werden Chargeback-Berichte durch qtrees angezeigt.
- Wenn Geschäftseinheiten nicht Volumes zugewiesen und nicht qtrees zugewiesen sind, wird das interne Volume durch Chargeback-Berichte angezeigt.
- Die Entscheidung, ob die Kostenzuordnung nach Volume, qtree oder internem Volume angezeigt werden soll, wird für jedes interne Volume getroffen. Somit ist es möglich, dass verschiedene interne Volumes im selben Storage Pool die Chargeback auf verschiedenen Ebenen zur Verfügung stehen.

Kapazitätfakten werden nach einem Standard-Zeitintervall gelöscht. Weitere Informationen finden Sie unter Data Warehouse-Prozesse.

Berichte, die das Chargeback-Datenmodell verwenden, können unter Umständen unterschiedliche Werte als Berichte mit dem Speicherkapazitätsdatenmodell anzeigen.

- Bei Storage Arrays, die keine NetApp Storage-Systeme sind, bleiben die Daten beider Datenmodelle gleich.
- Bei Storage-Systemen von NetApp und Celerra verwendet das Chargeback-Datenmodell eine einzelne Schicht (von Volumes, internen Volumes oder qtrees), um die Gebühren zu senken. Das Storage-Kapazitätsdatenmodell nutzt dagegen mehrere Schichten (von Volumes und internen Volumes), um ihre Gebühren zu sichern.

Bestandsdatenmodell

Mit Hilfe von Antworten auf Fragen zu Bestandsressourcen, einschließlich Hosts, Speichersystemen, Switches, Festplatten, Tapes Qtrees, Quotas, Virtual Machines und Server sowie generische Geräte. Das Bestandsdatenmodell enthält mehrere Unterverzeichnis, mit denen Sie Informationen zu Replikationen, FC-Pfaden, iSCSI-Pfaden, NFS-Pfaden und Verstößen anzeigen können. Das Bestandsdatenmodell enthält keine historischen Daten. Fragen, die Sie mit diesen Daten beantworten können

- Welche Assets habe ich und wo sind sie?
- Wer nutzt die Ressourcen?
- Welche Gerätetypen habe ich und welche Komponenten sind diese Geräte?
- Wie viele Hosts je Betriebssystem habe ich und wie viele Ports sind auf diesen Hosts vorhanden?
- Welche Storage-Arrays pro Anbieter gibt es in den einzelnen Datacentern?
- Über wie viele Switches je Anbieter verfügt ich in jedem Datacenter?
- Wie viele Ports sind nicht lizenziert?
- Welche Anbieter-Tapes verwenden wir und wie viele Ports sind auf jedem Tape vorhanden? Re alle generischen Geräte, die identifiziert wurden, bevor wir mit der Arbeit an Berichten beginnen?
- Welche Pfade sind zwischen den Hosts und Storage Volumes oder Tapes?
- Welche Pfade gibt es zwischen generischen Geräten und Speicher-Volumes oder Bändern?
- Wie viele Verstöße gegen die einzelnen Typen gibt es pro Datacenter?
- Was sind die Quell- und Ziel-Volumes für jedes replizierte Volume?
- Erhalte ich Firmware-Inkompatibilitäten oder falsche Portgeschwindigkeiten zwischen Fibre Channel Host HBAs und Switches?

Performance-Datenmodell

Antworten auf Fragen zur Performance von Volumes, Applikations-Volumes, internen Volumes, Switches, Applikationen VMs, VMDKs, ESX und VM, Hosts und Applikations-Nodes. Viele dieser Berichte *hourly* Daten, *Daily* Daten oder beides. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen zum Performance-Management beantworten:

- Auf welche Volumes oder internen Volumes wurde in einem bestimmten Zeitraum nicht zugegriffen?
- Können wir mögliche Fehlkonfigurationen beim Storage für eine (nicht verwendete) Applikation ermitteln?
- Wie sieht das Zugriffsverhalten einer Applikation insgesamt aus?
- Werden für eine bestimmte Applikation entsprechend Tiered Volumes zugewiesen?
- Könnten wir für eine Applikation, die derzeit läuft, einen günstigeren Storage nutzen, ohne die Applikations-Performance zu beeinträchtigen?
- Welche Applikationen bieten mehr Zugriffe auf den derzeit konfigurierten Storage?

Wenn Sie die Switch-Leistungstabellen verwenden, können Sie folgende Informationen abrufen:

- Ist mein Host-Verkehr durch verbundene Ports ausgeglichen?
- Welche Switches oder Ports weisen eine hohe Anzahl an Fehlern auf?
- Welche Switches werden am häufigsten an der Port-Performance verwendet?
- Welche nicht ausgelasteten Switches basieren auf der Port-Performance?
- Welcher Durchsatz beim Trending des Hosts basiert auf der Port-Performance?
- Wie hoch ist die Performance-Auslastung der letzten X Tage für einen angegebenen Host, ein Storage-System, ein Tape oder Switch?
- Welche Geräte erzeugen Datenverkehr auf einem bestimmten Switch (z. B. welche Geräte sind für den Einsatz eines stark genutzten Switches verantwortlich)?
- Wie hoch ist der Durchsatz für einen bestimmten Geschäftsbereich in unserer Umgebung?

Wenn Sie die Tabellen zur Festplatten-Performance verwenden, erhalten Sie folgende Informationen:

- Wie ist der Durchsatz für einen angegebenen Storage-Pool auf Basis von Festplatten-Performance-Daten?
- Was ist der am höchsten genutzte Storage-Pool?
- Wie hoch ist die durchschnittliche Festplattenauslastung für einen bestimmten Storage?
- Was ist der Trend zur Nutzung eines Storage-Systems oder eines Storage-Pools basierend auf den Festplatten-Performance-Daten?
- Wie sieht der Trend zur Festplattennutzung für einen bestimmten Storage Pool aus?

Wenn Sie VM- und VMDK-Performance-Tabellen verwenden, erhalten Sie folgende Informationen:

- Arbeitet meine virtuelle Umgebung mit optimaler Performance?
- Welche VMDKs stellen die höchsten Workloads dar?
- Wie kann ich die von VMDs gemeldete Performance bei verschiedenen Datastores nutzen, um Entscheidungen zum Re-Tiering zu treffen.

Das Performance-Datenmodell enthält Informationen, mit denen Sie die Angemessenheit von Tiers, Storage-Fehlkonfigurationen für Applikationen und die letzten Zugriffszeiten von Volumes und internen Volumes ermitteln können. Dieses Datenmodell bietet Daten wie Reaktionszeiten, IOPS, Durchsatz, Anzahl der

ausstehenden Schreibvorgänge und den Status des Datenzugriffs.

Storage-Effizienz-Datenmodell

Nachverfolgung des Storage-Effizienz-Ergebnisses und des Potenzials im Laufe der Zeit Dieses Datenmodell speichert Messungen nicht nur der bereitgestellten Kapazität, sondern auch der genutzten oder verbrauchten Menge (der physischen Messung). Wenn beispielsweise Thin Provisioning aktiviert ist, gibt Cloud Insights an, wie viel Kapazität das Gerät benötigt. Mithilfe dieses Modells lässt sich außerdem die Effizienz bei aktivierter Deduplizierung bestimmen. Sie können verschiedene Fragen mithilfe des Storage-Effizienz-Data Marts beantworten:

- Wie hoch sind unsere Storage-Effizienzeinsparungen als Ergebnis der Implementierung von Thin Provisioning und Deduplizierungstechnologien?
- Wie hoch sind die Storage-Einsparungen in den gesamten Datacentern?
- Wann müssen wir, basierend auf Trends bei früheren Kapazitäten, zusätzlichen Storage erwerben?
- Was würde der Kapazitätsgewinn bedeuten, wenn wir Technologien wie Thin Provisioning und Deduplizierung aktivieren würden?
- Sind Sie hinsichtlich der Storage-Kapazität aktuell in Gefahr?

Daten-Modell-Fakt- und Bemaßungstabellen

Jedes Datenmodell enthält Fakt- und Bemaßungstabellen.

- Fact-Tabellen: Enthalten Daten, die gemessen werden, z. B. Menge, Rohkapazität und nutzbare Kapazität. Fremdschlüssel in Bemaßungstabellen enthalten.
- Bemaßungstabellen: Enthalten beschreibende Informationen zu Fakten, beispielsweise Datacenter und Geschäftseinheiten. Eine Dimension ist eine Struktur, die häufig aus Hierarchien besteht, die Daten kategorisiert. Maßattribute helfen, die Maßwerte zu beschreiben.

Mithilfe verschiedener oder mehrerer Bemaßungsattribute (siehe Spalten in den Berichten) erstellen Sie Berichte, die für jede im Datenmodell beschriebene Dimension auf Daten zugreifen.

Farben, die in Datenmodellelementen verwendet werden

Farben auf Datenmodellelementen haben unterschiedliche Indikationen.

- Gelbe Werte: Stellen Messungen dar.
- Nicht-gelbe Werte: Repräsentieren Attribute. Diese Werte aggregieren nicht.

Verwenden mehrerer Datenmodelle in einem Bericht

Normalerweise verwenden Sie ein Datenmodell pro Bericht. Sie können jedoch einen Bericht schreiben, in dem Daten aus mehreren Datenmodellen kombiniert werden.

Um einen Bericht zu schreiben, der Daten aus mehreren Datenmodellen zusammenfasst, wählen Sie eines der Datenmodelle aus, die als Basis verwendet werden sollen, und schreiben Sie dann SQL-Abfragen, um auf die Daten der zusätzlichen Datentabellen zuzugreifen. Sie können die SQL-Join-Funktion verwenden, um die Daten aus den verschiedenen Abfragen in einer einzigen Abfrage zu kombinieren, mit der Sie den Bericht schreiben können.

Beispielsweise möchten Sie die aktuelle Kapazität für jedes Storage Array bereitstellen und benutzerdefinierte Anmerkungen zu den Arrays erfassen. Sie können den Bericht mithilfe des Datenmodells für die Storage-Kapazität erstellen. Sie können die Elemente aus den Tabellen „Aktuelle Kapazität und Dimension“ verwenden

und eine separate SQL-Abfrage hinzufügen, um auf die Annotationsinformationen im Bestandsdatenmodell zuzugreifen. Abschließend können Sie die Daten kombinieren, indem Sie die Bestandsspeicherdaten mit der Tabelle Speicherdimension verknüpfen, indem Sie den Speichernamen und die Kriterien für den Beitritt verwenden.

Greifen Sie über die API auf die Berichtsdatenbank zu

Mit der leistungsstarken API von Cloud Insights können Benutzer die Cloud Insights Reporting-Datenbank direkt abfragen, ohne über die Cognos Reporting-Umgebung zu gehen.

> Diese Dokumentation bezieht sich auf die Cloud Insights-Berichtsfunktion, die in der Cloud Insights Premium Edition verfügbar ist.

Odata

Die Cloud Insights-Reporting-API folgt der "OData v4" (Open Data Protocol)-Standard für die Abfrage der Reporting-Datenbank. Weitere Informationen finden Sie unter "Dieses Lernprogramm" Zu OData.

Alle Anfragen beginnen mit der url *https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata*

APIKey wird generiert

Weitere Informationen "Cloud Insights APIs".

Gehen Sie zum Generieren eines API-Schlüssels wie folgt vor:

- Melden Sie sich in Ihrer Cloud Insights-Umgebung an und wählen Sie **Admin > API-Zugriff**.
- Klicken Sie auf „+ API Access Token“.
- Geben Sie einen Namen und eine Beschreibung ein.
- Wählen Sie für Typ *Data Warehouse*.
- Legen Sie Berechtigungen als Lese-/Schreibzugriff fest.
- Legen Sie ein Ablaufdatum für „Wünsche“ fest.
- Klicken Sie auf „Speichern“, dann kopieren Sie den Schlüssel und speichern Sie ihn* irgendwo sicher. Sie können später nicht auf den vollständigen Schlüssel zugreifen.

APIkeys sind gut für *Sync* oder *Async*.

Direkte Abfrage von Tabellen

Mit dem vorhandenen API-Schlüssel sind nun direkte Abfragen der Reporting-Datenbank möglich. Lange URLs können für Anzeigezwecke auf https://…/odata/ vereinfacht werden und nicht für die volle https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/

Versuchen Sie einfache Abfragen wie

- https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/dwh_Custom
- https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/dwh_Inventory
- https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/dwh_Inventory/Storage

- https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/dwh_Inventory/Disk
- https://…/odata/dwh_custom/custom_queries

Beispiele FÜR REST-API

Die URL für alle Anrufe lautet *https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata*.

- GET /{Schema}/** - ruft Daten aus der Berichtsdatenbank ab.

Format: *https://<Cloud Insights URL>/Rest/v1/dwh-Management/odata/<Schema_Name>/<query>*

Beispiel:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Ergebnis:
```


```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```

Hilfreiche Tipps

Beachten Sie bei der Arbeit mit Reporting API-Abfragen Folgendes:

- Die Zuladung der Abfrage muss ein gültiger JSON-String sein
- Die Zuladung der Abfrage muss in einer einzigen Zeile enthalten sein
- Doppelte Anführungszeichen müssen entfloh werden, d. h. \“
- Registerkarten werden als \t unterstützt
- Kommentare vermeiden
- Tabellennamen mit niedrigerer Groß-/Kleinschreibung werden unterstützt

Zusätzlich:

- 2 Kopfzeilen sind erforderlich:
  - Name „X-CloudInsights-ApiKey“
  - Attributwert „<apikey>“

Der API-Schlüssel ist spezifisch für Ihre Cloud Insights-Umgebung.

Synchron oder asynchron?

Standardmäßig wird ein API-Befehl im *synchronen*-Modus ausgeführt, d. h., Sie senden die Anforderung und die Antwort wird sofort zurückgegeben. Manchmal kann die Ausführung einer Abfrage jedoch lange dauern, was zu einer Zeitüberschreitung der Anfrage führen kann. Um dies zu umgehen, können Sie eine Anfrage *asynchron* ausführen. Im asynchronen Modus gibt die Anforderung eine URL zurück, über die die Ausführung überwacht werden kann. Die URL gibt das Ergebnis zurück, wenn sie fertig ist.

Um eine Abfrage im asynchronen Modus auszuführen, fügen Sie den Header hinzu **`Prefer: respond-async`** Auf die Anfrage. Nach erfolgreicher Ausführung enthält die Antwort die folgenden Kopfzeilen:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Cloud Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

Wenn Sie die URL für den Speicherort abfragen, werden die gleichen Header zurückgegeben, wenn die Antwort noch nicht bereit ist, oder wenn die Antwort bereit ist, wird sie mit dem Status 200 zurückgegeben. Der Antwortinhalt ist vom Typ Text und enthält den http-Status der ursprünglichen Abfrage sowie einige Metadaten, gefolgt von den Ergebnissen der ursprünglichen Abfrage.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Um eine Liste aller asynchronen Abfragen zu sehen und welche davon bereit sind, verwenden Sie den folgenden Befehl:

```
 GET https://<Cloud Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
Die Antwort hat das folgende Format:
```

```
{
   "queries" : [
       {
           "Query": "https://<Cloud Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Cloud Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

Aufbewahrung historischer Daten für die Berichterstellung

Cloud Insights speichert Verlaufsdaten für die Verwendung in Berichten basierend auf den Datentabellen und Granularität der Daten, wie in der folgenden Tabelle dargestellt.

Datentabellen	Gemessenes Objekt	Granularität	Aufbewahrungszeitraum
Performance Marts	Volumes und interne Volumes	Stündlich	14 Tage
Performance Marts	Volumes und interne Volumes	Täglich	13 Monaten
Performance Marts	Applikation	Stündlich	13 Monaten
Performance Marts	Host	Stündlich	13 Monaten
Performance Marts	Switch-Leistung für Port	Stündlich	35 Tage
Performance Marts	Performance-Switch für Host, Storage und Tape	Stündlich	13 Monaten
Performance Marts	Storage-Node	Stündlich	14 Tage
Performance Marts	Storage-Node	Täglich	13 Monaten
Performance Marts	VM-Performance	Stündlich	14 Tage
Performance Marts	VM-Performance	Täglich	13 Monaten
Performance Marts	Hypervisor-Performance	Stündlich	35 Tage
Performance Marts	Hypervisor-Performance	Täglich	13 Monaten

Performance Marts	VMDK-Performance	Stündlich	35 Tage
Performance Marts	VMDK-Performance	Täglich	13 Monaten
Performance Marts	Disk Performance	Stündlich	14 Tage
Performance Marts	Disk Performance	Täglich	13 Monaten
Capacity Marts	Alle (außer einzelne Volumes)	Täglich	13 Monaten
Capacity Marts	Alle (außer einzelne Volumes)	Monatlicher Vertreter	14 Monaten und darüber hinaus
Inventarmarke	Einzelne Volumes	Aktueller Stand	1 Tag (oder bis zum nächsten ETL)

Cloud Insights-Berichtschemadiagramme

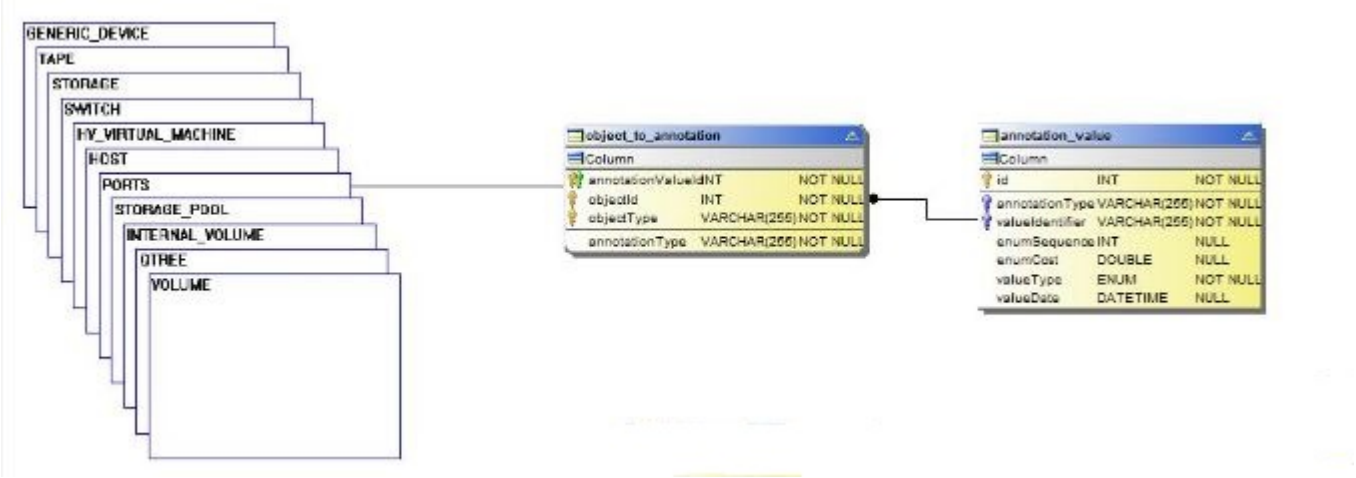
Dieses Dokument enthält die Schemadiagramme für die Berichtsdatenbank. Sie können auch eine Datei mit der herunterladen "Schematabellen".

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

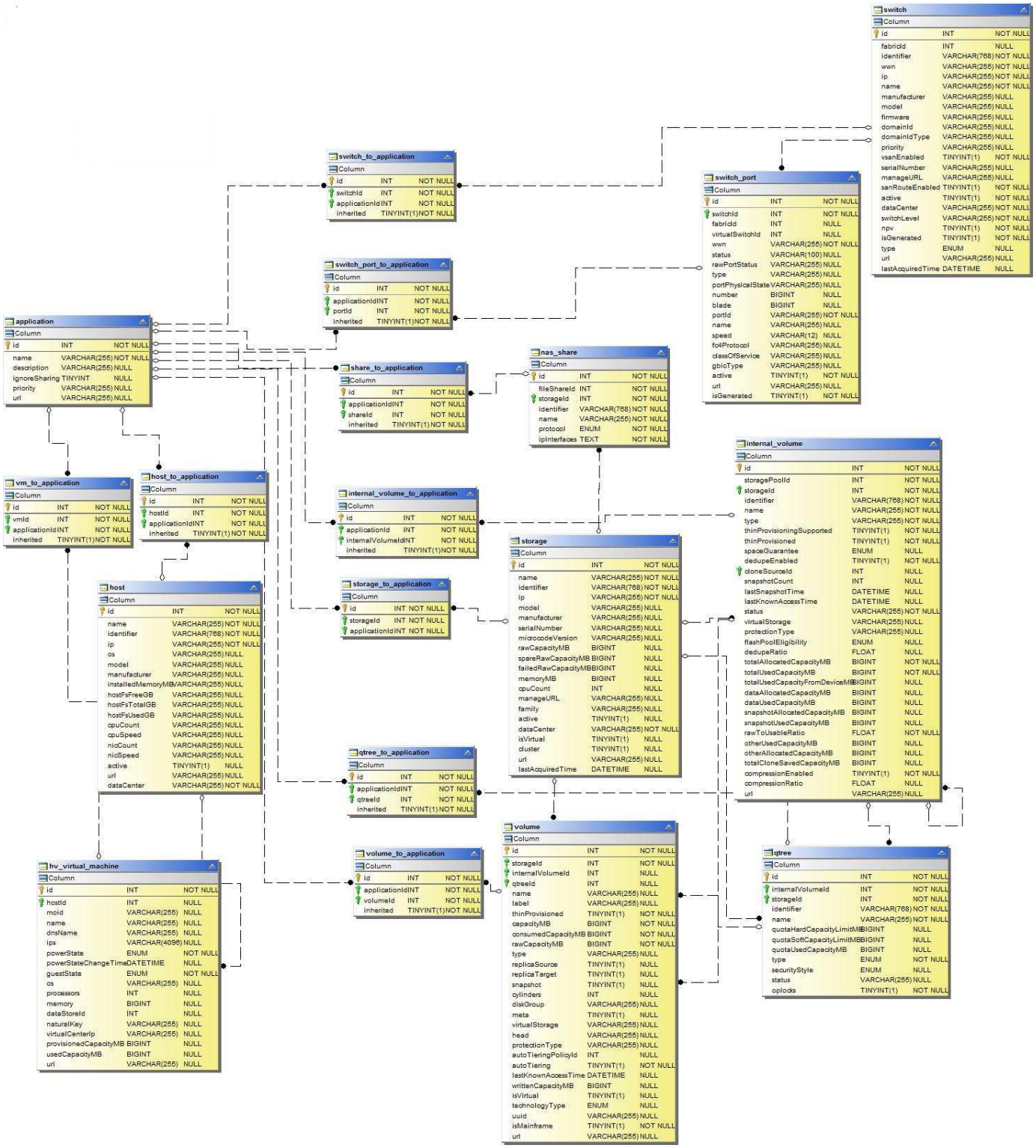
Inventory Datamart

Die folgenden Bilder beschreiben das Inventurdatamart.

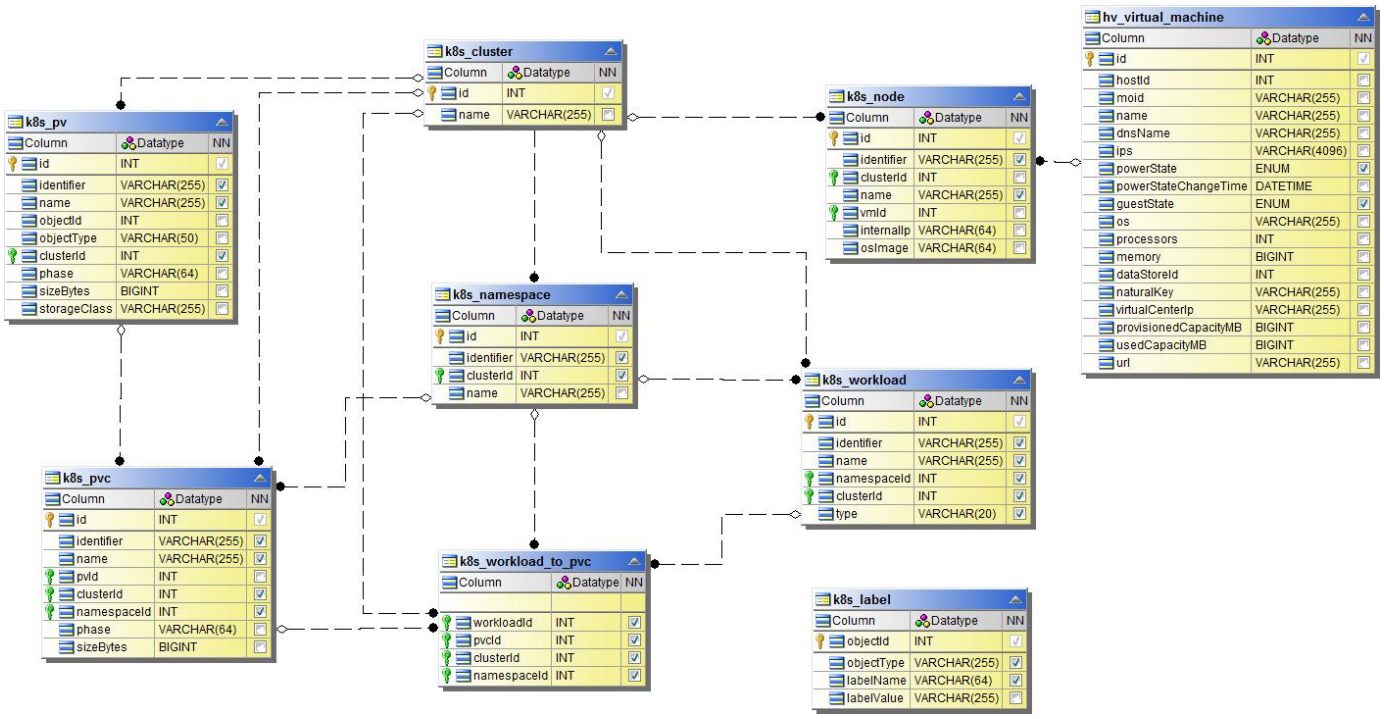
Anmerkungen



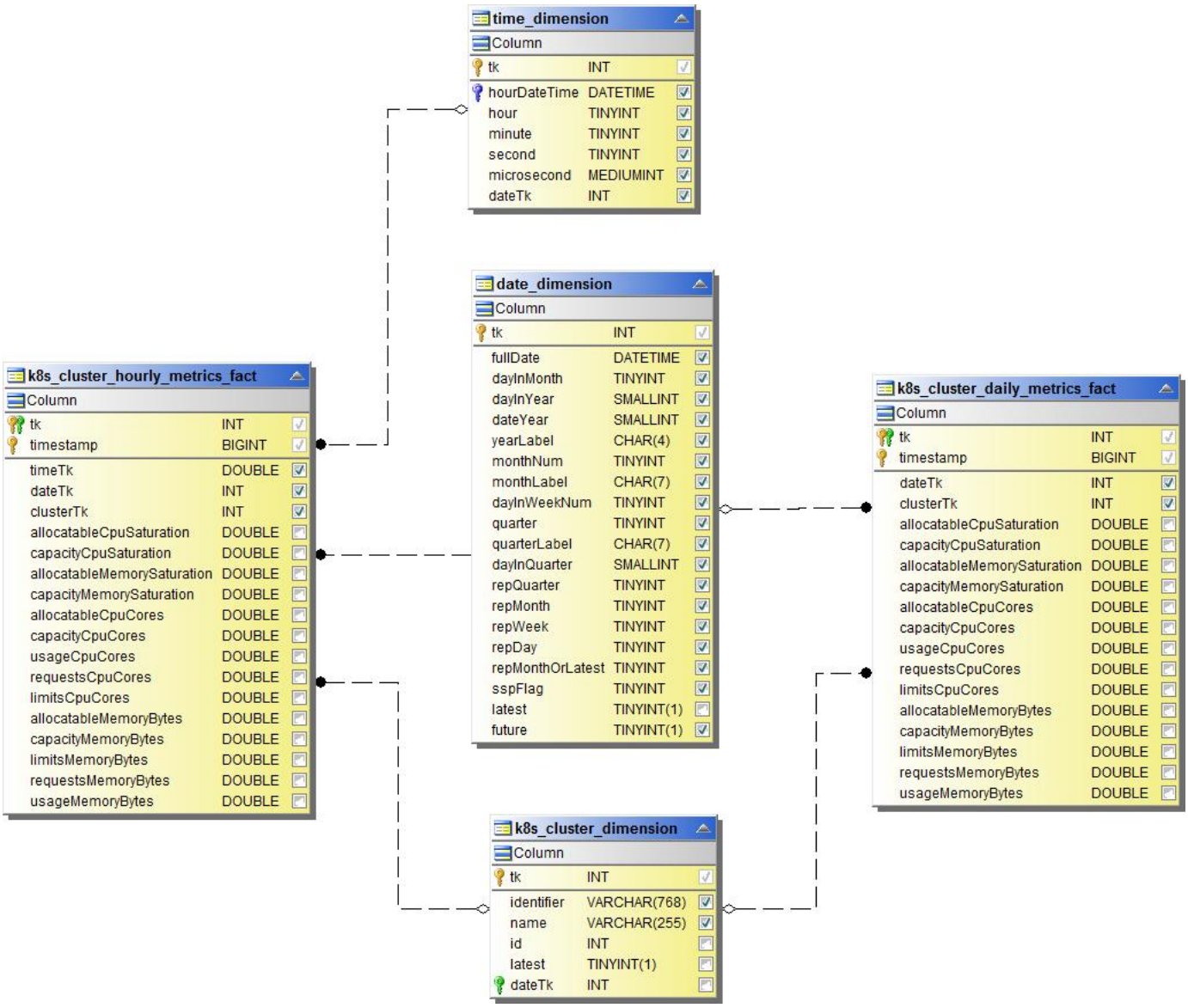
Applikationen Unterstützt



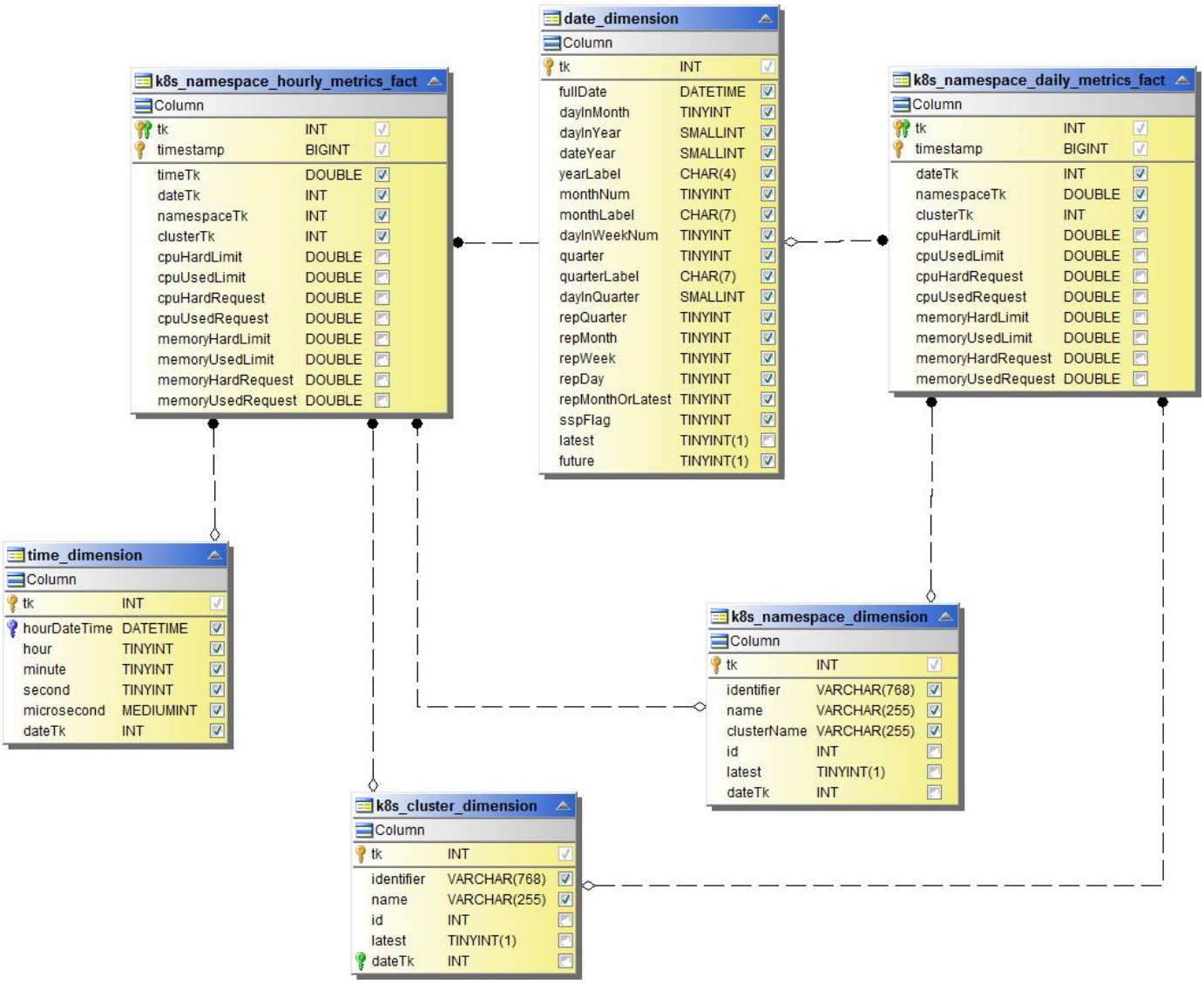
Kubernetes-Kennzahlen



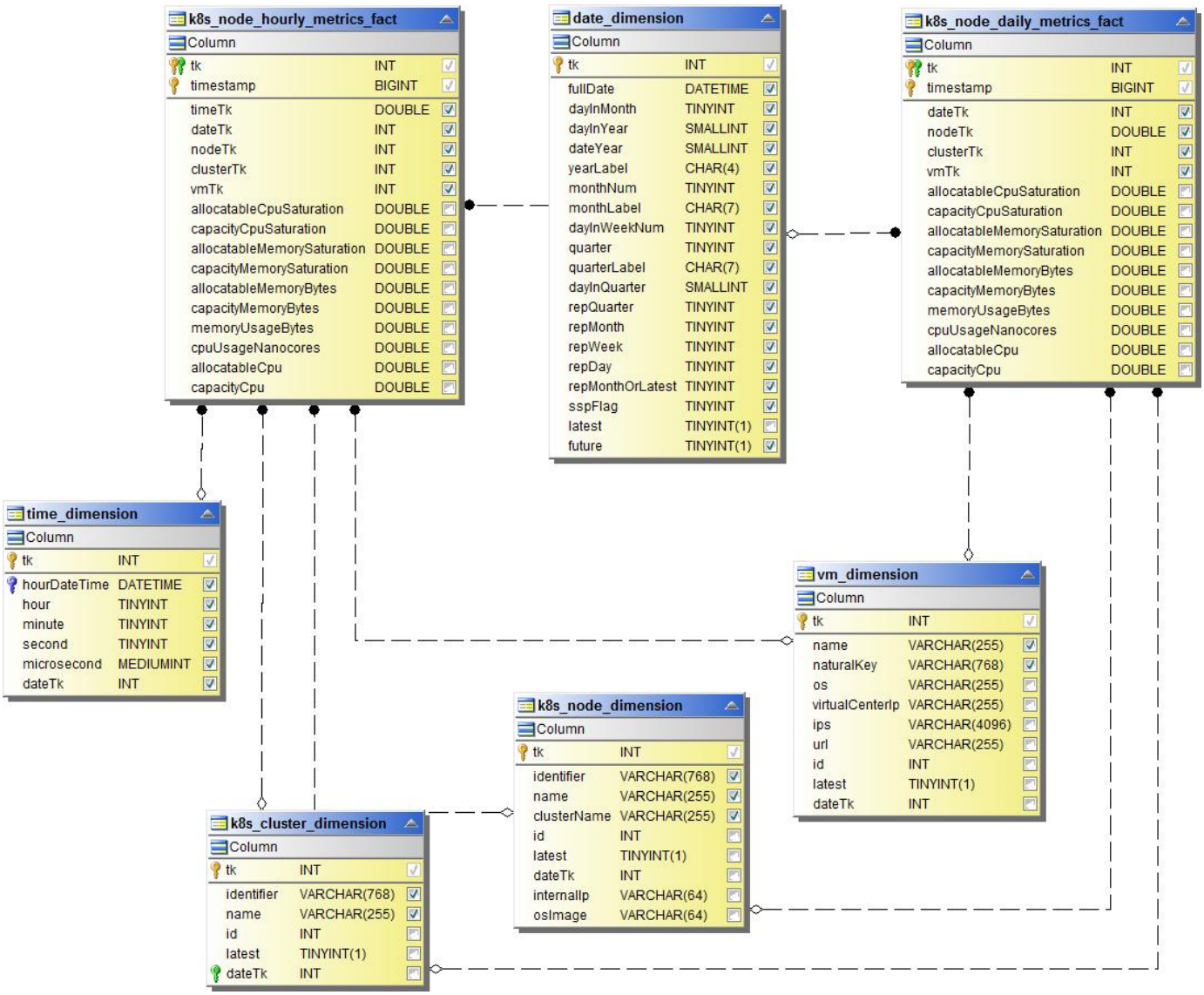
Kennzahlen Für Kubernetes Cluster



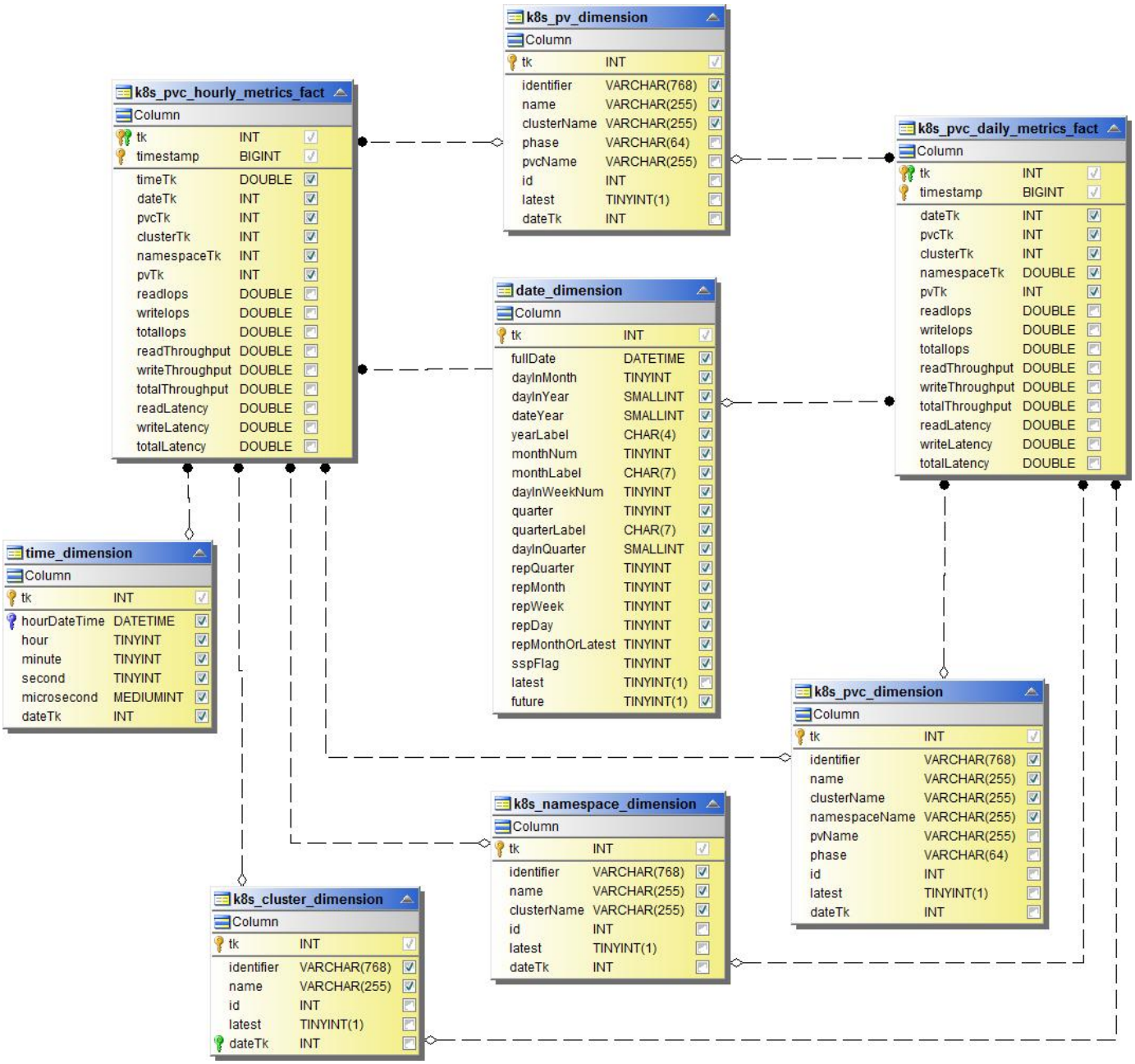
Kenngrößen Für Kubernetes-Namespace



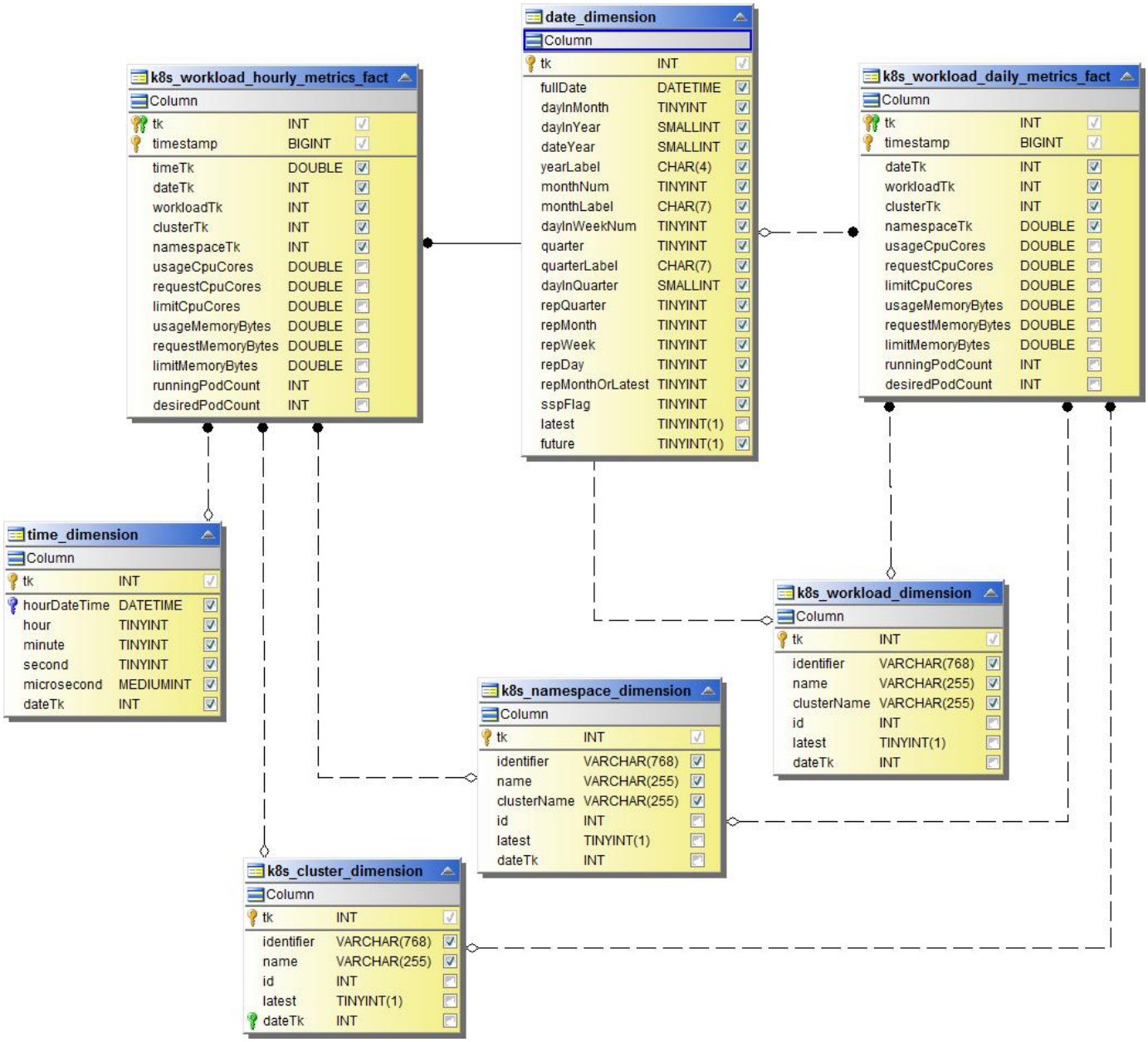
Kenngrößen Für Kubernetes-Nodes



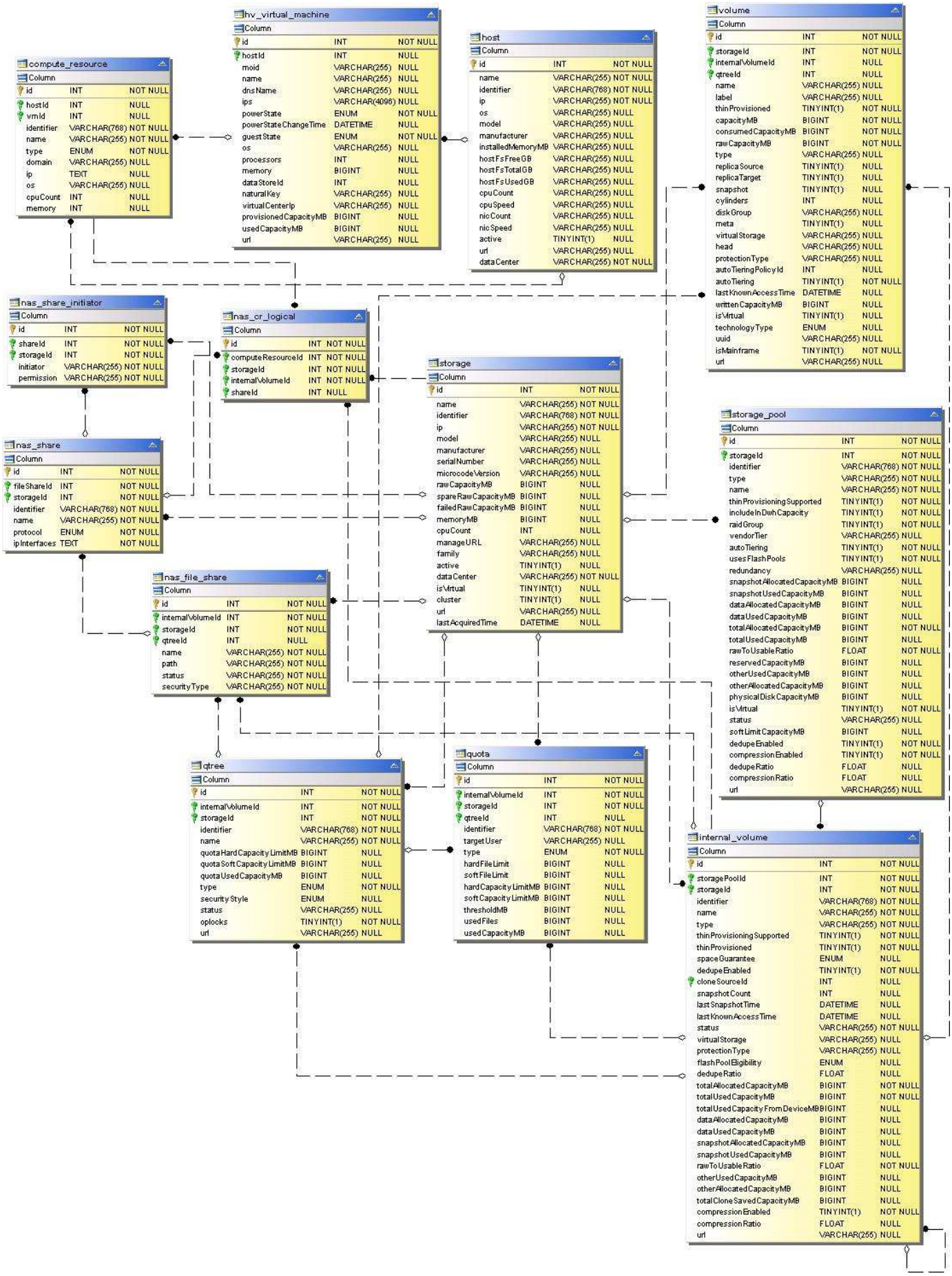
Kennzahl der Kubernetes PVC



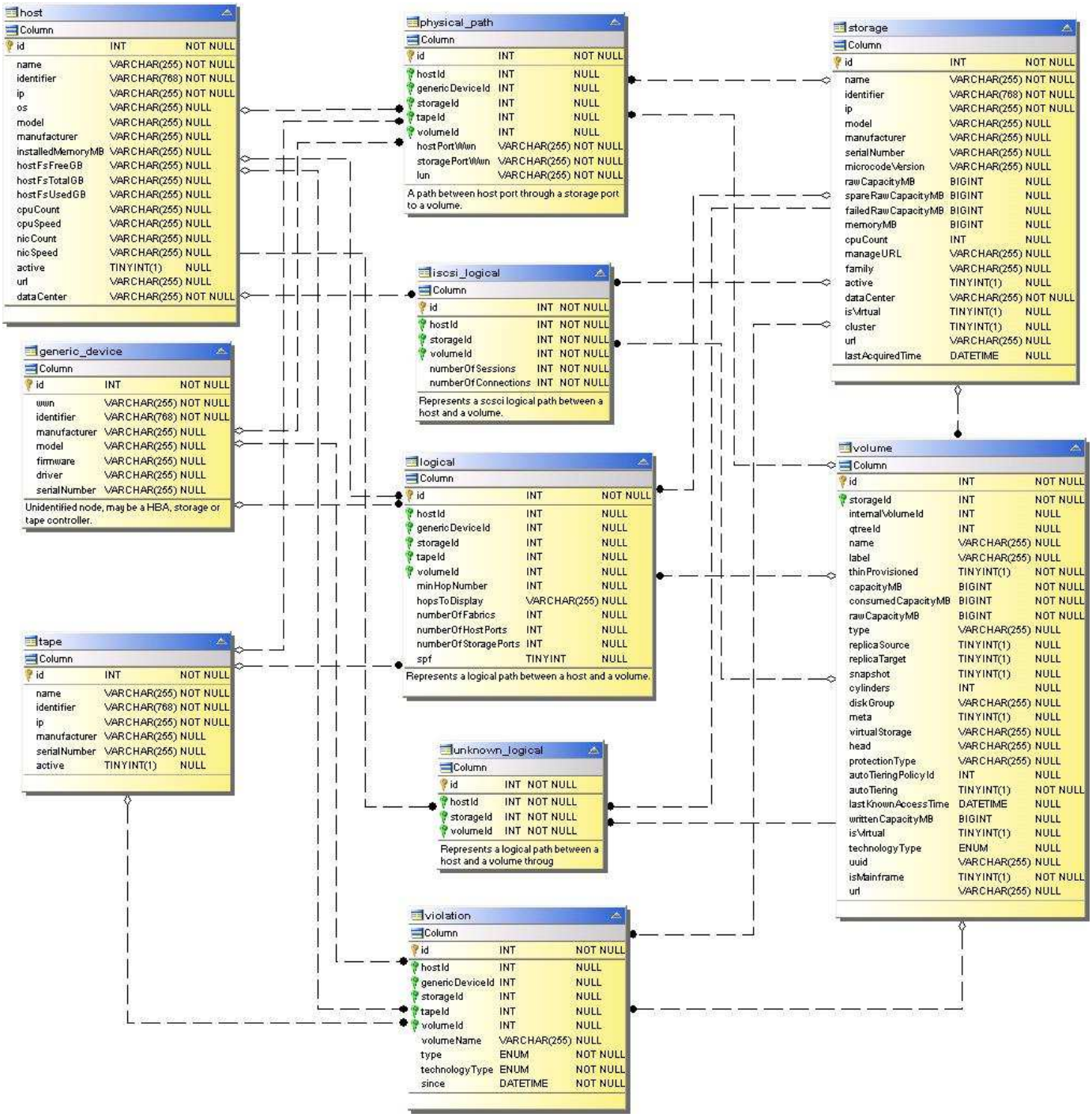
Kenngrößen Für Kubernetes-Workloads


k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

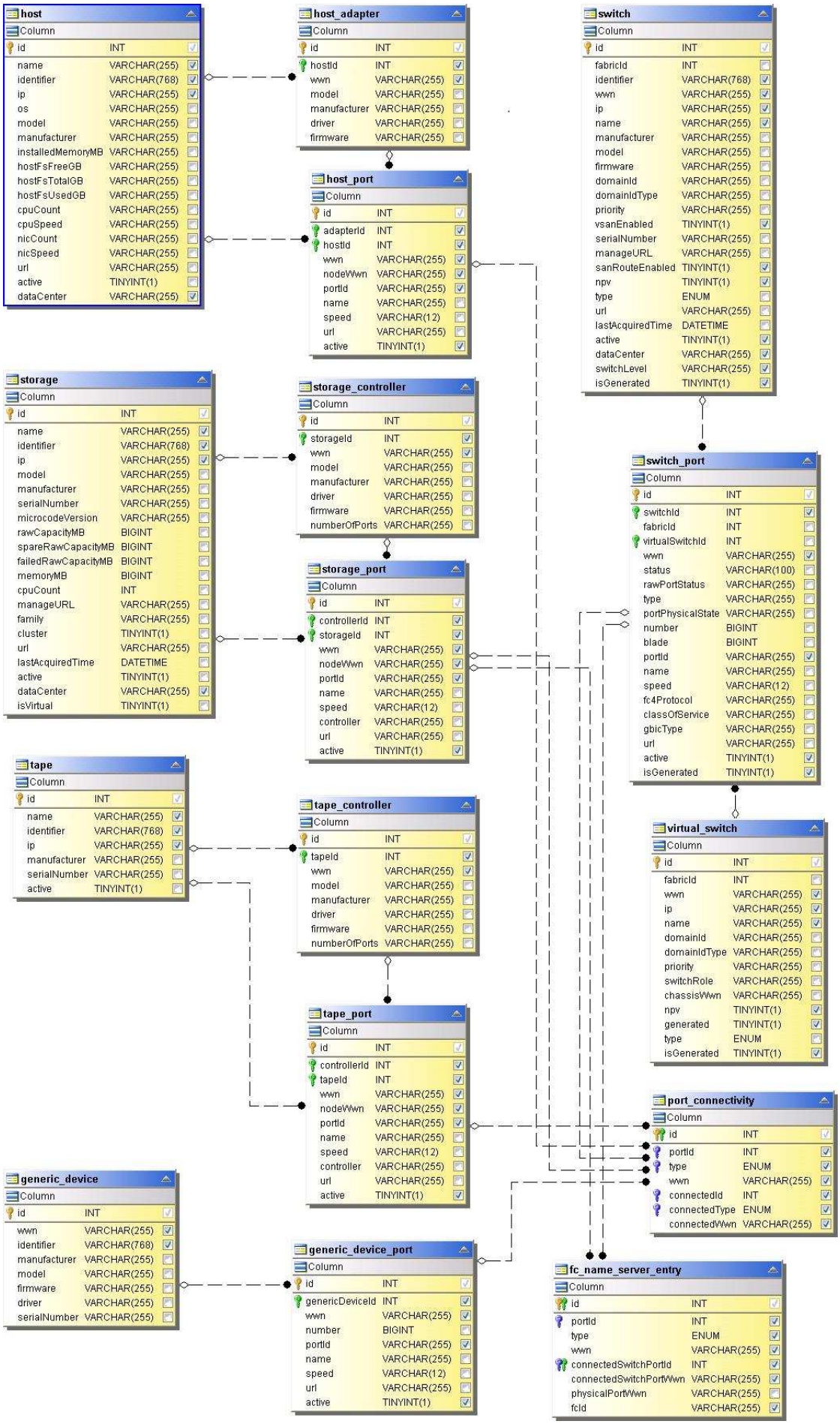
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL

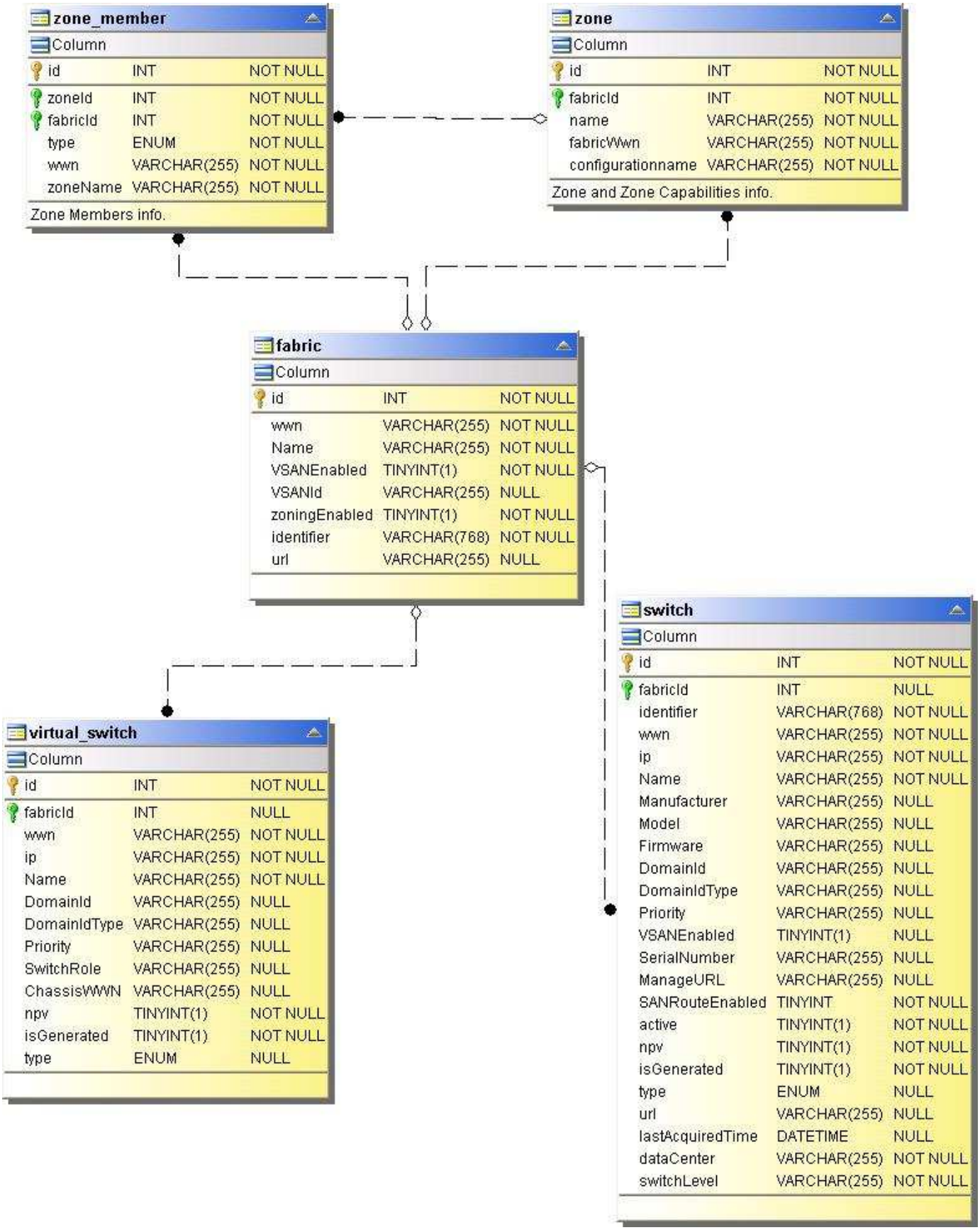
Pfade und Verstöße



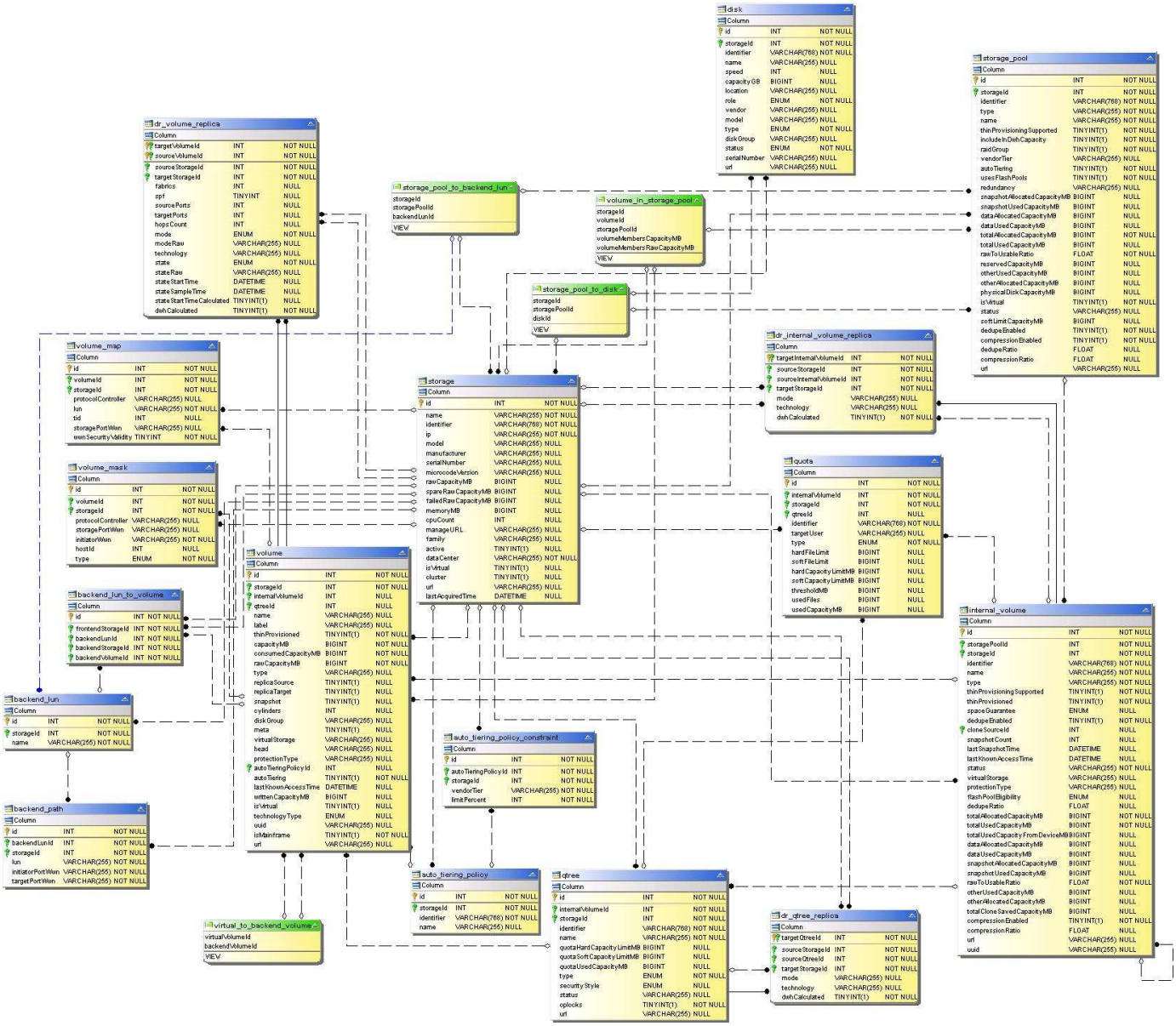
Port-Konnektivität


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

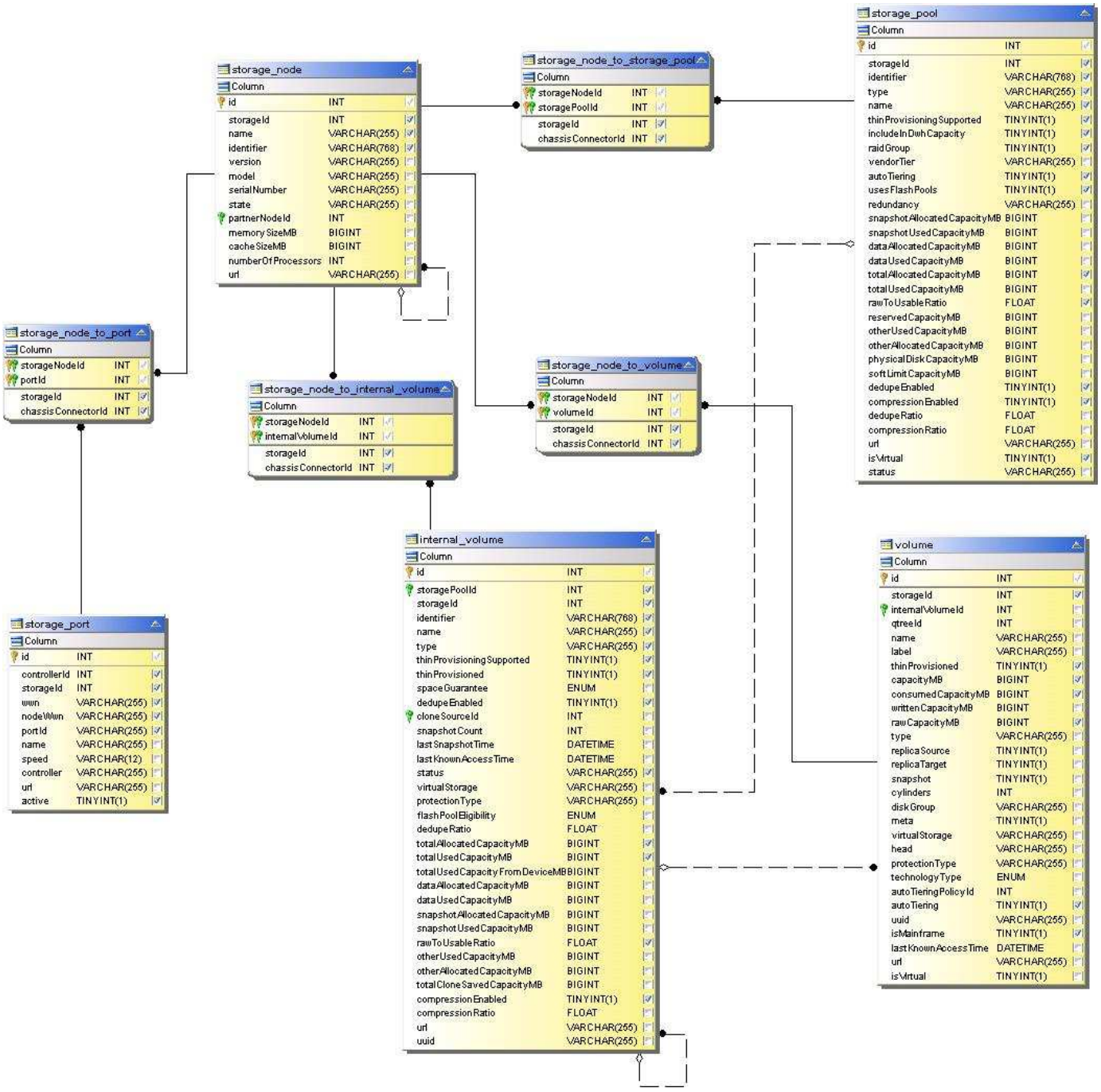
SAN-Fabric


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL

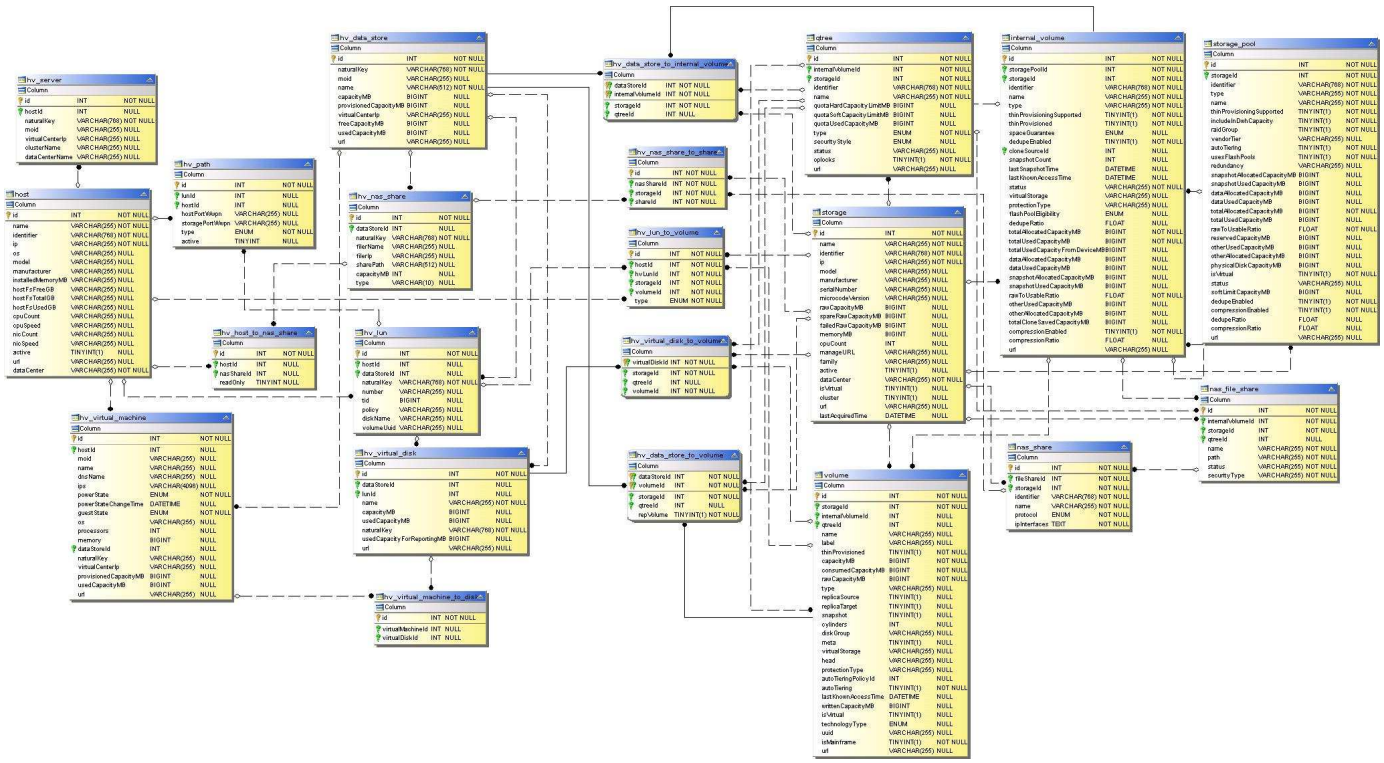
Storage



Storage-Node


storage_node
Column
id INT
storageId INT
name VARCHAR(255)
identifier VARCHAR(768)
version VARCHAR(255)
model VARCHAR(255)
serialNumber VARCHAR(255)
state VARCHAR(255)
partnerNodeId INT
memorySizeMB BIGINT
cacheSizeMB BIGINT
numberOfProcessors INT
url VARCHAR(255)
storage_node_to_storage_pool
Column
storageNodeId INT
storagePoolId INT
storageId INT
chassisConnectorId INT
storage_pool
Column
id INT
storageId INT
identifier VARCHAR(768)
type VARCHAR(255)
name VARCHAR(255)
thinProvisioningSupported TINYINT(1)
includeInDwhCapacity TINYINT(1)
raidGroup TINYINT(1)
vendorTier VARCHAR(255)
autoTiering TINYINT(1)
usesFlashPools TINYINT(1)
redundancy VARCHAR(255)
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
reservedCapacityMB BIGINT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
physicalDiskCapacityMB BIGINT
softLimitCapacityMB BIGINT
dedupeEnabled TINYINT(1)
compressionEnabled TINYINT(1)
dedupeRatio FLOAT
compressionRatio FLOAT
url VARCHAR(255)
isVirtual TINYINT(1)
status VARCHAR(255)
storage_node_to_port
Column
storageNodeId INT
portId INT
storageId INT
chassisConnectorId INT
storage_node_to_internal_volume
Column
storageNodeId INT
internalVolumeId INT
storageId INT
chassisConnectorId INT
storage_node_to_volume
Column
storageNodeId INT
volumeId INT
storageId INT
chassisConnectorId INT
internal_volume
Column
id INT
storagePoolId INT
storageId INT
identifier VARCHAR(768)
name VARCHAR(255)
type VARCHAR(255)
thinProvisioningSupported TINYINT(1)
thinProvisioned TINYINT(1)
spaceGuarantee ENUM
dedupeEnabled TINYINT(1)
cloneSourceId INT
snapshotCount INT
lastSnapshotTime DATETIME
lastKnownAccessTime DATETIME
status VARCHAR(255)
virtualStorage VARCHAR(255)
protectionType VARCHAR(255)
flashPoolEligibility ENUM
dedupeRatio FLOAT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
totalUsedCapacityFromDeviceMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
totalCloneSavedCapacityMB BIGINT
compressionEnabled TINYINT(1)
compressionRatio FLOAT
url VARCHAR(255)
uuid VARCHAR(255)
volume
Column
id INT
storageId INT
internalVolumeId INT
qtreeId INT
name VARCHAR(255)
label VARCHAR(255)
thinProvisioned TINYINT(1)
capacityMB BIGINT
consumedCapacityMB BIGINT
writtenCapacityMB BIGINT
rawCapacityMB BIGINT
type VARCHAR(255)
replicaSource TINYINT(1)
replicaTarget TINYINT(1)
snapshot TINYINT(1)
cylinders INT
diskGroup VARCHAR(255)
meta TINYINT(1)
virtualStorage VARCHAR(255)
head VARCHAR(255)
protectionType VARCHAR(255)
technologyType ENUM
autoTieringPolicyId INT
autoTiering TINYINT(1)
uuid VARCHAR(255)
isMainframe TINYINT(1)
lastKnownAccessTime DATETIME
url VARCHAR(255)
isVirtual TINYINT(1)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)

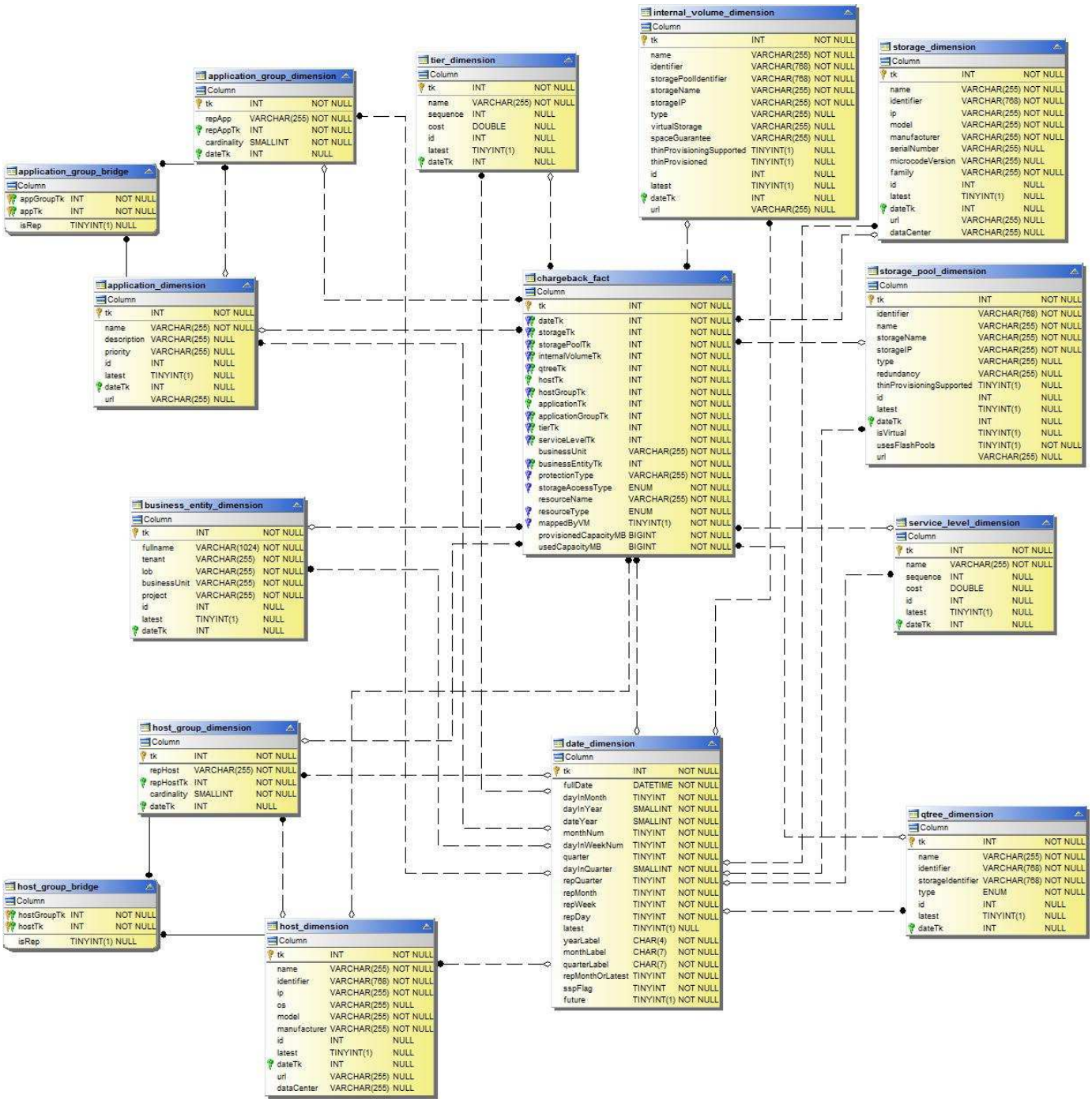
VM



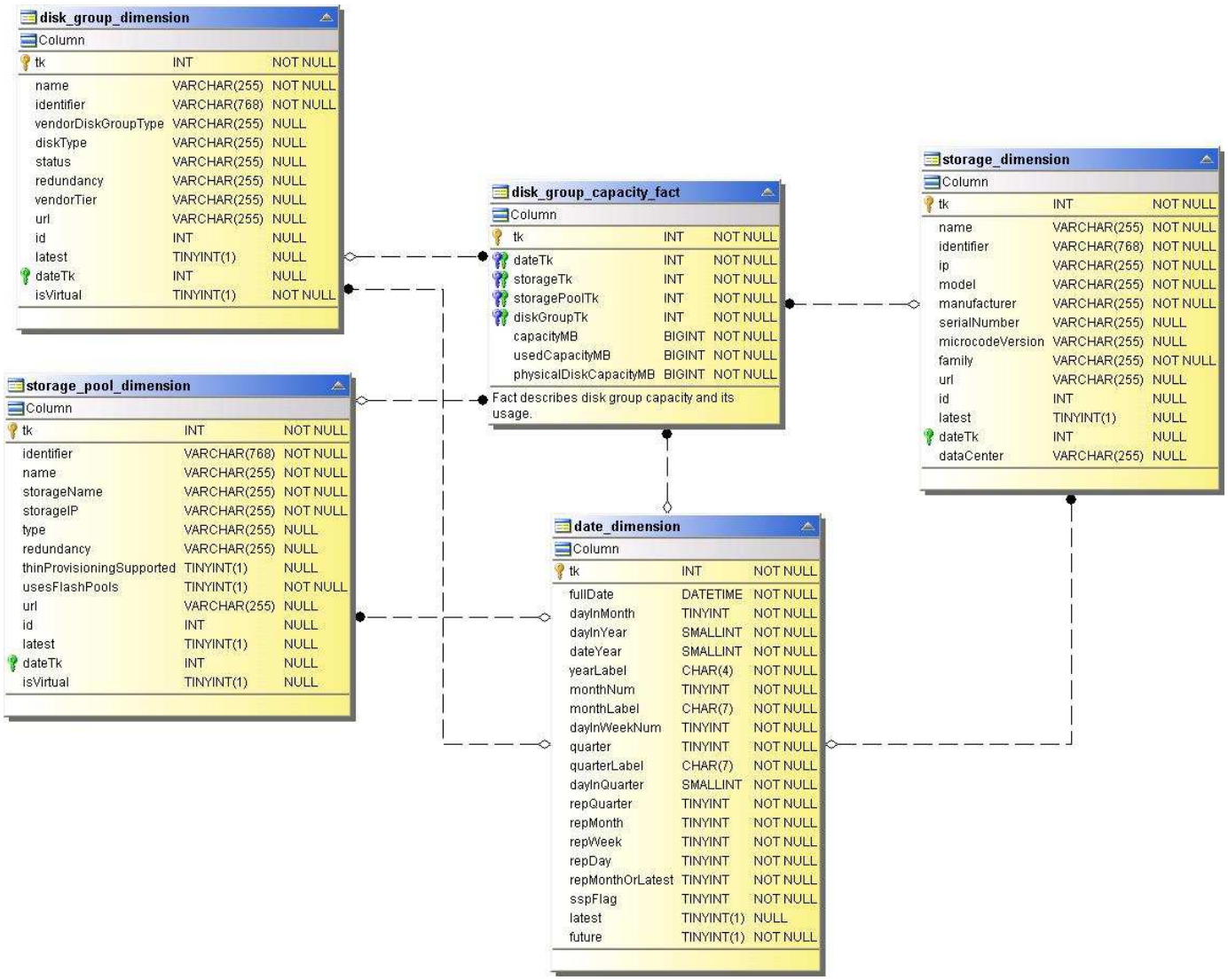
Kapazitätsdatamart

Die folgenden Bilder beschreiben die Datenkapazität.

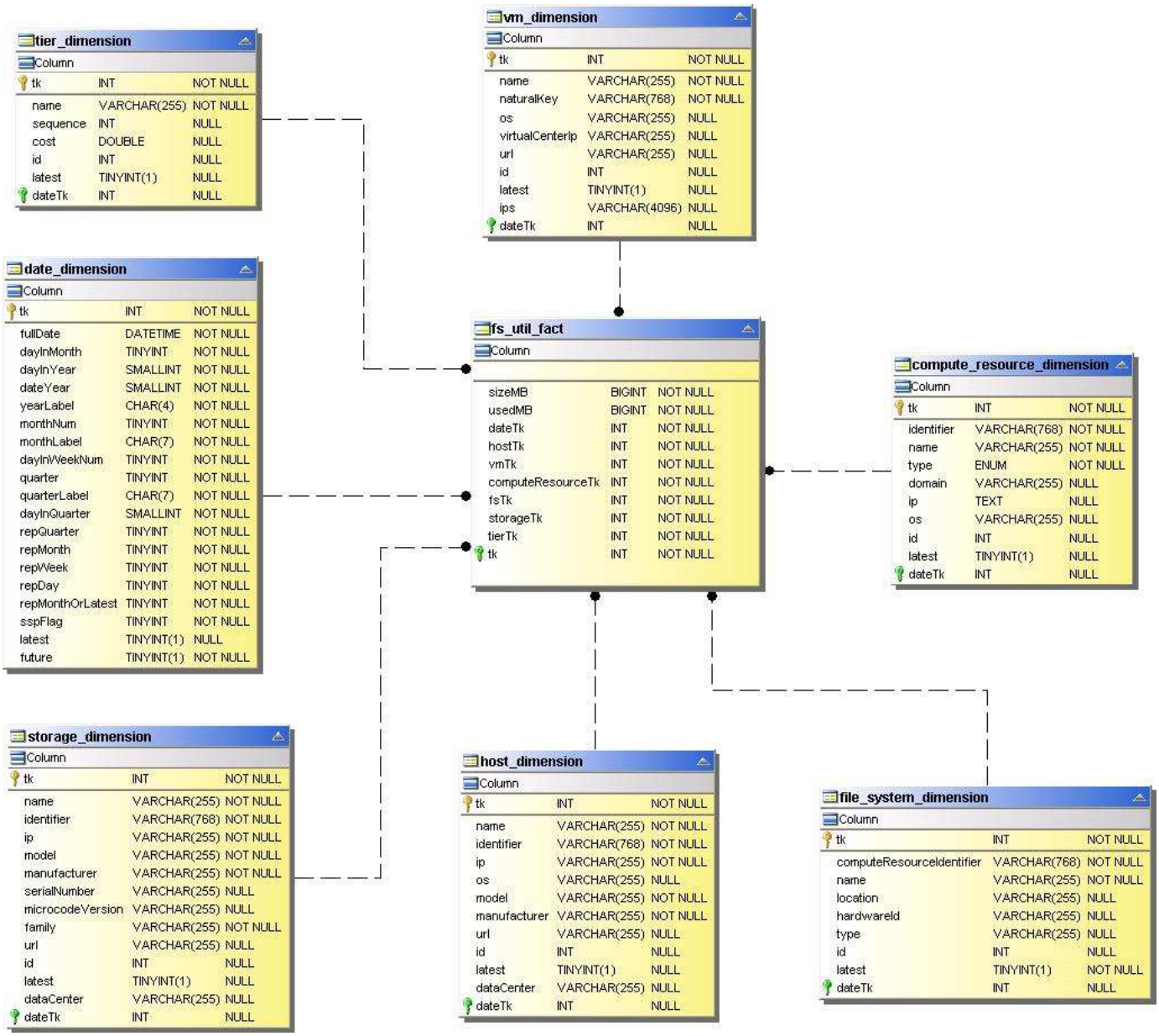
Kostenverrechnung



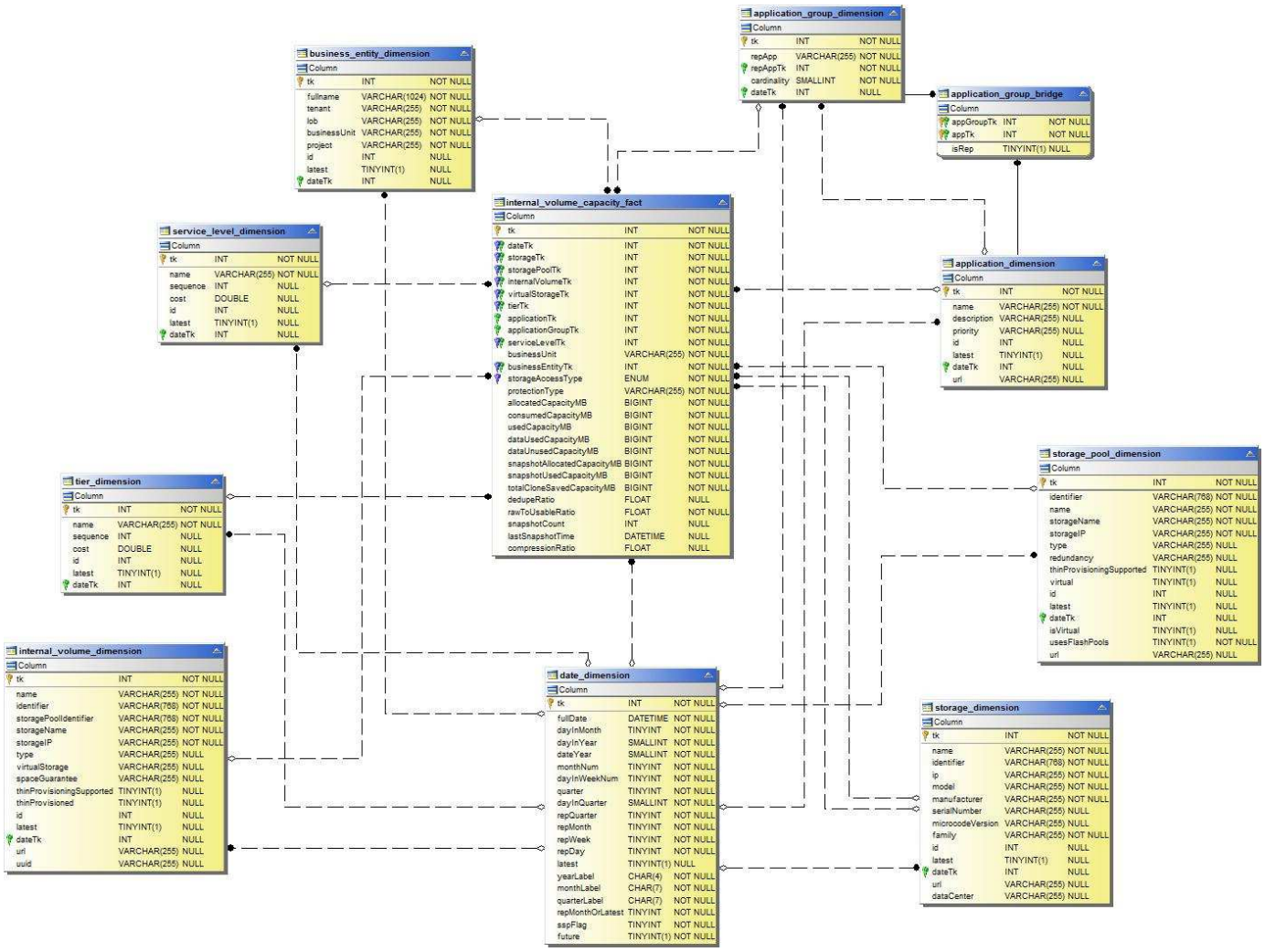
Kapazität Der Festplattengruppe



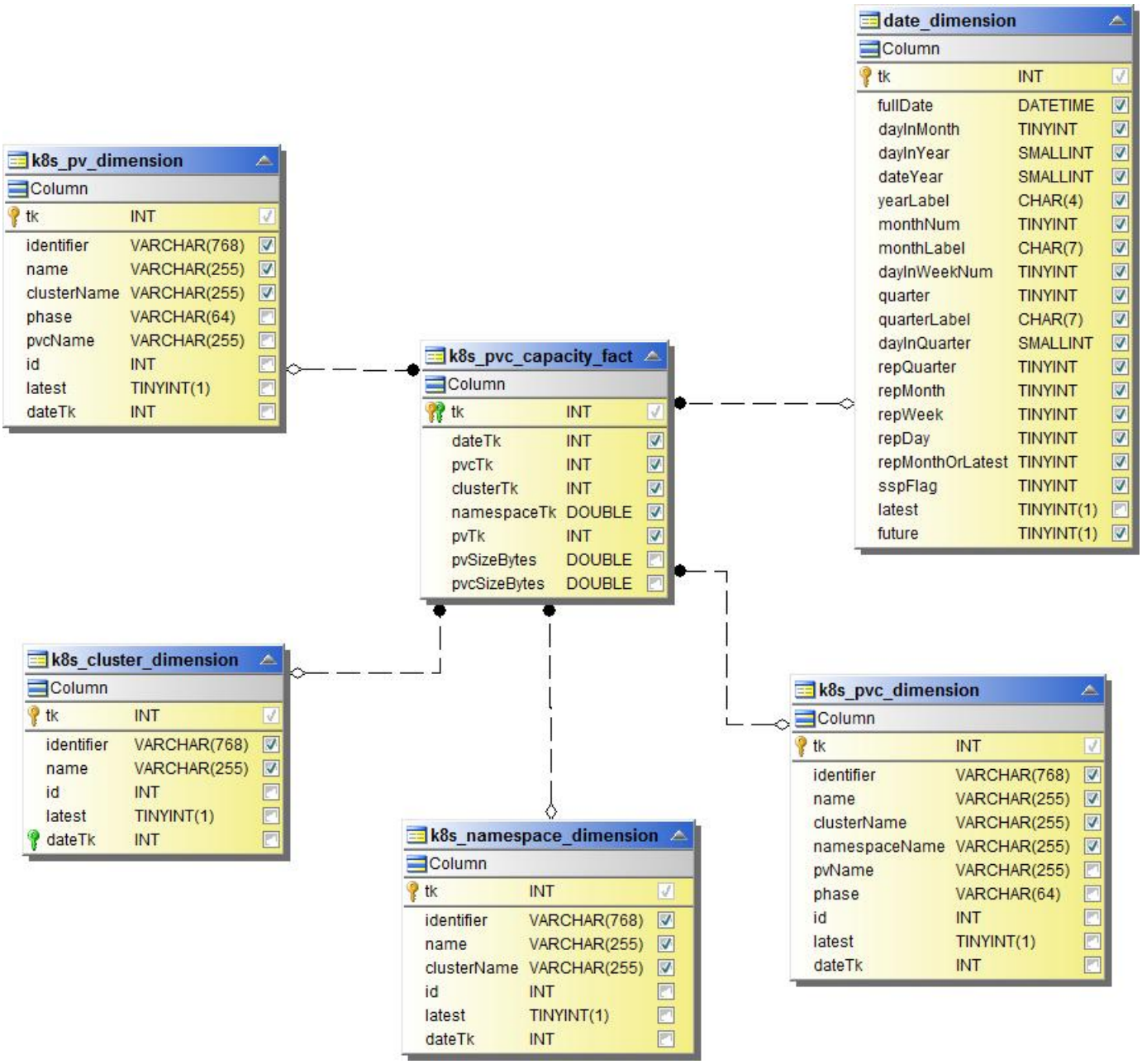
Auslastung Des Filesystems



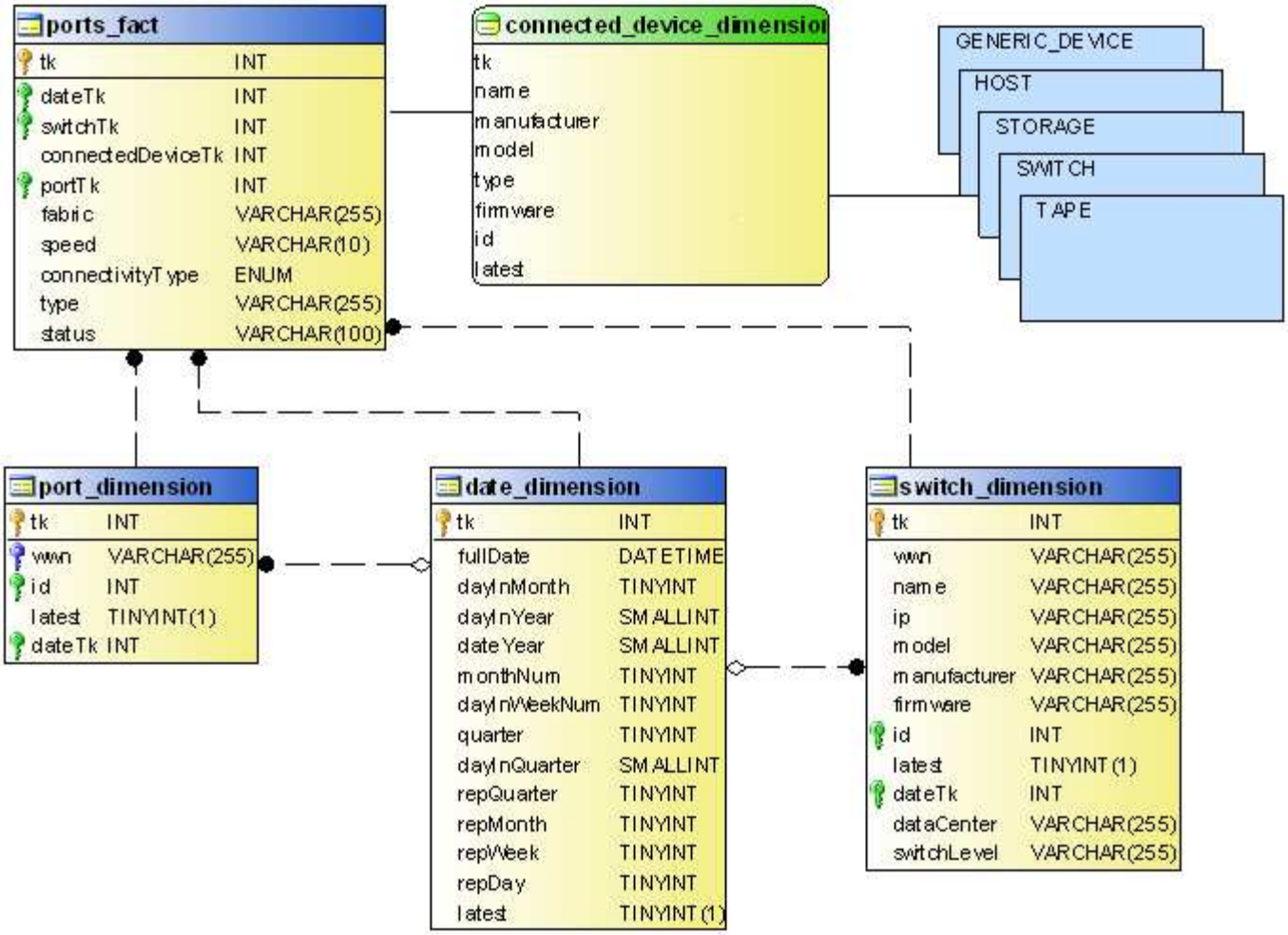
Kapazität Des Internen Volumes



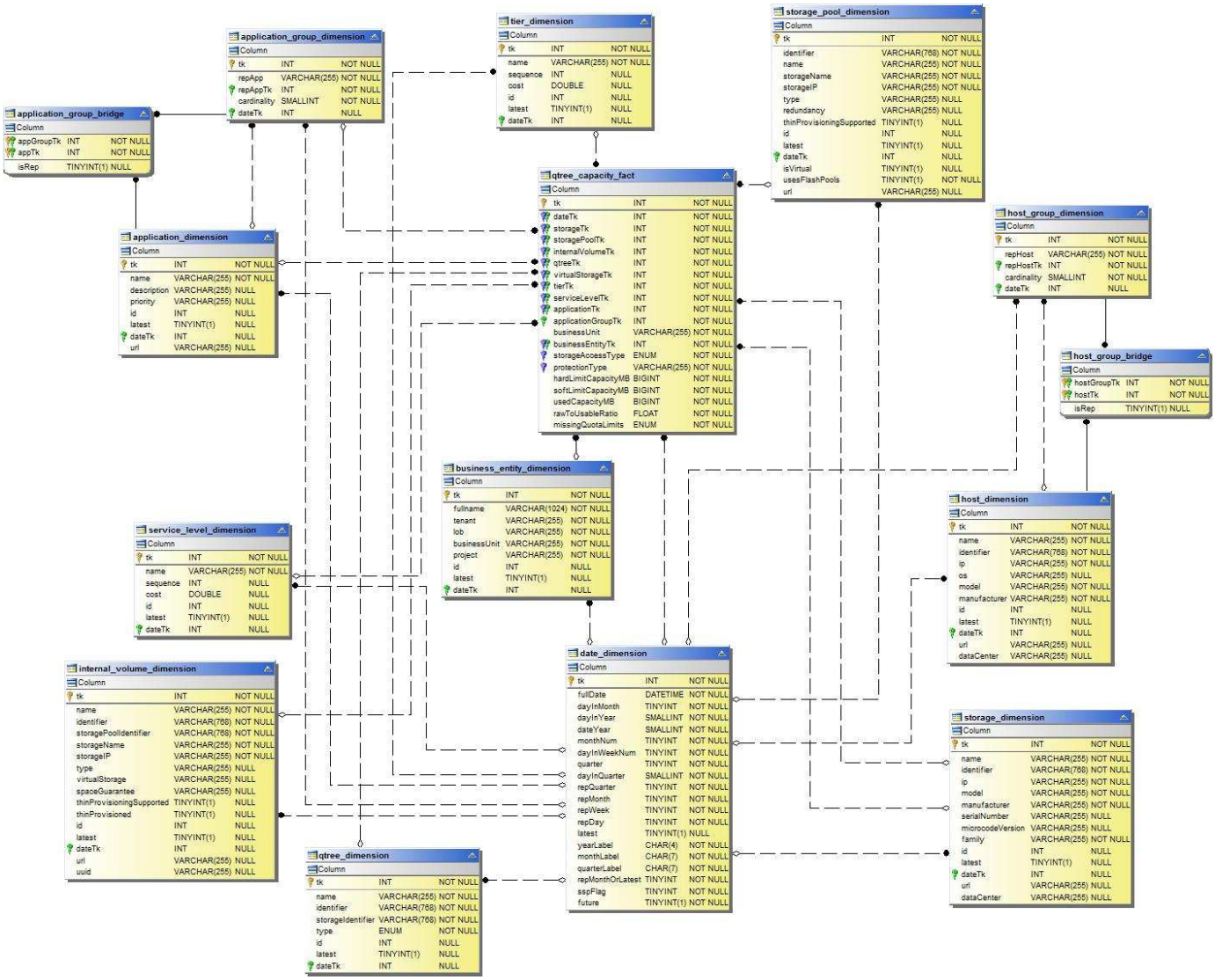
Kubernetes PV-Kapazität



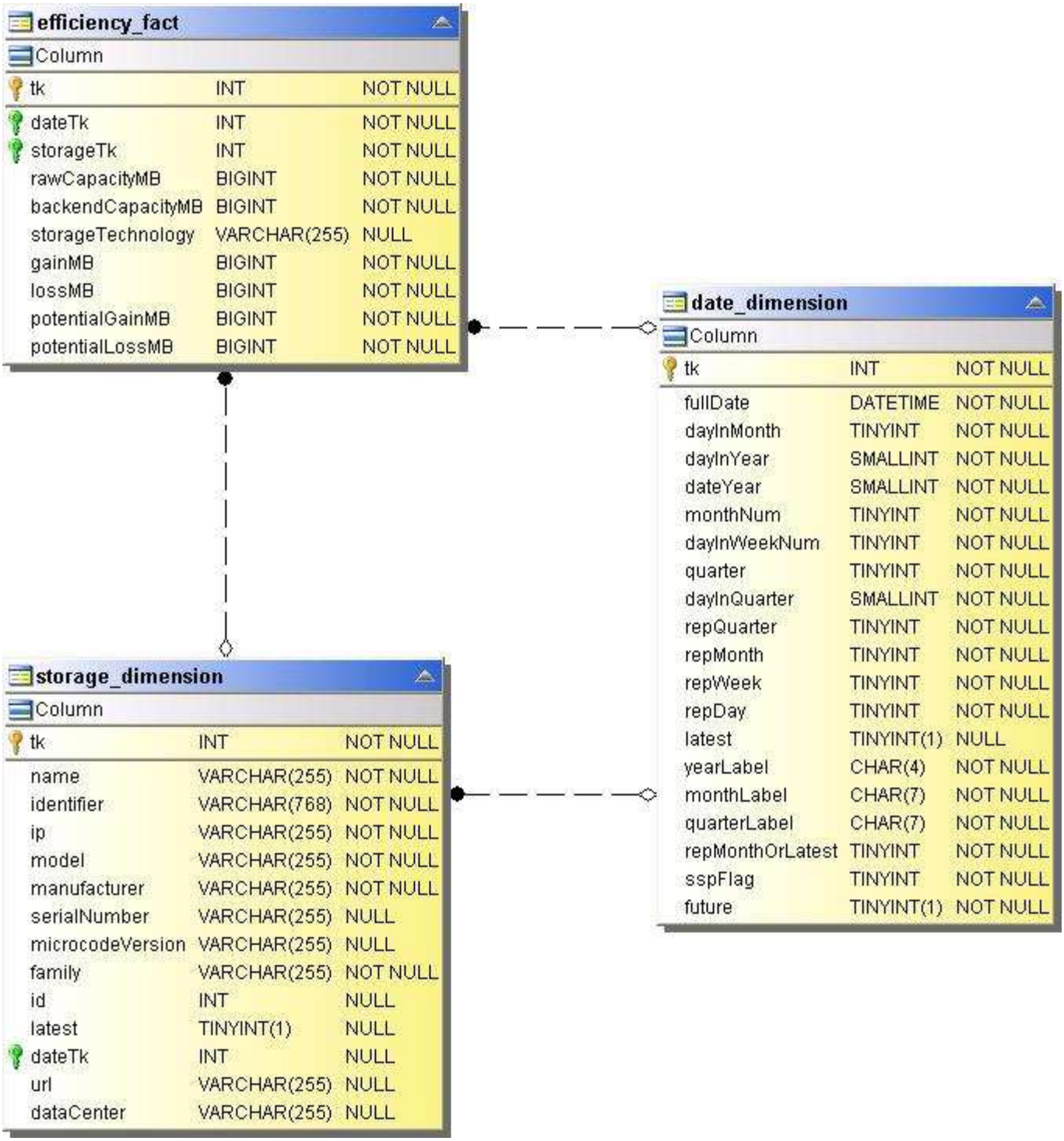
Port-Kapazität



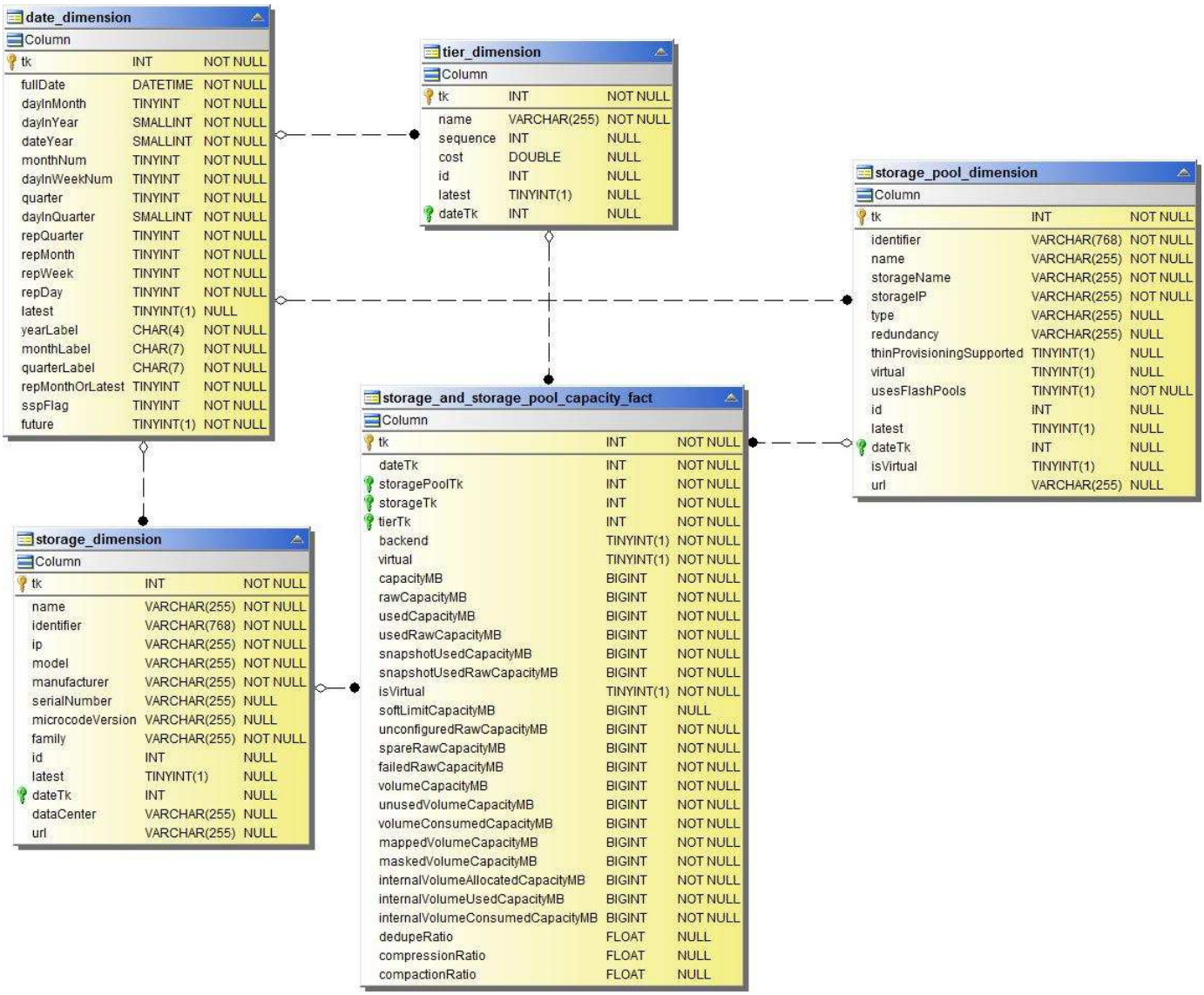
Qtree-Kapazität



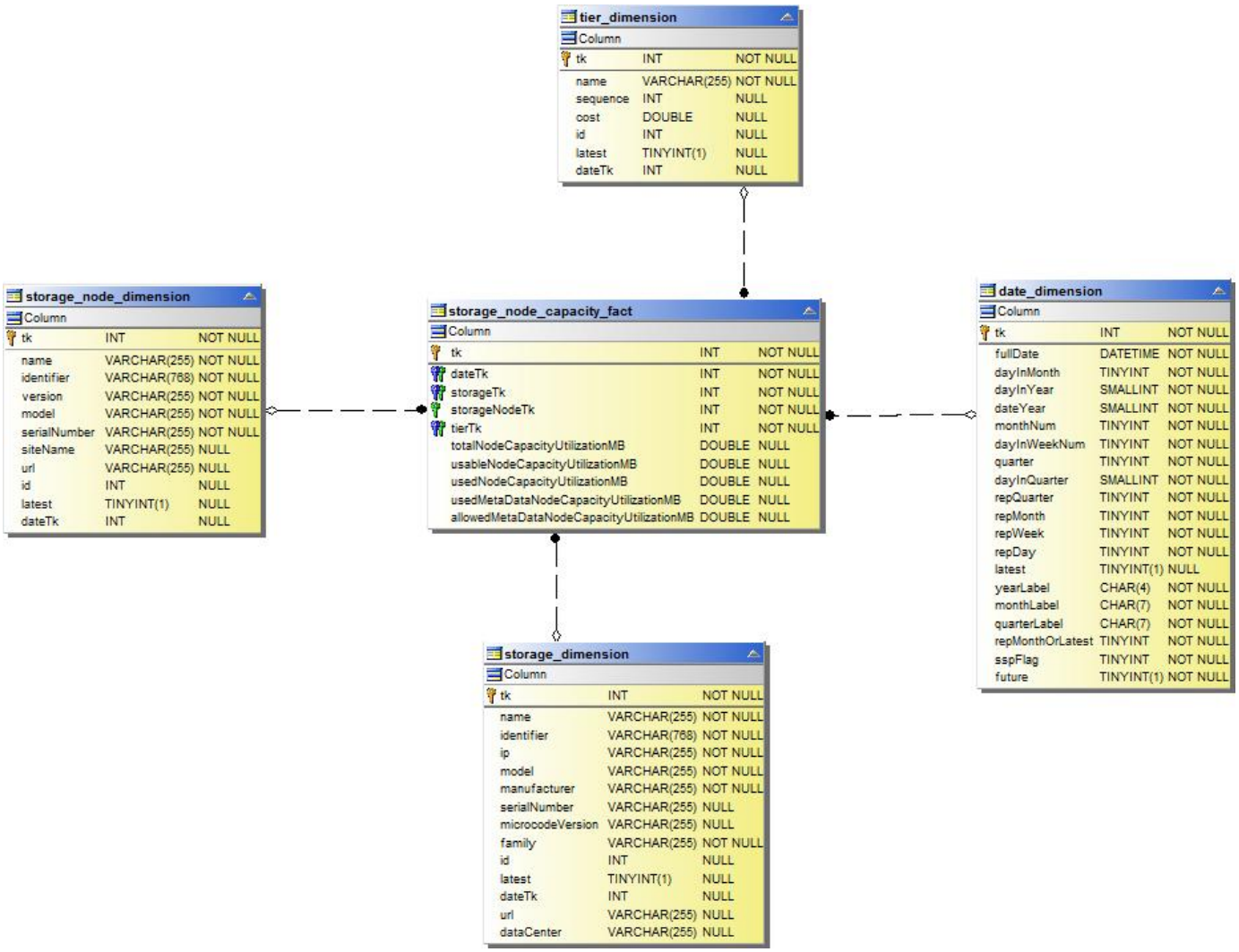
Storage-Kapazitätseffizienz



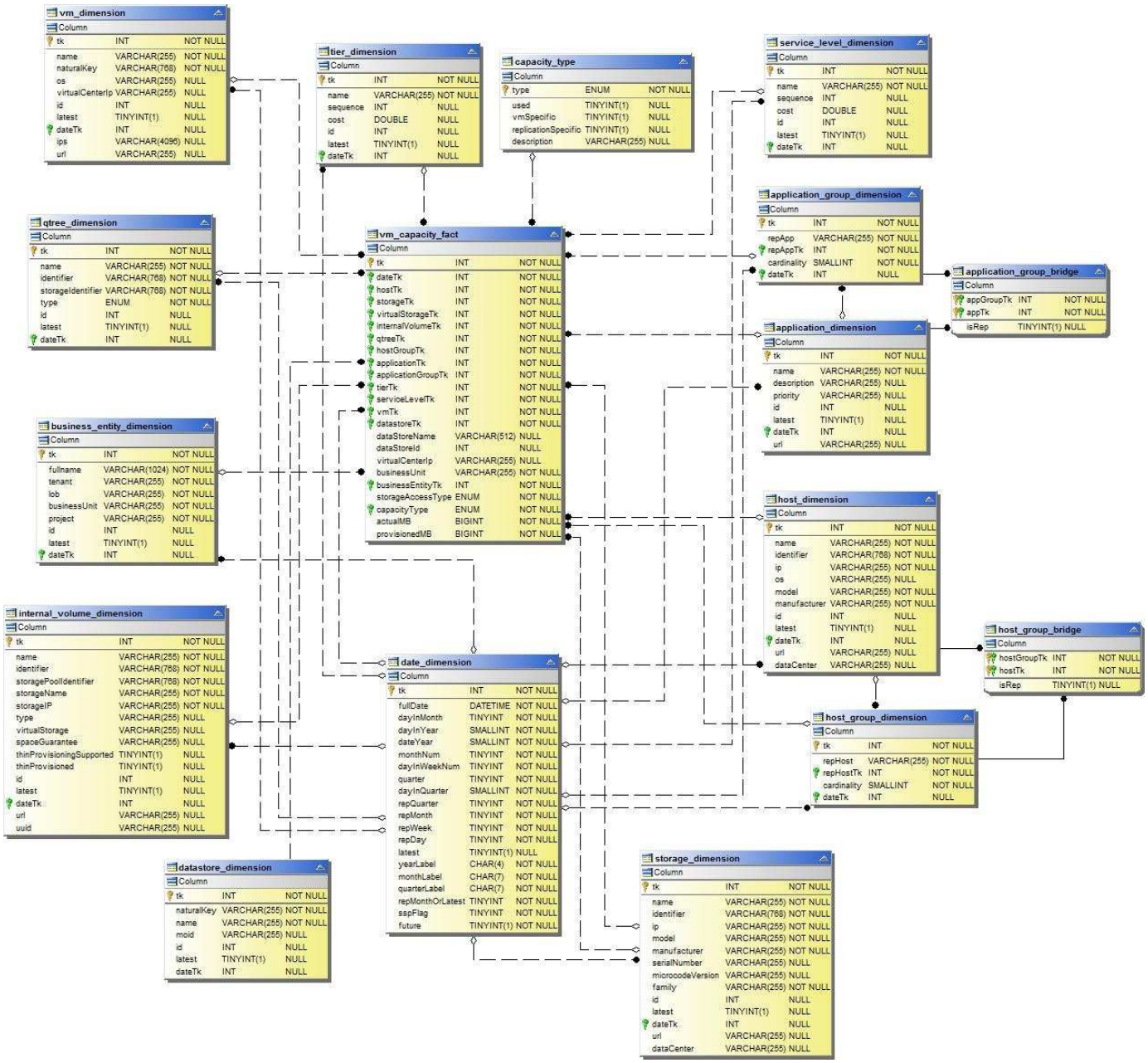
Kapazität im Storage- und Speicherpool



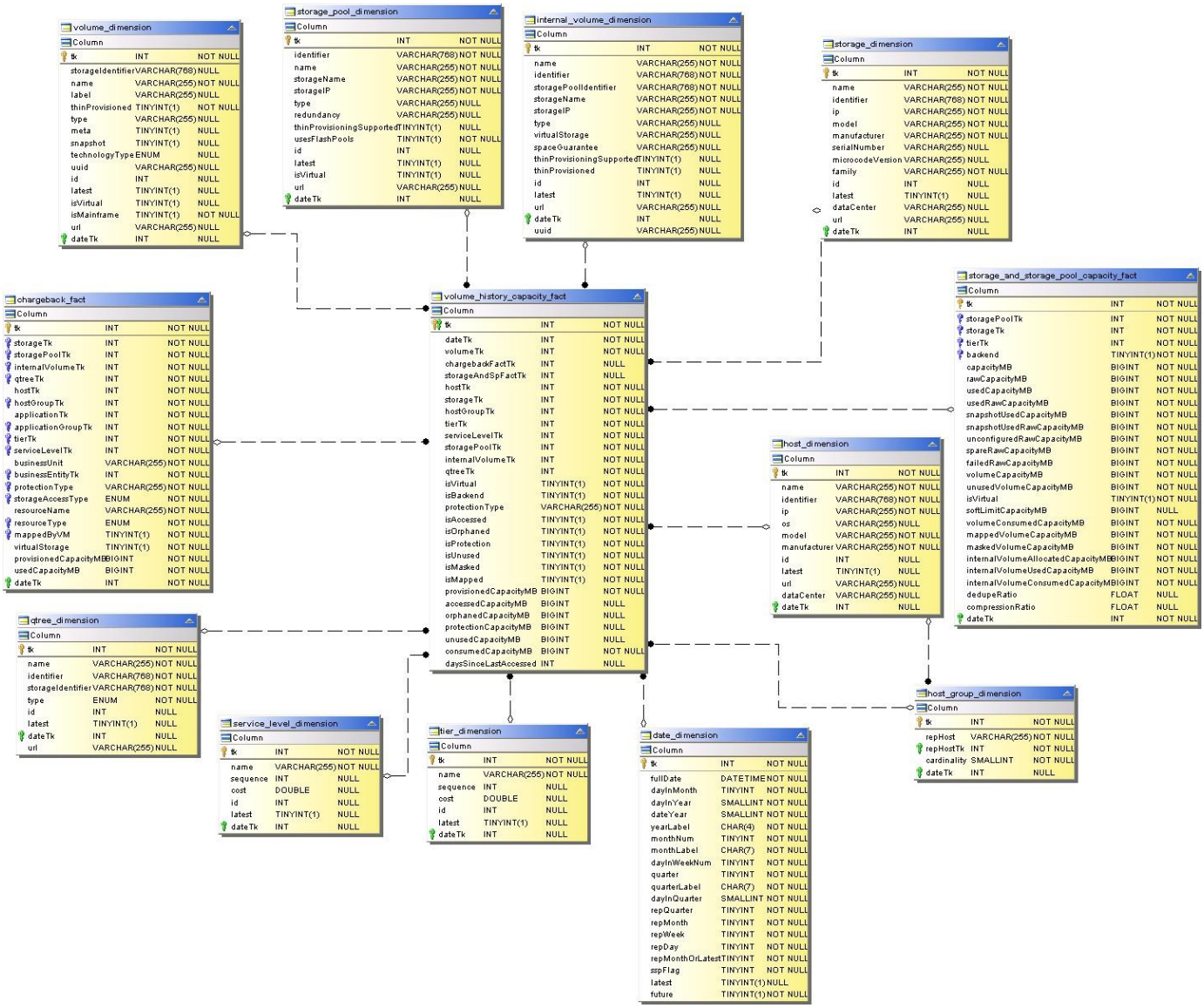
Kapazität Des Storage-Nodes



VM-Kapazität



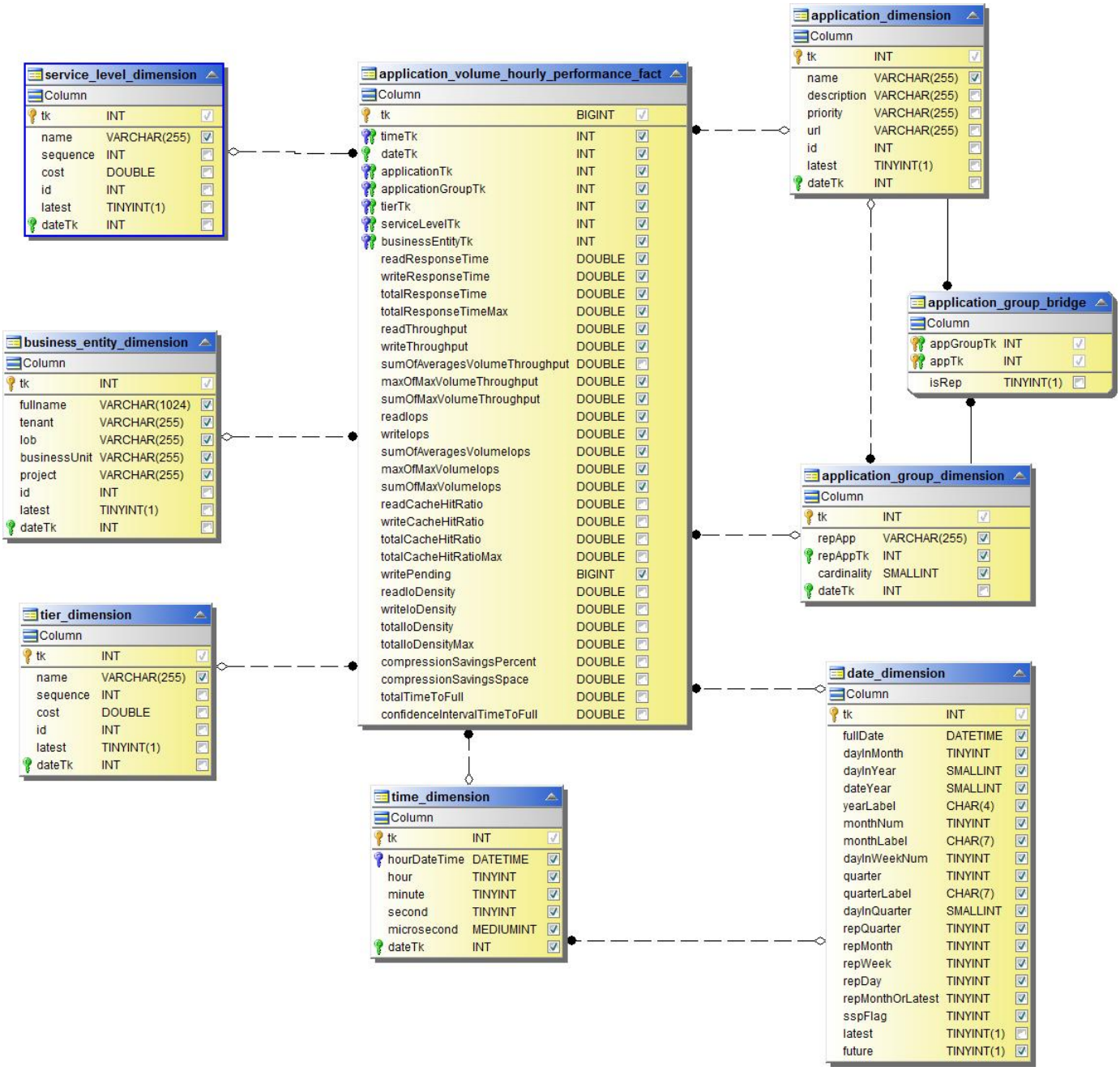
Volume-Kapazität



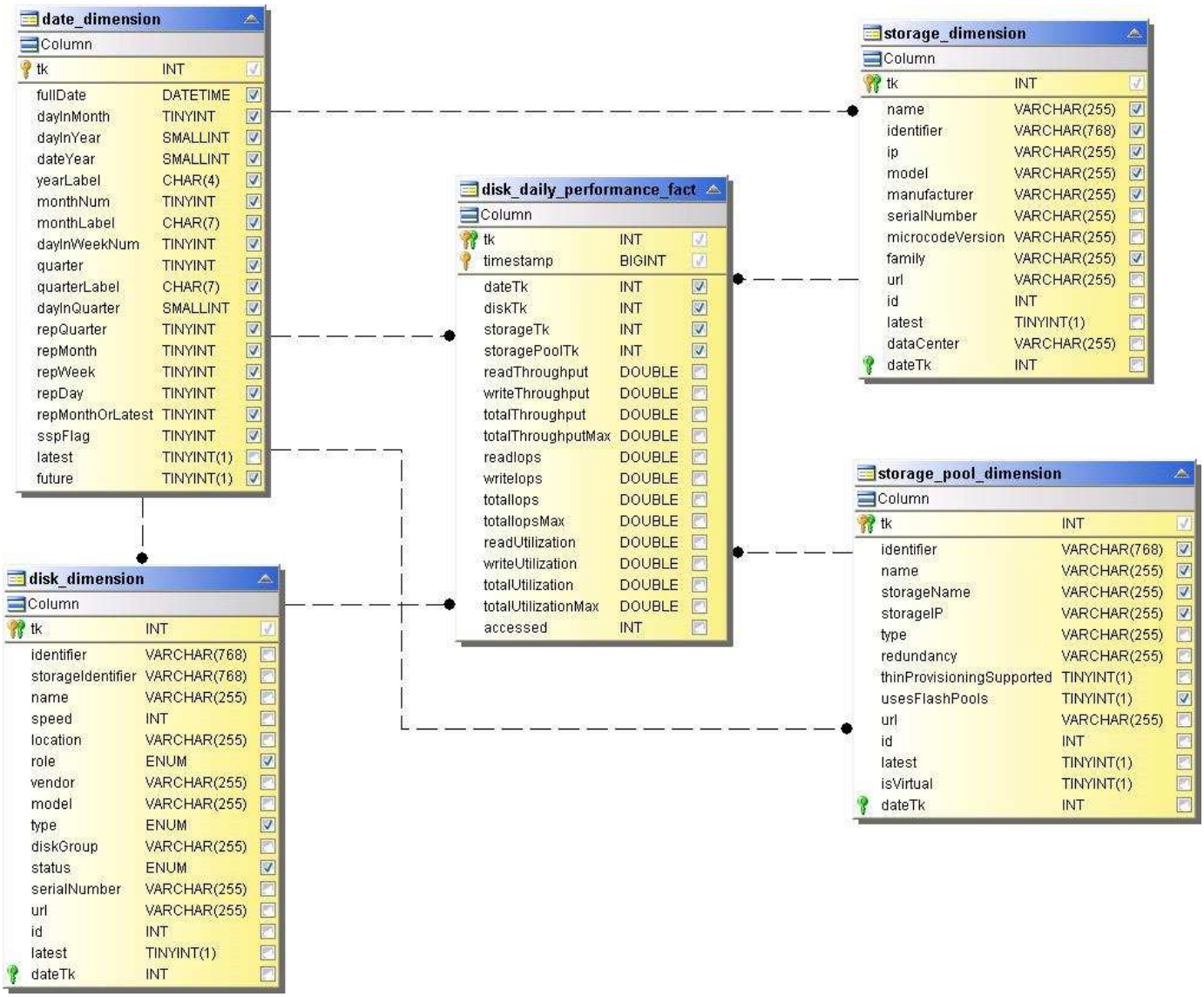
Performance Datamart

Die folgenden Bilder beschreiben das Performance-Datum.

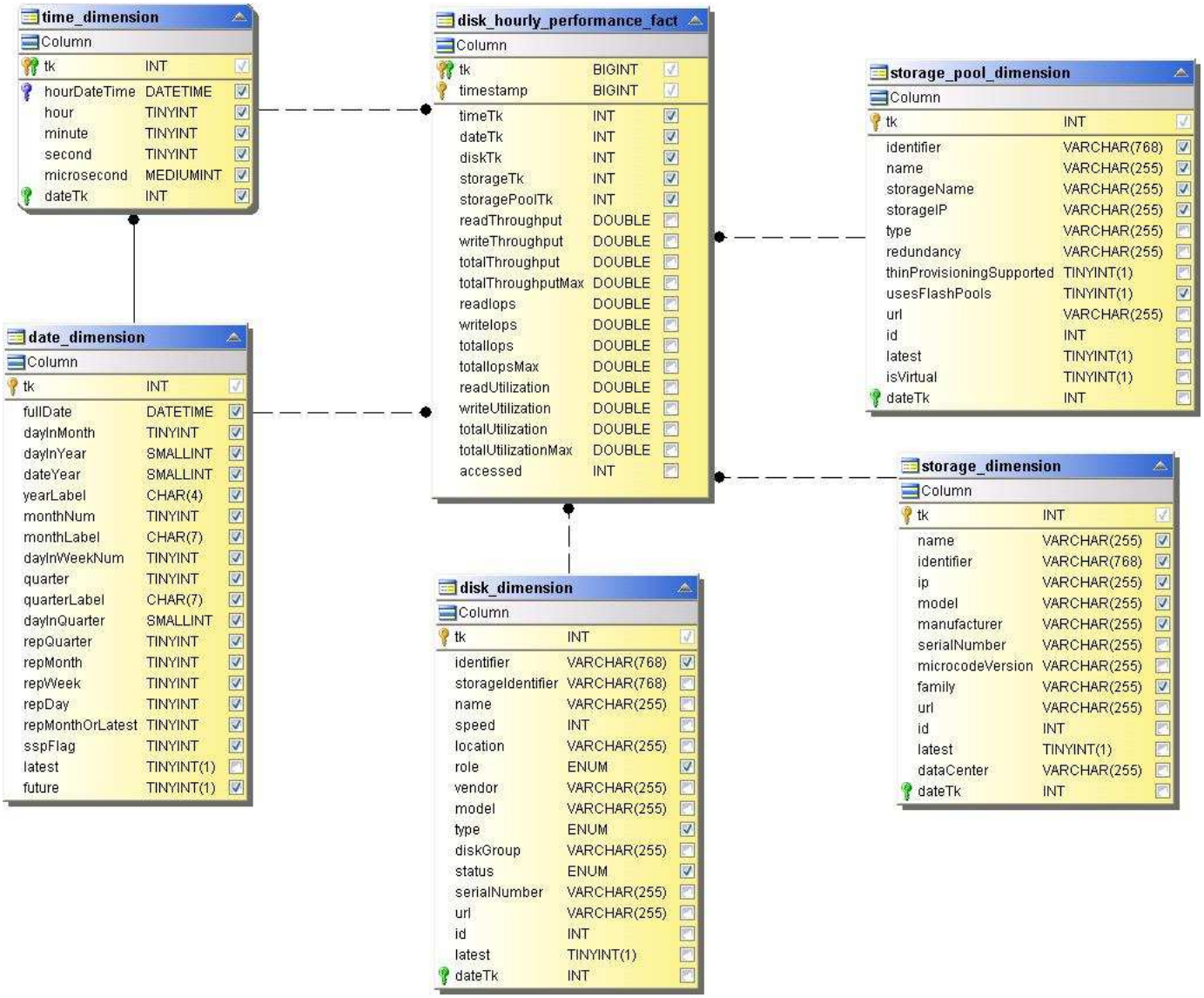
Stündliche Performance Des Applikations-Volumes



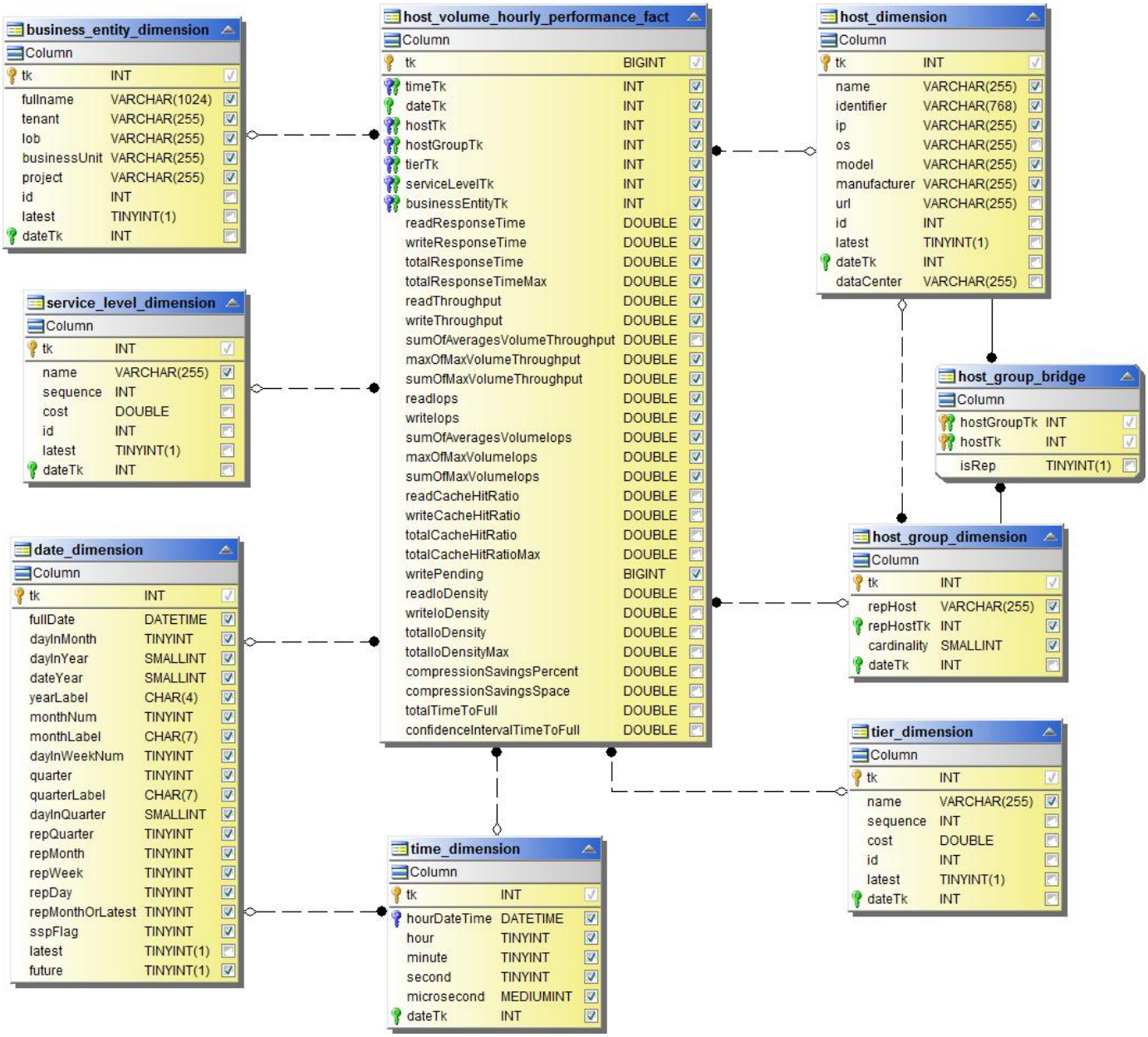
Tägliche Festplatten-Performance



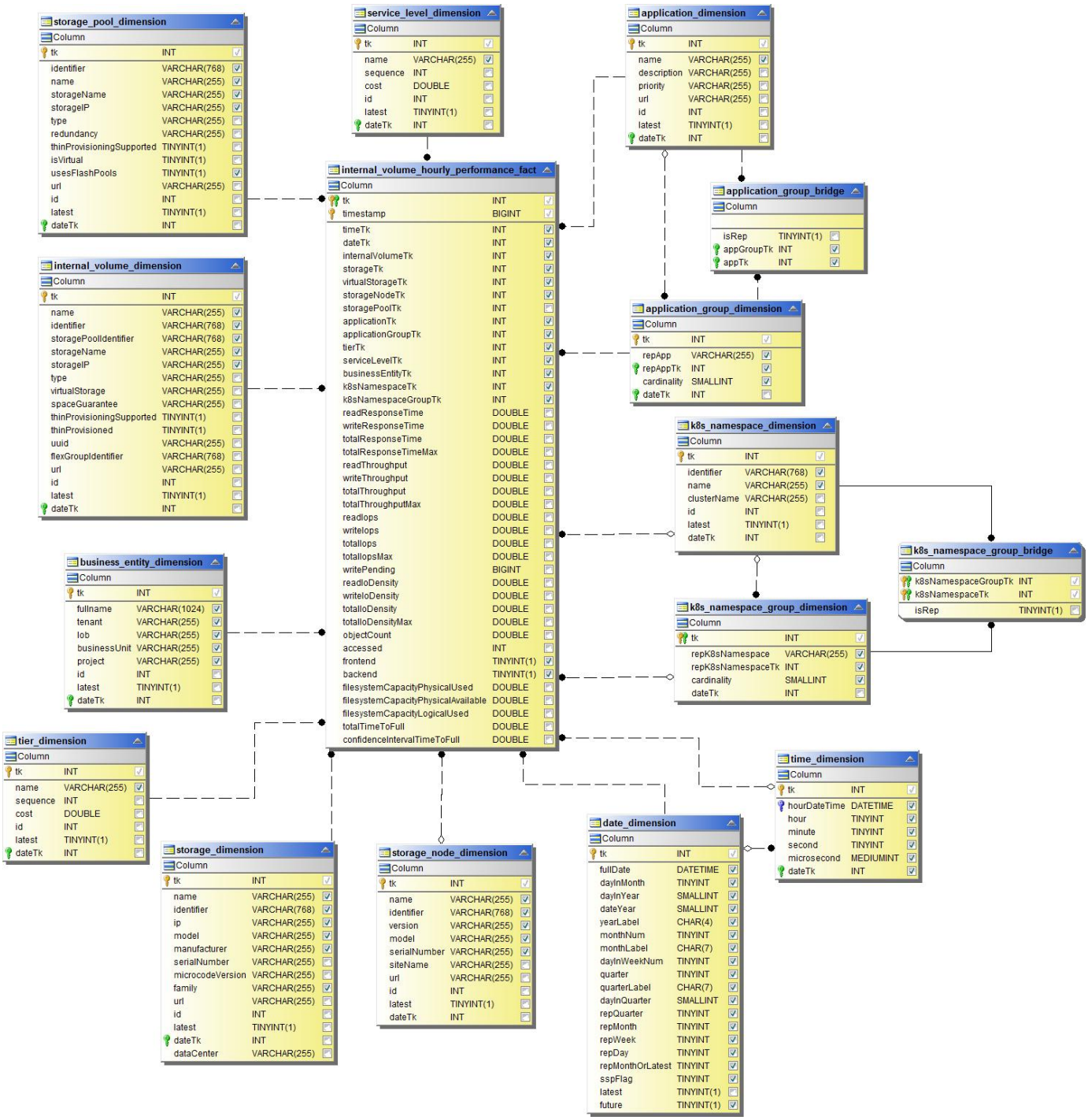
Stündliche Festplatten-Performance



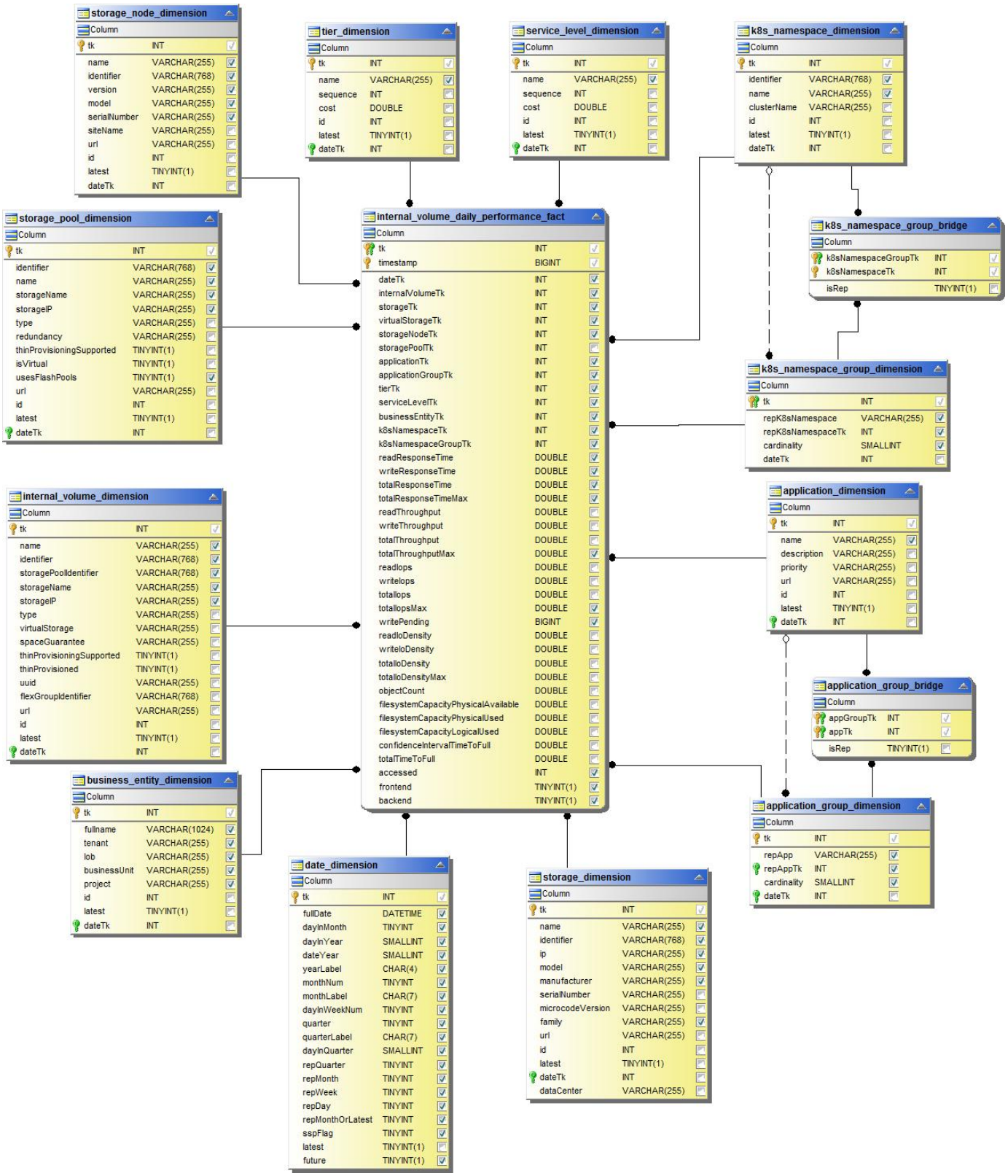
Stündliche Host-Performance



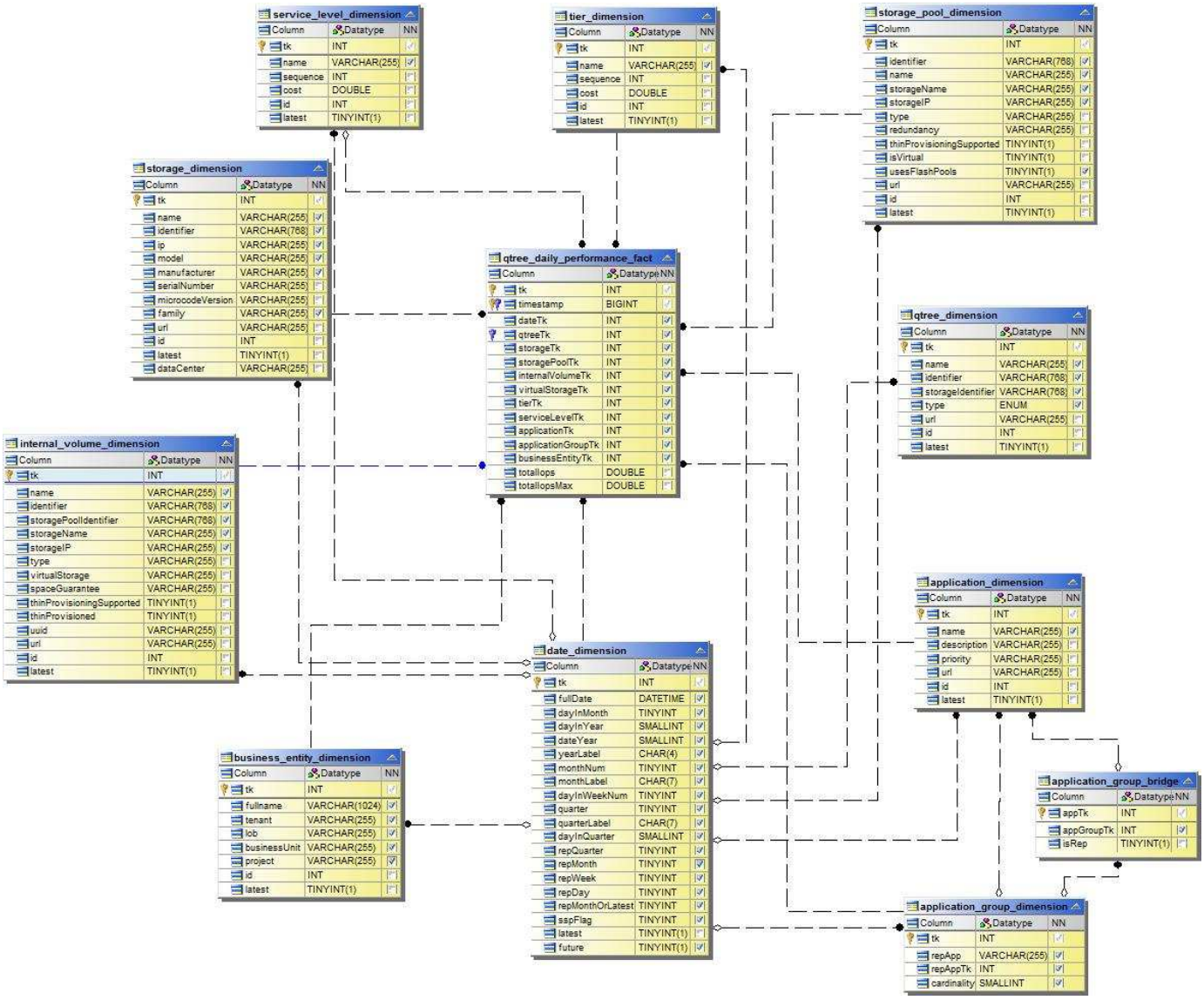
Stündliche Performance Des Internen Volumes



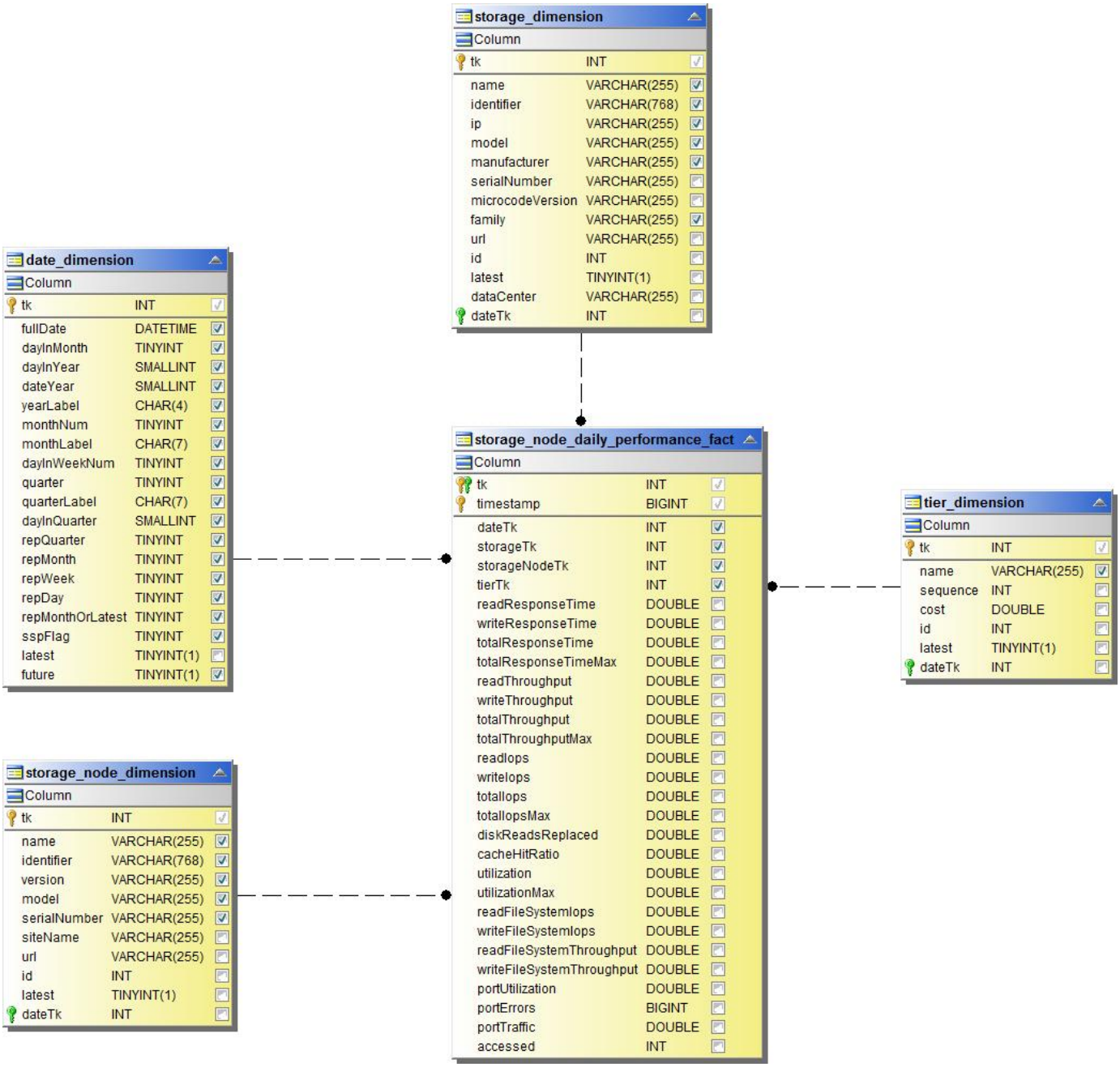
Tägliche Performance Des Internen Volumes



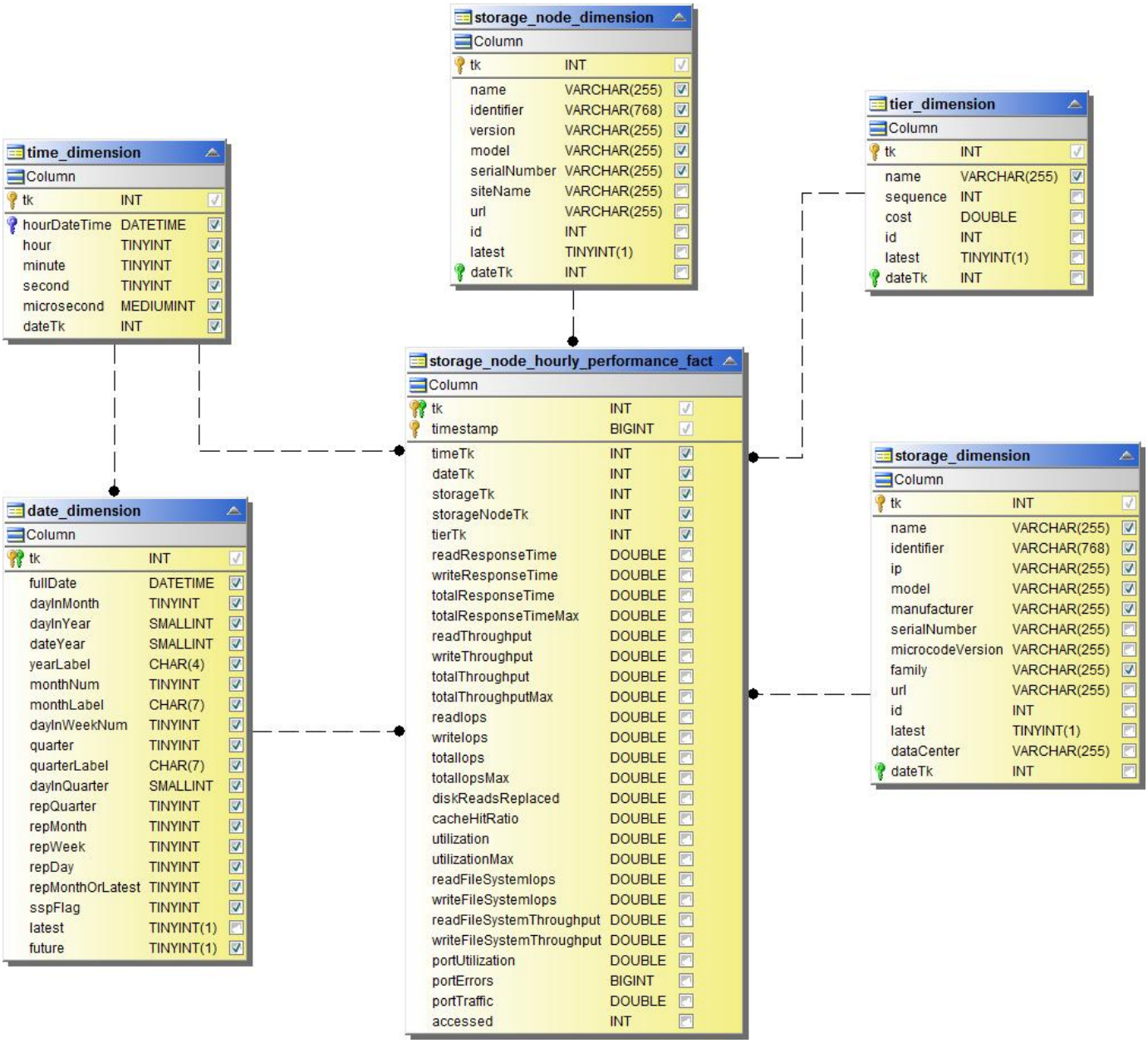
Tägliche Qtree Performance



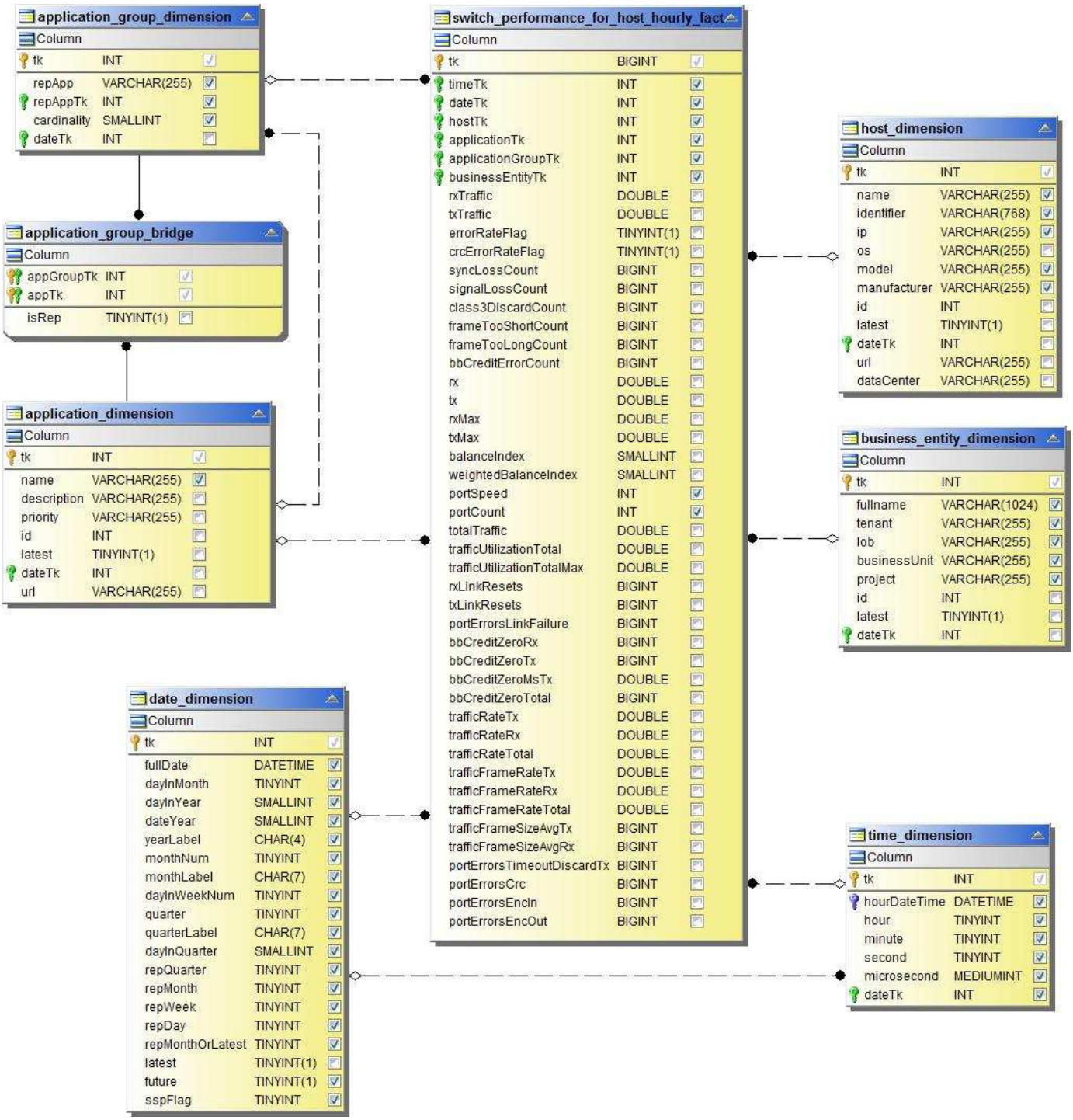
Tägliche Storage-Node-Performance



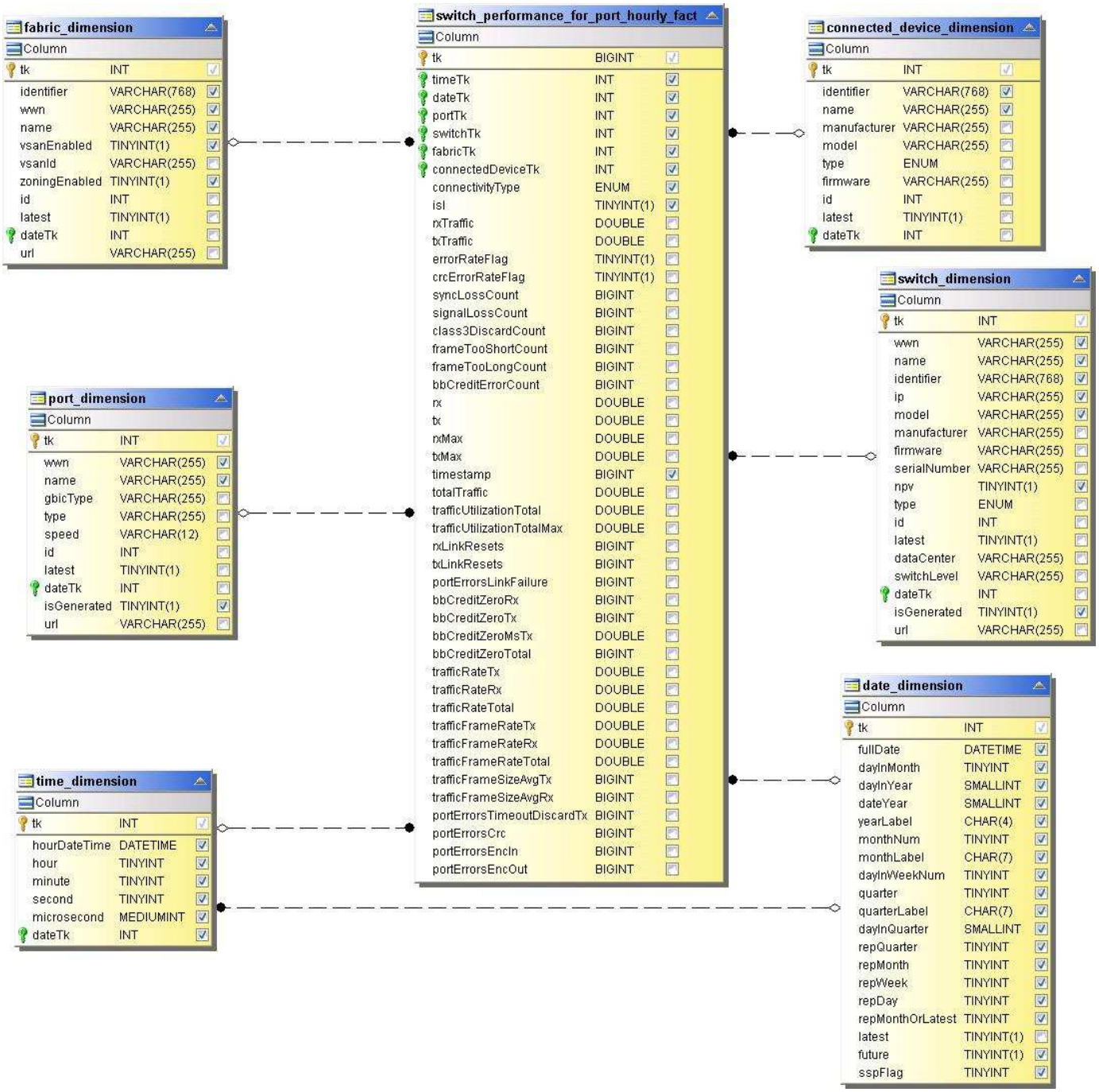
Stündliche Storage-Node-Performance



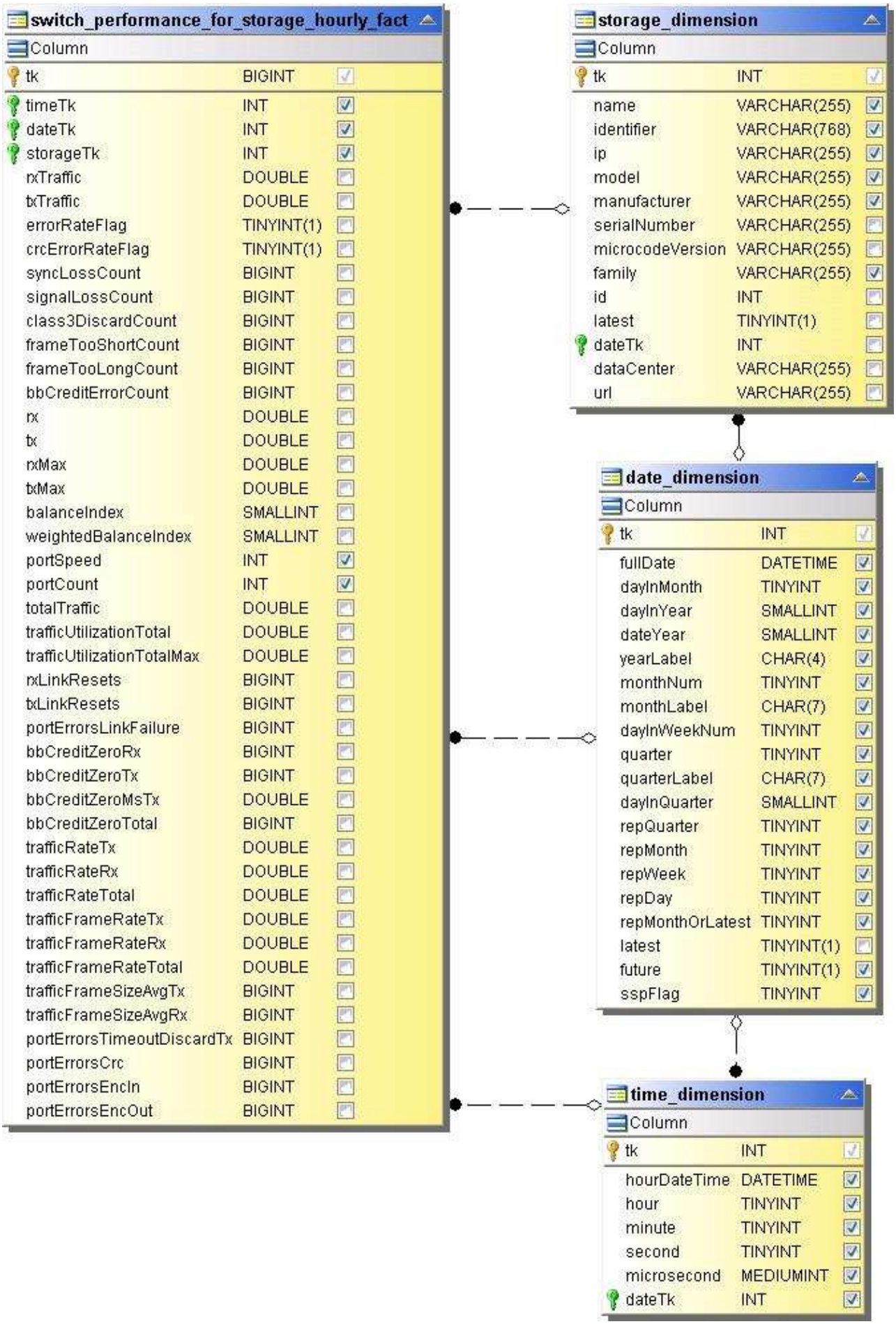
Wechseln Sie die stündliche Performance für den Host



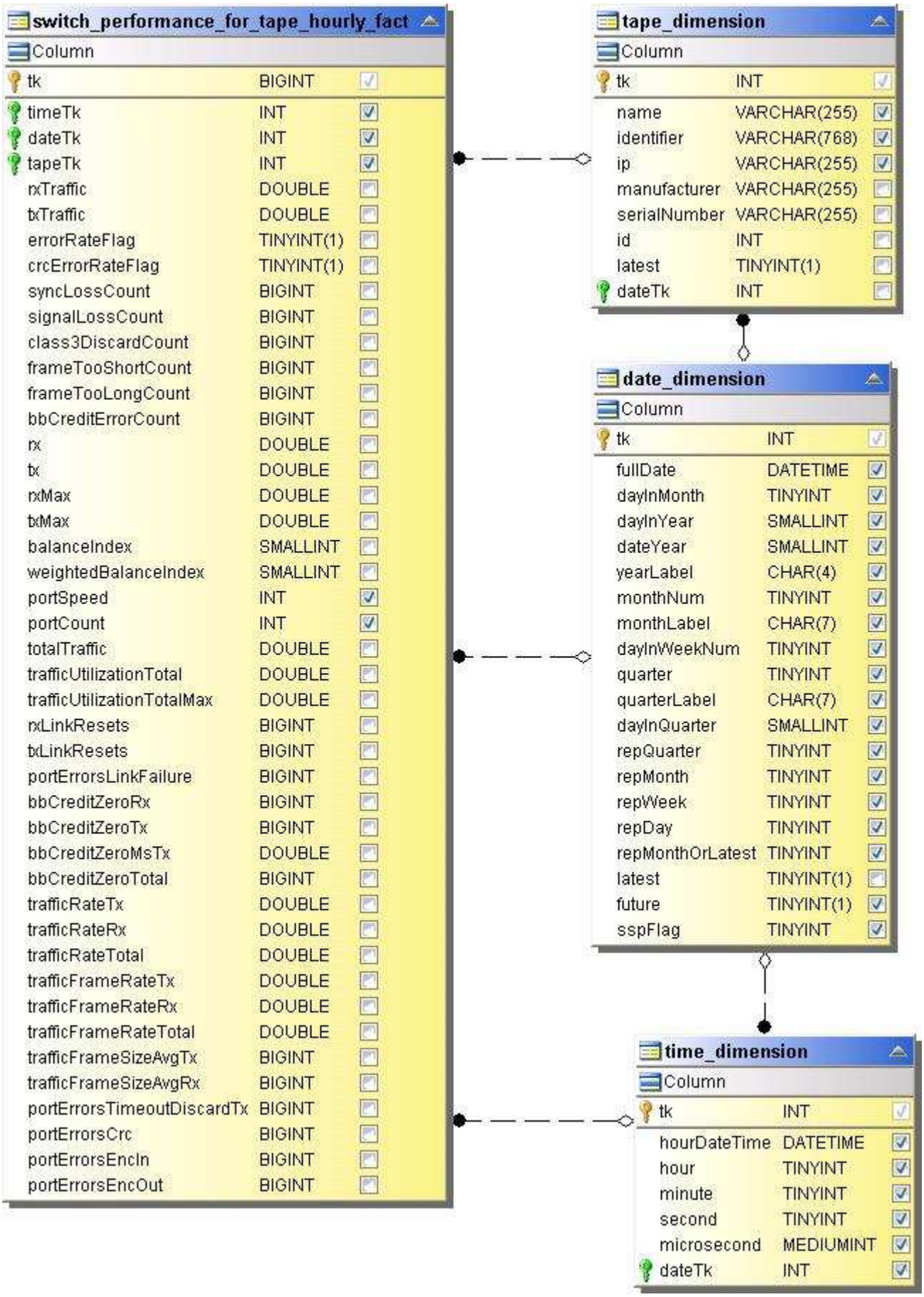
Wechseln Sie die stündliche Leistung für den Port



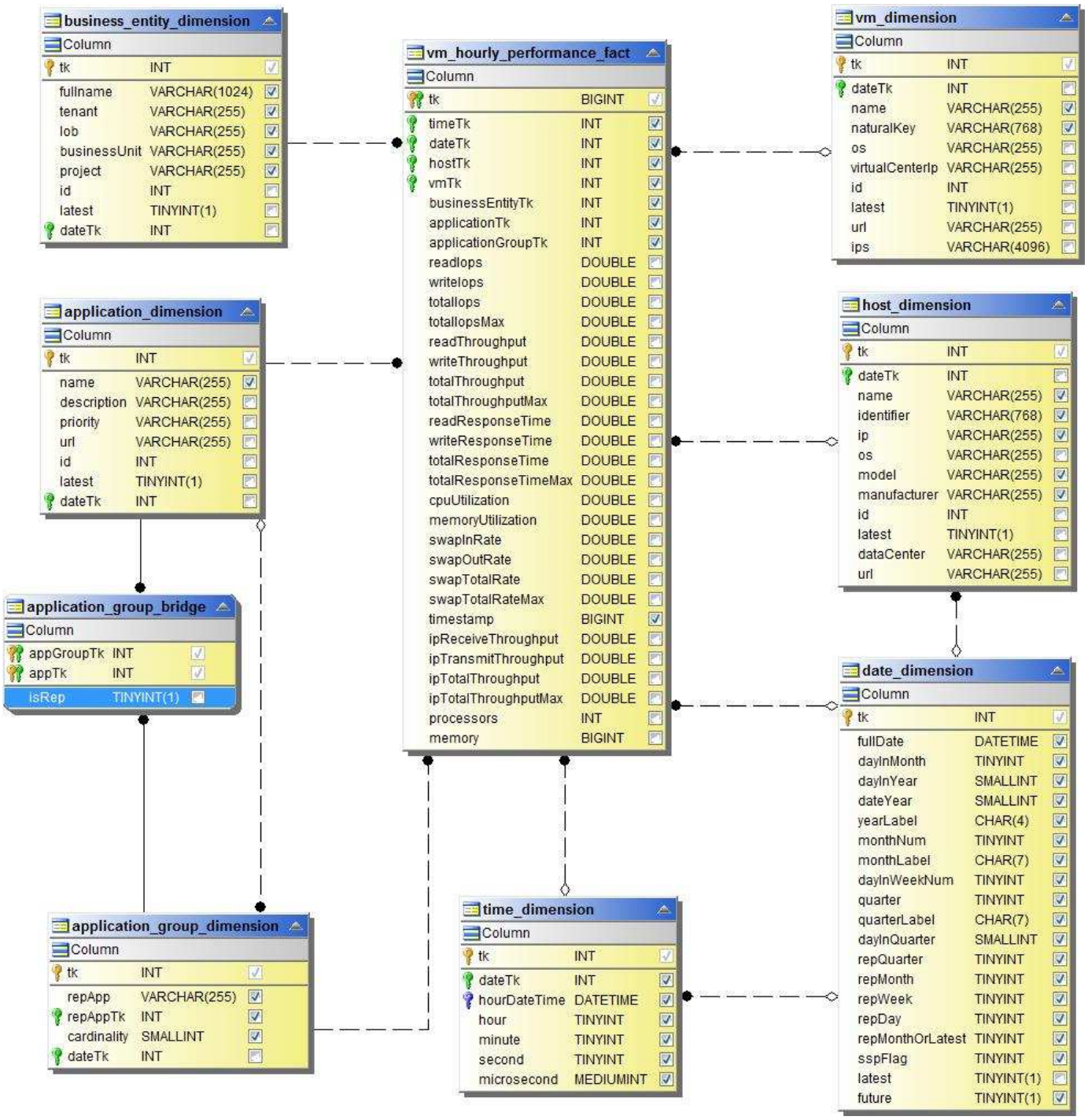
Stündliche Wechsel der Performance für Storage erforderlich


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

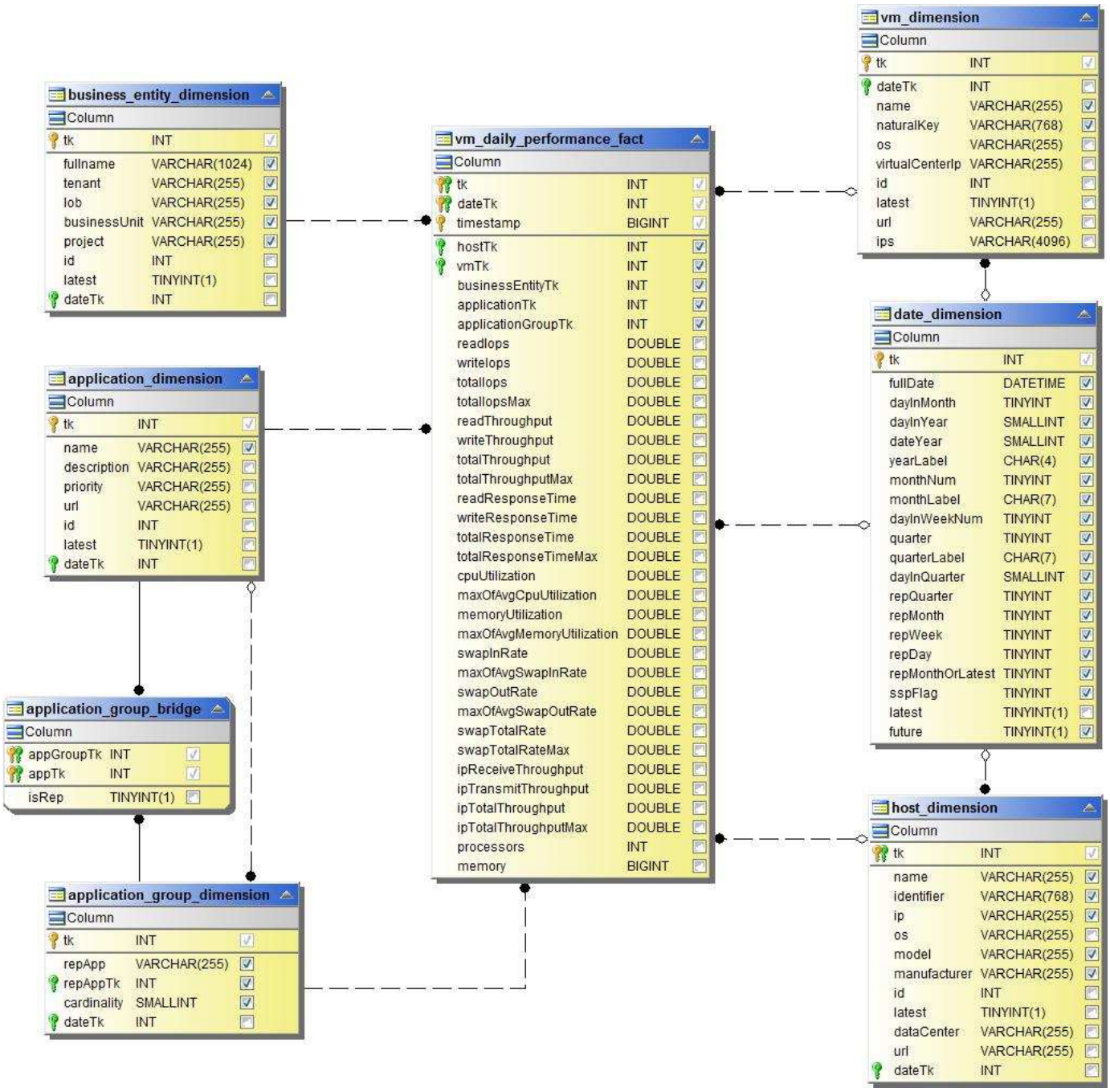
Stündliche Wechsel der Performance für Tape möglich



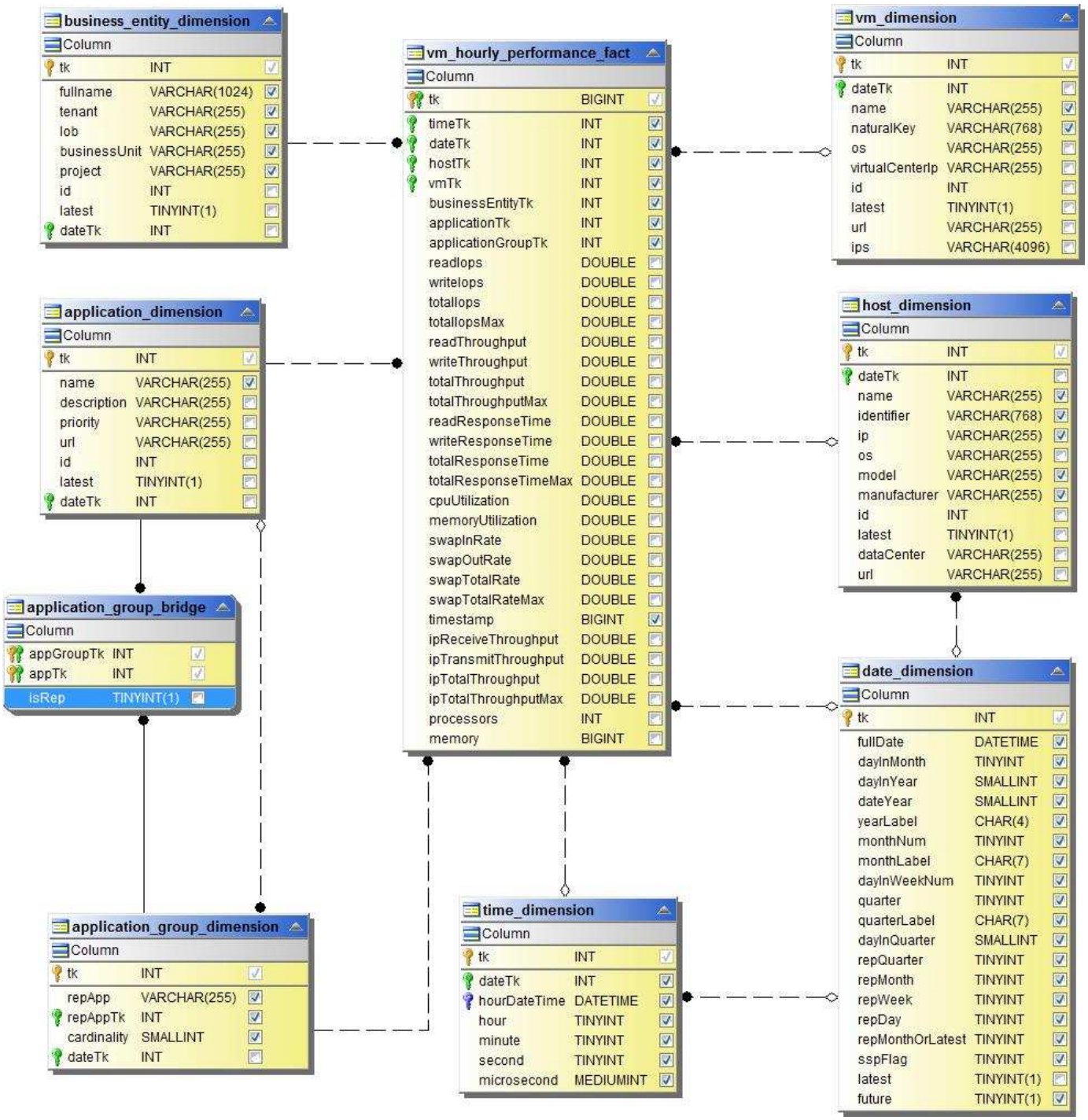
VM Performance



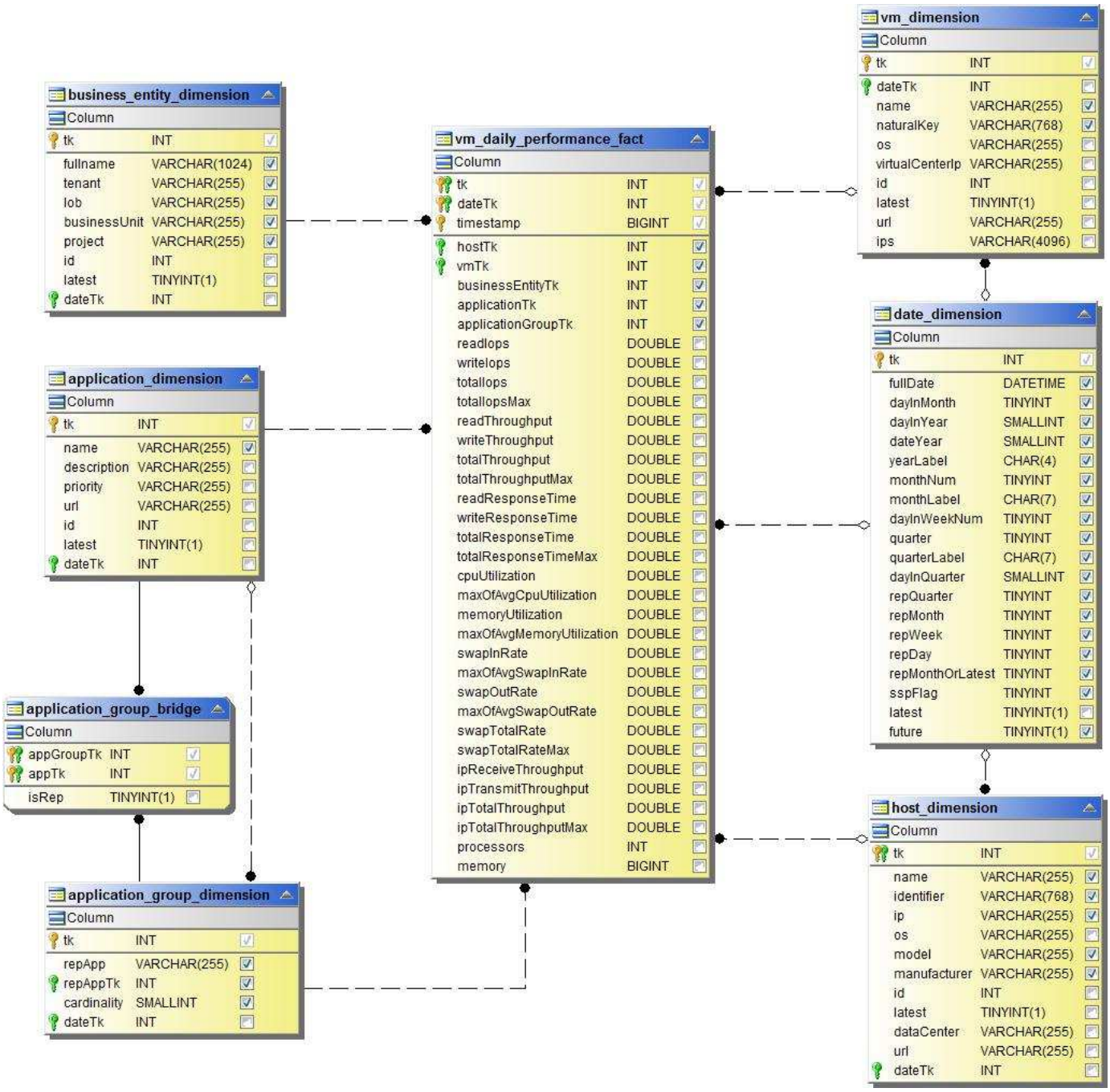
VM tägliche Performance für Host



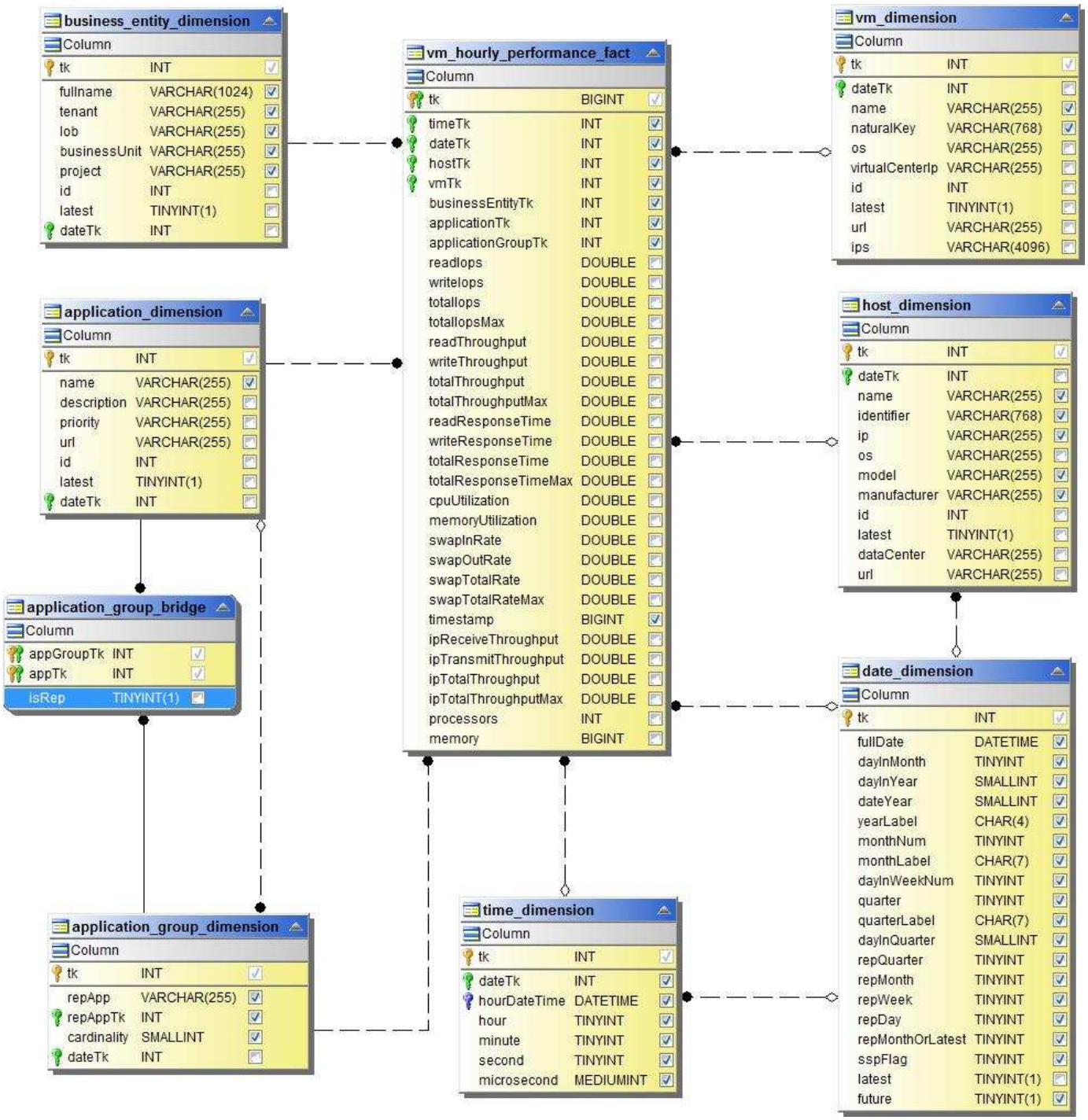
VM stündliche Performance für Host



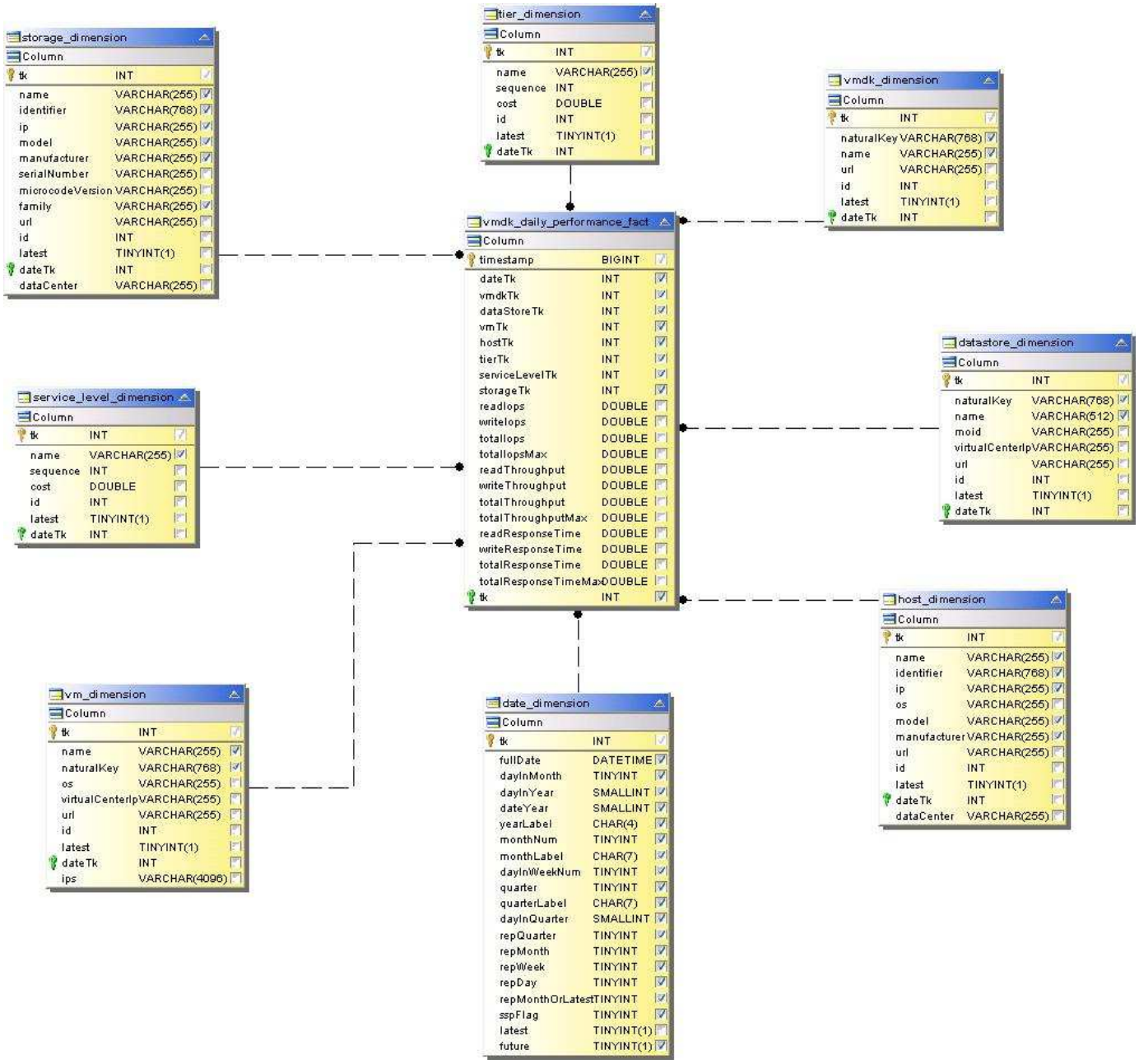
VM tägliche Performance für Host



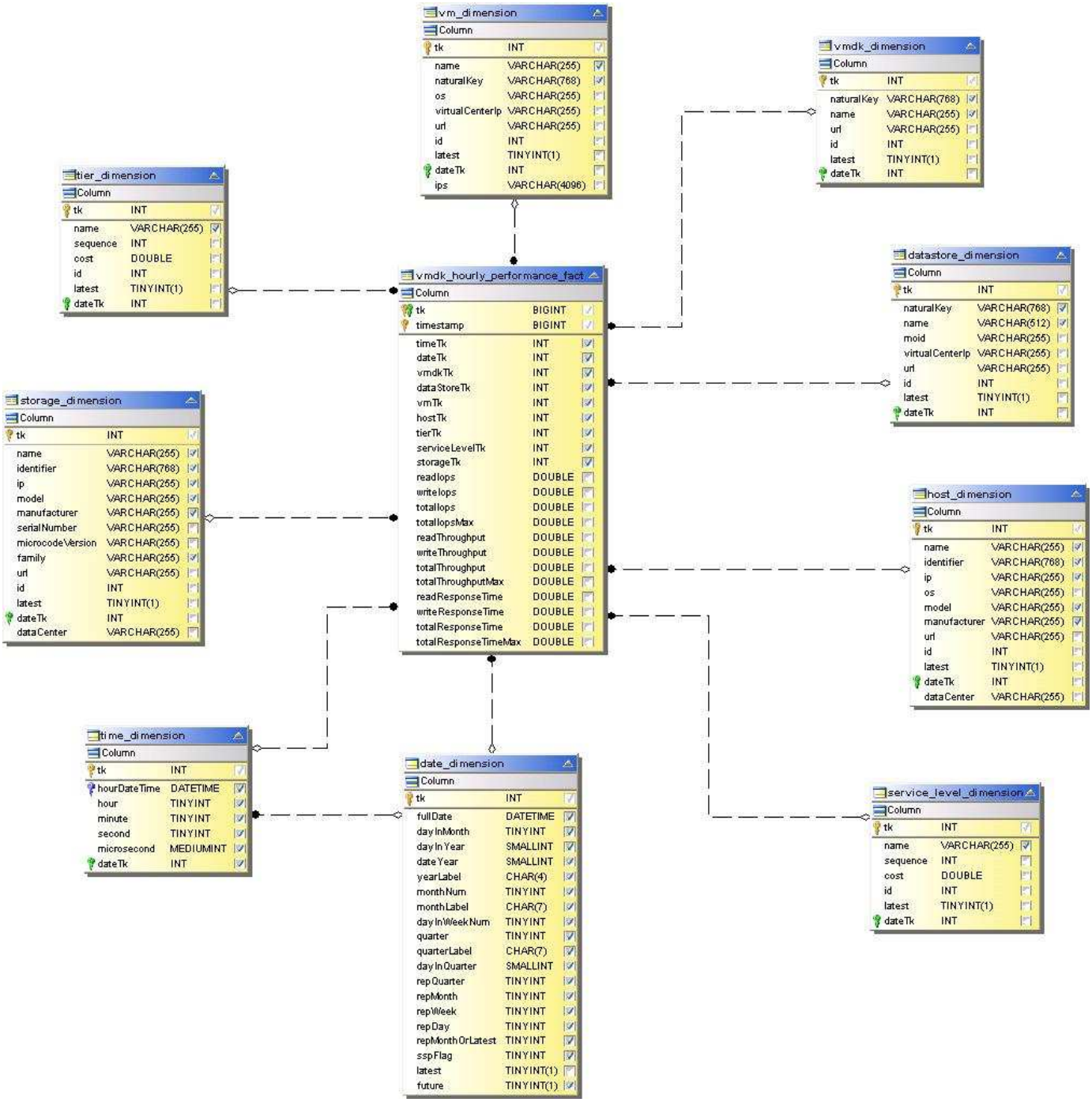
VM stündliche Performance für Host



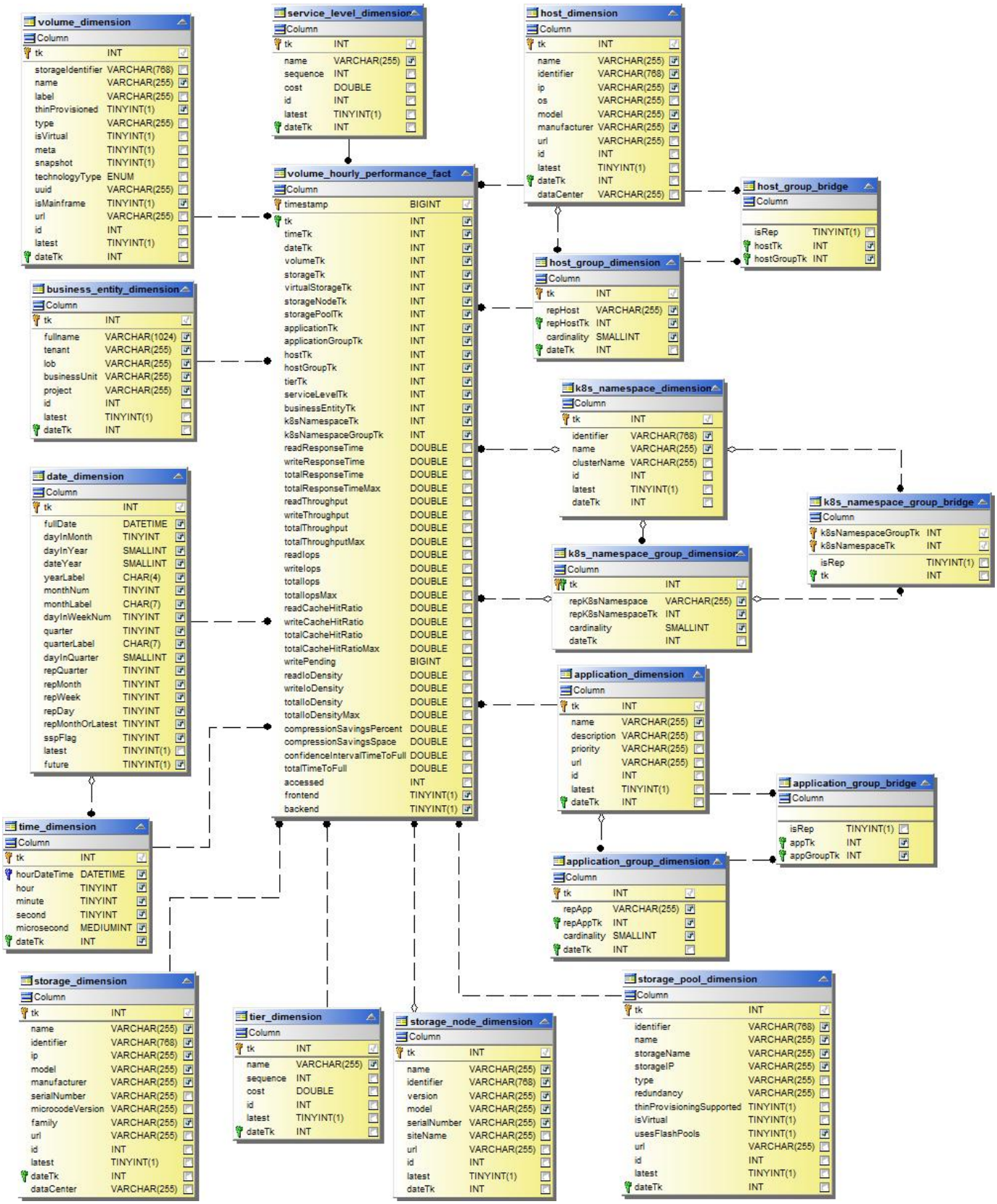
VMDK tägliche Performance



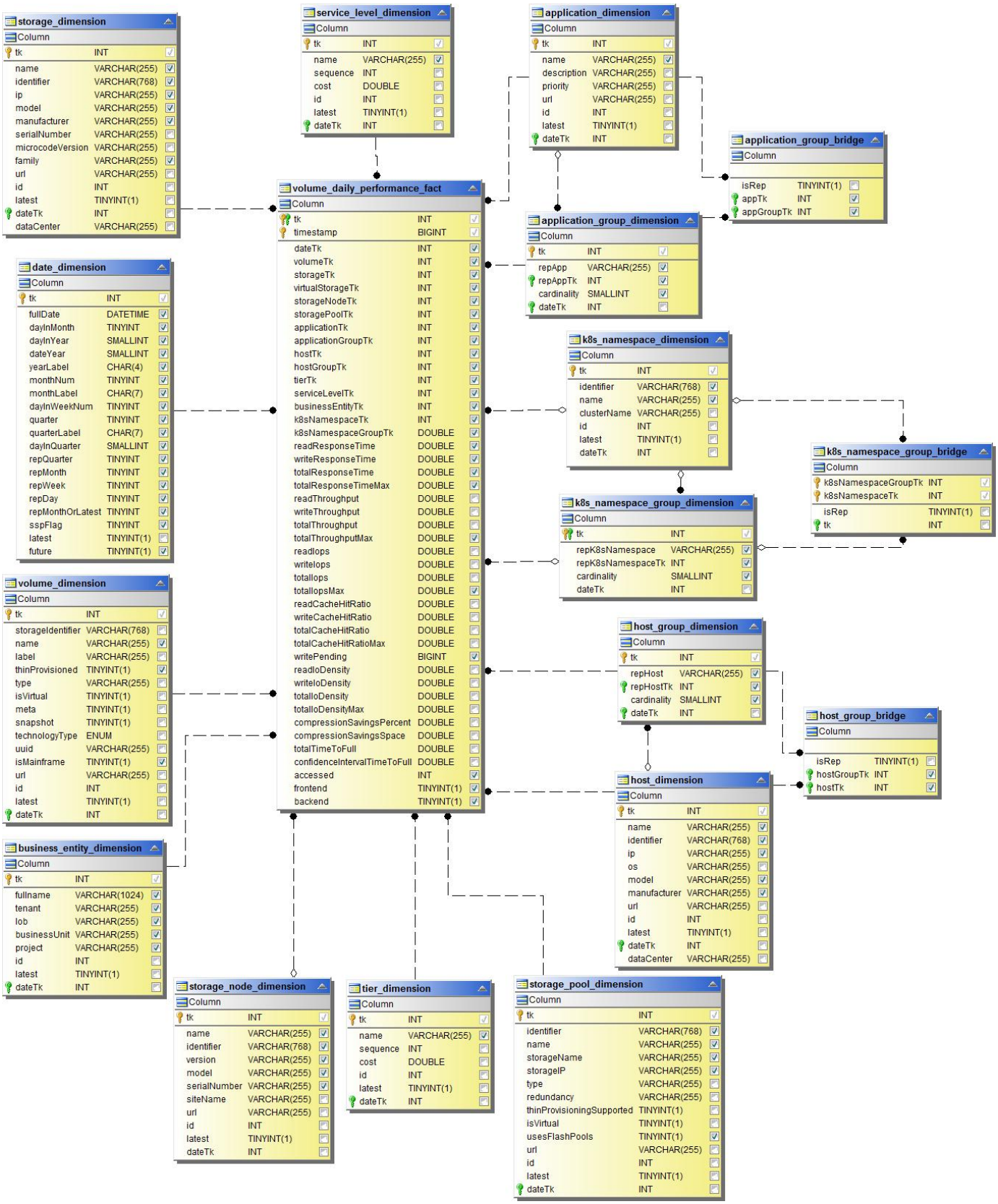
Stündliche VMDK-Performance



Stündliche Volume-Performance



Tägliche Volume Performance



Cloud Insights Schemas für Reporting

Diese Schematabellen und -Diagramme werden hier als Referenz für Cloud Insights-Berichte bereitgestellt.

"Schema-Tabellen" Im PDF-Format. Klicken Sie auf den Link zum Öffnen, oder klicken Sie mit der rechten Maustaste, und wählen Sie zum Herunterladen *Speichern unter…*.

"Schema Diagramme"

Die Berichtsfunktion ist in Cloud Insights verfügbar "Premium Edition".

Copyright-Informationen

Markeninformationen