



Beobachtbarkeit

Data Infrastructure Insights

NetApp

February 11, 2026

This PDF was generated from https://docs.netapp.com/de-de/data-infrastructure-insights/concept_dashboards_overview.html on February 11, 2026. Always check docs.netapp.com for the latest.

Inhalt

Beobachtbarkeit	1
Dashboards erstellen	1
Dashboards – Übersicht	1
Dashboard-Funktionen	5
Dashboard-Zugriffsverwaltung	39
Best Practices für Dashboards und Widgets	40
Beispiel-Dashboards	43
Arbeiten mit Abfragen	49
Abfragen von Assets und Metriken	49
Erstellen von Abfragen	50
Anzeigen von Abfragen	57
Exportieren von Abfrageergebnissen in eine CSV-Datei	58
Ändern oder Löschen einer Abfrage	59
Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen von Assets	60
Tabellenwerte kopieren	61
Protokoll-Explorer	61
Identifizieren inaktiver Geräte	67
Einblicke	68
Einblicke	68
Einblicke: Gemeinsam genutzte Ressourcen unter Druck	68
Einblicke: Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz	71
Einblicke: ONTAP Cold Storage zurückgewinnen	72
Monitore und Warnungen	75
Alarmierung mit Monitoren	75
Anzeigen und Verwalten von Warnungen von Monitoren	86
Konfigurieren von E-Mail-Benachrichtigungen	89
Anomalieerkennungsmontore	92
Systemmonitore	96
Webhook-Benachrichtigungen	184
Arbeiten mit Anmerkungen	198
Anmerkungen definieren	198
Verwenden von Anmerkungen	201
Erstellen von Anmerkungsregeln	203
Anmerkungen importieren	205
Arbeiten mit Anwendungen	208
Nachverfolgen der Asset-Nutzung nach Anwendung	208
Erstellen von Anwendungen	208
Automatische Geräteauflösung	209
Übersicht über die automatische Geräteauflösung	210
Regeln zur Geräteauflösung	212
Fibre Channel-Geräteauflösung	215
IP-Geräteauflösung	217
Einstelloptionen auf der Registerkarte „Einstellungen“	219

Beispiele für reguläre Ausdrücke	220
Informationen zur Asset-Seite	227
Übersicht über die Asset-Seite	227
Filtern nach Objekten im Kontext	233
Speichervirtualisierung	234
Hinweise und Tipps zur Suche nach Assets und Warnungen	236
Daten analysieren	238
SAN Analyzer – Übersicht	238
VM Analyzer – Übersicht	241
Überwachen des Infrastrukturzustands	243
Berichterstattung	245
Übersicht über die Data Infrastructure Insights	245
Benutzerrollen für Data Infrastructure Insights Reporting	246
Vordefinierte Berichte leicht gemacht	248
Storage Manager-Dashboard	251
Erstellen eines Berichts (Beispiel)	255
Berichte verwalten	258
Erstellen benutzerdefinierter Berichte	262
Zugriff auf die Berichtsdatenbank über die API	269
Veröffentlichung und Aufhebung der Veröffentlichung von Anmerkungen für Berichte	273
So werden historische Daten für die Berichterstellung aufbewahrt	274
Schemadiagramme für die Data Infrastructure Insights -Berichterstattung	275
Data Infrastructure Insights Schemas für die Berichterstellung	328

Beobachtbarkeit

Dashboards erstellen

Dashboards – Übersicht

Data Infrastructure Insights bietet Benutzern die Flexibilität, Betriebsansichten von Infrastrukturdaten zu erstellen, indem Sie benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen können, von denen jedes umfassende Flexibilität bei der Anzeige und Diagrammerstellung Ihrer Daten bietet.



Die Beispiele in diesen Abschnitten dienen nur zu Erklärungs Zwecken und decken nicht jedes mögliche Szenario ab. Mit den hierin enthaltenen Konzepten und Schritten können Sie Ihre eigenen Dashboards erstellen, um die Daten hervorzuheben, die für Ihre speziellen Anforderungen spezifisch sind.

Erstellen eines Dashboards

Sie erstellen ein neues Dashboard an einem von zwei Orten:

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

Sehen Sie es in Aktion

[Erstellen Sie leistungsstarke Dashboards mit NetApp \(Video\)](#), [Fenster=Später lesen](#)

Dashboard-Steuerelemente

Der Dashboard-Bildschirm verfügt über mehrere Steuerelemente:

- **Zeitauswahl:** Ermöglicht Ihnen die Anzeige von Dashboard-Daten für einen Zeitraum von den letzten 15 Minuten bis zu den letzten 30 Tagen oder einen benutzerdefinierten Zeitraum von bis zu 31 Tagen. Sie können diesen globalen Zeitbereich in einzelnen Widgets überschreiben.
- Schaltfläche **Speichern:** Ermöglicht Ihnen, das Dashboard zu speichern oder zu löschen.

Sie können das aktuelle Dashboard umbenennen, indem Sie im Menü „Speichern“ auf „Umbenennen“ klicken.

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

Die Größe von Widgets kann geändert und sie können an verschiedene Positionen innerhalb des Dashboards verschoben werden, um Ihnen entsprechend Ihren aktuellen Anforderungen die beste Ansicht Ihrer Daten zu bieten.

- Schaltfläche **+ Variable hinzufügen**, mit der Sie Variablen verwenden können, um die Dashboard-Daten aktiv zu filtern.

Widget-Typen

Sie können aus den folgenden Widget-Typen wählen:

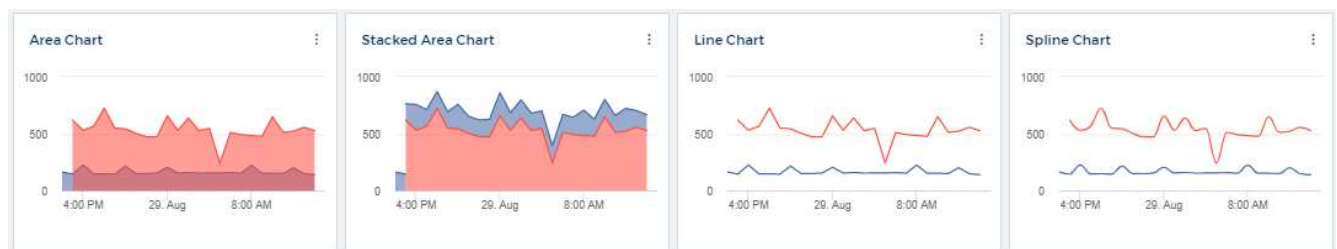
- **Tabellen-Widget:** Eine Tabelle, die Daten entsprechend den von Ihnen ausgewählten Filtern und Spalten anzeigt. Tabellendaten können in Gruppen zusammengefasst werden, die ein- und ausgeblendet werden können.

GroupBy Date 🔄 1h

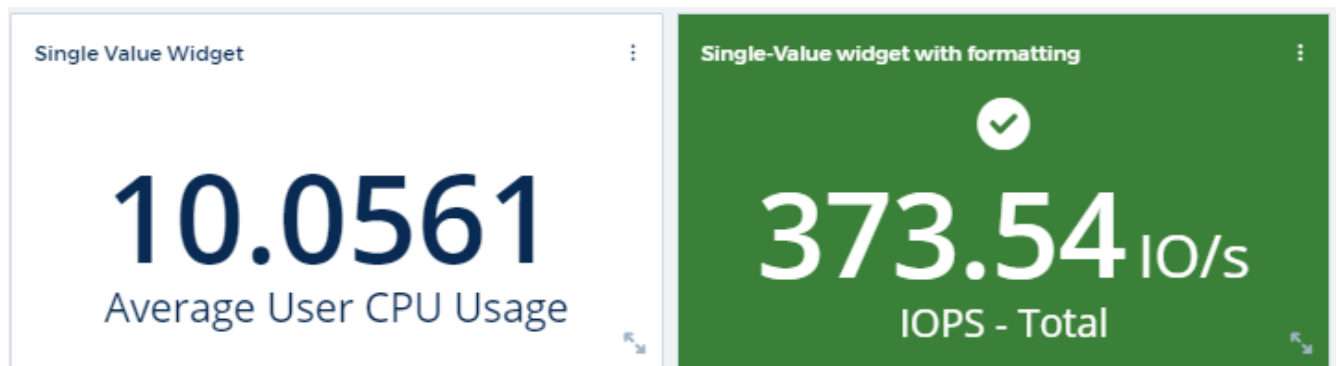
4 items found in 2 groups

Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...	IOPS - Write (I...	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

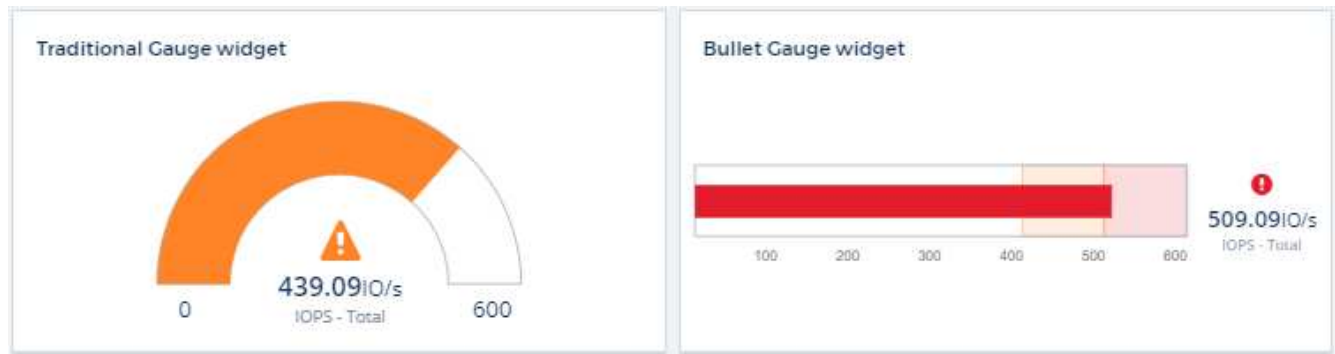
- **Linien-, Spline-, Flächen- und gestapelte Flächendiagramme:** Dies sind Zeitreihendiagramm-Widgets, auf denen Sie die Leistung und andere Daten im Zeitverlauf anzeigen können.



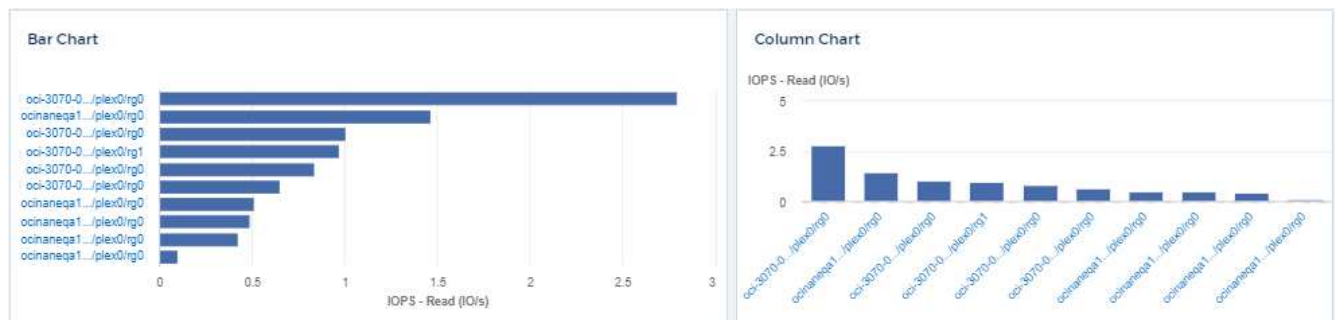
- **Einzelwert-Widget:** Ein Widget, mit dem Sie einen einzelnen Wert anzeigen können, der entweder direkt von einem Zähler abgeleitet oder mithilfe einer Abfrage oder eines Ausdrucks berechnet werden kann. Sie können Schwellenwerte für die Farbformatierung definieren, um anzuzeigen, ob der Wert im erwarteten, Warn- oder kritischen Bereich liegt.



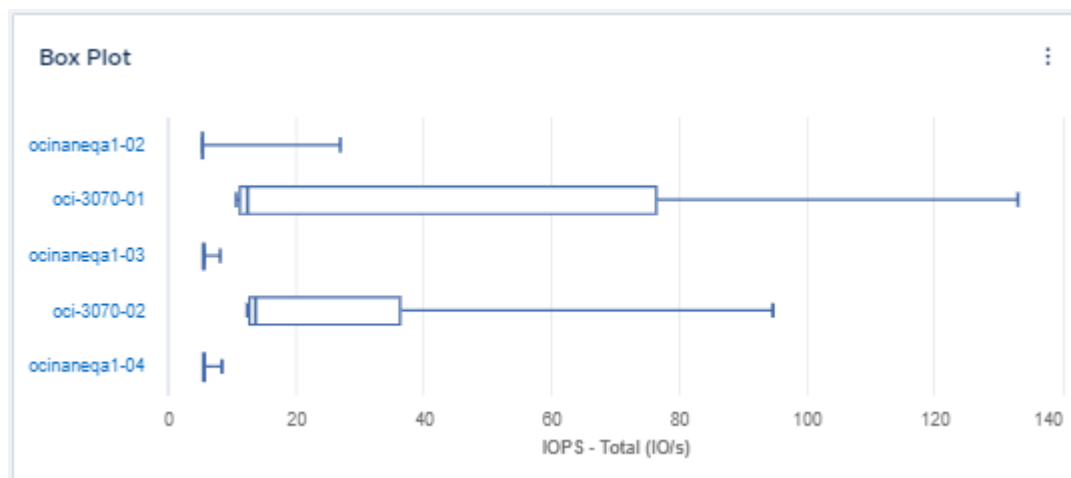
- **Messgerät-Widget:** Zeigt Einzelwertdaten in einem herkömmlichen (durchgezogenen) Messgerät oder Bullet-Messgerät an, mit Farben basierend auf den von Ihnen gewählten "Warn-" oder "Kritischen" Werten "anpassen" .



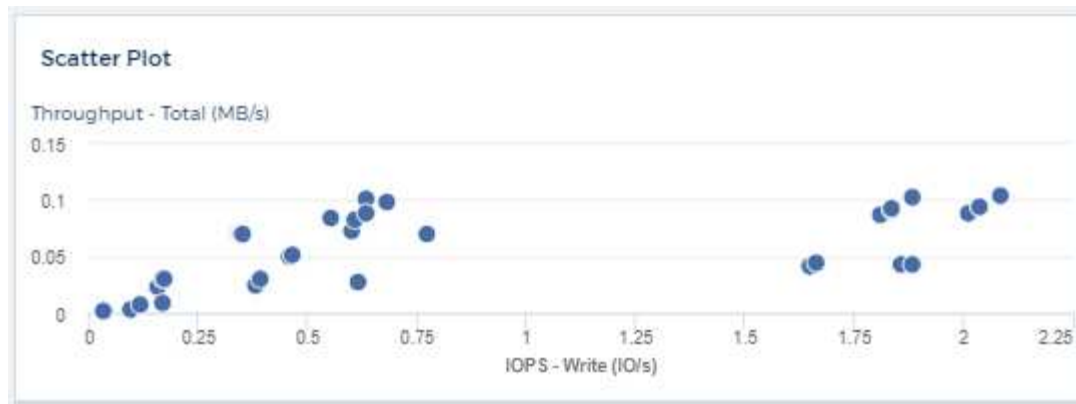
- **Balken-, Säulendiagramme:** Zeigt die höchsten oder niedrigsten N-Werte an, z. B. die zehn größten Speicher nach Kapazität oder die fünf untersten Volumes nach IOPS.



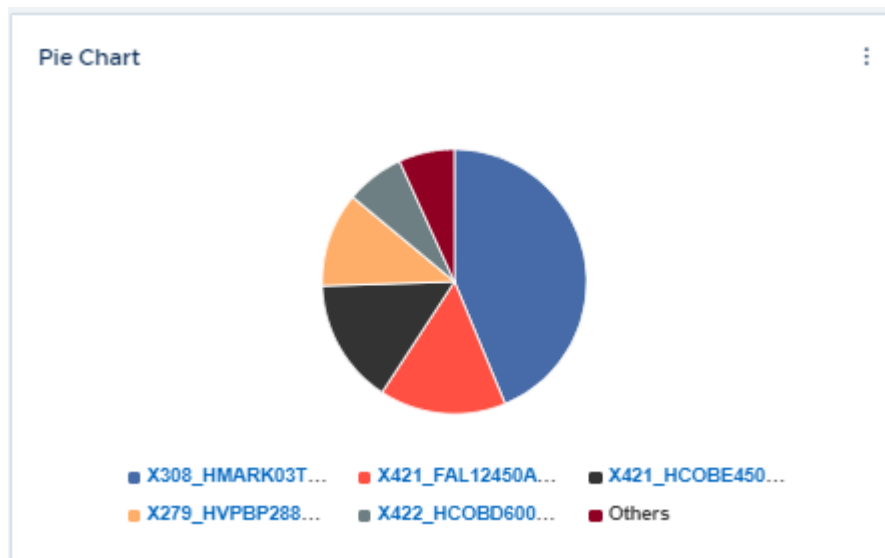
- **Boxplot-Diagramm:** Eine Darstellung des Minimums, Maximums, Medians und des Bereichs zwischen dem unteren und oberen Quartil der Daten in einem einzigen Diagramm.



- **Streudiagramm:** Stellt verwandte Daten als Punkte dar, beispielsweise IOPS und Latenz. In diesem Beispiel können Sie schnell Assets mit hohem Durchsatz und niedrigem IOPS finden.



- **Kreisdiagramm:** ein traditionelles Kreisdiagramm zur Anzeige von Daten als Teil des Gesamtwerts.



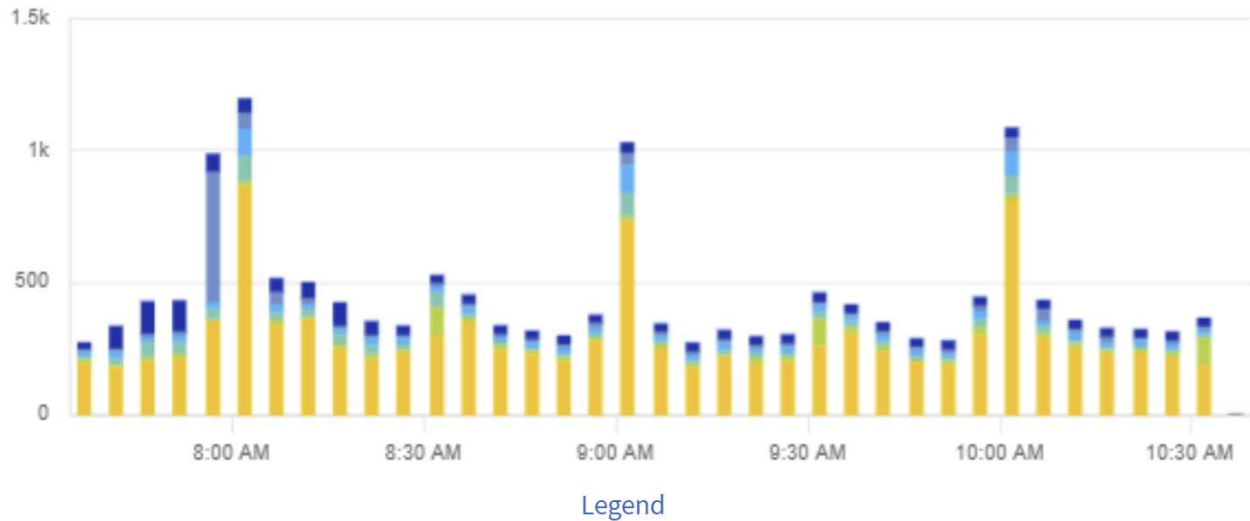
- **Notiz-Widget:** Bis zu 1000 Zeichen Freitext.

Note Widget (with link)

This is a note. You can type any text you like in here, for example, to give details about the purpose of a particular dashboard.

You can also include [links](#) in your note.

- **Zeitbalkendiagramm:** Zeigt Protokoll- oder Messdaten im Zeitverlauf an.



- **Warnungstabelle:** Zeigt bis zu den letzten 1.000 Warnungen an.

Ausführlichere Erklärungen zu diesen und anderen Dashboard-Funktionen finden Sie unter ["klicken Sie hier,"](#).

Ein Dashboard als Startseite festlegen

Sie können mit einer der folgenden Methoden auswählen, welches Dashboard als **Startseite** Ihres Mandanten festgelegt werden soll:

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

Dashboard-Funktionen

Dashboards und Widgets ermöglichen große Flexibilität bei der Datenanzeige. Hier sind einige Konzepte, die Ihnen dabei helfen, das Beste aus Ihren benutzerdefinierten Dashboards herauszuholen.

Inhaltsverzeichnis:[]

Widget-Benennung

Widgets werden automatisch basierend auf dem Objekt, der Metrik oder dem Attribut benannt, das für die erste Widget-Abfrage ausgewählt wurde. Wenn Sie zusätzlich eine Gruppierung für das Widget wählen, werden die „Gruppieren nach“-Attribute in die automatische Benennung (Aggregationsmethode und Metrik) einbezogen.

Maximum cpu.time_active by agent_node_ip

Cancel
Save

C
B
A

☒ A) Query

Chart Type: Bar Chart ▼

Chart Color: ■ ▼

Decimal Places: 2 ▼

Convert to Expression

Object agent.node x ▼

Metric cpu.time_active x ▼

Display Unit: cpu.time_active (None)

Display Last 24 Hours ▼

Aggregated by Last ▼

Save
Reset

Filter by Attribute +

Filter by Metric +

Group by agent_node_ip x ▼

aggregated by Maximum ▼

Apply f(x)

Rank Top ▼

10

A
C

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.

Platzierung und Größe des Widgets

Alle Dashboard-Widgets können entsprechend Ihren Anforderungen für das jeweilige Dashboard positioniert und in der Größe angepasst werden.

Duplizieren eines Widgets

Klicken Sie im Dashboard-Bearbeitungsmodus auf das Menü im Widget und wählen Sie **Duplizieren**. Der Widget-Editor wird gestartet und ist bereits mit der Konfiguration des Original-Widgets und dem Suffix „Kopie“ im Widget-Namen ausgefüllt. Sie können problemlos alle erforderlichen Änderungen vornehmen und das neue Widget speichern. Das Widget wird unten in Ihrem Dashboard platziert und Sie können es nach Bedarf positionieren. Denken Sie daran, Ihr Dashboard zu speichern, wenn alle Änderungen abgeschlossen sind.

Anzeigen von Widget-Legenden

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

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

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

Wenn Legenden angezeigt werden und die Zielseite des durch die Legende angegebenen Assets aufgerufen werden kann, wird die Legende als Link zu dieser Asset-Seite angezeigt. Wenn in der Legende „Alle“ angezeigt wird, wird durch Klicken auf den Link eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Metriken transformieren

Data Infrastructure Insights bietet verschiedene *Transformations*optionen für bestimmte Metriken in Widgets (insbesondere die als „Benutzerdefiniert“ oder „Integrationsmetriken“ bezeichneten Metriken, z. B. von Kubernetes, ONTAP Advanced Data, Telegraf-Plugins usw.), sodass Sie die Daten auf verschiedene Arten anzeigen können. Wenn Sie einem Widget transformierbare Metriken hinzufügen, wird Ihnen ein Dropdown-

Menü mit den folgenden Transformationsoptionen angezeigt:

Keine: Die Daten werden unverändert und ohne Manipulation angezeigt.

Rate: Aktueller Wert geteilt durch den Zeitraum seit der letzten Beobachtung.

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

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

Deltarate: Deltawert geteilt durch den Zeitraum seit der letzten Beobachtung.

Kumulative Rate: Kumulativer Wert geteilt durch den Zeitraum seit der letzten Beobachtung.

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

Dashboard-Widget-Abfragen und -Filter

Abfragen

Die Abfrage in einem Dashboard-Widget ist ein leistungsstarkes Tool zum Verwalten der Anzeige Ihrer Daten. Hier sind einige Dinge, die Sie bei Widget-Abfragen beachten sollten.

Einige Widgets können bis zu fünf Abfragen haben. Jede Abfrage zeichnet ihren eigenen Satz von Linien oder Diagrammen im Widget. Das Festlegen von Rollup, Gruppierung, Top-/Bottom-Ergebnissen usw. für eine Abfrage hat keine Auswirkungen auf andere Abfragen für das Widget.

Sie können auf das Augensymbol klicken, um eine Abfrage vorübergehend auszublenden. Die Widget-Anzeige wird automatisch aktualisiert, wenn Sie eine Abfrage ausblenden oder anzeigen. Auf diese Weise können Sie beim Erstellen Ihres Widgets Ihre angezeigten Daten für einzelne Abfragen überprüfen.

Die folgenden Widgettypen können mehrere Abfragen haben:

- Flächendiagramm
- Gestapeltes Flächendiagramm
- Liniendiagramm
- Spline-Diagramm
- Einzelwert-Widget

Die übrigen Widgettypen können nur eine einzige Abfrage haben:

- Tabelle
- Balkendiagramm
- Boxplot
- Streudiagramm

Filtern in Dashboard-Widget-Abfragen

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

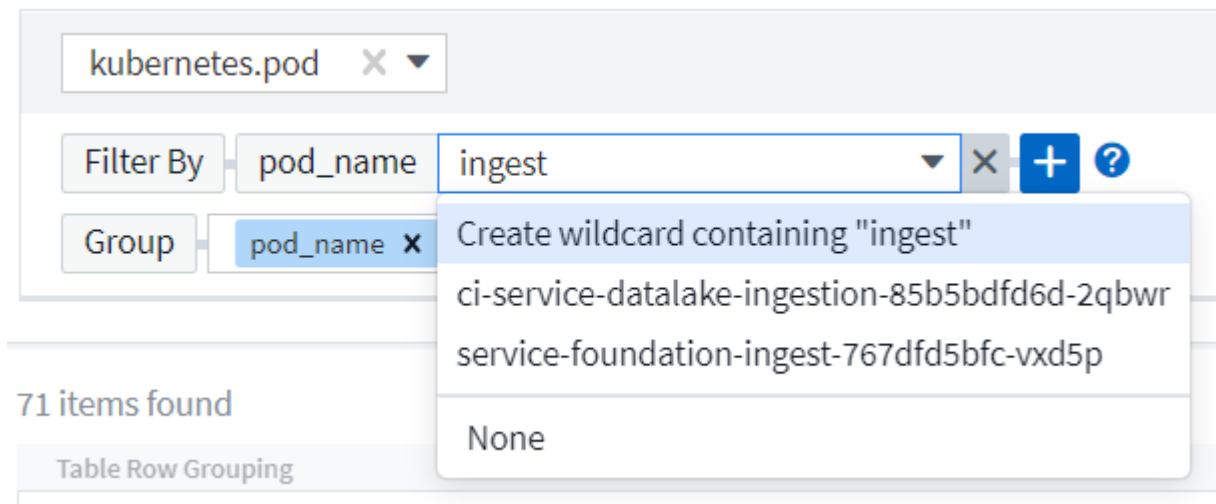
Filtern nach exakter Übereinstimmung

Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren AND, OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Sie können Filter für exakte Übereinstimmungen verwenden, um bestimmte Ressourcen zu finden, beispielsweise den Hostnamen. Wenn Sie nur den Hostnamen „marketing“ suchen, aber „marketing01“, „marketing-boston“ usw. ausschließen möchten, schließen Sie den Namen „marketing“ einfach in Anführungszeichen ein.

Platzhalter und Ausdrücke

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text oder Listenwerten filtern, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können **Ausdrücke** auch mit NOT oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.



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

kubernetes.pod

Filter By
pod_name
ingest
ci-service-audit-5f775dd975-brfdc
+
?

Group
pod_name

3 items found

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit Zahlen, Datumsangaben oder Booleschen Werten.

Erweiterte Textfilterung mit kontextbezogenen Type-Ahead-Vorschlägen

Das Filtern in Widget-Abfragen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für ein Feld auswählen, zeigen die anderen Filter für diese Abfrage die für diesen Filter relevanten Werte an. Wenn Sie beispielsweise einen Filter für einen bestimmten Objektnamen festlegen, werden im Feld zum Filtern nach Modell nur Werte angezeigt, die für diesen Objektnamen relevant sind.

Die kontextbezogene Filterung gilt auch für Dashboard-Seitenvariablen (nur Textattribute oder Anmerkungen). Wenn Sie einen Filterwert für eine Variable auswählen, werden für alle anderen Variablen, die verwandte Objekte verwenden, nur mögliche Filterwerte basierend auf dem Kontext dieser verwandten Variablen angezeigt.

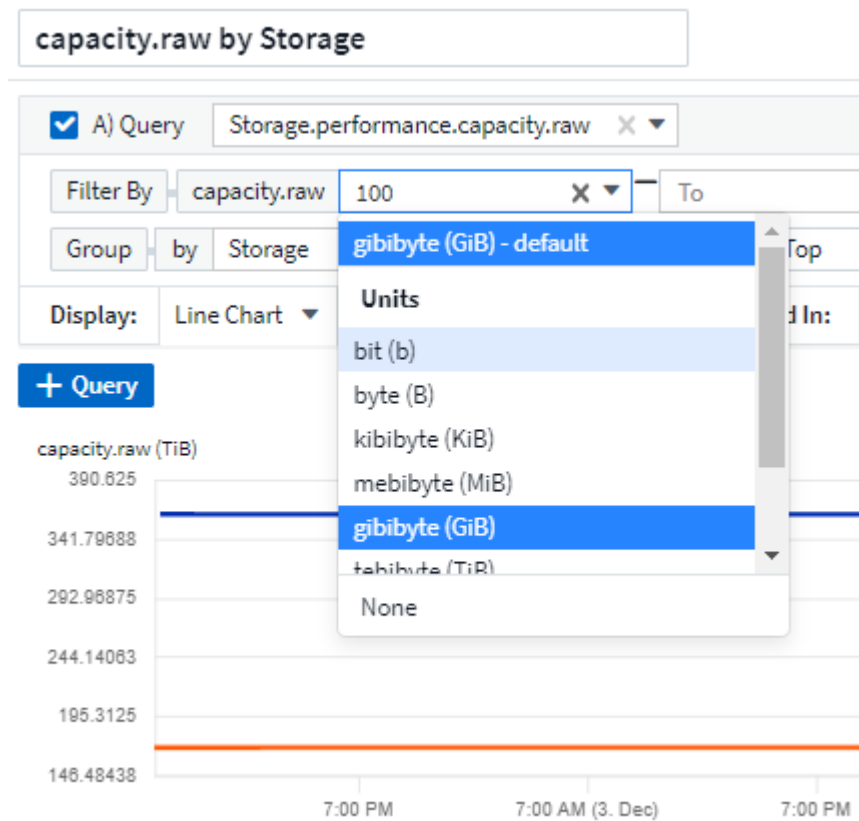
Beachten Sie, dass nur Textfilter kontextbezogene Type-Ahead-Vorschläge anzeigen. Für Datum, Enumeration (Liste) usw. werden keine Vorschläge zur Typvervollständigung angezeigt. Das heißt, Sie *können* einen Filter auf ein Enumerationsfeld (d. h. ein Listenfeld) setzen und andere Textfelder im Kontext filtern lassen. Wenn Sie beispielsweise einen Wert in einem Enumerationsfeld wie „Rechenzentrum“ auswählen, werden in anderen Filtern nur die Modelle/Namen in diesem Rechenzentrum angezeigt, aber nicht umgekehrt.

Der ausgewählte Zeitraum bietet auch Kontext für die in den Filtern angezeigten Daten.

Auswahl der Filtereinheiten

Wenn Sie einen Wert in ein Filterfeld eingeben, können Sie die Einheiten auswählen, in denen die Werte im Diagramm angezeigt werden sollen. Sie können beispielsweise nach Rohkapazität filtern und die Anzeige im Standard-GiB oder ein anderes Format wie TiB auswählen. Dies ist nützlich, wenn Sie auf Ihrem Dashboard mehrere Diagramme haben, die Werte in TiB anzeigen, und Sie möchten, dass alle Ihre Diagramme

konsistente Werte anzeigen.



Zusätzliche Filterverfeinerungen

Mit den folgenden Angaben können Sie Ihre Filter weiter verfeinern.

- Mit einem Sternchen können Sie nach allem suchen. Zum 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. Zum Beispiel,

`BOS-PRD??-S12`

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

- Mit dem ODER-Operator können Sie mehrere Entitäten angeben. Zum Beispiel,

`FAS2240 OR CX600 OR FAS3270`

findet mehrere Speichermodelle.

- Mit dem Operator „NOT“ können Sie Text aus den Suchergebnissen ausschließen. Zum Beispiel,

NOT EMC*

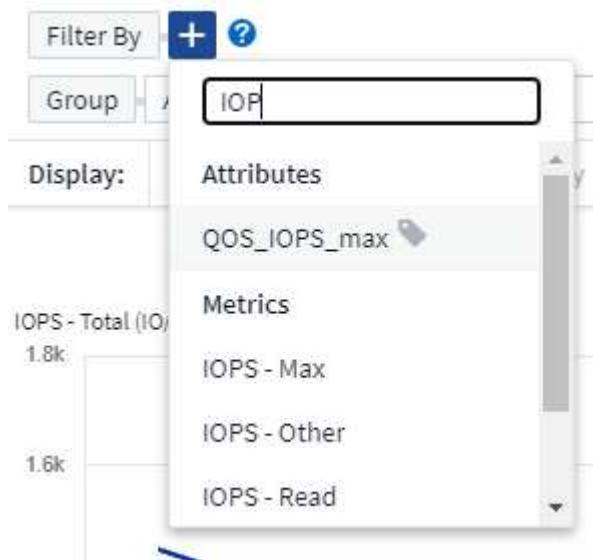
findet alles, was nicht mit „EMC“ beginnt. Sie können

NOT *

um Felder anzuzeigen, die keinen Wert enthalten.

Identifizieren von Objekten, die von Abfragen und Filtern zurückgegeben werden

Die von Abfragen und Filtern zurückgegebenen Objekte ähneln denen in der folgenden Abbildung. Objekte mit zugewiesenen „Tags“ sind Anmerkungen, während Objekte ohne Tags Leistungsindikatoren oder Objektattribute sind.



Gruppieren, Identifizieren und Aggregieren

Gruppierung (Aufrollen)

Die in einem Widget angezeigten Daten werden aus den während der Erfassung gesammelten zugrunde liegenden Datenpunkten gruppiert (manchmal auch als zusammengefasst bezeichnet). Wenn Sie beispielsweise über ein Liniendiagramm-Widget verfügen, das die Speicher-IOPS im Zeitverlauf anzeigt, möchten Sie möglicherweise für jedes Ihrer Rechenzentren eine separate Linie anzeigen, um einen schnellen Vergleich zu ermöglichen. Im Feld „Gruppieren nach“ wählen Sie den Objekttyp selbst aus, um einzelne Linien, Bereiche, Balken, Spalten usw. (abhängig vom Widget-Typ) für jedes Objekt anzuzeigen. Sie können die Objekte nach jedem in der Liste verfügbaren Attribut gruppieren. Wenn Sie beispielsweise Daten für ein internes Volume anzeigen, möchten Sie die Daten möglicherweise nach dem Speichernamen gruppieren.

Um die konsolidierten Daten anzuzeigen, entfernen Sie alle Gruppierungsattribute. Standardmäßig wird dann nach „Alle“ gruppiert.

Sie können diese Daten auf verschiedene Arten aggregieren:

- **Durchschnitt:** zeigt jede Zeile als *Durchschnitt* 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.
- **Summe:** zeigt jede Zeile als *Summe* der zugrunde liegenden Daten an.

Beim Betrachten des Dashboards öffnet die Auswahl der Legende für ein beliebiges Widget, dessen Daten nach „Alle“ gruppiert sind, eine Abfrageseite, die die Ergebnisse der ersten im Widget verwendeten Abfrage anzeigt.

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

Identifizierung kundenspezifischer Daten

Wenn Sie ein Widget erstellen oder ändern, das auf Ihren eigenen benutzerdefinierten Daten basiert, werden Ihre Daten im Widget möglicherweise nicht korrekt dargestellt, wenn kein identifizierendes Attribut vorhanden ist. Falls DII das von Ihnen für Ihr Widget ausgewählte Objekt nicht identifizieren kann, wird Ihnen im Bereich „Gruppieren nach“ ein Link zur *Erweiterten Konfiguration* angezeigt. Erweitern Sie diese Option, um das Attribut auszuwählen, anhand dessen Sie Ihre Daten identifizieren möchten.



The screenshot shows the configuration interface for a dashboard widget. It includes three main dropdown menus: 'Group by' (set to 'cluster_name'), 'Aggregated by' (set to 'Average'), and 'Identify by' (set to 'None'). A 'Reset' button with a help icon is on the right. The 'Identify by' dropdown is open, showing a list of attributes: 'cluster_fqdn', 'cluster_model', 'cluster_name', 'cluster_serial_number' (highlighted), 'cluster_type', 'cluster_uuid', and 'cluster_vendor'.

Daten aggregieren

Sie können Ihre Diagramme noch besser ausrichten, indem Sie Datenpunkte in Minuten-, Stunden- oder Tagesintervalle aggregieren, bevor diese Daten anschließend nach Attributen zusammengefasst werden (falls ausgewählt). Sie können Datenpunkte nach ihrem *Durchschnitt*, *Maximum*, *Minimum*, *ihrer Summe* oder *ihrer _Anzahl* aggregieren.

Ein kleines Intervall in Kombination mit einem langen Zeitbereich kann zu der Warnung „Aggregationsintervall ergab zu viele Datenpunkte.“ führen. Dies wird möglicherweise angezeigt, wenn Sie ein kleines Intervall haben und den Zeitrahmen des Dashboards auf 7 Tage erhöhen. In diesem Fall erhöht Insight vorübergehend das Aggregationsintervall, bis Sie einen kleineren Zeitrahmen auswählen.

Die meisten Asset-Zähler ergeben standardmäßig den *Durchschnitt*. Einige Zähler werden standardmäßig zu *Max*, *Min* oder *Sum* aggregiert. Beispielsweise werden Portfehler standardmäßig zu *Summe* aggregiert, während Speicher-IOPS zu *Durchschnitt* aggregiert werden.

Anzeigen der Top-/Bottom-Ergebnisse

In einem Diagramm-Widget können Sie entweder die **obersten** oder **untersten** Ergebnisse für zusammengefasste Daten anzeigen und die Anzahl der angezeigten Ergebnisse aus der bereitgestellten

Dropdown-Liste auswählen. In einem Tabellen-Widget können Sie nach jeder Spalte sortieren.

Diagramm-Widget oben/unten

Wenn Sie in einem Diagramm-Widget die Daten nach einem bestimmten Attribut zusammenfassen, haben Sie die Möglichkeit, entweder die obersten N oder die untersten N Ergebnisse anzuzeigen. Beachten Sie, dass Sie nicht die obersten oder untersten Ergebnisse auswählen können, wenn Sie die Zusammenfassung nach *allen* Attributen auswählen.

Sie können auswählen, welche Ergebnisse angezeigt werden sollen, indem Sie im Feld **Anzeigen** der Abfrage entweder **Oben** oder **Unten** auswählen und einen Wert aus der bereitgestellten Liste auswählen.

Tabellen-Widget zeigt Einträge an

In einem Tabellen-Widget können Sie die Anzahl der in den Tabellenergebnissen angezeigten Ergebnisse auswählen. Sie haben nicht die Möglichkeit, die obersten oder untersten Ergebnisse auszuwählen, da Sie in der Tabelle bei Bedarf nach jeder Spalte aufsteigend oder absteigend sortieren können.

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

Gruppierung im Tabellen-Widget

Daten in einem Tabellen-Widget können nach jedem verfügbaren Attribut gruppiert werden, sodass Sie eine Übersicht über Ihre Daten erhalten und für weitere Details tiefer in die Daten einsteigen können. Die Messwerte in der Tabelle werden zur einfacheren Anzeige in jeder reduzierten Zeile zusammengefasst.

Mit Tabellen-Widgets können Sie Ihre Daten basierend auf den von Ihnen festgelegten Attributen gruppieren. Beispielsweise möchten Sie möglicherweise, dass Ihre Tabelle die gesamten Speicher-IOPS gruppiert nach den Rechenzentren anzeigt, in denen sich diese Speicher befinden. Oder Sie möchten eine Tabelle mit virtuellen Maschinen anzeigen, die nach dem Hypervisor gruppiert sind, auf dem sie gehostet werden. In der Liste können Sie jede Gruppe erweitern, um die Assets in dieser Gruppe anzuzeigen.

Gruppierung ist nur im Widgettyp „Tabelle“ verfügbar.

Gruppierungsbeispiel (mit Erläuterung der Zusammenfassung)

Mit Tabellen-Widgets können Sie Daten zur einfacheren Anzeige gruppieren.

In diesem Beispiel erstellen wir ein Tabellen-Widget, das alle VMs gruppiert nach Rechenzentrum anzeigt.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard und fügen Sie ein **Tabellen**-Widget hinzu.
2. Wählen Sie *Virtuelle Maschine* als Asset-Typ für dieses Widget.
3. Klicken Sie auf den Spaltenselektor und wählen Sie *Hypervisorname* und *IOPS – Gesamt*.

Diese Spalten werden jetzt in der Tabelle angezeigt.

4. Lassen Sie uns alle VMs ohne IOPS außer Acht lassen und nur VMs einbeziehen, deren Gesamt-IOPS größer als 1 ist. Klicken Sie auf die Schaltfläche **Filtern nach [+]** und wählen Sie *IOPS – Gesamt* aus. Klicken Sie auf *Beliebig* und geben Sie im Feld **Von 1** ein. Lassen Sie das Feld **An** leer. Drücken Sie die Eingabetaste oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

Die Tabelle zeigt jetzt alle VMs mit einem Gesamt-IOPS größer oder gleich 1. Beachten Sie, dass in der

Tabelle keine Gruppierung vorhanden ist. Alle VMs werden angezeigt.

5. Klicken Sie auf die Schaltfläche **Gruppieren nach [+]**.

Sie können nach jedem angezeigten Attribut oder jeder angezeigten Anmerkung gruppieren. Wählen Sie *Alle*, um alle VMs in einer einzigen Gruppe anzuzeigen.

Jede Spaltenüberschrift für eine Leistungsmetrik zeigt ein Drei-Punkte-Menü mit einer **Rollup**-Option an. Die Standard-Rollup-Methode ist *Durchschnitt*. Dies bedeutet, dass die für die Gruppe angezeigte Zahl der Durchschnitt aller für jede VM innerhalb der Gruppe gemeldeten Gesamt-IOPS ist. Sie können diese Spalte nach *Durchschnitt*, *Summe*, *Minimum* oder *Maximum* aufrollen. Jede von Ihnen angezeigte Spalte mit Leistungsmetriken kann einzeln zusammengefasst werden.



6. Klicken Sie auf *Alle* und wählen Sie *Hypervisorname* 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 nach Wunsch ändern oder es verschieben.

8. Klicken Sie auf **Speichern**, um das Dashboard zu speichern.

Leistungsdaten-Rollup

Wenn Sie in ein Tabellen-Widget eine Spalte für Leistungsdaten (z. B. *IOPS – Gesamt*) aufnehmen und die Daten gruppieren möchten, können Sie anschließend eine Rollup-Methode für diese Spalte auswählen. Die Standard-Rollup-Methode besteht darin, den Durchschnitt (*avg*) der zugrunde liegenden Daten in der Gruppenzeile anzuzeigen. Sie können auch wählen, ob die Summe, das Minimum oder das Maximum der Daten angezeigt werden soll.

Dashboard-Zeitbereichsauswahl

Sie können den Zeitraum für Ihre Dashboard-Daten auswählen. In Widgets auf dem Dashboard werden nur Daten angezeigt, die für den ausgewählten Zeitraum relevant sind. Sie können aus folgenden Zeiträumen auswählen:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Letzte 2 Stunden
- Letzte 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

Mit dem benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinanderfolgende Tage auswählen. Sie können auch die Start- und Endzeit des Tages für diesen Bereich festlegen. Die Standardstartzeit ist 0:00 Uhr am ersten ausgewählten Tag und die Standardendzeit ist 23:59 Uhr am letzten ausgewählten Tag. Durch Klicken auf **Übernehmen** wird der benutzerdefinierte Zeitraum auf das Dashboard angewendet.

In einen Zeitbereich hineinzoomen

Beim Anzeigen eines Zeitreihen-Widgets (Linie, Spline, Fläche, gestapelte Fläche) – oder eines Diagramms auf einer Zielseite – können Sie die Maus über das Diagramm ziehen, um es zu vergrößern. Oben rechts auf dem Bildschirm können Sie dann diesen Zeitraum sperren, sodass Diagramme auf anderen Seiten Daten für diesen gesperrten Zeitraum widerspiegeln. Wählen Sie zum Entsperrn einen anderen Zeitraum aus der Liste aus.

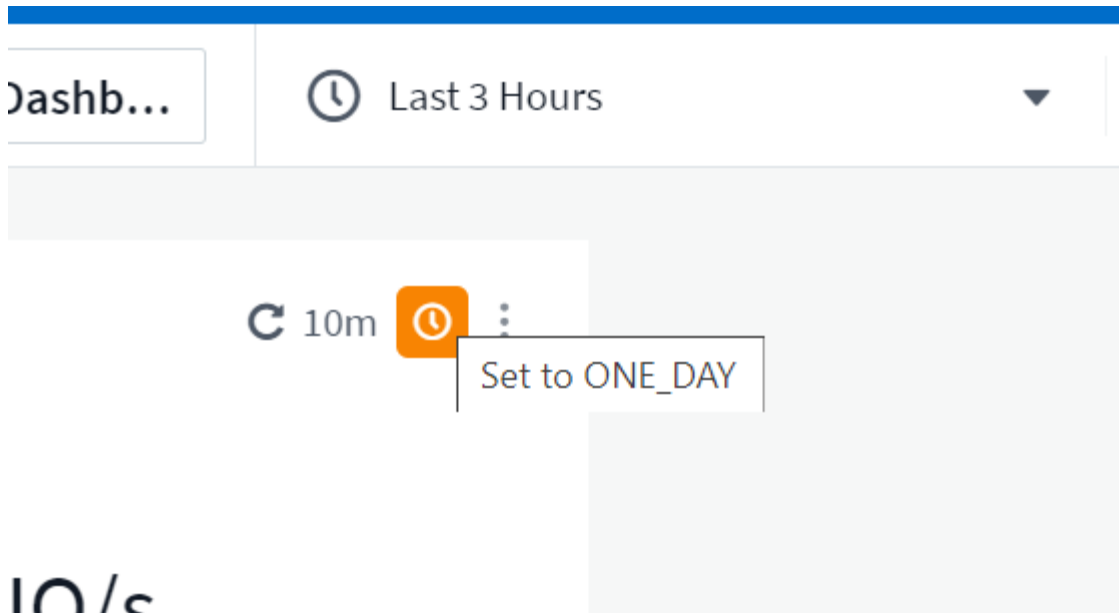
Überschreiben der Dashboard-Zeit in einzelnen Widgets

Sie können die Zeitbereichseinstellung des Haupt-Dashboards in einzelnen Widgets überschreiben. Diese Widgets zeigen Daten basierend auf ihrem festgelegten Zeitrahmen an, nicht auf dem Zeitrahmen des Dashboards.

Um die Dashboard-Zeit zu überschreiben und ein Widget zu zwingen, seinen eigenen Zeitrahmen zu verwenden, wählen Sie im Bearbeitungsmodus des Widgets den gewünschten Zeitraum aus und speichern Sie das Widget im Dashboard.

Das Widget zeigt seine Daten entsprechend dem dafür festgelegten Zeitrahmen an, unabhängig von dem Zeitrahmen, den Sie auf dem Dashboard selbst auswählen.

Der Zeitrahmen, den Sie für ein Widget festlegen, wirkt sich nicht auf andere Widgets auf dem Dashboard aus.



Primäre und sekundäre Achse

Verschiedene Metriken verwenden unterschiedliche Maßeinheiten für die Daten, die sie in einem Diagramm darstellen. Bei IOPS beispielsweise ist die Maßeinheit die Anzahl der E/A-Vorgänge pro Sekunde (IO/s), während die Latenz ein reines Zeitmaß ist (Millisekunden, Mikrosekunden, Sekunden usw.). Wenn Sie beide Metriken in einem einzelnen Liniendiagramm mit einem einzigen Satz von Werten für die Y-Achse darstellen, werden die Latenzzahlen (normalerweise einige Millisekunden) auf derselben Skala wie die IOPS (normalerweise im Tausenderbereich) dargestellt, und die Latenzlinie geht in dieser Skala verloren.

Es ist jedoch möglich, beide Datensätze in einem einzigen aussagekräftigen Diagramm darzustellen, indem man eine Maßeinheit auf der primären (linken) Y-Achse und die andere Maßeinheit auf der sekundären (rechten) Y-Achse festlegt. Jede Metrik wird in einem eigenen Maßstab dargestellt.

Schritte

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

1. Erstellen oder öffnen Sie ein Dashboard. Fügen Sie dem Dashboard ein Liniendiagramm-, Spline-Diagramm-, Flächendiagramm- oder gestapeltes Flächendiagramm-Widget hinzu.
2. Wählen Sie einen Asset-Typ (z. B. *Speicher*) und wählen Sie *IOPS – Gesamt* für Ihre erste Metrik. Legen Sie beliebige Filter fest und wählen Sie bei Bedarf eine Rollup-Methode.

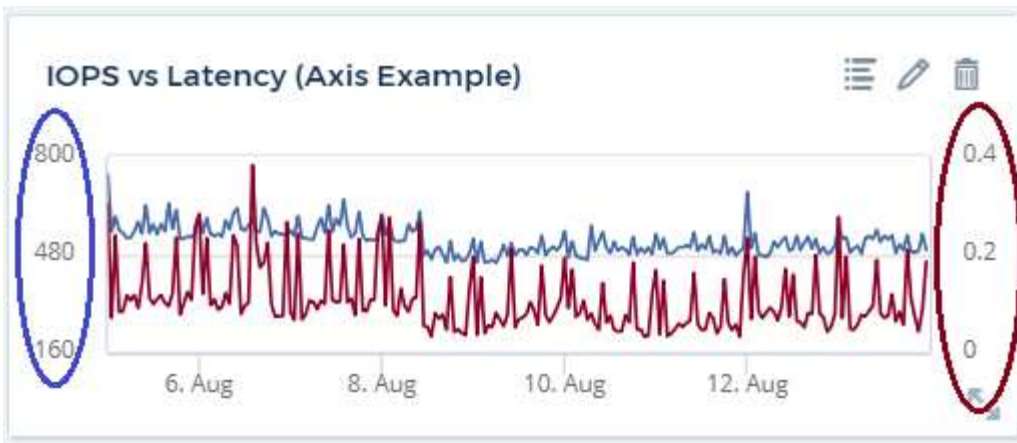
Die IOPS-Linie wird im Diagramm angezeigt, ihre Skala ist links dargestellt.

3. Klicken Sie auf **[+Abfrage]**, um dem Diagramm eine zweite Linie hinzuzufügen. Wählen Sie für diese Zeile als Metrik *Latenz – Gesamt*.

Beachten Sie, dass die Linie unten im Diagramm flach angezeigt wird. Dies liegt daran, dass sie *im gleichen Maßstab* wie die IOPS-Linie gezeichnet wird.

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

Die Latenzlinie wird jetzt in einer eigenen Skala gezeichnet, die auf der rechten Seite des Diagramms angezeigt wird.



Ausdrücke in Widgets

In einem Dashboard können Sie mit jedem Zeitreihen-Widget (Linie, Spline, Fläche, gestapelte Fläche), Balkendiagramm, Säulendiagramm, Kreisdiagramm oder Tabellen-Widget Ausdrücke aus den von Ihnen gewählten Metriken erstellen und das Ergebnis dieser Ausdrücke in einem einzelnen Diagramm (oder einer Spalte im Fall des [Tabellen-Widget](#)). In den folgenden Beispielen werden Ausdrücke verwendet, um bestimmte Probleme zu lösen. Im ersten Beispiel möchten wir die Lese-IOPS als Prozentsatz der Gesamt-IOPS für alle Speicherressourcen Ihres Mandanten anzeigen. Das zweite Beispiel bietet Einblick in die „System“- oder „Overhead“-IOPS, die auf Ihrem Mandanten auftreten – jene IOPS, die nicht direkt durch das Lesen oder Schreiben von Daten entstehen.

Sie können Variablen in Ausdrücken verwenden (z. B. $\$Var1 * 100$).

Ausdrucksbeispiel: IOPS-Prozentsatz lesen

In diesem Beispiel möchten wir die Lese-IOPS als Prozentsatz der Gesamt-IOPS anzeigen. Sie können sich dies als folgende Formel vorstellen:

$\text{Read Percentage} = (\text{Read IOPS} / \text{Total IOPS}) \times 100$
 Diese Daten können in einem Liniendiagramm auf Ihrem Dashboard angezeigt werden. Gehen Sie hierzu folgendermaßen vor:

Schritte

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

Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage angezeigt, die *IOPS – Gesamt* für *Speicher-Assets* anzeigt. 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 Ausdrucksmodus nicht ändern können. Während Sie sich im Ausdrucksmodus befinden, ändert sich der Link in **Zurück zur Abfrage**. Klicken Sie hierauf, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass beim Wechseln zwischen den Modi die Felder auf ihre Standardwerte zurückgesetzt werden.

Bleiben Sie vorerst im Ausdrucksmodus.

4. Die Metrik **IOPS – Gesamt** befindet sich jetzt im alphabetischen Variablenfeld „a“. Klicken Sie im Variablenfeld „b“ auf **Auswählen** und wählen Sie **IOPS – Lesen**.

Sie können Ihrem Ausdruck bis zu fünf alphabetische Variablen hinzufügen, indem Sie auf die Schaltfläche + hinter den Variablenfeldern klicken. Für unser Beispiel mit dem Leseprozentsatz benötigen wir nur die Gesamt-IOPS („a“) und die Lese-IOPS („b“).

5. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die den einzelnen Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir wissen, dass der Leseprozentsatz = (Lese-IOPS / Gesamt-IOPS) x 100 ist, daher würden wir diesen Ausdruck wie folgt schreiben:

```
(b / a) * 100
. Das Feld *Label* identifiziert den Ausdruck. Ändern Sie die
Beschriftung in „Leseprozentsatz“ oder etwas für Sie ähnlich Sinnvolles.
. Ändern Sie das Feld *Einheiten* in „%“ oder „Prozent“.
```

Das Diagramm zeigt den IOPS-Leseprozentsatz im Zeitverlauf für die ausgewählten Speichergeräte an. Bei Bedarf können Sie einen Filter setzen oder eine andere Rollup-Methode wählen. Beachten Sie, dass bei Auswahl von „Summe“ als Rollup-Methode alle Prozentwerte addiert werden, was möglicherweise über 100 % liegen kann.

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

Ausdrucksbeispiel: „System“-E/A

Beispiel 2: Zu den aus Datenquellen gesammelten Metriken gehören Lese-, Schreib- und Gesamt-IOPS. Allerdings umfasst die Gesamtzahl der von einer Datenquelle gemeldeten IOPS manchmal auch „System“-IOPS, also E/A-Vorgänge, die nicht direkt zum Lesen oder Schreiben von Daten gehören. Diese System-E/A kann auch als „Overhead“-E/A betrachtet werden, die für den ordnungsgemäßen Systembetrieb erforderlich ist, aber nicht direkt mit Datenoperationen zusammenhängt.

Um diese System-E/As anzuzeigen, können Sie die Lese- und Schreib-IOPS von den gesamten IOPS abziehen, die bei der Erfassung gemeldet wurden. Die Formel könnte folgendermaßen aussehen:

```
System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Diese Daten können dann in einem Liniendiagramm auf Ihrem Dashboard
angezeigt werden. Gehen Sie hierzu folgendermaßen vor:
```

Schritte

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

Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage angezeigt, die **IOPS – Gesamt** für **Speicher**-Assets anzeigt. 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 Linie mit der Summe aller IOPS.

4. Klicken Sie auf das Symbol „Diese Abfrage duplizieren“, um eine Kopie der Abfrage zu erstellen.

Unter dem Original wird ein Duplikat der Abfrage 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 **Zurück zur Abfrage**, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass beim Wechseln zwischen den Modi die Felder auf ihre Standardwerte zurückgesetzt werden.

Bleiben Sie vorerst im Ausdrucksmodus.

6. Die Metrik *IOPS – Gesamt* befindet sich jetzt im alphabetischen Variablenfeld „a“. Klicken Sie auf *IOPS – Gesamt* und ändern Sie es in *IOPS – Lesen*.
7. Klicken Sie im Variablenfeld „b“ auf **Auswählen** und wählen Sie *IOPS – Schreiben*.
8. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die den einzelnen Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir würden unseren Ausdruck einfach so schreiben:

a + b

Wählen Sie im Abschnitt „Anzeige“ für diesen Ausdruck **Flächendiagramm** aus.

9. Das Feld **Label** identifiziert den Ausdruck. Ändern Sie die Bezeichnung in „System-IOPS“ oder etwas für Sie ebenso Sinnvolles.

Das Diagramm zeigt die gesamten IOPS als Liniendiagramm an, darunter ein Flächendiagramm, das die Kombination aus Lese- und Schreib-IOPS zeigt. Die Lücke zwischen den beiden zeigt die IOPS, die nicht direkt mit Datenlese- oder -schreibvorgängen zusammenhängen. Dies sind Ihre „System“-IOPS.

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

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen ein, zum Beispiel *\$var1 * 100*. In Ausdrücken können nur numerische Variablen verwendet werden.

Ausdrücke in einem Tabellen-Widget

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 deren Grundlage die Berechnung durchgeführt wird. Sie können der Spalte ganz einfach einen aussagekräftigen Namen geben.



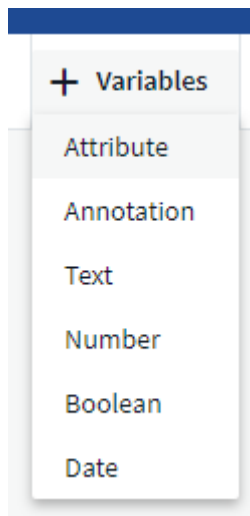
Variablen

Mithilfe von Variablen können Sie die in einigen oder allen Widgets auf einem Dashboard angezeigten Daten gleichzeitig ändern. Indem Sie ein oder mehrere Widgets so einstellen, dass sie eine gemeinsame Variable verwenden, führen an einer Stelle vorgenommene Änderungen dazu, dass die in jedem Widget angezeigten Daten automatisch aktualisiert werden.

Variablentypen

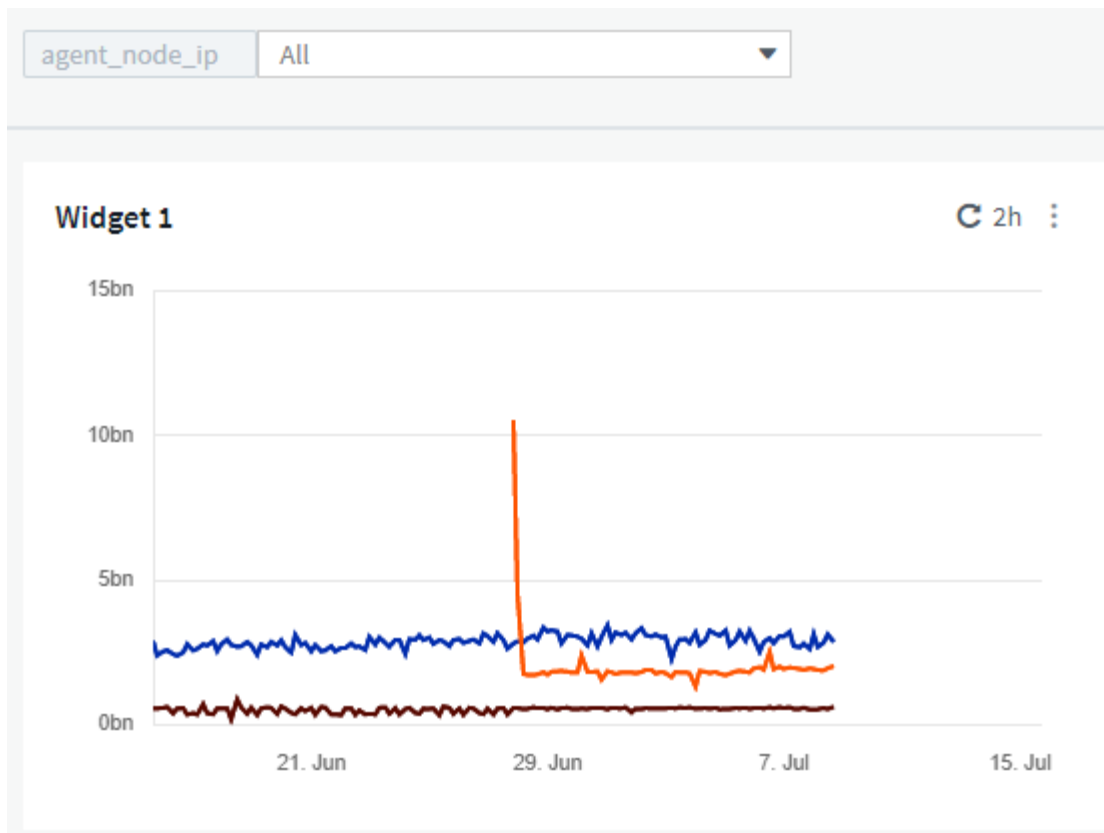
Eine Variable kann einen der folgenden Typen haben:

- **Attribut:** Verwenden Sie die Attribute oder Metriken eines Objekts zum Filtern
- **Anmerkung:** Verwenden Sie eine vordefinierte "[Anmerkung](#)" um Widget-Daten zu filtern.
- **Text:** Eine alphanumerische Zeichenfolge.
- **Numerisch:** Ein Zahlenwert. Verwenden Sie es allein oder als „Von“- oder „Bis“-Wert, abhängig von Ihrem Widget-Feld.
- **Boolesch:** Für Felder mit den Werten „Wahr/Falsch“, „Ja/Nein“ usw. verwenden. Für die boolesche Variable stehen die Auswahlmöglichkeiten „Ja“, „Nein“, „Keine“ und „Beliebig“ zur Verfügung.
- **Datum:** Ein Datumswert. Verwenden Sie es als „Von“- oder „Bis“-Wert, abhängig von der Konfiguration Ihres Widgets.

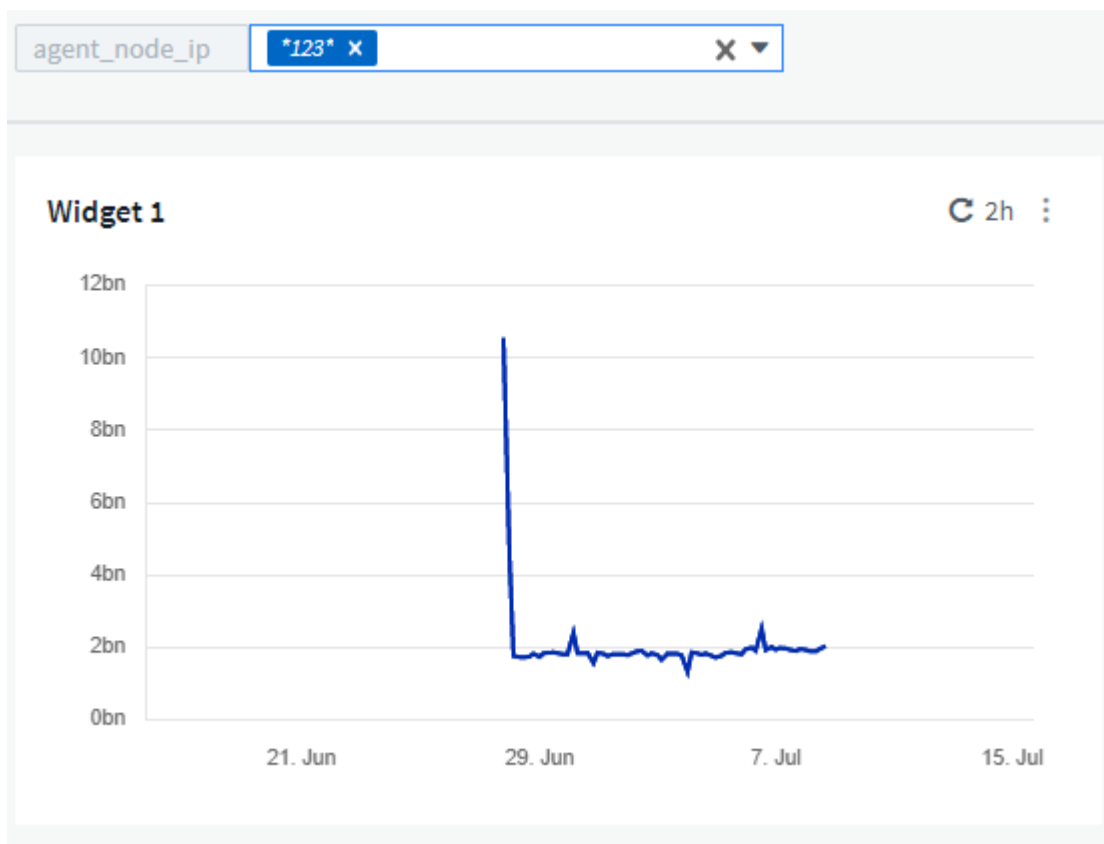


Attributvariablen

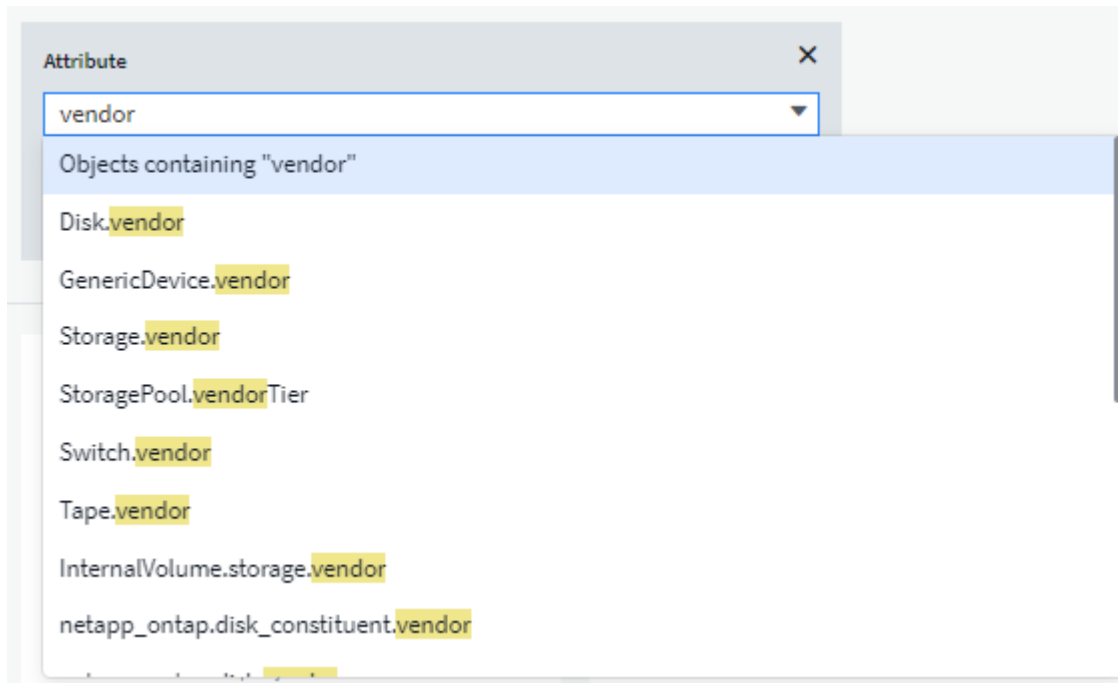
Durch Auswahl einer Attributtypvariable können Sie nach Widgetdaten filtern, die den oder die angegebenen Attributwerte enthalten. Das folgende Beispiel zeigt ein Linien-Widget, das Trends zum freien Speicher für Agent-Knoten anzeigt. Wir haben eine Variable für Agent-Knoten-IPs erstellt, die derzeit so eingestellt ist, dass alle IPs angezeigt werden:



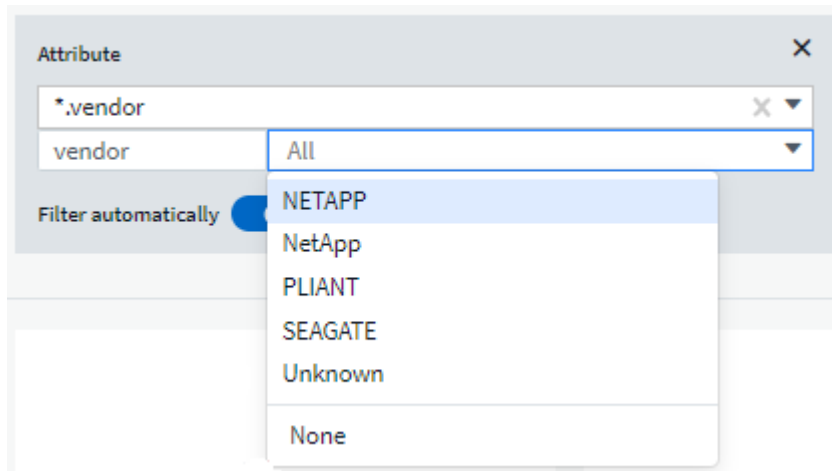
Wenn Sie jedoch vorübergehend nur Knoten in einzelnen Subnetzen Ihres Mandanten sehen möchten, können Sie die Variable auf eine oder mehrere bestimmte Agent-Knoten-IPs festlegen oder ändern. Hier sehen wir nur die Knoten im Subnetz „123“:



Sie können auch eine Variable festlegen, um nach *allen* Objekten mit einem bestimmten Attribut zu filtern, unabhängig vom Objekttyp, beispielsweise nach Objekten mit dem Attribut „Anbieter“, indem Sie **.Anbieter* im Variablenfeld angeben. Sie müssen das „*.“ nicht eingeben. Data Infrastructure Insights liefert dies, wenn Sie die Platzhalteroption auswählen.



Wenn Sie die Auswahlliste für den Variablenwert herunterklappen, werden die Ergebnisse gefiltert, sodass nur die verfügbaren Anbieter basierend auf den Objekten auf Ihrem Dashboard angezeigt werden.



Wenn Sie ein Widget auf Ihrem Dashboard bearbeiten, bei dem der Attributfilter relevant ist (d. h. die Objekte des Widgets enthalten ein **.vendor-Attribut*), wird Ihnen angezeigt, dass der Attributfilter automatisch angewendet wird.

Count of Storages

A) Query Storage.performance.iops.total

Filter By name All vendor NETAPP

Group Count More Options

Formatting: If value is > Warning Optional IO/s and/or Critical Optional IO/s Showing In Range as green

Description e.g. Total IOPS Calculation A Reset Defaults

Decimal Places: 0 Units Displayed In: Whole Number

+ Query

14

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

Annotationsvariablen

Durch Auswahl einer Annotation-Variable können Sie nach Objekten filtern, die mit dieser Annotation verknüpft sind, beispielsweise nach Objekten, die zum selben Rechenzentrum gehören.

Annotation

Data Center

Data Center All

Filter automatically

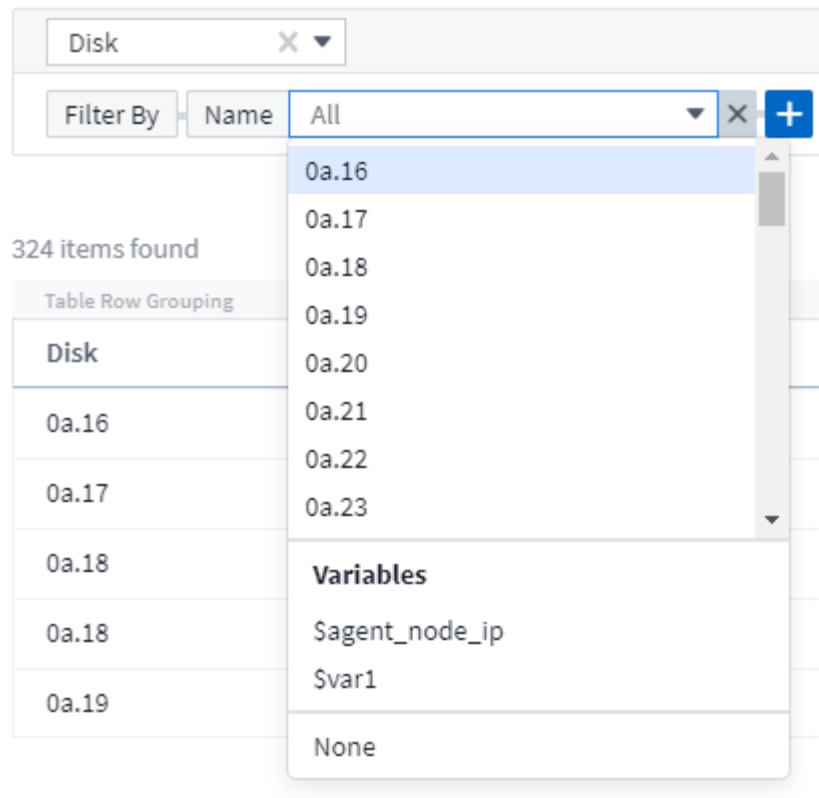
Boston

London

None

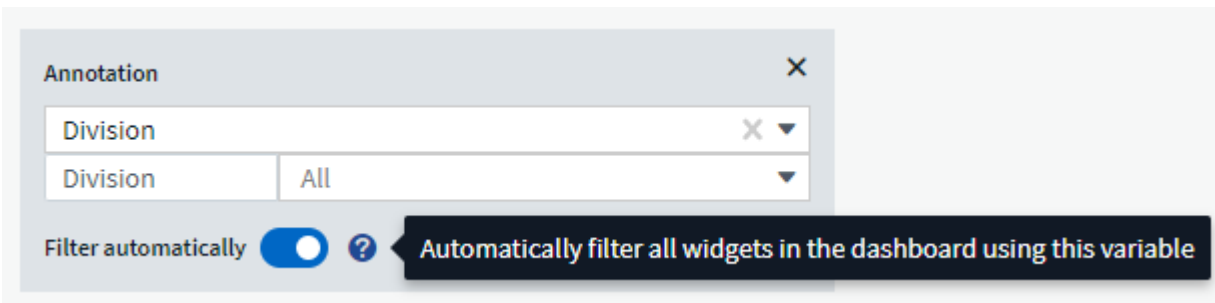
Text, Zahl, Datum oder Boolesche Variable

Sie können generische Variablen erstellen, die keinem bestimmten Attribut zugeordnet sind, indem Sie einen Variablentyp aus *Text*, *Zahl*, *Boolean* oder *Datum* auswählen. Sobald die Variable erstellt wurde, können Sie sie in einem Widget-Filterfeld auswählen. Wenn Sie in einem Widget einen Filter festlegen, werden neben bestimmten Werten, die Sie für den Filter auswählen können, alle für das Dashboard erstellten Variablen in der Liste angezeigt. Diese sind im Dropdown-Menü unter dem Abschnitt „Variablen“ gruppiert und haben Namen, die mit „\$“ beginnen. Wenn Sie in diesem Filter eine Variable auswählen, können Sie nach Werten suchen, die Sie in das Variablenfeld auf dem Dashboard selbst eingeben. Alle Widgets, die diese Variable in einem Filter verwenden, werden dynamisch aktualisiert.



Variabler Filterbereich

Wenn Sie Ihrem Dashboard eine Anmerkungs- oder Attributvariable hinzufügen, kann die Variable auf *alle* Widgets im Dashboard angewendet werden. Dies bedeutet, dass alle Widgets auf Ihrem Dashboard Ergebnisse anzeigen, die nach dem von Ihnen in der Variable festgelegten Wert gefiltert sind.



Beachten Sie, dass nur Attribut- und Anmerkungsvariablen auf diese Weise automatisch gefiltert werden können. Nicht-Annotation- oder -Attributvariablen können nicht automatisch gefiltert werden. Einzelne Widgets müssen jeweils für die Verwendung von Variablen dieser Typen konfiguriert werden.

Um die automatische Filterung zu deaktivieren, sodass die Variable nur für die Widgets gilt, für die Sie sie ausdrücklich festgelegt haben, klicken Sie auf den Schieberegler „Automatisch filtern“, um sie zu deaktivieren.

Um eine Variable in einem einzelnen Widget festzulegen, öffnen Sie das Widget im Bearbeitungsmodus und wählen Sie die spezifische Anmerkung oder das Attribut im Feld *Filtern nach* aus. Mit einer Annotation-Variable können Sie einen oder mehrere bestimmte Werte auswählen oder den Variablennamen (gekennzeichnet durch das vorangestellte „\$“) auswählen, um die Eingabe der Variable auf Dashboard-Ebene zu ermöglichen. Dasselbe gilt für Attributvariablen. Nur die Widgets, für die Sie die Variable festlegen, zeigen die gefilterten Ergebnisse an.

Das Filtern in Variablen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für eine Variable auswählen, werden in den anderen Variablen auf Ihrer Seite nur die für diesen Filter relevanten Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf ein bestimmtes Speichermodell einstellen, werden für alle Variablen, die auf den Filter für den Speichernamen eingestellt sind, nur die für dieses Modell relevanten Werte angezeigt.

Um eine Variable in einem Ausdruck zu verwenden, geben Sie einfach den Variablennamen als Teil des Ausdrucks ein, zum Beispiel `$var1 * 100`. In Ausdrücken können nur numerische Variablen verwendet werden. Sie können in Ausdrücken keine numerischen Anmerknungs- oder Attributvariablen verwenden.

Das Filtern in Variablen ist *kontextbezogen*. Wenn Sie einen oder mehrere Filterwerte für eine Variable auswählen, werden in den anderen Variablen auf Ihrer Seite nur die für diesen Filter relevanten Werte angezeigt. Wenn Sie beispielsweise einen Variablenfilter auf ein bestimmtes Speichermodell einstellen, werden für alle Variablen, die auf den Filter für den Speichernamen eingestellt sind, nur die für dieses Modell relevanten 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.
- Unterscheiden zwischen Groß- und Kleinschreibung: `$CityName` und `$cityname` sind unterschiedliche Variablen.
- Darf nicht mit einem vorhandenen Variablennamen identisch sein.
- Darf nicht leer sein.

Formatieren von Messinstrument-Widgets

Mit den Widgets „Vollständige Anzeige“ und „Aufzählungszeichen“ können Sie Schwellenwerte für die Stufen „Warnung“ und/oder „Kritisch“ festlegen und so eine klare Darstellung der von Ihnen angegebenen Daten bereitstellen.

Widget 12 Override Dashboard Time ⌚ ✕

✓ A) Query Storage,performance.iops.total ✕ 📄 🗑️

Filter By +

Group Avg Time aggregate by Avg Less Options

Formatting: If value is > Warning 500 IO/s and/or Critical 1000 IO/s Showing 🟢 In Range as green

Description IOPS - Total Calculation A Min Value Optional Max Value 1200

Display: Bullet Gauge Decimal Places: 2 Color: 🟡 Units Displayed In: Auto Format

+ Query

904.21 IO/s 🟡
IOPS - Total

200 400 600 800 1k 1.2k

Cancel Save

Um die Formatierung für diese Widgets festzulegen, führen Sie die folgenden Schritte aus:

1. Wählen Sie, ob Sie Werte hervorheben möchten, die größer (>) oder kleiner (<) als Ihre Schwellenwerte sind. In diesem Beispiel markieren wir Werte, die größer (>) als die Schwellenwerte sind.
2. Wählen Sie einen Wert für den Schwellenwert „Warnung“. Wenn das Widget Werte anzeigt, die über diesem Niveau liegen, wird die Anzeige in Orange angezeigt.
3. Wählen Sie einen Wert für den Schwellenwert „Kritisch“. Bei Werten über diesem Wert wird die Anzeige rot angezeigt.

Optional können Sie einen Minimal- und Maximalwert für die Anzeige wählen. Bei Werten unter dem Minimum wird die Anzeige nicht angezeigt. Bei Werten über dem Maximum wird eine volle Anzeige angezeigt. Wenn Sie keine Mindest- oder Höchstwerte auswählen, wählt das Widget basierend auf dem Wert des Widgets die optimalen Mindest- und Höchstwerte aus.



Formatieren des Einzelwert-Widgets

Im Einzelwert-Widget können Sie zusätzlich zur Einstellung der Warnschwellen (orange) und der kritischen Schwelle (rot) wählen, ob Werte „im Bereich“ (unter der Warnstufe) mit grünem oder weißem Hintergrund angezeigt werden sollen.



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

Tabellen-Widgets formatieren

Wie bei Einzelwert- und Mess-Widgets können Sie in Tabellen-Widgets eine bedingte Formatierung festlegen, sodass Sie Daten mit Farben und/oder speziellen Symbolen hervorheben können.

Mit der bedingten Formatierung können Sie Schwellenwerte für Warn- und kritische Werte in Tabellen-Widgets festlegen und hervorheben, sodass Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar werden.

14 items found in 1 group

Table Row Grouping	Expanded Detail	Metrics & Attributes
All	Storage Pool	capacityRatio.used (%)
All (14)	--	95.15
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45
--	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15
--	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15

Formatting: ☒ Show Expanded Details Conditional Formatting: Background Color + Icon ☐ Show In Range as green

capacity.provisioned (GiB)

> Aggregation

> Unit Display

Conditional Formatting Reset

If value is > (Greater than)

Warning 70 %

Critical 90 %

> Rename Column

Die bedingte Formatierung wird für jede Spalte einer Tabelle separat festgelegt. Sie können beispielsweise einen Schwellenwertsatz für eine Kapazitätsspalte und einen anderen Satz für eine Durchsatzspalte auswählen.

Wenn Sie die Einheitenanzeige für eine Spalte ändern, bleibt die bedingte Formatierung erhalten und spiegelt die Werteänderung wider. Die folgenden Bilder zeigen dieselbe bedingte Formatierung, obwohl die Anzeigeeinheit unterschiedlich ist.

capacity.used (GiB) ↓

40,754.06
10,313.56
9,544.84
8,438.99
6,671.72

throughput.total (MiB/s)

> Aggregation

> Unit Display

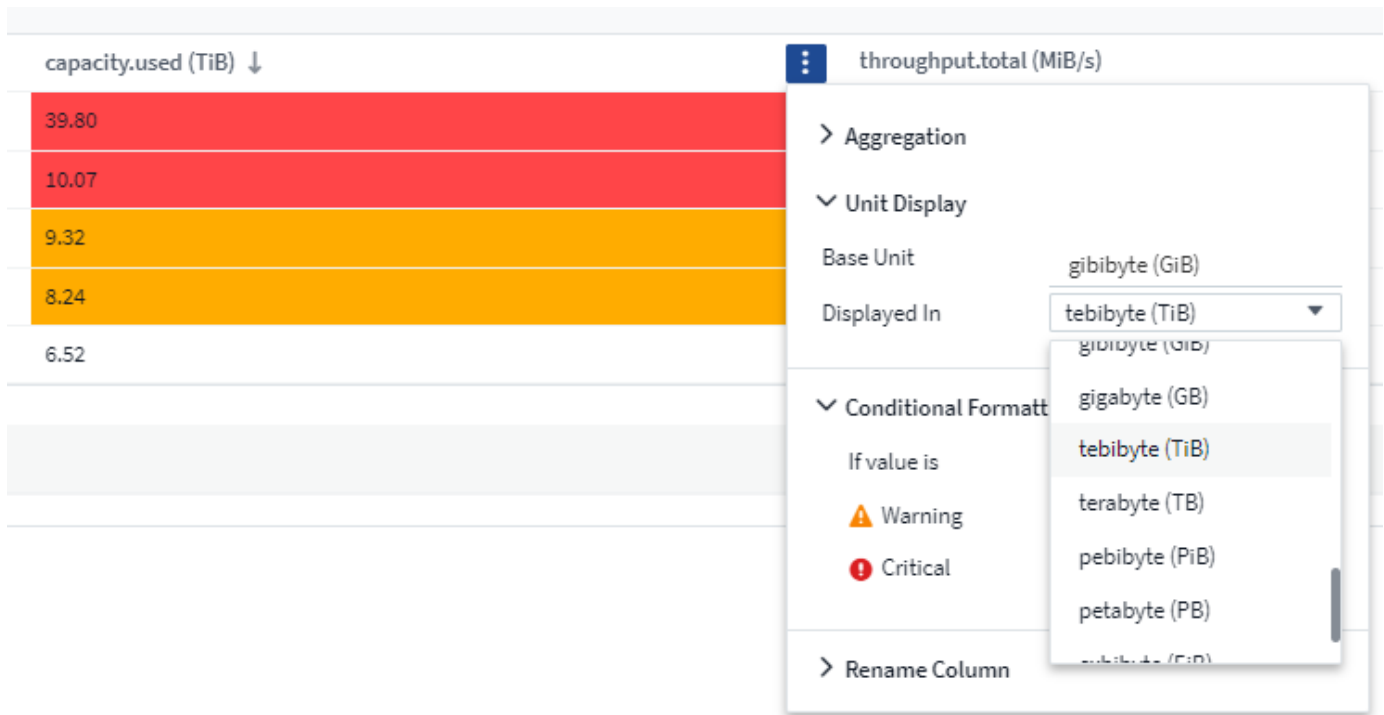
Conditional Formatting Reset

If value is > (Greater than)

Warning 8000 GiB

Critical 10000 GiB

> Rename Column

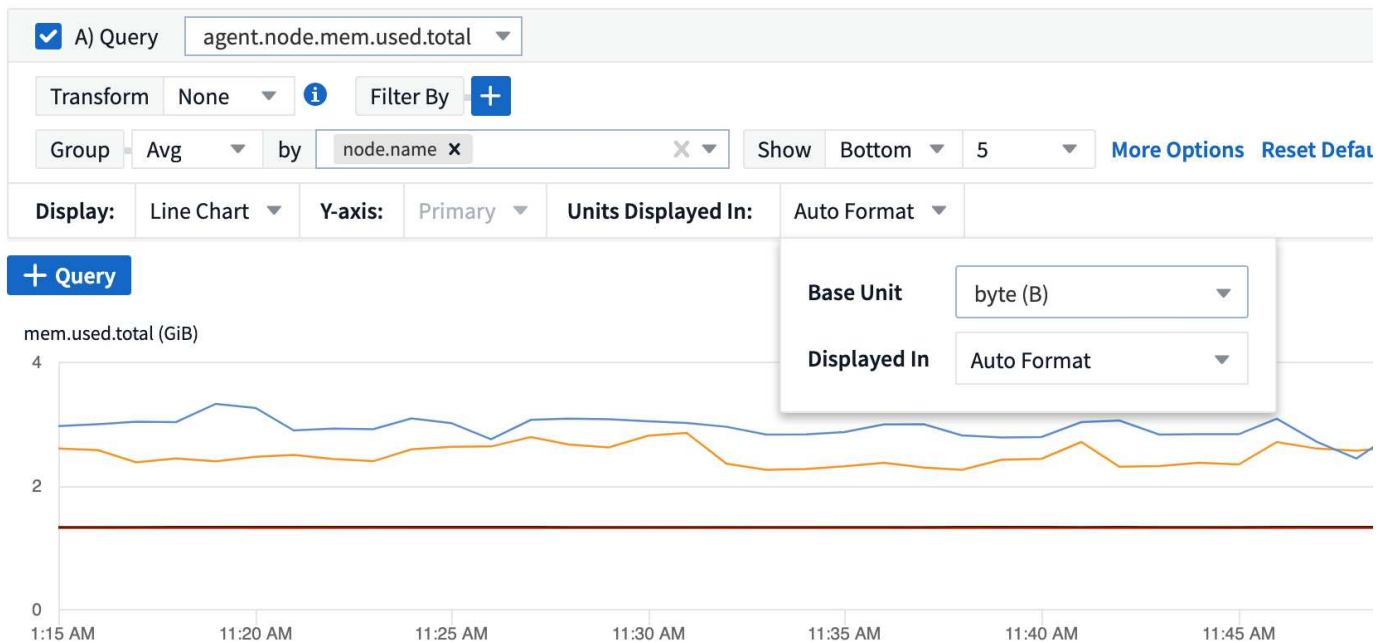


Sie können wählen, ob die Bedingungsformatierung als Farbe, Symbole oder beides angezeigt werden soll.

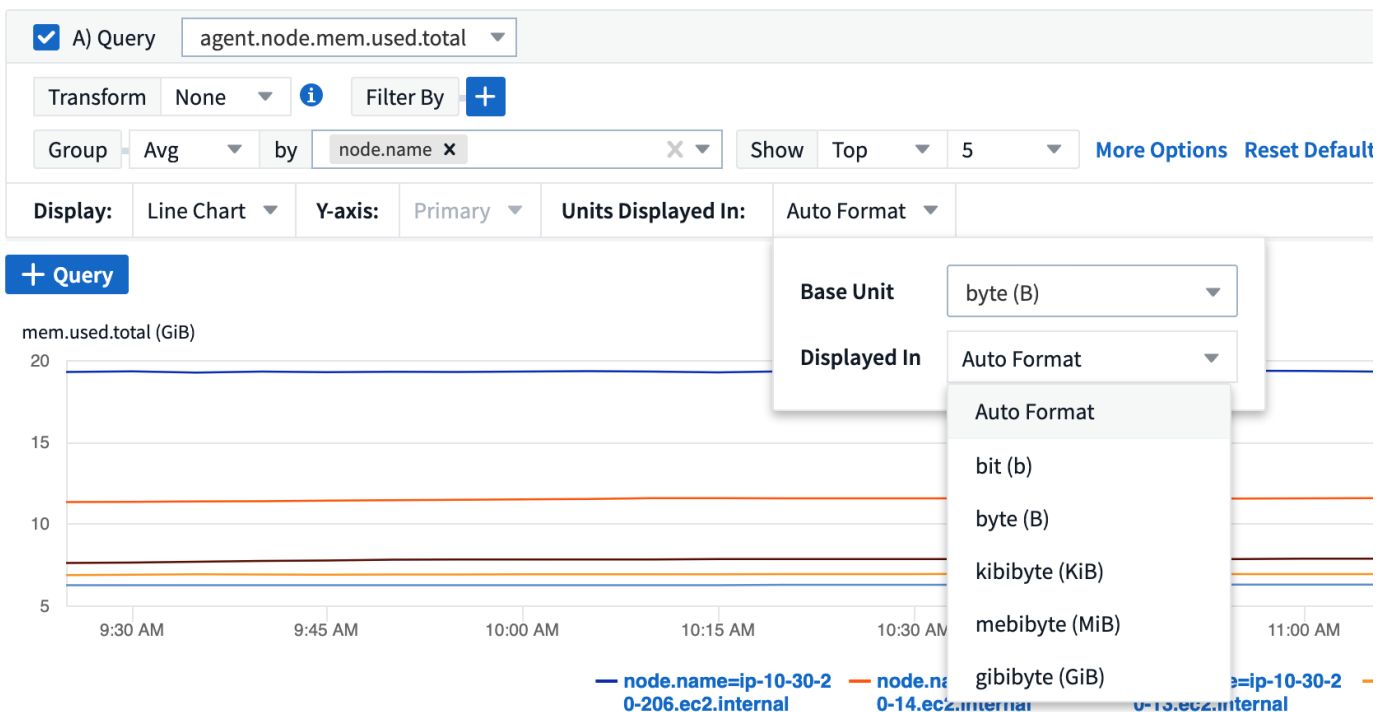
Auswählen der Einheit zur Datenanzeige

Bei den meisten Widgets auf einem Dashboard können Sie die Einheiten angeben, in denen Werte angezeigt werden sollen, beispielsweise *Megabyte*, *Tausende*, *Prozent*, *Millisekunden (ms)* usw. In vielen Fällen kennt Data Infrastructure Insights das beste Format für die erfassten Daten. In Fällen, in denen das beste Format nicht bekannt ist, können Sie das gewünschte Format festlegen.

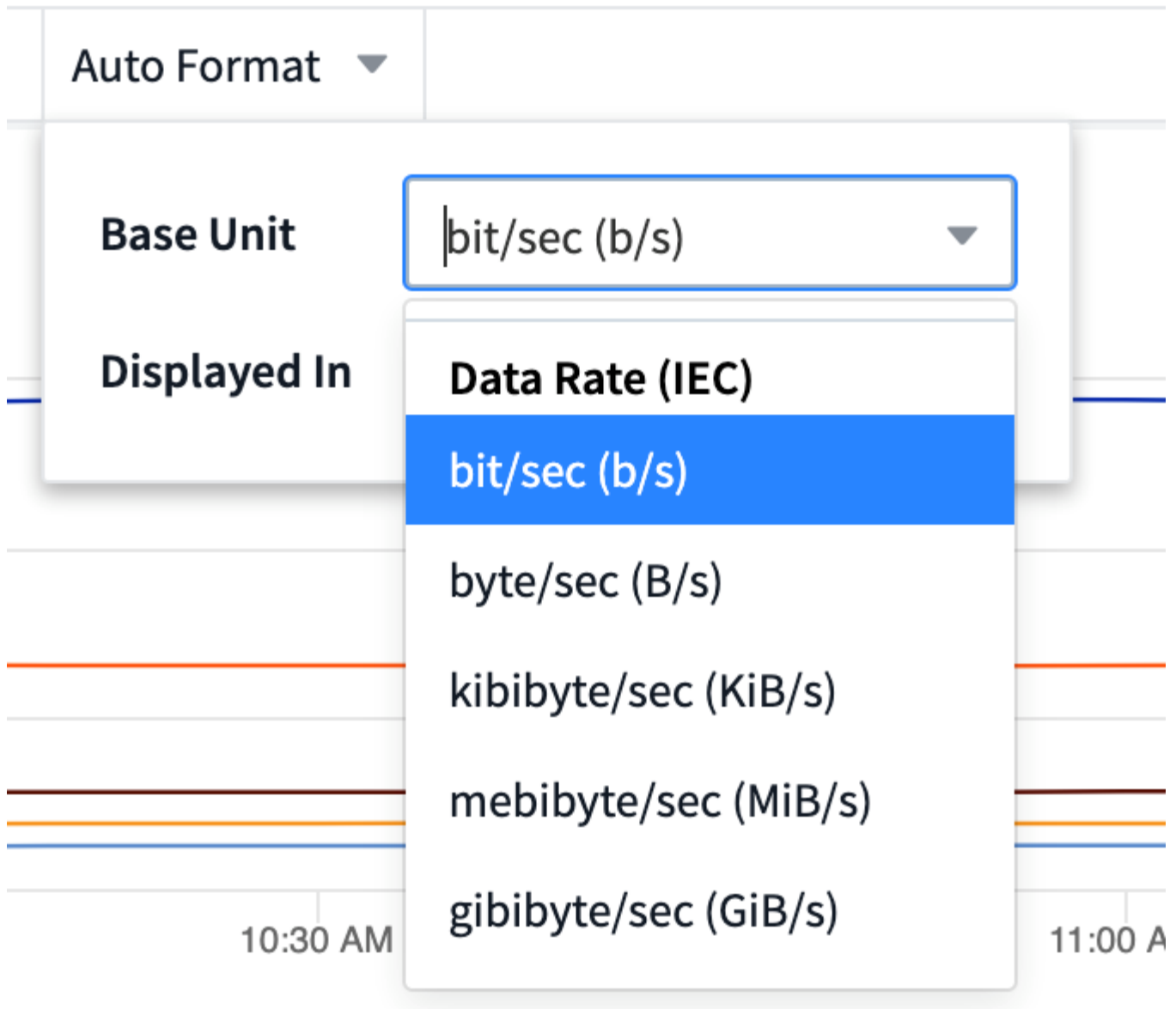
Im folgenden Liniendiagrammbeispiel liegen die für das Widget ausgewählten Daten bekanntermaßen in *Bytes* vor (die grundlegende IEC-Dateneinheit: siehe Tabelle unten), daher wird die Basiseinheit automatisch als „Byte (B)“ ausgewählt. Die Datenwerte sind jedoch groß genug, um als Gibibyte (GiB) dargestellt zu werden, sodass Data Infrastructure Insights die Werte standardmäßig automatisch als GiB formatiert. Die Y-Achse im Diagramm zeigt „GiB“ als Anzeigeeinheit und alle Werte werden in dieser Einheit angezeigt.



Wenn Sie das Diagramm in einer anderen Einheit anzeigen möchten, können Sie ein anderes Format für die Anzeige der Werte auswählen. Da die Basiseinheit in diesem Beispiel *Byte* ist, können Sie aus den unterstützten „bytebasierten“ Formaten wählen: Bit (b), Byte (B), Kibibyte (KiB), Mebibyte (MiB), Gibibyte (GiB). Die Beschriftung und die Werte der Y-Achse ändern sich je nach dem von Ihnen gewählten Format.



In Fällen, in denen die Basiseinheit nicht bekannt ist, können Sie eine Einheit aus den folgenden "verfügbare Einheiten", oder geben Sie Ihren eigenen ein. Nachdem Sie eine Basiseinheit zugewiesen haben, können Sie die Daten in einem der entsprechenden unterstützten Formate anzeigen.



Um Ihre Einstellungen zu löschen und neu zu beginnen, klicken Sie auf **Auf Standard zurücksetzen**.

Ein Wort zur automatischen Formatierung

Die meisten Messwerte werden von Datensammlern in der kleinsten Einheit gemeldet, beispielsweise als ganze Zahl wie 1.234.567.890 Bytes. Standardmäßig formatiert Data Infrastructure Insights den Wert automatisch für die am besten lesbare Anzeige. Beispielsweise würde ein Datenwert von 1.234.567.890 Bytes automatisch auf 1,23 *Gibibytes* formatiert. Sie können es auch in einem anderen Format anzeigen, beispielsweise *Mebibyte*. Der Wert wird entsprechend angezeigt.



Data Infrastructure Insights verwendet amerikanische englische Nummernbenennungsstandards. Die amerikanische „Milliarde“ entspricht „Tausend Millionen“.

Widgets mit mehreren Abfragen

Wenn Sie ein Zeitreihen-Widget (z. B. Linie, Spline, Fläche, gestapelte Fläche) mit zwei Abfragen haben, die beide auf der primären Y-Achse dargestellt werden, wird die Basiseinheit oben auf der Y-Achse nicht angezeigt. Wenn Ihr Widget jedoch eine Abfrage auf der primären Y-Achse und eine Abfrage auf der

sekundären Y-Achse hat, werden die Basiseinheiten für jede angezeigt.



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

Verfügbare Einheiten

Die folgende Tabelle zeigt alle verfügbaren Einheiten nach Kategorie.

Kategorie	Einheiten
Währung	Cent-Dollar
Daten (IEC)	Bit Byte Kibibyte Mebibyte 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/Sek. Megabyte/Sek. Gigabyte/Sek. Terabyte/Sek. Petabyte/Sek. Exabyte/Sek.
IEC	kibi mebi gibi tebi pebi exbi
Dezimal	ganze Zahl Tausend Millionen Milliarden Billionen
Prozentsatz	Prozentsatz
Zeit	Nanosekunde Mikrosekunde Millisekunde Sekunde Minute Stunde
Temperatur	Celsius Fahrenheit
Frequenz	Hertz Kilohertz Megahertz Gigahertz
CPU	Nanokerne, Mikrokerne, Millikerne, Kerne, Kilokerne, Megakerne, Gigakerne, Terakerne, Petakerne, Exakerne
Durchsatz	E/A-Operationen/Sek. Operationen/Sek. Anfragen/Sek. Lesevorgänge/Sek. Schreibvorgänge/Sek. Operationen/Min. Lesevorgänge/Min. Schreibvorgänge/Min.

TV-Modus und automatische Aktualisierung

Daten in Widgets auf Dashboards und Asset-Landingpages werden automatisch gemäß einem Aktualisierungsintervall aktualisiert, das durch den ausgewählten Dashboard-Zeitbereich bestimmt wird. Das

Aktualisierungsintervall hängt davon ab, ob es sich bei dem Widget um ein Zeitreihen- (Linien-, Spline-, Flächen-, gestapeltes Flächendiagramm) oder Nicht-Zeitreihen- (alle anderen Diagramme) Widget handelt.

Dashboard-Zeitbereich	Aktualisierungsintervall für Zeitreihen	Nicht-Zeitreihen-Aktualisierungsintervall
Letzte 15 Minuten	10 Sekunden	1 Minute
Letzte 30 Minuten	15 Sekunden	1 Minute
Letzte 60 Minuten	15 Sekunden	1 Minute
Letzte 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 automatisches Aktualisierungsintervall in der oberen rechten Ecke des Widgets an.

Die automatische Aktualisierung ist für den benutzerdefinierten Dashboard-Zeitbereich nicht verfügbar.

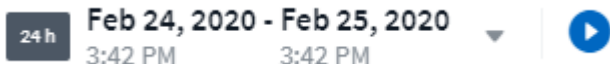
In Kombination mit dem **TV-Modus** ermöglicht die automatische Aktualisierung die Anzeige von Daten auf einem Dashboard oder einer Asset-Seite nahezu in Echtzeit. Der TV-Modus bietet eine übersichtliche Anzeige; das Navigationsmenü ist ausgeblendet, wodurch mehr Platz auf dem Bildschirm für die Anzeige Ihrer Daten zur Verfügung steht, ebenso wie die Schaltfläche „Bearbeiten“. Der TV-Modus ignoriert typische Timeouts von Data Infrastructure Insights und lässt die Anzeige aktiv, bis Sie manuell oder automatisch durch Autorisierungssicherheitsprotokolle abgemeldet werden.



Da die NetApp Console über ein eigenes Zeitlimit für die Benutzeranmeldung von 7 Tagen verfügt, muss sich Data Infrastructure Insights bei diesem Ereignis ebenfalls abmelden. Sie können sich einfach erneut anmelden und Ihr Dashboard wird weiterhin angezeigt.

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

Sie können die automatische Aktualisierung vorübergehend unterbrechen, indem Sie auf die Schaltfläche „Pause“ in der oberen rechten Ecke klicken. Während der Pause zeigt das Zeitbereichsfeld des Dashboards den aktiven Zeitbereich der angehaltenen Daten an. Ihre Daten werden weiterhin erfasst und aktualisiert, während die automatische Aktualisierung angehalten ist. Klicken Sie auf die Schaltfläche „Fortsetzen“, um die automatische Aktualisierung der Daten fortzusetzen.



Dashboard-Gruppen

Durch Gruppieren können Sie zugehörige Dashboards anzeigen und verwalten. Sie können beispielsweise eine Dashboard-Gruppe einrichten, die ausschließlich dem Speicher Ihres Mandanten gewidmet ist. Dashboard-Gruppen werden auf der Seite **Dashboards > Alle Dashboards anzeigen** verwaltet.

Dashboard Groups (3)

All Dashboards (60)

My Dashboards (11)

Storage Group (7)

☐

Dashboards (7)

Name ↑

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Dashboard - Storage Overview

Gauges Storage Performance

Storage Admin - Which nodes are in high demand?

Storage Admin - Which pools are in high demand?

Storage IOPs

Standardmäßig werden zwei Gruppen angezeigt:

- **Alle Dashboards** listet alle erstellten Dashboards auf, unabhängig vom Besitzer.
- **Meine Dashboards** listet nur die vom aktuellen Benutzer erstellten Dashboards auf.

Die Anzahl der in jeder Gruppe enthaltenen Dashboards 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**. Es wird eine leere Gruppe mit diesem Namen erstellt.

Um Dashboards zur Gruppe hinzuzufügen, klicken Sie auf die Gruppe „Alle Dashboards“, um alle Dashboards Ihres Mandanten anzuzeigen, oder klicken Sie auf „Meine Dashboards“, wenn Sie nur die Dashboards sehen möchten, die Ihnen gehören, und führen Sie einen der folgenden Schritte aus:

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

Entfernen Sie Dashboards auf die gleiche Weise aus der aktuellen Gruppe, indem Sie *Aus Gruppe entfernen* auswählen. Sie können keine Dashboards aus der Gruppe „Alle Dashboards“ oder „Meine Dashboards“ entfernen.



Durch das Entfernen eines Dashboards aus einer Gruppe wird das Dashboard nicht aus Data Infrastructure Insights gelöscht. Um ein Dashboard vollständig zu entfernen, wählen Sie das Dashboard aus und klicken Sie auf *Löschen*. Dadurch wird es aus allen Gruppen entfernt, zu denen es gehörte, und steht keinem Benutzer mehr zur Verfügung.

Pinn deine Lieblings-Dashboards an

Sie können Ihre Dashboards weiter verwalten, indem Sie Ihre Favoriten oben in Ihrer Dashboard-Liste anheften. Um ein Dashboard anzuheften, klicken Sie einfach auf die Reißzwecken-Schaltfläche, die angezeigt wird, wenn Sie mit der Maus über ein Dashboard in einer beliebigen Liste fahren.

Das Anheften/Lösen des Dashboards ist eine individuelle Benutzereinstellung und unabhängig von der Gruppe (oder den Gruppen), zu der/denen das Dashboard gehört.

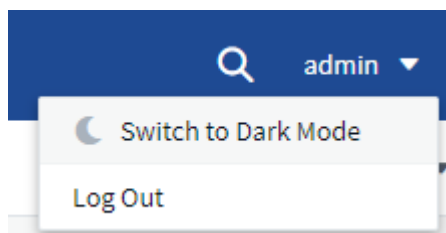
Dashboards (7)

<input type="checkbox"/>	Name ↑
	Dashboard - Storage Overview
	Storage Admin - Which nodes are in high demand?
	Storage IOPs
	Dashboard - Storage Cost
	Dashboard - Storage IO Detail
	Gauges Storage Performance
	Storage Admin - Which pools are in high demand?

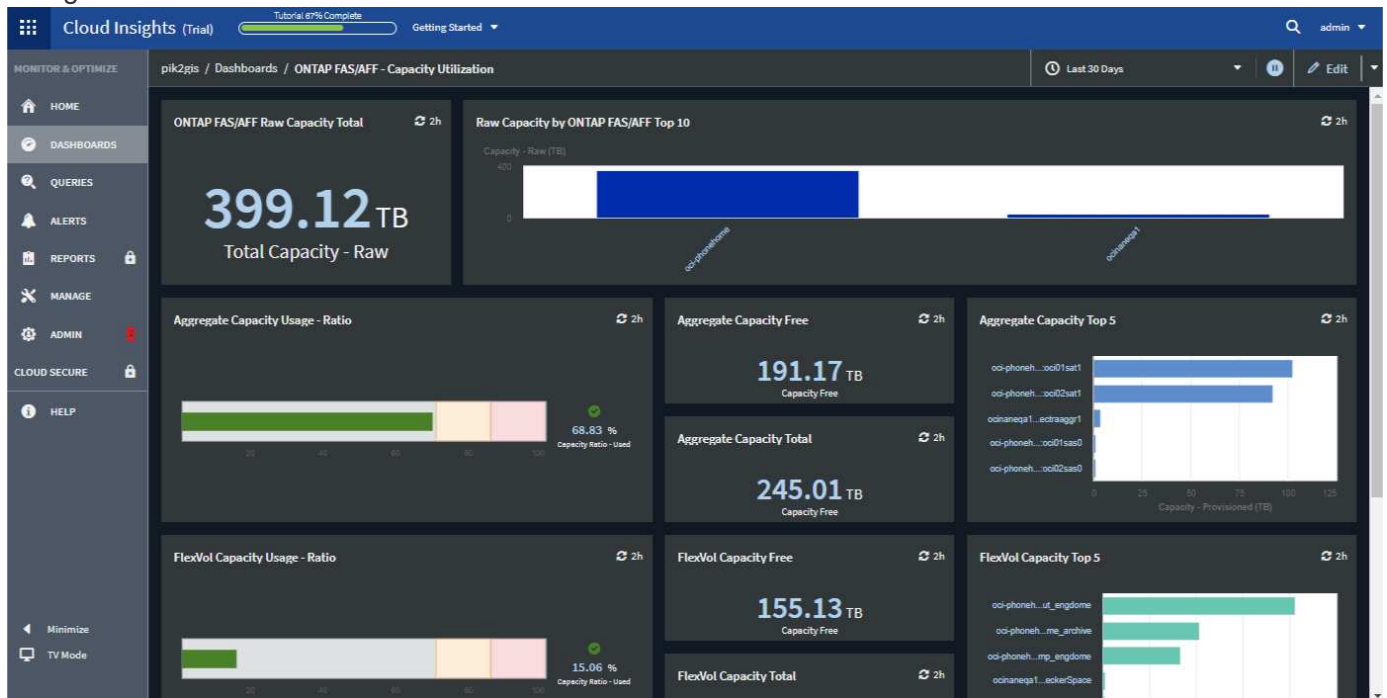
Dunkles Design

Sie können Data Infrastructure Insights entweder mit einem hellen Design (Standard) anzeigen, bei dem die meisten Bildschirme mit einem hellen Hintergrund und dunklem Text angezeigt werden, oder mit einem dunklen Design, bei dem die meisten Bildschirme mit einem dunklen Hintergrund und hellem Text angezeigt werden.

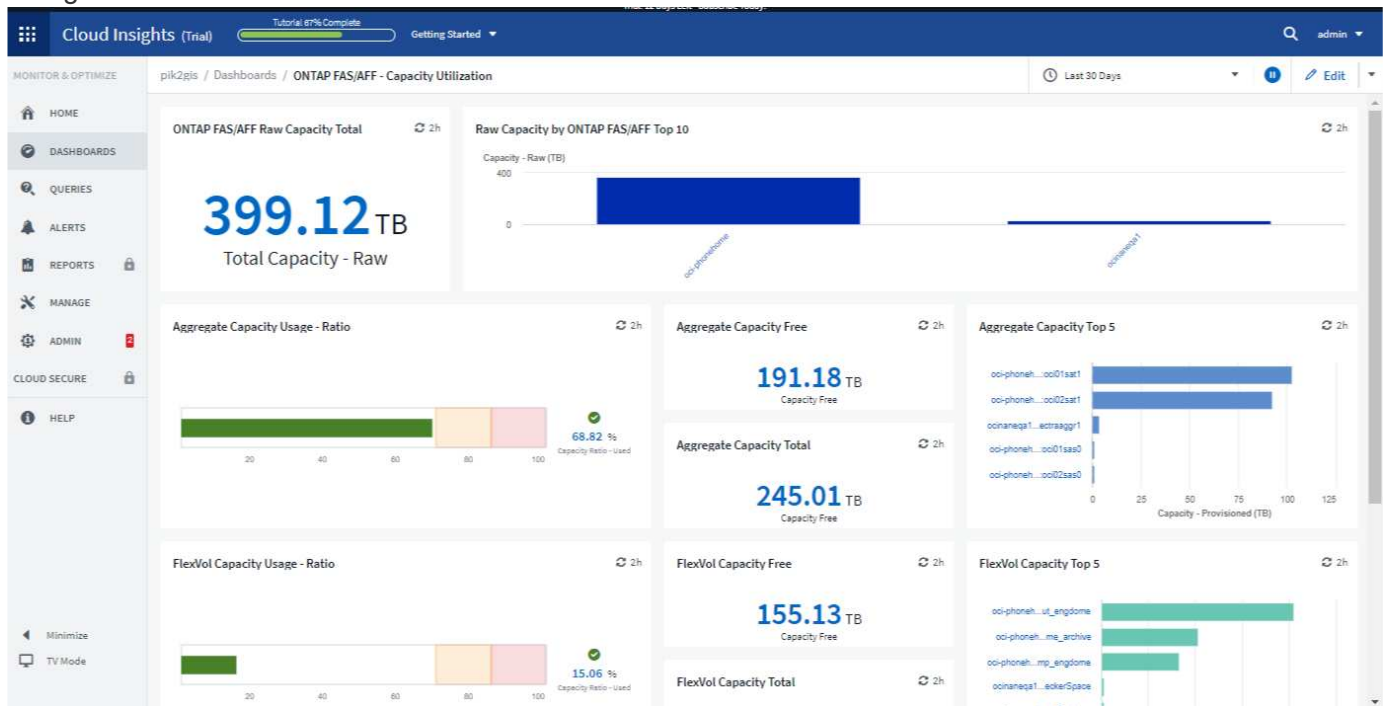
Um zwischen hellen und dunklen Designs zu wechseln, klicken Sie auf die Schaltfläche mit dem Benutzernamen in der oberen rechten Ecke des Bildschirms und wählen Sie das gewünschte Design aus.



Dashboard-Ansicht im dunklen Design:



Dashboard-Ansicht mit hellem Design:



Einige Bildschirmbereiche, wie etwa bestimmte Widget-Diagramme, zeigen auch bei Anzeige im dunklen Design noch immer helle Hintergründe.

Liniendiagramm-Interpolation

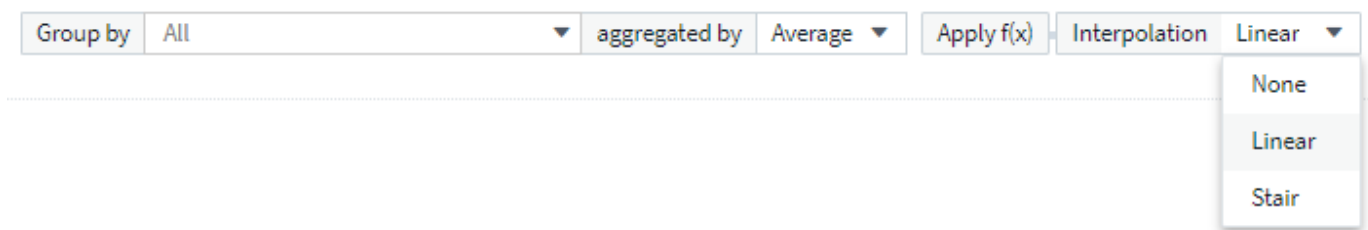
Verschiedene Datensammler fragen ihre Daten oft in unterschiedlichen Intervallen ab. Beispielsweise kann Datensammler A alle 15 Minuten eine Abfrage durchführen, während Datensammler B alle fünf Minuten eine

Abfrage durchführt. Wenn ein Liniendiagramm-Widget (auch Spline-, Flächen- und gestapelte Flächendiagramme) diese Daten aus mehreren Datensammlern in einer einzigen Linie aggregiert (z. B. wenn das Widget nach „alle“ gruppiert) und die Linie alle fünf Minuten aktualisiert, werden die Daten von Sammler B möglicherweise genau angezeigt, während die Daten von Sammler A Lücken aufweisen können, wodurch die Aggregation beeinträchtigt wird, bis Sammler A erneut abfragt.

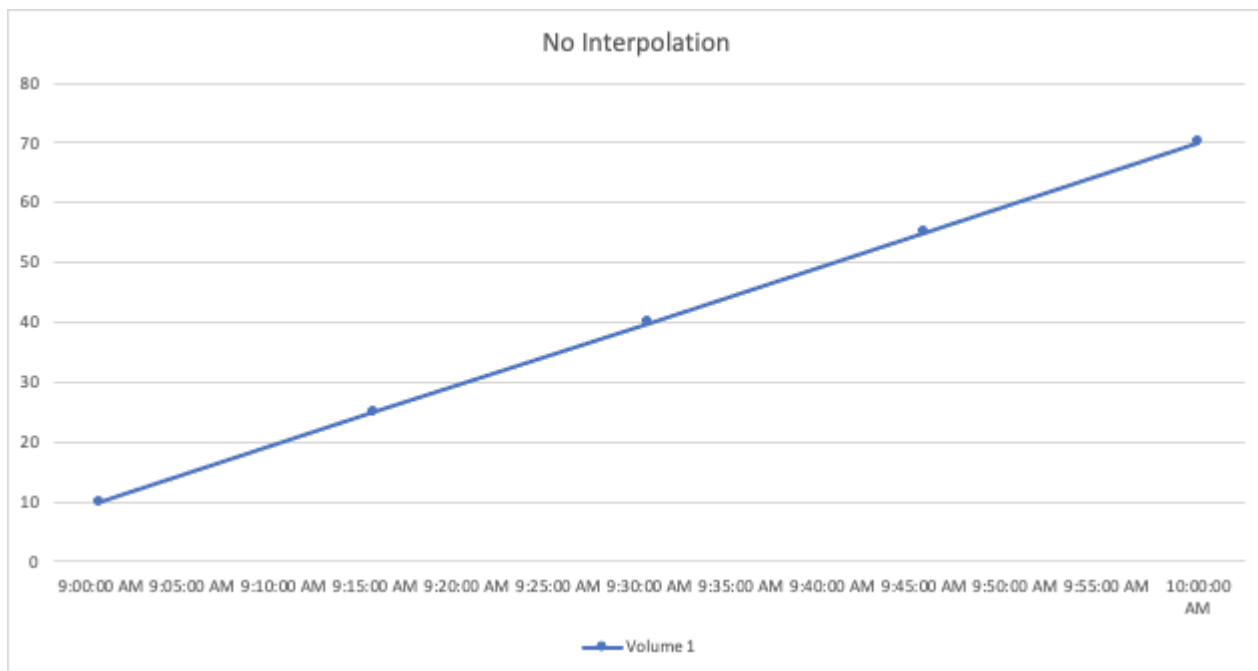
Um dies zu verhindern, interpoliert Data Infrastructure Insights die Daten beim Aggregieren und verwendet die umgebenden Datenpunkte, um eine bestmögliche Schätzung der Daten vorzunehmen, bis die Datensammler eine erneute Abfrage durchführen. Sie können die Objektdaten jedes Datensammlers jederzeit einzeln anzeigen, indem Sie die Gruppierung des Widgets anpassen.

Interpolationsmethoden

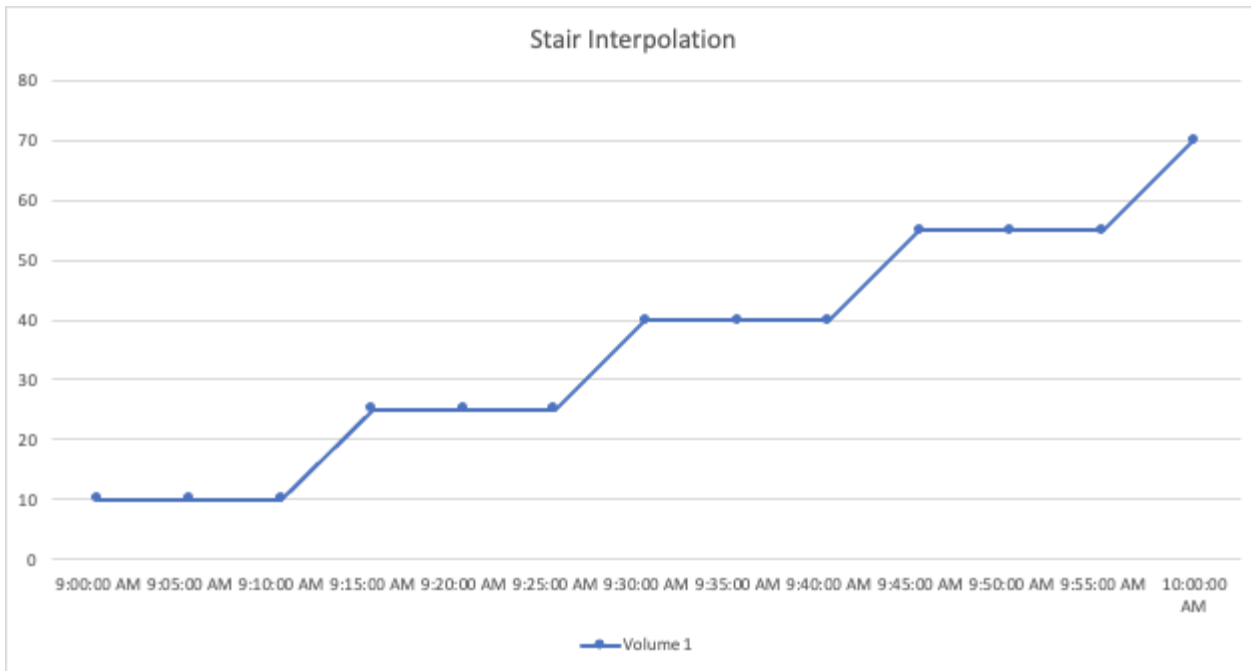
Beim Erstellen oder Ändern eines Liniendiagramms (oder Spline-, Flächen- oder gestapelten Flächendiagramms) können Sie die Interpolationsmethode auf einen von drei Typen einstellen. Wählen Sie im Abschnitt „Gruppieren nach“ die gewünschte Interpolation aus.



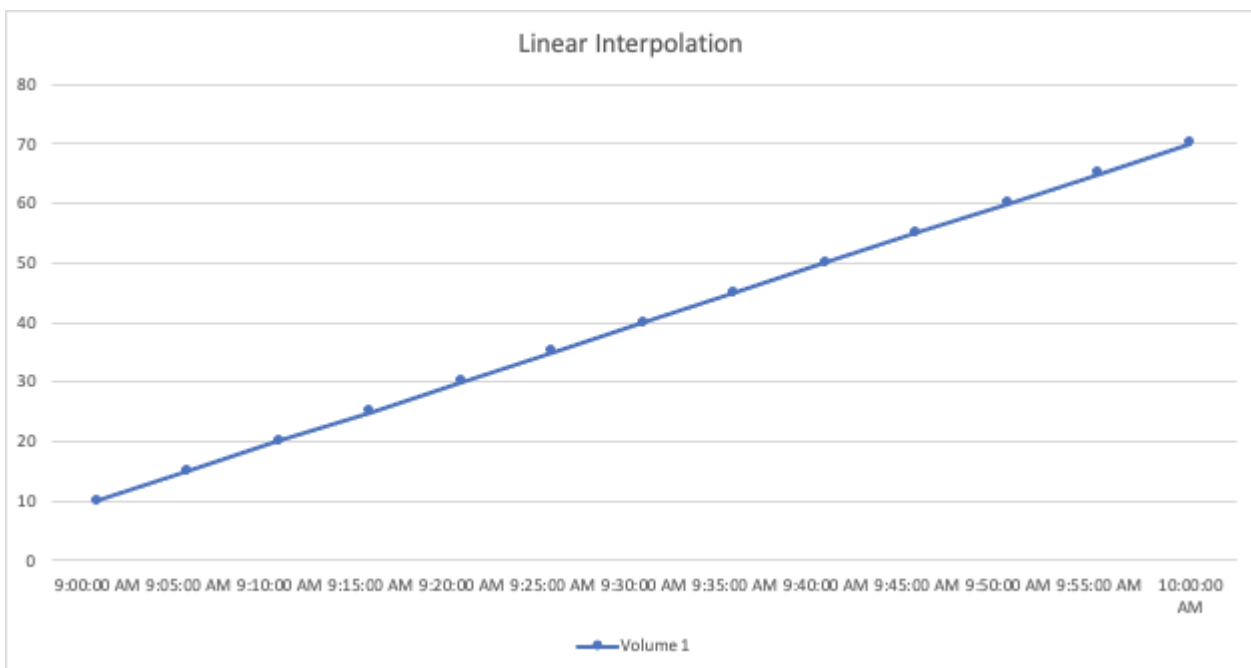
- **Keine:** Nichts tun, d. h. zwischendurch keine Punkte generieren.



- **Treppe:** Aus dem Wert des vorherigen Punkts wird ein Punkt generiert. In einer geraden Linie würde dies als typisches „Treppen“-Layout angezeigt.



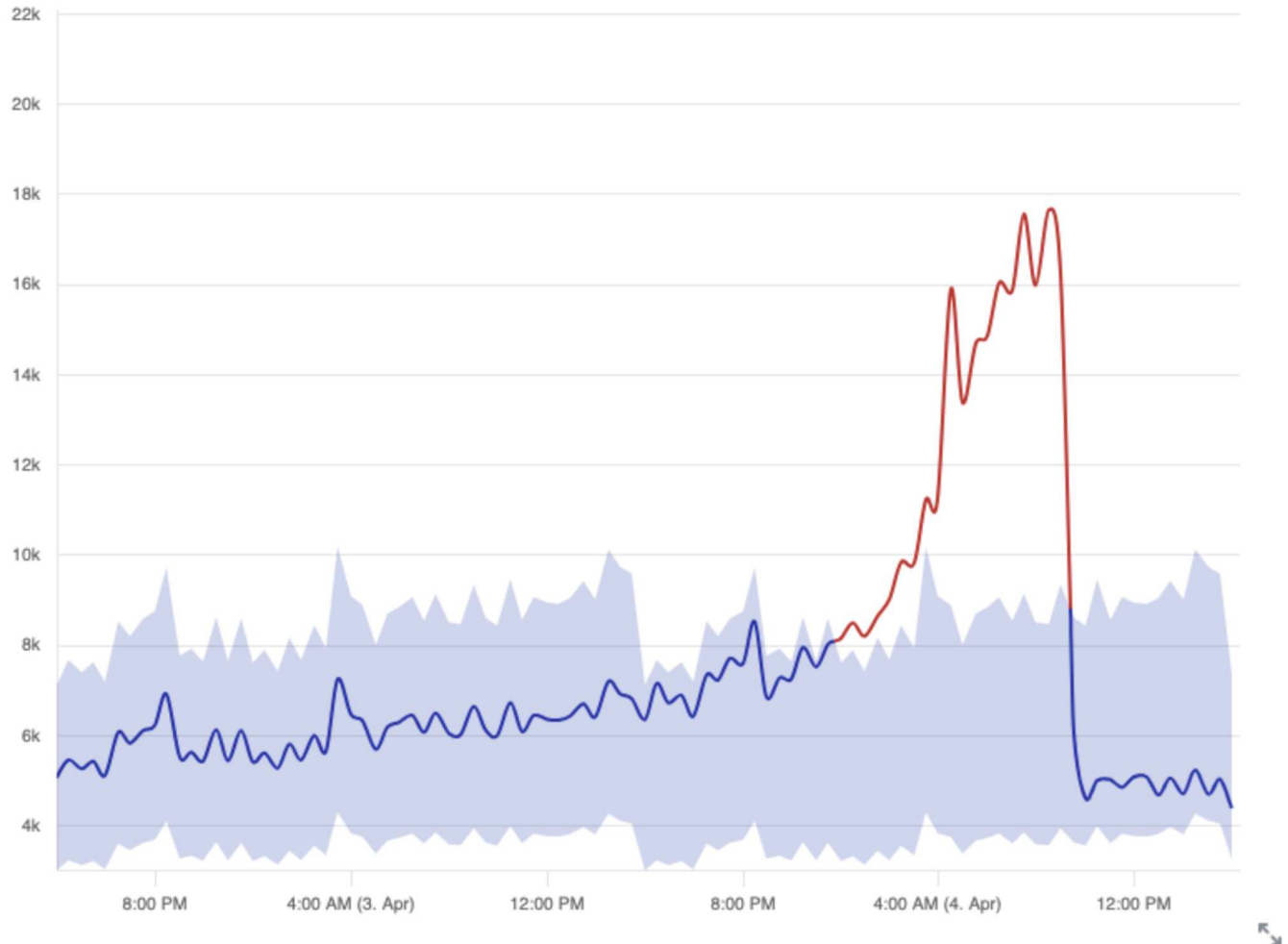
- **Linear:** Ein Punkt wird als Wert zwischen den beiden Verbindungspunkten generiert. Erzeugt eine Linie, die wie die Verbindungslinie zwischen den beiden Punkten aussieht, jedoch mit zusätzlichen (interpolierten) Datenpunkten.



Anomaliegrenzen in Linien-Widgets

Wenn Sie ein Linien- oder Spline-Diagramm-Widget in ein Dashboard oder eine Zielseite einbinden, können Sie das Diagramm im Kontext der **erwarteten Grenzen** für die Daten anzeigen. Sie können sich das so vorstellen, als würden Sie in den Mustern Ihrer Daten nach Anomalien suchen.

DII verwendet saisonale Daten (stündlich oder täglich), um Ober- und Untergrenzen für die *erwarteten* Werte der Daten zu einem bestimmten Zeitpunkt festzulegen. Wenn die Daten über oder unter diese erwarteten Grenzen steigen, wird dies im Diagramm als Anomalie hervorgehoben.



Um Anomaliegrenzen anzuzeigen, bearbeiten Sie das Widget und wählen Sie *Anomaliegrenzen anzeigen*. Sie können zwischen zwei Erkennungsalgorithmen wählen:

- **Adaptiver Detektor** passt sich schnell an Änderungen an und ist daher hilfreich für detaillierte Untersuchungen.
- **Smooth Detector** minimiert Rauschen und Fehllarme, filtert kurzfristige Schwankungen heraus und erkennt dennoch signifikante Verschiebungen.

Darüber hinaus können Sie wählen, ob die Saisonalität stündlich oder täglich angezeigt werden soll, und die Empfindlichkeit der Erkennung festlegen. Bei *hoher* Empfindlichkeit werden mehr Grenzüberschreitungen erkannt, bei *niedriger* Empfindlichkeit weniger.

☒ Show Expected Bounds: Adaptive Detector ? Seasonality: Hourly Sensitivity: High


Beachten Sie, dass Sie die erwarteten Grenzen möglicherweise nur dann sehen, wenn das Diagramm auf die Anzeige einer einzelnen Linie eingestellt ist. Wenn Ihre „Gruppieren nach“-Einstellungen oder Filter mehrere Zeilen anzeigen oder wenn Sie mehrere Abfragen für das Widget festgelegt haben, wird die Option zum Anzeigen der erwarteten Grenzen deaktiviert.


Dashboard-Zugriffsverwaltung

Data Infrastructure Insights gibt Ihnen jetzt mehr Kontrolle über den Zugriff auf die von Ihnen erstellten Dashboards. Sie entscheiden, wer Ihre Diagramme ändern kann. Sie kontrollieren die Offenlegung potenziell sensibler Informationen. Wenn Sie ein Dashboard privat halten, können Sie Ihre Visualisierungen fertigstellen, bis sie für die Nutzung durch andere in Ihrer Organisation bereit sind.


Edit Dashboard Access Settings

Select dashboard sharing access:

☐  Private

☒  Share

Select Editor:


Everyone 

Select Viewer:

None

Everyone

Specific Users



Wenn Sie ein neues Dashboard erstellen, ist dieses Dashboard standardmäßig nur für Sie als Ersteller sichtbar. Kein anderer Benutzer kann das Dashboard sehen oder ändern.

Wenn Sie Ihr Dashboard fertiggestellt haben, können Sie es auch anderen Personen in Ihrer Organisation zur Anzeige gestatten. Um ein Dashboard freizugeben, wählen Sie in der Dashboard-Liste im rechten Menü die

Option „Freigeben“ aus.

<input type="checkbox"/>	★ Tony Dashboard Dec 13 2024 15:48	📄 Tony L	Private	⋮
	Tony Dashboard Jan 10 2025 13:39	Tony L	Private	
	Tony Dashboard Oct 8 2024 11:16	Tony L	👤 Shared	<div>Duplicate Add to Group Share Pin to Top Delete</div>

Sie können das Dashboard für alle oder für ausgewählte Benutzer freigeben, entweder mit Bearbeitungs- oder Nur-Lese-Berechtigungen.

Edit Dashboard Access Settings

Select dashboard sharing access:

☐ Private

☒ Share

Select Editor: Everyone

Select Viewer:

None
Everyone
Specific Users

Best Practices für Dashboards und Widgets

Tipps und Tricks, die Ihnen helfen, die leistungsstarken Funktionen von Dashboards und Widgets optimal zu nutzen.

Die richtige Metrik finden

Data Infrastructure Insights erfasst Zähler und Metriken unter Verwendung von Namen, die sich manchmal von Datensammler zu Datensammler unterscheiden.

Bedenken Sie bei der Suche nach der richtigen Metrik oder dem richtigen Zähler für Ihr Dashboard-Widget, dass die gewünschte Metrik möglicherweise einen anderen Namen hat als den, an den Sie denken. Während Dropdown-Listen in Data Infrastructure Insights normalerweise alphabetisch geordnet sind, kann es vorkommen, dass ein Begriff nicht dort in der Liste angezeigt wird, wo er Ihrer Meinung nach hingehört. Beispielsweise erscheinen Begriffe wie „Rohkapazität“ und „genutzte Kapazität“ in den meisten Listen nicht zusammen.

Best Practice: Verwenden Sie die Suchfunktion in Feldern wie „Filtern nach“ oder an Stellen wie der Spaltenauswahl, um das Gesuchte zu finden. Wenn Sie beispielsweise nach „cap“ suchen, werden alle Metriken angezeigt, deren Name „capacity“ enthält, unabhängig davon, wo sie in der Liste vorkommen. Sie

können dann ganz einfach die gewünschten Metriken aus dieser kürzeren Liste auswählen.

Hier sind einige alternative Ausdrücke, die Sie bei der Suche nach Metriken ausprobieren können:

Wenn Sie Folgendes finden möchten:	Versuchen Sie auch, nach Folgendem zu suchen:
CPU	Prozessor
Kapazität	Genutzte Kapazität Rohkapazität Bereitgestellte Kapazität Speicherpoolkapazität <anderer Assettyp>-Kapazität Geschriebene Kapazität
Festplattengeschwindigkeit	Niedrigste Festplattengeschwindigkeit Festplattentyp mit der geringsten Leistung
Gastgeber	Hypervisor-Hosts
Hypervisor	Host ist Hypervisor
Mikrocode	Firmware
Name	Alias Hypervisorname Speichernamen <anderer Assettyp> Name Einfacher Name Ressourcenname Fabric-Alias
Lesen / Schreiben	Teilweise R/W Ausstehende Schreibvorgänge IOPS – Schreibkapazität Latenz – Lesen Cache-Auslastung – Lesen
Virtuelle Maschine	VM ist virtuell

Dies ist keine vollständige Liste. Dies sind lediglich Beispiele für mögliche Suchbegriffe.

Die richtigen Vermögenswerte finden

Die Assets, 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-Typ-Zähler, nach denen Sie filtern oder eine Spalte hinzufügen können. Beachten Sie beim Erstellen Ihres Widgets Folgendes:

Dieser Asset-Typ/Zähler:	Kann nach diesen Assets gefiltert werden:
Virtuelle Maschine	VMDK
Datenspeicher	Internes Volume VMDK-Volume der virtuellen Maschine
Hypervisor	Virtuelle Maschine ist Hypervisor-Host
Gastgeber	Internes Volume Volume Cluster Host Virtuelle Maschine
Stoff	Hafen

Dies ist keine vollständige Liste.

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

Streudiagramm-Beispiel: Kennen Sie Ihre Achse

Durch Ändern der Reihenfolge der Zähler in einem Streudiagramm-Widget werden die Achsen geändert, auf denen die Daten angezeigt werden.

Informationen zu diesem Vorgang

In diesem Beispiel wird ein Streudiagramm erstellt, mit dem Sie VMs mit geringer Leistung und hoher Latenz im Vergleich zu niedrigen IOPS erkennen können.

Schritte

1. Erstellen oder öffnen Sie ein Dashboard im Bearbeitungsmodus und fügen Sie ein **Streudiagramm**-Widget hinzu.
2. Wählen Sie einen Asset-Typ aus, beispielsweise *Virtuelle Maschine*.
3. Wählen Sie den ersten Zähler aus, den Sie darstellen möchten. Wählen Sie für dieses Beispiel *Latenz – Gesamt*.

Latenz – Gesamt wird entlang der X-Achse des Diagramms dargestellt.

4. Wählen Sie den zweiten Zähler aus, den Sie darstellen möchten. Wählen Sie für dieses Beispiel *IOPS – Gesamt* aus.

IOPS – Gesamt wird im Diagramm entlang der Y-Achse dargestellt. VMs mit höherer Latenz werden auf der rechten Seite des Diagramms angezeigt. Es werden nur die 100 VMs mit der höchsten Latenz angezeigt, da die Einstellung **Top nach X-Achse** aktuell ist.

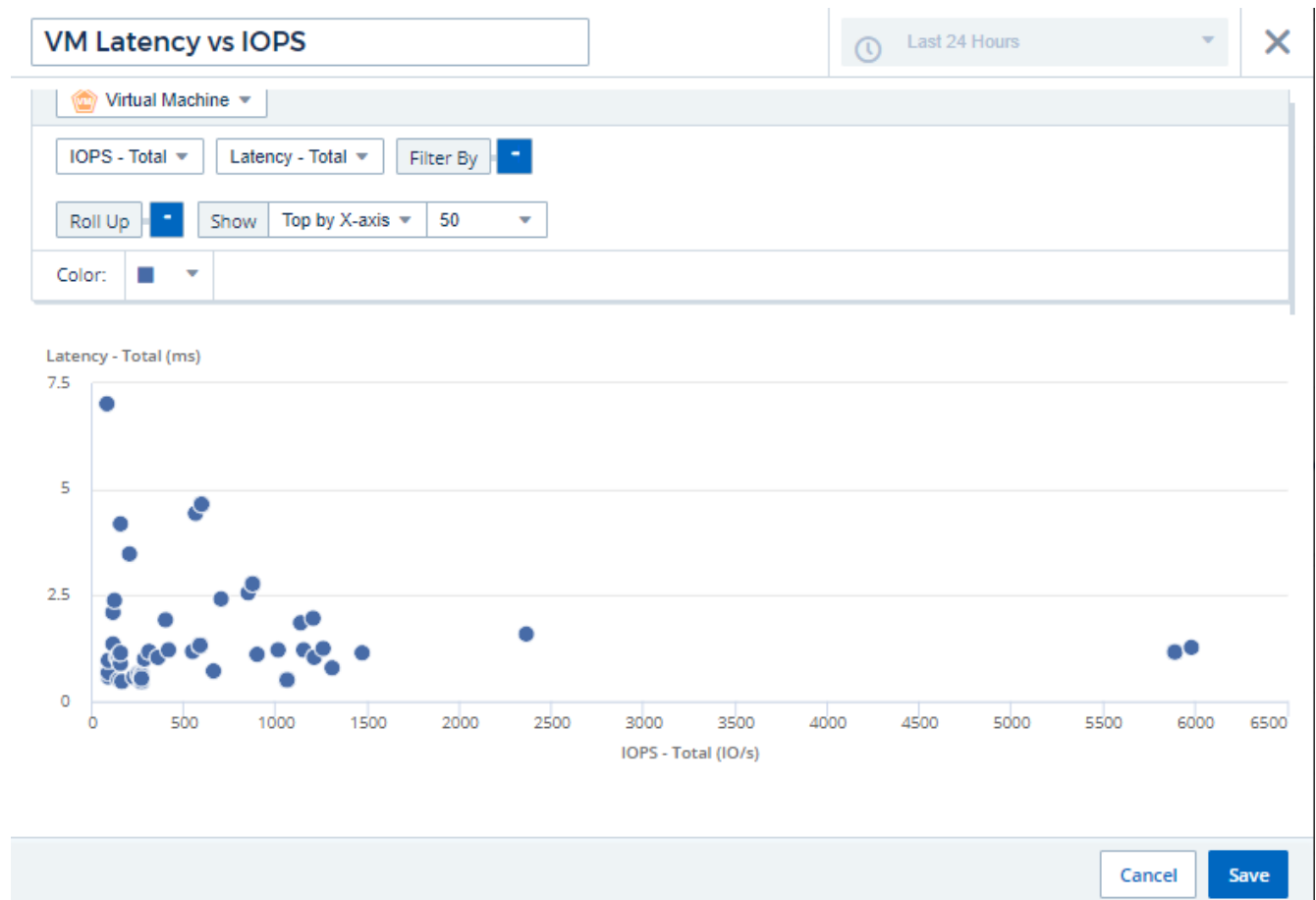


5. Kehren Sie nun die Reihenfolge der Zähler um, indem Sie den ersten Zähler auf *IOPS – Gesamt* und den

zweiten auf *Latenz – Gesamt* setzen.

Im Diagramm wird nun die *Latenz – Gesamt* entlang der Y-Achse und die *IOPS – Gesamt* entlang der X-Achse dargestellt. VMs mit höheren IOPS werden jetzt auf der rechten Seite des Diagramms angezeigt.

Beachten Sie, dass das Widget jetzt die 100 VMs mit den höchsten IOPS anzeigt, da wir die Einstellung **Top by X-Axis** nicht geändert haben, da diese derzeit entlang der X-Achse dargestellt werden.



Sie können für das Diagramm auswählen, ob die obersten N der X-Achse, die obersten N der Y-Achse, die untersten N der X-Achse oder die untersten N der Y-Achse angezeigt werden sollen. In unserem letzten Beispiel zeigt das Diagramm die Top 100 VMs mit den höchsten Gesamt-IOPS. Wenn wir es in **Top nach Y-Achse** ändern, zeigt das Diagramm erneut die 100 VMs mit der höchsten Gesamtlatenz an.

Beachten Sie, dass Sie in einem Streudiagramm auf einen Punkt klicken können, um zur Asset-Seite für diese Ressource zu gelangen.

Beispiel-Dashboards

Dashboard-Beispiel: Leistung virtueller Maschinen

Der IT-Betrieb steht heute vor zahlreichen Herausforderungen. Von Administratoren wird verlangt, mit weniger mehr zu erreichen, und die vollständige Transparenz Ihrer dynamischen Rechenzentren ist ein Muss. In diesem Beispiel zeigen wir Ihnen, wie Sie ein Dashboard mit Widgets erstellen, die Ihnen betriebliche Einblicke in die Leistung der virtuellen Maschine (VM) auf Ihrem Mandanten geben. Wenn Sie diesem Beispiel folgen

und Widgets erstellen, die auf Ihre eigenen spezifischen Anforderungen zugeschnitten sind, können Sie beispielsweise die Backend-Speicherleistung im Vergleich zur Frontend-Leistung virtueller Maschinen visualisieren oder die VM-Latenz im Vergleich zur E/A-Nachfrage anzeigen.

Informationen zu diesem Vorgang

Hier erstellen wir ein Dashboard zur Leistung virtueller Maschinen mit den folgenden Informationen:

- eine Tabelle mit VM-Namen und Leistungsdaten
- ein Diagramm, das die VM-Latenz mit der Speicherlatenz vergleicht
- ein Diagramm, das Lese-, Schreib- und Gesamt-IOPS für VMs zeigt
- ein Diagramm, das den maximalen Durchsatz für Ihre VMs zeigt

Dies ist nur ein einfaches Beispiel. Sie können Ihr Dashboard anpassen, um beliebige Leistungsdaten hervorzuheben und zu vergleichen und so Ihre eigenen betrieblichen Best Practices zu verfolgen.

Schritte

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

Die Seite **Neues Dashboard** wird geöffnet.

3. Geben Sie oben auf der Seite einen eindeutigen Namen für das Dashboard ein, beispielsweise „VM-Leistung nach Anwendung“.
4. Klicken Sie auf **Speichern**, um das Dashboard unter 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** aus, um dem Dashboard ein neues Tabellen-Widget hinzuzufügen.

Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Die angezeigten Standarddaten gelten für alle Speicher Ihres Mandanten.

Table Widget 10m

1,746 items found in 71 groups

Hypervisor Name ↑	Virtual Machine	Capacity - Total (GB)	IOPS - Total (IO/s)	Latency - Total (ms)
10.197.143.53 (9)	--	1,690.58	1.80	12.04
10.197.143.54 (7)	--	1,707.60	4.62	12.69
10.197.143.57 (11)	--	1,509.94	1.14	1.15
10.197.143.58 (10)	--	1,818.34	5.83	2.57
AzureComputeDefaultAvailabilitySet (363)	N/A	N/A	N/A	N/A
anandh9162020113920-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh916202013287-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh91720201288-rg-avset.anandh91720201	--	N/A	N/A	N/A
anjalivIngrun48-rg-avset.anjalivIngrun48-rg.398	--	N/A	N/A	N/A
anjalivIngrun50-rg-avset.anjalivIngrun50-rg.398	--	N/A	N/A	N/A
batutiscanaryHA97a-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A
batutiscanaryHA97b-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A

- Wir können dieses Widget anpassen. Löschen Sie im Feld „Name“ oben „Widget 1“ und geben Sie „Virtual Machine Performance table“ ein.
- Klicken Sie auf das Dropdown-Menü „Asset-Typ“ und ändern Sie „*Speicher*“ in „*Virtuelle Maschine*_“.

Die Tabellendaten ändern sich, um alle virtuellen Maschinen auf Ihrem Mandanten anzuzeigen.

- Fügen wir der Tabelle einige Spalten hinzu. Klicken Sie rechts auf das Zahnradsymbol und wählen Sie *Hypervisorname*, *IOPS – Gesamt* und *Latenz – Gesamt* aus. Sie können auch versuchen, den Namen in die Suche einzugeben, um schnell das gewünschte Feld anzuzeigen.

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

- Für diese Übung schließen wir VMs aus, die nicht aktiv verwendet werden. Filtern wir also alles heraus, was weniger als 10 IOPS insgesamt hat. Klicken Sie auf die Schaltfläche **[+]** neben **Filtern nach** und wählen Sie *IOPS – Gesamt* aus. Klicken Sie auf **Beliebig** und geben Sie „10“ in das Feld **Von** ein. Lassen Sie das Feld **An** leer. Klicken Sie außerhalb des Filterfelds oder drücken Sie die Eingabetaste, um den Filter festzulegen.

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

- Wir können die Tabelle weiter reduzieren, indem wir die Ergebnisse gruppieren. Klicken Sie auf die Schaltfläche **[+]** neben **Gruppieren nach** und wählen Sie ein Feld zum Gruppieren aus, z. B. *Anwendung* oder *Hypervisorname*. Die Gruppierung wird automatisch angewendet.

Die Tabellenzeilen werden nun entsprechend Ihrer Einstellung gruppiert. Sie können die Gruppen nach Bedarf erweitern und reduzieren. Gruppierte Zeilen zeigen zusammengefasste Daten für jede Spalte. Bei einigen Spalten können Sie die Rollup-Methode für die jeweilige Spalte auswählen.

Virtual Machine Performance Table

☐ Override dashboard time

Last 24 hours

×

Virtual Machine

Filter by

IOPS - Total (IO/s)

>= 10

×

+

Group by

Hypervisor name

×

181 items found in 4 groups

Hypervisor name ↓	Name	Hypervisor name	IOPS - Total	Latency - Total (ms)
us-east-1d (62)		us-east-1d		1.94
us-east-1c (80)		us-east-1c		0.80
us-east-1b (1)	TBDemoEnv	us-east-1b	32.66	0.70
us-east-1a (38)		us-east-1a	121.22	0.81

Cancel

Save

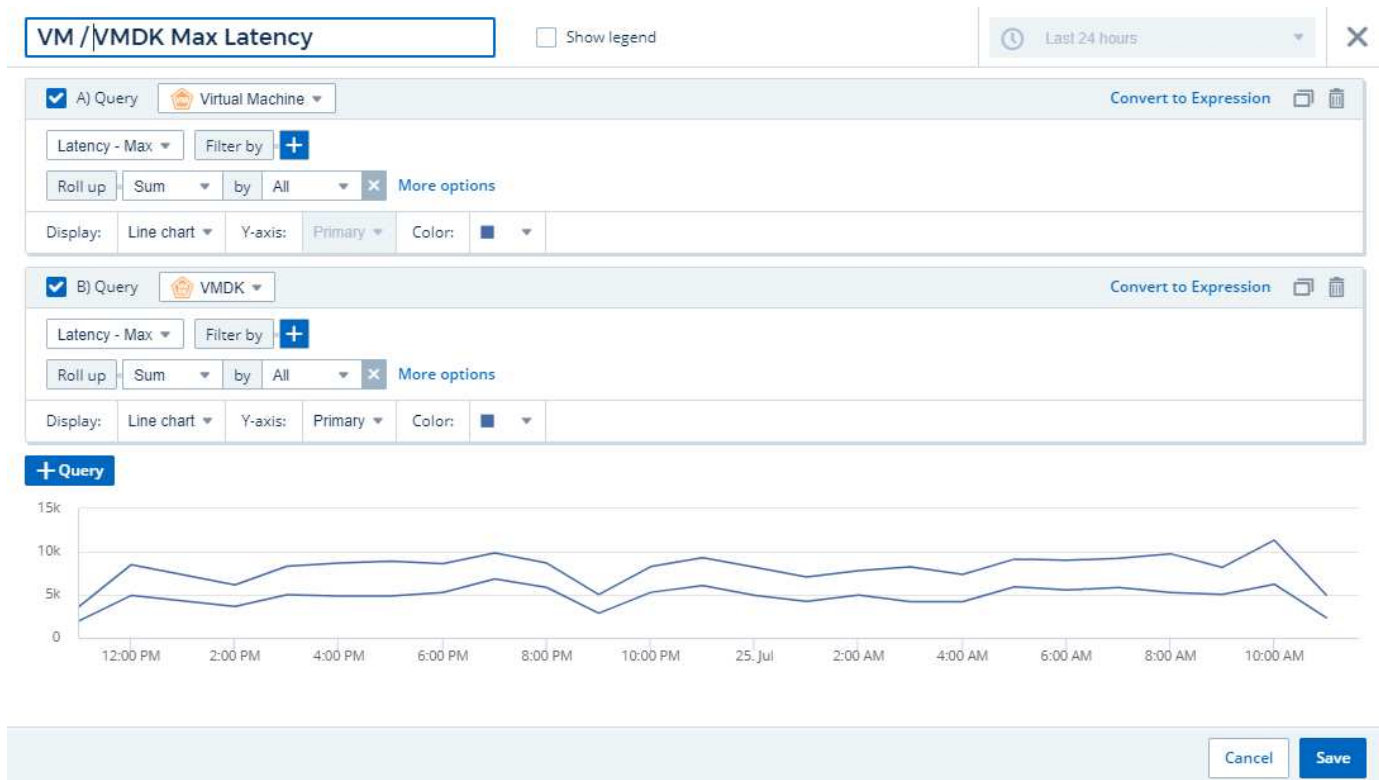
- Wenn Sie das Tabellen-Widget nach Ihren Wünschen angepasst haben, klicken Sie auf die Schaltfläche **[Speichern]**.

Das Tabellen-Widget 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.

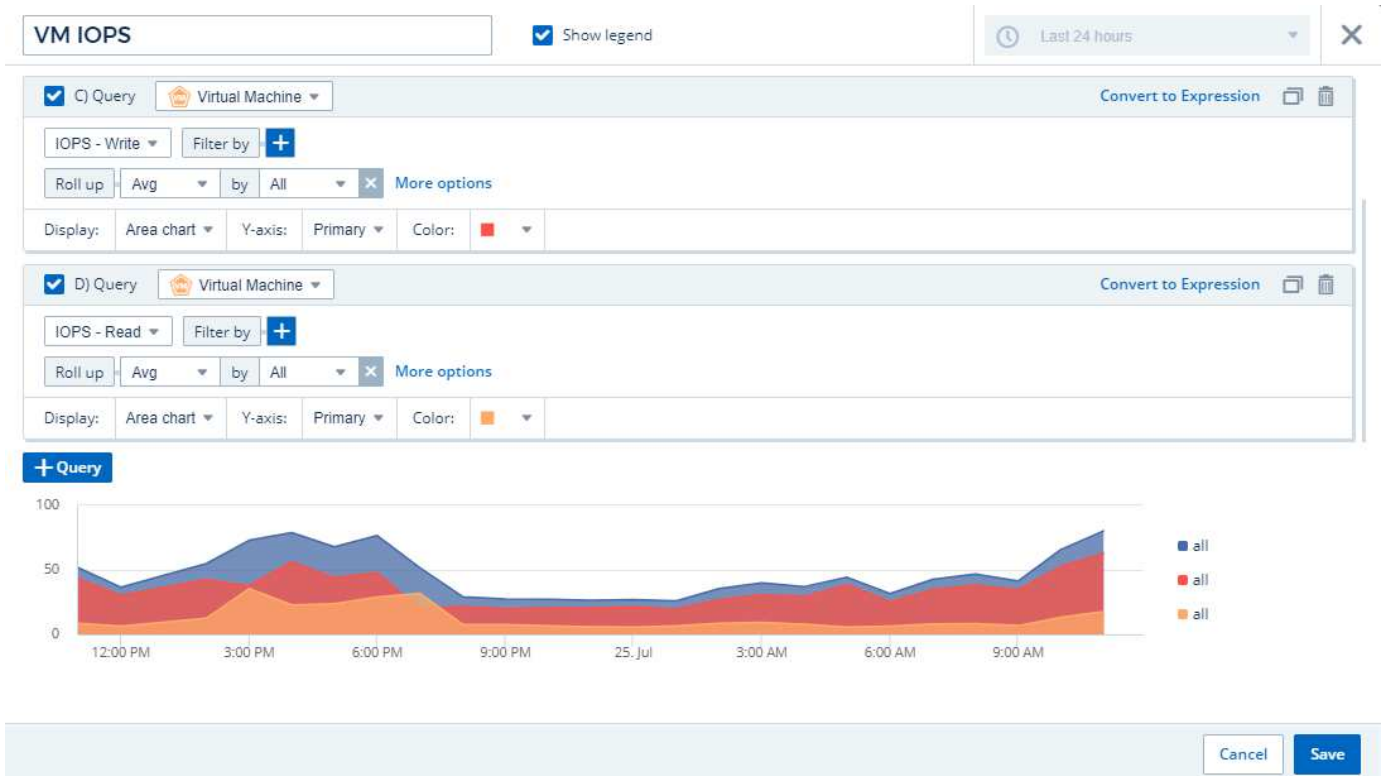
Als Nächstes fügen wir einige Diagramme hinzu, um die Leistung unserer VM anzuzeigen. Erstellen wir ein Liniendiagramm, das die VM-Latenz mit der VMDK-Latenz vergleicht.

- Klicken Sie bei Bedarf auf das Symbol **Bearbeiten** im Dashboard, um den Bearbeitungsmodus zu aktivieren.
- Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm* aus, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
- Das Dialogfeld **Widget bearbeiten** wird geöffnet. Nennen Sie dieses Widget „VM / VMDK Max Latency“
- Wählen Sie **Virtuelle Maschine** und wählen Sie *Latenz – Max*. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Rollup** *Sum by All*. Zeigen Sie diese Daten als *Liniendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
- Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile *VMDK* und *Latency – Max* aus. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Rollup** *Sum by All*. Zeigen Sie diese Daten als *Liniendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
- Klicken Sie auf **[Speichern]**, um dieses Widget zum Dashboard hinzuzufügen.



Als Nächstes fügen wir ein Diagramm hinzu, das die Lese-, Schreib- und Gesamt-IOPS der VM in einem einzigen Diagramm zeigt.

1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Flächendiagramm* aus, um dem Dashboard ein neues Flächendiagramm-Widget hinzuzufügen.
2. Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Nennen Sie dieses Widget „VM IOPS“
3. Wählen Sie **Virtuelle Maschine** und wählen Sie *IOPS – Gesamt*. Legen Sie die gewünschten Filter fest oder lassen Sie **Filtern nach** leer. Wählen Sie für **Aufsummieren** *Summe* nach *Alle*. Zeigen Sie diese Daten als *Flächendiagramm* an und belassen Sie die *Y-Achse* als *Primär*.
4. Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und dann *IOPS – Lesen*.
5. Klicken Sie auf die Schaltfläche **[+Abfrage]**, um eine dritte Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und dann *IOPS – Write* aus.
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.

Als Nächstes fügen wir ein Diagramm hinzu, das den VM-Durchsatz für jede mit der VM verknüpfte Anwendung zeigt. Wir werden hierfür die Roll-Up-Funktion verwenden.

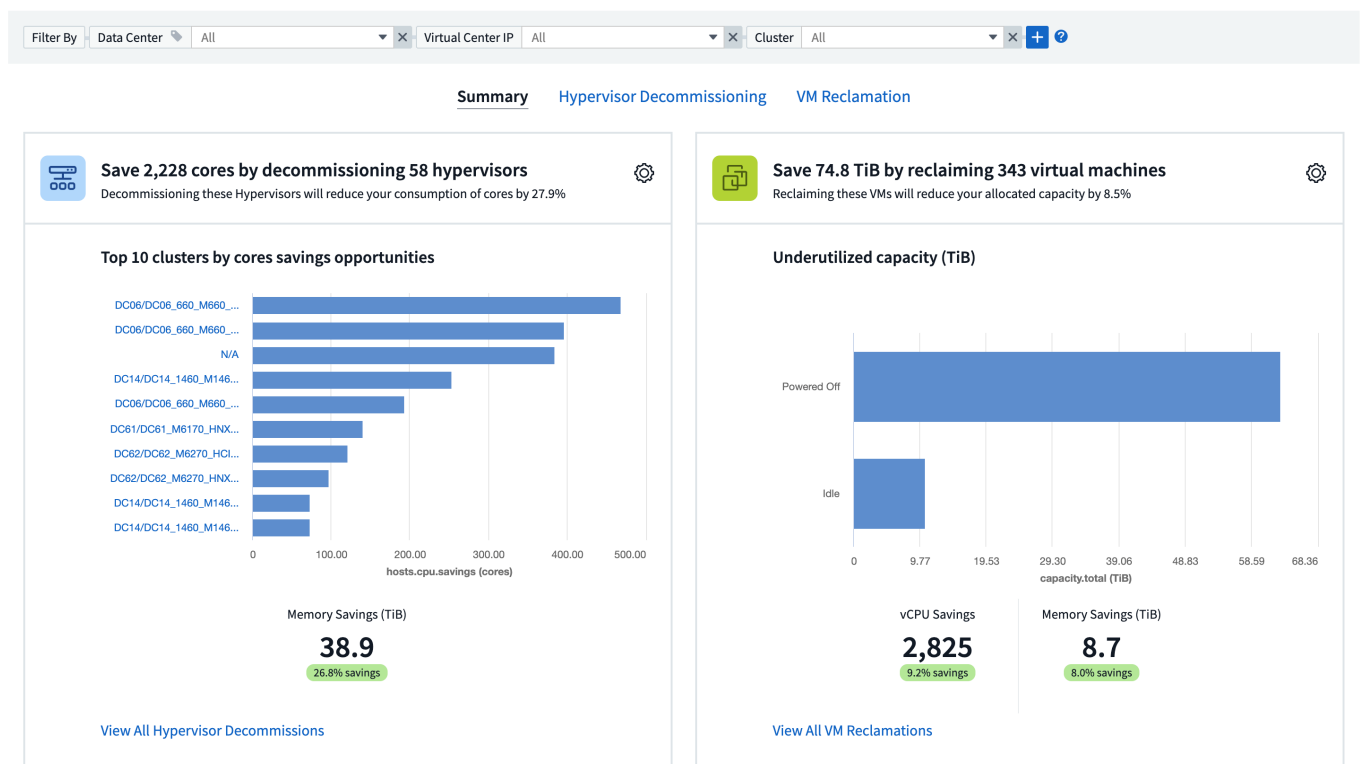
1. Klicken Sie auf das Symbol **[Widget hinzufügen]** und wählen Sie *Liniendiagramm* aus, um dem Dashboard ein neues Liniendiagramm-Widget hinzuzufügen.
2. Das Dialogfeld „Widget bearbeiten“ wird geöffnet. Nennen Sie dieses Widget „VM-Durchsatz nach Anwendung“.
3. Wählen Sie „Virtuelle Maschine“ und dann „Durchsatz – Gesamt“. Legen Sie die gewünschten Filter fest oder lassen Sie das Feld „Filtern nach“ leer. Wählen Sie für Rollup „Max“ und wählen Sie nach „Anwendung“ oder „Name“ aus. Zeigen Sie die Top 10-Anwendungen. Zeigen Sie diese Daten als Liniendiagramm an und belassen Sie die Y-Achse als primär.
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 oben im Widget gedrückt halten und es an eine neue Position ziehen.

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

Denken Sie daran, das Dashboard nach dem Vornehmen Ihrer Änderungen **[Speichern]** zu speichern.

Ihr endgültiges VM-Leistungs-Dashboard sieht ungefähr so aus:



Arbeiten mit Abfragen

Abfragen von Assets und Metriken

Fragen Sie die physischen und virtuellen Assets Ihrer Infrastruktur ab, um die Leistung zu überwachen, Probleme zu beheben und granulare Suchen anhand benutzerdefinierter Kriterien wie Annotationen durchzuführen. Data Infrastructure Insights ermöglicht Abfragen über verschiedene Asset-Typen hinweg – von Storage-Arrays und Hosts bis hin zu Anwendungen und virtuellen Maschinen – zusammen mit Integrationsmetriken von Kubernetes, Docker und ONTAP Advanced Data für umfassende Sichtbarkeit.

Beachten Sie, dass Annotationsregeln, die automatisch Annotationen Assets zuweisen, eine Abfrage erfordern, die für alle freigegeben wurde. Weitere Informationen zum Freigeben von Abfragen finden Sie unten.

Sie können die physischen oder virtuellen Inventarressourcen (und die zugehörigen Metriken) Ihres Mandanten oder die mit der Integration bereitgestellten Metriken wie Kubernetes oder ONTAP Advanced Data abfragen.

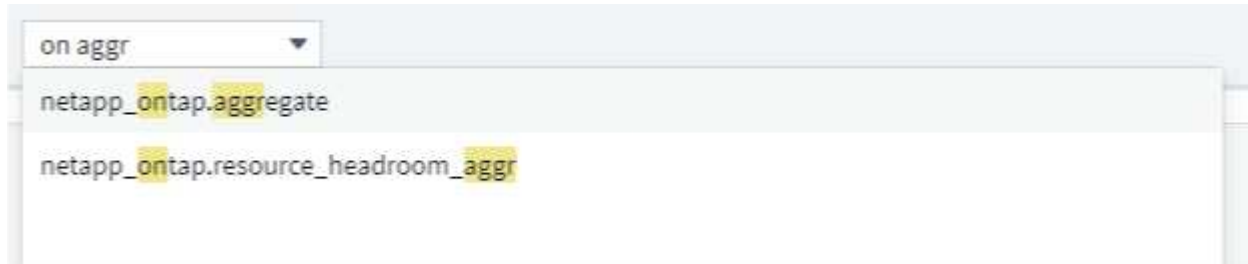
Inventarvermögen

Alle Inventar- (auch Infrastruktur-) Asset-Typen (Storage, Switch, VM, Application usw.) können in Abfragen, Dashboard-Widgets und benutzerdefinierten Asset-Landingpages verwendet werden. Die für Filter, Ausdrücke und Anzeige verfügbaren Felder und Zähler variieren je nach Asset-Typ.

Integrationsmetriken

Zusätzlich zur Abfrage von Inventarressourcen und den zugehörigen Leistungsmetriken können Sie auch

Integrationsdaten-Metriken abfragen, wie sie beispielsweise von Kubernetes oder Docker generiert oder mit ONTAP Advanced Metrics bereitgestellt werden.



Abfragen freigeben

Steuern Sie den Zugriff auf Ihre Abfragen, indem Sie festlegen, wer sie anzeigen und bearbeiten darf. Standardmäßig sind neue Abfragen privat und nur für Sie sichtbar, und Sie können sie mit bestimmten Benutzern oder Ihrer gesamten Organisation mit flexiblen Berechtigungsstufen (Nur Lesen oder Bearbeiten) teilen.

Sie können wählen, die Abfrage für alle oder für ausgewählte Benutzer freizugeben, mit entweder Bearbeitungs- oder Nur-Lese-Berechtigungen.



Benutzer mit der Berechtigung „Account Owner“ können alle Anfragen sehen, unabhängig von der Datenschutzeinstellung.

Erstellen von Abfragen

Mithilfe von Abfragen können Sie die Assets Ihres Mandanten auf granularer Ebene durchsuchen, die gewünschten Daten filtern und die Ergebnisse nach Ihren Wünschen sortieren.

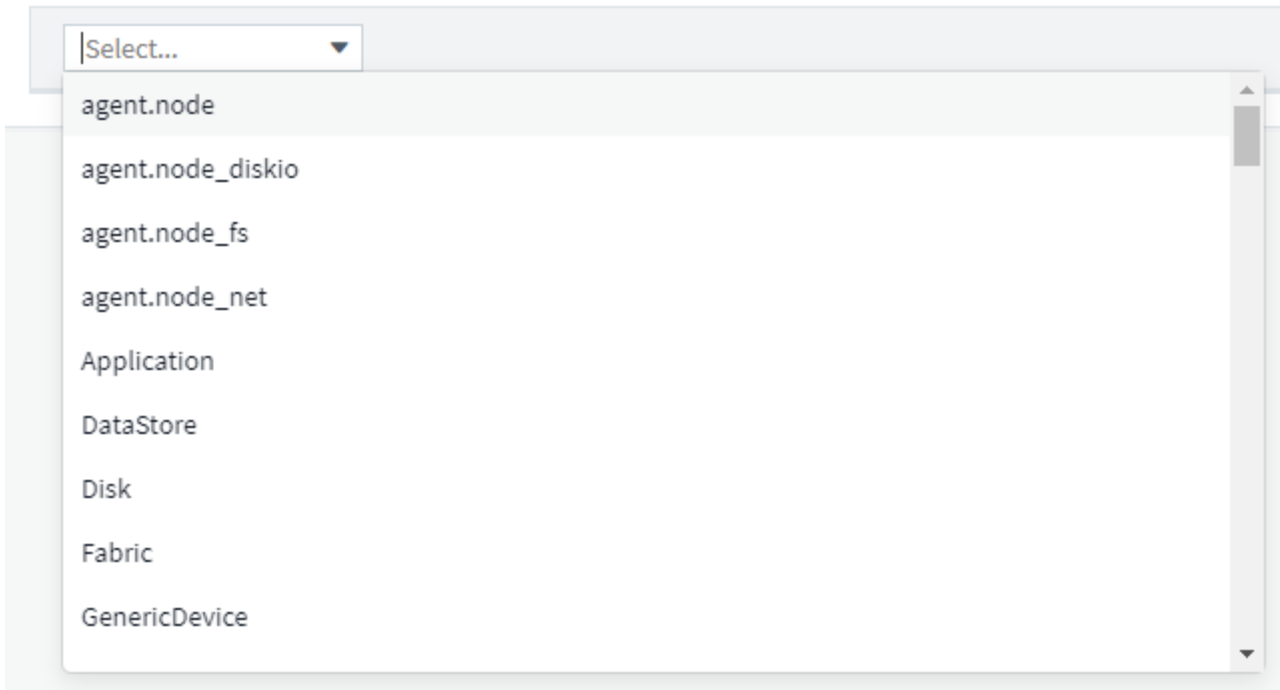
Sie können beispielsweise eine Abfrage für *Volumes* erstellen, einen Filter hinzufügen, um bestimmte *Speicher* zu finden, die mit den ausgewählten Volumes verknüpft sind, einen weiteren Filter hinzufügen, um eine bestimmte *Annotation* wie „Tier 1“ auf den ausgewählten Speichern zu finden, und schließlich einen weiteren Filter hinzufügen, um alle Speicher mit *IOPS – Lesen (IO/s)* größer als 25 zu finden. Wenn die Ergebnisse angezeigt werden, können Sie die mit der Abfrage verknüpften Informationsspalten in aufsteigender oder absteigender Reihenfolge sortieren.

Hinweis: Wenn ein neuer Datensammler hinzugefügt wird, der Assets erfasst, oder wenn Anmerkungen oder Anwendungszuweisungen vorgenommen werden, können Sie diese neuen Assets, Anmerkungen oder Anwendungen erst abfragen, nachdem die Abfragen indiziert wurden. Die Indizierung erfolgt in regelmäßigen Abständen oder während bestimmter Ereignisse, beispielsweise beim Ausführen von Anmerkungsregeln.

Das Erstellen einer Abfrage ist ganz einfach:

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

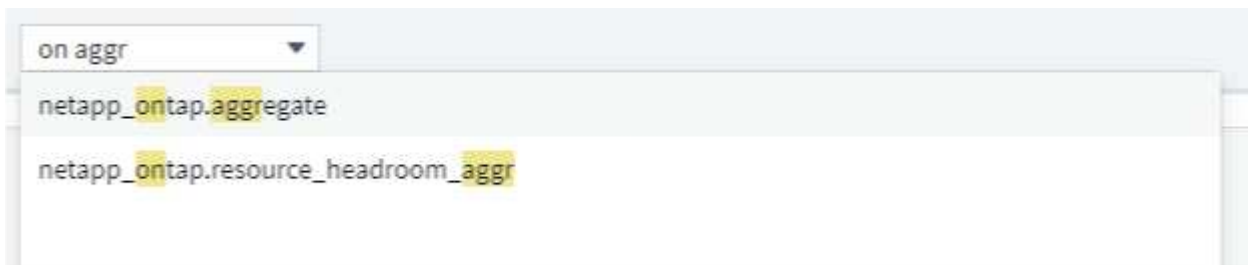
Scrollliste:



A screenshot of a web interface showing a dropdown menu. The dropdown is open, displaying a list of query types. The first item, 'agent.node', is highlighted. The dropdown is located within a light gray container.

- agent.node
- agent.node_diskio
- agent.node_fs
- agent.node_net
- Application
- DataStore
- Disk
- Fabric
- GenericDevice

Zum Suchen eingeben:



A screenshot of a web interface showing a search dropdown menu. The dropdown is open, displaying a list of search results. The first item, 'netapp_ontap.aggregate', is highlighted. The dropdown is located within a light blue container.

- on aggr
- netapp_ontap.aggregate
- netapp_ontap.resource_headroom_aggr

Sie können Filter hinzufügen, um Ihre Abfrage weiter einzugrenzen, indem Sie im Feld **Filtern nach** auf die Schaltfläche **+** klicken. Gruppieren Sie Zeilen nach Objekt oder Attribut. Wenn Sie mit Integrationsdaten (Kubernetes, ONTAP Advanced Metrics usw.) arbeiten, können Sie bei Bedarf nach mehreren Attributen gruppieren.

netapp_ontap.aggregate X ▼

Filter By cluster_name ci- X +

Group aggr_name X ▼

5 items found

Table Row Grouping	Metrics & Attributes	
aggr_name	cp_read_blocks	cluster_name ↓
oci02sat0	0.59	oci-phonehome
oci02sat1	0.15	oci-phonehome
oci02sat2	212.64	oci-phonehome
oci01sat0	0.39	oci-phonehome
oci01sat1	48.89	oci-phonehome

Die Abfrageergebnisliste zeigt je nach gesuchtem Objekttyp eine Reihe von Standardspalten. Um Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle. Die verfügbaren Spalten variieren je nach Asset-/Metriktyp.

netapp_ontap.aggregate X ▼

Filter By +

Group aggr_name X ▼

14 items found

Table Row Grouping	Metrics & Attributes	
aggr_name	cp_read_blocks	agent_version ↑
aggr0_optimus_02	1.72	Apache-HttpCli
aggr1_optimus_02	408.84	Apache-HttpCli
ocinaneqa1_04_aggr0	6.19	Apache-HttpCli
ocinaneqa1_03_aggr0	6.48	Apache-HttpCli
oci02sat0	1.04	Apache-HttpCli

Search...

☐ Show Selected Only

☒ agent_version

☐ aggr_name

☐ cluster_location

☒ cluster_name

☐ cluster_serial_number

☐ cluster_version

Sehen Sie es in Aktion

["Erkunden und Analysieren mit Abfragen in Data Infrastructure Insights \(Video\)"](#)

Auswählen von Aggregation, Einheiten und bedingter Formatierung

Aggregation und Einheiten

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

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (ms)
nvme0n1	20,604,960.00
nvme0n1	29,184,970.00
nvme0n1	4,642,684.00
nvme0n1	31,918,988.00
nvme0n1	29,258,256.00
nvme0n1	18,022,164.00
nvme0n1	28,483,300.00
nvme0n1	69,835,016.00
nvme0n1	15,952,780.00
nvme0n1	44,169,696.00
nvme0n1	12,138,928.00
nvme0n1	5,234,528.00
nvme0n1	34,260,552.00

Aggregation

Group By
 Avg

Time Aggregate By
 Last

Unit Display

Base Unit
 millisecond (ms)

Displayed In
 millisecond (ms)

Conditional Formatting

If value is
 > (Greater than)

Warning
 Optional
 ms

Critical
 Optional
 ms

Rename Column

Einheiten

Sie können die Einheiten auswählen, in denen die Werte angezeigt werden sollen. Wenn die ausgewählte Spalte beispielsweise die Rohkapazität anzeigt und die Werte in GiB angezeigt werden, Sie sie aber lieber als TiB anzeigen möchten, wählen Sie einfach TiB aus der Dropdown-Liste „Einheitenanzeige“ aus.

Aggregation

Wenn die angezeigten Werte aus den zugrunde liegenden Daten als „Durchschnitt“ aggregiert werden, Sie aber lieber die Summe aller Werte anzeigen möchten, wählen Sie „Summe“ entweder aus der Dropdown-Liste „Gruppieren nach“ (wenn Sie möchten, dass alle gruppierten Werte die Summen anzeigen) oder aus der Dropdown-Liste „Zeitaggregieren nach“ (wenn Sie möchten, dass die Zeilenwerte Summen der zugrunde liegenden Daten anzeigen).

Sie können gruppierte Datenpunkte nach *Durchschnitt*, *Maximum*, *Minimum* oder *Summe* aggregieren.

Sie können einzelne Zeilendaten nach *Durchschnitt*, *zuletzt erfasstem Datenpunkt*, *Maximum*, *Minimum* oder *Summe* aggregieren.

Bedingte Formatierung

Mit der bedingten Formatierung können Sie Schwellenwerte der Warn- und kritischen Stufen in der Liste der Abfrageergebnisse hervorheben, sodass Ausreißer und außergewöhnliche Datenpunkte sofort sichtbar werden.

143 items found

Table Row Grouping	Metrics & Attributes	
agent.node_diskio ↑	io_time (sec)	
nvme0n1	20,604.96	
nvme0n1	29,184.97	
nvme0n1	4,642.68	
nvme0n1	31,918.99	
nvme0n1	29,258.26	
nvme0n1	18,022.16	
nvme0n1	28,483.30	
nvme0n1	69,835.02	
nvme0n1	15,952.78	

> Aggregation

> Unit Display

Conditional Formatting [Reset](#)

If value is > (Greater than)

Warning 10000 sec

Critical 20000 sec

> Rename Column

Die bedingte Formatierung wird für jede Spalte separat festgelegt. Sie können beispielsweise einen Schwellenwertsatz für eine Kapazitätsspalte und einen anderen Satz für eine Durchsatzspalte auswählen.

Spalte umbenennen

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

Speichern

Nachdem Sie Ihre Abfrage so konfiguriert haben, dass die gewünschten Ergebnisse angezeigt werden, 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, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können **Ausdrücke** auch mit NOT oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten im Feld zu filtern.

kubernetes.pod X ▼

Filter By

pod_name

ingest ▼ X + ?

Group

pod_name X

Create wildcard containing "ingest"

ci-service-datalake-ingestion-85b5bdfd6d-2qbwr

service-foundation-ingest-767dfd5bfc-vxd5p

None

71 items found

Table Row Grouping

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

kubernetes.pod X ▼

Filter By

pod_name

ingest X

ci-service-audit-5f775dd975-brfdc X

X ▼ X + ?

Group

pod_name X

X ▼

3 items found

Table Row Grouping

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit Zahlen, Datumsangaben oder Booleschen Werten.

Filter verfeinern

Sie können Ihren Filter folgendermaßen verfeinern:

Filter	Was es bewirkt	Beispiel	Ergebnis
--------	----------------	----------	----------

* (Sternchen)	ermöglicht Ihnen die Suche nach allem	vol*rhel	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 12 -S12, BOS-PRD 23 -S12 usw. zurück
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten	FAS2240 ODER CX600 ODER FAS3270	gibt einen der folgenden Werte zurück: FAS2440, CX600 oder FAS3270
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen	NICHT EMV*	gibt alles zurück, was nicht mit "EMC" beginnt
<i>Keiner</i>	sucht in allen Feldern nach NULL-Werten	<i>Keiner</i>	gibt Ergebnisse zurück, bei denen das Zielfeld leer ist
Nicht *	sucht nach NULL-Werten in <i>Nur-Text</i> -Feldern	Nicht *	gibt Ergebnisse zurück, bei denen das Zielfeld leer ist

Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Filtern nach Booleschen Werten

Beim Filtern nach einem Booleschen Wert werden Ihnen möglicherweise die folgenden Filteroptionen angezeigt:

- **Beliebig:** Dies gibt *alle* Ergebnisse zurück, einschließlich der Ergebnisse, die auf „Ja“, „Nein“ oder gar nicht festgelegt sind.
- **Ja:** Gibt nur „Ja“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Ja“ als Häkchen anzeigt. Die Werte können auf „True“, „On“ usw. gesetzt werden; DII behandelt alle diese Werte als „Yes“.
- **Nein:** Gibt nur „Nein“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Nein“ als „X“ anzeigt. Die Werte können auf „Falsch“, „Aus“ usw. gesetzt werden; DII behandelt alle diese Werte als „Nein“.
- **Keine:** Gibt nur Ergebnisse zurück, bei denen der Wert überhaupt nicht festgelegt wurde. Auch als „Null“-Werte bezeichnet.

Was mache ich jetzt, da ich Abfrageergebnisse habe?

Durch Abfragen können auf einfache Weise Anmerkungen hinzugefügt oder Anwendungen Assets zugewiesen werden. Beachten Sie, dass Sie Ihren Inventarressourcen (Festplatte, Speicher usw.) nur Anwendungen oder Anmerkungen zuweisen können. Integrationsmetriken können keine Anmerkungen oder Anwendungszuweisungen übernehmen.

Um den aus Ihrer Abfrage resultierenden Assets eine Anmerkung oder Anwendung zuzuweisen, wählen Sie

einfach das/die Asset(s) mithilfe der Kontrollkästchenspalte links in der Ergebnistabelle aus und klicken Sie dann rechts auf die Schaltfläche **Massenaktionen**. Wählen Sie die gewünschte Aktion aus, die auf die ausgewählten Assets angewendet werden soll.

Volume X

Filter By Name Any X +

Query Results (5) | 2 Selected

Bulk Actions

Add Annotation
Remove Annotation
Add Application
Remove Application
US:windows_zu08

<input type="checkbox"/>	Name ↑	Storage Pools	Capacity - Raw (GB)	Mapped Ports
<input type="checkbox"/>	DmoESX_optimus:mc_Dm...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/>	DmoSAN_optimus:hoffma...	optimus-02:aggr1_optimu...	N/A	
<input checked="" type="checkbox"/>	DmoSAN_optimus:mc_D...	optimus-02:aggr1_optimu...	N/A	
<input type="checkbox"/>	oci-3070-01:/vol/vfiler_lun...	oci-3070-01:aggr5	N/A	OS:windows
<input type="checkbox"/>	spectravs1:sjimmyscsi:/v...	ocinaneqa1-01:spectraaggr1	N/A	OS:linux

Anmerksungsregeln erfordern eine Abfrage

Wenn Sie konfigurieren "[Anmerksungsregeln](#)", jeder Regel muss eine zugrunde liegende Abfrage zugrunde liegen, mit der gearbeitet werden kann. Aber wie Sie oben gesehen haben, können Abfragen so weit oder so eng gefasst werden, wie Sie es benötigen.

Anzeigen von Abfragen

Sie können Ihre Abfragen anzeigen, um Ihre Vermögenswerte zu überwachen und die Anzeige der mit Ihren Vermögenswerten verbundenen Daten in Ihren Abfragen zu ändern.

Schritte

1. Melden Sie sich bei Ihrem Data Infrastructure Insights Mandanten an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Abfragen anzeigen**. Sie können die Anzeige von Abfragen wie folgt ändern:
3. Sie können Text in das Filterfeld eingeben, um nach bestimmten Abfragen zu suchen.
4. Sie können die Sortierreihenfolge der Spalten in der Abfragetabelle entweder aufsteigend (Pfeil nach oben) oder absteigend (Pfeil nach unten) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken.
5. Um die Größe einer Spalte zu ändern, bewegen Sie die Maus über die Spaltenüberschrift, bis ein blauer Balken angezeigt wird. Platzieren Sie die Maus über der 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 Durchblättern der Abfrageergebnisse, dass sich die Ergebnisse ändern können, da Data Infrastructure Insights Ihre Datensammler automatisch abfragt. Dies kann dazu führen, dass einige Elemente fehlen oder einige Elemente je nach Sortierung in der falschen Reihenfolge angezeigt werden.

Exportieren von Abfrageergebnissen in eine CSV-Datei

Sie können die Ergebnisse jeder Abfrage in eine CSV-Datei exportieren, sodass Sie die Daten analysieren oder in eine andere Anwendung importieren können.

Schritte

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

Die Seite „Abfragen“ wird angezeigt.

3. Klicken Sie auf eine Abfrage.
4. Klicken Sie  um die Abfrageergebnisse in eine CSV-Datei zu exportieren.

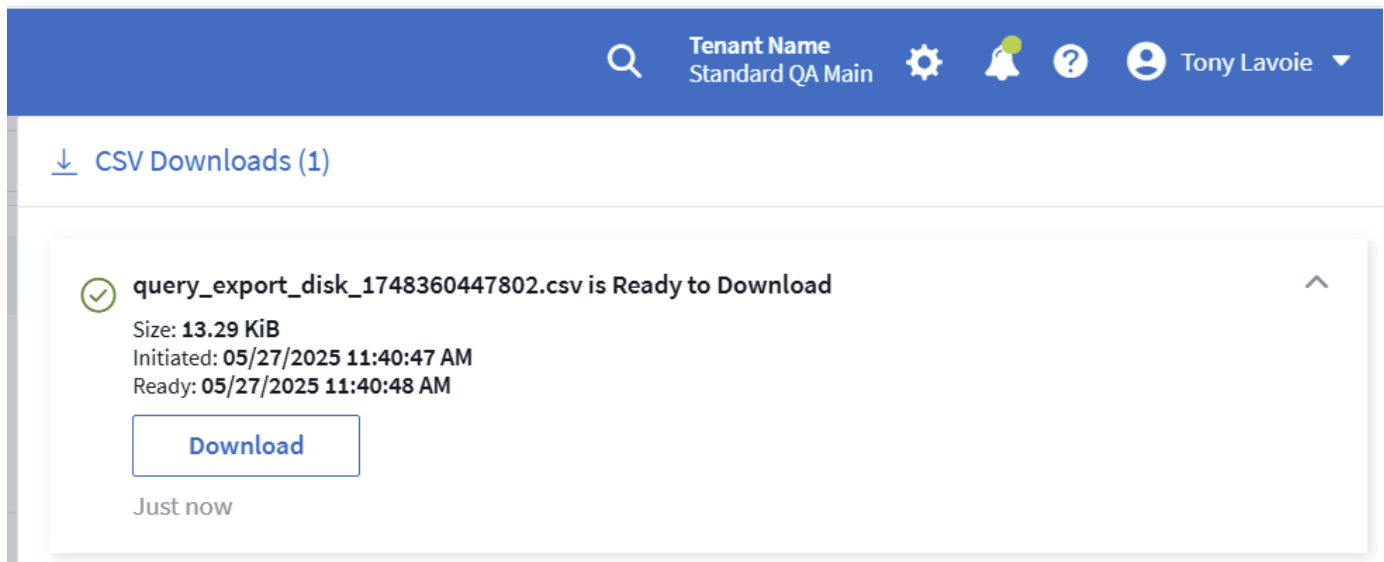


Der Export in .CSV ist auch im Menü „Drei Punkte“ in Dashboard-Tabellen-Widgets sowie in den meisten Landingpage-Tabellen verfügbar.

Asynchroner Export

Das Exportieren von Daten in das CSV-Format kann je nach der zu exportierenden Datenmenge zwischen einigen Sekunden und mehreren Stunden dauern. Data Infrastructure Insights exportiert diese Daten asynchron, sodass Sie weiterarbeiten können, während die CSV-Datei kompiliert wird.

Zeigen Sie Ihre CSV-Exporte an und laden Sie sie herunter, indem Sie in der oberen rechten Symbolleiste das Glockensymbol auswählen.



The screenshot shows the top navigation bar of Data Infrastructure Insights with a search icon, tenant name 'Standard QA Main', settings, notifications, help, and user profile 'Tony Lavoie'. Below the bar, a section titled 'CSV Downloads (1)' contains a notification card. The card has a green checkmark icon and the text 'query_export_disk_1748360447802.csv is Ready to Download'. It also displays the file size '13.29 KiB', the initiation time '05/27/2025 11:40:47 AM', and the ready time '05/27/2025 11:40:48 AM'. A 'Download' button is present, and the text 'Just now' is at the bottom of the card.

Die exportierten Daten spiegeln die aktuelle Filterung, die angezeigten Spalten und Spaltennamen wider.

Kommas in Asset-Namen

Hinweis: Wenn in einem Asset-Namen ein Komma erscheint, wird der Name beim Export in Anführungszeichen gesetzt, wodurch der Asset-Name und das richtige CSV-Format erhalten bleiben.

Zeitformat oder kein Zeitformat?

Wenn Sie eine exportierte CSV-Datei mit Excel öffnen und ein Objektname oder ein anderes Feld im Format NN:NN (zwei Ziffern gefolgt von einem Doppelpunkt und zwei weiteren Ziffern) vorliegt, interpretiert Excel diesen Namen manchmal als Zeitformat statt als Textformat. Dies kann dazu führen, dass Excel in diesen Spalten falsche Werte anzeigt. Beispielsweise würde ein Objekt mit dem Namen „81:45“ in Excel als „81:45:00“ angezeigt.

Um dieses Problem zu umgehen, importieren Sie die CSV-Datei mit den folgenden Schritten in Excel:

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 „Getrennt“ und klicken Sie auf „Weiter“.
5. Wählen Sie „Komma“ als Trennzeichen und klicken Sie auf „Weiter“.
6. Wählen Sie die gewünschten Spalten aus und wählen Sie „Text“ als Spaltendatenformat.
7. Klicken Sie auf Fertig stellen.

Ihre Objekte sollten in Excel im richtigen Format angezeigt werden.

Ändern oder Löschen einer Abfrage

Sie können die mit einer Abfrage verknüpften Kriterien ändern, wenn Sie die Suchkriterien für die abgefragten Assets ändern möchten.

Ändern einer Abfrage

Schritte

1. Klicken Sie auf **Erkunden** und wählen Sie **Alle Metrikabfragen** aus.

Die Seite „Abfragen“ wird angezeigt.

2. Klicken Sie auf den Abfragenamen
3. Um der Abfrage ein Kriterium hinzuzufügen, klicken Sie auf das Spaltensymbol und wählen Sie eine Metrik oder ein Attribut aus der Liste aus.

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

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

Löschen einer Abfrage

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

1. Klicken Sie auf das Drei-Punkte-Menü rechts neben der Abfrage und klicken Sie auf **Löschen**.
2. Klicken Sie auf den Abfragenamen und wählen Sie **Löschen** aus dem Dropdown-Menü **Speichern**.

Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen von Assets

Sie können mehrere "**Anwendungen**" Sie können mehrere Anwendungen mithilfe einer Abfrage zu Assets hinzufügen oder daraus entfernen, anstatt sie manuell zuweisen oder entfernen zu müssen.



Mit diesen Schritten können Sie hinzufügen oder entfernen "**Anmerkungen**" auf die gleiche Weise.

Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets findet, die Sie bearbeiten möchten.

Schritte

1. Klicken Sie auf **Erkunden** und wählen Sie **Metrikabfragen** aus.

Die Seite „Abfragen“ wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets findet.

Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus oder klicken Sie auf das obere Kontrollkästchen, um „Alle“ auszuwählen.

Das Dropdown-Menü „Massenaktionen“ wird angezeigt.

4. Um den ausgewählten Assets eine Anwendung hinzuzufügen, klicken Sie auf Massenaktionen und wählen Sie **Anwendung hinzufügen**.

5. Wählen Sie eine oder mehrere Anwendungen aus.

Sie können mehrere Anwendungen für Hosts, interne Volumes, Qtrees und virtuelle Maschinen auswählen. Für ein Volume oder eine Freigabe können Sie jedoch nur eine Anwendung auswählen.

6. Klicken Sie auf **Speichern**.

7. Um eine den Assets zugewiesene Anwendung zu entfernen, klicken Sie auf „Massenaktionen“ und wählen Sie „Anwendung entfernen“ aus.

8. Wählen Sie die Anwendung(en) aus, die Sie entfernen möchten.

9. Klicken Sie auf **Löschen**.

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

Anwendung.

Nachdem Sie bei einer Massenhinzufügungsaktion auf *Speichern* oder bei einer Massenlöschaktion auf *Entfernen* geklickt haben, werden Sie von Data Infrastructure Insights darüber informiert, dass die Aktion einige Zeit in Anspruch nehmen wird. Sie können diese Meldung ignorieren; die Aktion wird im Hintergrund fortgesetzt.



In Umgebungen mit einer großen Menge verwandter Assets kann die Vererbung von Anwendungszuweisungen zu diesen Assets mehrere Minuten dauern. Bitte rechnen Sie mit einer längeren Vererbungszeit, wenn Sie über viele zusammenhängende Vermögenswerte verfügen.

Tabellenwerte kopieren

Sie können Werte in Tabellen in die Zwischenablage kopieren, um sie in Suchfeldern oder anderen Anwendungen zu verwenden.

Informationen zu diesem Vorgang

Es gibt zwei Methoden, mit denen Sie Werte aus Tabellen oder Abfrageergebnissen in die Zwischenablage kopieren 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 bei Einzelwertfeldern den Mauszeiger über das Feld und klicken Sie auf das angezeigte Zwischenablatesymbol. Der Wert wird zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopiert.

Beachten Sie, dass mit dieser Methode nur Werte kopiert werden können, die Links zu Assets sind. Nur Felder, die einzelne Werte enthalten (also keine Listen sind), verfügen über das Kopiersymbol.

Protokoll-Explorer

Der Data Infrastructure Insights Log Explorer ist ein leistungsstarkes Tool zum Abfragen von Systemprotokollen. Zusätzlich zur Unterstützung bei Untersuchungen können Sie auch eine Protokollabfrage in einem Monitor speichern, um Warnungen bereitzustellen, wenn diese bestimmten Protokollauslöser aktiviert werden.

Um mit der Untersuchung der Protokolle zu beginnen, klicken Sie auf **Protokollabfragen > +Neue Protokollabfrage**.

Wählen Sie ein verfügbares Protokoll aus der Liste aus.

Select...

logs.kubernetes

logs.kubernetes.events

logs.netapp.ems

logs.ontapems

logs.syslog



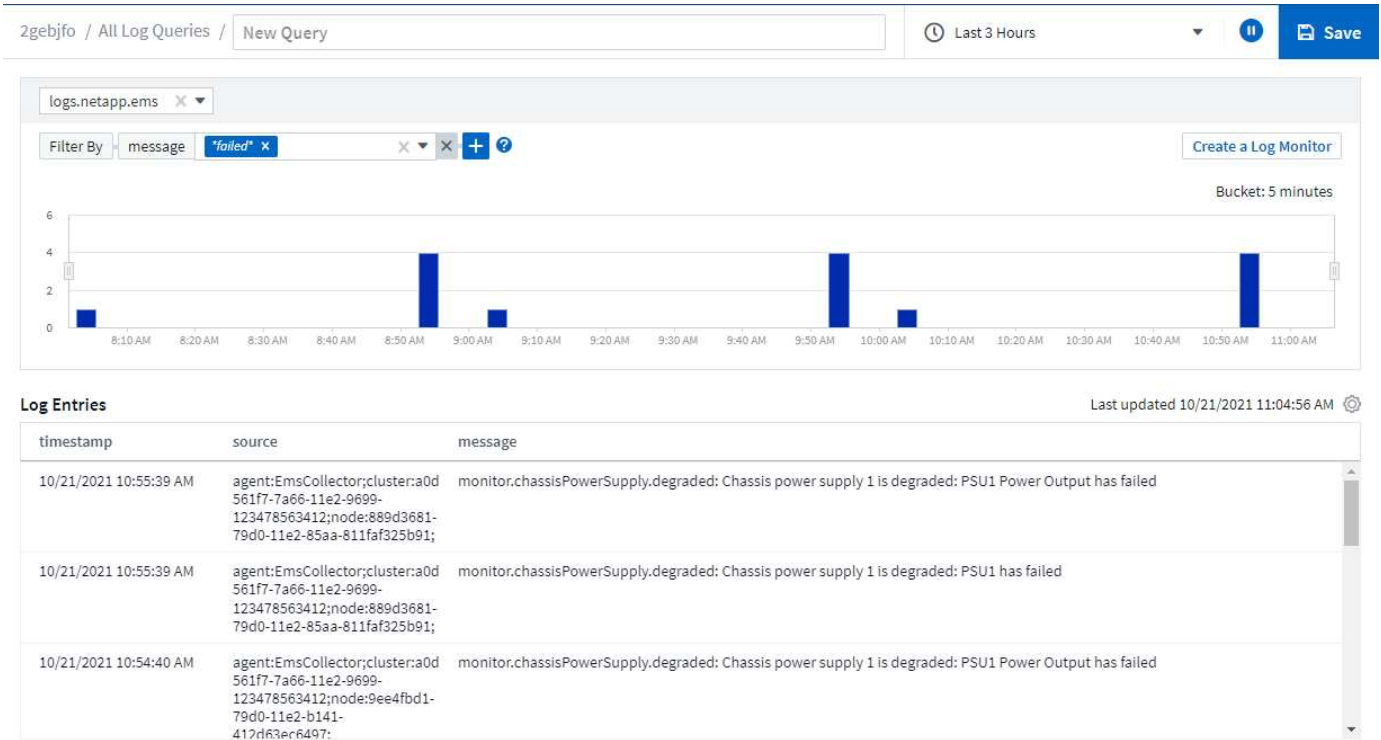
Die für die Abfrage verfügbaren Protokolltypen können je nach Umgebung variieren. Im Laufe der Zeit können weitere Protokolltypen hinzugefügt werden.

Sie können Filter setzen, um die Ergebnisse der Abfrage weiter zu verfeinern. Um beispielsweise alle Protokollmeldungen zu finden, die einen Fehler anzeigen, legen Sie einen Filter für *Meldungen* fest, die das Wort „fehlgeschlagen“ enthalten.



Sie können mit der Eingabe des gewünschten Textes in das Filterfeld beginnen. Data Infrastructure Insights fordert Sie während der Eingabe auf, eine Platzhaltersuche mit der Zeichenfolge zu erstellen.

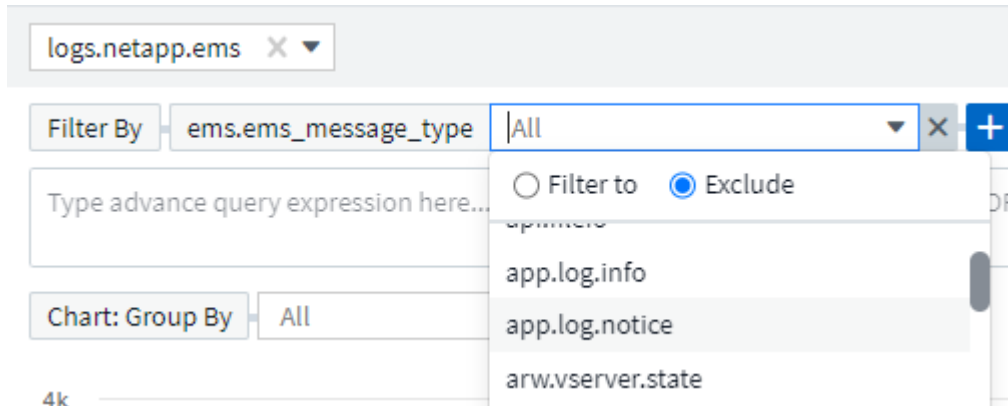
Die Ergebnisse werden in einem Diagramm angezeigt, das die Anzahl der Protokollinstanzen in jedem angezeigten Zeitraum zeigt. Unter dem Diagramm befinden sich die Protokolleinträge selbst. Das Diagramm und die Einträge werden basierend auf dem ausgewählten Zeitraum automatisch aktualisiert.



Filtern

Einschließen / Ausschließen

Beim Filtern der Protokolle können Sie wählen, ob Sie die eingegebenen Zeichenfolgen **einschließen** (d. h. „Filtern nach“) oder **ausschließen** möchten. Ausgeschlossene Zeichenfolgen werden im vervollständigten Filter als „NOT <string>“ angezeigt.



Filter, die auf Platzhaltern oder Ausdrücken basieren (z. B. NICHT, ODER, „Keine“ usw.), werden 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.

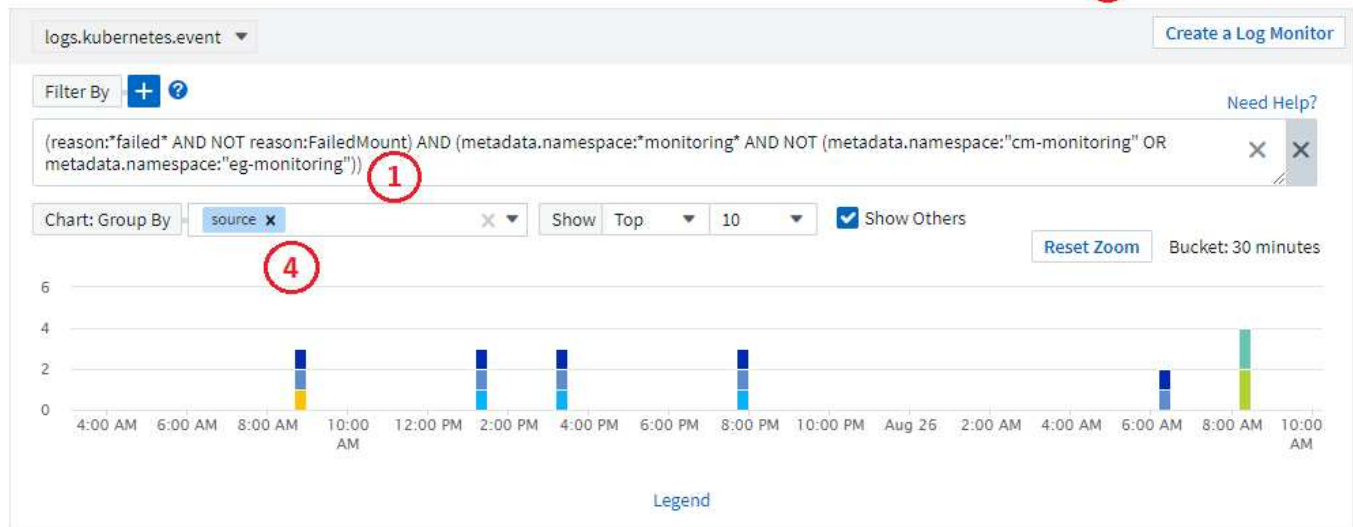
Erweiterte Filterung

Wenn Sie in Abfragen oder Dashboard-Widgets nach Text oder Listenwerten filtern, wird Ihnen beim Eintippen die Option angezeigt, einen **Platzhalterfilter** basierend auf dem aktuellen Text zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse zurückgegeben, die mit dem Platzhalterausdruck übereinstimmen. Sie können auch Ausdrücke mit NOT, AND oder OR erstellen oder die Option „Keine“ auswählen, um nach Nullwerten zu filtern.



Denken Sie daran, Ihre Abfrage frühzeitig und häufig zu speichern, während Sie Ihre Filterung erstellen. Bei der erweiterten Abfrage handelt es sich um eine Zeichenfolgengabe in „freier Form“, und beim Erstellen können Analysefehler auftreten.

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



Log Entries

Last updated 08/30/2023 9:54:13 AM

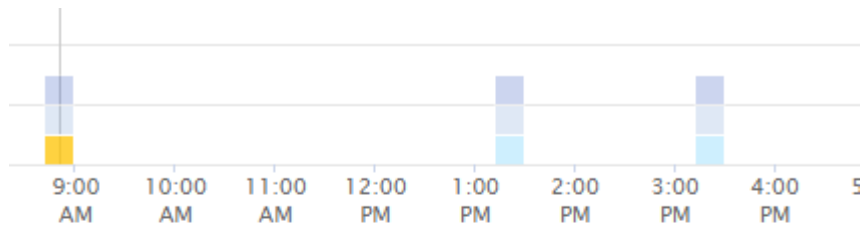
timestamp	source	message	metadata.namespace ↑	reason
08/26/2023 8:40:28 AM	kubernetes_cluster:reg-stream;namespace:33994-monitoring;pod_name:event-exporter-5db67db995-bxmkk;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:28 AM	kubernetes_cluster:reg-stream;namespace:ph-monitoring;pod_name:event-exporter-c4446976c-jxrdc;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:29 AM	kubernetes_cluster:reg-	Error: failed to reserve	k3s-cm-monitoring	Failed

1. Diese erweiterte Abfragezeichenfolge filtert nach Folgendem:

- Filtern Sie nach Protokolleinträgen mit einem *Grund*, der das Wort „fehlgeschlagen“ enthält, aber nicht nach Einträgen mit dem spezifischen Grund „FailedMount“.
- Schließen Sie alle Einträge ein, die auch einen *metadata.namespace* mit dem Wort „monitoring“ enthalten, schließen Sie jedoch die spezifischen Namespaces „cm-monitoring“ oder „eg-monitoring“ aus.

Beachten Sie, dass im obigen Fall sowohl „cm-monitoring“ als auch „eg-monitoring“ einen Bindestrich („-“) enthalten. Daher müssen die Zeichenfolgen in Anführungszeichen gesetzt werden, da sonst ein Analysefehler angezeigt wird. Zeichenfolgen, die keine Bindestriche, Leerzeichen usw. enthalten, müssen nicht in Anführungszeichen gesetzt werden. Versuchen Sie im Zweifelsfall, die Zeichenfolge in Anführungszeichen zu setzen.

- 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 zusätzliche Spalten anzuzeigen, wählen Sie das Zahnradsymbol aus.
- Das Diagramm wurde vergrößert, um nur Protokollergebnisse anzuzeigen, die innerhalb eines bestimmten Zeitrahmens aufgetreten sind. Der hier angezeigte Zeitbereich spiegelt die aktuelle Zoomstufe wider. Wählen Sie die Schaltfläche *Zoom zurücksetzen*, um die Zoomstufe wieder auf den aktuellen Data Infrastructure Insights -Zeitbereich zurückzusetzen.
- Die Diagrammergebnisse wurden nach dem Feld *Quelle* gruppiert. Das Diagramm zeigt die Ergebnisse in jeder Spalte, gruppiert nach Farben. Wenn Sie mit der Maus über eine Spalte im Diagramm fahren, werden einige Details zu den jeweiligen Einträgen angezeigt.



Friday 08/25/2023 08:51:00 AM			
■	kubernetes_cluster:vanilla25;namespace:docker-monitoring;pod_name:event-exporter-7d468bbf5b-8bzqt;	1	33.33%
■	kubernetes_cluster:vanilla25;namespace:eg-monitoring;pod_name:event-exporter-7c4cb666d6-xd9mb;	1	33.33%
■	kubernetes_cluster:vanilla25;namespace:oc-k3s-monitoring;pod_name:event-exporter-99d5fcfd8-lbg99;	1	33.33%
Total		3	

Filter verfeinern

Sie können Ihren Filter folgendermaßen verfeinern:

Filter	Was es bewirkt
* (Sternchen)	ermöglicht Ihnen die Suche nach allem
? (Fragezeichen)	ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen
<i>Keiner</i>	sucht in allen Feldern nach NULL-Werten
Nicht *	sucht nach NULL-Werten in <i>Nur-Text</i> -Feldern

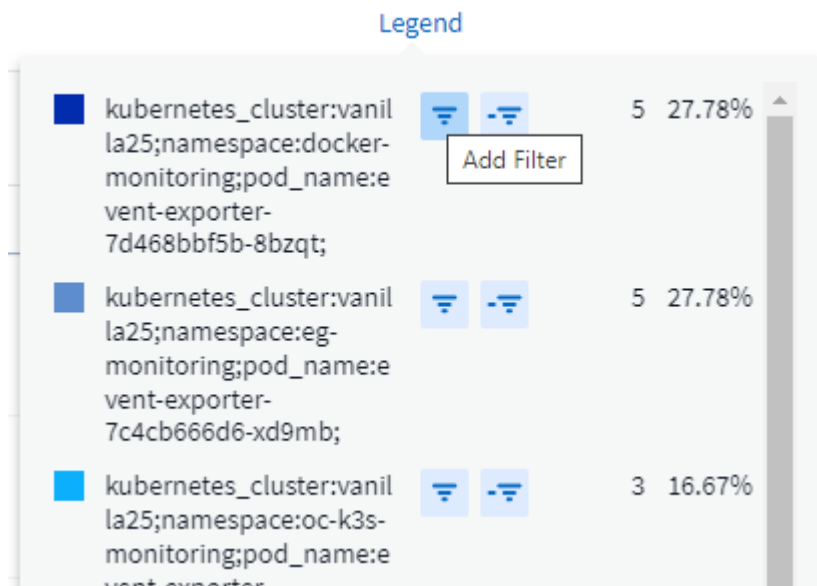
Wenn Sie eine Filterzeichenfolge in doppelte Anführungszeichen setzen, behandelt Insight alles zwischen dem ersten und letzten Anführungszeichen als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren innerhalb der Anführungszeichen werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, werden Ergebnisse zurückgegeben, die ein Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelte Anführungszeichen eingeschlossen sind.

Sie können einen einfachen Filter mit einem erweiterten Abfragefilter kombinieren. Der resultierende Filter ist ein „UND“ der beiden.

Die Chart-Legende

Auch die *Legende* unter dem Diagramm hält einige Überraschungen bereit. 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 alle Ergebnisse anzuzeigen, die NICHT für diese Zeile gelten (Ausschlussfilter hinzufügen). Das Diagramm und die Liste der Protokolleinträge werden aktualisiert, um die Ergebnisse basierend auf Ihrer Auswahl anzuzeigen. Um diese Filterung zu entfernen, öffnen Sie die Legende erneut und wählen Sie das [X] aus, um den legendenbasierten Filter zu löschen.



Protokolldetails

Wenn Sie irgendwo in der Liste auf einen Protokolleintrag klicken, wird ein Detailbereich für diesen Eintrag geöffnet. Hier können Sie weitere Informationen zur Veranstaltung finden.

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

Beachten Sie, dass einige Felder nicht als Filter hinzugefügt werden können. In diesen Fällen ist das Symbol „Filter hinzufügen“ nicht verfügbar.

Log Details

×

timestamp

09/20/2021 9:03:36 PM

message

2021-09-20T15:33:36Z E! [processors.execd] stderr: "Total time to process mountstats file: /hostfs/proc/1/mountstats, was: 0s"

id: 227814532095936770

node_name: ci-auto-dsacq-insights-1.cloudinsights-dev.netapp.com

Add Filter

source: telegraf-ds-dfcc5

type: logs.kubernetes

[-] kubernetes

kubernetes.annotations.openshift.io_scc:

telegraf-hostaccess

kubernetes.container_hash:

ci-registry.nane.openenglab.netapp.com:8077/telegraf@sha256:00b45a7cc0761c

Fehlerbehebung

Hier finden Sie Vorschläge zur Behebung von Problemen mit Protokollabfragen.

Problem:	Versuchen Sie Folgendes:
Ich sehe keine „Debug“-Meldungen in meiner Protokollabfrage	Debug-Protokollnachrichten werden nicht erfasst. Um die gewünschten Nachrichten zu erfassen, ändern Sie den Schweregrad der entsprechenden Nachricht auf die Ebene „Information“, „Fehler“, „Alarm“, „Notfall“ oder „Hinweis“.

Identifizieren inaktiver Geräte

Um die richtige Größe zu finden und ungenutzte Infrastruktur freizugeben, ist es entscheidend, die vorhandenen Ressourcen und deren Nutzer zu identifizieren. Sie können nicht ausgelastete Ressourcen problemlos neu zuweisen oder außer Betrieb nehmen und unnötige Käufe vermeiden.

Führen Sie die folgenden Schritte aus, um inaktive Assets zu identifizieren.

Schritte

- Navigieren Sie zu **Observability > Explore** → **+Neue Metrikabfrage**.
- Wählen Sie *Speicher* aus der Dropdown-Liste.
- Klicken Sie auf das Zahnrad und fügen Sie *isActive* als Spalte hinzu.

Zeilen mit einem Häkchen sind aktiv. „X“ zeigt inaktive Geräte an.

Um inaktive Geräte zu entfernen, wählen Sie einfach die zu entfernenden Geräte aus und wählen Sie im Dropdown-Menü **Massenaktionen** die Option *Inaktive Geräte löschen*.

Einblicke

Einblicke

Mithilfe von Insights können Sie beispielsweise die Ressourcennutzung und ihre Auswirkungen auf andere Ressourcen untersuchen oder die Zeit bis zur Fertigstellung analysieren.

Es stehen zahlreiche Einblicke zur Verfügung. Navigieren Sie zu **Dashboards > Insights**, um einzutauchen. Sie können aktive Insights (aktuell auftretende Insights) auf der Hauptregisterkarte oder inaktive Insights auf der Registerkarte *Inaktive Insights* anzeigen. Inaktive Erkenntnisse sind Erkenntnisse, die zuvor aktiv waren, aber nicht mehr auftreten.

Erkenntnistypen

Gemeinsam genutzte Ressourcen unter Stress

Workloads mit hoher Auswirkung können die Leistung anderer Workloads in einer gemeinsam genutzten Ressource beeinträchtigen. Dadurch wird die gemeinsam genutzte Ressource belastet. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und die Auswirkungen auf Ihren Mandanten untersuchen können. ["Weitere Informationen"](#)

Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz

Die Einblicke in „Kubernetes-Namespaces, denen der Speicherplatz ausgeht“ geben Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass ihnen der Speicherplatz ausgeht, und enthalten eine Schätzung der verbleibenden Tage, bis jeder Speicherplatz voll ist. ["Weitere Informationen"](#)

ONTAP Cold Storage zurückgewinnen

Der *Reclaim ONTAP Cold Storage* Insight bietet Daten zur Kalkapazität, zu potenziellen Kosten-/Stromeinsparungen und empfohlenen Aktionselementen für Volumes auf ONTAP Systemen. ["Weitere Informationen"](#)



Dies ist eine *Vorschau*-Funktion und kann sich im Laufe der Zeit ändern, wenn Verbesserungen vorgenommen werden. ["Mehr erfahren"](#) Informationen zu den Vorschaufunktionen von Data Infrastructure Insights .

Einblicke: Gemeinsam genutzte Ressourcen unter Druck

Workloads mit hoher Auswirkung können die Leistung anderer Workloads in einer

gemeinsam genutzten Ressource beeinträchtigen. Dadurch wird die gemeinsam genutzte Ressource belastet. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und die Auswirkungen auf Ihren Mandanten untersuchen können.

Terminologie

Wenn es um Arbeitsbelastung oder Ressourcenauswirkungen geht, sind die folgenden Definitionen hilfreich.

Eine **anspruchsvolle Arbeitslast** ist eine Arbeitslast, die sich derzeit auf andere Ressourcen im gemeinsam genutzten Speicherpool auswirkt. Diese Workloads führen beispielsweise zu höheren IOPS und reduzieren so die IOPS in den betroffenen Workloads. Anspruchsvolle Arbeitslasten werden manchmal als *arbeitsintensive Arbeitslasten* bezeichnet.

Eine **betroffene Arbeitslast** ist eine Arbeitslast, die von einer Arbeitslast mit hohem Verbrauch im gemeinsam genutzten Speicherpool betroffen ist. Bei diesen Workloads kommt es aufgrund der anspruchsvollen Workloads zu reduzierten IOPS und/oder einer höheren Latenz.

Beachten Sie: Wenn Data Infrastructure Insights die führende Rechenarbeitslast nicht ermittelt hat, wird das Volume oder das interne Volume selbst als Arbeitslast erkannt. Dies gilt sowohl für anspruchsvolle als auch für beeinträchtigte Arbeitslasten.

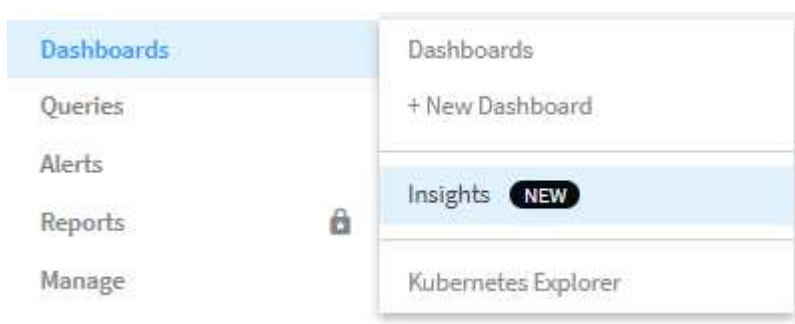
Shared Resource Saturation ist das Verhältnis der beeinflussenden IOPS zum *Basiswert*.

Baseline wird als der maximal gemeldete Datenpunkt für jede Arbeitslast in der Stunde unmittelbar vor der erkannten Sättigung definiert.

Eine **Konfliktsituation** oder **Sättigung** tritt auf, wenn festgestellt wird, dass IOPS andere Ressourcen oder Arbeitslasten im gemeinsam genutzten Speicherpool beeinträchtigen.

Anspruchsvolle Arbeitslasten

Um anspruchsvolle und beeinträchtigte Arbeitslasten in Ihren gemeinsam genutzten Ressourcen zu untersuchen, klicken Sie auf **Dashboards > Einblicke** und wählen Sie den Einblick **Gemeinsam genutzte Ressourcen unter Stress** aus.



Data Infrastructure Insights zeigt eine Liste aller Workloads an, bei denen eine Sättigung erkannt wurde. Beachten Sie, dass Data Infrastructure Insights Workloads anzeigt, bei denen mindestens eine *anspruchsvolle Ressource* **oder** *beeinträchtigte Ressource* erkannt wurde.

Klicken Sie auf eine Arbeitslast, um die Detailseite dazu anzuzeigen. Das obere Diagramm zeigt die Aktivität auf der gemeinsam genutzten Ressource (z. B. einem Speicherpool), auf der die Konflikte/Sättigungen auftreten.



Shared resource sp-444 was under stress

The IOPS of 1 workload had saturated the shared resource **sp-444** and were impacting the performance of 1 other workload.

69%
Shared Resource
Utilization

1
Demanding
Workloads

1
Impacted
Workloads

Shared Resource sp-444 ⓘ

Utilization (%)



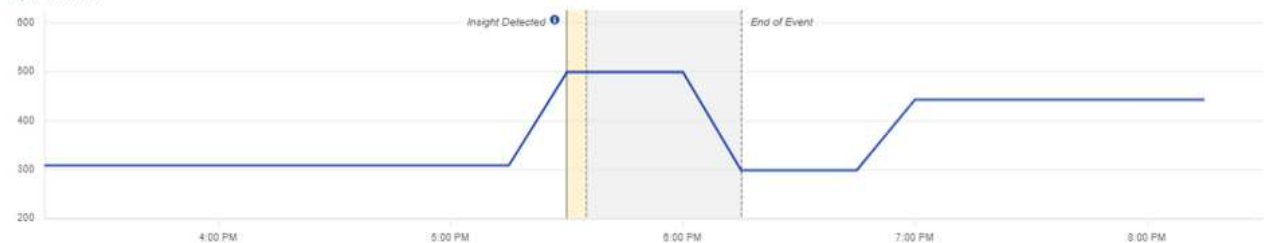
Darunter befinden sich zwei Diagramme, die die *anspruchsvollen* Arbeitslasten und die Arbeitslasten zeigen, die von diesen anspruchsvollen Arbeitslasten *beeinflusst* werden.

Demanding Workloads (1) ⓘ

Potentially impacted the shared resource and other related workloads

Contributing IOPS

lops.total (IOPS)



Workload	Current Contributing IOPS (IOPS) ↓	Change Since Detection (IOPS)
 internal-volume-331	500.00	+190.00

Impacted Workloads (1) ⓘ

Impacted by changed workloads on the shared resource

Latency

latency.total (ms)



Workload	Current Latency (ms) ↓	Change Since Detection (ms)
 internal-volume-332	200.00	+110.00

Unter jeder Tabelle befindet sich eine Liste der Arbeitslasten und/oder Ressourcen, die den Konflikt beeinflussen oder davon betroffen sind. Wenn Sie auf eine Ressource (z. B. eine VM) klicken, wird eine Detailseite für diese Ressource geöffnet. Durch Klicken auf eine Arbeitslast wird eine Abfrageseite geöffnet, auf der die beteiligten Pods angezeigt werden. Beachten Sie: Wenn der Link eine leere Abfrage öffnet, kann dies daran liegen, dass der betroffene Pod nicht mehr Teil der aktiven Konkurrenz ist. Sie können den Zeitbereich der Abfrage ändern, um die Pod-Liste in einem größeren oder fokussierteren Zeitbereich anzuzeigen.

Was kann ich tun, um die Sättigung zu beheben?

Sie können eine Reihe von Schritten unternehmen, um die Gefahr einer Überlastung Ihres Mieters zu verringern oder auszuschließen. Diese werden durch Erweitern des Links **+Empfehlungen anzeigen** auf der Seite angezeigt. Hier sind ein paar Dinge, die Sie ausprobieren können.

- Verschieben von Verbrauchern mit hohem IOPS-Aufkommen

Verschieben Sie die „gierigen“ Workloads in weniger gesättigte Speicherpools. Es wird empfohlen, die Ebene und Kapazität dieser Pools zu bewerten, bevor Sie die Workloads verschieben, um unnötige Kosten oder zusätzliche Konflikte zu vermeiden.

- Implementieren Sie eine Quality of Service (QoS)-Richtlinie

Durch die Implementierung einer QoS-Richtlinie pro Arbeitslast, um sicherzustellen, dass genügend freie Ressourcen verfügbar sind, wird die Sättigung des Speicherpools verringert. Dies ist eine langfristige Lösung.

- Hinzufügen zusätzlicher Ressourcen

Wenn die gemeinsam genutzte Ressource (z. B. der Speicherpool) den IOPS-Sättigungspunkt erreicht hat, können Sie durch Hinzufügen weiterer oder schnellerer Festplatten zum Pool sicherstellen, dass genügend freie Ressourcen zur Verfügung stehen, um die Sättigung zu verringern.

Abschließend können Sie auf **Insight-Link kopieren** klicken, um die Seiten-URL in die Zwischenablage zu kopieren und sie einfacher mit Kollegen zu teilen.

Einblicke: Kubernetes-Namespaces haben nicht mehr genügend Speicherplatz

Es ist nie eine gute Situation, wenn auf Ihrem Mandanten der Speicherplatz ausgeht. Mithilfe von Data Infrastructure Insights können Sie vorhersagen, wie viel Zeit Ihnen bleibt, bevor die persistenten Kubernetes-Volumes voll sind.

Der Einblick „Kubernetes-Namespaces laufen Gefahr, nicht mehr genügend Speicherplatz zu haben“ bietet Ihnen einen Überblick über die Workloads in Ihren Kubernetes-Namespaces, bei denen das Risiko besteht, dass der Speicherplatz knapp wird, und enthält eine Schätzung der verbleibenden Tage, bis jedes persistente Volume voll ist.

Sie können diesen Insight anzeigen, indem Sie zu **Dashboards > Insights** 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 eine Arbeitslast, um eine Detailseite für den Insight zu öffnen. Auf dieser Seite sehen Sie ein Diagramm mit den Trends der Arbeitslastkapazität sowie eine Tabelle mit den folgenden Informationen:

- Name der Arbeitslast
- Betroffen ist das dauerhafte Volume
- Voraussichtliche Zeit bis zur Fertigstellung in Tagen
- Persistente Volume-Kapazität
- Betroffen ist die Back-End-Speicherressource, wobei die aktuelle Kapazität im Vergleich zur Gesamtkapazität genutzt wird. Durch Klicken auf diesen Link wird die detaillierte Zielseite für das Backend-Volume geöffnet.

Workloads at risk (2)

Workloads	Persistent Volume (pvClaim)	Time to Full (Days) ↓	Persistent 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 Speicherplatz ausgeht?

Klicken Sie auf der Insight-Seite auf **+Empfehlungen anzeigen**, um mögliche Lösungen anzuzeigen. Die einfachste Option bei Speicherplatzmangel besteht immer darin, mehr Kapazität hinzuzufügen. Data Infrastructure Insights zeigt Ihnen die optimale Kapazität an, die Sie hinzufügen müssen, um die Zeit bis zur vollständigen Belegung auf eine Zielvorgabe von 60 Tagen zu erhöhen. Darüber hinaus werden auch andere Empfehlungen angezeigt.

Show Recommendations

1
Get time to full back up to 60 days by adding more capacity to backend resources
Add to the following resources to bring time-to-full up to ideal capacity.

Backend Resource ↓	Current Capacity (time to full)	Recommended Capacity to Add	Ideal Capacity (time to full)
internal-volume-601	2.00 GiB 1 Days	+ 518.79 GiB	= 520.79 GiB 60 Days

2
Use NetApp Astra Trident with your K8s to automatically grow capacity
Astra Trident can keep your capacity lean without risk of running out of space.

[Learn more about Astra Trident](#)

[Copy Insight Link](#)

Hier können Sie auch bequem einen Link zu diesem Insight kopieren, die Seite mit einem Lesezeichen versehen oder sie einfach mit Ihrem Team teilen.

Einblicke: ONTAP Cold Storage zurückgewinnen

Der *Reclaim ONTAP Cold Storage* Insight bietet Daten zur Kalkapazität, zu potenziellen Kosten-/Stromeinsparungen und empfohlenen Aktionselementen für Volumes auf ONTAP Systemen.

Um diese Insights anzuzeigen, navigieren Sie zu **Dashboards > Insights** und werfen Sie einen Blick auf den Insight „Reclaim ONTAP Cold Storage“. Beachten Sie, dass dieser Insight betroffene Speicher nur auflistet, wenn Data Infrastructure Insights Cold Storage erkannt hat. Andernfalls wird die Meldung „Entwarnung“

angezeigt.

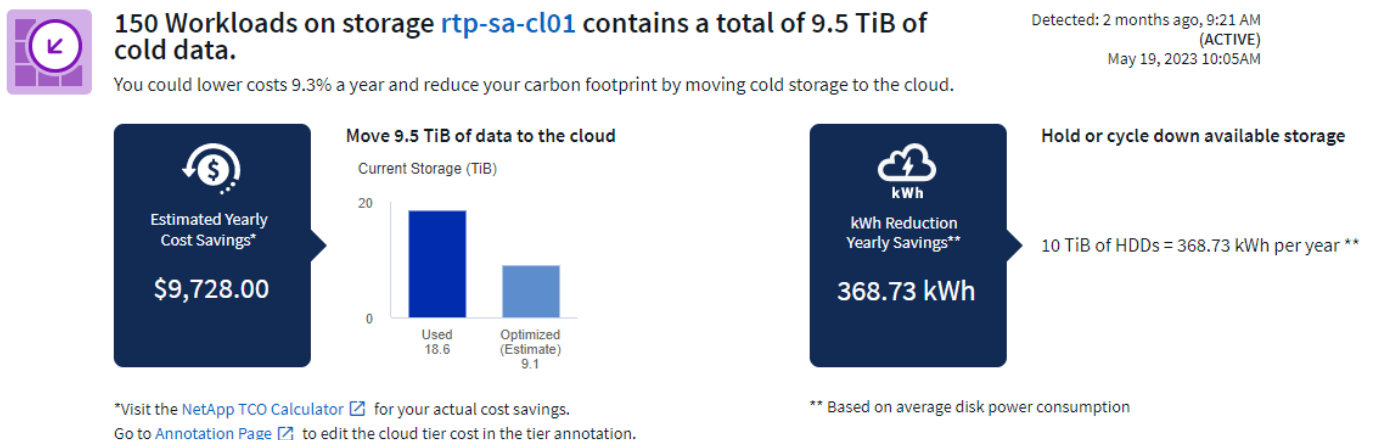
Beachten Sie, dass Kälte­daten, die jün­ger als 30 Tage sind, nicht ange­zeigt wer­den.

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 Insight-Beschreibung gibt einen schnellen Hinweis auf die Menge der als „kalt“ erkannten Daten und auf welchem Speicher sich diese Daten befinden. Die Tabelle enthält außerdem eine Zählung 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 unisierter Datenträger sowie geschätzte Kosten- und Energieeinsparungen, die Sie möglicherweise durch die Umsetzung dieser Empfehlungen erzielen könnten. Die Seite bietet sogar einen praktischen Link zu ["TCO-Rechner von NetApp"](#) Sie können also mit den Zahlen experimentieren.



Empfehlungen

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

- Verschieben Sie ungenutzte Workloads (Zombies) auf eine kostengünstigere Speicherebene (HDD).

Suchen Sie mithilfe der Zombie-Flagge, des Cold Storage und der Anzahl der Tage die kälteste und größte Datenmenge und verschieben Sie die Arbeitslast auf eine kostengünstigere Speicherebene (z. B. einen Speicherpool mit Festplattenspeicher). Eine Arbeitslast wird als „Zombie“ betrachtet, wenn sie 30 Tage oder länger keine nennenswerten E/A-Anfragen erhalten hat.

- Löschen Sie nicht verwendete Workloads

Überprüfen Sie, welche Workloads nicht verwendet werden, und ziehen Sie in Erwägung, sie zu archivieren oder aus dem Speichersystem zu entfernen.

- Ziehen Sie die Fabric Pool-Lösung von NetApp in Betracht

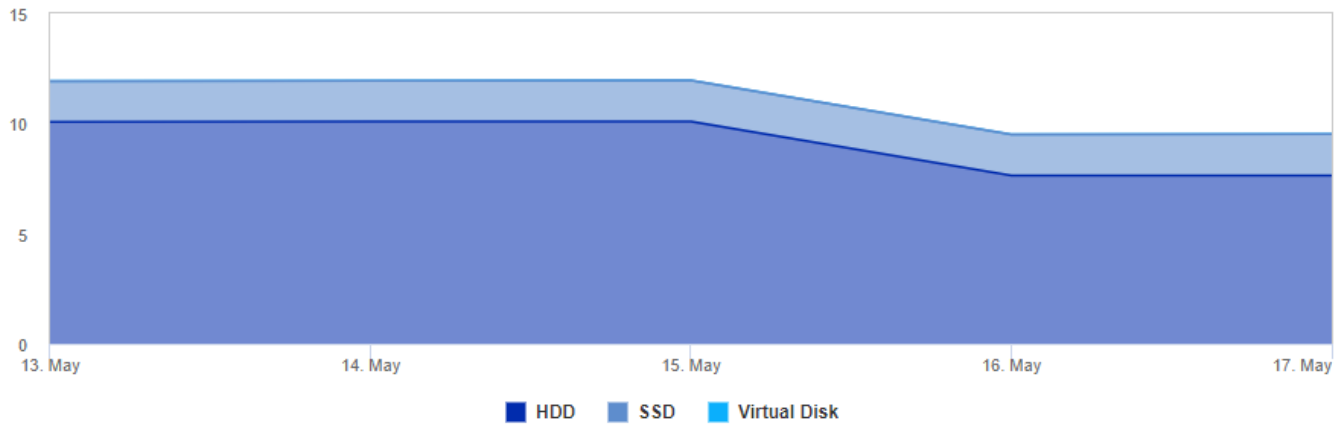
NetApps"Fabric Pool-Lösung" verteilt kalte Daten automatisch auf kostengünstigen Cloud-Speicher und erhöht so die Effizienz Ihrer Leistungsebene und bietet Remote-Datenschutz.

Visualisieren und erkunden

Die Diagramme und Tabellen liefern zusätzliche Trendinformationen und ermöglichen Ihnen, die einzelnen Arbeitslasten genauer zu untersuchen.

Cluster Cold Storage Trend [Show Details](#)

Cold Data (TiB)



Cold Storage by Days Cold (TiB)



Workloads with cold data (150) [View all workloads](#)

Filter...

Workloads	# Days cold	↑	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	i 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 Warnungen

Alarmierung mit Monitoren

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

Mithilfe von Monitoren können Sie Schwellenwerte für Metriken festlegen, die von „Infrastruktur“-Objekten wie Speicher, VM, EC2 und Ports generiert werden, sowie für „Integration“-Daten, wie sie beispielsweise für Kubernetes, erweiterte ONTAP -Metriken und Telegraf-Plugins erfasst werden. Diese *metrischen* Monitore warnen Sie, wenn Warnschwellen oder kritische Schwellenwerte überschritten werden.

Sie können auch Monitore erstellen, um Warnungen auf Warn-, kritischer oder informativer Ebene auszulösen, wenn bestimmte *Protokollereignisse* erkannt werden.

Data Infrastructure Insights bietet eine Reihe von ["Systemdefinierte Monitore"](#) auch basierend auf Ihrer Umgebung.

Best Practice für die Sicherheit

Die Warnmeldungen von Data Infrastructure Insights sollen Datenpunkte und Trends zu Ihrem Mandanten hervorheben. Außerdem können Sie mit Data Infrastructure Insights eine beliebige gültige E-Mail-Adresse als Warnmeldungsempfänger eingeben. Wenn Sie in einer sicheren Umgebung arbeiten, achten Sie besonders

darauf, wer die Benachrichtigung erhält oder anderweitig Zugriff auf die Warnung hat.

Metrik- oder Protokollmonitor?

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Warnungen > Monitore verwalten**

Die Seite mit der Monitorliste wird angezeigt und zeigt die aktuell konfigurierten Monitore.

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 Metrikmonitor oder einen Protokollmonitor zu erstellen.

- *Metric* überwacht Warnungen bei infrastruktur- oder leistungsbezogenen Auslösern
- *Log* überwacht Warnungen bei protokollbezogenen Aktivitäten

Nachdem Sie Ihren Monitortyp ausgewählt haben, wird das Dialogfeld „Monitorkonfiguration“ angezeigt. Die Konfiguration variiert je nach dem von Ihnen erstellten Monitortyp.

Metrikmonitor

1. Suchen Sie in der Dropdown-Liste nach einem zu überwachenden Objekttyp und einer Metrik und wählen Sie diese aus.

Sie können Filter festlegen, um einzugrenzen, welche Objektattribute oder Metriken überwacht werden sollen.

1 Select a metric to monitor

The screenshot shows a web interface for selecting a metric to monitor. At the top, a text input field contains the metric name 'netapp_ontap.aggregate.cp_reads'. Below this, there are three buttons: 'Filter By', 'Group', and 'Unit Display'. A blue button with a white plus sign is positioned to the right of the 'Filter By' button. A dropdown menu is open, showing a search bar with the text 'Search...'. Below the search bar, the word 'Metrics' is displayed. A list of metrics follows: 'cp_read_blocks', 'cp_reads' (which is highlighted), 'data_compaction_space_saved', 'data_compaction_space_saved_percent', and 'size_total'.

Beim Arbeiten mit Integrationsdaten (Kubernetes, ONTAP Advanced Data usw.) entfernt die Metrikfilterung die einzelnen/nicht übereinstimmenden Datenpunkte aus der dargestellten Datenreihe. Bei Infrastrukturdaten (Speicher, VM, Ports usw.) hingegen arbeiten Filter mit dem aggregierten Wert der Datenreihe und entfernen möglicherweise das gesamte Objekt aus dem Diagramm.

Metrikmonitore gelten für Inventarobjekte wie Speicher, Switch, Host, VM usw. sowie für Integrationsmetriken wie ONTAP Advanced oder Kubernetes-Daten. Beachten Sie beim Überwachen von Inventarobjekten, dass Sie keine „Gruppieren nach“-Methode auswählen können. Bei der Überwachung von Integrationsdaten ist jedoch eine Gruppierung zulässig.

Multi-Condition-Monitore

Sie können Ihren Metrikmonitor durch Hinzufügen einer zweiten Bedingung weiter verfeinern. Erweitern Sie einfach die Eingabeaufforderung „+Sekundäre Metrikbedingung hinzufügen“ und konfigurieren Sie die zusätzliche Bedingung.

The screenshot shows the configuration interface for a Multi-Condition Monitor. It features two main sections. The top section is for the primary condition, with a warning icon and the text 'Warning'. It includes a dropdown menu for 'Alert if the iops.read is', a value of '1000', a unit of 'IO/s and/or', and a dropdown menu for 'Warning or Critical required'. The bottom section is for the secondary condition, with an 'AND' button, a dropdown menu for 'iops.total', a value of 'Value required', a unit of 'IO/s', and a dropdown menu for 'Once'.

Der Monitor gibt einen Alarm aus, wenn beide Bedingungen erfüllt sind.

Beachten Sie, dass Sie eine zweite Bedingung nur mit einem „UND“ verknüpfen können. Sie können nicht wählen, ob Sie bei der einen ODER der anderen Bedingung eine Warnung erhalten möchten.

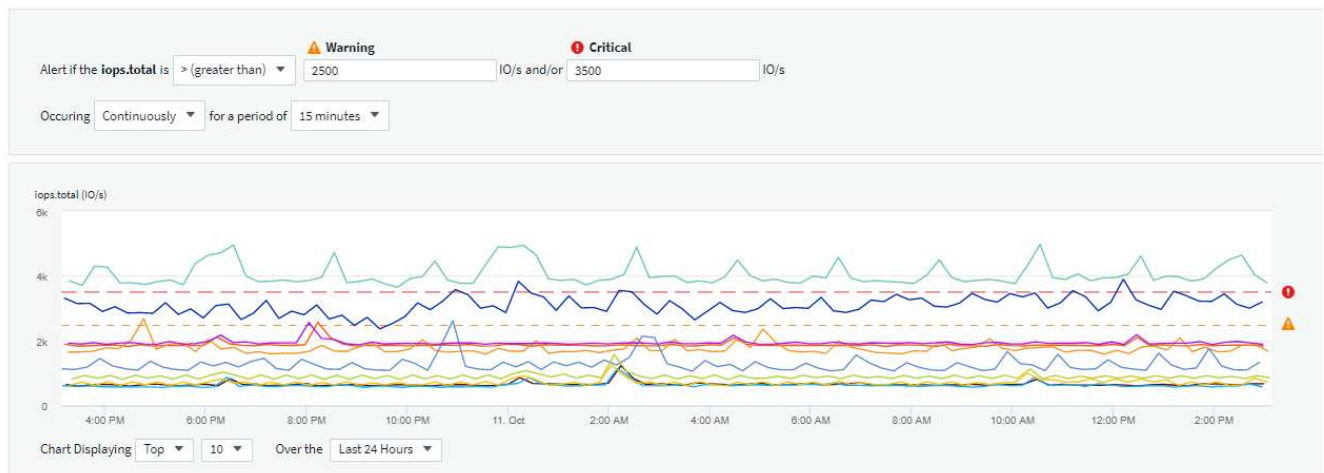
Definieren Sie die Bedingungen des Monitors.

1. Nachdem Sie das zu überwachende Objekt und die Metrik ausgewählt haben, legen Sie die Schwellenwerte für die Warnstufe und/oder die kritische Stufe fest.
2. Geben Sie für die Warnstufe in unserem Beispiel 200 ein. Die gestrichelte Linie, die diese Warnstufe anzeigt, wird im Beispieldiagramm angezeigt.
3. Geben Sie für die Stufe *Kritisch* den Wert 400 ein. Die gestrichelte Linie, die diesen kritischen Pegel anzeigt, wird im Beispieldiagramm angezeigt.

Das Diagramm zeigt historische Daten. Die Warn- und Kritisch-Level-Linien im Diagramm sind eine visuelle Darstellung des Monitors, sodass Sie leicht erkennen können, wann der Monitor in jedem Fall eine Warnung auslösen könnte.

4. Wählen Sie für das Auftretensintervall *Kontinuierlich* für einen Zeitraum von *15 Minuten*.

Sie können wählen, ob Sie einen Alarm auslösen möchten, sobald ein Schwellenwert überschritten wird, oder ob Sie warten möchten, bis der Schwellenwert über einen bestimmten Zeitraum hinweg kontinuierlich überschritten wurde. In unserem Beispiel möchten wir nicht jedes Mal benachrichtigt werden, wenn die Gesamt-IOPS den Warn- oder kritischen Wert überschreiten, sondern nur, wenn ein überwachtes Objekt mindestens 15 Minuten lang kontinuierlich einen dieser Werte überschreitet.



Definieren des Alarmauflösungsverhaltens

Sie können auswählen, wie eine Metriküberwachungswarnung aufgelöst wird. Ihnen stehen zwei Möglichkeiten zur Verfügung:

- Lösen Sie das Problem, wenn die Metrik wieder in den akzeptablen Bereich zurückkehrt.
- Lösen Sie das Problem, wenn die Metrik für einen bestimmten Zeitraum (von 1 Minute bis 7 Tagen) im akzeptablen Bereich liegt.

Protokollmonitor

Wählen Sie beim Erstellen eines **Protokollmonitors** zunächst aus der verfügbaren Protokollliste aus, welches Protokoll überwacht werden soll. Anschließend können Sie wie oben beschrieben anhand der verfügbaren Attribute filtern. Sie können auch ein oder mehrere „Gruppieren nach“-Attribute auswählen.



Der Log-Monitor-Filter darf nicht leer sein.

1 Select the log to monitor

Log Source logs.netapp.ems

Filter By ems.ems_message_type Nblade.vscanConnBackPressure ems.cluster_vendor NetApp

ems.cluster_model FAS AFF ASA FDvM + ?

Group By ems.cluster_uuid ems.cluster_vendor ems.cluster_model ems.cluster_name ems.svm_uuid ems.svm_name

Definieren Sie das Alarmverhalten

Sie können den Monitor so erstellen, dass er mit dem Schweregrad *Kritisch*, *Warnung* oder *Informativ* warnt, wenn die oben definierten Bedingungen einmal (also sofort) eintreten, oder mit der Warnung warten, bis die Bedingungen zweimal oder öfter eintreten.

Definieren des Alarmauflösungsverhaltens

Sie können auswählen, wie eine Warnung des Protokollmonitors aufgelöst wird. Ihnen stehen drei Auswahlmöglichkeiten zur Verfügung:

- **Sofort lösen:** Der Alarm wird sofort gelöst, es sind keine weiteren Maßnahmen erforderlich
- **Auflösung basierend auf Zeit:** Der Alarm wird nach Ablauf der angegebenen Zeit aufgelöst
- **Auflösung basierend auf Protokolleintrag:** Der Alarm wird aufgelöst, wenn eine nachfolgende Protokollaktivität aufgetreten ist. Beispielsweise wenn ein Objekt als „verfügbar“ protokolliert wird.

- ☐ Resolve instantly
- ☐ Resolve based on time
- ☒ Resolve based on log entry

Log Source logs.netapp.ems

Filter By ems.ems_message_type "object.store.available" +

Anomalieerkennungsmonitor

1. Suchen Sie in der Dropdown-Liste nach einem zu überwachenden Objekttyp und einer Metrik und wählen Sie diese aus.

Sie können Filter festlegen, um einzugrenzen, welche Objektattribute oder Metriken überwacht werden sollen.

1 Select a metric anomaly to monitor

Object	Storage	X ▼	Metric	iops.total	X ▼
Filter by Attribute		+	?		
Filter by Metric		+	?		
Group by		Storage ▼			
Unit Displayed In		Whole Number ▼			

Definieren Sie die Bedingungen des Monitors.

1. Nachdem Sie das zu überwachende Objekt und die Metrik ausgewählt haben, legen Sie die Bedingungen fest, unter denen eine Anomalie erkannt wird.
 - Wählen Sie, ob eine Anomalie erkannt werden soll, wenn die gewählte Metrik die vorhergesagten Grenzen **überschreitet**, **unterschreitet** oder **über oder unterschreitet**.
 - Stellen Sie die **Empfindlichkeit** der Erkennung ein. **Niedrig** (weniger Anomalien werden erkannt), **Mittel** oder **Hoch** (mehr Anomalien werden erkannt).
 - Stellen Sie die Warnungen auf **Warnung** oder **Kritisch** ein.
 - Bei Bedarf können Sie das Rauschen reduzieren und Anomalien ignorieren, wenn die gewählte Metrik unter einem von Ihnen festgelegten Schwellenwert liegt.

2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above ▼ the predicted bounds.

Set sensitivity: Low (detect fewer anomalies) ▼

Alert severity: Critical ▼

To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s

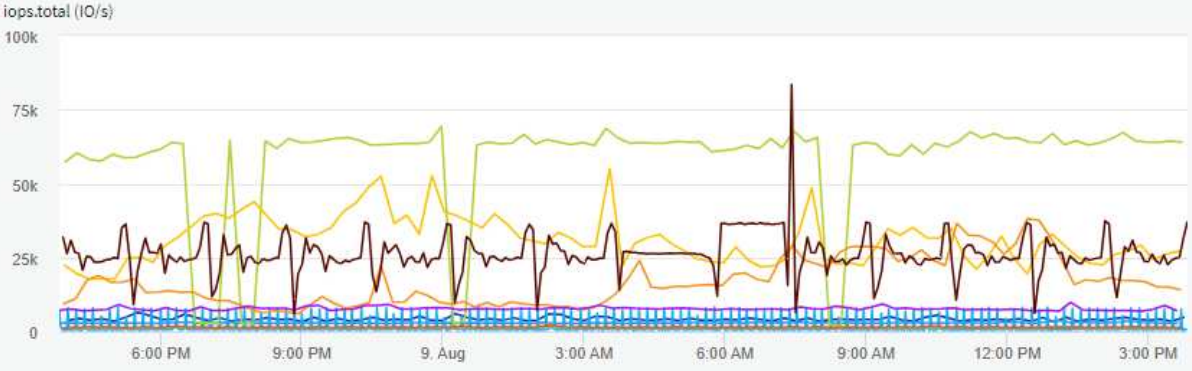


Chart Displaying Top ▼ 10 ▼ Over the Last 24 Hours ▼

Benachrichtigungstyp und Empfänger auswählen

Im Abschnitt „Teambenachrichtigung(en) einrichten“ können Sie auswählen, ob Ihr Team per E-Mail oder Webhook benachrichtigt werden soll.

3 Set up team notification(s) (alert your team via email, or Webhook)

Add Delivery Method ▼

- Email
- Webhook

Benachrichtigung per E-Mail:

Geben Sie die E-Mail-Empfänger für Warnbenachrichtigungen an. Bei Bedarf können Sie für Warnungen oder kritische Alarmer unterschiedliche Empfänger auswählen.

3 Set up team notification(s)

The screenshot shows two identical configuration blocks for email notifications. Each block has a 'Notify team on' dropdown menu and an 'Add Recipients (Required)' field. In the first block, the dropdown is open, showing 'Critical' (checked), 'Warning' (unchecked), and 'Resolved' (checked). The recipients field contains 'user_1@email.com' and 'user_2@email.com'. In the second block, the dropdown is set to 'Warning' and the recipients field contains 'user_3@email.com'.

Alarmierung per Webhook:

Geben Sie den/die Webhook(s) für Warnbenachrichtigungen an. Bei Bedarf können Sie verschiedene Webhooks für Warnungen oder kritische Alarmer auswählen.

3 Set up team notification(s) (alert your team via email, or Webhook)

The screenshot shows three configuration blocks for webhook notifications. Each block has a 'Notify team on' dropdown menu and a 'Use Webhook(s)' field. The first block is for 'Critical' events with 'Slack' and 'Teams' selected. The second block is for 'Resolved' events with 'Slack' and 'Teams' selected. The third block is for 'Warning' events with 'Slack' and 'Teams' selected.



ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitor-Benachrichtigungen, die für den Cluster/Data Collector relevant sind. Die Empfängerliste, die Sie für den Datensammler selbst festlegen, erhält die Warnungen des Datensammlers. Wenn keine aktiven Datensammlerwarnungen vorliegen, werden vom Monitor generierte Warnungen an bestimmte Monitorempfänger gesendet.

Festlegen von Korrekturmaßnahmen oder zusätzlichen Informationen

Sie können eine optionale Beschreibung sowie zusätzliche Erkenntnisse und/oder Korrekturmaßnahmen hinzufügen, indem Sie den Abschnitt **Warnungsbeschreibung hinzufügen** ausfüllen. Die Beschreibung kann bis zu 1024 Zeichen lang sein und wird mit der Warnung gesendet. Das Feld „Erkenntnisse/Korrekturmaßnahmen“ kann bis zu 67.000 Zeichen umfassen und wird im Zusammenfassungsbereich der Zielseite der Warnung angezeigt.

In diesen Feldern können Sie Notizen, Links oder Schritte zur Korrektur oder anderweitigen Bearbeitung der Warnung angeben.

Sie können einer Alarmbeschreibung jedes beliebige Objektattribut (z. B. den Speichernamen) als Parameter hinzufügen. Sie können beispielsweise Parameter für den Volumenamen und den Speichernamen in einer

Beschreibung wie folgt festlegen: „Hohe Latenz für Volume: `%%relatedObject.volume.name%%`, Speicher: `%%relatedObject.storage.name%%`“.

4 Add an alert description (optional)

Add a description

Enter a description that will be sent with this alert (1024 character limit)

Add insights and corrective actions

Enter a url or details about the suggested actions to fix the issue raised by the alert

Speichern Sie Ihren Monitor

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

Ihr neuer Monitor wird der Liste der aktiven Monitore hinzugefügt.

Monitorliste

Auf der Seite „Monitor“ werden die aktuell konfigurierten Monitore aufgelistet und Folgendes angezeigt:

- Monitorname
- Status
- Überwachtes Objekt/Metrik
- Bedingungen des Monitors

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

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

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

Monitorgruppen

Durch Gruppieren können Sie zusammengehörige Monitore anzeigen und verwalten. Sie können beispielsweise eine Monitorgruppe speziell für den Speicher Ihres Mandanten einrichten oder Monitore, die für eine bestimmte Empfängerliste relevant sind.

Monitor Groups (5)



Search groups...

- All Monitors (5)
- Custom Monitors (5)
- Agent Monitors (3)
- ONTAP Aggregate Monitors (2)

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

- **Alle Monitore** listet alle Monitore auf.
- **Benutzerdefinierte Monitore** listet alle vom Benutzer erstellten Monitore auf.
- **Angehaltene Monitore** listet alle Systemmonitore auf, die von Data Infrastructure Insights angehalten wurden.
- Data Infrastructure Insights zeigt auch eine Reihe von **System Monitor Groups** an, die eine oder mehrere Gruppen von "systemdefinierte Monitore", einschließlich ONTAP -Infrastruktur- und Workload-Monitoren.



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

Hängende Monitore

Diese Gruppe wird nur angezeigt, wenn Data Infrastructure Insights einen oder mehrere Monitore angehalten hat. Ein Monitor kann ausgesetzt werden, wenn er übermäßig viele oder kontinuierliche Warnungen generiert. Wenn es sich bei dem Monitor um einen benutzerdefinierten Monitor handelt, ändern Sie die Bedingungen, um die kontinuierliche Alarmierung zu verhindern, und setzen Sie den Monitor dann fort. Der Monitor wird aus der Gruppe „Angehaltene Monitore“ entfernt, wenn das Problem, das zur Anhaltung geführt hat, behoben ist.

Systemdefinierte Monitore

Diese Gruppen zeigen die von Data Infrastructure Insights bereitgestellten 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 einen Systemmonitor duplizieren und das Duplikat ändern oder verschieben.

Systemmonitore können Monitore für die ONTAP Infrastruktur (Speicher, Volume usw.) oder Workloads (d. h. Protokollmonitore) oder andere Gruppen umfassen. NetApp wertet ständig die Kundenbedürfnisse und Produktfunktionen aus und aktualisiert oder ergänzt Systemmonitore und -gruppen nach Bedarf.

Benutzerdefinierte Monitorgruppen

Sie können Ihre eigenen Gruppen erstellen, um Monitore entsprechend Ihren Anforderungen zu enthalten. Beispielsweise möchten Sie möglicherweise eine Gruppe für alle Ihre 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**. Es wird eine leere Gruppe mit diesem Namen 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 *Zur Gruppe hinzufügen*. Wählen Sie die Gruppe aus, zu 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.

5 Associate to a monitor group (optional)

ONTAP Monitors

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

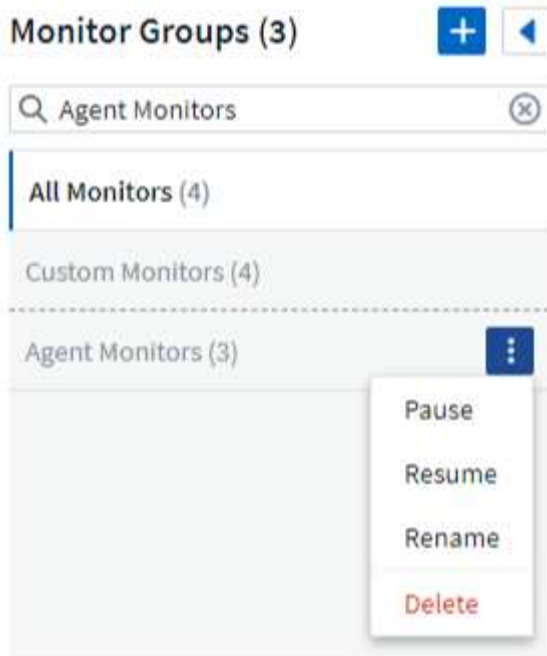


Durch das Entfernen eines Monitors aus einer Gruppe wird der Monitor nicht aus Data Infrastructure Insights gelöscht. Um einen Monitor vollständig zu entfernen, wählen Sie den Monitor aus und klicken Sie auf *Löschen*. Dadurch wird es auch aus der Gruppe entfernt, zu der es gehörte, und steht keinem Benutzer mehr zur Verfügung.

Sie können einen Monitor auf die gleiche Weise auch in eine andere Gruppe verschieben, indem Sie *In Gruppe verschieben* auswählen.

Um alle Monitore einer Gruppe gleichzeitig anzuhalten oder fortzusetzen, 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 Data Infrastructure Insights gelöscht. Sie sind weiterhin unter „Alle Monitore“ verfügbar.



Systemdefinierte Monitore

Data Infrastructure Insights umfasst eine Reihe systemdefinierter Monitore für Metriken und Protokolle. Die verfügbaren Systemmonitore hängen von den auf Ihrem Mandanten vorhandenen Datensammlern ab. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.

Sehen Sie sich die ["Systemdefinierte Monitore"](#) Seite mit Beschreibungen der in Data Infrastructure Insights enthaltenen Monitore.

Weitere Informationen

- ["Anzeigen und Verwerfen von Warnungen"](#)

Anzeigen und Verwalten von Warnungen von Monitoren

Data Infrastructure Insights zeigt Warnungen an, wenn ["überwachte Schwellenwerte"](#) überschritten werden.



Monitore und Warnungen sind in der Data Infrastructure Insights Standard Edition und höher verfügbar.

Anzeigen und Verwalten von Warnungen

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

1. Navigieren Sie zur Seite **Warnungen > Alle Warnungen**.
2. Es wird eine Liste mit bis zu 1.000 der letzten Warnungen angezeigt. Sie können diese Liste nach jedem Feld sortieren, indem Sie auf die Spaltenüberschrift des Felds klicken. Die Liste zeigt die folgenden Informationen an. Beachten Sie, dass nicht alle dieser Spalten standardmäßig angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnradsymbol klicken:
 - **Alarm-ID:** Vom System generierte eindeutige Alarm-ID

- **Auslösezeit:** Der Zeitpunkt, zu dem der entsprechende Monitor den Alarm ausgelöst hat
- **Aktueller Schweregrad** (Registerkarte „Aktive Warnungen“): Der aktuelle Schweregrad der aktiven Warnung
- **Höchster Schweregrad** (Registerkarte „Behobene Warnungen“): Der maximale Schweregrad der Warnung, bevor sie behoben wurde.
- **Monitor:** Der Monitor, der zum Auslösen des Alarms konfiguriert ist
- **Ausgelöst am:** Das Objekt, bei dem der überwachte Schwellenwert überschritten wurde
- **Status:** Aktueller Alarmstatus, *Neu* oder *In Bearbeitung*
- **Aktivstatus:** *Aktiv* oder *Gelöst*
- **Bedingung:** Die Schwellenwertbedingung, die den Alarm ausgelöst hat
- **Metrik:** Die Metrik des Objekts, bei der der überwachte Schwellenwert überschritten wurde
- **Monitorstatus:** Aktueller Status des Monitors, der den Alarm ausgelöst hat
- **Hat Korrekturmaßnahmen:** Die Warnung hat Korrekturmaßnahmen vorgeschlagen. Öffnen Sie die Warnseite, um diese anzuzeigen.

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

- **In Bearbeitung**, um anzuzeigen, dass die Warnung untersucht wird oder aus anderen Gründen offen gehalten werden muss
- **Ablehnen**, 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 „Status ausgewählter Warnungen ändern“ klicken.

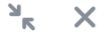
Durch Klicken auf eine Alarm-ID wird die Alarmdetailseite geöffnet.

Alarmdetailbereich

Wählen Sie eine beliebige Alarmzeile aus, um das Detailfenster des Alarms zu öffnen. Das Alarmdetailfenster bietet zusätzliche Einzelheiten zum Alarm, darunter eine *Zusammenfassung*, einen Abschnitt *Leistung* mit Diagrammen zu den Daten des Objekts, alle *zugehörigen Assets* und *Kommentare*, die von den Alarmermittlern eingegeben wurden.

Metric Alert

Jun 3, 2025
9:29 AM - 10:47 AM



Critical Alert AL-14930837 ACTIVE [Collapse Details](#)

Triggered On

Storage:
 CI-GDL1-Ontap-fas8080

Details

Top Severity: Critical
Condition: **Average iops.total** is > (greater than) 1,700 IO/s and/or 2,000 IO/s all the time in 15-minute window.

Monitor

altimeout

Attributes

Filters Applied: N/A

Description

No Description Provided

Resolution conditions

Resolve when metric is within acceptable range for 10 mins

Status

New

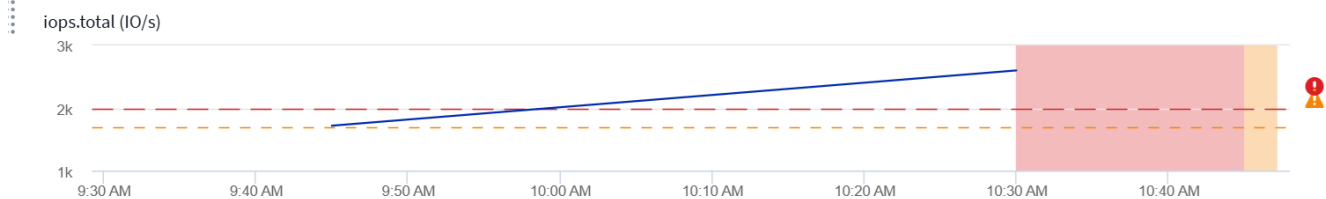
Time

Triggered time: Jun 3, 2025 10:44 AM Duration: 17m (Active)

Alert Summary

[Alert Attributes](#)

Jun 03, 2025 09:29 AM - 10:47 AM [Settings](#)



Close

Warnmeldungen bei fehlenden Daten

Um in einem Echtzeitsystem wie Data Infrastructure Insights die Analyse eines Monitors auszulösen und zu entscheiden, ob eine Warnung generiert werden soll, verlassen wir uns auf eines von zwei Dingen:

- der nächste ankommende Datenpunkt
- ein Timer, der ausgelöst wird, wenn kein Datenpunkt vorhanden ist und Sie lange genug gewartet haben

Wie bei langsamem Dateneingang – oder keinem Dateneingang – muss der Zeitgebermechanismus eingreifen, da die Dateneingangsrate nicht ausreicht, um Warnungen in „Echtzeit“ auszulösen. Daher lautet die Frage normalerweise: „Wie lange muss ich warten, bevor ich das Analysefenster schließe und mir ansehe, was ich habe?“ Wenn Sie zu lange warten, generieren Sie die Warnungen nicht schnell genug, um nützlich zu sein.

Wenn Sie einen Monitor mit einem 30-Minuten-Fenster haben, der erkennt, dass eine Bedingung durch den

letzten Datenpunkt vor einem langfristigen Datenverlust verletzt wurde, wird eine Warnung generiert, da der Monitor keine anderen Informationen erhalten hat, um eine Wiederherstellung der Metrik zu bestätigen oder festzustellen, dass die Bedingung weiterhin besteht.

„Dauerhaft aktive“ Warnungen

Es ist möglich, einen Monitor so zu konfigurieren, dass die Bedingung für das überwachte Objekt **immer** erfüllt ist – beispielsweise $IOPS > 1$ oder $Latenz > 0$. Diese werden oft als „Test“-Monitore erstellt und dann vergessen. Solche Monitore erstellen Warnungen, die für die einzelnen Objekte dauerhaft offen bleiben, was mit der Zeit zu Systembelastungen und Stabilitätsproblemen führen kann.

Um dies zu verhindern, schließt Data Infrastructure Insights alle „dauerhaft aktiven“ Warnungen nach 7 Tagen automatisch. Beachten Sie, dass die zugrunde liegenden Überwachungsbedingungen möglicherweise (wahrscheinlich) weiterhin bestehen bleiben, sodass fast sofort eine neue Warnung ausgegeben wird. Durch das Schließen der „immer aktiven“ Warnungen wird jedoch ein Teil der Systembelastung gemildert, die andernfalls auftreten kann.

Konfigurieren von E-Mail-Benachrichtigungen

Sie können eine E-Mail-Liste für abonnementbezogene Benachrichtigungen sowie eine globale E-Mail-Liste mit Empfängern für Benachrichtigungen über Verstöße gegen Schwellenwerte der Leistungsrichtlinie konfigurieren.

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

Subscription Notification Recipients

Send subscription related notifications to the following:

- ☒ All Account Owners
- ☒ All Monitor & Optimize Administrators
- ☒ Additional Email Addresses

name@email.com X

Save

Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- ☐ All Account Owners
- ☒ All Monitor & Optimize Administrators
- ☐ Additional Email Addresses

Save

Empfänger von Abonnementbenachrichtigungen

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

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

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

Benachrichtigung:	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.	Wenn „Automatische Verlängerung“ aktiviert ist, sind keine Maßnahmen erforderlich. Wenden Sie sich an den NetApp -Vertrieb, um das Abonnement zu verlängern.
Testversion endet in 2 Tagen	Testversion erneuern von " Abonnement " Seite. Sie können eine Testversion einmal verlängern. Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben
Testversion oder Abonnement ist abgelaufen. Das Konto wird in 48 Stunden keine Daten mehr sammeln. Das Konto wird nach 48 Stunden gelöscht.	Kontaktieren Sie den NetApp -Vertrieb, um ein Abonnement zu erwerben



Um sicherzustellen, dass Ihre Empfänger Benachrichtigungen von Data Infrastructure Insights erhalten, fügen Sie die folgenden E-Mail-Adressen zu allen Zulassungslisten hinzu:

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

Globale Empfängerliste für Warnmeldungen

Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen zu Warnungen an die Warnungsempfängerliste gesendet. Sie können Warnbenachrichtigungen an eine globale Empfängerliste senden.

Um globale Alarmempfänger zu konfigurieren, wählen Sie die gewünschten Empfänger im Abschnitt **Globale Monitor-Benachrichtigungsempfänger** aus.

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

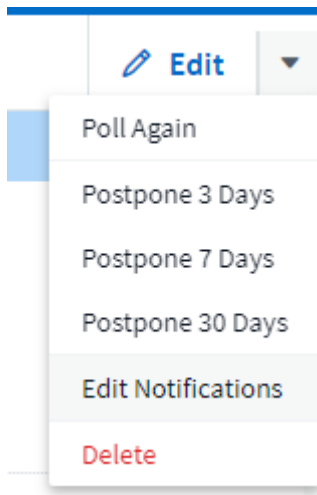


ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitor-Benachrichtigungen, die für den Cluster/Data Collector relevant sind. Die Empfängerliste, die Sie für den Datensammler selbst festlegen, erhält die Warnungen des Datensammlers. Wenn keine aktiven Datensammlerwarnungen vorliegen, werden vom Monitor generierte Warnungen an bestimmte Monitorempfänger gesendet.

Bearbeiten von Benachrichtigungen für ONTAP

Sie können Benachrichtigungen für ONTAP Cluster ändern, indem Sie auf einer Speicher-Landingpage im

Dropdown-Menü oben rechts „Benachrichtigungen bearbeiten“ auswählen.



Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder behobene Alarme festlegen. Jedes Szenario kann die globale Empfängerliste oder andere von Ihnen ausgewählte Empfänger benachrichtigen.

☒ By Email

Notify team on

Critical, Warn... ▼

Send to

- ☐ Global Monitor Recipient List
- ☒ Other Email Recipients



email@email.one ✕

email2@email2.two ✕ |

Notify team on

Resolved ▼

Send to

- ☒ Global Monitor Recipient List
- ☐ Other Email Recipients

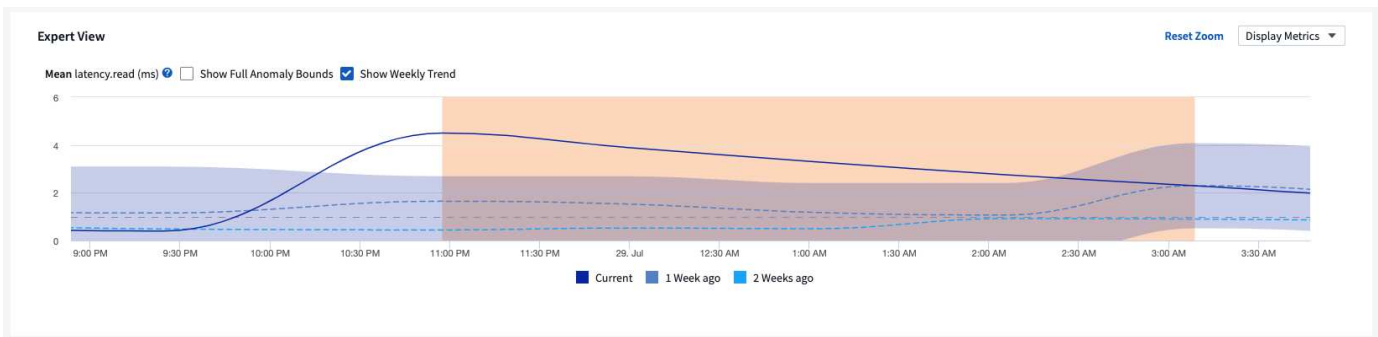
☐ By Webhook

Enable webhook notification to add recipients

Anomalieerkennungsmonitore

Die Anomalieerkennung bietet Einblick in unerwartete Änderungen in den Datenmustern Ihres Mandanten. Eine Anomalie tritt auf, wenn sich das Verhaltensmuster eines Objekts ändert. Wenn beispielsweise ein Objekt mittwochs zu einer bestimmten Uhrzeit eine bestimmte Latenz aufweist, die Latenz am darauffolgenden Mittwoch jedoch zu dieser Uhrzeit über diesen Wert ansteigt, wird dieser Anstieg als Anomalie betrachtet. Data Infrastructure Insights ermöglicht die Erstellung von Monitoren, die beim Auftreten solcher Anomalien eine Warnung ausgeben.

Die Anomalieerkennung eignet sich für Objektmetriken, die ein wiederkehrendes, vorhersehbares Muster aufweisen. Wenn diese Objektmetriken über oder unter die erwarteten Werte steigen, kann Data Infrastructure Insights eine Warnung generieren, um eine Untersuchung einzuleiten.



Was ist Anomalieerkennung?

Eine Anomalie tritt auf, wenn der Mittelwert einer Metrik um eine bestimmte Anzahl von Standardabweichungen vom gewichteten Mittelwert dieser Metrik der letzten Wochen abweicht, wobei die letzten Wochen stärker gewichtet werden als die vorherigen Wochen. Data Infrastructure Insights bietet die Möglichkeit, Daten zu überwachen und bei erkannten Anomalien eine Warnung auszugeben. Sie haben die Möglichkeit, die Empfindlichkeitsstufen der Erkennung einzustellen. Eine höhere Empfindlichkeit liegt beispielsweise vor, wenn der Mittelwert weniger Standardabweichungen vom Mittelwert aufweist und somit mehr Warnungen generiert werden. Umgekehrt gilt: geringere Empfindlichkeit = mehr Standardabweichungen vom Mittelwert = weniger Warnungen.

Die Überwachung der Anomalieerkennung unterscheidet sich von der Schwellenwertüberwachung.

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

Metric Monitor

Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

- Bei der **Überwachung der Anomalieerkennung** werden Algorithmen des maschinellen Lernens verwendet, um Ausreißer zu identifizieren, die von der Norm abweichen, wenn die Definition von „normal“ nicht klar ist.

Anomaly Detection Monitor

Detect and be alerted to abnormal performance changes



Use when you want to trigger alerts against performance spikes and drops

Wann benötige ich eine Anomalieerkennung?

Die Überwachung der Anomalieerkennung kann in vielen Situationen hilfreiche Warnungen liefern, darunter in

den folgenden:

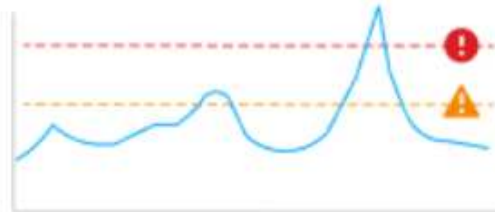
- Wenn die Definition von *normal* unklar ist. Beispielsweise kann es je nach Port zu unterschiedlich hohen SAN-Fehlerraten kommen. Eine Warnung bei einem einzelnen Fehler ist unnötig und unauffällig, ein plötzlicher oder deutlicher Anstieg kann jedoch auf ein weitverbreitetes Problem hinweisen.
- Wo es im Laufe der Zeit zu Veränderungen kommt. Arbeitslasten, die Saisonalität aufweisen (d. h. zu bestimmten Zeiten sind sie ausgelastet oder ruhig). Hierzu können unerwartete Ruhephasen gehören, die auf einen Batch-Stillstand hindeuten können.
- Arbeiten mit großen Datenmengen, bei denen das manuelle Definieren und Anpassen von Schwellenwerten unpraktisch ist. Beispielsweise ein Mandant mit einer großen Anzahl von Hosts und/oder Volumes mit unterschiedlichen Arbeitslasten. Jeder hat möglicherweise andere SLAs, daher ist es wichtig zu verstehen, welche die Norm überschreiten.

Erstellen eines Anomalieerkennungsmonitors

Um bei Anomalien Warnungen auszugeben, erstellen Sie einen Monitor, indem Sie zu **Beobachtbarkeit > Warnungen > +Monitor** navigieren. Wählen Sie *Anomaly Detection Monitor* als Monitortyp aus.

Metric Monitor

Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

Log Monitor

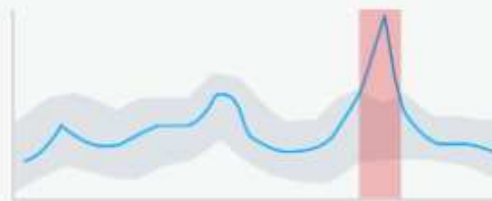
Monitor logs and configure alerts



Use when you want to trigger alerts in response to log activity

Anomaly Detection Monitor

Detect and be alerted to abnormal performance changes



Use when you want to trigger alerts against performance spikes and drops

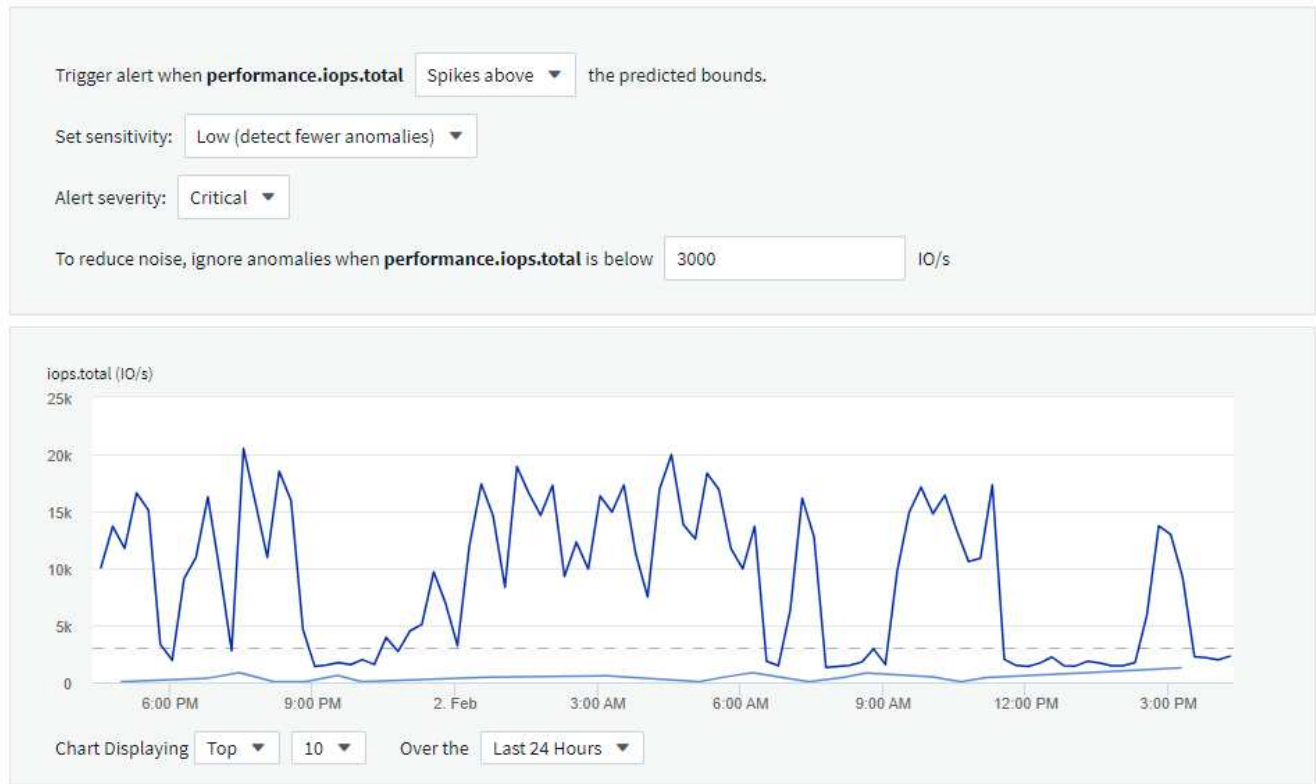
Wählen Sie das Objekt und die Metrik aus, die Sie überwachen möchten. Sie können Filter und Gruppierungen wie bei anderen Monitortypen festlegen.

Legen Sie als Nächstes die Bedingungen für den Monitor fest.

- Lösen Sie eine Warnung aus, wenn die ausgewählte Metrik entweder über die vorhergesagten Grenzen *steigt*, *unter diese Grenzen fällt* oder beides.

- Stellen Sie die Empfindlichkeit auf *Mittel*, *Niedrig* (es werden weniger Anomalien erkannt) oder *Hoch* (es werden mehr Anomalien erkannt) ein.
- Bestimmen Sie, ob die Warnstufe *Kritisch* oder *Warnung* ist.
- Legen Sie optional einen Wert fest, unterhalb dessen Anomalien *ignoriert* werden. Dies kann zur Lärmreduzierung beitragen. Dieser Wert wird im Beispieldiagramm als gestrichelte Linie angezeigt.

2 Define the monitor's conditions



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

Speichern Sie den Monitor unter einem aussagekräftigen Namen und fertig.

Nach der Erstellung analysiert der Monitor die Daten der vorherigen Woche, um eine erste Basislinie festzulegen. Die Anomalieerkennung wird mit der Zeit und mit zunehmender Historie genauer.

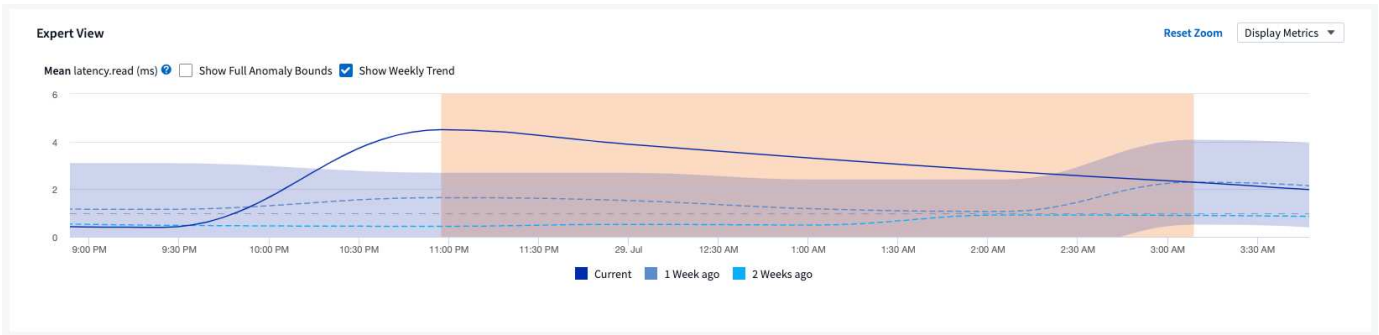


Wenn ein Monitor erstellt wird, prüft DII alle vorhandenen Daten der vorherigen Woche auf signifikante Datenspitzen oder -abfälle. Diese werden als Anomalien betrachtet. Während der ersten Woche nach der Monitorerstellung (der „Lernphase“) besteht die Möglichkeit, dass es bei den Warnungen zu verstärktem „Rauschen“ kommt. Um dieses Rauschen zu mildern, werden nur Spitzen oder Einbrüche, die länger als 30 Minuten andauern, als Anomalien betrachtet und lösen Warnungen aus. Wenn in der darauffolgenden Woche weitere Daten analysiert werden, nimmt das Rauschen normalerweise ab und ein signifikanter Anstieg oder Abfall, der länger anhält, wird als Anomalie betrachtet.

Anzeigen der Anomalien

Auf einer Warnmeldungs-Landingpage werden Warnmeldungen, die bei der Erkennung von Anomalien

ausgelöst werden, im Diagramm durch ein hervorgehobenes Band angezeigt, und zwar von dem Zeitpunkt an, als die Metrik die vorhergesagten Grenzen überschritt, bis zu dem Zeitpunkt, als sie wieder innerhalb dieser Grenzen lag.



Beim Anzeigen eines Anomaliediagramms auf einer Warnmeldungs-Zielseite können Sie die folgenden Optionen auswählen:

- Wöchentlicher Trend: Vergleichen Sie Werte mit der gleichen Uhrzeit und dem gleichen Tag der vorherigen Wochen für bis zu 5 vorherige Wochen.
- Vollständige Anomaliegrenzen: Standardmäßig konzentriert sich das Diagramm auf den Metrikwert, damit Sie das Metrikverhalten besser analysieren können. Wählen Sie diese Option aus, um die vollständigen Anomaliegrenzen (Maximalwert usw.) anzuzeigen.

Sie können auch Objekte anzeigen, die zur Anomalie beigetragen haben, indem Sie diese im Leistungsbereich der Zielseite auswählen. Das Diagramm zeigt das Verhalten der ausgewählten Objekte.



Systemmonitore

Data Infrastructure Insights umfasst eine Reihe systemdefinierter Monitore für Metriken und Protokolle. Die verfügbaren Systemmonitore hängen von den auf Ihrem Mandanten vorhandenen Datensammlern ab. Aus diesem Grund können sich die in Data Infrastructure Insights verfügbaren Monitore ändern, wenn Datensammler hinzugefügt oder ihre Konfigurationen geändert werden.



Viele Systemmonitore befinden sich standardmäßig im Status *Pausiert*. Sie können einen Systemmonitor aktivieren, indem Sie die Option *Fortsetzen* für den Monitor auswählen. Stellen Sie sicher, dass „Erweiterte Zählerdatenerfassung“ und „ONTAP EMS-Protokollerfassung aktivieren“ im Datensammler aktiviert sind. Diese Optionen finden Sie im ONTAP Data Collector

☒ Enable ONTAP EMS log collection

unter *Erweiterte Konfiguration*: ☒ Opt in for Advanced Counter Data Collection rollout.

Inhaltsverzeichnis:[]

Monitorbeschreibungen

Systemdefinierte Monitore bestehen aus vordefinierten Metriken und Bedingungen sowie Standardbeschreibungen und Korrekturmaßnahmen, die nicht geändert werden können. Sie *können* die Benachrichtigungsempfängerliste für systemdefinierte Monitore ändern. Um die Kennzahlen, 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 angegebenen Gruppen verfügbar.

- * ONTAP -Infrastruktur* umfasst Monitore für infrastrukturbezogene Probleme in ONTAP Clustern.
- * ONTAP Workload-Beispiele* umfassen Monitore für Workload-bezogene Probleme.
- Monitore in beiden Gruppen befinden sich standardmäßig im Status „Angehalten“.

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

Metrische Monitore

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
-------------	---------	---------------------	-------------------

Hohe Auslastung der Fiber Channel-Ports	KRITISCH	<p>Fiber Channel Protocol-Ports werden zum Empfangen und Übertragen des SAN-Verkehrs zwischen dem Kundenhostsystem und den ONTAP LUNs verwendet. Eine hohe Portauslastung führt zu einem Engpass und beeinträchtigt letztendlich die Leistung sensibler Fiber Channel Protocol-Workloads. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten. ... Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten, um die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie Workloads auf einen anderen FCP-Port mit geringerer Auslastung. 2. Beschränken Sie den Datenverkehr bestimmter LUNs auf unbedingt erforderliche Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über die Konfiguration auf Hostseite, um die Auslastung der FCP-Ports zu verringern. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Konfigurieren Sie mehrere FCP-Ports zur Abwicklung des Datenverkehrs, sodass die Portauslastung auf mehrere Ports verteilt wird. 2. Verschieben Sie Workloads auf einen anderen FCP-Port mit geringerer Auslastung. 3. Beschränken Sie den Datenverkehr bestimmter LUNs auf unbedingt erforderliche Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über die Konfiguration auf Hostseite, um die Auslastung der FCP-Ports zu verringern.</p>
---	----------	---	--

Lun-Latenz hoch	KRITISCH	<p>LUNs sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungsempfindlichen Anwendungen wie Datenbanken verursacht wird. Hohe LUN-Latenzen bedeuten, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Knoten oder das entsprechende Aggregat zu verschieben. ... Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Dienstkontinuität sicherzustellen. Die erwarteten Latenzen basieren auf dem Medientyp: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn mit der LUN oder ihrem Volume eine QoS-Richtlinie verknüpft ist, bewerten Sie deren Schwellenwerte und überprüfen Sie, ob diese zu einer Drosselung der LUN-Arbeitslast führen. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Maßnahmen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie die LUN in ein anderes Aggregat. 2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens. 3. Wenn der LUN oder ihrem Volume eine QoS-Richtlinie zugeordnet ist, bewerten Sie deren Schwellenwerte und überprüfen Sie, ob diese zu einer Drosselung der LUN-Arbeitslast führen.</p>
-----------------	----------	---	---

<p>Hohe Netzwerk-Port-Auslastung</p>	<p>KRITISCH</p>	<p>Netzwerkports werden zum Empfangen und Übertragen des NFS-, CIFS- und iSCSI-Protokollverkehrs zwischen den Hostsystemen des Kunden und den ONTAP-Volumes verwendet. Wenn die Portauslastung hoch ist, wird dies zu einem Engpass und beeinträchtigt letztendlich die Leistung von NFS-, CIFS- und iSCSI-Workloads. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zum Ausgleich des Netzwerkverkehrs ergriffen werden sollten. ... Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um den Netzwerkverkehr auszugleichen und so die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Beschränken Sie den Datenverkehr bestimmter Volumes auf die unbedingt erforderlichen Aufgaben, entweder über QoS-Richtlinien in ONTAP oder über eine hostseitige Analyse, um die Auslastung der Netzwerkports zu verringern. 2. Konfigurieren Sie ein oder mehrere Volumes so, dass sie einen anderen, weniger ausgelasteten Netzwerkport verwenden. ... Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Konfigurieren Sie mehrere Netzwerkports zur Abwicklung des Datenverkehrs, sodass die Portauslastung auf mehrere Ports verteilt wird. 2. Konfigurieren Sie ein oder mehrere Volumes so, dass sie einen anderen, weniger ausgelasteten Netzwerkport verwenden.</p>
--------------------------------------	-----------------	---	--

NVMe-Namespaces-Latenz hoch	KRITISCH	<p>NVMe-Namespace sind Objekte, die den E/A-Verkehr bedienen, der von leistungsempfindlichen Anwendungen wie Datenbanken gesteuert wird. Eine hohe Latenz der NVMe-Namespace bedeutet, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Knoten oder das entsprechende Aggregat zu verschieben. ... Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn dem NVMe-Namespaces oder seinem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der NVMe-Namespaces-Workload führen. ... Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen in Erwägung ziehen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie die LUN in ein anderes Aggregat. 2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens. 3. Wenn dem NVMe-Namespaces oder seinem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie die Grenzwerte, falls diese zu einer Drosselung der NVMe-Namespaces-Workload führen.</p>
-----------------------------	----------	--	---

QTree-Kapazität voll	KRITISCH	<p>Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Standardspeicherkontingent oder ein durch eine Kontingentrichtlinie definiertes Kontingent, um die im Baum gespeicherte Datenmenge innerhalb der Volumekapazität zu begrenzen. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zur Vergrößerung des Speicherplatzes ergriffen werden sollten. ... Eine kritische Meldung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Speicherplatz freizugeben und die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Platz des Qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Platz des Qtree, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben.</p>
----------------------	----------	---	--

QTree-Kapazitätsgrenze	KRITISCH	<p>Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein in KBytes gemessenes Speicherplatzkontingent, das zum Speichern von Daten verwendet wird, um das Wachstum des Benutzerdatenvolumens zu kontrollieren und seine Gesamtkapazität nicht zu überschreiten. ... Ein Qtree verwaltet ein weiches Speicherkapazitätskontingent, das den Benutzer proaktiv warnt, bevor das Gesamtkapazitätskontingentlimit im Qtree erreicht wird und keine Daten mehr gespeichert werden können. Durch die Überwachung der in einem Qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie das Baumflächenkontingent, um dem Wachstum Rechnung zu tragen 2. Weisen Sie den Benutzer an, unerwünschte Daten im Baum zu löschen, um Speicherplatz freizugeben</p>
------------------------	----------	--	---

QTree-Kapazitäts-Softlimit	WARNING (Warnung)	<p>Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein in KBytes gemessenes Speicherplatzkontingent, das er zum Speichern von Daten verwenden kann, um das Wachstum des Benutzerdatenvolumens zu kontrollieren und seine Gesamtkapazität nicht zu überschreiten. ... Ein Qtree verwaltet ein weiches Speicherkapazitätskontingent, das den Benutzer proaktiv warnt, bevor das Gesamtkapazitätskontingentlimit im Qtree erreicht wird und keine Daten mehr gespeichert werden können. Durch die Überwachung der in einem Qtree gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Erhöhen Sie das Baumplatzkontingent, um dem Wachstum Rechnung zu tragen. 2. Weisen Sie den Benutzer an, nicht benötigte Daten im Baum zu löschen, um Speicherplatz freizugeben.</p>
----------------------------	-------------------	---	--

QTree-Dateien – hartes Limit	KRITISCH	<p>Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Kontingent für die Anzahl der Dateien, die er enthalten kann, um eine verwaltbare Dateisystemgröße innerhalb des Datenträgers aufrechtzuerhalten. ... Ein Qtree verwaltet ein festes Dateianzahlkontingent, über dem neue Dateien im Baum abgelehnt werden. Durch die Überwachung der Anzahl der Dateien innerhalb eines Qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie das Dateianzahlkontingent für den Qtree. 2. Löschen Sie unerwünschte Dateien aus dem Qtree-Dateisystem.</p>
------------------------------	----------	--	--

QTree-Dateien Soft Limit	WARNING (Warnung)	<p>Ein Qtree ist ein logisch definiertes Dateisystem, das als spezielles Unterverzeichnis des Stammverzeichnisses innerhalb eines Volumes existieren kann. Jeder Qtree verfügt über ein Kontingent für die Anzahl der Dateien, die er enthalten kann, um eine verwaltbare Dateisystemgröße innerhalb des Datenträgers aufrechtzuerhalten. ... Ein Qtree verwaltet ein weiches Dateianzahlkontingent, um den Benutzer proaktiv zu warnen, bevor das Dateilimit im Qtree erreicht wird und keine weiteren Dateien mehr gespeichert werden können. Durch die Überwachung der Anzahl der Dateien innerhalb eines Qtree wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie das Dateianzahlkontingent für den Qtree. 2. Löschen Sie unerwünschte Dateien aus dem Qtree-Dateisystem.</p>
--------------------------	-------------------	--	--

<p>Snapshot-Reservespeicherplatz voll</p>	<p>KRITISCH</p>	<p>Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten im Volume verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere, nicht mehr benötigte Snapshots, um Speicherplatz freizugeben. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Snapshot-Reservespeicherplatz innerhalb des Volumes, um dem Wachstum Rechnung zu tragen. 2. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist.</p>
---	-----------------	---	--

Speicherkapazitätsgrenze	KRITISCH	<p>Wenn sich ein Speicherpool (Aggregat) füllt, verlangsamen sich die E/A-Vorgänge und werden schließlich gestoppt, was zu einem Speicherausfall führt. Eine Warnmeldung weist darauf hin, dass bald eine geplante Aktion durchgeführt werden sollte, um den minimalen freien Speicherplatz wiederherzustellen. Eine kritische Warnung weist darauf hin, dass eine Dienstunterbrechung unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Speicherplatz freizugeben und die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofort die folgenden Maßnahmen in Betracht ziehen, um die Dienstunterbrechung zu minimieren: 1. Löschen Sie Snapshots auf nicht kritischen Volumes. 2. Löschen Sie Volumes oder LUNs, die keine wesentlichen Arbeitslasten darstellen und die möglicherweise aus externen Speicherkopien wiederhergestellt werden können.....Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Verschieben Sie ein oder mehrere Volumes an einen anderen Speicherort. 2. Fügen Sie mehr Speicherkapazität hinzu. 3. Ändern Sie die Einstellungen für die Speichereffizienz oder verschieben Sie inaktive Daten in den Cloud-Speicher.</p>
--------------------------	----------	--	--

Speicherleistungsgrenze	KRITISCH	<p>Wenn ein Speichersystem seine Leistungsgrenze erreicht, verlangsamen sich die Vorgänge, die Latenz steigt und es kann zu Ausfällen bei Arbeitslasten und Anwendungen kommen. ONTAP wertet die Speicherpoolauslastung für Workloads aus und schätzt, wie viel Prozent der Leistung verbraucht wurden. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen zur Reduzierung der Speicherpoolauslastung ergriffen werden sollten, um sicherzustellen, dass genügend Speicherpoolleistung übrig bleibt, um Workloadspitzen zu bewältigen. ... Eine kritische Meldung weist darauf hin, dass ein Leistungsabfall unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um die Speicherpoolauslastung zu reduzieren und so die Servicekontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Unterbrechen Sie geplante Aufgaben wie Snapshots oder SnapMirror -Replikation. 2. Leerlauf, nicht unbedingt erforderliche Arbeitslasten. ... Wenn der Warnschwellenwert überschritten wird, ergreifen Sie sofort die folgenden Maßnahmen: 1. Verschieben Sie eine oder mehrere Workloads an einen anderen Speicherort. 2. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 3. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching).</p>
-------------------------	----------	---	---

<p>Hartes Limit für die Benutzerkontingentkapazität</p>	<p>KRITISCH</p>	<p>ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte zum Zugriff auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes verfügen. Daher ermöglicht ONTAP den Kunden, die Speicherkapazität für ihre Benutzer oder Benutzergruppen ihrer Linux- oder Windows-Systeme zu konfigurieren. Das Benutzer- oder Gruppenrichtlinienkontingent begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann. ... Eine harte Begrenzung dieses Kontingents ermöglicht die Benachrichtigung des Benutzers, wenn die innerhalb des Volumes genutzte Kapazität kurz vor dem Erreichen des Gesamtkapazitätskontingents liegt. Durch die Überwachung der innerhalb eines Benutzer- oder Gruppenkontingents gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Benutzer- oder Gruppenkontingents, um dem Wachstum Rechnung zu tragen. 2. Weisen Sie den Benutzer oder die Gruppe an, nicht benötigte Daten zu löschen, um Speicherplatz freizugeben.</p>
---	-----------------	---	--

<p>Soft-Limit für Benutzerkontingentkapazität</p>	<p>WARNING (Warnung)</p>	<p>ONTAP erkennt die Benutzer von Unix- oder Windows-Systemen, die über die Rechte zum Zugriff auf Volumes, Dateien oder Verzeichnisse innerhalb eines Volumes verfügen. Daher ermöglicht ONTAP den Kunden, die Speicherkapazität für ihre Benutzer oder Benutzergruppen ihrer Linux- oder Windows-Systeme zu konfigurieren. Das Benutzer- oder Gruppenrichtlinienkontingent begrenzt den Speicherplatz, den der Benutzer für seine eigenen Daten nutzen kann. ... Eine weiche Begrenzung dieses Kontingents ermöglicht eine proaktive Benachrichtigung des Benutzers, wenn die innerhalb des Volumes genutzte Kapazität das Gesamtkapazitätskontingent erreicht. Durch die Überwachung der innerhalb eines Benutzer- oder Gruppenkontingents gespeicherten Datenmenge wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.</p>	<p>Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Speicherplatz des Benutzer- oder Gruppenkontingents, um dem Wachstum Rechnung zu tragen. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben.</p>
---	--------------------------	--	---

Volumenkapazität Voll	KRITISCH	<p>Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Je mehr Daten im ONTAP -Volume gespeichert werden, desto geringer ist die Speicherverfügbarkeit für zukünftige Daten.</p> <p>Wenn die Datenspeicherkapazität innerhalb eines Volumes die Gesamtspeicherkapazität erreicht, kann dies dazu führen, dass der Kunde aufgrund fehlender Speicherkapazität keine Daten speichern kann. Durch die Überwachung der genutzten Speicherkapazität wird die Kontinuität der Datendienste gewährleistet.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Volumens, um dem Wachstum gerecht zu werden. 2. Löschen Sie nicht benötigte Daten, um Speicherplatz freizugeben. 3. Wenn Snapshot-Kopien mehr Speicherplatz belegen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume-Snapshots. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Erhöhen Sie den Platz im Volumen, um dem Wachstum gerecht zu werden 2. Wenn Snapshot-Kopien mehr Speicherplatz belegen als die Snapshot-Reserve, löschen Sie alte Snapshots oder aktivieren Sie die automatische Löschung von Volume-Snapshots.....</p>
-----------------------	----------	--	--

Volume-Inodes-Limit	KRITISCH	<p>Volumes, die Dateien speichern, verwenden Indexknoten (Inode) zum Speichern von Dateimetadaten. Wenn ein Volume seine Inode-Zuweisung erschöpft, können keine weiteren Dateien hinzugefügt werden. ... Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen. ... Eine kritische Meldung weist darauf hin, dass die Erschöpfung des Dateilimits unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Inodes freizugeben und so die Dienstkontinuität sicherzustellen.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Inodes-Wert für das Volume. Wenn der Inodes-Wert bereits den Maximalwert erreicht hat, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe hinausgewachsen ist. 2. Verwenden Sie FlexGroup, da es bei der Unterbringung großer Dateisysteme hilft. ... Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Erhöhen Sie den Inodes-Wert für das Volume. Wenn der Inodes-Wert bereits das Maximum erreicht hat, teilen Sie das Volume in zwei oder mehr Volumes auf, da das Dateisystem über die maximale Größe hinausgewachsen ist. 2. Verwenden Sie FlexGroup, da es bei der Unterbringung großer Dateisysteme hilft</p>
---------------------	----------	---	---

Lautstärkelatenz hoch	KRITISCH	<p>Volumes sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungsempfindlichen Anwendungen wie DevOps-Anwendungen, Home-Verzeichnissen und Datenbanken gesteuert wird. Hohe Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung der Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten. Je nach Medientyp sind folgende Latenzen zu erwarten: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA-HDD 17–20 Millisekunden.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen ergreifen, um die Dienstunterbrechung zu minimieren: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen. ... Wenn der Warnschwellenwert überschritten wird, sollten Sie die folgenden Sofortmaßnahmen in Betracht ziehen: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie das Volume auf ein anderes Aggregat. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. 3. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens.</p>
Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme

Knoten mit hoher Latenz	WARNUNG / KRITISCH	<p>Die Knotenlatenz hat ein Niveau erreicht, bei dem sie die Leistung der Anwendungen auf dem Knoten beeinträchtigen könnte. Eine geringere Knotenlatenz gewährleistet eine konsistente Leistung der Anwendungen. Die erwarteten Latenzen je nach Medientyp sind: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder die SnapMirror -Replikation 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Deaktivieren Sie nicht unbedingt erforderliche Workloads. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einen oder mehrere Workloads an einen anderen Speicherort 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)</p>
-------------------------	--------------------	---	---

Knotenleistungsgrenze	WARNUNG / KRITISCH	<p>Die Leistungsauslastung des Knotens hat ein Niveau erreicht, bei dem sie die Leistung der E/As und der vom Knoten unterstützten Anwendungen beeinträchtigen könnte. Eine geringe Knotenleistungsauslastung gewährleistet eine gleichbleibende Leistung der Anwendungen.</p>	<p>Um die Serviceunterbrechung bei einer Überschreitung eines kritischen Schwellenwerts zu minimieren, sollten umgehend Maßnahmen ergriffen werden: 1. Unterbrechen Sie geplante Aufgaben, Snapshots oder die SnapMirror -Replikation 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Deaktivieren Sie nicht unbedingt erforderliche Workloads. Erwägen Sie die folgenden Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einen oder mehrere Workloads an einen anderen Speicherort 2. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität über QoS-Grenzen 3. Fügen Sie weitere Speicherknoten (AFF) oder Festplattenregale (FAS) hinzu und verteilen Sie die Arbeitslasten neu 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)</p>
-----------------------	--------------------	--	---

Hohe Latenz der Speicher-VM	WARNUNG / KRITISCH	<p>Die Latenz der Storage-VM (SVM) hat ein Niveau erreicht, bei dem sie die Leistung der Anwendungen auf der Storage-VM beeinträchtigen könnte. Eine geringere Speicher-VM-Latenz gewährleistet eine konsistente Leistung der Anwendungen. Die erwarteten Latenzen je nach Medientyp sind: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA HDD 17–20 Millisekunden.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, bewerten Sie sofort die Schwellenwerte für Volumes der Speicher-VM mit einer zugewiesenen QoS-Richtlinie, um zu überprüfen, ob sie eine Drosselung der Volume-Workloads verursachen. Erwägen Sie die folgenden Sofortmaßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Wenn das Aggregat ebenfalls eine hohe Auslastung aufweist, verschieben Sie einige Volumes der Speicher-VM in ein anderes Aggregat. 2. Bewerten Sie für Volumes der Speicher-VM mit zugewiesener QoS-Richtlinie die Schwellenwerte, wenn diese zu einer Drosselung der Volume-Workloads führen 3. Wenn der Knoten eine hohe Auslastung aufweist, verschieben Sie einige Volumes der Speicher-VM auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens</p>
-----------------------------	--------------------	--	--

Hartes Limit für Benutzerkontingentdateien	KRITISCH	Die Anzahl der im Volume erstellten Dateien hat die kritische Grenze erreicht und es können keine weiteren Dateien erstellt werden. Durch die Überwachung der Anzahl der gespeicherten Dateien wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich. ... Erwägen Sie die Durchführung der folgenden Maßnahmen: 1. Erhöhen Sie das Dateianzahlkontingent für den jeweiligen Benutzer 2. Löschen Sie nicht benötigte Dateien, um den Druck auf das Dateikontingent für den jeweiligen Benutzer zu verringern
Soft-Limit für Benutzerkontingentdateien	WARNING (Warnung)	Die Anzahl der im Volume erstellten Dateien hat den Schwellenwert des Kontingents erreicht und liegt nahe der kritischen Grenze. Sie können keine weiteren Dateien erstellen, wenn das Kontingent die kritische Grenze erreicht. Durch die Überwachung der Anzahl der von einem Benutzer gespeicherten Dateien wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Erwägen Sie sofortige Maßnahmen, wenn die Warnschwelle überschritten wird: 1. Erhöhen Sie das Dateianzahlkontingent für das spezifische Benutzerkontingent 2. Löschen Sie nicht benötigte Dateien, um den Druck auf das Dateikontingent für den jeweiligen Benutzer zu verringern

Volume-Cache-Fehlerquote	WARNUNG / KRITISCH	<p>Die Volume Cache Miss Ratio ist der Prozentsatz der Leseanforderungen der Clientanwendungen, die von der Festplatte und nicht vom Cache zurückgegeben werden. Dies bedeutet, dass die Lautstärke den eingestellten Schwellenwert erreicht hat.</p>	<p>Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Falls er sich noch nicht auf dem Knoten des Volumes befindet, erhöhen Sie den WAFL Cache, indem Sie einen Flash Cache 3 kaufen und hinzufügen. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Falls er sich noch nicht auf dem Knoten des Volumes befindet, erhöhen Sie den WAFL Cache, indem Sie einen Flash Cache 3 kaufen und hinzufügen. Verringern Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte 4. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)</p>
--------------------------	--------------------	---	---

Volume Qtree-Kontingentüberbelegung	WARNUNG / KRITISCH	Volume Qtree Quota Overcommit gibt den Prozentsatz an, ab dem ein Volume als durch die Qtree-Kontingente überbelegt gilt. Der festgelegte Schwellenwert für das Qtree-Kontingent ist für das Volume erreicht. Durch die Überwachung der Überbelegung des Volume-Qtree-Kontingents wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Erhöhen Sie den Speicherplatz des Bandes 2. Löschen Sie nicht benötigte Daten. Wenn der Warnschwellenwert überschritten wird, sollten Sie den Speicherplatz des Datenträgers vergrößern.
-------------------------------------	--------------------	---	--

[Zurück nach oben](#)

Protokollmonitore

Monitorname	Schwere	Beschreibung	Korrekturmaßnahme
AWS-Anmeldeinformationen nicht initialisiert	INFO	Dieses Ereignis tritt auf, wenn ein Modul versucht, auf rollenbasierte Anmeldeinformationen von Amazon Web Services (AWS) Identity and Access Management (IAM) aus dem Cloud-Anmeldeinformations-Thread zuzugreifen, bevor diese initialisiert werden.	Warten Sie, bis der Thread mit den Cloud-Anmeldeinformationen und das System die Initialisierung abgeschlossen haben.

Cloud-Ebene nicht erreichbar	KRITISCH	Ein Speicherknoten kann keine Verbindung zur Cloud Tier-Objektspeicher-API herstellen. Auf einige Daten kann nicht zugegriffen werden.	<p>Wenn Sie lokale Produkte verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. ... Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. ... Stellen Sie Folgendes sicher: ... Die Konfiguration Ihres Objektspeichers hat sich nicht geändert. ... Die Anmelde- und Konnektivitätsinformationen sind weiterhin gültig. ... Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht. Wenn Sie Cloud Volumes ONTAP verwenden, führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie sicher, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat.... Stellen Sie sicher, dass die Anmelde- und Verbindungsinformationen noch gültig sind. ... Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.</p>
------------------------------	----------	--	--

Festplatte außer Betrieb	INFO	Dieses Ereignis tritt ein, wenn eine Festplatte außer Betrieb genommen wird, weil sie als fehlerhaft markiert wurde, bereinigt wird oder in das Wartungscenter gelangt ist.	Keiner.
FlexGroup -Bestandteil Voll	KRITISCH	Ein Bestandteil eines FlexGroup -Volumes ist voll, was zu einer möglichen Dienstunterbrechung führen kann. Sie können weiterhin Dateien auf dem FlexGroup -Volume erstellen oder erweitern. Allerdings können keine der auf der Komponente gespeicherten Dateien geändert werden. Daher treten möglicherweise zufällige Fehlermeldungen wegen unzureichendem Speicherplatz auf, wenn Sie versuchen, Schreibvorgänge auf dem FlexGroup -Volume durchzuführen.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. ...Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
Flexgroup-Bestandteil fast voll	WARNING (Warnung)	Ein Bestandteil eines FlexGroup -Volumes hat fast keinen Speicherplatz mehr, was zu einer möglichen Dienstunterbrechung führen kann. Dateien können erstellt und erweitert werden. Wenn jedoch der Speicherplatz der Komponente ausgeht, können Sie die Dateien auf der Komponente möglicherweise nicht anhängen oder ändern.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. ...Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.

FlexGroup -Bestandteil hat fast keine Inodes mehr	WARNING (Warnung)	Ein Bestandteil eines FlexGroup -Volumes hat fast keine Inodes mehr, was zu einer möglichen Dienstunterbrechung führen kann. Der Bestandteil erhält weniger Erstellungsanfragen als der Durchschnitt. Dies kann die Gesamtleistung des FlexGroup -Volumes beeinträchtigen, da die Anforderungen an Bestandteile mit mehr Inodes weitergeleitet werden.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. ...Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
FlexGroup -Bestandteil außerhalb der Inodes	KRITISCH	Einem Bestandteil eines FlexGroup -Volumes sind die Inodes ausgegangen, was zu einer möglichen Dienstunterbrechung führen kann. Sie können für diesen Bestandteil keine neuen Dateien erstellen. Dies kann zu einer insgesamt unausgewogenen Verteilung der Inhalte über das FlexGroup -Volumen führen.	Es wird empfohlen, die Kapazität des FlexGroup -Volumes mit dem Befehl „volume modify -files +X“ zu erhöhen. ...Alternativ können Sie Dateien aus dem FlexGroup -Volume löschen. Allerdings ist es schwierig festzustellen, welche Dateien beim Wähler gelandet sind.
LUN offline	INFO	Dieses Ereignis tritt auf, wenn eine LUN manuell offline geschaltet wird.	Bringen Sie die LUN wieder online.
Lüfter der Haupteinheit ausgefallen	WARNING (Warnung)	Ein oder mehrere Lüfter der Haupteinheit sind ausgefallen. Das System bleibt betriebsbereit. ...Wenn der Zustand jedoch zu lange anhält, kann die Übertemperatur eine automatische Abschaltung auslösen.	Setzen Sie die ausgefallenen Lüfter neu ein. Wenn der Fehler weiterhin besteht, ersetzen Sie sie.
Lüfter der Haupteinheit im Warnzustand	INFO	Dieses Ereignis tritt auf, wenn sich ein oder mehrere Lüfter der Haupteinheit in einem Warnzustand befinden.	Ersetzen Sie die angegebenen Lüfter, um eine Überhitzung zu vermeiden.

NVRAM -Batterie schwach	WARNING (Warnung)	Die NVRAM Batteriekapazität ist kritisch niedrig. Wenn der Akku leer ist, kann es zu einem Datenverlust kommen. ... Ihr System generiert und überträgt eine AutoSupport oder „Call Home“-Nachricht an den technischen Support von NetApp und die konfigurierten Ziele, sofern es entsprechend konfiguriert ist. Die erfolgreiche Zustellung einer AutoSupport -Nachricht verbessert die Problembestimmung und -lösung erheblich.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Zeigen Sie den aktuellen Status, die Kapazität und den Ladezustand der Batterie mit dem Befehl „Systemknoten-Umgebungssensoren anzeigen“ an. ... Wenn die Batterie vor Kurzem ausgetauscht wurde oder das System längere Zeit nicht betriebsbereit war, überwachen Sie die Batterie, um sicherzustellen, dass sie ordnungsgemäß geladen wird. ... Wenden Sie sich an den technischen Support von NetApp , wenn die Batterielaufzeit weiterhin unter kritische Werte sinkt und das Speichersystem automatisch herunterfährt.
Serviceprozessor nicht konfiguriert	WARNING (Warnung)	Dieses Ereignis tritt wöchentlich auf, um Sie daran zu erinnern, den Serviceprozessor (SP) zu konfigurieren. Der SP ist ein physisches Gerät, das in Ihr System integriert wird, um Fernzugriff und Fernverwaltungsfunktionen bereitzustellen. Sie sollten den SP so konfigurieren, dass er seine volle Funktionalität nutzt.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Konfigurieren Sie den SP mit dem Befehl „system service-processor network modify“. ... Ermitteln Sie optional die MAC-Adresse des SP mit dem Befehl „system service-processor network show“. ... Überprüfen Sie die SP Netzwerkkonfiguration mit dem Befehl „system service-processor network show“. ... Überprüfen Sie mit dem Befehl „system service-processor autosupport invoke“, ob der SP eine AutoSupport E-Mail senden kann. HINWEIS: AutoSupport E-Mail-Hosts und -Empfänger sollten in ONTAP konfiguriert werden, bevor Sie diesen Befehl ausführen.

Serviceprozessor offline	KRITISCH	ONTAP empfängt keine Heartbeats mehr vom Serviceprozessor (SP), obwohl alle SP Wiederherstellungsmaßnahmen durchgeführt wurden. ONTAP kann den Zustand der Hardware ohne den SP nicht überwachen. ... Das System wird heruntergefahren, um Hardwareschäden und Datenverlust zu verhindern. Richten Sie einen Panikalarm ein, um sofort benachrichtigt zu werden, wenn der SP offline geht.	Führen Sie einen Neustart des Systems durch, indem Sie die folgenden Aktionen ausführen: ... Ziehen Sie den Controller aus dem Gehäuse. ... Schieben Sie den Controller wieder hinein. ... Schalten Sie den Controller wieder ein. ... Wenn das Problem weiterhin besteht, ersetzen Sie das Controllermodul.
Regallüfter ausgefallen	KRITISCH	Der angegebene Kühl Lüfter oder das Lüftermodul des Regals ist ausgefallen. Die Festplatten im Regal erhalten möglicherweise nicht genügend Kühlluftstrom, was zu einem Festplattenausfall führen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie sicher, dass das Lüftermodul vollständig sitzt und gesichert ist. HINWEIS: Bei einigen Festplatten-Shelves ist der Lüfter in das Stromversorgungsmodul integriert. ... Wenn das Problem weiterhin besteht, ersetzen Sie das Lüftermodul. ... Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von NetApp, um Hilfe zu erhalten.
Das System kann aufgrund eines Lüfterfehlers der Haupteinheit nicht betrieben werden	KRITISCH	Ein oder mehrere Lüfter der Haupteinheit sind ausgefallen, wodurch der Systembetrieb unterbrochen wird. Dies kann zu einem möglichen Datenverlust führen.	Ersetzen Sie die ausgefallenen Lüfter.

Nicht zugewiesene Datenträger	INFO	Dem System sind keine Festplatten zugewiesen – Kapazität wird verschwendet und Ihr System weist möglicherweise eine Fehlkonfiguration auf oder es wurden teilweise Konfigurationsänderungen vorgenommen.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Ermitteln Sie mit dem Befehl „disk show -n“, welche Datenträger nicht zugewiesen sind. ... Weisen Sie die Datenträger mit dem Befehl „disk assign“ einem System zu.
Antivirus-Server ausgelastet	WARNING (Warnung)	Der Antivirenservers ist zu ausgelastet, um neue Scananforderungen anzunehmen.	Wenn diese Meldung häufig auftritt, stellen Sie sicher, dass genügend Antivirenservers vorhanden sind, um die von der SVM generierte Virenskanlast zu bewältigen.
AWS-Anmeldeinformationen für IAM-Rolle abgelaufen	KRITISCH	Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden. Die rollenbasierten Anmeldeinformationen für Identity and Access Management (IAM) sind abgelaufen. Die Anmeldeinformationen werden mithilfe der IAM-Rolle vom Metadatenserver von Amazon Web Services (AWS) abgerufen und zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet.	Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsolle an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. ... Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.
AWS-Anmeldeinformationen für IAM-Rolle nicht gefunden	KRITISCH	Der Thread für Cloud-Anmeldeinformationen kann die rollenbasierten Anmeldeinformationen für das Identity and Access Management (IAM) von Amazon Web Services (AWS) nicht vom AWS-Metadatenserver abrufen. Die Anmeldeinformationen werden zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet. Cloud Volume ONTAP ist nicht mehr zugänglich. ...	Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsolle an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. ... Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.

<p>AWS-Anmeldeinformationen für IAM-Rolle ungültig</p>	<p>KRITISCH</p>	<p>Die rollenbasierten Anmeldeinformationen für Identity and Access Management (IAM) sind ungültig. Die Anmeldeinformationen werden mithilfe der IAM-Rolle vom Metadatenserver von Amazon Web Services (AWS) abgerufen und zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet. Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden.</p>	<p>Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsolle an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. ... Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.</p>
<p>AWS IAM-Rolle nicht gefunden</p>	<p>KRITISCH</p>	<p>Der Thread für Identity and Access Management (IAM)-Rollen kann auf dem AWS-Metadatenserver keine Amazon Web Services (AWS)-IAM-Rolle finden. Die IAM-Rolle ist erforderlich, um rollenbasierte Anmeldeinformationen zu erhalten, die zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet werden. Cloud Volume ONTAP ist nicht mehr zugänglich. ...</p>	<p>Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsolle an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. ... Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist.</p>

AWS IAM-Rolle ungültig	KRITISCH	Die Amazon Web Services (AWS) Identity and Access Management (IAM)-Rolle auf dem AWS-Metadatenserver ist ungültig. Auf Cloud Volume ONTAP kann nicht mehr zugegriffen werden. ...	Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP Bereitstellung und überprüfen Sie ihren Zustand. ... Stellen Sie sicher, dass die mit der Instanz verknüpfte AWS IAM-Rolle gültig ist und ihr die entsprechenden Berechtigungen für die Instanz erteilt wurden.
AWS-Metadatenserver-Verbindung fehlgeschlagen	KRITISCH	Der Rollenthread für Identity and Access Management (IAM) kann keine Kommunikationsverbindung mit dem Metadatenserver von Amazon Web Services (AWS) herstellen. Es sollte eine Kommunikation hergestellt werden, um die erforderlichen rollenbasierten AWS IAM-Anmeldeinformationen zu erhalten, die zum Signieren von API-Anfragen an Amazon Simple Storage Service (Amazon S3) verwendet werden. Cloud Volume ONTAP ist nicht mehr zugänglich. ...	Führen Sie Folgendes aus: ... Melden Sie sich bei der AWS EC2-Verwaltungskonsole an. ... Navigieren Sie zur Seite „Instanzen“. ... Suchen Sie die Instanz für die Cloud Volumes ONTAP -Bereitstellung und überprüfen Sie ihren Zustand. ...

FabricPool Speicherplatznutzungslimit fast erreicht	WARNING (Warnung)	Die gesamte clusterweite FabricPool Speicherplatznutzung von Objektspeichern von Anbietern mit Kapazitätslizenz hat fast das lizenzierte Limit erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Überprüfen Sie den Prozentsatz der lizenzierten Kapazität, die von jeder FabricPool Speicherebene verwendet wird, indem Sie den Befehl „storage aggregate object-store show-space“ verwenden. ... Löschen Sie Snapshot-Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „volume snapshot delete“ verwenden, um Speicherplatz freizugeben. ... Installieren Sie eine neue Lizenz auf dem Cluster, um die lizenzierte Kapazität zu erhöhen.
FabricPool Speicherplatznutzungslimit erreicht	KRITISCH	Die gesamte clusterweite FabricPool Speicherplatznutzung von Objektspeichern von Anbietern mit Kapazitätslizenz hat das Lizenzlimit erreicht.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Überprüfen Sie den Prozentsatz der lizenzierten Kapazität, die von jeder FabricPool Speicherebene verwendet wird, indem Sie den Befehl „storage aggregate object-store show-space“ verwenden. ... Löschen Sie Snapshot-Kopien von Volumes mit der Tiering-Richtlinie „Snapshot“ oder „Backup“, indem Sie den Befehl „volume snapshot delete“ verwenden, um Speicherplatz freizugeben. ... Installieren Sie eine neue Lizenz auf dem Cluster, um die lizenzierte Kapazität zu erhöhen.

Rückgabe des Aggregats fehlgeschlagen	KRITISCH	<p>Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Speicher-Failover-(SFO)-Rückgabe auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. ... Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. ... Überprüfen Sie mit dem Befehl „aggregate object-store config show“, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat und dass die Anmelde- und Verbindungsinformationen noch immer korrekt sind. ... Alternativ können Sie den Fehler überschreiben, indem Sie für den Parameter „require-partner-waiting“ des Giveback-Befehls „false“ angeben. ... Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.</p>
---------------------------------------	----------	---	---

<p>HA-Verbindung ausgefallen</p>	<p>WARNING (Warnung)</p>	<p>Die Hochverfügbarkeitsverbindung (HA) ist ausgefallen. Risiko eines Dienstausfalls, wenn kein Failover verfügbar ist.</p>	<p>Korrekturmaßnahmen hängen von der Anzahl und Art der von der Plattform unterstützten HA-Verbindungslinks sowie vom Grund für den Verbindungsausfall ab. ...Wenn die Links ausgefallen sind: ...Überprüfen Sie, ob beide Controller im HA-Paar betriebsbereit sind. ...Stellen Sie bei extern verbundenen Links sicher, dass die Verbindungskabel richtig angeschlossen sind und dass die Small Form-Factor Pluggables (SFPs), falls zutreffend, richtig auf beiden Controllern sitzen. ...Deaktivieren und aktivieren Sie bei intern verbundenen Links die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. ...Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl „ic link on“. ...Wenn kein Peer verbunden ist, deaktivieren und aktivieren Sie die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. ...Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.</p>
----------------------------------	--------------------------	--	--

Max. Sitzungen pro Benutzer überschritten	WARNING (Warnung)	<p>Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anfrage zum Herstellen einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden. ...</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: ...Überprüfen Sie alle Anwendungen, die auf dem Client ausgeführt werden, und beenden Sie alle, die nicht ordnungsgemäß funktionieren. ...Starten Sie den Client neu. ...Überprüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: ...Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. ...Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.</p>
---	-------------------	---	---

Maximale Anzahl der Öffnungen pro Datei überschritten	WARNING (Warnung)	<p>Sie haben die maximale Anzahl überschritten, die Sie die Datei über eine TCP-Verbindung öffnen können. Jede Anfrage zum Öffnen dieser Datei wird abgelehnt, bis Sie einige geöffnete Instanzen der Datei schließen. Dies weist normalerweise auf ein abnormales Anwendungsverhalten hin....</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: ...Überprüfen Sie die Anwendungen, die auf dem Client über diese TCP-Verbindung ausgeführt werden. Der Client funktioniert möglicherweise aufgrund der darauf ausgeführten Anwendung nicht richtig. ... Starten Sie den Client neu. ... Prüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: ... Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. ...Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.</p>
---	-------------------	--	---

NetBIOS-Namenskonflikt	KRITISCH	<p>Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Namensregistrierungsanforderung erhalten. Dies wird normalerweise durch einen Konflikt im NetBIOS-Namen oder einem Alias verursacht. Dies hat zur Folge, dass Clients möglicherweise nicht auf Daten zugreifen oder keine Verbindung zum richtigen Datenbereitstellungsknoten im Cluster herstellen können.</p>	<p>Führen Sie eine der folgenden Korrekturmaßnahmen durch: ...Wenn ein Konflikt im NetBIOS-Namen oder einem Alias vorliegt, führen Sie einen der folgenden Schritte aus: ...Löschen Sie den doppelten NetBIOS-Alias mit dem Befehl „vserver cifs delete -aliases alias -vserver vserver“.</p> <p>...Benennen Sie einen NetBIOS-Alias um, 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 ein Konflikt im NetBIOS-Namen vorliegt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -server netbiosname“ um.</p> <p>HINWEIS: Durch das Löschen eines CIFS-Servers kann der Zugriff auf die Daten unzugänglich werden.</p> <p>...Entfernen Sie den NetBIOS-Namen oder benennen Sie das NetBIOS auf dem Remotecomputer um.</p>
NFSv4-Speicherpool erschöpft	KRITISCH	Ein NFSv4-Speicherpool ist erschöpft.	<p>Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht reagiert, wenden Sie sich an den technischen Support von NetApp .</p>

Keine registrierte Scan-Engine	KRITISCH	Der Antivirus-Connector hat ONTAP benachrichtigt, dass er über keine registrierte Scan-Engine verfügt. Dies kann dazu führen, dass Daten nicht verfügbar sind, wenn die Option „Scan-obligatorisch“ aktiviert ist.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie sicher, dass die auf dem Antivirenservers installierte Scan-Engine-Software mit ONTAP kompatibel ist. ... Stellen Sie sicher, dass die Scan-Engine-Software ausgeführt wird und für die Verbindung mit dem Antiviren-Connector über lokales Loopback konfiguriert ist.
Keine Vscan-Verbindung	KRITISCH	ONTAP verfügt über keine Vscan-Verbindung, um Virenskan-Anfragen zu bedienen. Dies kann dazu führen, dass Daten nicht verfügbar sind, wenn die Option „Scan-obligatorisch“ aktiviert ist.	Stellen Sie sicher, dass der Scannerpool richtig konfiguriert ist und die Antivirenservers aktiv und mit ONTAP verbunden sind.
Knoten-Root-Volume-Speicherplatz niedrig	KRITISCH	Das System hat festgestellt, dass auf dem Stammvolume gefährlich wenig Speicherplatz vorhanden ist. Der Knoten ist nicht voll funktionsfähig. Möglicherweise ist innerhalb des Clusters ein Failover der Daten-LIFs aufgetreten, weshalb der NFS- und CIFS-Zugriff auf den Knoten eingeschränkt ist. Die Verwaltungsfunktionen sind auf lokale Wiederherstellungsverfahren für den Knoten beschränkt, um Speicherplatz auf dem Stammvolume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Schaffen Sie Speicherplatz auf dem Stammvolume, indem Sie alte Snapshot-Kopien löschen, nicht mehr benötigte Dateien aus dem Verzeichnis /mroot löschen oder die Kapazität des Stammvolumes erweitern. ... Starten Sie den Controller neu. ... Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.
Nicht vorhandene Admin-Freigabe	KRITISCH	Vscan-Problem: Ein Client hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN\$-Freigabe herzustellen.	Stellen Sie sicher, dass Vscan für die angegebene SVM-ID aktiviert ist. Durch die Aktivierung von Vscan auf einer SVM wird die ONTAP_ADMIN\$-Freigabe automatisch für die SVM erstellt.

Nicht genügend Speicherplatz für den NVMe-Namespace	KRITISCH	Ein NVMe-Namespace wurde aufgrund eines Schreibfehlers aufgrund von Speicherplatzmangel offline geschaltet.	Fügen Sie dem Volume Speicherplatz hinzu und bringen Sie dann den NVMe-Namespace online, indem Sie den Befehl „vserver nvme namespace modify“ verwenden.
NVMe-oF-Gnadenfrist aktiv	WARNING (Warnung)	Dieses Ereignis tritt täglich auf, wenn das NVMe over Fabrics (NVMe-oF)-Protokoll verwendet wird und die Nachfrist der Lizenz aktiv ist. Für die NVMe-oF-Funktionalität ist nach Ablauf der Lizenzfrist eine Lizenz erforderlich. Die NVMe-oF-Funktionalität wird deaktiviert, wenn die Lizenzfrist abgelaufen ist.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen, oder entfernen Sie alle Instanzen der NVMe-oF-Konfiguration aus dem Cluster.
NVMe-oF-Karenzzeit abgelaufen	WARNING (Warnung)	Die Nachfrist für die NVMe over Fabrics (NVMe-oF)-Lizenz ist abgelaufen und die NVMe-oF-Funktionalität ist deaktiviert.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
NVMe-oF-Gnadenfrist beginnt	WARNING (Warnung)	Die NVMe over Fabrics (NVMe-oF)-Konfiguration wurde während des Upgrades auf die ONTAP 9.5-Software erkannt. Für die NVMe-oF-Funktionalität ist nach Ablauf der Lizenzfrist eine Lizenz erforderlich.	Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine NVMe-oF-Lizenz zu erhalten und sie dem Cluster hinzuzufügen.
Objektspeicher-Host nicht auflösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicherclient kann ohne Auflösung in eine IP-Adresse nicht mit dem Objektspeicherserver kommunizieren. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie die DNS-Konfiguration, um sicherzustellen, dass der Hostname korrekt mit einer IP-Adresse konfiguriert ist.

Objektspeicher-Intercluster-LIF ausgefallen	KRITISCH	Der Objektspeicher-Client kann kein funktionsfähiges LIF für die Kommunikation mit dem Objektspeicher-Server finden. Der Knoten lässt keinen Objektspeicher-Clientverkehr zu, bis das Intercluster-LIF betriebsbereit ist. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Überprüfen Sie den Intercluster-LIF-Status mit dem Befehl „network interface show -role intercluster“. ... Stellen Sie sicher, dass das Intercluster-LIF richtig konfiguriert und betriebsbereit ist. ... Wenn kein Intercluster-LIF konfiguriert ist, fügen Sie es mit dem Befehl „network interface create -role intercluster“ hinzu.
Nichtübereinstimmung der Objektspeichersignatur	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie, ob der geheime Zugriffsschlüssel richtig konfiguriert ist. Wenn es richtig konfiguriert ist, wenden Sie sich an den technischen Support von NetApp, um Hilfe zu erhalten.

<p>READDIR- Zeitüberschreitung</p>	<p>KRITISCH</p>	<p>Ein READDIR-Dateivorgang hat das zulässige Zeitlimit für die Ausführung in WAFL überschritten. Dies kann an sehr großen oder spärlich gefüllten Verzeichnissen liegen. Es werden Korrekturmaßnahmen empfohlen.</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: ... Suchen Sie nach spezifischen Informationen zu aktuellen Verzeichnissen, bei denen READDIR-Dateivorgänge abgelaufen sind, indem Sie den folgenden NodeShell-CLI-Befehl mit der Berechtigung „diag“ verwenden: <code>wafl readdir notice show</code>. ... Überprüfen Sie, ob Verzeichnisse als spärlich gekennzeichnet sind oder nicht: ... Wenn ein Verzeichnis als spärlich gekennzeichnet ist, wird empfohlen, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die Spärlichkeit der Verzeichnisdatei zu beheben. ... Wenn ein Verzeichnis nicht als spärlich gekennzeichnet ist und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem Sie die Anzahl der Dateieinträge im Verzeichnis verringern.</p>
--	-----------------	---	---

Verlagerung des Aggregats fehlgeschlagen	KRITISCH	Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: ... Stellen Sie mithilfe des Befehls „network interface show“ sicher, dass Ihr Intercluster-LIF online und funktionsfähig ist. ... Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „ping“ über das Intercluster-LIF des Zielknotens ausführen. ... Überprüfen Sie mit dem Befehl „aggregate object-store config show“, dass sich die Konfiguration Ihres Objektspeichers nicht geändert hat und dass die Anmelde- und Verbindungsinformationen noch immer korrekt sind. ... Alternativ können Sie den Fehler mit dem Parameter „override-destination-checks“ des Umzugsbefehls überschreiben. ... Wenden Sie sich an den technischen Support von NetApp, um weitere Informationen oder Unterstützung zu erhalten.
--	----------	--	--

Schattenkopie fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Sicherungs- und Wiederherstellungsdienstvorgang von Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie anhand der in der Ereignismeldung bereitgestellten Informationen Folgendes: ... Ist die Schattenkopiekonfiguration aktiviert? ... Sind die entsprechenden Lizenzen installiert? ... Auf welchen Freigaben wird der Schattenkopievorgang ausgeführt? ... Ist der Freigabename korrekt? ... Existiert der Freigabepfad? ... Wie ist der Status des Schattenkopiesatzes und seiner Schattenkopien?
Ausfall der Stromversorgung des Speicherschalters	WARNING (Warnung)	Im Cluster-Switch fehlt eine Stromversorgung. Die Redundanz wird reduziert, das Risiko eines Stromausfalls bei weiteren Stromausfällen steigt.	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 die Stromversorgung angeschlossen ist. ... Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.
Zu viele CIFS-Authentifizierungen	WARNING (Warnung)	Viele Authentifizierungsverhandlungen fanden gleichzeitig statt. Von diesem Client liegen 256 unvollständige neue Sitzungsanforderungen vor.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanforderungen erstellt hat. Möglicherweise müssen Sie sich an den Anbieter des Clients oder der Anwendung wenden, um die Ursache des Fehlers zu ermitteln.

Unbefugter Benutzerzugriff auf die Administratorfreigabe	WARNING (Warnung)	Ein Client hat versucht, eine Verbindung zur privilegierten Freigabe ONTAP_ADMIN\$ herzustellen, obwohl der angemeldete Benutzer kein zulässiger 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 aktuell aktive Scannerpoolkonfiguration mit dem Befehl „vserver vscan scanner pool show-active“.
Virus erkannt	WARNING (Warnung)	Ein Vscan-Server hat dem Speichersystem einen Fehler gemeldet. Dies weist normalerweise darauf hin, dass ein Virus gefunden wurde. Dieses Ereignis kann jedoch auch durch andere Fehler auf dem Vscan-Server verursacht werden. ...Der Clientzugriff auf die Datei wird verweigert. Der Vscan-Server kann die Datei je nach seinen Einstellungen und seiner Konfiguration bereinigen, unter Quarantäne stellen oder löschen.	Überprüfen Sie das im „Syslog“-Ereignis gemeldete Protokoll des Vscan-Servers, um festzustellen, ob die infizierte Datei erfolgreich bereinigt, unter Quarantäne gestellt oder gelöscht werden konnte. Wenn dies nicht möglich ist, muss ein Systemadministrator die Datei möglicherweise manuell löschen.
Volume offline	INFO	Diese Meldung zeigt an, dass ein Volume offline geschaltet wurde.	Bringen Sie das Volume wieder online.
Volumenbeschränkt	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volumen eingeschränkt wird.	Bringen Sie das Volume wieder online.
Speicher-VM erfolgreich beendet	INFO	Diese Meldung wird angezeigt, wenn ein „vServer-Stopp“-Vorgang erfolgreich ist.	Verwenden Sie den Befehl „vserver start“, um den Datenzugriff auf einer Speicher-VM zu starten.
Knotenpanik	WARNING (Warnung)	Dieses Ereignis wird ausgelöst, wenn eine Panik auftritt	Wenden Sie sich an den NetApp Kundensupport.

[Zurück nach oben](#)

Anti-Ransomware-Protokollmonitore

Monitorname	Schwere	Beschreibung	Korrekturmaßnahme
Storage VM Anti-Ransomware-Überwachung deaktiviert	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für die Speicher-VM ist deaktiviert. Aktivieren Sie Anti-Ransomware, um die Speicher-VM zu schützen.	Keine
Storage VM Anti-Ransomware-Überwachung aktiviert (Lernmodus)	INFO	Die Anti-Ransomware-Überwachung für die Speicher-VM ist im Lernmodus aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung aktiviert	INFO	Die Anti-Ransomware-Überwachung für das Volume ist aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung deaktiviert	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume ist deaktiviert. Aktivieren Sie Anti-Ransomware, um das Volume zu schützen.	Keine
Volumen-Anti-Ransomware-Überwachung aktiviert (Lernmodus)	INFO	Die Anti-Ransomware-Überwachung für das Volume ist im Lernmodus aktiviert.	Keine
Volumen-Anti-Ransomware-Überwachung angehalten (Lernmodus)	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume wird im Lernmodus angehalten.	Keine
Volumen-Anti-Ransomware-Überwachung angehalten	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume ist angehalten.	Keine
Deaktivieren der Volumen-Anti-Ransomware-Überwachung	WARNING (Warnung)	Die Anti-Ransomware-Überwachung für das Volume wird deaktiviert.	Keine

Ransomware-Aktivität erkannt	KRITISCH	Um die Daten vor der erkannten Ransomware zu schützen, wurde eine Snapshot-Kopie erstellt, mit der die Originaldaten wiederhergestellt werden können. Ihr System generiert und überträgt eine AutoSupport oder „Call Home“-Nachricht an den technischen Support von NetApp und alle konfigurierten Ziele. AutoSupport -Nachrichten verbessern die Problembestimmung und -lösung.	Informationen zum Ergreifen von Abhilfemaßnahmen gegen Ransomware-Aktivitäten finden Sie im „FINAL-DOCUMENT-NAME“.
------------------------------	----------	--	--

[Zurück nach oben](#)

FSx für NetApp ONTAP -Monitore

Monitorname	Schwellenwerte	Monitorbeschreibung	Korrekturmaßnahme
Die FSx-Volumenkapazität ist voll	Warnung @ > 85 %...Kritisch @ > 95 %	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Je mehr Daten im ONTAP -Volume gespeichert werden, desto geringer ist die Speicherverfügbarkeit für zukünftige Daten. Wenn die Datenspeicherkapazität innerhalb eines Volumes die Gesamtspeicherkapazität erreicht, kann dies dazu führen, dass der Kunde aufgrund fehlender Speicherkapazität keine Daten speichern kann. Durch die Überwachung der genutzten Speicherkapazität wird die Kontinuität der Datendienste gewährleistet.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: ...1. Löschen Sie nicht mehr benötigte Daten, um Speicherplatz freizugeben.

FSx-Volumen, hohe Latenz	Warnung @ > 1000 µs...Kritisch @ > 2000 µs	Volumes sind Objekte, die den E/A-Verkehr bedienen, der häufig von leistungssensiblen Anwendungen wie DevOps-Anwendungen, Home-Verzeichnissen und Datenbanken gesteuert wird. Hohe Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung der Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: ...1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: ...1. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen. ...2. Wenn der Knoten ebenfalls stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Knoten oder reduzieren Sie die Gesamtarbeitslast des Knotens.
--------------------------	--	--	--

FSx-Volume-Inodes-Limit	Warnung @ > 85 %...Kritisch @ > 95 %	Volumes, die Dateien speichern, verwenden Indexknoten (Inode) zum Speichern von Dateimetadaten. Wenn ein Volume seine Inode-Zuweisung erschöpft, können ihm keine weiteren Dateien hinzugefügt werden. Eine Warnmeldung weist darauf hin, dass geplante Maßnahmen ergriffen werden sollten, um die Anzahl der verfügbaren Inodes zu erhöhen. Eine kritische Warnung weist darauf hin, dass die Erschöpfung des Dateilimits unmittelbar bevorsteht und Notfallmaßnahmen ergriffen werden sollten, um Inodes freizugeben und so die Servicekontinuität sicherzustellen.	Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: ...1. Erwägen Sie, den Inodes-Wert für das Volume zu erhöhen. Wenn der Inodes-Wert bereits das Maximum erreicht hat, sollten Sie das Volume in zwei oder mehr Volumes aufteilen, da das Dateisystem die maximale Größe überschritten hat. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: ...1. Erwägen Sie, den Inodes-Wert für das Volume zu erhöhen. Wenn der Inodes-Wert bereits das Maximum erreicht hat, sollten Sie das Volume in zwei oder mehr Volumes aufteilen, da das Dateisystem über die maximale Größe hinausgewachsen ist
FSx Volume Qtree-Kontingentüberbelegung	Warnung @ > 95 %...Kritisch @ > 100 %	Volume Qtree Quota Overcommit gibt den Prozentsatz an, ab dem ein Volume als durch die Qtree-Kontingente überbelegt gilt. Der festgelegte Schwellenwert für das Qtree-Kontingent ist für das Volume erreicht. Durch die Überwachung der Überbelegung des Volume-Qtree-Kontingents wird sichergestellt, dass der Benutzer einen unterbrechungsfreien Datendienst erhält.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Löschen Sie nicht benötigte Daten. Wenn der Warnschwellenwert überschritten wird, sollten Sie den Speicherplatz des Datenträgers vergrößern.

<p>Der reservierte Speicherplatz für FSx-Snapshots ist voll</p>	<p>Warnung @ > 90 %...Kritisch @ > 95 %</p>	<p>Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten im Volume verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.</p>	<p>Um Serviceunterbrechungen zu minimieren, wenn ein kritischer Schwellenwert überschritten wird, sind sofortige Maßnahmen erforderlich: ...1. Erwägen Sie die Konfiguration von Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist ... 2. Erwägen Sie, einige ältere Snapshots zu löschen, die möglicherweise nicht mehr benötigt werden, um Speicherplatz freizugeben. Planen Sie, bald die folgenden Maßnahmen zu ergreifen, wenn der Warnschwellenwert überschritten wird: ...1. Erwägen Sie, den Snapshot-Reservespeicherplatz innerhalb des Volumes zu erhöhen, um dem Wachstum Rechnung zu tragen...2. Erwägen Sie die Konfiguration von Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist</p>
---	---	---	--

FSx Volume Cache Miss Ratio	Warnung @ > 95 %...Kritisch @ > 100 %	Die Volume Cache Miss Ratio ist der Prozentsatz der Leseanforderungen der Clientanwendungen, die von der Festplatte und nicht vom Cache zurückgegeben werden. Dies bedeutet, dass die Lautstärke den eingestellten Schwellenwert erreicht hat.	Wenn ein kritischer Schwellenwert überschritten wird, sollten sofort Maßnahmen ergriffen werden, um die Dienstunterbrechung zu minimieren: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Reduzieren Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte. Erwägen Sie sofortige Maßnahmen, wenn der Warnschwellenwert überschritten wird: 1. Verschieben Sie einige Workloads vom Knoten des Volumes, um die E/A-Last 2 zu reduzieren. Verringern Sie die Nachfrage nach Workloads mit niedrigerer Priorität auf demselben Knoten über QoS-Grenzwerte 3. Ändern Sie die Arbeitslasteigenschaften (Blockgröße, Anwendungs-Caching usw.)
-----------------------------	---------------------------------------	--	--

[Zurück nach oben](#)

K8s-Monitore

Monitorname	Beschreibung	Korrekturmaßnahmen	Schweregrad/Schwellenwert
-------------	--------------	--------------------	---------------------------

Hohe Latenz bei persistentem Volume	Hohe, anhaltende Volumenlatenzen können dazu führen, dass die Anwendungen selbst darunter leiden und ihre Aufgaben nicht erfüllen können. Die Überwachung dauerhafter Volume-Latenzen ist entscheidend, um eine konsistente Anwendungsleistung aufrechtzuerhalten. Je nach Medientyp sind folgende Latenzen zu erwarten: SSD bis zu 1–2 Millisekunden, SAS bis zu 8–10 Millisekunden und SATA-HDD 17–20 Millisekunden.	<p>Sofortmaßnahmen Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um Dienstunterbrechungen zu minimieren: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, falls diese zu einer Drosselung der Volume-Arbeitslast führen.</p> <p>Bald zu ergreifende Maßnahmen Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Wenn auch der Speicherpool stark ausgelastet ist, verschieben Sie das Volume in einen anderen Speicherpool. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, prüfen Sie dessen Grenzwerte, um zu prüfen, ob diese zu einer Drosselung der Volume-Arbeitslast führen. 3. Wenn auch der Controller stark ausgelastet ist, verschieben Sie das Volume auf einen anderen Controller oder reduzieren Sie die Gesamtarbeitslast des Controllers.</p>	Warnung @ > 6.000 µs Kritisch @ > 12.000 µs
Cluster-Speichersättigung hoch	Die Sättigung des dem Cluster zuweisbaren Speichers ist hoch. Die CPU-Sättigung des Clusters wird berechnet als Summe der Speichernutzung geteilt durch die Summe des zuweisbaren Speichers aller K8s-Knoten.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %


POD-Anhängen fehlgeschlagen	Diese Warnung wird angezeigt, wenn ein Volume-Anhang mit POD fehlgeschlagen ist.		Warnung
Hohe Neuübertragungsrate	Hohe TCP-Neuübertragungsrate	Auf Netzwerküberlastung prüfen – Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 10 % Kritisch @ > 25 %
Knotendateisystemkapazität hoch	Knotendateisystemkapazität hoch	- Erhöhen Sie die Größe der Knotenfestplatten, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die Verwendung von Anwendungsdateien.	Warnung @ > 80 % Kritisch @ > 90 %
Hoher Netzwerk-Jitter bei der Arbeitslast	Hoher TCP-Jitter (hohe Latenz-/Antwortzeitschwankungen)	Überprüfen Sie, ob das Netzwerk überlastet ist. Identifizieren Sie Workloads, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Leistung des Hardwarenetzwerks	Warnung @ > 30 ms Kritisch @ > 50 ms

Durchsatz persistenter Volumes	MBPS-Schwellenwerte für persistente Volumes können verwendet werden, um einen Administrator zu warnen, wenn persistente Volumes vordefinierte Leistungserwartungen überschreiten, was sich möglicherweise auf andere persistente Volumes auswirkt. Durch die Aktivierung dieses Monitors werden Warnungen generiert, die für das typische Durchsatzprofil persistenter Volumes auf SSDs geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Überwachungszielen angepasst werden, indem Sie diesen Monitor duplizieren und für Ihre Speicherklasse geeignete Schwellenwerte festlegen. Ein duplizierter Monitor kann außerdem auf eine Teilmenge der persistenten Volumes Ihres Mandanten ausgerichtet werden.	Sofortmaßnahmen Wenn ein kritischer Schwellenwert überschritten wird, planen Sie Sofortmaßnahmen, um die Dienstunterbrechung zu minimieren: 1. Führen Sie QoS-MBPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien. Bald zu ergreifende Maßnahmen Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Führen Sie QoS-MBPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien.	Warnung @ > 10.000 MB/s Kritisch @ > 15.000 MB/s
Container, dem die Gefahr besteht, OOM zu werden, wurden getötet	Die Speichergrenzen des Containers sind zu niedrig eingestellt. Es besteht die Gefahr einer Räumung des Containers (Out of Memory Kill).	Erhöhen Sie die Speichergrenzen des Containers.	Warnung @ > 95 %
Arbeitsbelastung reduziert	Die Arbeitslast hat keine gesunden Pods.		Kritisch @ < 1
Bindung des Anspruchs auf persistentes Volume fehlgeschlagen	Diese Warnung wird angezeigt, wenn eine Bindung auf einem PVC fehlschlägt.		Warnung

ResourceQuota-Speicherlimits werden bald überschritten	Die Speichergrenzen für den Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
ResourceQuota-Speicheranforderungen werden bald überschritten	Speicheranforderungen für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Knotenerstellung fehlgeschlagen	Der Knoten konnte aufgrund eines Konfigurationsfehlers nicht geplant werden.	Suchen Sie im Kubernetes-Ereignisprotokoll nach der Ursache des Konfigurationsfehlers.	Kritisch
Die Wiederherstellung des persistenten Volumes ist fehlgeschlagen	Die automatische Wiederherstellung des Datenträgers ist fehlgeschlagen.		Warnung @ > 0 B
CPU-Drosselung für Container	Die CPU-Grenzen des Containers sind zu niedrig eingestellt. Containerprozesse werden verlangsamt.	Erhöhen Sie die CPU-Grenzen des Containers.	Warnung @ > 95 % Kritisch @ > 98 %
Service Load Balancer konnte nicht gelöscht werden			Warnung

Persistente Volume-IOPS	IOPS-Schwellenwerte für persistente Volumes können verwendet werden, um einen Administrator zu warnen, wenn persistente Volumes vordefinierte Leistungserwartungen überschreiten. Durch die Aktivierung dieses Monitors werden Warnungen generiert, die für das typische IOPS-Profil von Persistenzvolumes geeignet sind. Dieser Monitor deckt alle persistenten Volumes Ihres Mandanten ab. Die Warn- und kritischen Schwellenwerte können basierend auf Ihren Überwachungszielen angepasst werden, indem Sie diesen Monitor duplizieren und für Ihre Arbeitslast geeignete Schwellenwerte festlegen.	Sofortmaßnahmen Wenn ein kritischer Schwellenwert überschritten wird, planen Sie Sofortmaßnahmen, um die Dienstunterbrechung zu minimieren: 1. Führen Sie QoS-IOPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien. Bald zu ergreifende Maßnahmen Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Führen Sie QoS-IOPS-Grenzwerte für das Volume ein. 2. Überprüfen Sie die Anwendung, die die Arbeitslast auf dem Datenträger steuert, auf Anomalien.	Warnung bei > 20.000 IO/s Kritisch bei > 25.000 IO/s
Service Load Balancer konnte nicht aktualisiert werden			Warnung
POD-Mount fehlgeschlagen	Diese Warnung wird angezeigt, wenn die Bereitstellung eines POD fehlgeschlagen ist.		Warnung
Knoten-PID-Druck	Die Anzahl der verfügbaren Prozesskennungen auf dem (Linux-)Knoten ist unter einen Räumungsschwellenwert gefallen.	Suchen und beheben Sie Pods, die viele Prozesse generieren und dem Knoten die verfügbaren Prozess-IDs vorenthalten. Richten Sie PodPidsLimit ein, um Ihren Knoten vor Pods oder Containern zu schützen, die zu viele Prozesse erzeugen.	Kritisch @ > 0

Fehler beim Abrufen des Pod-Images	Kubernetes konnte das Pod-Container-Image nicht abrufen.	<ul style="list-style-type: none"> - Stellen Sie sicher, dass das Bild des Pods in der Pod-Konfiguration richtig geschrieben ist. - Überprüfen Sie, ob das Bild-Tag in Ihrer Registrierung vorhanden ist. - Überprüfen Sie die Anmeldeinformationen für die Image-Registrierung. - Überprüfen Sie, ob Probleme mit der Registrierungskonnektivität vorliegen. - Stellen Sie sicher, dass Sie die von öffentlichen Registrierungsanbietern auferlegten Ratenbeschränkungen nicht erreichen. 	Warnung
Job läuft zu lange	Der Job läuft zu lange		Warnung @ > 1 Std. Kritisch @ > 5 Std.
Knotenspeicher hoch	Die Knotenspeichernutzung ist hoch	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Warnung @ > 85 % Kritisch @ > 90 %
ResourceQuota-CPU-Grenzwerte werden bald überschritten	CPU-Grenzwerte für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Pod Crash Loop Backoff	Pod ist abgestürzt und hat mehrere Neustartversuche unternommen.		Kritisch @ > 3
Knoten-CPU hoch	Die CPU-Auslastung des Knotens ist hoch.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um CPU-Leistung auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %

Arbeitslast- Netzwerklatenz RTT Hoch	Hohe TCP RTT (Round Trip Time)-Latenz	Auf Netzwerküberlastung prüfen  Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 150 ms Kritisch @ > 300 ms
Auftrag fehlgeschlagen	Der Auftrag wurde aufgrund eines Knotenabsturzes oder Neustarts, einer Ressourcenerschöpfung, einer Auftragszeitüberschreitung oder eines Pod-Planungsfehlers nicht erfolgreich abgeschlossen.	Überprüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Warnung @ > 1
Dauerhaftes Volumen in wenigen Tagen voll	Der Speicherplatz des persistenten Volumes wird in einigen Tagen erschöpft sein	-Erhöhen Sie die Volumengröße, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die in Anwendungen gespeicherte Datenmenge.	Warnung @ < 8 Tage Kritisch @ < 3 Tage
Knotenspeicherdruck	Dem Knoten geht der Speicher aus. Der verfügbare Speicher hat den Auslagerungsschwellenwert erreicht.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um Speicher auf Knoten freizugeben.	Kritisch @ > 0
Knoten nicht bereit	Knoten ist seit 5 Minuten nicht bereit	Überprüfen Sie, ob der Knoten über genügend CPU-, Speicher- und Festplattenressourcen verfügt. Überprüfen Sie die Netzwerkkonnektivität des Knotens. Überprüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Kritisch @ < 1

Hohe persistente Volume-Kapazität	Die genutzte Kapazität des Persistent Volume-Backends ist hoch.	- Erhöhen Sie die Volumegröße, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die in Anwendungen gespeicherte Datenmenge.	Warnung @ > 80 % Kritisch @ > 90 %
Service Load Balancer konnte nicht erstellt werden	Erstellen des Service Load Balancers fehlgeschlagen		Kritisch
Workload-Replikat-Missverhältnis	Einige Pods sind derzeit nicht für eine Bereitstellung oder ein DaemonSet verfügbar.		Warnung @ > 1
ResourceQuota-CPU-Anfragen werden bald überschritten	CPU-Anforderungen für Namespace überschreiten bald ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Hohe Neuübertragungsrate	Hohe TCP-Neuübertragungsrate	Auf Netzwerküberlastung prüfen – Identifizieren Sie Arbeitslasten, die viel Netzwerkbandbreite verbrauchen. Überprüfen Sie, ob die CPU-Auslastung des Pods hoch ist. Überprüfen Sie die Hardware-Netzwerkleistung.	Warnung @ > 10 % Kritisch @ > 25 %
Knotenplattendruck	Der verfügbare Speicherplatz und die Inodes im Root-Dateisystem oder im Image-Dateisystem des Knotens haben einen Räumungsschwellenwert erreicht.	- Erhöhen Sie die Größe der Knotenfestplatten, um sicherzustellen, dass ausreichend Platz für die Anwendungsdateien vorhanden ist. - Reduzieren Sie die Verwendung von Anwendungsdateien.	Kritisch @ > 0
Cluster-CPU-Sättigung hoch	Die dem Cluster zuweisbare CPU-Sättigung ist hoch. Die CPU-Sättigung des Clusters wird berechnet als Summe der CPU-Auslastung geteilt durch die Summe der zuweisbaren CPUs aller K8s-Knoten.	Knoten hinzufügen. Reparieren Sie alle nicht geplanten Knoten. Passen Sie die Größe der Pods an, um CPU-Leistung auf Knoten freizugeben.	Warnung @ > 80 % Kritisch @ > 90 %

[Zurück nach oben](#)

Änderungsprotokoll-Monitore

Monitorname	Schwere	Monitorbeschreibung
Internes Volume entdeckt	Informativ	Diese Meldung wird angezeigt, wenn ein internes Volume erkannt wird.
Internes Volumen geändert	Informativ	Diese Meldung wird angezeigt, wenn ein internes Volume geändert wird.
Speicherknotten erkannt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknotten erkannt wird.
Speicherknotten entfernt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherknotten entfernt wird.
Speicherpool erkannt	Informativ	Diese Meldung wird angezeigt, wenn ein Speicherpool erkannt wird.
Virtuelle Speichermaschine erkannt	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine erkannt wird.
Geänderte virtuelle Speichermaschine	Informativ	Diese Meldung wird angezeigt, wenn eine Storage Virtual Machine geändert wird.

[Zurück nach oben](#)

Datenerfassungsmonitore

Monitorname	Beschreibung	Korrekturmaßnahme
-------------	--------------	-------------------

Abschaltung der Erfassungseinheit	Data Infrastructure Insights Acquisition Units werden im Rahmen von Upgrades regelmäßig neu gestartet, um neue Funktionen einzuführen. Dies geschieht in einer typischen Umgebung einmal im Monat oder seltener. Auf eine Warnmeldung, dass eine Erfassungseinheit heruntergefahren wurde, sollte bald darauf eine Lösung folgen, in der darauf hingewiesen wird, dass die neu gestartete Erfassungseinheit eine Registrierung bei Data Infrastructure Insights abgeschlossen hat. Normalerweise dauert dieser Zyklus vom Herunterfahren bis zur Registrierung 5 bis 15 Minuten.	Wenn der Alarm häufig auftritt oder länger als 15 Minuten anhält, überprüfen Sie den Betrieb des Systems, auf dem die Erfassungseinheit gehostet wird, des Netzwerks und aller Proxys, die die AU mit dem Internet verbinden.
Collector fehlgeschlagen	Bei der Abfrage eines Datensammlers ist eine unerwartete Fehlersituation aufgetreten.	Besuchen Sie die Datensammlerseite in Data Infrastructure Insights, um mehr über die Situation zu erfahren.
Sammlerwarnung	Dieser Alarm kann typischerweise aufgrund einer fehlerhaften Konfiguration des Datensammlers oder des Zielsystems auftreten. Überprüfen Sie die Konfigurationen erneut, um zukünftige Warnungen zu verhindern. Es kann auch daran liegen, dass unvollständige Daten abgerufen wurden, obwohl der Datensammler alle Daten gesammelt hat, die er konnte. Dies kann passieren, wenn sich die Situation während der Datenerfassung ändert (z. B. wenn eine zu Beginn der Datenerfassung vorhandene virtuelle Maschine während der Datenerfassung und vor der Erfassung ihrer Daten gelöscht wird).	Überprüfen Sie die Konfiguration des Datensammlers oder Zielsystems. Beachten Sie, dass der Monitor für Collector-Warnungen mehr Warnungen senden kann als andere Monitortypen. Daher wird empfohlen, keine Warnungsempfänger festzulegen, es sei denn, Sie führen eine Fehlerbehebung durch.

[Zurück nach oben](#)

Sicherheitsmonitore

Monitorname	Schwelle	Monitorbeschreibung	Korrekturmaßnahme
-------------	----------	---------------------	-------------------

AutoSupport HTTPS-Transport deaktiviert	Warnung @ < 1	AutoSupport unterstützt HTTPS, HTTP und SMTP als Transportprotokolle. Aufgrund der sensiblen Natur von AutoSupport Nachrichten empfiehlt NetApp dringend, HTTPS als Standardtransportprotokoll zum Senden von AutoSupport -Nachrichten an den NetApp Support zu verwenden.	Um HTTPS als Transportprotokoll für AutoSupport Nachrichten festzulegen, führen Sie den folgenden ONTAP Befehl aus: ...system node autosupport modify -transport https
Cluster Unsichere Chiffren für SSH	Warnung @ < 1	Zeigt an, dass SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP Befehl aus: ...security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Cluster-Anmeldebanner deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer deaktiviert ist, die auf das ONTAP -System zugreifen. Das Anzeigen eines Anmeldebanners ist hilfreich, um Erwartungen hinsichtlich des Zugriffs auf das System und seiner Nutzung zu wecken.	Um das Anmeldebanner für einen Cluster zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: ...security login banner modify -vserver <admin svm> -message "Access restricted to authorized users"

Cluster-Peer-Kommunikation nicht verschlüsselt	Warnung @ < 1	Wenn Sie Daten für die Notfallwiederherstellung, das Caching oder die Sicherung replizieren, müssen Sie diese Daten während des Transports über die Leitung von einem ONTAP Cluster zu einem anderen schützen. Die Verschlüsselung muss sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert werden.	Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, müssen der Quell- und der Zielcluster auf 9.6 aktualisiert werden. Verwenden Sie dann den Befehl „Cluster Peer Modify“, um sowohl die Quell- als auch die Ziel-Cluster-Peers so zu ändern, dass sie die Cluster-Peering-Verschlüsselung verwenden. ... Weitere Informationen finden Sie im NetApp Security Hardening Guide für ONTAP 9.
Standardmäßiger lokaler Administratorbenutzer aktiviert	Warnung @ > 0	NetApp empfiehlt, alle nicht benötigten Standard-Admin-Benutzerkonten (integriert) mit dem Sperrbefehl zu sperren (deaktivieren). Dabei handelt es sich in erster Linie um Standardkonten, deren 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, werden 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-Konformität aktiviert ist.	Um die FIPS 140-2-Konformität auf einem Cluster zu aktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: ...security config modify -interface SSL -is-fips -enabled true

Protokollweiterleitung nicht verschlüsselt	Warnung @ < 1	Das Auslagern von Syslog-Informationen ist notwendig, 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 Speicher- oder Aufbewahrungsort auszulagern.	Sobald ein Protokollweiterleitungsziel erstellt wurde, kann sein Protokoll nicht mehr geändert werden. Um zu einem verschlüsselten Protokoll zu wechseln, löschen Sie das Protokollweiterleitungsziel und erstellen Sie es mit dem folgenden ONTAP-Befehl neu: ...cluster log-forwarding create -destination <Ziel-IP> -protocol tcp-encrypted
MD5-gehashtes Passwort	Warnung @ > 0	NetApp empfiehlt dringend, für ONTAP Benutzerkontenkennwörter die sicherere Hash-Funktion SHA-512 zu verwenden. Konten, die die weniger sichere MD5-Hashfunktion verwenden, sollten zur SHA-512-Hashfunktion migrieren.	NetApp empfiehlt dringend, Benutzerkonten auf die sicherere 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	Zeigt an, dass für den Cluster keine NTP-Server konfiguriert sind. Aus Redundanzgründen und für optimalen Service empfiehlt NetApp, dem Cluster mindestens drei NTP-Server zuzuordnen.	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 or ip address>
Die Anzahl der NTP-Server ist niedrig	Warnung @ < 3	Zeigt an, dass der Cluster weniger als 3 konfigurierte NTP-Server hat. Aus Redundanzgründen und für optimalen Service empfiehlt NetApp, dem Cluster mindestens drei NTP-Server zuzuordnen.	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 or ip address>

Remote Shell aktiviert	Warnung @ > 0	Remote Shell ist keine sichere Methode zum Einrichten des Befehlszeilenzugriffs auf die ONTAP Lösung. Für einen sicheren Fernzugriff sollte Remote Shell deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Remote-Zugriff. ...Um Remote Shell auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: ...security protocol modify -application rsh- enabled false
Speicher-VM-Auditprotokoll deaktiviert	Warnung @ < 1	Zeigt an, dass die Audit-Protokollierung für SVM deaktiviert ist.	Um das Audit-Protokoll für einen virtuellen Server zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: ...vserver audit enable -vserver <svm>
Unsichere Verschlüsselungsverfahren für Storage-VMs für SSH	Warnung @ < 1	Zeigt an, dass SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP Befehl aus: ...security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Storage VM-Anmeldebanner deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer deaktiviert ist, die auf SVMs im System zugreifen. Das Anzeigen eines Anmeldebanners ist hilfreich, um Erwartungen hinsichtlich des Zugriffs auf das System und seiner Nutzung zu wecken.	Um das Anmeldebanner für einen Cluster zu konfigurieren, führen Sie den folgenden ONTAP -Befehl aus: ...security login banner modify -vserver <svm> -message "Access restricted to authorized users"
Telnet-Protokoll aktiviert	Warnung @ > 0	Telnet ist keine sichere Methode zum Herstellen eines Befehlszeilenzugriffs auf die ONTAP Lösung. Für einen sicheren Fernzugriff sollte Telnet deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Fernzugriff. Um Telnet auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP -Befehl im erweiterten Berechtigungsmodus aus: ...security protocol modify -application telnet -enabled false

Datenschutzmonitore

Monitorname	Schwellenwerte	Monitorbeschreibung	Korrekturmaßnahme
Nicht genügend Speicherplatz für die LUN-Snapshot-Kopie	(Filter contains_luns = Ja) Warnung @ > 95 % Kritisch @ > 100 %	Die Speicherkapazität eines Datenträgers ist zum Speichern von Anwendungs- und Kundendaten erforderlich. Ein Teil dieses Speicherplatzes, der sogenannte reservierte Snapshot-Speicherplatz, wird zum Speichern von Snapshots verwendet, die einen lokalen Schutz der Daten ermöglichen. Je mehr neue und aktualisierte Daten im ONTAP Volume gespeichert werden, desto mehr Snapshot-Kapazität wird verwendet und desto weniger Snapshot-Speicherkapazität steht für zukünftige neue oder aktualisierte Daten zur Verfügung. Wenn die Snapshot-Datenkapazität innerhalb eines Volumes den gesamten Snapshot-Reservespeicherplatz erreicht, kann dies dazu führen, dass der Kunde keine neuen Snapshot-Daten speichern kann und der Schutzgrad der Daten in den LUNs des Volumes verringert wird. Durch die Überwachung der Snapshot-Kapazität des verwendeten Volumes wird die Kontinuität der Datendienste sichergestellt.	Sofortmaßnahmen Wenn ein kritischer Schwellenwert überschritten wird, sollten Sie sofortige Maßnahmen in Betracht ziehen, um die Dienstunterbrechung zu minimieren: 1. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist. 2. Löschen Sie einige ältere, nicht mehr benötigte Snapshots, um Speicherplatz freizugeben. Bald zu ergreifende Maßnahmen Wenn der Warnschwellenwert überschritten wird, planen Sie die folgenden sofortigen Maßnahmen: 1. Erhöhen Sie den Snapshot-Reservespeicherplatz innerhalb des Volumes, um dem Wachstum Rechnung zu tragen. 2. Konfigurieren Sie Snapshots, um den Datenspeicherplatz im Volume zu nutzen, wenn die Snapshot-Reserve voll ist.

SnapMirror -Beziehungsverzögerung	Warnung bei > 150 % ... Kritisch bei > 300 %	Die SnapMirror Beziehungsverzögerung ist die Differenz zwischen dem Zeitstempel des Snapshots und der Zeit auf dem Zielsystem. Der lag_time_percent ist das Verhältnis der Verzögerungszeit zum Zeitplanintervall der SnapMirror -Richtlinie. Wenn die Verzögerungszeit dem Zeitplanintervall entspricht, beträgt der lag_time_percent 100 %. Wenn die SnapMirror -Richtlinie keinen Zeitplan hat, wird lag_time_percent nicht berechnet.	Überwachen Sie den SnapMirror -Status mit dem Befehl „snapmirror show“. Überprüfen Sie den SnapMirror Übertragungsverlauf mit dem Befehl „snapmirror show-history“
--------------------------------------	---	--	---

[Zurück nach oben](#)

Cloud Volume (CVO)-Monitore

Monitorname	CI-Schweregrad	Monitorbeschreibung	Korrekturmaßnahme
CVO-Festplatte außer Betrieb	INFO	Dieses Ereignis tritt ein, wenn eine Festplatte außer Betrieb genommen wird, weil sie als fehlerhaft markiert wurde, bereinigt wird oder in das Wartungscenter gelangt ist.	Keine

<p>CVO-Rückgabe des Speicherpools fehlgeschlagen</p>	<p>KRITISCH</p>	<p>Dieses Ereignis tritt während der Migration eines Aggregats im Rahmen einer Speicher-Failover-(SFO)-Rückgabe auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie mit dem Befehl „Network Interface Show“, ob Ihr Intercluster-LIF online und funktionsfähig ist. Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „Ping“ über den Intercluster-LIF des Zielknotens verwenden. Überprüfen Sie mit dem Befehl „aggregate object-store config show“, ob sich die Konfiguration Ihres Objektspeichers geändert hat und ob die Anmelde- und Verbindungsinformationen noch immer korrekt sind. Alternativ können Sie den Fehler überschreiben, indem Sie für den Parameter „require-partner-waiting“ des Giveback-Befehls „false“ angeben. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.</p>
--	-----------------	---	--

CVO HA-Verbindung ausgefallen	WARNING (Warnung)	Die Hochverfügbarkeitsverbindung (HA) ist ausgefallen. Risiko eines Dienstausfalls, wenn kein Failover verfügbar ist.	Korrekturmaßnahmen hängen von der Anzahl und Art der von der Plattform unterstützten HA-Verbindungslinks sowie vom Grund für den Verbindungsausfall ab. Wenn die Links ausgefallen sind: Überprüfen Sie, ob beide Controller im HA-Paar betriebsbereit sind. Stellen Sie bei extern angeschlossenen Links sicher, dass die Verbindungskabel richtig angeschlossen sind und dass die Small Form-Factor Pluggables (SFPs), falls vorhanden, richtig auf beiden Controllern sitzen. Deaktivieren und aktivieren Sie intern verbundene Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. Wenn Links deaktiviert sind, aktivieren Sie die Links mit dem Befehl „ic link on“. Wenn kein Peer verbunden ist, deaktivieren und aktivieren Sie die Links nacheinander mit den Befehlen „ic link off“ und „ic link on“. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem weiterhin besteht.
-------------------------------	-------------------	---	--

CVO-Maximale Sitzungen pro Benutzer überschritten	WARNING (Warnung)	<p>Sie haben die maximal zulässige Anzahl von Sitzungen pro Benutzer über eine TCP-Verbindung überschritten. Jede Anfrage zum Herstellen einer Sitzung wird abgelehnt, bis einige Sitzungen freigegeben werden.</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie alle auf dem Client ausgeführten Anwendungen und beenden Sie alle, die nicht ordnungsgemäß funktionieren. Starten Sie den Client neu. Überprüfen Sie, ob das Problem durch eine neue oder vorhandene Anwendung verursacht wird: Wenn die Anwendung neu ist, legen Sie mit dem Befehl „cifs option modify -max-opens -same-file-per-tree“ einen höheren Schwellenwert für den Client fest. In einigen Fällen funktionieren die Clients wie erwartet, erfordern jedoch eine höhere Schwelle. Sie sollten über erweiterte Berechtigungen verfügen, um einen höheren Schwellenwert für den Client festzulegen. Wenn das Problem durch eine vorhandene Anwendung verursacht wird, liegt möglicherweise ein Problem mit dem Client vor. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.</p>
---	-------------------	---	---

CVO NetBIOS-Namenskonflikt	KRITISCH	Der NetBIOS-Namensdienst hat von einem Remotecomputer eine negative Antwort auf eine Namensregistrierungsanforderung erhalten. Dies wird normalerweise durch einen Konflikt im NetBIOS-Namen oder einem Alias verursacht. Dies hat zur Folge, dass Clients möglicherweise nicht auf Daten zugreifen oder keine Verbindung zum richtigen Datenbereitstellungsknoten im Cluster herstellen können.	Führen Sie eine der folgenden Korrekturmaßnahmen durch: Wenn ein Konflikt im NetBIOS-Namen oder einem Alias vorliegt, 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 um, 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 ein Konflikt im NetBIOS-Namen vorliegt, benennen Sie den CIFS-Server mit den Befehlen „vserver cifs delete -vserver vserver“ und „vserver cifs create -cifs -server netbiosname“ um. HINWEIS: Durch das Löschen eines CIFS-Servers kann der Zugriff auf die Daten unzugänglich werden. Entfernen Sie den NetBIOS-Namen oder benennen Sie das NetBIOS auf dem Remotecomputer um.
CVO NFSv4-Speicherpool erschöpft	KRITISCH	Ein NFSv4-Speicherpool ist erschöpft.	Wenn der NFS-Server nach diesem Ereignis länger als 10 Minuten nicht reagiert, wenden Sie sich an den technischen Support von NetApp .
CVO-Knotenpanik	WARNING (Warnung)	Dieses Ereignis wird ausgelöst, wenn eine Panik auftritt	Wenden Sie sich an den NetApp Kundensupport.

CVO-Knoten-Root-Volume-Speicherplatz niedrig	KRITISCH	Das System hat festgestellt, dass auf dem Stammvolume gefährlich wenig Speicherplatz vorhanden ist. Der Knoten ist nicht voll funktionsfähig. Möglicherweise ist innerhalb des Clusters ein Failover der Daten-LIFs aufgetreten, weshalb der NFS- und CIFS-Zugriff auf den Knoten eingeschränkt ist. Die Verwaltungsfunktionen sind auf lokale Wiederherstellungsverfahren für den Knoten beschränkt, um Speicherplatz auf dem Stammvolume freizugeben.	Führen Sie die folgenden Korrekturmaßnahmen durch: Schaffen Sie Speicherplatz auf dem Stammvolume, indem Sie alte Snapshot-Kopien löschen, nicht mehr benötigte Dateien aus dem Verzeichnis /mroot löschen oder die Kapazität des Stammvolumes erweitern. Starten 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 Client hat versucht, eine Verbindung zu einer nicht vorhandenen ONTAP_ADMIN\$-Freigabe herzustellen.	Stellen Sie sicher, dass Vscan für die angegebene SVM-ID aktiviert ist. Durch die Aktivierung von Vscan auf einer SVM wird die ONTAP_ADMIN\$-Freigabe automatisch für die SVM erstellt.
CVO Object Store Host nicht auflösbar	KRITISCH	Der Hostname des Objektspeicherservers kann nicht in eine IP-Adresse aufgelöst werden. Der Objektspeicherclient kann ohne Auflösung in eine IP-Adresse nicht mit dem Objektspeicherserver kommunizieren. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie die DNS-Konfiguration, um sicherzustellen, dass der Hostname korrekt mit einer IP-Adresse konfiguriert ist.

CVO Object Store Intercluster LIF Down	KRITISCH	Der Objektspeicher-Client kann kein funktionsfähiges LIF für die Kommunikation mit dem Objektspeicher-Server finden. Der Knoten lässt keinen Objektspeicher-Clientverkehr zu, bis das Intercluster-LIF betriebsbereit ist. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie den LIF-Status zwischen Clustern mit dem Befehl „network interface show -role intercluster“. Überprüfen Sie, ob das Intercluster-LIF richtig konfiguriert und betriebsbereit ist. Wenn kein Intercluster-LIF konfiguriert ist, fügen Sie es mit dem Befehl „network interface create -role intercluster“ hinzu.
CVO- Objektspeichersignatur stimmt nicht überein	KRITISCH	Die an den Objektspeicherserver gesendete Anforderungssignatur stimmt nicht mit der vom Client berechneten Signatur überein. Dies kann dazu führen, dass auf die Daten nicht zugegriffen werden kann.	Überprüfen Sie, ob der geheime Zugriffsschlüssel richtig konfiguriert ist. Wenn es richtig konfiguriert ist, wenden Sie sich an den technischen Support von NetApp, um Hilfe zu erhalten.
CVO QoS-Monitor- Speicher voll ausgelastet	KRITISCH	Der dynamische Speicher des QoS-Subsystems hat für die aktuelle Plattformhardware seine Grenze erreicht. Einige QoS-Funktionen sind möglicherweise nur eingeschränkt verfügbar.	Löschen Sie einige aktive Workloads oder Streams, um Speicher freizugeben. Verwenden Sie den Befehl „statistics show -object workload -counter ops“, um zu ermitteln, welche Workloads aktiv sind. Aktive Workloads zeigen Operationen ungleich Null. Verwenden Sie dann den Befehl „workload delete <workload_name>“ mehrmals, um bestimmte Workloads zu entfernen. Alternativ können Sie den Befehl „stream delete -workload <workload name> *“ verwenden, um die zugehörigen Streams aus der aktiven Workload zu löschen.

CVO READDIR- Zeitüberschreitung	KRITISCH	Ein READDIR- Dateivorgang hat das zulässige Zeitlimit für die Ausführung in WAFL überschritten. Dies kann an sehr großen oder spärlich gefüllten Verzeichnissen liegen. Es werden Korrekturmaßnahmen empfohlen.	Führen Sie die folgenden Korrekturmaßnahmen durch: Suchen Sie nach spezifischen Informationen zu aktuellen Verzeichnissen, bei denen READDIR-Dateivorgänge abgelaufen sind, indem Sie den folgenden NodeShell-CLI-Befehl mit der Berechtigung „diag“ verwenden: <code>wافل readdir notice show</code> . Überprüfen Sie, ob Verzeichnisse als spärlich gekennzeichnet sind oder nicht: Wenn ein Verzeichnis als spärlich gekennzeichnet ist, wird empfohlen, den Inhalt des Verzeichnisses in ein neues Verzeichnis zu kopieren, um die spärliche Verzeichnisdatei zu entfernen. Wenn ein Verzeichnis nicht als spärlich gekennzeichnet ist und das Verzeichnis groß ist, wird empfohlen, die Größe der Verzeichnisdatei zu reduzieren, indem Sie die Anzahl der Dateieinträge im Verzeichnis verringern.
------------------------------------	----------	---	---

<p>CVO-Verlagerung des Speicherpools fehlgeschlagen</p>	<p>KRITISCH</p>	<p>Dieses Ereignis tritt während der Verschiebung eines Aggregats auf, wenn der Zielknoten die Objektspeicher nicht erreichen kann.</p>	<p>Führen Sie die folgenden Korrekturmaßnahmen durch: Überprüfen Sie mit dem Befehl „Network Interface Show“, ob Ihr Intercluster-LIF online und funktionsfähig ist. Überprüfen Sie die Netzwerkkonnektivität zum Objektspeicherserver, indem Sie den Befehl „Ping“ über den Intercluster-LIF des Zielknotens verwenden. Überprüfen Sie mit dem Befehl „aggregate object-store config show“, ob sich die Konfiguration Ihres Objektspeichers geändert hat und ob die Anmelde- und Verbindungsinformationen noch immer korrekt sind. Alternativ können Sie den Fehler überschreiben, indem Sie den Parameter „override-destination-checks“ des Umzugsbefehls verwenden. Wenden Sie sich an den technischen Support von NetApp , um weitere Informationen oder Unterstützung zu erhalten.</p>
---	-----------------	---	---

CVO-Schattenkopie fehlgeschlagen	KRITISCH	Ein Volume Shadow Copy Service (VSS), ein Sicherungs- und Wiederherstellungsdienstvorgang von Microsoft Server, ist fehlgeschlagen.	Überprüfen Sie anhand der in der Ereignismeldung bereitgestellten Informationen Folgendes: Ist die Schattenkopiekonfiguration aktiviert? Sind die entsprechenden Lizenzen installiert? Auf welchen Freigaben wird der Schattenkopievorgang ausgeführt? Ist der Freigabename korrekt? Existiert der Freigabepfad? Wie ist der Status des Schattenkopiesatzes und seiner Schattenkopien?
CVO Storage VM-Stopp erfolgreich	INFO	Diese Meldung wird angezeigt, wenn ein „vServer-Stopp“-Vorgang erfolgreich ist.	Verwenden Sie den Befehl „vserver start“, um den Datenzugriff auf einer Speicher-VM zu starten.
CVO Zu viele CIFS-Authentifizierungen	WARNING (Warnung)	Viele Authentifizierungsverhandlungen fanden gleichzeitig statt. Von diesem Client liegen 256 unvollständige neue Sitzungsanforderungen vor.	Untersuchen Sie, warum der Client 256 oder mehr neue Verbindungsanforderungen erstellt hat. Möglicherweise müssen Sie sich an den Anbieter des Clients oder der Anwendung wenden, um die Ursache des Fehlers zu ermitteln.
Nicht zugewiesene CVO-Datenträger	INFO	Dem System sind keine Festplatten zugewiesen – Kapazität wird verschwendet und Ihr System weist möglicherweise eine Fehlkonfiguration auf oder es wurden teilweise Konfigurationsänderungen vorgenommen.	Führen Sie die folgenden Korrekturmaßnahmen durch: Ermitteln Sie mit dem Befehl „disk show -n“, welche Datenträger nicht zugewiesen sind. Weisen Sie die Datenträger mit dem Befehl „disk assign“ einem System zu.

CVO: Unbefugter Benutzerzugriff auf die Admin-Freigabe	WARNING (Warnung)	Ein Client hat versucht, eine Verbindung zur privilegierten Freigabe ONTAP_ADMIN\$ herzustellen, obwohl der angemeldete Benutzer kein zulässiger 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 aktuell aktive Scannerpool-Konfiguration mit dem Befehl „vserver vscan scanner pool show-active“.
CVO-Virus erkannt	WARNING (Warnung)	Ein Vscan-Server hat dem Speichersystem einen Fehler gemeldet. Dies weist normalerweise darauf hin, dass ein Virus gefunden wurde. Dieses Ereignis kann jedoch auch durch andere Fehler auf dem Vscan-Server verursacht werden. Der Clientzugriff auf die Datei wird verweigert. Der Vscan-Server kann die Datei je nach seinen Einstellungen und seiner Konfiguration bereinigen, unter Quarantäne stellen oder löschen.	Überprüfen Sie das im „Syslog“-Ereignis gemeldete Protokoll des Vscan-Servers, um festzustellen, ob die infizierte Datei erfolgreich bereinigt, unter Quarantäne gestellt oder gelöscht werden konnte. Wenn dies nicht möglich ist, muss ein Systemadministrator die Datei möglicherweise manuell löschen.
CVO-Volumen offline	INFO	Diese Meldung zeigt an, dass ein Volume offline geschaltet wurde.	Bringen Sie das Volume wieder online.
CVO-Volumen beschränkt	INFO	Dieses Ereignis zeigt an, dass ein flexibles Volumen eingeschränkt wird.	Bringen Sie das Volume wieder online.

[Zurück nach oben](#)

SnapMirror für Business Continuity (SMBC) Mediator Log Monitors

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
ONTAP Mediator hinzugefügt	INFO	Diese Meldung wird angezeigt, wenn ONTAP Mediator erfolgreich zu einem Cluster hinzugefügt wurde.	Keine

ONTAP Mediator nicht zugänglich	KRITISCH	Diese Meldung wird angezeigt, wenn entweder der ONTAP Mediator einem anderen Zweck zugeführt 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 mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
ONTAP Mediator entfernt	INFO	Diese Meldung wird angezeigt, wenn ONTAP Mediator erfolgreich aus einem Cluster entfernt wurde.	Keine
ONTAP Mediator nicht erreichbar	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn der ONTAP Mediator in einem Cluster nicht erreichbar ist. Daher ist ein SnapMirror Failover nicht möglich.	Überprüfen Sie die Netzwerkkonnektivität zum ONTAP Mediator mithilfe der Befehle „Network Ping“ und „Network Traceroute“. Wenn das Problem weiterhin besteht, entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC CA-Zertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues CA-Zertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

SMBC CA-Zertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das Zertifikat der ONTAP Mediator-Zertifizierungsstelle (CA) innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues CA-Zertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Client-Zertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Client-Zertifikat abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Client-Zertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das Client-Zertifikat des ONTAP Mediators innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

SMBC-Beziehung nicht synchron Hinweis: UM hat diese nicht	KRITISCH	Diese Meldung wird angezeigt, wenn sich der Status einer SnapMirror for Business Continuity (SMBC)-Beziehung von „synchronisiert“ in „nicht synchron“ ändert. Dadurch wird der Datenschutz bei RPO=0 gestört.	Überprüfen Sie die Netzwerkverbindung zwischen dem Quell- und dem Zielvolume. Überwachen Sie den SMBC-Beziehungsstatus, indem Sie auf dem Ziel den Befehl „snapmirror show“ und auf der Quelle den Befehl „snapmirror list-destinations“ verwenden. Durch die automatische Neusynchronisierung wird versucht, die Beziehung wieder in den Status „synchronisiert“ zu versetzen. Wenn die Neusynchronisierung fehlschlägt, überprüfen Sie, ob alle Knoten im Cluster im Quorum sind und fehlerfrei funktionieren.
SMBC-Serverzertifikat abgelaufen	KRITISCH	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Serverzertifikat abgelaufen ist. Infolgedessen ist jegliche weitere Kommunikation mit dem ONTAP Mediator nicht möglich.	Entfernen Sie die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues Serverzertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.
SMBC-Serverzertifikat läuft ab	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn das ONTAP Mediator-Serverzertifikat innerhalb der nächsten 30 Tage abläuft.	Entfernen Sie vor Ablauf dieses Zertifikats die Konfiguration des aktuellen ONTAP Mediators mit dem Befehl „snapmirror mediator remove“. Aktualisieren Sie ein neues Serverzertifikat auf dem ONTAP Mediator-Server. Konfigurieren Sie den Zugriff auf den ONTAP Mediator neu, indem Sie den Befehl „snapmirror mediator add“ verwenden.

Zusätzliche Strom-, Heartbeat- und sonstige Systemmonitore

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Disk Shelf-Stromversorgung entdeckt	INFORMATION	Diese Meldung wird angezeigt, wenn dem Festplattenregal ein Netzteil hinzugefügt wird.	KEINER
Stromversorgung der Festplattenregale entfernt	INFORMATION	Diese Meldung tritt auf, wenn ein Netzteil aus dem Festplattenregal entfernt wird.	KEINER
Automatische ungeplante Umschaltung von MetroCluster deaktiviert	KRITISCH	Diese Meldung wird angezeigt, wenn die Funktion zur automatischen ungeplanten Umschaltung deaktiviert ist.	Führen Sie den Befehl „metrocluster modify -node-name <Knotenname> -automatic -switchover-onfailure true“ für jeden Knoten im Cluster aus, um die automatische Umschaltung zu aktivieren.
MetroCluster Speicherbrücke nicht erreichbar	KRITISCH	Die Speicherbrücke ist über das Verwaltungsnetzwerk nicht erreichbar	1) Wenn die Bridge per SNMP überwacht wird, überprüfen Sie mit dem Befehl „Network Interface Show“, ob das Knotenverwaltungs-LIF aktiv ist. Überprüfen Sie mit dem Befehl „Netzwerk-Ping“, ob die Bridge aktiv ist. 2) Wenn die Bridge In-Band überwacht wird, überprüfen Sie die Fabric-Verkabelung zur Bridge und stellen Sie dann sicher, dass die Bridge eingeschaltet ist.
MetroCluster Bridge-Temperatur anormal – unter dem kritischen Wert	KRITISCH	Der Sensor auf der Fibre Channel Bridge meldet eine Temperatur, die unterhalb des kritischen Schwellenwerts liegt.	1) Überprüfen Sie den Betriebsstatus der Lüfter auf der Speicherbrücke. 2) Stellen Sie sicher, dass die Brücke unter den empfohlenen Temperaturbedingungen betrieben wird.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Temperatur der MetroCluster -Brücke abnormal – über dem kritischen Wert	KRITISCH	Der Sensor auf der Fibre Channel Bridge meldet eine Temperatur, die über dem kritischen Schwellenwert liegt.	1) Überprüfen Sie den Betriebsstatus des Gehäusetemperatursensors auf der Speicherbrücke mit dem Befehl „storage bridge show -cooling“. 2) Stellen Sie sicher, dass die Speicherbrücke unter den empfohlenen Temperaturbedingungen betrieben wird.
MetroCluster -Aggregat bleibt zurück	WARNING (Warnung)	Das Aggregat wurde beim Zurückfahren 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 Besitzer zurück.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Alle Verbindungen zwischen Metrocluster-Partnern unterbrochen	KRITISCH	RDMA-Verbindungsadapter und Intercluster-LIFs haben die Verbindung zum Peering-Cluster unterbrochen oder der Peering-Cluster ist ausgefallen.	1) Stellen Sie sicher, dass die Intercluster-LIFs betriebsbereit sind. Reparieren Sie die Intercluster-LIFs, wenn sie ausgefallen sind. 2) Überprüfen Sie mit dem Befehl „Cluster Peer Ping“, ob der Peering-Cluster betriebsbereit ist. Wenn der Peering-Cluster ausgefallen ist, lesen Sie den MetroCluster Disaster Recovery Guide. 3) Überprüfen Sie für Fabric MetroCluster, ob die Back-End-Fabric-ISLs betriebsbereit sind. Reparieren Sie die Back-End-Fabric-ISLs, wenn sie ausgefallen sind. 4) Überprüfen Sie bei MetroCluster-Konfigurationen ohne Fabric, ob die Verkabelung zwischen den RDMA-Verbindungsadaptern korrekt ist. Konfigurieren Sie die Verkabelung neu, wenn die Verbindungen unterbrochen sind.
MetroCluster Partner über Peering-Netzwerk nicht erreichbar	KRITISCH	Die Verbindung zum Peer-Cluster ist unterbrochen.	1) Stellen Sie sicher, dass der Port mit dem richtigen Netzwerk/Switch verbunden ist. 2) Stellen Sie sicher, dass das Intercluster-LIF mit dem Peered-Cluster verbunden ist. 3) Stellen Sie mit dem Befehl „Cluster Peer Ping“ sicher, dass der Peering-Cluster betriebsbereit ist. Wenn der Peering-Cluster ausgefallen ist, lesen Sie den MetroCluster Disaster Recovery Guide.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
MetroCluster Inter Switch: Alle Links ausgefallen	KRITISCH	Alle Inter-Switch Links (ISLs) auf dem Speicher-Switch sind ausgefallen.	1) Reparieren Sie die Back-End-Fabric-ISLs auf dem Speicher-Switch. 2) Stellen Sie sicher, dass der Partner-Switch aktiv ist und seine ISLs betriebsbereit sind. 3) Stellen Sie sicher, dass Zwischengeräte wie xWDM-Geräte betriebsbereit sind.
MetroCluster -Knoten zum Speicherstapel SAS-Verbindung unterbrochen	WARNING (Warnung)	Möglicherweise liegt ein Fehler am SAS-Adapter oder am daran angeschlossenen Kabel vor.	1. Stellen Sie sicher, dass der SAS-Adapter online und betriebsbereit ist. 2. Überprüfen Sie, ob die physische Kabelverbindung sicher und funktionsfähig ist, und ersetzen Sie das Kabel bei Bedarf. 3. Wenn der SAS-Adapter an Festplatten-Shelves angeschlossen ist, stellen Sie sicher, dass die IOMs und Festplatten richtig sitzen.
Links zum MetroClusterFC-Initiator ausgefallen	KRITISCH	Der FC-Initiatoradapter ist fehlerhaft.	1. Stellen Sie sicher, dass die FC-Initiatorverbindung nicht manipuliert wurde. 2. Überprüfen Sie den Betriebsstatus des FC-Initiatoradapters mit dem Befehl „system node run -node local -command storage show adapter“.
FC-VI-Verbindungsverbindung unterbrochen	KRITISCH	Die physische Verbindung am FC-VI-Port ist offline.	1. Stellen Sie sicher, dass die FC-VI-Verbindung nicht manipuliert wurde. 2. Überprüfen Sie mit dem Befehl „metrocluster interconnect adapter show“, ob der physische Status des FC-VI-Adapters „Aktiv“ lautet. 3. Wenn die Konfiguration Fabric-Switches umfasst, stellen Sie sicher, dass diese ordnungsgemäß verkabelt und konfiguriert sind.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Zurückgelassene MetroCluster -Ersatzfestplatten	WARNING (Warnung)	Die Ersatzfestplatte wurde beim Switchback zurückgelassen.	Wenn die Festplatte nicht ausgefallen ist, geben Sie sie mit dem Befehl „metrocluster switchback“ an ihren ursprünglichen Besitzer zurück.
MetroCluster Speicherbrücken-Port ausgefallen	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) Überprüfen Sie die logische und physische Konnektivität zum Port.
Lüfter des MetroCluster Speicher-Switches ausgefallen	KRITISCH	Der Lüfter am Speicherschalter ist ausgefallen.	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 richtig eingesetzt und betriebsbereit sind.
MetroCluster Speicher-Switch nicht erreichbar	KRITISCH	Der Speicher-Switch ist über das Verwaltungsnetzwerk nicht erreichbar.	1) Stellen Sie sicher, dass das Knotenverwaltungs-LIF aktiv ist, indem Sie den Befehl „Network Interface Show“ verwenden. 2) Stellen Sie mit dem Befehl „Netzwerk-Ping“ sicher, dass der Switch aktiv ist. 3) Stellen Sie sicher, dass der Switch über SNMP erreichbar ist, indem Sie nach der Anmeldung beim Switch seine SNMP-Einstellungen überprüfen.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Stromversorgung des MetroCluster -Switches ausgefallen	KRITISCH	Ein Netzteil am Speicherswitch ist nicht betriebsbereit.	1) Überprüfen Sie die Fehlerdetails mit dem Befehl „storage switch show -error -switch-name <switch 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.
Temperatursensoren des MetroCluster -Switches ausgefallen	KRITISCH	Der Sensor am Fibre-Channel-Switch ist ausgefallen.	1) Überprüfen Sie den Betriebszustand der Temperatursensoren am Speicherswitch mit dem Befehl „storage switch show -cooling“. 2) Stellen Sie sicher, dass der Schalter unter den empfohlenen Temperaturbedingungen arbeitet.
MetroCluster -Switch -Temperatur abnormal	KRITISCH	Der Temperatursensor am Fibre-Channel-Switch hat eine abnormale Temperatur gemeldet.	1) Überprüfen Sie den Betriebszustand der Temperatursensoren am Speicherswitch mit dem Befehl „storage switch show -cooling“. 2) Stellen Sie sicher, dass der Schalter unter den empfohlenen Temperaturbedingungen arbeitet.

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Heartbeat des Serviceprozessors verpasst	INFORMATIONEN	Diese Meldung wird angezeigt, wenn ONTAP kein erwartetes „Heartbeat“-Signal vom Serviceprozessor (SP) empfängt. Zusammen mit dieser Nachricht werden Protokolldateien vom SP zum Debuggen gesendet. ONTAP setzt den SP zurück, um zu versuchen, die Kommunikation wiederherzustellen. Während des Neustarts ist der SP bis zu zwei Minuten lang nicht verfügbar.	Wenden Sie sich an den technischen Support von NetApp .

Monitorname	Schwere	Monitorbeschreibung	Korrekturmaßnahme
Heartbeat des Serviceprozessors gestoppt	WARNING (Warnung)	Diese Meldung wird angezeigt, wenn ONTAP keine Heartbeats mehr vom Serviceprozessor (SP) empfängt. Je nach Hardwaredesign kann das System weiterhin Daten bereitstellen oder sich zum Herunterfahren entschließen, um Datenverlust oder Hardwareschäden zu verhindern. Das System stellt weiterhin Daten bereit, aber da der SP möglicherweise nicht funktioniert, kann das System keine Benachrichtigungen über ausgefallene Geräte, Startfehler oder Power-On Self-Test (POST)-Fehler der Open Firmware (OFW) senden. Wenn Ihr System entsprechend konfiguriert ist, generiert und überträgt es eine AutoSupport Nachricht (oder „Call Home“-Nachricht) an den technischen Support von NetApp und an die konfigurierten Ziele. Die erfolgreiche Übermittlung einer AutoSupport -Nachricht verbessert die Problembestimmung und -lösung erheblich.	Wenn das System heruntergefahren wurde, versuchen Sie einen Hard Power Cycle: Ziehen Sie den Controller aus dem Gehäuse, drücken Sie ihn wieder hinein und schalten Sie dann das System ein. Wenden Sie sich an den technischen Support von NetApp, wenn das Problem nach dem Aus- und Wiedereinschalten weiterhin besteht oder wenn ein anderer Zustand vorliegt, der Ihre Aufmerksamkeit erfordert.

[Zurück nach oben](#)

Weitere Informationen

- ["Anzeigen und Verwerfen von Warnungen"](#)

Webhook-Benachrichtigungen

Benachrichtigung mittels Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, beispielsweise: Slack, PagerDuty, Teams und Discord unterstützen alle Webhooks. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Data Infrastructure Insights viele dieser Bereitstellungskanäle unterstützen. Informationen zu Webhooks finden Sie auf diesen Anwendungswebsites. Slack bietet beispielsweise ["dieser nützliche Leitfaden"](#) .

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck dient: separaten Anwendungen, verschiedenen Empfängern usw.

Die Webhook-Kanalinstanz besteht aus den folgenden Elementen:

Name	Eindeutiger Name
URL	Webhook-Ziel-URL, einschließlich des Präfixes <i>http://</i> oder <i>https://</i> zusammen mit den URL-Parametern
Verfahren	GET, POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Kopfzeilen an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

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

Das folgende Bild zeigt ein Beispiel für einen für Slack konfigurierten Webhook:

Edit a Webhook

Name

Slack Test

Template Type

Slack

URL

https://hooks.slack.com/services/<token>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "**Cloud Insights Alert - %%%alertid%%%\nSeverity - *%%severity%%**"
      }
    }
  ],
  "type": "mrkdwn"
}
```

Cancel

Test Webhook

Save Webhook

Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie nach Abschluss auf „Speichern“.

Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.

Data Infrastructure Insights -Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten 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 <code>https://%%cloudInsightsHostName%%%%alertRelativeUrl%%</code>
%%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 verwende ich sie?

Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter `%%TriggeredOn%%` durch das Objekt ersetzt, bei dem der Alarm ausgelöst wurde.

Sie können einem Webhook jedes beliebige Objektattribut (z. B. Speichernamen) als Parameter hinzufügen. Sie können beispielsweise Parameter für den Volumenamen und den Speichernamen in einer Webhook-Beschreibung wie folgt festlegen: „Hohe Latenz für Volume: `%%relatedObject.volume.name%%`, Speicher: `%%relatedObject.storage.name%%`“.

Beachten Sie, dass in diesem Abschnitt beim Klicken auf die Schaltfläche „Webhook testen“ *keine* Ersetzungen durchgeführt werden. Die Schaltfläche sendet eine Nutzlast, die die %% Ersetzungen anzeigt, sie jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Aus Sicherheitsgründen kann nur der Ersteller des Webhooks diesen Webhook-Kanal ändern, wenn ein Geheimnis definiert ist. Für andere ist es schreibgeschützt. Sie können Geheimnisse in URLs/Headern als %%<secret_name>%% verwenden.

Webhooks-Listenseite

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt.

Auswählen einer Webhook-Benachrichtigung in einem Monitor

Um die Webhook-Benachrichtigung in einem **"Monitor"**, gehen Sie zu **Warnungen > Monitore verwalten** und wählen Sie den gewünschten Monitor aus oder fügen Sie einen neuen Monitor hinzu. Wählen Sie im Abschnitt „Teambenachrichtigungen einrichten“ „Webhook“ als Übermittlungsmethode. Wählen Sie die Warnstufen (Kritisch, Warnung, Gelöst) und dann den gewünschten Webhook aus.

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook

Notify team on

Critical, Warning, Resolved

Use Webhook

Please Select

Search...

ci-alerts-notifications-dev

ci-alerts-notifications-qa

Webhook-Beispiele:

Webhooks für ["Locker"](#) Webhooks für ["PagerDuty"](#) Webhooks für ["Teams"](#) Webhooks für ["Zwietracht"](#)

Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im ["Discord-Dokumentation"](#) für die aktuellsten Informationen.

Discord-Setup:

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

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

Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Discord“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.

Edit a Webhook

Name

Discord Webhook

Template Type

Discord ▼

URL

https://discord.com/api/webhooks/<token string>

Method

POST ▼

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%%severity%% | %%alertId%% | %%triggeredOn%%",
      "description": "%%monitorName%%",
      "url": "https://%%cloudInsightsHostname%%/%%alertRelativeUrl%%",
      "color": 3244733,
      "fields": [
        {
          "name": "%%metricName%%"
```

Cancel

Test Webhook

Save Webhook



Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. <https://netapp.com>) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen "Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Discord“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)

3 Set up team notification(s) (alert your team via email, or Webhook)

Webhook-Beispiel für PagerDuty

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für PagerDuty.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im "[PagerDuty-Dokumentation](#)" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Klicken Sie auf *Dienst hinzufügen*.

Add a Service

A service may represent an application, component or team you wish to open incidents against.

General Settings


Name


Description

Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for [change events](#).

Integration Type 

☐ Select a tool 

PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines. This may involve configuration steps in the tool you are integrating with PagerDuty.

☐ Integrate via email


If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

☒ Use our API directly

If you're writing your own integration, use our Events API. More information is in our developer documentation.

☐ Don't use an integration

If you only want incidents to be manually created. You can always add additional integrations later.

Events API v2 


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


PagerDuty [Incidents](#) [Services](#) [People](#) [Analytics](#) [Status](#)

Incidents on All Teams

Your open incidents: 4 triggered, 2 acknowledged

All open incidents: 4 triggered, 2 acknowledged

1 acknowledged 20 triggered 47 resolved 10 Service - 

Go to incident #  All Teams

[Open](#) [Triggered](#) [Acknowledged](#) [Resolved](#) [Any Status](#) [Assigned to me](#) [All](#)

<input type="checkbox"/> Status	Urgency	Title	Details	Service	Assigned To
<input checked="" type="checkbox"/> Triggered	High	WARNING! AL-18 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-20 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-19 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-17 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-16 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-15 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-14 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-13 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-12 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-11 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-10 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-09 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-08 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-07 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-06 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-05 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-04 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-03 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-02 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung
<input type="checkbox"/> Triggered	High	WARNING! AL-01 / aggregate_name_team02test ID: 6400-007x1C3 / triggered-yes	at 5:48 PM	Test3	Edwin Chung


Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „PagerDuty Trigger“. Sie verwenden diesen Webhook für Ereignisse der Stufen „kritisch“ und „Warnung“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „PagerDuty“ aus.
4. Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den PagerDuty-*Integrationsschlüssel*-Wert von oben fest.

Custom Parameters and Secrets

Name	Value ↑	Description
%%routingKey%%	*****	⋮

+ Parameter

Name 	Value
<input type="text" value="routingKey"/>	<input type="text" value="....."/>
Type	Description
<input type="text" value="Secret"/>	<div></div>

Cancel

Save Parameter

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

PagerDuty zur Data Infrastructure Insights -Feldzuordnung

Die folgende Tabelle und das Bild zeigen die Zuordnung der Felder zwischen PagerDuty und Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Alarmschlüssel	Warnmeldungs-ID
Quelle	Ausgelöst am
Komponente	Metrikname
Gruppe	Objekttyp

PagerDuty	Data Infrastructure Insights
Klasse	Monitorname

Message Body



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

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen "Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den Webhook „PagerDuty Trigger“ für Ereignisse der Stufen „Kritisch“ und „Warnung“.
- Wählen Sie „PagerDuty Resolve“ für gelöste Ereignisse.

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook	Notify team on <div>Critical, Warning ▼</div>	Use Webhook(s)  <div>PagerDuty Trigger x ▼</div>
	Notify team on <div>Resolved ▼</div>	Use Webhook(s)  <div>PagerDuty Resolve x ▼</div>



Das Festlegen separater Benachrichtigungen für Trigger-Ereignisse im Vergleich zu aufgelösten Ereignissen ist eine bewährte Methode, da PagerDuty Trigger-Ereignisse anders behandelt als aufgelöste Ereignisse.

Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im "[Slack-Dokumentation](#)" für die aktuellsten Informationen.

Slack-Beispiel:

- Gehe zu <https://api.slack.com/apps> und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie den Slack-Arbeitsbereich aus.

Create a Slack App ×

App Name

e.g. Super Service

Don't worry; you'll be able to change this later.

Development Slack Workspace

Development Slack Workspace ▼

Your app belongs to this workspace—leaving this workspace will remove your ability to manage this app. Unfortunately, this can't be changed later.

By creating a Web API Application, you agree to the [Slack API Terms of Service](#).

CancelCreate App

- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, „Anforderung zum Hinzufügen eines neuen Webhooks“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Webhook-Konfiguration von Data Infrastructure Insights einfügen.

Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Slack Webhook“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Slack** aus.
4. Fügen Sie die URL von oben in das Feld *URL* ein.

Edit a Webhook

Name

Slack

Template Type

Slack ▼

URL

https://hooks.slack.com/services/<token string>

Method

POST ▼

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "blocks":[
    {
      "type":"section",
      "text":{
        "type":"mrkdwn",
        "text":"*Cloud Insights Alert - %%alertId%%*  
Severity - *%%severity%%*"
      }
    }
  ],
  ...
}
```

Cancel

Test Webhook

Save Webhook

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen "Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Slack“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook	Notify team on Critical, Warning, Resolved ▼	Use Webhook(s) Slack x ▼
------------	---	-----------------------------

Weitere Informationen:

- Informationen zum Ändern des Nachrichtenformats und -layouts finden Sie unter <https://api.slack.com/messaging/composing>
- Fehlerbehandlung: https://api.slack.com/messaging/webhooks#handling_errors

Webhook-Beispiel für Microsoft Teams

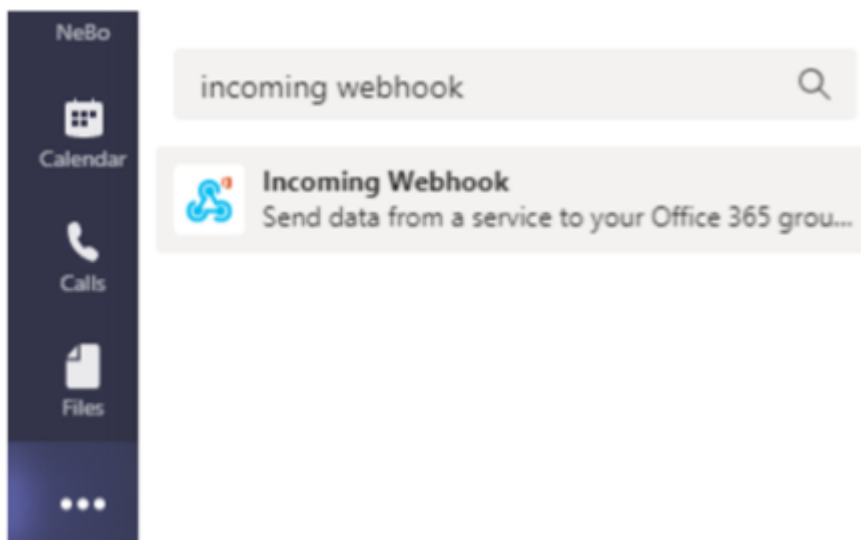
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Teams.



Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen können. Weitere Informationen finden Sie im "[Teams-Dokumentation](#)" für die aktuellsten Informationen.

Teams-Setup:

1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Webhook-Konfiguration von Data Infrastructure Insights einfügen.

Erstellen Sie einen Data Infrastructure Insights -Webhook:

1. Navigieren Sie in Data Infrastructure Insights zu **Admin > Benachrichtigungen** und wählen Sie die Registerkarte **Webhooks** aus. Klicken Sie auf **+Webhook**, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen, beispielsweise „Teams Webhook“.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.

Edit a Webhook

Name

Template Type

Teams ▼

URL

Method

POST ▼

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "@type": "MessageCard",
  "@context": "http://schema.org/extensions",
  "themeColor": "0076D7",
  "summary": "Cloud Insights Alert",
  "sections": [
    {
      "activityTitle": "%%severity%% | %%alertid%% | %%triggeredOn%%",
      "activitySubtitle": "%%triggerTime%%",
      "markdown": false,
      "facts": [
```

Cancel Test Webhook Save Webhook

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

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook zu benachrichtigen, navigieren Sie in Data Infrastructure Insights zu **Alerts > Monitors** und klicken Sie auf **+Monitor**, um einen neuen "Monitor" .

- Wählen Sie eine Metrik aus und definieren Sie die Bedingungen des Monitors.
- Wählen Sie unter „Teambenachrichtigung(en) einrichten“ die Übermittlungsmethode „Webhook“ aus.
- Wählen Sie den „Teams“-Webhook für die gewünschten Ereignisse (Kritisch, Warnung, Gelöst)

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook

Notify team on

Critical, Warning, Resolved

Use Webhook(s)

Teams - Edwin x

Arbeiten mit Anmerkungen

Anmerkungen definieren

Wenn Sie Data Infrastructure Insights anpassen, um Daten für Ihre Unternehmensanforderungen zu verfolgen, können Sie spezielle Notizen, sogenannte Anmerkungen, definieren und sie Ihren Assets zuweisen.

Sie können Assets Anmerkungen mit Informationen wie dem Ende der Lebensdauer des Assets, dem Rechenzentrum, dem Gebäudestandort, der Speicherebene oder dem Volume-Servicelevel zuweisen.

Die Verwendung von Anmerkungen zur Überwachung Ihrer Umgebung umfasst die folgenden übergeordneten Aufgaben:

- Erstellen oder Bearbeiten von Definitionen für alle Anmerkungstypen.
- Anzeigen von Asset-Seiten und Zuordnen jedes Assets zu einer oder mehreren Anmerkungen.

Wenn beispielsweise ein Vermögenswert geleast wird und der Leasingvertrag innerhalb von zwei Monaten abläuft, möchten Sie dem Vermögenswert möglicherweise eine End-of-Life-Anmerkung hinzufügen. Dadurch wird verhindert, dass andere dieses Gut über einen längeren Zeitraum hinweg verwenden.

- Erstellen von Regeln zum automatischen Anwenden von Anmerkungen auf mehrere Assets desselben Typs.
- Filtern Sie Assets nach ihren Anmerkungen.

Standard-Annotationstypen

Data Infrastructure Insights bietet einige Standardanmerkungstypen. Diese Anmerkungen können zum Filtern oder Gruppieren von Daten verwendet werden.

Sie können Assets mit Standardanmerkungstypen wie den folgenden verknüpfen:

- Lebenszyklus von Anlagen, z. B. Geburtstag, Sonnenuntergang oder Ende der Lebensdauer
- Standortinformationen zu einem Gerät, z. B. Rechenzentrum, Gebäude oder Stockwerk
- Klassifizierung von Assets, beispielsweise nach Qualität (Tiers), nach angeschlossenen Geräten (Switch-Level) oder nach Service-Level
- Status, z. B. „heiß“ (hohe Auslastung)

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

Anmerkungstypen	Beschreibung	Typ
Alias	Benutzerfreundlicher Name für eine Ressource	Text
Compute-Ressourcengruppe	Vom Host- und VM-Dateisystem-Datensammler verwendete Gruppenzuweisung	Liste
Rechenzentrum	Physischer Standort	Liste
Heiß	Geräte, die regelmäßig stark beansprucht werden oder an der Grenze ihrer Kapazität stehen	Boolescher Wert
Hinweis	Mit einer Ressource verknüpfte Kommentare	Prüfen
Service-Level	Eine Reihe unterstützter Servicelevel, die Sie Ressourcen zuweisen können. Bietet eine geordnete Optionsliste für interne Volumes, Qtree und Volumes. Bearbeiten Sie Service-Levels, um Leistungsrichtlinien für verschiedene Level festzulegen.	Liste
Sonnenuntergang	Festgelegter Schwellenwert, nach dessen Überschreitung keine neuen Zuweisungen mehr zu diesem Gerät vorgenommen werden können. Nützlich für geplante Migrationen und andere anstehende Netzwerkänderungen.	Datum
Schalterebene	Vordefinierte Optionen zum Einrichten von Kategorien für Schalter. Normalerweise bleiben diese Bezeichnungen für die gesamte Lebensdauer des Geräts bestehen, Sie können sie jedoch bearbeiten. Nur für Schalter verfügbar.	Liste
Stufe	Kann verwendet werden, um verschiedene Serviceebenen innerhalb Ihrer Umgebung zu definieren. Mit den Stufen kann die Art des Levels definiert werden, beispielsweise die erforderliche Geschwindigkeit (z. B. Gold oder Silber). Diese Funktion ist nur auf internen Volumes, Qtrees, Speicher-Arrays, Speicherpools und Volumes verfügbar.	Liste
Schweregrad des Verstoßes	Rang (z. B. schwerwiegend) eines Verstoßes (z. B. fehlende Host-Ports oder fehlende Redundanz) in einer Hierarchie von der höchsten bis zur niedrigsten Wichtigkeit.	Liste



Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Tier und Violation Severity sind Anmerkungen auf Systemebene, die Sie nicht löschen oder umbenennen können. Sie können nur die ihnen zugewiesenen Werte ändern.

Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Anmerkungen können Sie den Assets benutzerdefinierte, geschäftsspezifische Daten hinzufügen, die Ihren Geschäftsanforderungen entsprechen. Obwohl Data Infrastructure Insights eine Reihe von Standardanmerkungen bereitstellt, möchten Sie die Daten möglicherweise auf andere Weise anzeigen. Die Daten in benutzerdefinierten Anmerkungen ergänzen bereits erfasste Gerätedaten, wie etwa Speicherhersteller, Anzahl der Datenträger und Leistungsstatistiken. Die Daten, die Sie mithilfe von Anmerkungen hinzufügen, werden von Data Infrastructure Insights nicht erkannt.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerkungen**.

Auf der Seite „Anmerkungen“ wird die Liste der Anmerkungen angezeigt.

2. Klicken Sie auf **+Hinzufügen**

3. Geben Sie einen **Namen** 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 Dropdownliste mit den Auswahlmöglichkeiten „Ja“ und „Nein“. Beispielsweise ist die Anmerkung „Direkt verbunden“ boolesch.
- **Datum:** Dadurch wird ein Feld erstellt, das ein Datum enthält. Wenn die Anmerkung beispielsweise ein Datum sein soll, wählen Sie dies aus.
- **Liste:** Erstellt eines der folgenden Elemente:

- Eine Dropdown-Liste mit festen

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

- Eine flexible Dropdown-Liste

Wenn Sie beim Erstellen dieser Liste die Option „Neue Werte spontan hinzufügen“ auswählen, können andere Personen, die diesen Anmerkungstyp einem Gerät zuweisen, der Liste weitere Werte hinzufügen.

- **Nummer:** Erstellt ein Feld, in das der Benutzer, der die Anmerkung zuweist, eine Nummer eingeben kann. Wenn der Anmerkungstyp beispielsweise „Etagé“ ist, kann der Benutzer den Werttyp „Nummer“ auswählen und die Etagennummer eingeben.
- **Text:** Erstellt ein Feld, das Freitext zulässt. Sie können beispielsweise „Sprache“ als Anmerkungstyp eingeben, „Text“ als Werttyp auswählen und eine Sprache als Wert eingeben.



Nachdem Sie den Typ festgelegt und Ihre Änderungen gespeichert haben, können Sie den Typ der Anmerkung nicht mehr 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 wie folgt vor:
 - a. Wählen Sie **Neue Werte spontan hinzufügen**, wenn Sie der Anmerkung auf einer Asset-Seite weitere Werte hinzufügen möchten, wodurch eine flexible Liste erstellt wird.

Angenommen, Sie befinden sich auf einer Asset-Seite und das Asset verfügt über die Stadtanmerkung mit den Werten Detroit, Tampa und Boston. Wenn Sie die Option **Neue Werte spontan hinzufügen** ausgewählt haben, können Sie der Stadt zusätzliche Werte wie San Francisco und Chicago direkt auf der Asset-Seite hinzufügen, anstatt sie auf der Anmerkungsseite hinzufügen zu müssen. Wenn Sie diese Option nicht wählen, können Sie beim Anwenden der Annotation keine neuen Annotationswerte hinzufügen. Dadurch wird eine feste Liste erstellt.

- b. Geben Sie in die Felder **Wert** und **Beschreibung** einen Wert und eine Beschreibung ein.
- c. Klicken Sie auf **Hinzufügen**, um weitere Werte hinzuzufügen.
- d. Klicken Sie auf das Papierkorbsymbol, um einen Wert zu löschen.

2. Klicken Sie auf **Speichern**

Ihre Anmerkungen werden in der Liste auf der Anmerkungsseite angezeigt.

Ein Hinweis zu Booleschen Anmerkungen

Beim Filtern nach einer Booleschen Anmerkung werden Ihnen möglicherweise die folgenden Werte zum Filtern angezeigt:

- **Beliebig:** Dies gibt *alle* Ergebnisse zurück, einschließlich der Ergebnisse, die auf „Ja“, „Nein“ oder gar nicht festgelegt sind.
- **Ja:** Gibt nur „Ja“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Ja“ als Häkchen anzeigt. Die Werte können auf „True“, „On“ usw. gesetzt werden; DII behandelt alle diese Werte als „Yes“.
- **Nein:** Gibt nur „Nein“-Ergebnisse zurück. Beachten Sie, dass DII in den meisten Tabellen „Nein“ als „X“ anzeigt. Die Werte können auf „Falsch“, „Aus“ usw. gesetzt werden; DII behandelt alle diese Werte als „Nein“.
- **Keine:** Gibt nur Ergebnisse zurück, bei denen die Anmerkung überhaupt nicht festgelegt wurde. Auch als „Null“-Werte bezeichnet.

Nach Abschluss

In der Benutzeroberfläche steht die Anmerkung sofort zur Verwendung bereit.

Verwenden von Anmerkungen

Sie erstellen Anmerkungen und weisen sie den von Ihnen überwachten Assets zu. Anmerkungen sind Hinweise, die Informationen zu einem Asset liefern, beispielsweise den physischen Standort, das Ende der Lebensdauer, die Speicherebene oder die Volumen-Servicelevel.

Anmerkungen definieren

Mithilfe von Anmerkungen können Sie den Assets benutzerdefinierte, geschäftsspezifische Daten hinzufügen, die Ihren Geschäftsanforderungen entsprechen. Obwohl Data Infrastructure Insights eine Reihe von Standardanmerkungen bereitstellt, wie etwa den Lebenszyklus der Anlage (Geburtsstag oder Ende der Lebensdauer), den Standort des Gebäudes oder Rechenzentrums und die Ebene, möchten Sie die Daten möglicherweise auf andere Weise anzeigen.

Die Daten in benutzerdefinierten Anmerkungen ergänzen bereits erfasste Gerätedaten, wie etwa Switch-Hersteller, Anzahl der Ports und Leistungsstatistiken. Die Daten, die Sie mithilfe von Anmerkungen hinzufügen, werden von Data Infrastructure Insights nicht erkannt.

Bevor Sie beginnen

- Listen Sie alle Branchenterminologien auf, mit denen Umgebungsdaten verknüpft werden müssen.
- Listen Sie die Unternehmensterminologie auf, mit der Umgebungsdaten verknüpft werden müssen.
- Identifizieren Sie alle Standardanmerkungstypen, die Sie möglicherweise 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 „Data Infrastructure Insights“ auf **Observability > Enrich > Annotations**
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 Textanmerkung zu erstellen, die den physischen Standort eines Assets im Rechenzentrum 4 definiert:

- Geben Sie einen Namen für die Anmerkung ein, beispielsweise „Standort“.
- Geben Sie eine Beschreibung der Anmerkung ein, z. B. „Physischer Standort ist Rechenzentrum 4“.
- Geben Sie den „Typ“ der Anmerkung ein, beispielsweise „Text“.

Manuelles Zuweisen von Anmerkungen zu Assets

Durch die Zuweisung von Anmerkungen zu Anlagen können Sie Anlagen auf für Ihr Unternehmen relevante Weise sortieren, gruppieren und darüber berichten. Obwohl Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen zu Assets eines bestimmten Typs zuweisen können, können Sie Anmerkungen zu einem einzelnen Asset über die Asset-Seite zuweisen.

Bevor Sie beginnen

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

Schritte

1. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an.
2. Suchen Sie das Asset, auf das Sie die Anmerkung anwenden möchten.
 - Sie können Assets durch Abfragen, Auswählen aus einem Dashboard-Widget oder Suchen finden. Wenn Sie das gewünschte Asset gefunden haben, klicken Sie auf den Link, um die Zielseite des Assets zu öffnen.
3. Klicken Sie auf der Asset-Seite 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 je nach ausgewähltem Anmerkungstyp einen der folgenden Schritte aus:
 - Wenn der Anmerkungstyp „Liste“, „Datum“ oder „Boolesch“ ist, wählen Sie einen Wert aus der Liste aus.
 - Wenn der Anmerkungstyp Text ist, 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 Typ Liste ist und die Option „Neue Werte spontan hinzufügen“ ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

Zuweisen von Anmerkungen mithilfe von Anmerksungsregeln

Um Assets basierend auf von Ihnen definierten Kriterien automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerksungsregeln. Data Infrastructure Insights weist die Anmerkungen den Assets basierend auf diesen Regeln zu. Data Infrastructure Insights bietet außerdem zwei Standardanmerksungsregeln, die Sie Ihren Anforderungen entsprechend ändern oder entfernen können, wenn Sie sie nicht verwenden möchten.

Erstellen von Anmerksungsregeln

Als Alternative zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerksungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Manuell auf einzelnen Asset-Seiten festgelegte Anmerkungen haben Vorrang vor regelbasierten Anmerkungen, wenn Insight die Anmerksungsregeln auswertet.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerksungsregel erstellt haben.

Informationen zu diesem Vorgang

Obwohl Sie die Anmerkungstypen beim Erstellen der Regeln bearbeiten können, sollten Sie die Typen vorher definiert haben.

Schritte

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

Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

2. Klicken Sie auf **+ Hinzufügen**.

3. Gehen Sie folgendermaßen vor:

- a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

Dieser Name wird auf der Seite „Annotationsregeln“ angezeigt.

- b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die zum Anwenden der Anmerkung auf Assets verwendet wird.
- c. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie anwenden möchten.
- d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

Wenn Sie beispielsweise „Geburtsdag“ als Anmerkung wählen, geben Sie ein Datum für den Wert an.

- e. Klicken Sie auf **Speichern**

- f. Klicken Sie auf **Alle Regeln ausführen**, wenn Sie alle Regeln sofort ausführen möchten. Andernfalls werden die Regeln in regelmäßigen Abständen ausgeführt.

Erstellen von Anmerksungsregeln

Mithilfe von Anmerksungsregeln können Sie Anmerkungen basierend auf den von Ihnen definierten Kriterien automatisch auf mehrere Assets anwenden. Data Infrastructure Insights weist die Anmerkungen den Assets basierend auf diesen Regeln zu. Manuell auf einzelnen Asset-Seiten festgelegte Anmerkungen haben Vorrang vor regelbasierten Anmerkungen, wenn Cloud Insight die Anmerksungsregeln auswertet.

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerksungsregel erstellt haben.

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerksungsregeln**.
2. Klicken Sie auf **+ Regel**, um eine neue Anmerksungsregel hinzuzufügen.

Das Dialogfeld „Regel hinzufügen“ wird angezeigt.

3. Gehen Sie folgendermaßen vor:

- a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

Der Name wird auf der Seite „Anmerksungsregeln“ angezeigt.

- b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die Data Infrastructure Insights verwendet, um die Assets zu identifizieren, auf die sich die Anmerkung bezieht.
- c. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie anwenden möchten.
- d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

Wenn Sie beispielsweise „Geburtstag“ als Anmerkung wählen, geben Sie ein Datum für den Wert an.

- e. Klicken Sie auf **Speichern**

- f. Klicken Sie auf **Alle Regeln ausführen**, wenn Sie alle Regeln sofort ausführen möchten. Andernfalls werden die Regeln in regelmäßigen Abständen ausgeführt.



In einer großen Data Infrastructure Insights -Umgebung stellen Sie möglicherweise fest, dass die Ausführung von Anmerksungsregeln eine Weile zu dauern scheint. Dies liegt daran, dass der Indexer zuerst ausgeführt wird und vor der Ausführung der Regeln abgeschlossen sein muss. Der Indexer gibt Data Infrastructure Insights die Möglichkeit, in Ihren Daten nach neuen oder aktualisierten Objekten und Zählern zu suchen oder diese zu filtern. Die Regel-Engine wartet, bis der Indexer seine Aktualisierung abgeschlossen hat, bevor sie die Regeln anwendet.

Ändern von Anmerksungsregeln

Sie können eine Anmerksungsregel 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 Data Infrastructure Insights -Menü auf **Verwalten > Anmerksungsregeln**.

Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

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

Sie können die Anmerksungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerksungsregeln seitenweise 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 Anmerkung, den Wert oder die Abfrage der Anmerksungsregel.

Ändern der Reihenfolge der Regeln

Anmerksungsregeln werden von oben nach unten in der Regelliste 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 je nach Bedarf auf **Nach oben verschieben** oder **Nach unten verschieben**, bis die Regel an der gewünschten Stelle angezeigt wird.

Beachten Sie, dass beim Ausführen mehrerer Regeln, die dieselbe Anmerkung zu einem Asset aktualisieren, die erste Regel (von oben nach unten ausgeführt) die Anmerkung anwendet und das Asset aktualisiert. Anschließend wird die zweite Regel angewendet, ändert jedoch keine Anmerkungen, die bereits von der vorherigen Regel festgelegt wurden.

Löschen von Anmerksungsregeln

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

Schritte

1. Klicken Sie im Data Infrastructure Insights -Menü auf **Verwalten > Anmerksungsregeln**.

Auf der Seite „Annotationsregeln“ wird die Liste der vorhandenen Annotationsregeln angezeigt.

2. Suchen Sie die Anmerksungsregel, die Sie löschen möchten.

Sie können die Anmerksungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben oder auf eine Seitenzahl klicken, um die Anmerksungsregeln seitenweise 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 importieren

Data Infrastructure Insights enthält eine API zum Importieren von Anmerkungen oder Anwendungen aus einer CSV-Datei und zum Zuweisen dieser zu von Ihnen angegebenen Objekten.



Die Data Infrastructure Insights API ist in der * Data Infrastructure Insights Premium Edition* verfügbar.

Importieren

Die Links **Admin > API-Zugriff** enthalten "[Dokumentation](#)" für die **Assets/Import-API**. Diese Dokumentation enthält Informationen zum CSV-Dateiformat.

ASSETS.import

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

```
Project
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>
```

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. Anschließend folgen für jede Anmerkung bzw. Anwendung separate Zeilen. Sie müssen nicht jedes Feld definieren. Die nachfolgenden Anmerkungszeilen müssen jedoch der gleichen Reihenfolge wie die Definitionszeile folgen.

```
[Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type, ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
```

Beispiele für CSV-Dateien finden Sie in der API-Dokumentation.

Sie können Anmerkungen aus einer CSV-Datei direkt aus dem API-Swagger importieren und zuweisen. Wählen Sie einfach die zu verwendende Datei aus und klicken Sie auf die Schaltfläche *Ausführen*:

Parameters

Cancel

No parameters

Request body

multipart/form-data

CSV file to import

data

string(\$binary)

Choose File

 No file chosen

Execute

Clear

Responses

Importverhalten

Während des Importvorgangs werden Daten hinzugefügt, zusammengeführt oder ersetzt, je nachdem, welche Objekte und Objekttypen importiert werden. Beachten Sie beim Importieren die folgenden Verhaltensweisen.

- Fügt eine Anmerkung oder Anwendung hinzu, wenn im Zielsystem keine mit demselben Namen vorhanden ist.

- Führt eine Annotation zusammen, wenn der Annotationstyp eine Liste ist und im Zielsystem eine Annotation mit demselben Namen vorhanden ist.
- Ersetzt eine Annotation, wenn der Annotationstyp nicht eine Liste ist und im Zielsystem eine Annotation mit demselben Namen vorhanden ist.

Hinweis: Wenn im Zielsystem eine Annotation mit demselben Namen, aber einem anderen Typ vorhanden ist, schlägt der Import fehl. Wenn Objekte von der fehlgeschlagenen Annotation abhängen, können diese Objekte falsche oder unerwünschte Informationen anzeigen. Sie müssen alle Anmerkungsabhängigkeiten überprüfen, nachdem der Importvorgang abgeschlossen ist.

- Wenn ein Annotationswert leer ist, wird diese Annotation aus dem Objekt entfernt. Vererbte Anmerkungen sind davon nicht betroffen.
- Annotationswerte vom Typ „Datum“ müssen als Unix-Zeit in Millisekunden übergeben werden.
- Beim Kommentieren von Volumes oder internen Volumes ist der Objektname eine Kombination aus Speichername und Volumenname unter Verwendung des Trennzeichens "->". Beispiel: <Speichername>-><Volumename>
- Wenn ein Objektname ein Komma enthält, muss der gesamte Name in doppelte Anführungszeichen gesetzt werden. Beispiel: "NetApp1,NetApp2"->023F
- Beim Anhängen von Anmerkungen an Speicher, Switches und Ports wird die Spalte „Anwendung“ ignoriert.
- Mieter, Geschäftsweig, Geschäftseinheit und/oder Projekt bilden eine Geschäftseinheit. Wie bei allen Geschäftseinheiten kann jeder der Werte leer sein.

Die folgenden Objekttypen können mit Anmerkungen versehen werden.

OBJEKTTYPE	NAME ODER SCHLÜSSEL
Gastgeber	id-><id> oder <Name> oder <IP>
VM	id-><id> oder <Name>
Speicherpool	id-><id> oder <Speichername>-><Speicherpoolname>
Internes Volumen	id-><id> oder <Speichername>-><Name des internen Datenträgers>
Volumen	id-><id> oder <Speichername>-><Volumename>
Storage	id-><id> oder <Name> oder <IP>
Schalten	id-><id> oder <Name> oder <IP>
Hafen	id-><id> oder <WWN>
Qtree	id-><id> oder <Speichername>-><Name des internen Datenträgers>-><Qtree-Name>
Aktie	id-><id> oder <Speichername>-><Name des internen Datenträgers>-><Freigabename>-><Protokoll>[-><Qtree-Name (optional im Fall des Standard-Qtree)>]

Arbeiten mit Anwendungen

Nachverfolgen der Asset-Nutzung nach Anwendung

Wenn Sie wissen, welche Anwendungen in der Umgebung Ihres Unternehmens verwendet werden, können Sie die Nutzung und Kosten Ihrer Anlagen besser im Auge behalten.

Bevor Sie Daten zu den auf Ihrem Mandanten ausgeführten Anwendungen verfolgen können, müssen Sie diese Anwendungen zunächst definieren und sie den entsprechenden Assets zuordnen. Sie können Anwendungen mit den folgenden Assets verknüpfen: Hosts, virtuelle Maschinen, Volumes, interne Volumes, Qtrees, Freigaben und Hypervisoren.

Dieses Thema bietet ein Beispiel für die Verfolgung der Nutzung virtueller Maschinen, die das Marketingteam für seine Exchange-E-Mails verwendet.

Sie können eine Tabelle ähnlich der folgenden erstellen, um die auf Ihrem Mandanten verwendeten Anwendungen zu identifizieren und die Gruppe oder Geschäftseinheit zu notieren, die die einzelnen Anwendungen verwendet.

Mieter	Geschäftszweig	Geschäftseinheit	Projekt	Anwendungen
NetApp	Datenspeicherung	Rechtliches	Patente	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Datenspeicherung	Marketing	Verkaufsveranstaltungen	Exchange, Oracle Shared DataBase, BlastOff-Eventplaner

Die Tabelle zeigt, dass das Marketingteam die Exchange-Anwendung verwendet. Wir möchten die Auslastung ihrer virtuellen Maschinen für Exchange verfolgen, damit wir vorhersagen können, wann wir mehr Speicher hinzufügen müssen. Wir können die Exchange-Anwendung mit allen virtuellen Maschinen von Marketing 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).

Angenommen, alle VMs des Marketingteams haben einen Namen, der die Zeichenfolge „mkt“ enthält, erstellen Sie Ihre Abfrage, um den VM-Namen nach „mkt“ zu filtern.

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

Erstellen von Anwendungen

Um Daten zu verfolgen, die mit bestimmten Anwendungen verknüpft sind, die auf Ihrem

Mandanten ausgeführt werden, können Sie die Anwendungen in Data Infrastructure Insights definieren.

Informationen zu diesem Vorgang

Mit Data Infrastructure Insights können Sie Daten von Assets, die mit Anwendungen verknüpft sind, für Zwecke wie Nutzungs- oder Kostenberichte verfolgen.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Enrich > Applications**. Auswählen

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**.

Nachdem eine Anwendung definiert wurde, kann sie den Assets zugewiesen werden.

Zuweisen von Anwendungen zu Assets

Dieses Verfahren weist die Anwendung beispielhaft einem Host zu. Sie können einer Anwendung Host, virtuelle Maschine, Volume oder interne Volumes zuweisen.

Schritte

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

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



In Umgebungen mit einer großen Menge verwandter Assets kann die Vererbung von Anwendungszuweisungen zu diesen Assets mehrere Minuten dauern. Bitte rechnen Sie mit einer längeren Vererbungszeit, wenn Sie über viele zusammenhängende Vermögenswerte verfügen.

Nach Abschluss

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

Automatische Geräteauflösung

Übersicht über die automatische Geräteauflösung

Sie müssen alle Geräte identifizieren, die Sie mit Data Infrastructure Insights überwachen möchten. Eine Identifizierung ist erforderlich, um die Leistung und den Bestand Ihres Mieters genau zu verfolgen. Normalerweise wird die Mehrheit der auf Ihrem Mandanten erkannten Geräte durch die *Automatische Geräteauflösung* identifiziert.

Nachdem Sie Datensammler konfiguriert haben, werden Geräte auf Ihrem Mandanten identifiziert, darunter Switches, Speicher-Arrays und Ihre virtuelle Infrastruktur aus Hypervisoren und VMs. Allerdings werden dadurch normalerweise nicht 100 % der Geräte Ihres Mandanten identifiziert.

Nachdem Geräte vom Typ „Datensammler“ konfiguriert wurden, besteht die bewährte Vorgehensweise darin, Geräteauflösungsregeln zu nutzen, um die verbleibenden unbekannten Geräte auf Ihrem Mandanten zu identifizieren. Mithilfe der Geräteauflösung können Sie unbekannte Geräte als folgende Gerätetypen auflösen:

- Physische Hosts
- Speicher-Arrays
- Bänder

Geräte, die nach der Geräteauflösung als unbekannt verbleiben, gelten als generische Geräte, die Sie auch in Abfragen und auf Dashboards anzeigen können.

Die wiederum erstellten Regeln identifizieren automatisch neue Geräte mit ähnlichen Attributen, wenn sie Ihrer Umgebung hinzugefügt werden. In einigen Fällen ermöglicht die Geräteauflösung auch eine manuelle Identifizierung, indem die Geräteauflösungsregeln für nicht erkannte Geräte in Data Infrastructure Insights umgangen werden.

Eine unvollständige Identifizierung von Geräten kann zu folgenden Problemen führen:

- Unvollständige Pfade
- Nicht identifizierte Mehrwegeverbindungen
- Die Unfähigkeit, Anwendungen zu gruppieren
- Ungenaue Topologieansichten
- Ungenaue Daten im Data Warehouse und Reporting

Die Funktion zur Geräteauflösung (Verwalten > Geräteauflösung) umfasst die folgenden Registerkarten, die jeweils eine Rolle bei der Planung der Geräteauflösung und der Anzeige der Ergebnisse spielen:

- **Fibre Channel Identify** enthält eine Liste mit WWNs und Portinformationen von Fibre Channel-Geräten, die nicht durch die automatische Geräteauflösung aufgelöst wurden. Auf der Registerkarte wird auch der Prozentsatz der identifizierten Geräte angegeben.
- **IP-Adressidentifizierung** enthält eine Liste von Geräten, die auf CIFS-Freigaben und NFS-Freigaben zugreifen und nicht durch die automatische Geräteauflösung identifiziert wurden. Auf der Registerkarte wird auch der Prozentsatz der identifizierten Geräte angegeben.
- **Regeln zur automatischen Auflösung** enthält die Liste der Regeln, die bei der Auflösung von Fibre-Channel-Geräten ausgeführt werden. Dies sind Regeln, die Sie erstellen, um nicht identifizierte Fibre-Channel-Geräte aufzulösen.
- **Einstellungen** bietet Konfigurationsoptionen, mit denen Sie die Geräteauflösung an Ihre Umgebung anpassen können.

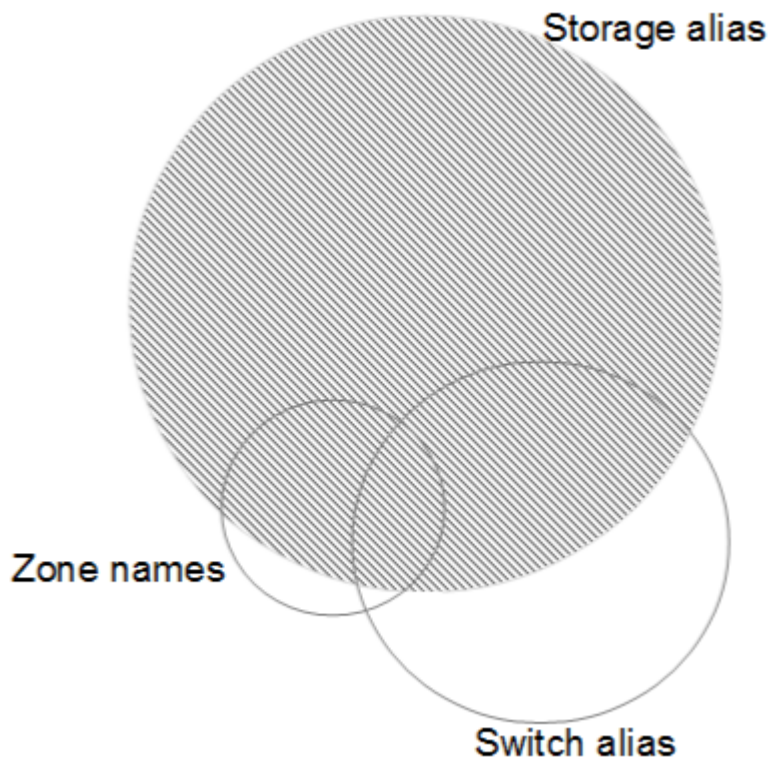
Bevor Sie beginnen

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

Um genaue Regeln erstellen zu können, müssen Sie Fragen wie die folgenden beantworten:

- Verfügt Ihre Umgebung über Benennungsstandards für Zonen oder Hosts und wie viel Prozent davon sind korrekt?
- Verwendet Ihre Umgebung einen Switch-Alias oder Speicheralias und stimmen diese mit dem Hostnamen überein?
- Wie oft ändern sich die Benennungsschemata Ihres Mandanten?
- Gab es Übernahmen oder Fusionen, die zu unterschiedlichen Namensgebungen geführt haben?

Nach der Analyse Ihrer Umgebung sollten Sie in der Lage sein, die vorhandenen Namensstandards zu ermitteln, die Sie voraussichtlich zuverlässig antreffen werden. Die von Ihnen gesammelten Informationen können grafisch in einer Abbildung ähnlich der folgenden dargestellt werden:



In diesem Beispiel wird die größte Anzahl von Geräten zuverlässig durch Speicheralias dargestellt. Regeln, die Hosts mithilfe von Speicheraliasen identifizieren, sollten zuerst geschrieben werden, Regeln mit Switch-Aliasen sollten als Nächstes geschrieben werden und die zuletzt erstellten Regeln sollten Zonen-Alias verwenden. Aufgrund der Überschneidung bei der Verwendung von Zonenaliasen und Switch-Aliasen können einige Speicheraliasregeln zusätzliche Geräte identifizieren, sodass weniger Regeln für Zonenalias und Switch-Alias erforderlich sind.

Schritte zum Identifizieren von Geräten

Normalerweise verwenden Sie einen Workflow ähnlich dem folgenden, um Geräte auf Ihrem Mandanten zu identifizieren. Die Identifizierung ist ein iterativer Prozess und kann mehrere Schritte der Planung und

Verfeinerung von Regeln erfordern.

- Forschungsumfeld
- Planregeln
- Regeln erstellen/überarbeiten
- Ergebnisse überprüfen
- Erstellen Sie zusätzliche Regeln oder identifizieren Sie Geräte manuell
- Erledigt



Wenn sich auf Ihrem Mandanten nicht identifizierte Geräte (auch als unbekannte oder generische Geräte bezeichnet) befinden und Sie anschließend eine Datenquelle konfigurieren, die diese Geräte bei der Abfrage identifiziert, werden sie nicht mehr als generische Geräte angezeigt oder gezählt.

Verwandt: ["Erstellen von Geräteauflösungsregeln"](#) ["Fibre Channel-Geräteauflösung"](#) ["IP-Geräteauflösung"](#) ["Festlegen der Geräteauflösungseinstellungen"](#)

Regeln zur Geräteauflösung

Sie erstellen Geräteauflösungsregeln, um Hosts, Speicher und Bänder zu identifizieren, die derzeit nicht automatisch von Data Infrastructure Insights identifiziert werden. Die von Ihnen erstellten Regeln identifizieren Geräte, die sich derzeit in Ihrer Umgebung befinden, und identifizieren auch ähnliche Geräte, wenn sie Ihrer Umgebung hinzugefügt werden.

Erstellen von Geräteauflösungsregeln

Wenn Sie Regeln erstellen, identifizieren Sie zunächst die Informationsquelle, auf die die Regel angewendet wird, die zum Extrahieren der Informationen verwendete Methode und ob auf die Ergebnisse der Regel eine DNS-Suche angewendet wird.

Quelle, die zur Identifizierung des Geräts verwendet wird	* SRM-Aliase für Hosts * Speicheralias mit eingebettetem Host- oder Bandnamen * Switch-Alias mit eingebettetem Host- oder Bandnamen * Zonennamen mit eingebettetem Hostnamen
Methode, die zum Extrahieren des Gerätenamens aus der Quelle verwendet wird	* Wie es ist (einen Namen aus einem SRM extrahieren) * Trennzeichen * Reguläre Ausdrücke
DNS-Suche	Gibt an, ob Sie DNS zur Überprüfung des Hostnamens verwenden

Sie erstellen Regeln auf der Registerkarte „Regeln für die automatische Auflösung“. Die folgenden Schritte beschreiben den Regelerstellungsprozess.

Verfahren

1. Klicken Sie auf **Verwalten > Geräteauflösung**
2. Klicken Sie auf der Registerkarte **Regeln zur automatischen Auflösung** auf **+ Host-Regel** oder **+ Bandregel**.

Der Bildschirm **Auflösungsregel** wird angezeigt.



Klicken Sie auf den Link „Übereinstimmungskriterien anzeigen“, um Hilfe und Beispiele zum Erstellen regulärer Ausdrücke zu erhalten.

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

Sie können *Host* oder *Tape* auswählen.

4. Wählen Sie in der Liste **Quelle** die Quelle aus, die Sie zur Identifizierung des Hosts verwenden möchten.

Abhängig von der ausgewählten Quelle zeigt Data Infrastructure Insights die folgende Antwort an:

- a. **Zonen** listet die Zonen und WWN auf, die von Data Infrastructure Insights identifiziert werden müssen.
 - b. **SRM** listet die nicht identifizierten Aliase auf, die von Data Infrastructure Insights identifiziert werden müssen
 - c. **Speicheralias** listet Speicheralias und WWN auf, die von Data Infrastructure Insights identifiziert werden müssen
 - d. **Switch-Alias** listet die Switch-Aliase auf, die von Data Infrastructure Insights identifiziert werden müssen
5. Wählen Sie in der Liste **Methode** die Methode aus, die Sie zur Identifizierung des Hosts verwenden möchten.

Quelle	Verfahren
SRM	Wie es ist, Trennzeichen, reguläre Ausdrücke
Speicheralias	Trennzeichen, reguläre Ausdrücke
Alias wechseln	Trennzeichen, reguläre Ausdrücke
Zonen	Trennzeichen, reguläre Ausdrücke

- Regeln mit Trennzeichen erfordern die Trennzeichen und die Mindestlänge des Hostnamens. Die Mindestlänge des Hostnamens ist die Anzahl der Zeichen, die Data Infrastructure Insights zur Identifizierung eines Hosts verwenden soll. Data Infrastructure Insights führt DNS-Lookups nur für Hostnamen durch, die so lang oder länger sind.

Bei Regeln mit Trennzeichen wird die Eingabezeichenfolge durch das Trennzeichen tokenisiert und eine Liste mit Hostnamenkandidaten wird erstellt, indem mehrere Kombinationen des angrenzenden Tokens erstellt werden. Die Liste wird dann von groß nach klein sortiert. Beispielsweise würde die Liste bei einer Eingabezeichenfolge von *vipsnq03_hba3_emc3_12ep0* 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 Auswahl der Groß-/Kleinschreibung.
6. Klicken Sie auf **AR ausführen**, um alle Regeln auszuführen, oder klicken Sie auf den Abwärtspfeil in der Schaltfläche, um die von Ihnen erstellte Regel auszuführen (und alle anderen Regeln, die seit der letzten vollständigen Ausführung von AR erstellt wurden).

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

Starten einer automatischen Aktualisierung der Geräteauflösung

Bei einer Aktualisierung der Geräteauflösung werden manuelle Änderungen übernommen, die seit dem letzten vollautomatischen Geräteauflösungslauf hinzugefügt wurden. Durch Ausführen eines Updates können nur die neuen manuellen Einträge in der Geräteauflösungskonfiguration übernommen und ausgeführt werden. Es wird kein vollständiger Geräteauflösungslauf durchgeführt.

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie im Bildschirm **Geräteauflösung** auf den Abwärtspfeil in der Schaltfläche **AR ausführen**.
4. Klicken Sie auf **Aktualisieren**, um das Update zu starten.

Regelgestützte manuelle Identifikation

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

Bevor Sie beginnen

Sie haben 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 reguläre Ausdrucksregel und formatieren Sie sie, um den fehlenden Text hinzuzufügen.

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights 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 Bildschirm „Identifizieren“ an, der eine Liste aller Regeln enthält, die Geräte erfolgreich identifiziert haben.

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

Die Reihenfolge der Regeln wird im Identifizierungsbildschirm geändert, jedoch nicht global.

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

Data Infrastructure Insights führt den Hostauflösungsprozess in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit denen ganz oben.

Wenn zutreffende Regeln gefunden werden, werden die Regelnamen in der Spalte „Regeln“ angezeigt und als „manuell“ gekennzeichnet.

Verwandt: ["Fibre Channel-Geräteauflösung"](#) ["IP-Geräteauflösung"](#) ["Festlegen der Geräteauflösungseinstellungen"](#)

Fibre Channel-Geräteauflösung

Der Bildschirm „Fibre Channel-Identifizierung“ zeigt die WWN und WWPN von Fibre-Channel-Geräten an, deren Hosts nicht durch die automatische Geräteauflösung identifiziert wurden. Auf dem Bildschirm werden auch alle Geräte angezeigt, die durch manuelle Geräteauflösung aufgelöst wurden.

Geräte, die durch manuelle Auflösung aufgelöst wurden, weisen den Status *OK* auf und identifizieren die Regel, die zur Identifizierung des Geräts verwendet wurde. Fehlende Geräte haben den Status *Unidentifiziert*. Geräte, die ausdrücklich von der Identifizierung ausgeschlossen sind, haben den Status *Ausgeschlossen*. Die Gesamtabdeckung zur Identifizierung von Geräten ist auf dieser Seite aufgeführt.

Sie führen Massenaktionen durch, indem Sie auf der linken Seite des Fibre Channel-Identifizierungsbildschirms mehrere Geräte auswählen. Aktionen können auf einem einzelnen Gerät ausgeführt werden, indem Sie mit der Maus über ein Gerät fahren und die Schaltflächen „Identifizieren“ oder „Nicht identifizieren“ ganz rechts in der Liste auswählen.

Der Link „Gesamtabdeckung“ zeigt eine Liste der Anzahl der identifizierten Geräte/der für Ihre Konfiguration verfügbaren Geräte an:

- SRM-Alias
- Speicheralias
- Alias wechseln
- Zonen
- Benutzerdefiniert

Manuelles Hinzufügen eines Fibre Channel-Geräts

Sie können Data Infrastructure Insights manuell ein Fibre-Channel-Gerät hinzufügen, indem Sie die Funktion „Manuell hinzufügen“ verwenden, die auf der Registerkarte „Fibre-Channel-Identifizierung“ der Geräteauflösung verfügbar ist. Dieser Prozess kann zur Voridentifizierung eines Geräts verwendet werden, das voraussichtlich in der Zukunft entdeckt wird.

Bevor Sie beginnen

Um dem System erfolgreich eine Geräteidentifikation hinzuzufügen, müssen Sie die WWN- oder IP-Adresse und den Gerätenamen kennen.

Informationen zu diesem Vorgang

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

Verfahren

1. Melden Sie sich bei der Data Infrastructure Insights -Webbenutzeroberfläche an
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte **Fibre Channel Identify**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Dialog **Gerät hinzufügen** wird angezeigt

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

Das von Ihnen eingegebene Gerät wird der Geräteliste auf der Registerkarte „Fibre Channel-Identifizierung“ hinzugefügt. Die Regel wird als *Manuell* gekennzeichnet.

Importieren der Fibre Channel-Geräteidentifikation aus einer CSV-Datei

Sie können die Fibre-Channel-Geräteidentifikation manuell in die Data Infrastructure Insights -Geräteauflösung importieren, indem Sie eine Geräteliste in einer CSV-Datei verwenden.

1. Bevor Sie beginnen

Sie müssen über eine korrekt formatierte CSV-Datei verfügen, um Geräteidentifikationen direkt in die Geräteauflösung zu importieren. Die CSV-Datei für Fibre-Channel-Geräte erfordert die folgenden Informationen:

WWN	IP	Name	Typ
-----	----	------	-----

Die Datenfelder müssen in Anführungszeichen gesetzt 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 bewährte Methode 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 Fibre Channel Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten vorhanden und in der richtigen Reihenfolge sind.

So importieren Sie Fibre Channel-Identifikationsinformationen:

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**

3. Wählen Sie die Registerkarte **Fibre Channel Identify**.
4. Klicken Sie auf die Schaltfläche **Identifizieren > Aus Datei identifizieren**.
5. Navigieren Sie zu dem Ordner, der Ihre zu importierenden CSV-Dateien enthält, und wählen Sie die gewünschte Datei aus.

Die von Ihnen eingegebenen Geräte werden der Geräteliste auf der Registerkarte „Fibre Channel-Identifizierung“ hinzugefügt. Die „Regel“ wird als „Manuell“ gekennzeichnet.

Exportieren von Fibre Channel-Gerätekennungen in eine CSV-Datei

Sie können vorhandene Fibre-Channel-Geräteidentifikationen aus der Geräteauflösungsfunktion von Data Infrastructure Insights in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können, wo sie dann zum Identifizieren von Geräten verwendet wird, die denen ähneln, die ursprünglich mit der exportierten Kennung übereinstimmen.


Informationen zu diesem Vorgang

Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die in der CSV-Datei einfach 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 bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte **Fibre Channel Identify**.
4. Wählen Sie das oder die Fibre-Channel-Geräte aus, deren Identifikation Sie exportieren möchten.
5. Klicken Sie auf *Exportieren*  Taste.

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

Verwandt: ["IP-Geräteauflösung"](#) ["Erstellen von Geräteauflösungsregeln"](#) ["Festlegen der Geräteauflösungseinstellungen"](#)

IP-Geräteauflösung

Der Bildschirm „IP-Identifizierung“ zeigt alle iSCSI- und CIFS- oder NFS-Freigaben an, die durch automatische oder manuelle Geräteauflösung identifiziert wurden. Es werden auch nicht identifizierte Geräte angezeigt. Der Bildschirm enthält die IP-Adresse, den Namen, den Status, den iSCSI-Knoten und den Freigabenamen für Geräte. Außerdem wird der Prozentsatz der erfolgreich identifizierten Geräte angezeigt.

[+ Add](#)
Total coverage
20% (2/10)

IP identify (10)

Identify
Unidentify

↑
↓

<input type="checkbox"/>	Address	IP	Name	Status	iSCSI node	Share name
<input type="checkbox"/>	1.1.1.1	1.1.1.1	LA3-CNS-SQL-06A	OK		/vol/ServerLogs_STG/
<input type="checkbox"/>	0.0.0.0/0					/vol/ServerLogs_STG/
<input type="checkbox"/>	10.56.100.18				iqn.1991-05.com.microsoft:la3-cns-sql-06b.cns.comcastnets.com	
<input type="checkbox"/>	10.56.100.19				iqn.1991-05.com.microsoft:jec20643597717.tfyd.com	/vol/wc_sc_libraries_prod/libraries_qtree/
<input type="checkbox"/>	100.54.18.100	100.54.18.100	ushapl00096ib	OK		

IP-Geräte manuell hinzufügen

Sie können Data Infrastructure Insights manuell ein IP-Gerät hinzufügen, indem Sie die Funktion zum manuellen Hinzufügen im Bildschirm „IP-Identifizierung“ verwenden.

Verfahren

- 1. Melden Sie sich bei der Data Infrastructure Insights Webbenutzeroberfläche an.
- 2. Klicken Sie auf **Verwalten > Geräteauflösung**
- 3. Klicken Sie auf die Registerkarte **IP-Adresse identifizieren**.
- 4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der Dialog „Gerät hinzufügen“ wird angezeigt

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

Ergebnis

Das von Ihnen eingegebene Gerät wird der Geräteliste auf der Registerkarte „IP-Adresse identifizieren“ hinzugefügt.

Importieren der IP-Geräteidentifikation aus einer CSV-Datei

Sie können IP-Gerätekennungen manuell in die Funktion „Geräteauflösung“ importieren, indem Sie eine Liste von Gerätekennungen in einer CSV-Datei verwenden.

- 1. Bevor Sie beginnen

Sie müssen über eine korrekt formatierte CSV-Datei verfügen, um Geräteidentifikationen direkt in die Funktion „Geräteauflösung“ zu importieren. Die CSV-Datei für IP-Geräte erfordert die folgenden Informationen:

Adresse	IP	Name
---------	----	------

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

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



Als bewährte Methode wird empfohlen, zunächst die IP-Adressidentifizierungsinformationen in eine CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in IP Address Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten vorhanden und in der richtigen Reihenfolge sind.

Exportieren der IP-Geräteidentifikation in eine CSV-Datei

Sie können vorhandene IP-Geräteidentifikationen aus der Geräteauflösungsfunktion von Data Infrastructure Insights in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Geräteerkennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können, wo sie dann zum Identifizieren von Geräten verwendet wird, die denen ähneln, die ursprünglich mit der exportierten Kennung übereinstimmen.


Informationen zu diesem Vorgang

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

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

Adresse	IP	Name
---------	----	------

Verfahren

1. Melden Sie sich bei der Web-Benutzeroberfläche von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte **IP-Adresse identifizieren**.
4. Wählen Sie das oder die IP-Geräte aus, deren Identifikation Sie exportieren möchten.
5. Klicken Sie auf *Exportieren*  Taste.

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

Verwandt: ["Fibre Channel-Geräteauflösung"](#) ["Erstellen von Geräteauflösungsregeln"](#) ["Festlegen der Geräteauflösungseinstellungen"](#)

Einstelloptionen auf der Registerkarte „Einstellungen“

Auf der Registerkarte „Einstellungen für die Geräteauflösung“ können Sie einen Zeitplan für die automatische Auflösung erstellen, Speicher- und Bandanbieter angeben, die in die Identifizierung einbezogen oder davon ausgeschlossen werden sollen, und DNS-Suchoptionen festlegen.

Zeitplan für die automatische Auflösung

Ein Zeitplan für die automatische Auflösung kann angeben, wann die automatische Geräteauflösung ausgeführt wird:

Option	Beschreibung
--------	--------------

Jeder	Verwenden Sie diese Option, um die automatische Geräteauflösung in Intervallen von Tagen, Stunden oder Minuten auszuführen.
Täglich	Verwenden Sie diese Option, um die automatische Geräteauflösung täglich zu einer bestimmten Zeit auszuführen.
Manuell	Verwenden Sie diese Option, um die automatische Geräteauflösung nur 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-Suchergebnisse aktiviert ist, können Sie eine Liste mit DNS-Namen hinzufügen, die an aufgelöste Geräte angehängt werden sollen.
- Sie können „Automatische Auflösung von IPs“ auswählen, um die automatische Hostauflösung für iSCSI-Initiatoren und Hosts zu aktivieren, die per DNS-Lookup auf NFS-Freigaben zugreifen. Wenn dies nicht angegeben ist, wird nur eine FC-basierte Auflösung durchgeführt.
- Sie können Unterstriche in Hostnamen zulassen und in Ergebnissen einen „Verbunden mit“-Alias anstelle des Standard-Port-Alias verwenden.

Einbeziehung oder Ausschluss bestimmter Speicher- und Bandanbieter

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



Geräteauflösungsregeln für Bänder funktionieren nur für WWNs, bei denen der Anbieter für dieses WWN in den Anbietereinstellungen auf *Nur als Band enthalten* eingestellt ist.

Siehe auch: "[Beispiele für reguläre Ausdrücke](#)"

Beispiele für reguläre Ausdrücke

Wenn Sie den Ansatz mit regulären Ausdrücken als Ihre Quellenbenennungsstrategie ausgewählt haben, können Sie die Beispiele für reguläre Ausdrücke als Leitfaden für Ihre eigenen Ausdrücke verwenden, die in den automatischen Auflösungsmethoden von Data Infrastructure Insights verwendet werden.

Formatieren regulärer Ausdrücke

Beim Erstellen regulärer Ausdrücke für die automatische Auflösung von Data Infrastructure Insights können Sie das Ausgabeformat konfigurieren, indem Sie Werte in ein Feld mit dem Namen *FORMAT* eingeben.

Die Standardeinstellung ist \1, was bedeutet, dass ein Zonenname, der mit dem regulären Ausdruck übereinstimmt, durch den Inhalt der ersten durch den regulären Ausdruck erstellten Variable ersetzt wird. In einem regulären Ausdruck werden Variablenwerte durch Klammerausagen erstellt. Wenn mehrere Klammerausagen vorkommen, werden die Variablen numerisch von links nach rechts referenziert. Die Variablen können im Ausgabeformat in beliebiger Reihenfolge verwendet werden. In die Ausgabe kann auch konstanter Text eingefügt werden, indem dieser zum Feld FORMAT hinzugefügt wird.

Beispielsweise könnten Sie für diese Zonenbenennungskonvention die folgenden Zonennamen haben:

```
[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_hostname4_solaris_FC1
```

Und Sie möchten vielleicht, dass die Ausgabe das folgende Format hat:

```
[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 bewirken:
```

```
. *?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Da es drei 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 erhalten:

```
\2-\1-\3
Ihre Ausgabe würde wie folgt aussehen:
```

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

Die Bindestriche zwischen den Variablen stellen ein Beispiel für konstanten Text dar, 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 über etwas Ähnliches wie die folgenden Zonennamen verfügen:

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

Der reguläre Ausdruck, den Sie zum Erfassen des Hostnamens verwenden könnten, wäre:

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

Das Ergebnis ist eine Übereinstimmung aller Zonen, die mit S beginnen und auf die eine beliebige Kombination aus Ziffern folgt, gefolgt von einem Unterstrich, dem alphanumerischen Hostnamen (myComputer1Name), einem Unterstrich oder Bindestrich, den Großbuchstaben HBA und einer einzelnen Ziffer (0-9). In der Variable `*\1*` wird nur der Hostname gespeichert.

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- „S“ steht für den Zonennamen und leitet den Ausdruck ein. Dies entspricht nur einem „S“ am Anfang des Zonennamens.
- Die Zeichen [0-9] in Klammern geben an, dass auf „S“ eine Ziffer zwischen 0 und 9 (einschließlich) folgen muss.
- Das +-Zeichen gibt an, dass die Angabe in der vorhergehenden Klammer 1 oder mehrere Male vorkommen muss.
- Das _ (Unterstrich) bedeutet, dass auf die Ziffern nach S im Zonennamen unmittelbar nur ein Unterstrichzeichen folgen darf. In diesem Beispiel wird in der Zonenbenennungskonvention der Unterstrich verwendet, um den Zonennamen vom Hostnamen zu trennen.
- Nach dem erforderlichen Unterstrich zeigen die Klammern an, dass das darin enthaltene Muster in der Variable `\1` gespeichert wird.
- Die eingeklammerten Zeichen [a-zA-Z0-9] geben an, dass es sich bei den übereinstimmenden Zeichen ausschließlich um Buchstaben (unabhängig von der Groß-/Kleinschreibung) und Zahlen handelt.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Die eingeklammerten Zeichen [_-] (Unterstrich und Bindestrich) geben an, dass auf das alphanumerische Muster ein Unterstrich oder ein Bindestrich folgen muss.
- Die Buchstaben HBA im regulären Ausdruck geben an, dass genau diese Zeichenfolge im Zonennamen vorkommen muss.
- Der letzte Satz eingeklammerter Zeichen [0-9] entspricht einer einzelnen Ziffer von 0 bis einschließlich 9.

Beispiel 2

In diesem Beispiel wird bis zum ersten Unterstrich „*gesprungen*, dann wird *E* und alles danach bis zum zweiten „*abgeglichen* und dann alles danach übersprungen.

Zone: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

Regulärer Ausdruck: `.(E.?).*?`

Beispiel 3

Die Klammern „()“ um den letzten Abschnitt im regulären Ausdruck (unten) geben an, welcher Teil der Hostname ist. Wenn Sie VSAN3 als Hostnamen verwenden möchten, lautet dieser: `_[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 komplizierteres Benennungsmuster

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

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
([a-zA-Z0-9]*)_.*
```

Die Variable `\1` würde nach der Auswertung durch diesen Ausdruck nur `_myComputerName123_` enthalten.

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable `\1` gespeichert wird.
- Die eingeklammerten Zeichen `[a-zA-Z0-9]` bedeuten, dass jeder Buchstabe (unabhängig von der Groß-/Kleinschreibung) oder jede Ziffer übereinstimmt.
- Das `*` (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Das Zeichen `_` (Unterstrich) im regulären Ausdruck bedeutet, dass der Zonenname unmittelbar nach der alphanumerischen Zeichenfolge, die mit den vorhergehenden Klammern übereinstimmt, einen Unterstrich haben muss.
- Der `.` (Punkt) entspricht einem beliebigen Zeichen (einem Platzhalter).
- Das `*` (Sternchen) zeigt an, dass der Platzhalter für den vorangehenden Punkt 0 oder mehr Mal vorkommen kann.

Mit anderen Worten: Die Kombination `.*` steht für ein beliebiges Zeichen, beliebig oft.

Beispiel 5 mit Zonennamen ohne Muster

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

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
(.*?)_.*
```

Die Variable \1 würde _myComputerName_ (im ersten Zonennamenbeispiel) oder _myComputerName123_ (im zweiten Zonennamenbeispiel) enthalten. Dieser reguläre Ausdruck würde also auf alles vor dem ersten Unterstrich passen.

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Das Zeichen ? macht die Übereinstimmung nicht gierig. Dadurch wird die Suche beim ersten Unterstrich beendet und nicht beim letzten.
- Die Zeichen _.* entsprechen dem ersten gefundenen Unterstrich und allen darauf folgenden Zeichen.

Beispiel 6 mit Computernamen mit einem Muster

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

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

Der reguläre Ausdruck, den Sie zum Erfassen dieser Daten verwenden könnten, wäre:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Da die Zonenbenennungskonvention eher einem Muster folgt, könnten wir den obigen Ausdruck verwenden, der alle Instanzen eines Hostnamens (im Beispiel myComputerName) abgleicht, der entweder mit A, B oder T endet, und diesen Hostnamen in die Variable \1 einfügt.

Der reguläre Ausdruck kann in seine Komponenten zerlegt werden:

- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.
- Das Zeichen ? macht die Übereinstimmung nicht gierig. Dadurch wird die Suche beim ersten Unterstrich beendet und nicht beim letzten.
- Das Unterstrichzeichen entspricht dem ersten Unterstrich im Zonennamen.
- Daher entspricht die erste .*?-Kombination den Zeichen Storage1 im ersten Zonennamenbeispiel.
- Die zweite .*?-Kombination verhält sich wie die erste, entspricht aber Switch1 im ersten

Zonennamenbeispiel.

- Die Klammern zeigen an, dass das darin enthaltene Muster in der Variable \1 gespeichert wird.
- Die eingeklammerten Zeichen [a-zA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig von der Groß-/Kleinschreibung) oder jede Ziffer übereinstimmt.
- Das * (Sternchen) nach den Klammern gibt an, dass die eingeklammerten Zeichen 0 oder mehr Mal vorkommen.
- Die eingeklammerten Zeichen im regulären Ausdruck [ABT] entsprechen einem einzelnen Zeichen im Zonennamen, das A, B oder T sein muss.
- Der _ (Unterstrich) nach den Klammern gibt an, dass auf die Zeichenübereinstimmung [ABT] ein Unterstrich folgen muss.
- Der .* (Punkt Sternchen) passt zu jedem beliebigen Zeichen, beliebig oft.

Das Ergebnis wäre daher, dass die Variable \1 eine beliebige alphanumerische Zeichenfolge enthält, die:

- wurde durch eine Anzahl alphanumerischer Zeichen und zwei Unterstriche eingeleitet
- gefolgt von einem Unterstrich (und dann einer beliebigen Anzahl alphanumerischer Zeichen)
- hatte vor dem dritten Unterstrich ein letztes Zeichen von A, B oder T.

Beispiel 7

Zone: myComputerName123_HBA1_Symm1_FA1

Hostname: meinComputername123

Regulärer Ausdruck: ([a-zA-Z0-9]+)_.*

Beispiel 8

Dieses Beispiel findet alles vor dem ersten _.

Zone: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname: MeinComputername

Regulärer Ausdruck: (.*?)_.

Beispiel 9

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

Zone: Z_MeinComputername_Speichername

Hostname: MeinComputername

Regulärer Ausdruck: .?(.?).*?

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: MeinComputername123

RegExp: .?.?([a-zA-Z0-9]+)[ABT]_.

Beispiel 11

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Hostname: MyComputerName123A

RegExp: .?.?([a-zA-z0-9]+). *?

Beispiel 12

Das ^ (Zirkumflex oder Caretzeichen) **in eckigen Klammern** negiert den Ausdruck. Beispielsweise bedeutet [^Ff] alles außer dem großen oder kleinen F und [^az] bedeutet alles außer den kleinen Buchstaben a bis z und im obigen Fall alles außer dem _. Die Formatanweisung fügt dem Ausgabehostnamen das „-“ hinzu.

Zone: mhs_apps44_d_A_10a0_0429

Hostname: mhs-apps44-d

Regulärer Ausdruck: ()_([AB]).*Format in Data Infrastructure Insights: \1-\2 ([^_])_ ([^_]).*Format in Data Infrastructure Insights: \1-\2-\3

Beispiel 13

In diesem Beispiel wird der Speicheralias durch „\“ abgegrenzt und der Ausdruck muss „\\“ verwenden, um zu definieren, dass in der Zeichenfolge tatsächlich „\“ verwendet werden und dass diese nicht Teil des Ausdrucks selbst sind.

Speicheralias: \Hosts\E2DOC01C1\E2DOC01N1

Hostname: E2DOC01N1

Regulärer Ausdruck: \\?.?\\(.*?)

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

Regulärer Ausdruck: -(.*-\\d).*

Beispiel 15

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

Zone: SRV_USBVM11_F1

Hostname: US-BV-M11

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

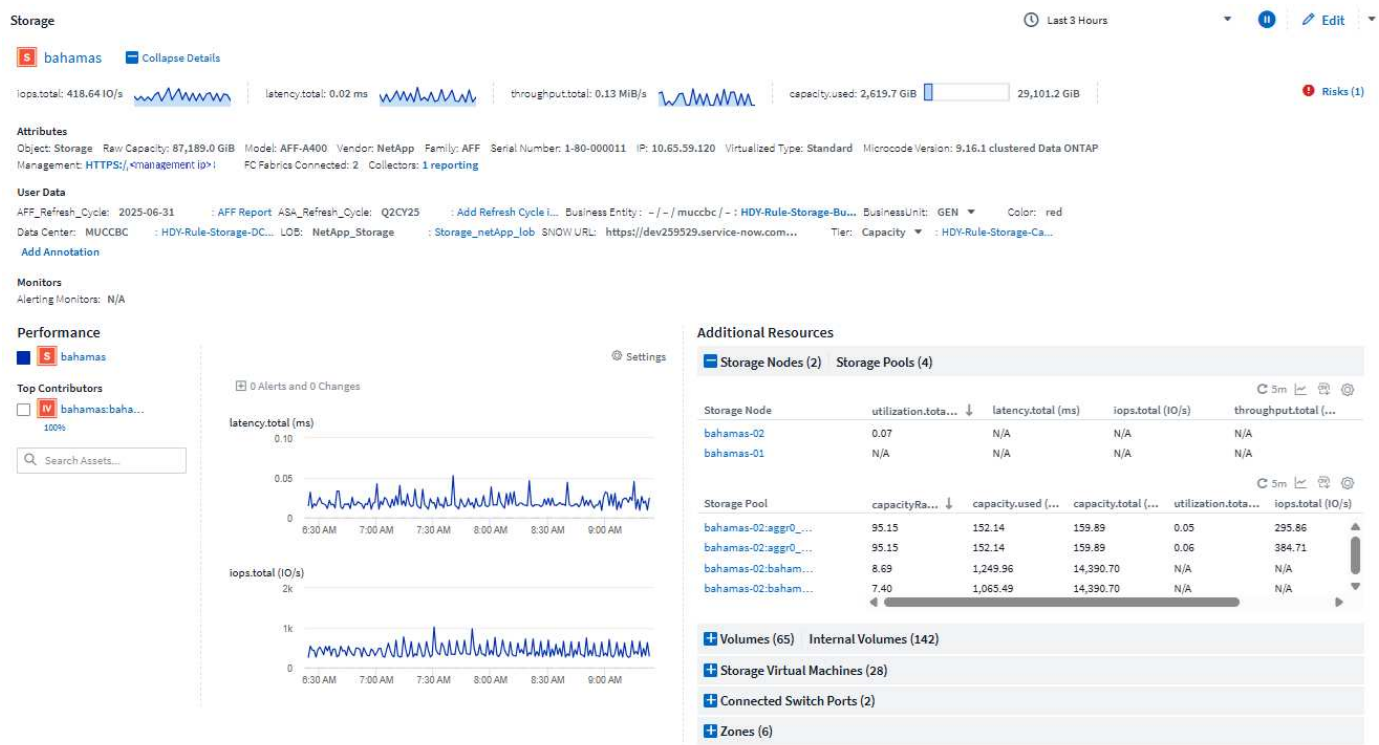
Format: US-BV-1

Informationen zur Asset-Seite

Übersicht über die Asset-Seite

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

Auf Zielseiten erhalten Sie eine Einzelseitenansicht des Objekts mit Informationen zu Zusammenfassung, Leistung und zugehörigen Ressourcen.



Zusammenfassung

Oben auf einer Zielseite befindet sich der erweiterbare Abschnitt „Zusammenfassung“, der mehrere Sparkline-Diagramme enthält, die aktuelle Datentrends für Dinge wie Durchsatz oder Latenz sowie Objektinformationen und -attribute und alle Monitore anzeigen, die möglicherweise Warnungen für das Objekt ausgeben.

Im Abschnitt „Zusammenfassung“ werden auch die dem Asset zugewiesenen Anmerkungen angezeigt und Sie können diese ändern.

Leistungsbereich

Im Abschnitt „Leistung“ werden Leistungsdaten für das Objekt angezeigt. Wählen Sie *Einstellungen*, um der

Anzeige zusätzliche Diagramme wie Durchsatz oder Kapazität hinzuzufügen, oder wählen Sie korrelierte oder beitragende Ressourcen aus, um deren Daten neben denen des Objekts darzustellen. Geräte, die möglicherweise Konflikte verursachen, werden auch im Abschnitt „Leistung“ aufgeführt. Die Daten in den Diagrammen werden automatisch aktualisiert, wenn Datensammler Abfragen durchführen und aktualisierte Daten erfasst werden.

Sie können die **Metriken** Sie im Leistungsdiagramm für den ausgewählten Zeitraum anzeigen möchten. Klicken Sie auf das Dropdown-Menü „Einstellungen“ und wählen Sie aus den aufgelisteten Metriken aus.

Zusätzlich zu den Leistungsdaten werden auch alle Warnungen angezeigt, die innerhalb des ausgewählten Seitenzeitraums aktiv sind oder waren.



Sie können aus den folgenden Geräten auswählen, die im Abschnitt „Leistung“ aufgeführt sein können:

- Am stärksten korreliert

Zeigt die Vermögenswerte an, die eine hohe Korrelation (Prozentsatz) mit einer oder mehreren Leistungskennzahlen zum Basisvermögenswert aufweisen.

- Top-Mitwirkende

Zeigt die Vermögenswerte an, die (prozentual) zum Basisvermögen beitragen.

- Wichtigste Änderungen

Vermögenswerte im Zusammenhang mit den jüngsten Änderungen.

- Workload-Konflikte

Zeigt die Assets an, die sich auf andere gemeinsam genutzte Ressourcen wie Hosts, Netzwerke und Speicher auswirken oder von diesen beeinflusst werden. Diese werden manchmal als *gierige* und *verschlechterte* Ressourcen bezeichnet.

Abschnitt „Zusätzliche Ressourcen“

Im Abschnitt „Zusätzliche Ressourcen“ werden Datentabellen für Ressourcen angezeigt, die sich auf den aktuellen Objekttyp beziehen. Sie können diese Tabellen erweitern und reduzieren, um sich auf bestimmte Ressourcen zu konzentrieren. Wählen Sie das Zahnradsymbol aus, um vorübergehend zusätzliche Metriken oder Attribute in einer Tabelle anzuzeigen.

Benutzerdefinierte Widgets hinzufügen

Sie können jeder Asset-Seite Ihre eigenen Widgets hinzufügen. Von Ihnen hinzugefügte Widgets werden auf den Asset-Seiten für alle Objekte dieses Typs angezeigt. Wenn Sie beispielsweise einer Speicher-Asset-Seite ein benutzerdefiniertes Widget hinzufügen, wird dieses Widget auf den Asset-Seiten für alle Speicher-Assets angezeigt.

Benutzerdefinierte Widgets werden unten auf einer Zielseite unter den Abschnitten „Leistung“ und „Ressourcen“ platziert.

Arten von Asset-Seiten

Data Infrastructure Insights bietet Asset-Seiten für die folgenden Assets:

- Virtuelle Maschine
- Virtuelle Speichermaschine (SVM)
- Volumen
- Internes Volumen
- Host (einschließlich Hypervisor)
- Speicherpool
- Storage
- Datenspeicher
- Anwendung
- Speicherknoten
- Qtree
- Scheibe
- VMDK
- Hafen
- Schalten
- Stoff
- Gastgeber
- Zone

Ändern des Zeitbereichs der angezeigten Daten

Standardmäßig werden auf einer Asset-Seite die Daten der letzten drei Stunden angezeigt. Sie können den Zeitabschnitt der angezeigten Daten jedoch mithilfe einer Option ändern, die sich auf jeder Asset-Seite befindet, unabhängig vom Asset-Typ. Um den Zeitraum zu ändern, klicken Sie auf den angezeigten Zeitraum in der oberen Leiste und wählen Sie aus den folgenden Zeitsegmenten:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Letzte 2 Stunden
- Letzte 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 14 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

Mit dem benutzerdefinierten Zeitbereich können Sie bis zu 31 aufeinanderfolgende Tage auswählen. Sie können auch die Start- und Endzeit des Tages für diesen Bereich festlegen. Die Standardstartzeit ist 0:00 Uhr am ersten ausgewählten Tag und die Standardendzeit ist 23:59 Uhr am letzten ausgewählten Tag. Durch Klicken auf „Übernehmen“ wird der benutzerdefinierte Zeitbereich auf die Asset-Seite angewendet.

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

Definitionen von Leistungsmetriken

Im Abschnitt „Leistung“ können basierend auf dem für das Asset ausgewählten Zeitraum mehrere Kennzahlen angezeigt werden. Jede Metrik wird in einem eigenen Leistungsdiagramm angezeigt. Sie können den Diagrammen Metriken und zugehörige Assets hinzufügen oder daraus entfernen, je nachdem, welche Daten Sie sehen möchten. Die zur Auswahl stehenden Metriken variieren je nach Asset-Typ.

Metrisch	Beschreibung
BB-Guthaben Null Rx, Tx	Gibt an, wie oft der Puffer-zu-Puffer-Guthabenzähler während des Abtastzeitraums auf Null gewechselt ist. Diese Metrik gibt an, wie oft der angeschlossene Port die Übertragung stoppen musste, weil dieser Port keine Credits mehr bereitstellen konnte.
BB Kredit Null Dauer Tx	Zeit in Millisekunden, während der das Sende-BB-Guthaben während des Abtastintervalls Null war.
Cache-Trefferquote (Gesamt, Lesen, Schreiben) %	Prozentsatz der Anfragen, die zu Cache-Treffern führen. Je höher die Anzahl der Treffer im Verhältnis zu den Zugriffen auf das Volume ist, desto besser ist die Leistung. Diese Spalte ist für Speicher-Arrays leer, die keine Cache-Trefferinformationen erfassen.
Cache-Auslastung (Gesamt) %	Gesamtprozentsatz der Cache-Anfragen, die zu Cache-Treffern führen

Rückwürfe der Klasse 3	Anzahl der beim Fibre Channel Class 3-Datentransport verworfenen Daten.
CPU-Auslastung (Gesamt) %	Menge der aktiv genutzten CPU-Ressourcen als Prozentsatz der insgesamt verfügbaren Ressourcen (über alle virtuellen CPUs).
CRC-Fehler	Anzahl der Frames mit ungültigen zyklischen Redundanzprüfungen (CRCs), die vom Port während des Abtastzeitraums erkannt wurden
Bildrate	Übertragungsbildrate in Bildern pro Sekunde (FPS)
Durchschnittliche Framegröße (Rx, Tx)	Verhältnis von Datenverkehr zu Framegröße. Mit dieser Kennzahl können Sie feststellen, ob sich im Gewebe Überkopfrahmen befinden.
Rahmengröße zu lang	Anzahl der zu langen Fibre-Channel-Datenübertragungsrahmen.
Rahmengröße zu klein	Anzahl der zu kurzen Fibre Channel-Datenübertragungsframes.
I/O-Dichte (Gesamt, Lesen, Schreiben)	Anzahl der IOPS geteilt durch die genutzte Kapazität (wie aus der letzten Bestandsabfrage der Datenquelle ermittelt) für das Volume, das interne Volume oder das Speicherelement. Gemessen in der Anzahl der E/A-Vorgänge pro Sekunde pro TB.
IOPS (Gesamt, Lesen, Schreiben)	Anzahl der Lese-/Schreib-E/A-Dienstanforderungen, die pro Zeiteinheit den E/A-Kanal oder einen Teil dieses Kanals durchlaufen (gemessen in E/A pro Sekunde)
IP-Durchsatz (Gesamt, Lesen, Schreiben)	Gesamt: Aggregierte Rate, mit der IP-Daten in Megabyte pro Sekunde gesendet 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): Rate, mit der Daten in einer festgelegten Zeitspanne von den virtuellen Maschinen gelesen oder auf diese geschrieben werden. Der Wert wird in Megabyte pro Sekunde gemessen.
Latenz:	Durchschnittliche Antwortzeit der virtuellen Maschinen in einem Datenspeicher.
Höchste Latenz:	Die höchste Antwortzeit der virtuellen Maschinen in einem Datenspeicher.
Verbindungsfehler	Anzahl der vom Port während des Stichprobenzeitraums erkannten Verbindungsfehler.

Link-Reset Rx, Tx	Anzahl der Zurücksetzungen der Empfangs- oder Sende-Verbindung während des Abtastzeitraums. Diese Metrik stellt die Anzahl der Link-Resets dar, die vom angeschlossenen Port an diesen Port ausgegeben wurden.
Speicherauslastung (Gesamt) %	Schwellenwert für den vom Host verwendeten Speicher.
Teilweise R/W (Gesamt) %	Gesamtzahl der Male, die ein Lese-/Schreibvorgang eine Streifengrenze auf einem beliebigen Festplattenmodul in einem RAID 5-, RAID 1/0- oder RAID 0-LUN überschreitet. Im Allgemeinen sind Streifenüberschreitungen nicht vorteilhaft, da jede einen zusätzlichen E/A-Vorgang erfordert. Ein niedriger Prozentsatz weist auf eine effiziente Stripe-Elementgröße hin und ist ein Hinweis auf eine falsche Ausrichtung eines Volumes (oder einer NetApp LUN). Bei CLARiiON ist dieser Wert die Anzahl der Stripe-Übergänge geteilt durch die Gesamtzahl der IOPS.
Portfehler	Bericht über Portfehler über den Abtastzeitraum/angegebenen Zeitraum.
Signalverlustzähler	Anzahl der Signalverlustfehler. Wenn ein Signalverlustfehler auftritt, besteht keine elektrische Verbindung und es liegt ein physikalisches Problem vor.
Swapsatz (Gesamtsatz, Eingangssatz, Ausgangssatz)	Rate, mit der während des Stichprobenzeitraums Speicher von der Festplatte in den aktiven Speicher ein- und ausgelagert wird oder beides. Dieser Zähler gilt für virtuelle Maschinen.
Anzahl der Synchronisierungsverluste	Anzahl der Synchronisierungsverlustfehler. Wenn ein Synchronisierungsverlustfehler auftritt, kann die Hardware den Datenverkehr nicht verstehen oder sich darauf fixieren. Möglicherweise verwenden nicht alle Geräte dieselbe Datenrate oder die optische oder physische Verbindung ist von schlechter Qualität. Der Port muss nach jedem solchen Fehler neu synchronisiert werden, was sich auf die Systemleistung auswirkt. Gemessen in KB/Sek.
Durchsatz (Gesamt, Lesen, Schreiben)	Rate, mit der Daten als Antwort auf E/A-Dienstanforderungen in einer festgelegten Zeitspanne gesendet, empfangen oder beides werden (gemessen in MB pro Sekunde).
Timeout-Verwerfungsrahmen - Tx	Anzahl der durch Timeout verworfenen Sendeframes.
Verkehrsrate (Gesamt, Lesen, Schreiben)	Während des Stichprobenzeitraums gesendeter, empfangener oder beides empfangener Datenverkehr in Megabyte pro Sekunde.
Verkehrsauslastung (Gesamt, Lesen, Schreiben)	Verhältnis des empfangenen/gesendeten/gesamten Datenverkehrs zur Empfangs-/Sende-/Gesamtkapazität während des Stichprobenzeitraums.

Auslastung (Gesamt, Lesen, Schreiben) %	Prozentsatz der verfügbaren Bandbreite, die für Übertragung (Tx) und Empfang (Rx) verwendet wird.
Ausstehendes Schreiben (Gesamt)	Anzahl der ausstehenden Schreib-E/A-Dienstanforderungen.

Filtern nach Objekten im Kontext

Wenn Sie ein Widget auf der Zielseite eines Assets konfigurieren, können Sie *Kontextfilter* festlegen, um nur Objekte anzuzeigen, die in direktem Zusammenhang mit dem aktuellen Asset stehen. Wenn Sie ein Widget hinzufügen, werden standardmäßig *alle* Objekte des ausgewählten Typs auf Ihrem Mandanten angezeigt. Mithilfe von Kontextfiltern können Sie nur die für Ihr aktuelles Asset relevanten Daten anzeigen.

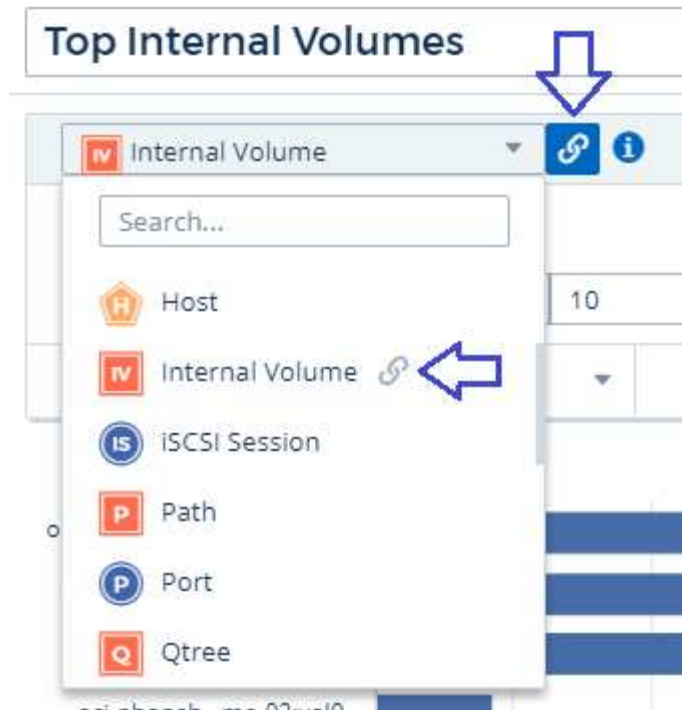
Auf den meisten Asset-Landingpages können Sie mithilfe von Widgets nach Objekten filtern, die mit dem aktuellen Asset in Zusammenhang stehen. In Filter-Dropdowns können Objekttypen, die ein Linksymbol anzeigen, im Kontext des aktuellen Assets gefiltert werden.

Sie können beispielsweise auf einer Speicher-Asset-Seite ein Balkendiagramm-Widget hinzufügen, um die höchsten IOPS auf internen Volumes nur auf diesem Speicher anzuzeigen. Wenn Sie ein Widget hinzufügen, werden standardmäßig *alle* internen Volumes Ihres Mandanten angezeigt.

Um nur interne Volumes auf dem aktuellen Speicher-Asset anzuzeigen, gehen Sie wie folgt vor:

Schritte

1. Öffnen Sie eine Asset-Seite für ein beliebiges **Speicher**-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** als Objekttyp aus, der im Balkendiagramm angezeigt werden soll.
Beachten Sie, dass neben dem Objekttyp „internes Volume“ ein Linksymbol angezeigt wird. Das Symbol „Verknüpft“ ist standardmäßig aktiviert.



5. Wählen Sie *IOPS – Gesamt* und legen Sie alle gewünschten zusätzlichen Filter fest.
6. Reduzieren Sie das Feld **Roll Up**, indem Sie auf das [X] daneben klicken. Das Feld **Anzeigen** wird angezeigt.
7. Wählen Sie die Anzeige der Top 10.
8. Speichern Sie das Widget.

Das Balkendiagramm zeigt nur die internen Volumes, die sich auf dem aktuellen Speicher-Asset befinden.

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

Um die Verknüpfung der Objektdaten aufzuheben, bearbeiten Sie das Widget und klicken Sie auf das Verknüpfungssymbol neben dem Objekttyp. Der Link wird deaktiviert und das Diagramm zeigt Daten für *alle* Objekte Ihres Mandanten an.

Sie können auch "[spezielle Variablen in Widgets](#)" um anlagenbezogene Informationen auf Zielseiten anzuzeigen.

Speichervirtualisierung

Data Infrastructure Insights kann zwischen einem Speicherarray mit lokalem Speicher oder der Virtualisierung anderer Speicherarrays unterscheiden. Dadurch haben Sie die Möglichkeit, Kosten in Beziehung zu setzen und die Leistung vom Front-End bis zum Back-End Ihrer Infrastruktur zu unterscheiden.

Virtualisierung in einem Tabellen-Widget

Eine der einfachsten Möglichkeiten, sich mit der Virtualisierung Ihres Speichers zu befassen, besteht darin, ein Dashboard-Tabellen-Widget zu erstellen, das den Typ „Virtualisiert“ anzeigt. Fügen Sie beim Erstellen der

Abfrage für das Widget einfach „virtualizedType“ zu Ihrer Gruppierung oder Ihrem Filter hinzu.

Storage

X

Display

Last 3 Hours (Dashboard Time)

☐ Override Dashboard Time

Filter by Attribute

+

Filter by Metric

+

Group by

virtualizedType

X

Das resultierende Tabellen-Widget zeigt Ihnen die *Standard*-, *Backend*- und *Virtual*-Speicher auf Ihrem Mandanten.

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

Auf der Zielseite zu Speicher, Volume, internem Volume oder Datenträger können Sie relevante Virtualisierungsinformationen sehen. Wenn Sie sich beispielsweise die Speicher-Landingpage unten ansehen, können Sie erkennen, dass es sich um einen virtuellen Speicher handelt und welches Backend-Speichersystem gilt. In allen relevanten Tabellen auf den Zielseiten werden gegebenenfalls auch Virtualisierungsinformationen angezeigt.

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:

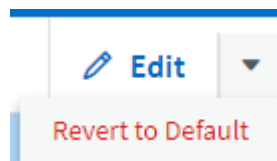
FC Fabrics Connected:
7

Alert Monitors:

Vorhandene Landingpages und Dashboards

Beachten Sie, dass, wenn Sie derzeit benutzerdefinierte Zielseiten oder Dashboards auf Ihrem Mandanten haben, diese standardmäßig nicht automatisch alle Virtualisierungsinformationen anzeigen. Sie können jedoch jedes benutzerdefinierte Dashboard oder jede benutzerdefinierte Zielseite auf die Standardeinstellungen zurücksetzen (Sie müssen Ihre Anpassungen erneut implementieren) oder die entsprechenden Widgets ändern, um die gewünschten Virtualisierungsattribute oder -metriken einzuschließen.

„Auf Standard zurücksetzen“ ist in der oberen rechten Ecke eines benutzerdefinierten Dashboards oder Zielseitenbildschirms verfügbar.



Hinweise und Tipps zur Suche nach Assets und Warnungen

Zur Suche nach Daten oder Objekten in Ihrer überwachten Umgebung können mehrere Suchtechniken verwendet werden.

- **Platzhaltersuche**

Sie können eine Platzhaltersuche mit mehreren Zeichen durchführen, indem Sie das Zeichen * verwenden. Beispielsweise würde *applic*n application* zurückgeben.

- **Bei der Suche verwendete Ausdrücke**

Eine Phrase ist eine Gruppe von Wörtern, die von doppelten Anführungszeichen umgeben sind, beispielsweise „VNX LUN 5“. Sie können doppelte Anführungszeichen verwenden, um nach Dokumenten zu suchen, deren Namen oder Attribute Leerzeichen enthalten.

- **Boolesche Operatoren**

Mithilfe der Booleschen Operatoren OR, AND und NOT können Sie mehrere Begriffe kombinieren, um eine komplexere Abfrage zu erstellen.

ODER

Der ODER-Operator ist der Standard-Konjunktionsoperator.

Wenn zwischen zwei Begriffen kein Boolescher Operator steht, wird der ODER-Operator verwendet.

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

Beispielsweise sucht *storage OR netapp* nach Dokumenten, die entweder *storage* oder *netapp* enthalten.

Dokumente, die den meisten Begriffen entsprechen, erhalten hohe Punktzahlen.

UND

Mit dem UND-Operator können Sie nach Dokumenten suchen, in denen beide Suchbegriffe in einem einzigen Dokument vorkommen. Beispielsweise sucht *storage AND netapp* nach Dokumenten, die sowohl *storage* als auch *netapp* enthalten.

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

NICHT

Wenn Sie den Operator NOT verwenden, werden alle Dokumente, die den Begriff nach NOT enthalten, aus den Suchergebnissen ausgeschlossen. Beispielsweise sucht *storage NOT netapp* nach Dokumenten, die nur *storage* und nicht *netapp* enthalten.

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

Bei der Suche wird die Groß-/Kleinschreibung nicht berücksichtigt.

Suche mit indexierten Begriffen

Suchen, die mit mehr indexierten Begriffen übereinstimmen, führen zu höheren Punktzahlen.

Der Suchstring wird durch Leerzeichen in einzelne Suchbegriffe aufgeteilt. Beispielsweise wird die Suchzeichenfolge „storage aurora netapp“ in drei Schlüsselwörter aufgeteilt: „storage“, „aurora“ und „netapp“. Die Suche wird mit allen drei Begriffen durchgeführt. Die Dokumente, die den meisten dieser Begriffe entsprechen, erhalten die höchste Punktzahl. Je mehr Informationen Sie angeben, desto besser sind die Suchergebnisse. Sie können beispielsweise nach einem Speicher anhand seines Namens und Modells suchen.

Die Benutzeroberfläche zeigt die Suchergebnisse kategorienübergreifend an, mit den drei besten Ergebnissen pro Kategorie. Wenn Sie ein erwartetes Objekt nicht gefunden haben, können Sie weitere Begriffe in den Suchbegriff aufnehmen, um die Suchergebnisse zu verbessern.

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

Kategorie	Indizierte Begriffe
Storage	"Speicher" Name Anbieter Modell

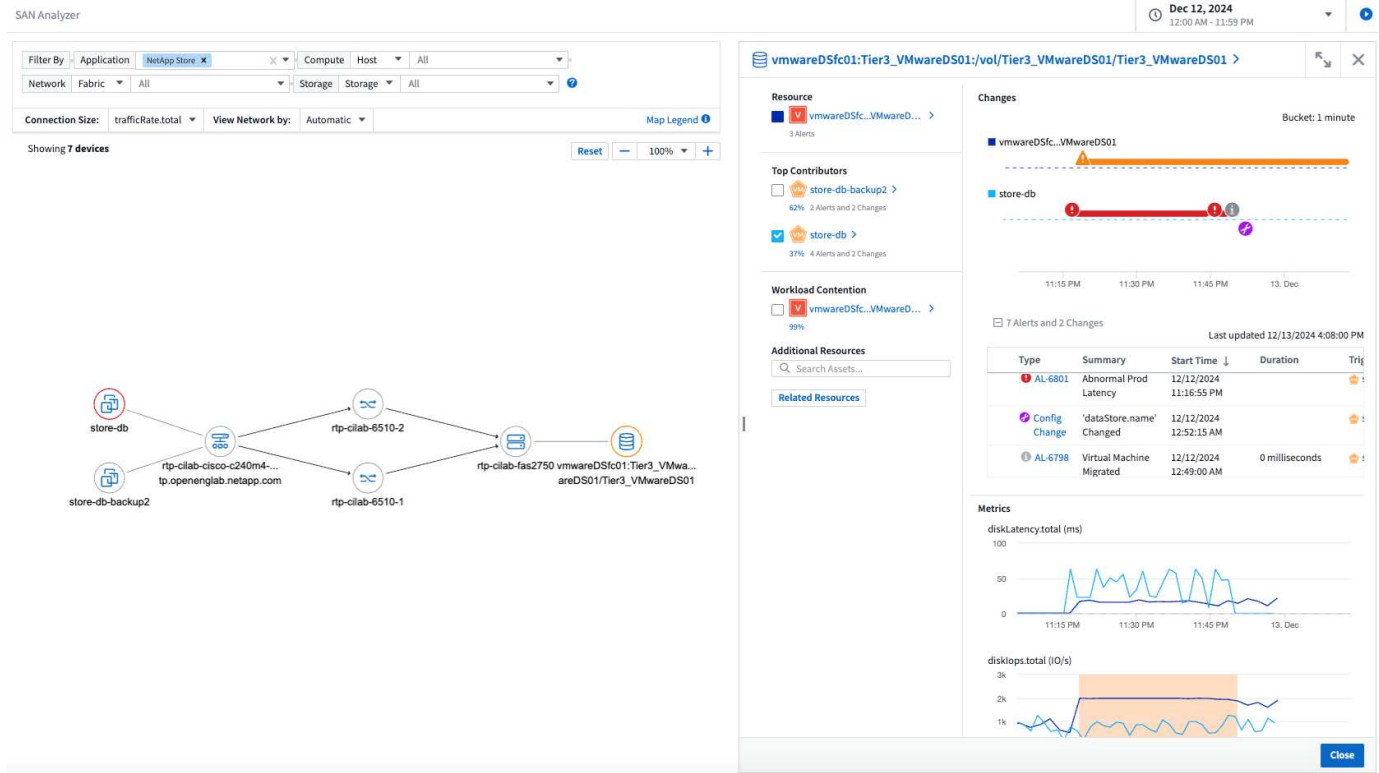
Kategorie	Indizierte Begriffe
Speicherpool	Name des „Speicherpools“ Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell Namen aller zugehörigen internen Volumes Namen aller zugehörigen Datenträger
Internes Volumen	Name des „internen Datenträgers“ Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell Name des Speicherpools Namen aller zugehörigen Freigaben Namen aller zugehörigen Anwendungen
Volumen	„Volume“-Name Bezeichnung Namen aller internen Volumes Name des Speicherpools Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell
Speicherknoten	"storage node" Name Name des Speichers IP-Adressen des Speichers Seriennummer des Speichers Speicheranbieter Speichermodell
Gastgeber	„Host“-Name IP-Adressen Namen aller zugehörigen Anwendungen
Datenspeicher	Name des „Datenspeichers“ Virtuelles Zentrum IP-Namen aller Datenträger Namen aller internen Datenträger
Virtuelle Maschinen	Name der „virtuellen Maschine“ DNS-Name IP-Adressen Name des Hosts IP-Adressen der Hostnamen aller Datenspeicher Namen aller zugehörigen Anwendungen
Switches (regulär und NPV)	"Switch" IP-Adresse WWN-Name Seriennummer Modell Domänen-ID Name des Fabric WWN des Fabric
Anwendung	"Anwendung" Name Mandant Geschäftsbereich Geschäftseinheit Projekt
Band	"Band" IP-Adresse Name Seriennummer Hersteller
Hafen	"Port" WWN-Name
Stoff	"Stoff" WWN-Name
Virtuelle Speichermaschine (SVM)	"storagevirtualmachine" Name UUID

Daten analysieren

SAN Analyzer – Übersicht

SAN spielt eine entscheidende Rolle bei der Bewältigung wichtiger Arbeitslasten, seine Komplexität kann jedoch zu erheblichen Ausfällen und Störungen für die Kunden führen. Mit dem **SAN Analyzer** von DII wird die SAN-Verwaltung einfacher und effizienter. Dieses

leistungsstarke Tool bietet End-to-End-Sichtbarkeit und bildet Abhängigkeiten von VM/Host über Netzwerk bis hin zu LUN und Speicher ab. Durch die Bereitstellung einer interaktiven Topologiekarte ermöglicht Ihnen SAN Analyzer, Probleme zu lokalisieren, Änderungen zu verstehen und das Verständnis des Datenflusses zu verbessern. Optimieren Sie die SAN-Verwaltung in komplexen IT-Umgebungen mit SAN Analyzer und erhöhen Sie Ihre Transparenz bei Block-Workloads.



Untersuchen Sie die Verbindungen zwischen Ihren Assets

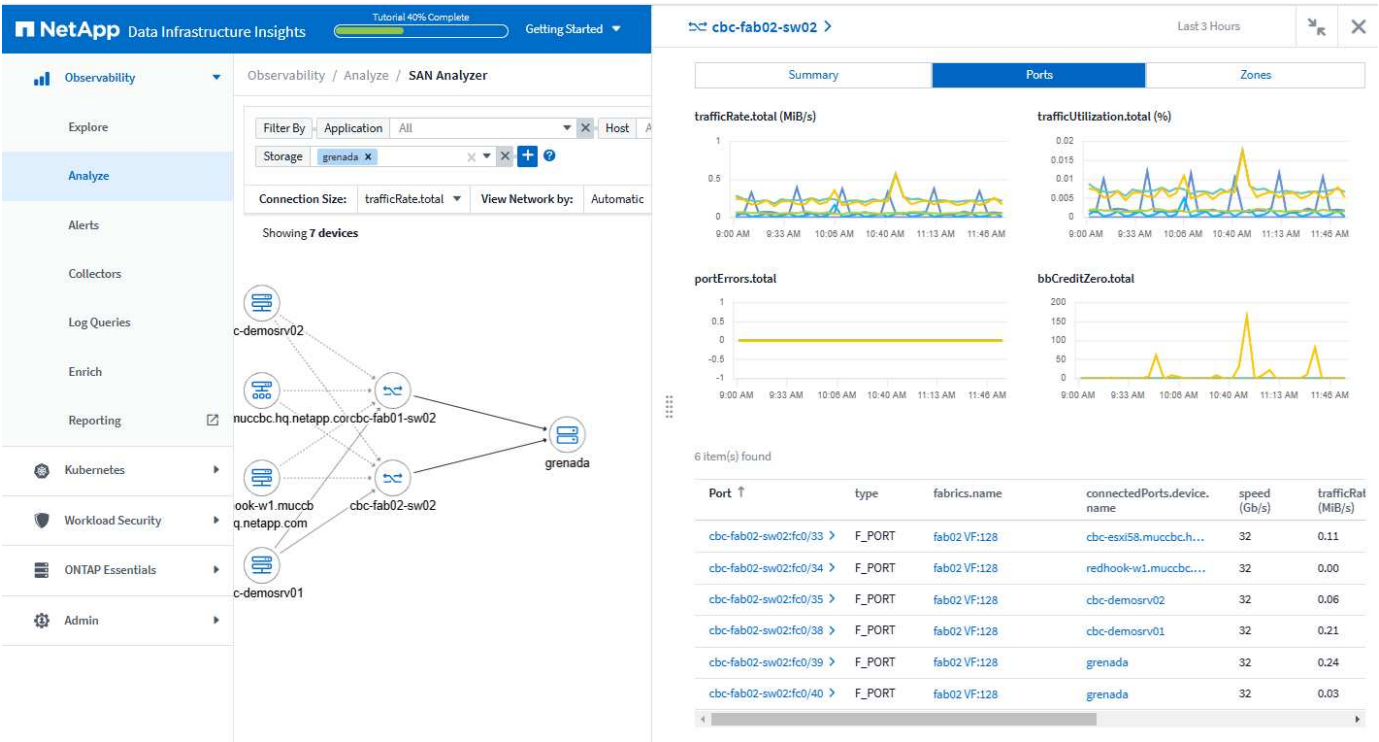
Wählen Sie **Beobachtbarkeit > Analysieren > SAN-Analysator**, um den SAN-Analysator anzuzeigen. Legen Sie einen Filter für Anwendung, Host, Fabric und/oder Speicher fest. Die Karte für die Objekte wird angezeigt und zeigt verbundene Objekte. Bewegen Sie den Mauszeiger über ein Objekt, um die Verkehrsmetriken für diese Verbindungen anzuzeigen.



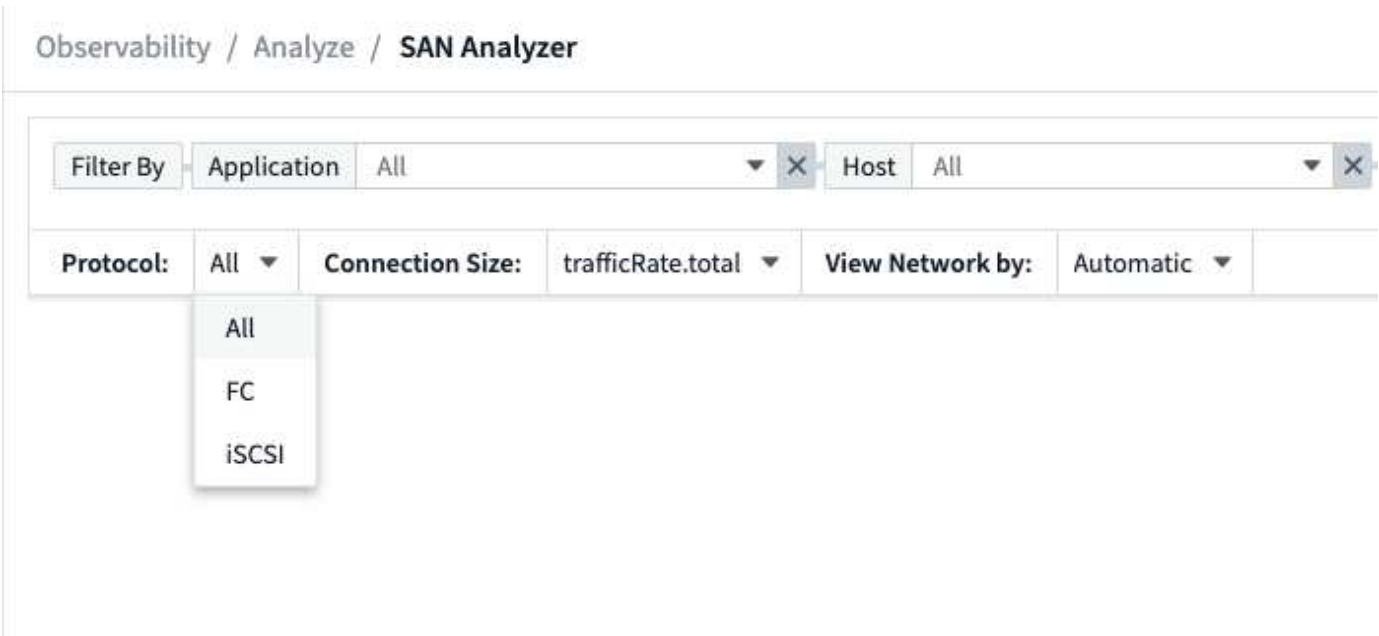
Die meisten SAN Analyzer-Filter (einschließlich derer, die Sie hinzufügen können) sind kontextbezogen. Wenn Sie in einem dieser Filter ein Objekt auswählen, werden die in den anderen Filter-Dropdowns angezeigten Auswahlmöglichkeiten im Kontext des bzw. der ausgewählten Objekte aktualisiert. Die einzigen Ausnahmen hiervon sind Anwendung, Port und Switch; diese Filter sind nicht kontextbezogen.

Durch Klicken auf ein Objekt oder eine Gruppe wird ein Slideout-Fenster geöffnet, das zusätzliche Details zum Objekt und seinen Verbindungen bietet. Das Slideout-Panel zeigt eine Zusammenfassung mit Details zum ausgewählten Objekt (z. B. IP, Hypervisor, Connected Fabrics usw., je nach Objekttyp) und Diagramme mit Metriken für das Objekt wie Latenz oder IOPS sowie gegebenenfalls Änderungen und Warnungen. Sie können bei Bedarf auch die Anzeige von Metriken für die am stärksten korrelierten Objekte in den Diagrammen auswählen.

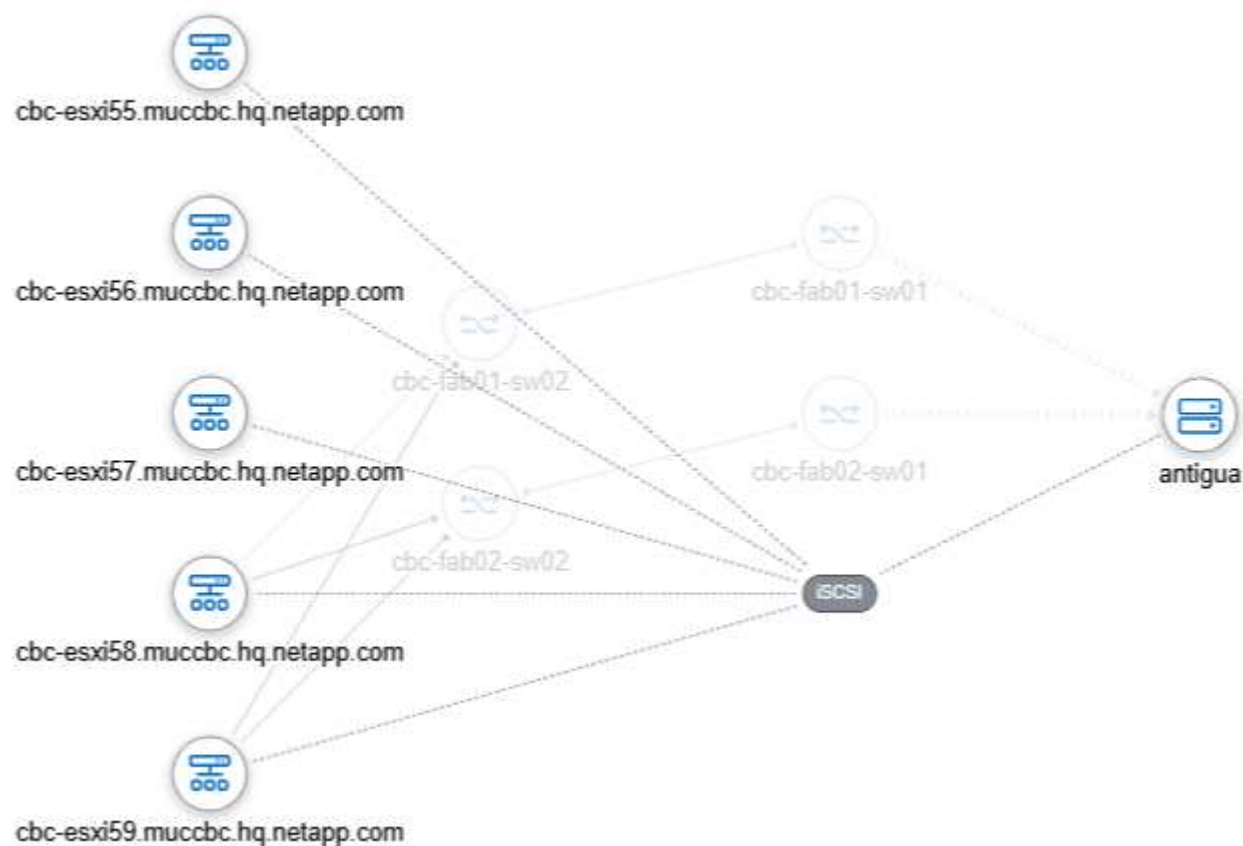
Zusätzlich zur Registerkarte „Zusammenfassung“ werden im Slideout-Bereich Registerkarten für Dinge wie Portdetails oder Zoneninformationen angezeigt, je nachdem, was für das ausgewählte Objekt zutrifft.



Wenn Ihre Umgebung über unterschiedliche Protokolle verfügt, können Sie nach iSCSI oder FC filtern:



Wenn Ihre Umgebung iSCSI-Geräte umfasst, werden durch Bewegen des Mauszeigers über das *iSCSI*-Objekt die Verbindungen hervorgehoben, die mit den entsprechenden iSCSI-Geräten in Zusammenhang stehen.



Tipps zur Fehlerbehebung

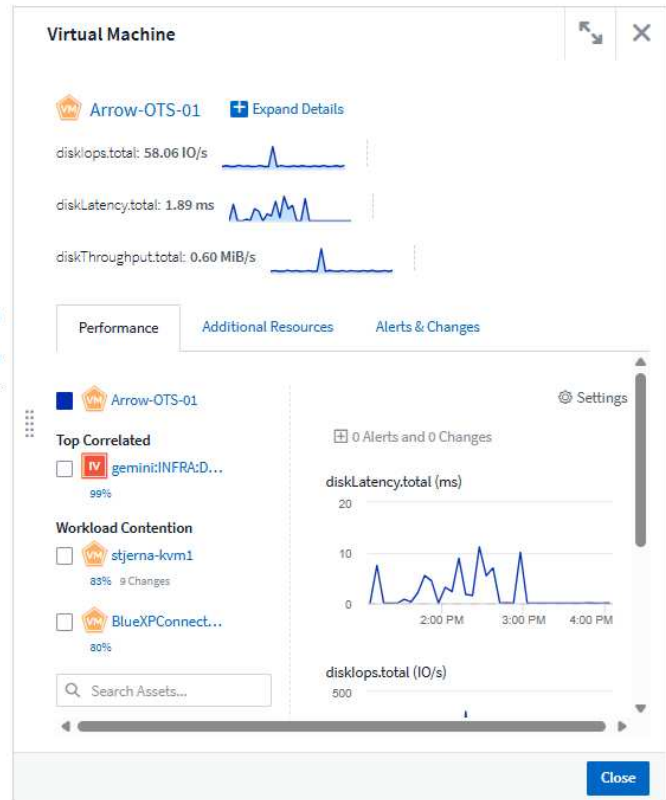
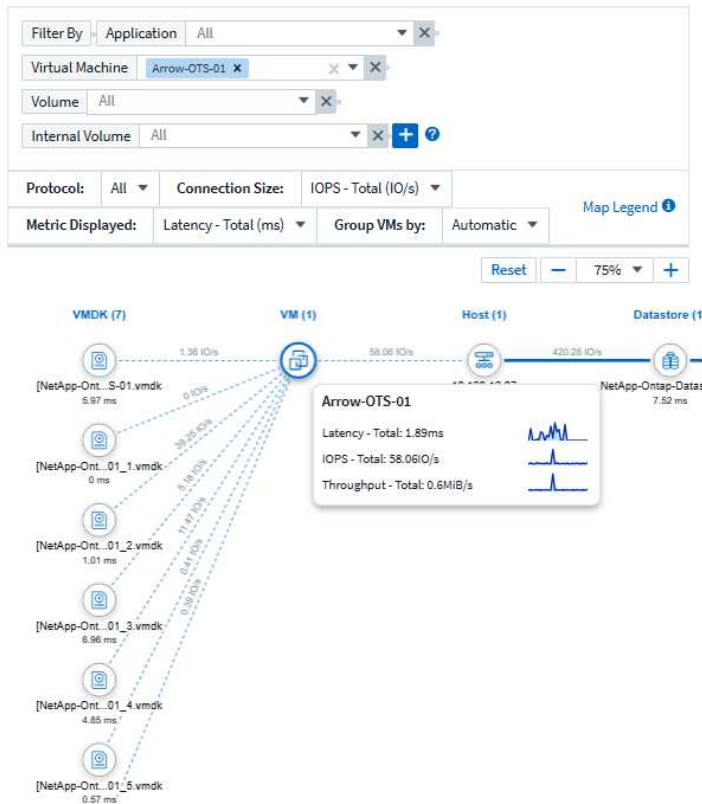
Wenn Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich sehe <0, =0 oder >0 in der Legende für Metriken wie <i>trafficUtilization</i> oder <i>trafficRate</i> .	Dies kann in sehr seltenen Fällen passieren, wenn die Metrikwerte weniger als zwei Dezimalstellen aufweisen, beispielsweise 0,000123. Eine Erweiterung des Zeitfensters kann dabei helfen, die Metrik effektiver zu analysieren.

VM Analyzer – Übersicht

Mit dem **VM Analyzer** von DII wird die Verwaltung Ihrer virtuellen Assets einfacher und effizienter. Dieses leistungsstarke Tool bietet End-to-End-Sichtbarkeit und ordnet Abhängigkeiten von VMDK/VM über Host und Datastore bis hin zu internem Volume/Volume und Speicher zu.

Durch die Bereitstellung einer interaktiven Topologiekarte ermöglicht Ihnen VM Analyzer, Probleme zu lokalisieren, Änderungen zu verstehen und das Verständnis des Datenflusses zu verbessern. Optimieren Sie die VM-Verwaltung und erhöhen Sie Ihre Transparenz bei virtuellen Workloads.



Untersuchen Sie die Verbindungen zwischen Ihren Assets

Wählen Sie **Beobachtbarkeit > Analysieren > VM-Analysator**, um den VM-Analysator anzuzeigen. Legen Sie einen Filter für Anwendung, virtuelle Maschine, Volume, internes Volume fest oder fügen Sie Ihre eigenen Filter hinzu. Die Karte für die Objekte wird angezeigt und zeigt verbundene Objekte. Bewegen Sie den Mauszeiger über ein Objekt, um die Verkehrsmetriken für diese Verbindungen anzuzeigen.



Die meisten VM Analyzer-Filter (einschließlich derer, die Sie hinzufügen können) sind kontextbezogen. Wenn Sie in einem dieser Filter ein Objekt auswählen, werden die in den anderen Filter-Dropdowns angezeigten Auswahlmöglichkeiten im Kontext mit dem bzw. den ausgewählten Objekten aktualisiert.

Durch Klicken auf ein Objekt oder eine Gruppe wird ein Slideout-Fenster geöffnet, das zusätzliche Details zum Objekt und seinen Verbindungen bietet. Das Slideout-Panel zeigt eine Zusammenfassung mit Details zum ausgewählten Objekt (z. B. Durchsatz oder Auslastung, je nach Objekttyp) sowie Diagramme mit Metriken für das Objekt wie Latenz oder IOPS. Über zusätzliche Registerkarten können Sie zugehörige zusätzliche

Ressourcen oder Änderungen und Warnungen erkunden. Sie können bei Bedarf auch die Anzeige von Metriken für die am stärksten korrelierten oder konkurrierenden Objekte in den Diagrammen auswählen.

Sehen Sie es in Aktion

[Vereinfachte Fehlerbehebung mit VM Analyzer \(Video\)](#), [Fenster=Später lesen](#)

Überwachen des Infrastrukturzustands

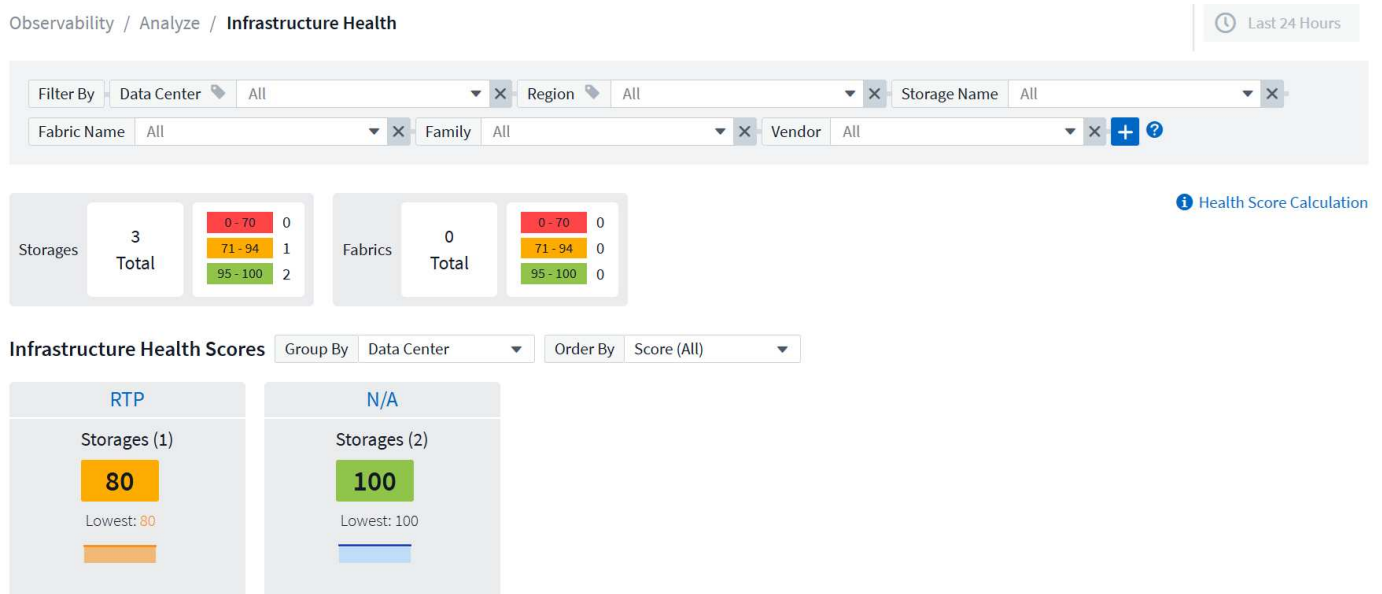
Data Infrastructure Insights bietet eine umfassende Überwachung der Infrastrukturintegrität, die Leistung, Kapazität, Konfiguration und Komponentenstatus Ihrer Speicherumgebung verfolgt. Die Integritätswerte werden auf Grundlage von Monitorwarnungen in diesen Kategorien berechnet. So erhalten Sie einen einheitlichen Überblick über die Systemintegrität und können Probleme proaktiv lösen.

Das Dashboard „Infrastructure Health“



Die Überwachung des Infrastrukturzustands ist eine **"Vorschau"** Funktion und kann sich ändern.

Navigieren Sie zu **Beobachtbarkeit > Analysieren** und wählen Sie **Infrastrukturzustand** aus. Das Dashboard bietet einen Überblick über den Zustand Ihres Systems, basierend auf den unten erläuterten Alarmkategorien und Bewertungen des Monitors. Legen Sie oben Filter fest, um den Fokus Ihrer Untersuchung einzuzugrenzen.



Standardmäßig werden Integritätswerte nach Rechenzentrum gruppiert. Sie können die Gruppierung auswählen, die für Ihre Sitzung am besten geeignet ist.

Konfigurieren Sie Monitore zur Überwachung der Infrastrukturintegrität

Die Integritätswerte werden durch Warnungen bestimmt, die für die Einbeziehung in die Berechnung der Systemintegrität konfiguriert sind.

Beim Erstellen eines Monitors für ein Infrastrukturobjekt können Sie auswählen, ob Warnungen vom Monitor in die Berechnungen einbezogen werden sollen. Erweitern Sie unten auf dem Bildschirm die erweiterte

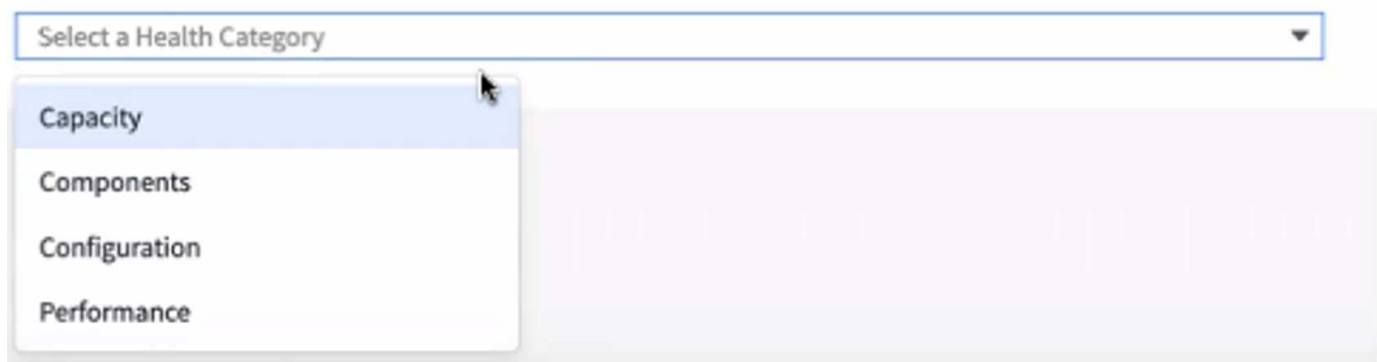
Konfiguration und wählen Sie „In Infrastrukturzustandsberechnung einbeziehen“ aus. Wählen Sie eine Kategorie aus, auf die die Berechnung für den Monitor angewendet werden soll:

- **Komponentenzustand** – Lüfterausfall, Serviceprozessor offline usw.
- **Leistungszustand** – hohe Speicherknotenauslastung, anormale Spitze der Knotenlatenz usw.
- **Kapazitätzustand** – Speicherpoolkapazität fast voll, nicht genügend Speicherplatz für LUN-Snapshot usw.
- **Konfigurationsintegrität** – Cloud-Ebene nicht erreichbar, SnapMirror -Beziehung nicht synchron usw.

☐ Advanced Configuration

Associate to an Infrastructure Health Category (optional)

☒ Include in Infrastructure Health Calculation



Gesundheitswerte erklärt

Die Punktzahlen werden auf einer Skala von 0 bis 100 angegeben, wobei 100 für volle Gesundheit steht. Überwachte Infrastrukturobjekte, bei denen derzeit oder in letzter Zeit Probleme aufgetreten sind, senken diesen Wert entsprechend den folgenden gewichteten Durchschnittswerten:

- Komponenten, Leistung oder Kapazität: jeweils 30 %
- Konfiguration: 10 %

Die Integritätswerte werden durch Warnungen beeinflusst, die von den Monitoren generiert werden, die Sie für die Berücksichtigung in der Berechnung der Infrastrukturintegrität konfiguriert haben. Dies geschieht auf folgende Weise:

- Kritische Warnungen senken den Gesundheitswert um das *volle* Kategoriegewicht
- Warnmeldungen senken die Punktzahl um die *Hälfte* des Kategoriegewichts.

Wenn für bestimmte Kategorien keine Meldungen vorliegen, wird der gewichtete Durchschnitt entsprechend angepasst.

Beispiel: 1 kritischer Alarm bei Komponenten (-30) und 1 Warnalarm bei Leistung (50 % von 30 = -15) ergeben einen Integritätswert von 55 (100 minus 45).

Wenn die Warnungen behoben werden, verschwinden diese Gesundheitsbewertungsminderungen allmählich und die Bewertung erholt sich innerhalb von zwei Stunden vollständig.

Berichterstattung

Übersicht über die Data Infrastructure Insights

Data Infrastructure Insights Reporting ist ein Business Intelligence-Tool, mit dem Sie vordefinierte Berichte anzeigen oder benutzerdefinierte Berichte erstellen können.



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar ["Premium Edition"](#). Die Verfügbarkeit der Berichtsfunktion unterliegt einer Mindestspeicherkapazitätsanforderung. ["Kontaktieren Sie Ihren NetApp Vertriebsmitarbeiter"](#) für weitere Informationen.

Mit Data Infrastructure Insights -Berichten können Sie die folgenden Aufgaben ausführen:

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

Data Infrastructure Insights Reporting kann benutzerdefinierte Berichte für Bereiche wie Chargeback, Verbrauchsanalyse und Prognose erstellen und bei der Beantwortung von Fragen wie den folgenden helfen:

- Welchen Bestand habe ich?
- Wo ist mein Inventar?
- Wer nutzt unsere Vermögenswerte?
- Wie hoch ist die Rückbuchung für zugewiesenen Speicher für eine Geschäftseinheit?
- Wie lange dauert es, bis ich zusätzliche Speicherkapazität benötige?
- Sind die Geschäftseinheiten auf die richtigen Speicherebenen ausgerichtet?
- Wie ändert sich die Speicherzuweisung im Laufe eines Monats, Quartals oder Jahres?

Zugriff auf Data Infrastructure Insights Reporting

Sie können auf die Data Infrastructure Insights -Berichterstellung zugreifen, indem Sie im Menü auf den Link **Berichte** klicken.

Sie werden zur Berichtsoberfläche weitergeleitet. Data Infrastructure Insights verwendet IBM Cognos Analytics für seine Berichts-Engine.

Was ist ETL?

Wenn Sie mit Reporting arbeiten, werden Sie die Begriffe „Data Warehouse“ und „ETL“ hören. ETL steht für „Extract, Transform, and Load“. Der ETL-Prozess ruft in Data Infrastructure Insights erfasste Daten ab und wandelt die Daten in ein Format um, das in der Berichterstattung verwendet werden kann. „Data Warehouse“ bezieht sich auf die gesammelten Daten, die für die Berichterstattung zur Verfügung stehen.

Der ETL-Prozess umfasst diese einzelnen Prozesse:

- **Extrahieren:** Nimmt Daten von Data Infrastructure Insights.
- **Transformieren:** Wendet Geschäftslogikregeln oder -funktionen auf die Daten an, während sie aus Data Infrastructure Insights extrahiert werden.
- **Laden:** Speichert die transformierten Daten zur Verwendung im Reporting im Data Warehouse.

Benutzerrollen für Data Infrastructure Insights Reporting

Wenn Sie über Data Infrastructure Insights Premium Edition mit Reporting verfügen, verfügt jeder Data Infrastructure Insights Benutzer auf Ihrem Mandanten auch über eine Single Sign-On-Anmeldung (SSO) 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 Data Infrastructure Insights bestimmt Ihre Reporting-Benutzerrolle:

Rolle „Data Infrastructure Insights“	Berichtsrolle	Berichtsberechtigungen
Gast	Verbraucher	Kann Berichte anzeigen, planen und ausführen und persönliche Einstellungen wie Sprachen und Zeitzone festlegen. Verbraucher können keine Berichte erstellen oder Verwaltungsaufgaben ausführen.
Benutzer	Autor	Kann alle Verbraucherkfunktionen ausführen sowie Berichte und Dashboards erstellen und verwalten.
Administrator	Administrator	Kann alle Autorenfunktionen sowie alle Verwaltungsaufgaben ausführen, z. B. die Konfiguration von Berichten und das Herunterfahren und Neustarten von Berichtsaufgaben.

Die folgende Tabelle zeigt die für jede Berichterstellungsrolle verfügbaren Funktionen.

Funktion	Verbraucher	Autor	Administrator
Berichte auf der Registerkarte „Teaminhalte“ anzeigen	Ja	Ja	Ja
Ausführen von Berichten	Ja	Ja	Ja
Berichte planen	Ja	Ja	Ja
Externe Dateien hochladen	Nein	Ja	Ja
Jobs erstellen	Nein	Ja	Ja
Geschichten erstellen	Nein	Ja	Ja

Erstellen von Berichten	Nein	Ja	Ja
Erstellen von Paketen und Datenmodulen	Nein	Ja	Ja
Ausführen administrativer Aufgaben	Nein	Nein	Ja
HTML-Element hinzufügen/bearbeiten	Nein	Nein	Ja
Bericht mit HTML-Element ausführen	Ja	Ja	Ja
Benutzerdefiniertes SQL hinzufügen/bearbeiten	Nein	Nein	Ja
Ausführen von Berichten mit benutzerdefiniertem SQL	Ja	Ja	Ja

Festlegen von E-Mail-Einstellungen für Reporting (Cognos)

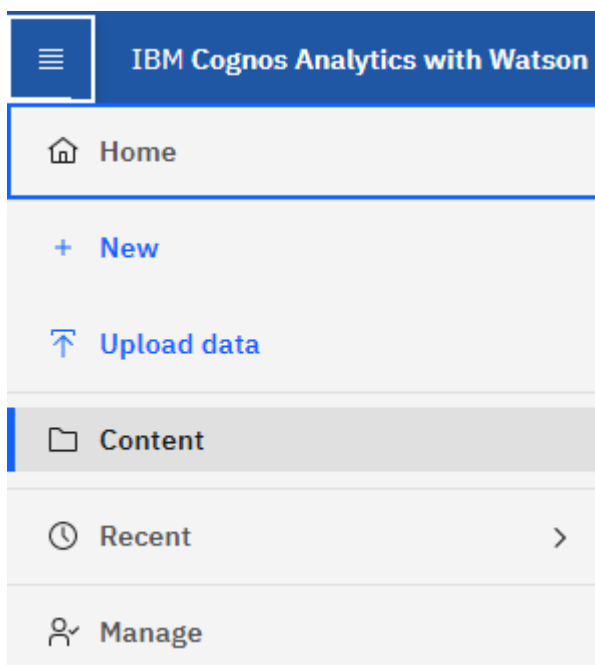


Wenn Sie Ihre E-Mail-Benutzereinstellungen in Data Infrastructure Insights Reporting (d. h. in der Cognos-Anwendung) ändern, sind diese Einstellungen *nur für die aktuelle Sitzung* aktiv. Wenn Sie sich bei Cognos ab- und wieder anmelden, werden Ihre E-Mail-Einstellungen zurückgesetzt.

Welche Schritte muss ich unternehmen, um meine vorhandene Umgebung für die Aktivierung von SSO vorzubereiten?

Um sicherzustellen, dass Ihre Berichte erhalten bleiben, migrieren Sie alle Berichte mit den folgenden Schritten von „Meine Inhalte“ zu „Teaminhalte“. Sie müssen dies tun, bevor Sie SSO auf Ihrem Mandanten aktivieren:

1. Navigieren Sie zu **Menü > Inhalt**



1. Erstellen Sie einen neuen Ordner in **Team Content**
 - a. Wenn mehrere Benutzer angelegt wurden, erstellen Sie bitte für jeden Benutzer einen eigenen Ordner, um das Überschreiben von Berichten mit doppelten Namen zu vermeiden.
2. Navigieren Sie zu **Meine Inhalte**
3. Wählen Sie alle Berichte aus, die Sie behalten möchten.
4. Wählen Sie in der oberen rechten Ecke des Menüs "Kopieren oder Verschieben"
5. Navigieren Sie zum neu erstellten Ordner in **Team Content**
6. Fügen Sie die Berichte mit den Schaltflächen „Kopieren nach“ oder „Verschieben nach“ in den neu erstellten Ordner ein
7. Sobald SSO für Cognos aktiviert ist, melden Sie sich bei Data Infrastructure Insights mit der E-Mail-Adresse an, die Sie zum Erstellen Ihres Kontos verwendet haben.
8. Navigieren Sie in Cognos zum Ordner „Team Content“ und kopieren oder verschieben Sie die zuvor gespeicherten Berichte zurück in „Meine Inhalte“.

Vordefinierte Berichte leicht gemacht

Data Infrastructure Insights Reporting umfasst vordefinierte Berichte, die eine Reihe gängiger Berichtsanforderungen erfüllen und wichtige Erkenntnisse liefern, die die Beteiligten benötigen, um fundierte Entscheidungen über ihre Speicherinfrastruktur zu treffen.



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar **"Premium Edition"** .

Sie können vordefinierte Berichte aus dem Data Infrastructure Insights Reporting Portal erstellen, sie per E-Mail an andere Benutzer senden und sie sogar ändern. Mehrere Berichte ermöglichen Ihnen das Filtern nach Gerät, Geschäftseinheit oder Ebene. Die Berichtstools verwenden IBM Cognos als Grundlage und bieten Ihnen zahlreiche Möglichkeiten zur Datenpräsentation.

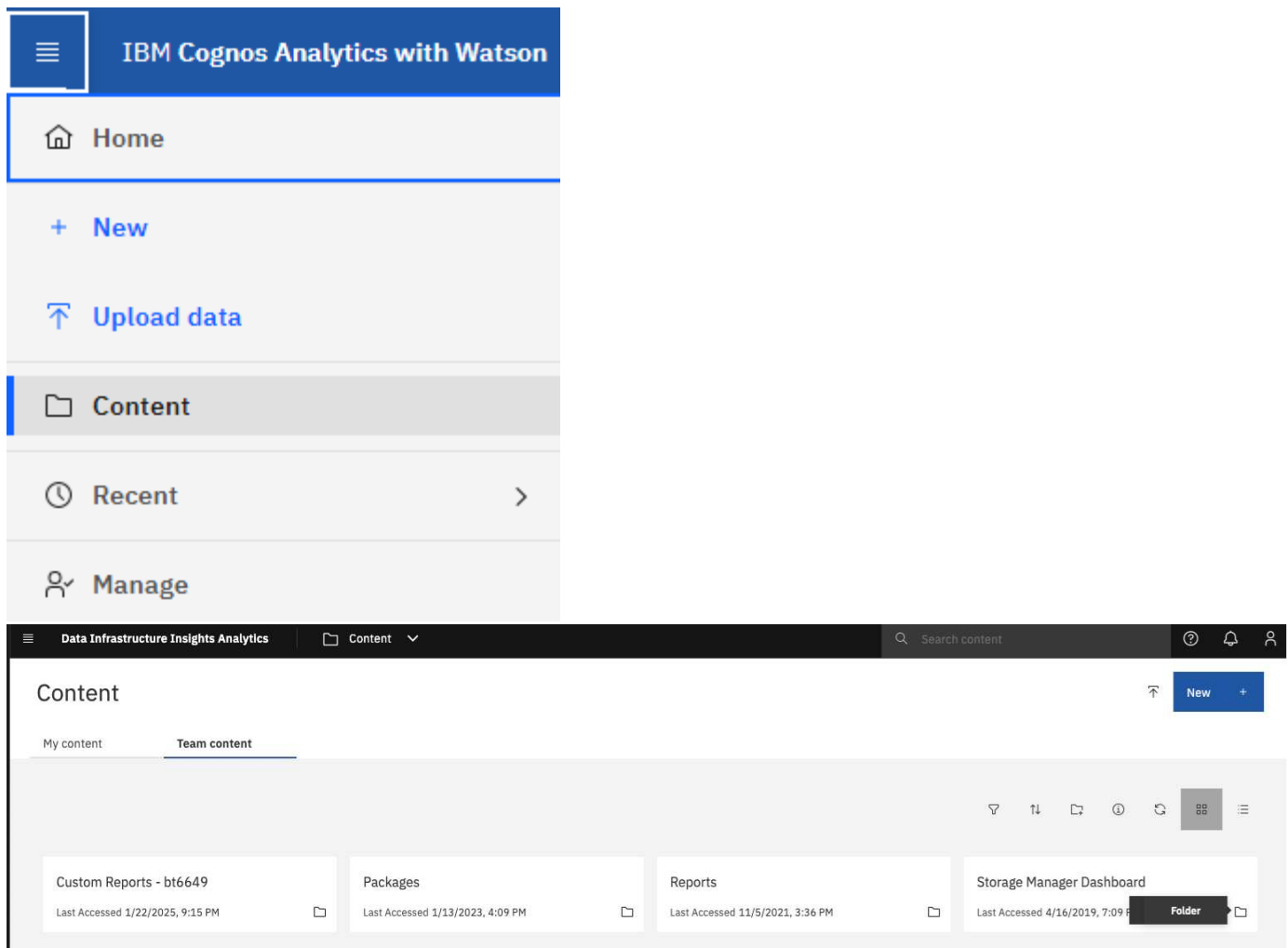
Die vordefinierten Berichte zeigen Ihre Daten zu Inventar, Speicherkapazität, Rückbuchung, Leistung, Speichereffizienz und Cloud-Kosten. Sie können diese vordefinierten Berichte ändern und Ihre Änderungen speichern.

Sie können Berichte in verschiedenen Formaten erstellen, darunter HTML, PDF, CSV, XML und Excel.

Navigieren zu vordefinierten Berichten

Wenn Sie das Reporting-Portal öffnen, ist der Ordner „Team Content“ der Ausgangspunkt für die Auswahl der Art von Informationen, die Sie in den Data Infrastructure Insights -Berichten benötigen.

1. Wählen Sie im linken Navigationsbereich **Inhalt > Teaminhalt** aus.
2. Wählen Sie **Berichte**, um auf die vordefinierten Berichte zuzugreifen.



Verwenden vordefinierter Berichte zum Beantworten häufiger Fragen

Die folgenden vordefinierten Berichte sind unter **Teaminhalte > Berichte** verfügbar.

Kapazität und Leistung der Anwendungsdienstebene

Der Bericht zur Service-Level-Kapazität und -Leistung von Anwendungen bietet einen umfassenden Überblick über Ihre Anwendungen. Sie können diese Informationen für die Kapazitätsplanung oder einen Migrationsplan verwenden.

Rückbuchung

Der Chargeback-Bericht bietet Informationen zum Chargeback der Speicherkapazität und zur Verantwortlichkeit nach Hosts, Anwendungen und Geschäftseinheiten und enthält sowohl aktuelle als auch historische Daten.

Um eine Doppelzählung zu vermeiden, schließen Sie keine ESX-Server ein, überwachen Sie nur die VMs.

Datenquellen

Der Bericht „Datenquellen“ zeigt alle auf Ihrer Site installierten Datenquellen, den Status der Datenquelle (Erfolg/Fehler) und Statusmeldungen. Der Bericht enthält Informationen dazu, wo Sie mit der Fehlerbehebung bei Datenquellen beginnen können. Fehlerhafte Datenquellen beeinträchtigen die Genauigkeit der Berichterstattung und die allgemeine Benutzerfreundlichkeit des Produkts.

ESX vs. VM-Leistung

Der Bericht „ESX vs. VM-Leistung“ bietet einen Vergleich von ESX-Servern und VMs und zeigt durchschnittliche und Spitzen-IOPs, Durchsatz sowie Latenz und Auslastung für ESX-Server und VMs. Um eine Doppelzählung zu vermeiden, schließen Sie die ESX-Server aus und schließen Sie nur die VMs ein. Eine aktualisierte Version dieses Berichts ist im NetApp Storage Automation Store verfügbar.

Stoffübersicht

Der Fabric-Zusammenfassungsbericht identifiziert Switches und Switch-Informationen, einschließlich Portanzahl, Firmware-Versionen und Lizenzstatus. Der Bericht enthält keine NPV-Switch-Ports.

Host-HBAs

Der Host-HBA-Bericht bietet einen Überblick über die Hosts in der Umgebung und gibt den Anbieter, das Modell und die Firmware-Version der HBAs sowie die Firmware-Ebene der Switches an, mit denen sie verbunden sind. Dieser Bericht kann verwendet werden, um die Firmware-Kompatibilität zu analysieren, wenn ein Firmware-Upgrade für einen Switch oder einen HBA geplant wird.

Kapazität und Leistung des Host-Service-Levels

Der Bericht „Host Service Level Capacity and Performance“ bietet einen Überblick über die Speicherauslastung nach Host für Nur-Block-Anwendungen.

Host-Zusammenfassung

Der Host-Zusammenfassungsbericht bietet einen Überblick über die Speicherauslastung jedes ausgewählten Hosts mit Informationen zu Fibre Channel- und iSCSI-Hosts. Mit dem Bericht können Sie Ports und Pfade, die Fibre Channel- und iSCSI-Kapazität sowie die Anzahl der Verstöße vergleichen.

Lizenzdetails

Der Bericht „Lizenzdetails“ zeigt die Menge der Ressourcen an, für die Sie über eine Lizenz verfügen, und zwar für alle Sites mit aktiven Lizenzen. Der Bericht zeigt auch eine Zusammenfassung der tatsächlichen Menge aller Sites mit aktiven Lizenzen. Die Summierung kann Überschneidungen von Speicher-Arrays enthalten, die von mehreren Servern verwaltet werden.

Zugeordnete, aber nicht maskierte Volumes

Der Bericht „Zugeordnete, aber nicht maskierte Volumes“ listet die Volumes auf, deren logische Gerätenummer (LUN) für die Verwendung durch einen bestimmten Host zugeordnet wurde, für diesen Host jedoch nicht maskiert ist. In einigen Fällen kann es sich dabei um stillgelegte LUNs handeln, die demaskiert wurden. Auf nicht maskierte Volumes kann von jedem Host aus zugegriffen werden, wodurch sie anfällig für Datenbeschädigungen sind.

NetApp Kapazität und Performance

Der NetApp Kapazitäts- und Leistungsbericht bietet globale Daten zur zugewiesenen, genutzten und zugesagten Kapazität mit Trend- und Leistungsdaten zur NetApp -Kapazität.

Scorecard

Der Scorecard-Bericht bietet eine Zusammenfassung und den allgemeinen Status aller von Data Infrastructure Insights erworbenen Assets. Der Status wird durch grüne, gelbe und rote Flaggen angezeigt:

- Grün zeigt den Normalzustand an
- Gelb weist auf ein potenzielles Problem in der Umgebung hin
- Rot weist auf ein Problem hin, das Aufmerksamkeit erfordert

Alle Felder im Bericht werden im mit dem Bericht bereitgestellten Datenwörterbuch beschrieben.

Speicherübersicht

Der Speicherzusammenfassungsbericht bietet eine globale Zusammenfassung der verwendeten und ungenutzten Kapazitätsdaten für Roh- und zugewiesene Speicherpools und Volumes. Dieser Bericht bietet einen Überblick über alle erkannten Speicher.

VM-Kapazität und -Leistung

Beschreibt die Umgebung der virtuellen Maschine (VM) und ihre Kapazitätsnutzung. Um bestimmte Daten anzuzeigen, beispielsweise wann VMs heruntergefahren wurden, müssen VM-Tools aktiviert sein.

VM-Pfade

Der Bericht „VM-Pfade“ liefert Daten zur Speicherkapazität und Leistungsmetriken für die virtuelle Maschine, die auf dem Host ausgeführt wird, die Hosts, die auf die freigegebenen Volumes zugreifen, den aktiven Zugriffspfad und die Kapazitätszuweisung und -nutzung.

HDS-Kapazität nach Thin Pool

Der Bericht „HDS-Kapazität nach Thin Pool“ zeigt die Menge der nutzbaren Kapazität eines Thin Provisioning-Speicherpools.

NetApp -Kapazität nach Aggregat

Der Bericht „NetApp -Kapazität nach Aggregat“ zeigt den gesamten Rohspeicherplatz, den gesamten, den genutzten, den verfügbaren und den zugesicherten Speicherplatz der Aggregate an.

Symmetrix-Kapazität durch Thick Array

Der Bericht „Symmetrix-Kapazität nach Thick-Array“ zeigt Rohkapazität, nutzbare Kapazität, freie Kapazität, zugeordnete, maskierte und gesamte freie Kapazität.

Symmetrix-Kapazität nach Thin Pool

Der Bericht „Symmetrix-Kapazität nach Thin Pool“ zeigt Rohkapazität, nutzbare Kapazität, genutzte Kapazität, freie Kapazität, genutzten Prozentsatz, abonnierte Kapazität und Abonnementrate.

XIV Kapazität nach Array

Der XIV-Kapazitätsbericht nach Array zeigt die verwendete und ungenutzte Kapazität für das Array.

XIV Kapazität nach Pool

Der XIV-Kapazitätsbericht nach Pool zeigt die genutzte und ungenutzte Kapazität für Speicherpools.

Storage Manager-Dashboard

Das Storage Manager Dashboard bietet Ihnen eine zentrale Visualisierung, mit der Sie

die Ressourcennutzung im Zeitverlauf mit den akzeptablen Bereichen und den Aktivitätstagen der vorherigen Tage vergleichen und gegenüberstellen können. Indem nur die wichtigsten Leistungskennzahlen für Ihre Speicherdienste angezeigt werden, können Sie Entscheidungen zur Wartung Ihrer Rechenzentren treffen.



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar ["Premium Edition"](#) .

Zusammenfassung

Wenn Sie unter „Teaminhalte“ das „Storage Manager Dashboard“ auswählen, erhalten Sie mehrere Berichte mit Informationen zu Ihrem Datenverkehr und Speicher.

IBM Cognos Analytics with Watson | Content

Storage Manager Dashboard

My content | **Team content**

Team content / Storage Manager Dashboard

Report Title	Last Accessed
Data Center Traffic Details	4/17/2019, 6:47 PM
Orphaned Storage Details	5/2/2019, 8:30 PM
<u>Storage Manager Report</u>	12/17/2019, 9:44 PM
Storage Pools Capacity and Performance Details	4/17/2019, 6:47 PM

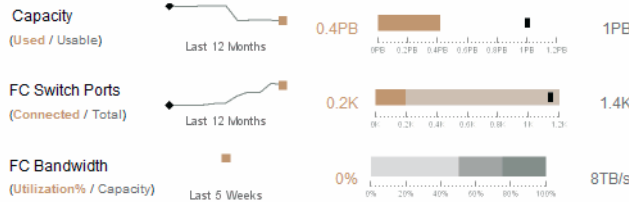
Für eine Übersicht auf einen Blick besteht der **Storage Manager-Bericht** aus sieben Komponenten, die Kontextinformationen zu vielen Aspekten Ihrer Speicherumgebung enthalten. Sie können die Aspekte Ihrer Speicherdienste genauer untersuchen, um eine eingehende Analyse des Abschnitts durchzuführen, der Sie am meisten interessiert.

NetApp Storage Manager Dashboard

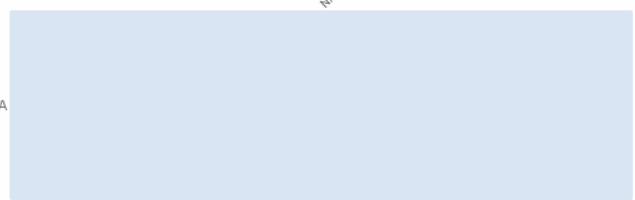
(Data as of Jan 28, 2016)

Summary

History (Target; Actual; Forecast; Low; Mid; High)

**Data Centers Time to Full**

(<3 months; 3-6 months; >6 months)

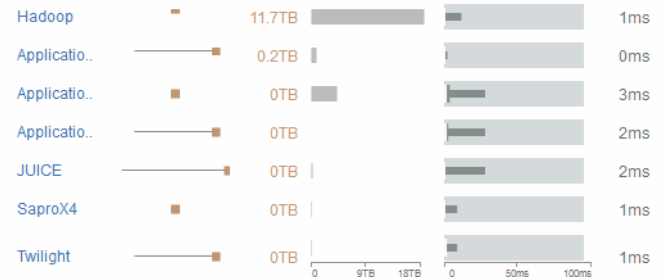
**Storage Tiers Capacity**

(Target; Actual; Forecast)

Last 12 Months Used Capacity Total Capacity Months to Full

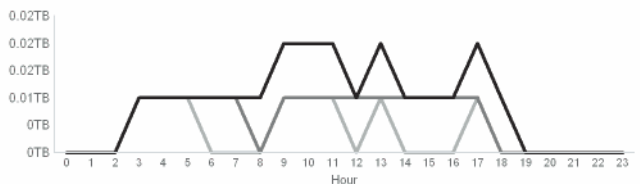
**Top 10 Applications**

Last 12 Months Used Allocated Response Time (Acceptable)

**Daily Storage Traffic**

(Terabytes)

Daily mean for last 6 months Daily mean for last 7 days Yesterday

**Storage Tiers Daily Performance**

(Acceptable)

Response Time Throughput (IOPS)

N/A 0 7350 14699ms 745ms 0 9534 19067IOPS 10211IOPS

Orphaned Capacity

35TB 3.4%

0TB 10TB 20TB 30TB 40TB

Auto Tie... N/A

Diese Komponente zeigt die verwendete Speicherkapazität im Vergleich zur nutzbaren Speicherkapazität, die Gesamtzahl der Switch-Ports im Vergleich zur Anzahl der verbundenen Switch-Ports und die Gesamtauslastung der verbundenen Switch-Ports im Vergleich zur Gesamtbandbreite sowie die Entwicklung dieser Werte im Zeitverlauf. Sie können die tatsächliche Nutzung im Vergleich zu den niedrigen, mittleren und hohen Bereichen anzeigen. So können Sie die Nutzung zwischen Prognosen und Ihren gewünschten tatsächlichen Werten auf der Grundlage eines Ziels vergleichen und gegenüberstellen. Für Kapazität und Switch-Ports können Sie dieses Ziel konfigurieren. Die Prognose basiert auf einer Extrapolation der aktuellen Wachstumsrate und des von Ihnen festgelegten Datums. Wenn die prognostizierte genutzte Kapazität, die auf dem Prognosedatum für die zukünftige Nutzung basiert, das Ziel überschreitet, wird neben „Kapazität“ eine Warnung (durchgezogener roter Kreis) angezeigt.

Speicherebenenkapazität

Diese Komponente zeigt die genutzte Kapazität der Stufe im Vergleich zur der Stufe zugewiesenen Kapazität. Dies gibt an, wie die genutzte Kapazität über einen Zeitraum von 12 Monaten zunimmt oder abnimmt und wie viele Monate bis zur vollständigen Auslastung verbleiben. Die Kapazitätsauslastung wird mit den angegebenen Werten für die tatsächliche Auslastung, die Auslastungsprognose und ein von Ihnen konfigurierbares Kapazitätsziel angezeigt. Wenn die prognostizierte genutzte Kapazität, die auf dem Prognosedatum für die zukünftige Nutzung basiert, die Zielkapazität überschreitet, wird neben einer Stufe eine Warnung (durchgezogener roter Kreis) angezeigt.

Sie können auf eine beliebige Ebene klicken, um den Bericht „Kapazitäts- und Leistungsdetails der Speicherpools“ anzuzeigen. Darin werden freie und genutzte Kapazitäten, die Anzahl der Tage bis zur vollständigen Belegung sowie Leistungsdetails (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Ebene angezeigt. Sie können in diesem Bericht auch auf einen beliebigen Speicher- oder Speicherpoolnamen klicken, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Täglicher Speicherverkehr

Diese Komponente zeigt die Leistung der Umgebung und ob es im Vergleich zu den letzten sechs Monaten zu starkem Wachstum, Änderungen oder potenziellen Problemen kommt. Außerdem wird der durchschnittliche Verkehr im Vergleich zum Verkehr der letzten sieben Tage und des Vortages angezeigt. Sie können alle Anomalien in der Leistung der Infrastruktur visualisieren, da Informationen bereitgestellt werden, die sowohl zyklische (letzte sieben Tage) als auch saisonale Schwankungen (letzte sechs Monate) hervorheben.

Sie können auf den Titel (Täglicher Speicherverkehr) klicken, um den Bericht „Speicherverkehrsdetails“ anzuzeigen, der die Heatmap des stündlichen Speicherverkehrs des vorherigen Tages für jedes Speichersystem zeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speichernamen, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Zeit bis zur Auslastung von Rechenzentren

Diese Komponente zeigt alle Rechenzentren im Vergleich zu allen Ebenen und wie viel Kapazität in jedem Rechenzentrum für jede Speicherebene basierend auf den prognostizierten Wachstumsraten verbleibt. Die Kapazitätsstufe wird in Blau angezeigt. Je dunkler die Farbe, desto weniger Zeit bleibt der Stufe am Standort, bevor sie voll ist.

Sie können auf einen Abschnitt einer Ebene klicken, um den Bericht „Tage bis zur vollständigen Belegung der Speicherpools“ anzuzeigen. Darin werden die Gesamtkapazität, die freie Kapazität und die Anzahl der Tage bis zur vollständigen Belegung für alle Pools in der ausgewählten Ebene und im Rechenzentrum angezeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speicher- oder Speicherpoolnamen, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Top 10 Anwendungen

Diese Komponente zeigt die Top 10-Anwendungen basierend auf der verwendeten Kapazität. Unabhängig davon, wie die Ebene die Daten organisiert, zeigt dieser Bereich die aktuell genutzte Kapazität und den Anteil der Infrastruktur an. Sie können die Bandbreite der Benutzererfahrung der letzten sieben Tage visualisieren, um zu sehen, ob die Verbraucher akzeptable (oder, noch wichtiger, inakzeptable) Reaktionszeiten erlebt haben.

In diesem Bereich werden auch Trends angezeigt, die darauf hinweisen, ob die Anwendungen ihre Leistungs-Servicelevelziele (SLO) erfüllen. Sie können die minimale Antwortzeit der vorherigen Woche, das erste Quartil, das dritte Quartil und die maximale Antwortzeit anzeigen, wobei ein Median gegenüber einem akzeptablen SLO angezeigt wird, das Sie konfigurieren können. Wenn die mittlere Antwortzeit für eine Anwendung außerhalb des akzeptablen SLO-Bereichs liegt, wird neben der Anwendung eine Warnung (durchgezogener roter Kreis) angezeigt. Sie können auf eine Anwendung klicken, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Tägliche Leistung der Speicherebenen

Diese Komponente zeigt eine Zusammenfassung der Leistung der Ebene hinsichtlich Reaktionszeit und IOPS für die letzten sieben Tage. Diese Leistung wird mit einem SLO verglichen, das Sie konfigurieren können. So können Sie erkennen, ob die Möglichkeit besteht, Ebenen zu konsolidieren, die von diesen Ebenen bereitgestellten Arbeitslasten neu auszurichten oder Probleme mit bestimmten Ebenen zu identifizieren. Wenn die mittlere Antwortzeit oder der mittlere IOPS außerhalb des akzeptablen SLO-Bereichs liegt, wird neben einer Stufe eine Warnung (durchgezogener roter Kreis) angezeigt.

Sie können auf einen Tier-Namen klicken, um den Bericht „Kapazitäts- und Leistungsdetails der Speicherpools“ anzuzeigen. Darin werden freie und genutzte Kapazitäten, die Anzahl der Tage bis zur vollständigen Befüllung sowie Leistungsdetails (IOPS und Reaktionszeit) für alle Pools im ausgewählten Tier angezeigt. Klicken Sie in diesem Bericht auf einen beliebigen Speicher oder Speicherpool, um die Asset-Seite

mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Verwaiste Kapazität

Diese Komponente zeigt die gesamte verwaiste Kapazität und die verwaiste Kapazität nach Ebene an, vergleicht sie mit akzeptablen Bereichen für die gesamte nutzbare Kapazität und zeigt die tatsächlich verwaiste Kapazität an. Verwaiste Kapazität wird durch Konfiguration und Leistung definiert. Durch Konfiguration verwaister Speicher beschreibt eine Situation, in der einem Host Speicher zugewiesen ist. Die Konfiguration wurde jedoch nicht ordnungsgemäß durchgeführt und der Host kann nicht auf den Speicher zugreifen. Von „verwaist durch Leistung“ spricht man, wenn der Speicher korrekt für den Zugriff durch einen Host konfiguriert ist. Es gab jedoch keinen Speicherverkehr.

Der horizontale gestapelte Balken zeigt die akzeptablen Bereiche. Je dunkler das Grau, desto inakzeptabler ist die Situation. Die tatsächliche Situation wird durch den schmalen bronzenen Balken dargestellt, der die tatsächlich verwaiste Kapazität anzeigt.

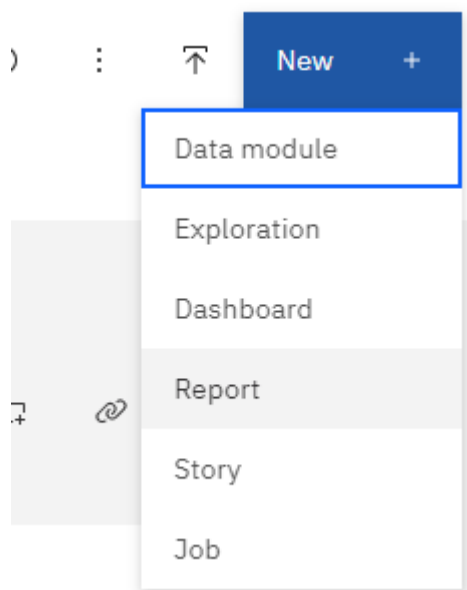
Sie können auf eine Ebene klicken, um den Bericht „Verwaiste Speicherdetails“ anzuzeigen. Darin sind alle Volumes aufgeführt, die aufgrund ihrer Konfiguration und Leistung für die ausgewählte Ebene als verwaist identifiziert wurden. Klicken Sie in diesem Bericht auf einen beliebigen Speicher, Speicherpool oder Datenträger, um die Asset-Seite mit einer Zusammenfassung des aktuellen Status dieser Ressource anzuzeigen.

Erstellen eines Berichts (Beispiel)

Verwenden Sie die Schritte in diesem Beispiel, um einen einfachen Bericht über die physische Kapazität von Speicher und Speicherpools in mehreren Rechenzentren zu erstellen.

Schritte

1. Navigieren Sie zu **Menü > Inhalt > Teaminhalt > Berichte**
2. Wählen Sie oben rechts auf dem Bildschirm **[Neu +]**
3. Wählen Sie **Bericht**



4. Wählen Sie auf der Registerkarte **Vorlagen Leer**

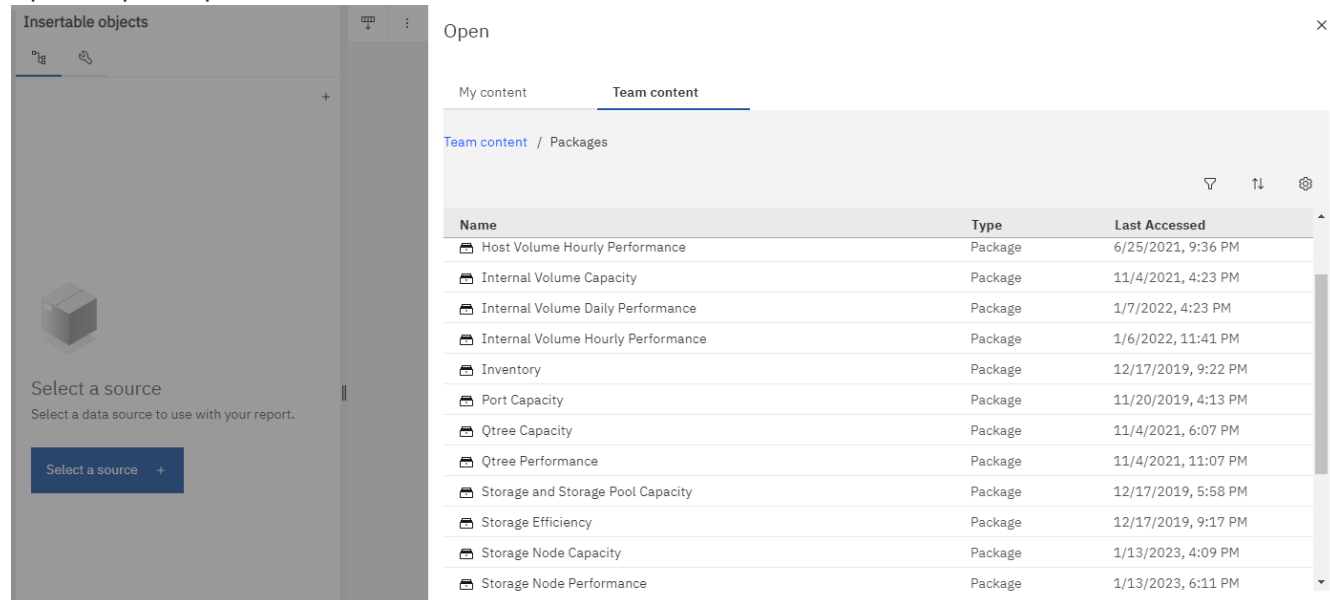
Die Registerkarten Quelle und Daten werden angezeigt

5. Öffnen **Quelle auswählen +**

6. Öffnen Sie unter **Teaminhalte Pakete**

Es wird eine Liste der verfügbaren Pakete angezeigt.

7. Wählen Sie ***Speicher und Speicherpoolkapazität***



The screenshot shows a software interface with two main panels. The left panel, titled 'Insertable objects', contains a 'Select a source' button. The right panel, titled 'Open', has tabs for 'My content' and 'Team content'. Under 'Team content', there is a sub-tab 'Packages' which displays a table of available data packages.

Name	Type	Last Accessed
Host Volume Hourly Performance	Package	6/25/2021, 9:36 PM
Internal Volume Capacity	Package	11/4/2021, 4:23 PM
Internal Volume Daily Performance	Package	1/7/2022, 4:23 PM
Internal Volume Hourly Performance	Package	1/6/2022, 11:41 PM
Inventory	Package	12/17/2019, 9:22 PM
Port Capacity	Package	11/20/2019, 4:13 PM
Qtree Capacity	Package	11/4/2021, 6:07 PM
Qtree Performance	Package	11/4/2021, 11:07 PM
Storage and Storage Pool Capacity	Package	12/17/2019, 5:58 PM
Storage Efficiency	Package	12/17/2019, 9:17 PM
Storage Node Capacity	Package	1/13/2023, 4:09 PM
Storage Node Performance	Package	1/13/2023, 6:11 PM

8. Wählen Sie **Öffnen**

Die verfügbaren Stile für Ihren Bericht werden angezeigt.

9. Wählen Sie **Liste**

Fügen Sie passende Namen für Liste und Abfrage hinzu

10. Wählen Sie **OK**

11. Erweitern Sie *Physische Kapazität*

12. Erweitern Sie auf die unterste Ebene des *Rechenzentrums*

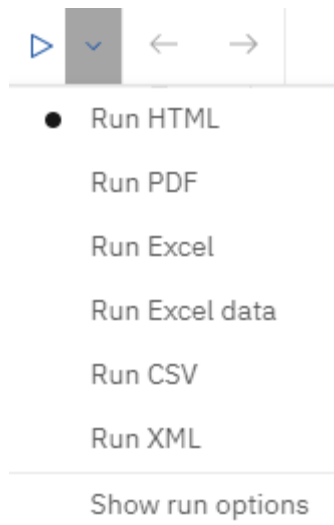
13. Ziehen Sie „Data Center“ in die Berichtspalette.

14. Erweitern Sie *Kapazität (MB)*

15. Ziehen Sie *Kapazität (MB)* in die Berichtspalette.














16. Ziehen Sie „Verwendete Kapazität (MB)“ in die Berichtspalette.

17. Führen Sie den Bericht aus, indem Sie im Menü **Ausführen** einen Ausgabetyt auswählen.



Ergebnis

Es wird ein Bericht ähnlich dem folgenden 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
 Top  Page up  Page down  Bottom			

Berichte verwalten

Sie können das Ausgabeformat und die Bereitstellung eines Berichts anpassen, Berichtseigenschaften oder Zeitpläne festlegen und Berichte per E-Mail versenden.



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar "[Premium Edition](#)".

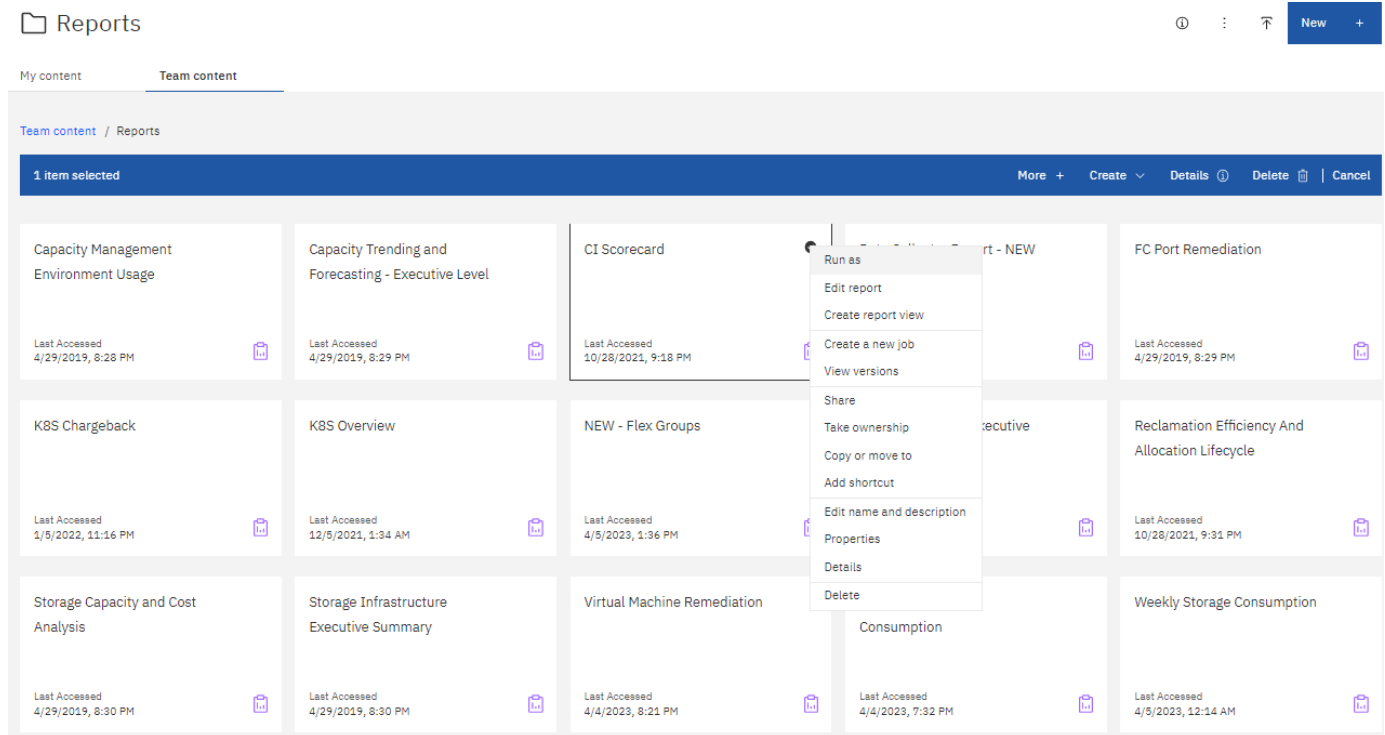


Bevor Sie Änderungen an den Berichtsberechtigungen oder der Sicherheit vornehmen, müssen Sie die Berichte „Meine Inhalte“ in den Ordner „Teaminhalte“ kopieren, um sicherzustellen, dass die Berichte gespeichert werden.

Anpassen des Ausgabeformats und der Bereitstellung eines Berichts

Sie können das Format und die Übermittlungsmethode von Berichten anpassen.

1. Gehen Sie im Data Infrastructure Insights Reporting Portal zu **Menü > Inhalt > Mein Inhalt/Teaminhalt**. Bewegen Sie die Maus über den Bericht, den Sie anpassen möchten, und öffnen Sie das Menü mit den drei Punkten.

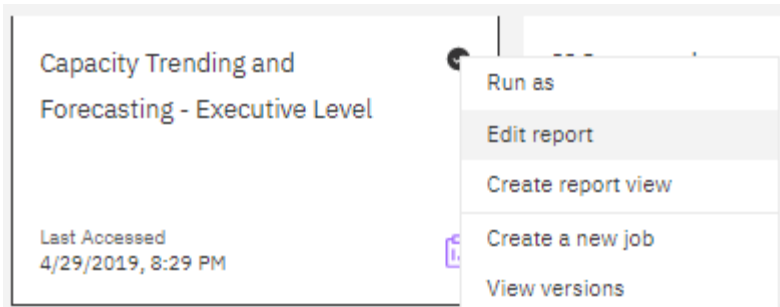


1. Klicken Sie auf **Eigenschaften > Zeitplan**
2. Sie können die folgenden Optionen festlegen:
 - **Planen** Sie, wann Berichte ausgeführt werden sollen.
 - Wählen Sie **Optionen** für Berichtsformat und -übermittlung (Speichern, Drucken, E-Mail) und Sprachen für den Bericht.
3. Klicken Sie auf **Speichern**, um den Bericht mit den von Ihnen getroffenen Auswahlen zu erstellen.

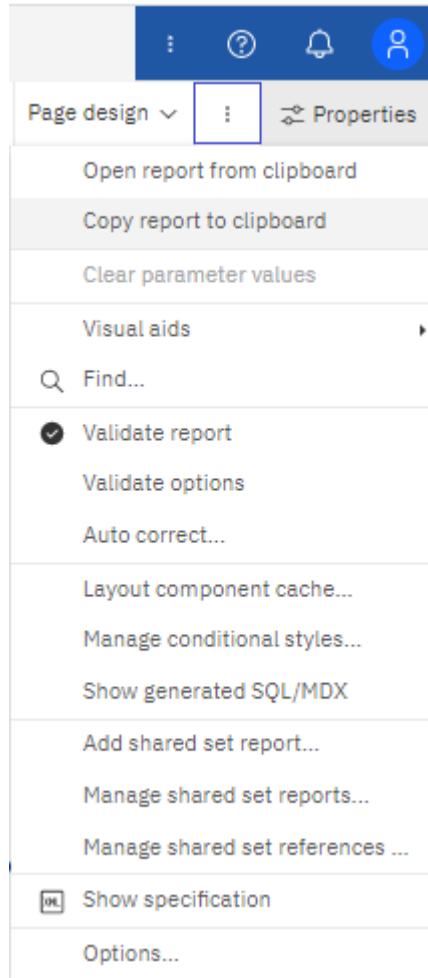
Kopieren eines Berichts in die Zwischenablage

Verwenden Sie diesen Vorgang, um einen Bericht in die Zwischenablage zu kopieren.

1. Wählen Sie einen Bericht zum Kopieren aus (**Menü > Inhalt > Mein Inhalt oder Teaminhalt**)
2. Wählen Sie *Bericht bearbeiten* aus dem Dropdown-Menü des Berichts



3. Öffnen Sie oben rechts auf dem Bildschirm das Menü mit den drei Punkten neben „Eigenschaften“.
4. Wählen Sie **Bericht in die Zwischenablage kopieren**.



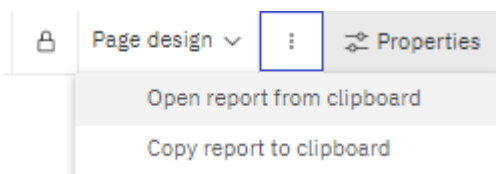
Öffnen von Berichten aus der Zwischenablage

Sie können eine Berichtsspezifikation öffnen, die zuvor in die Zwischenablage kopiert wurde.

Informationen zu diesem Vorgang: 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 mit den drei Punkten 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 (*Meine Inhalte*, *Teaminhalte* 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 beim Bearbeiten von Dateien an ihrem Standardspeicherort das Risiko besteht, dass diese Berichte bei der nächsten Aktualisierung des Berichtskatalogs überschrieben werden. Es wird empfohlen, den bearbeiteten Bericht unter einem neuen Namen oder an einem anderen als dem Standardspeicherort zu speichern.

Fehlerbehebung

Hier finden Sie Vorschläge zur Behebung von Problemen mit dem Reporting.

Problem:	Versuchen Sie Folgendes:
Wenn Sie einen Bericht zum Senden per E-Mail planen, wird der Name des angemeldeten Benutzers bereits in das Feld „An“ der E-Mail eingetragen. Der Name hat jedoch die Form „Vorname Nachname“ (Vorname, Leerzeichen, Nachname). Da es sich hierbei nicht um eine gültige E-Mail-Adresse handelt, kann die E-Mail beim Ausführen des geplanten Berichts nicht gesendet werden.	Wenn Sie den Bericht per E-Mail versenden möchten, löschen Sie den voreingestellten Namen und geben Sie im Feld „An“ eine gültige, richtig formatierte E-Mail-Adresse ein.
Mein geplanter Bericht wird per E-Mail versendet, aber auf den Bericht kann nicht zugegriffen werden, wenn er aus dem Ordner „Meine Inhalte“ stammt.	Um dies zu vermeiden, muss der Bericht oder die Berichtsansicht im Ordner „Teaminhalte > Benutzerdefinierte Berichte – xxxxxx“ gespeichert und der Zeitplan aus dieser gespeicherten Version erstellt werden. Der Ordner „Benutzerdefinierte Berichte – xxxxxx“ ist für alle Benutzer des Mandanten sichtbar.
Beim Speichern eines Jobs wird im Ordner möglicherweise „Teaminhalte“ mit der Inhaltsliste aus „Benutzerdefinierte Berichte – xxxxxx“ angezeigt. Sie können den Job hier jedoch nicht speichern, da Cognos davon ausgeht, dass dies der Ordner „Teaminhalte“ ist, für den Sie keinen Schreibzugriff haben.	Die Problemumgehung besteht darin, einen neuen Ordner mit einem eindeutigen Namen (z. B. „NewFolder“) zu erstellen und dort zu speichern oder in „Meine Inhalte“ zu speichern und dann nach „Benutzerdefinierte Berichte – xxxxxx“ zu kopieren/verschieben.

Erstellen benutzerdefinierter Berichte

Mit den Berichterstellungstools können Sie benutzerdefinierte Berichte erstellen. Nachdem Sie Berichte erstellt haben, können Sie diese speichern und regelmäßig ausführen. Die Ergebnisse der Berichte können automatisch per E-Mail an Sie selbst und andere gesendet werden.



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar ["Premium Edition"](#).

Die Beispiele in diesem Abschnitt zeigen den folgenden Prozess, der für alle Data Infrastructure Insights Reporting-Datenmodelle verwendet werden kann:

- Identifizieren einer Frage, die mit einem Bericht beantwortet werden soll
- Ermittlung der zur Unterstützung der Ergebnisse erforderlichen Daten
- Auswählen von Datenelementen für den Bericht

Bevor Sie Ihren benutzerdefinierten Bericht entwerfen, müssen Sie einige vorbereitende Aufgaben erledigen. Wenn Sie diese nicht ausfüllen, können die Berichte ungenau oder unvollständig sein.

Wenn Sie beispielsweise den Geräteidentifizierungsprozess nicht abschließen, sind Ihre Kapazitätsberichte nicht genau. Oder wenn Sie die Festlegung von Anmerkungen (wie Ebenen, Geschäftseinheiten und Rechenzentren) nicht abschließen, werden in Ihren benutzerdefinierten Berichten die Daten Ihrer Domäne möglicherweise nicht genau wiedergegeben oder für einige Datenpunkte wird „N/A“ angezeigt.

Bevor Sie Ihre Berichte entwerfen, führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie alle ["Datensammler"](#) richtig.
- Geben Sie Anmerkungen (wie Ebenen, Rechenzentren und Geschäftseinheiten) zu Geräten und Ressourcen Ihres Mandanten ein. Es ist von Vorteil, vor der Berichterstellung stabile Anmerkungen zu haben, da Data Infrastructure Insights Reporting historische Informationen sammelt.

Berichterstellungsprozess

Der Prozess der Erstellung benutzerdefinierter (auch „Ad-hoc“-)Berichte umfasst mehrere Aufgaben:

- Planen Sie die Ergebnisse Ihres Berichts.
- Identifizieren Sie Daten, die Ihre Ergebnisse unterstützen.
- Wählen Sie das Datenmodell (z. B. Chargeback-Datenmodell, Inventar-Datenmodell usw.) aus, das die Daten enthält.
- Wählen Sie Datenelemente für den Bericht aus.
- Formatieren, sortieren und filtern Sie Berichtsergebnisse optional.

Planen der Ergebnisse Ihres benutzerdefinierten Berichts

Bevor Sie die Tools zur Berichterstellung öffnen, möchten Sie möglicherweise die Ergebnisse planen, die Sie mit dem Bericht erzielen möchten. Mit Berichterstellungstools können Sie Berichte einfach erstellen und benötigen dafür möglicherweise nicht viel Planung. Es ist jedoch ratsam, sich beim Berichtsanforderer über die Berichtsanforderungen zu informieren.

- Identifizieren Sie die genaue Frage, die Sie beantworten möchten. Beispiel:

- Wie viel Kapazität habe ich noch?
- Wie hoch sind die Rückbuchungskosten pro Geschäftseinheit?
- Wie hoch ist die Kapazität pro Ebene, um sicherzustellen, dass die Geschäftseinheiten auf der richtigen Speicherebene ausgerichtet sind?
- Wie kann ich den Strom- und Kühlbedarf prognostizieren? (Fügen Sie benutzerdefinierte Metadaten hinzu, indem Sie den Ressourcen Anmerkungen hinzufügen.)
- Identifizieren Sie die Datenelemente, die Sie zur Unterstützung der Antwort benötigen.
- Identifizieren Sie die Beziehungen zwischen Daten, die Sie in der Antwort sehen möchten. Bauen Sie in Ihrer Frage keine unlogischen Zusammenhänge ein, wie zum Beispiel: „Ich möchte die Ports sehen, die mit der Kapazität in Zusammenhang stehen.“
- Identifizieren Sie alle für die Daten erforderlichen Berechnungen.
- Bestimmen Sie, welche Filtertypen erforderlich sind, um die Ergebnisse einzugrenzen.
- Bestimmen Sie, ob Sie aktuelle oder historische Daten verwenden müssen.
- Stellen Sie fest, ob Sie Zugriffsrechte für Berichte festlegen müssen, um die Daten auf bestimmte Zielgruppen zu beschränken.
- Legen Sie fest, wie der Bericht verteilt wird. Soll es beispielsweise nach einem festgelegten Zeitplan per E-Mail versendet oder in den Ordnerbereich „Teaminhalte“ aufgenommen werden?
- Bestimmen Sie, wer den Bericht pflegen soll. Dies kann sich auf die Komplexität des Designs auswirken.
- Erstellen Sie ein Modell des Berichts.

Tipps zum Gestalten von Berichten

Beim Entwerfen von Berichten können Ihnen einige Tipps hilfreich sein.

- Bestimmen Sie, ob Sie aktuelle oder historische Daten verwenden müssen.

Die meisten Berichte müssen nur über die neuesten in Data Infrastructure Insights verfügbaren Daten berichten.

- Data Infrastructure Insights Reporting bietet historische Informationen zu Kapazität und Leistung, jedoch nicht zum Inventar.
- Jeder sieht alle Daten. Möglicherweise müssen Sie die Daten jedoch auf bestimmte Zielgruppen beschränken.

Um die Informationen für verschiedene Benutzer zu segmentieren, können Sie Berichte erstellen und Zugriffsberechtigungen dafür festlegen.

Berichtsdatenmodelle

Data Infrastructure Insights umfasst mehrere Datenmodelle, aus denen Sie entweder vordefinierte Berichte auswählen oder Ihren eigenen benutzerdefinierten Bericht erstellen können.

Jedes Datenmodell enthält einen einfachen Data Mart und einen erweiterten Data Mart:

- Der einfache Data Mart bietet schnellen Zugriff auf die am häufigsten verwendeten Datenelemente und enthält nur den letzten Snapshot der Data Warehouse-Daten; historische Daten sind nicht enthalten.
- Der erweiterte Data Mart bietet alle im einfachen Data Mart verfügbaren Werte und Details und umfasst den Zugriff auf historische Datenwerte.

Kapazitätsdatenmodelle

Ermöglicht Ihnen, Fragen zur Speicherkapazität, Dateisystemauslastung, internen Volumekapazität, Portkapazität, Qtree-Kapazität und Kapazität virtueller Maschinen (VM) zu beantworten. Das Kapazitätsdatenmodell ist ein Container für mehrere Kapazitätsdatenmodelle. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen beantworten:

Datenmodell für Speicher und Speicherpoolkapazität

Ermöglicht Ihnen, Fragen zur Ressourcenplanung der Speicherkapazität zu beantworten, einschließlich Speicher und Speicherpools, und umfasst sowohl physische als auch virtuelle Speicherpooldaten. Dieses einfache Datenmodell kann Ihnen dabei helfen, Fragen zur Kapazität auf der Etage und zur Kapazitätsnutzung von Speicherpools nach Ebene und Rechenzentrum im Zeitverlauf zu beantworten. Wenn Sie mit der Kapazitätsberichterstattung noch nicht vertraut sind, sollten Sie mit diesem Datenmodell beginnen, da es sich um ein einfacheres, zielgerichteteres Datenmodell handelt. Mithilfe dieses Datenmodells können Sie Fragen wie die folgenden beantworten:

- Wann wird voraussichtlich die Kapazitätsschwelle von 80 % meines physischen Speichers erreicht?
- Wie groß ist die physische Speicherkapazität eines Arrays für eine bestimmte Ebene?
- Wie hoch ist meine Speicherkapazität nach Hersteller und Familie sowie nach Rechenzentrum?
- Wie ist der Trend zur Speicherauslastung eines Arrays für alle Ebenen?
- Welches sind meine Top 10 Speichersysteme mit der höchsten Auslastung?
- Wie ist der Trend zur Speicherauslastung der Speicherpools?
- Wie viel Kapazität ist bereits vergeben?
- Welche Kapazität steht zur Zuteilung zur Verfügung?

Datenmodell zur Dateisystemnutzung

Dieses Datenmodell bietet Einblick in die Kapazitätsauslastung durch Hosts auf Dateisystemebene. Administratoren können die zugewiesene und verwendete Kapazität pro Dateisystem ermitteln, den Typ des Dateisystems bestimmen und Trendstatistiken nach Dateisystemtyp identifizieren. Mit diesem Datenmodell können Sie folgende Fragen beantworten:

- Wie groß ist das Dateisystem?
- Wo werden die Daten gespeichert und wie wird darauf zugegriffen, beispielsweise lokal oder SAN?
- Was sind die historischen Trends bei der Dateisystemkapazität? Welchen zukünftigen Bedarf können wir auf dieser Grundlage voraussehen?

Datenmodell für die interne Volumekapazität

Ermöglicht Ihnen, Fragen zur genutzten Kapazität des internen Volumes, zur zugewiesenen Kapazität und zur Kapazitätsnutzung im Zeitverlauf zu beantworten:

- Welche internen Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Welche internen Volumina laufen aufgrund eines Trends Gefahr, ihre Kapazitäten zu erreichen? 8 Wie hoch ist die genutzte Kapazität im Vergleich zur zugewiesenen Kapazität auf unseren internen Datenträgern?

Datenmodell für die Portkapazität

Ermöglicht Ihnen, Fragen zur Switch-Port-Konnektivität, zum Port-Status und zur Port-Geschwindigkeit im Zeitverlauf zu beantworten. Sie können Fragen wie die folgenden beantworten, um die Anschaffung neuer Switches zu planen: Wie kann ich eine Port-Verbrauchsprognose erstellen, die die Ressourcenverfügbarkeit (Portverfügbarkeit) vorhersagt (je nach Rechenzentrum, Switch-Anbieter und Portgeschwindigkeit)?

- Welche Ports werden voraussichtlich nicht mehr über ausreichende Kapazitäten verfügen, was die Datengeschwindigkeit, das Rechenzentrum, den Anbieter und die Anzahl der Host- und Speicherports betrifft?
- Wie entwickeln sich die Kapazitäten der Switch-Ports im Laufe der Zeit?
- Wie hoch sind die Portgeschwindigkeiten?
- Welche Art von Portkapazität wird benötigt und welcher Organisation steht ein bestimmter Porttyp oder Anbieter bald nicht mehr zur Verfügung?
- Wann ist der optimale Zeitpunkt, diese Kapazität zu erwerben und bereitzustellen?

Qtree-Kapazitätsdatenmodell

Ermöglicht Ihnen, die Qtree-Auslastung (mit Daten wie genutzte Kapazität im Vergleich zur zugewiesenen Kapazität) im Zeitverlauf zu verfolgen. Sie können die Informationen nach verschiedenen Dimensionen anzeigen, beispielsweise nach Geschäftseinheit, Anwendung, Ebene und Servicelevel. Mit diesem Datenmodell können Sie folgende Fragen beantworten:

- Wie hoch ist die genutzte Kapazität für Qtrees im Vergleich zu den pro Anwendung oder Geschäftseinheit festgelegten Grenzwerten?
- Wie entwickeln sich unsere genutzten und freien Kapazitäten, damit wir eine Kapazitätsplanung durchführen können?
- Welche Geschäftseinheiten nutzen die größte Kapazität?
- Welche Anwendungen verbrauchen die meiste Kapazität?

VM-Kapazitätsdatenmodell

Ermöglicht Ihnen, Berichte über Ihre virtuelle Umgebung und deren Kapazitätsauslastung zu erstellen. Mit diesem Datenmodell können Sie über Änderungen der Kapazitätsnutzung im Zeitverlauf für VMs und Datenspeicher berichten. Das Datenmodell bietet auch Thin Provisioning- und Chargeback-Daten für virtuelle Maschinen.

- Wie kann ich die Kapazitätsrückbelastung basierend auf der für VMs und Datenspeicher bereitgestellten Kapazität ermitteln?
- Welche Kapazität wird von VMs nicht genutzt und welcher ungenutzte Anteil ist frei, verwaist oder anderweitig?
- Was müssen wir aufgrund der Konsumtrends kaufen?
- Welche Einsparungen bei der Speichereffizienz erziele ich durch den Einsatz von Storage Thin Provisioning- und Deduplizierungstechnologien?

Kapazitäten im VM-Kapazitätsdatenmodell werden von virtuellen Datenträgern (VMDKs) übernommen. Dies bedeutet, dass die bereitgestellte Größe einer VM unter Verwendung des VM-Kapazitätsdatenmodells der Größe ihrer virtuellen Datenträger entspricht. Dies unterscheidet sich von der bereitgestellten Kapazität in der Ansicht „Virtuelle Maschinen“ in Data Infrastructure Insights, die die bereitgestellte Größe für die VM selbst anzeigt.

Datenmodell „Volume Capacity“

Ermöglicht Ihnen, alle Aspekte der Volumes auf Ihrem Mandanten zu analysieren und Daten nach Anbieter, Modell, Ebene, Servicelevel und Rechenzentrum zu organisieren.

Sie können die Kapazität im Zusammenhang mit verwaisten Volumes, ungenutzten Volumes und Schutzvolumes (für die Replikation verwendet) anzeigen. Sie können auch verschiedene Volume-Technologien (iSCSI oder FC) sehen und virtuelle Volumes mit nicht-virtuellen Volumes hinsichtlich Array-Virtualisierungsproblemen vergleichen.

Mit diesem Datenmodell können Sie Fragen wie die folgenden beantworten:

- Welche Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Wie ist der Trend in meinem Rechenzentrum hinsichtlich der Kapazität verwaister Datenträger?
- Wie viel meiner Rechenzentrumskapazität ist virtualisiert oder Thin Provisioning-basiert?
- Wie viel meiner Rechenzentrumskapazität muss für die Replikation reserviert werden?

Chargeback-Datenmodell

Ermöglicht Ihnen, Fragen zur verwendeten Kapazität und zur zugewiesenen Kapazität von Speicherressourcen (Volumes, interne Volumes und Qtrees) zu beantworten. Dieses Datenmodell bietet Informationen zur Speicherkapazitätsrückbelastung und Verantwortlichkeit nach Hosts, Anwendungen und Geschäftseinheiten und umfasst sowohl aktuelle als auch historische Daten. Berichtsdaten können nach Servicelevel und Speicherebene kategorisiert werden.

Sie können dieses Datenmodell verwenden, um Rückbuchungsberichte zu erstellen, indem Sie die von einer Geschäftseinheit genutzte Kapazität ermitteln. Mit diesem Datenmodell können Sie einheitliche Berichte für mehrere Protokolle erstellen (einschließlich NAS, SAN, FC und iSCSI).

- Bei Speichern ohne interne Volumes zeigen Chargeback-Berichte die Rückbuchung nach Volumes an.
- Für Speicher mit internen Volumes:
 - Wenn Geschäftseinheiten Volumen zugewiesen sind, zeigen Rückbuchungsberichte die Rückbuchung nach Volumen an.
 - Wenn Geschäftseinheiten nicht Volumes, sondern Qtrees zugewiesen sind, zeigen Chargeback-Berichte Chargebacks nach Qtrees an.
 - Wenn Geschäftseinheiten keinen Volumes und keinen Qtrees zugewiesen sind, zeigen Chargeback-Berichte das interne Volume an.
 - Die Entscheidung, ob Chargeback nach Volume, Qtree oder internem Volume angezeigt wird, wird für jedes interne Volume einzeln getroffen. Daher ist es möglich, dass verschiedene interne Volumes im selben Speicherpool Chargebacks auf unterschiedlichen Ebenen anzeigen.

Kapazitätsfakten werden nach einem Standardzeitintervall gelöscht. Einzelheiten finden Sie unter Data Warehouse-Prozesse.

Berichte, die das Chargeback-Datenmodell verwenden, zeigen möglicherweise andere Werte an als Berichte, die das Speicherkapazitäts-Datenmodell verwenden.

- Bei Speicher-Arrays, die keine NetApp Speichersysteme sind, sind die Daten aus beiden Datenmodellen identisch.
- Bei NetApp und Celerra-Speichersystemen basiert das Chargeback-Datenmodell auf einer einzelnen Ebene (aus Volumes, internen Volumes oder Qtrees) zur Berechnung der Gebühren, während das Storage

Capacity-Datenmodell auf mehreren Ebenen (aus Volumes und internen Volumes) zur Berechnung der Gebühren basiert.

Inventardatenmodell

Ermöglicht Ihnen, Fragen zu Inventarressourcen zu beantworten, darunter Hosts, Speichersysteme, Switches, Festplatten, Bänder, Qtrees, Kontingente, virtuelle Maschinen und Server sowie generische Geräte. Das Inventory-Datenmodell umfasst mehrere Submarts, mit denen Sie Informationen zu Replikationen, FC-Pfaden, iSCSI-Pfaden, NFS-Pfaden und Verstößen anzeigen können. Das Inventardatenmodell enthält keine historischen Daten. Fragen, die Sie mit diesen Daten beantworten können

- Welche Vermögenswerte habe ich und wo sind sie?
- Wer nutzt die Vermögenswerte?
- Welche Arten von Geräten habe ich und was sind die Komponenten dieser Geräte?
- Wie viele Hosts pro Betriebssystem habe ich und wie viele Ports sind auf diesen Hosts vorhanden?
- Welche Speicher-Arrays pro Anbieter sind in jedem Rechenzentrum vorhanden?
- Wie viele Switches pro Anbieter habe ich in jedem Rechenzentrum?
- Wie viele Ports sind nicht lizenziert?
- Welche Bänder von welchem Anbieter verwenden wir und wie viele Ports sind auf jedem Band vorhanden? Werden alle generischen Geräte identifiziert, bevor wir mit der Arbeit an den Berichten beginnen?
- Wie lauten die Pfade zwischen Hosts und Speichervolumes oder Bändern?
- Welche Pfade gibt es zwischen generischen Geräten und Speichervolumes oder Bändern?
- Wie viele Verstöße jedes Typs habe ich pro Rechenzentrum?
- Was sind für jedes replizierte Volume die Quell- und Zielvolumes?
- Gibt es Firmware-Inkompatibilitäten oder nicht übereinstimmende Portgeschwindigkeiten zwischen Fibre Channel-Host-HBAs und Switches?

Leistungsdatenmodell

Ermöglicht Ihnen, Fragen zur Leistung von Volumes, Anwendungsvolumes, internen Volumes, Switches, Anwendungen, VMs, VMDKs, ESX im Vergleich zu VM, Hosts und Anwendungsknoten zu beantworten. Viele davon melden stündliche Daten, tägliche Daten oder beides. Mithilfe dieses Datenmodells können Sie Berichte erstellen, die verschiedene Arten von Fragen zum Leistungsmanagement beantworten:

- Welche Volumes oder internen Volumes wurden während eines bestimmten Zeitraums nicht verwendet oder nicht aufgerufen?
- Können wir eine mögliche Fehlkonfiguration des Speichers für eine Anwendung (unbenutzt) genau bestimmen?
- Wie war das allgemeine Zugriffsverhaltensmuster für eine Anwendung?
- Werden die abgestuften Volumes einer bestimmten Anwendung entsprechend zugewiesen?
- Könnten wir für eine derzeit laufende Anwendung günstigeren Speicher verwenden, ohne dass dies Auswirkungen auf die Anwendungsleistung hat?
- Welche Anwendungen führen zu mehr Zugriffen auf den aktuell konfigurierten Speicher?

Wenn Sie die Switch-Leistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Ist mein Host-Verkehr über verbundene Ports ausgeglichen?

- Welche Switches oder Ports weisen eine hohe Fehleranzahl auf?
- Welche Switches werden basierend auf der Portleistung am häufigsten verwendet?
- Welche Switches werden auf Grundlage der Portleistung nicht ausreichend genutzt?
- Wie hoch ist der Trenddurchsatz des Hosts basierend auf der Portleistung?
- Wie hoch war die Leistungsauslastung für die letzten X Tage für einen bestimmten Host, ein bestimmtes Speichersystem, ein bestimmtes Band oder einen bestimmten Switch?
- Welche Geräte erzeugen Verkehr auf einem bestimmten Switch (z. B. welche Geräte sind für die Nutzung eines stark ausgelasteten Switches verantwortlich)?
- Wie hoch ist der Durchsatz für eine bestimmte Geschäftseinheit in unserer Umgebung?

Wenn Sie die Festplattenleistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Wie hoch ist der Durchsatz für einen bestimmten Speicherpool basierend auf den Daten zur Festplattenleistung?
- Welcher Speicherpool wird am häufigsten genutzt?
- Wie hoch ist die durchschnittliche Festplattenauslastung für einen bestimmten Speicher?
- Wie ist der Nutzungstrend für ein Speichersystem oder einen Speicherpool basierend auf den Daten zur Festplattenleistung?
- Wie ist die Entwicklung der Datenträgenutzung für einen bestimmten Speicherpool?

Wenn Sie VM- und VMDK-Leistungstabellen verwenden, können Sie die folgenden Informationen erhalten:

- Erbringt meine virtuelle Umgebung die optimale Leistung?
- Welche VMDKs melden die höchsten Arbeitslasten?
- Wie kann ich die von VMDs, die verschiedenen Datenspeichern zugeordnet sind, gemeldete Leistung nutzen, um Entscheidungen über die Neuklassifizierung zu treffen?

Das Leistungsdatenmodell enthält Informationen, die Ihnen dabei helfen, die Eignung von Ebenen, Speicherfehlfunktionen für Anwendungen und die letzten Zugriffszeiten von Volumes und internen Volumes zu bestimmen. Dieses Datenmodell stellt Daten wie Antwortzeiten, IOPs, Durchsatz, Anzahl ausstehender Schreibvorgänge und Zugriffsstatus bereit.

Datenmodell zur Speichereffizienz

Ermöglicht Ihnen, den Speichereffizienzwert und das Speicherpotenzial im Laufe der Zeit zu verfolgen. In diesem Datenmodell werden nicht nur Messungen der bereitgestellten Kapazität gespeichert, sondern auch die Menge, die verwendet oder verbraucht wird (die physikalische Messung). Wenn beispielsweise Thin Provisioning aktiviert ist, zeigt Data Infrastructure Insights an, wie viel Kapazität vom Gerät genutzt wird. Sie können dieses Modell auch verwenden, um die Effizienz bei aktivierter Deduplizierung zu bestimmen. Mithilfe des Datamarts zur Speichereffizienz können Sie verschiedene Fragen beantworten:

- Wie hoch sind unsere Einsparungen bei der Speichereffizienz durch die Implementierung von Thin Provisioning- und Deduplizierungstechnologien?
- Wie hoch sind die Speichereinsparungen in den Rechenzentren?
- Wann müssen wir auf der Grundlage historischer Kapazitätstrends zusätzlichen Speicher kaufen?
- Welche Kapazitätssteigerung würde es geben, wenn wir Technologien wie Thin Provisioning und Deduplizierung aktivieren würden?

- Bin ich jetzt hinsichtlich der Speicherkapazität gefährdet?

Fakten- und Dimensionstabellen des Datenmodells

Jedes Datenmodell enthält sowohl Fakten- als auch Dimensionstabellen.

- Faktentabellen: Enthalten gemessene Daten, beispielsweise Menge, Roh- und Nutzkapazität. Enthalten Fremdschlüssel zu Dimensionstabellen.
- Dimensionstabellen: Enthalten beschreibende Informationen zu Fakten, beispielsweise Rechenzentren und Geschäftseinheiten. Eine Dimension ist eine Struktur, die häufig aus Hierarchien besteht und Daten kategorisiert. Dimensionsattribute helfen bei der Beschreibung der Dimensionswerte.

Mithilfe unterschiedlicher oder mehrerer Dimensionsattribute (die in den Berichten als Spalten angezeigt werden) erstellen Sie Berichte, die auf Daten für jede im Datenmodell beschriebene Dimension zugreifen.

In Datenmodellelementen verwendete Farben

Die Farben der Datenmodellelemente haben unterschiedliche Bedeutungen.

- Gelbe Assets: Stellen Messungen dar.
- Nicht gelbe Vermögenswerte: Stellen Attribute dar. Diese Werte werden nicht aggregiert.

Verwenden mehrerer Datenmodelle in einem Bericht

Normalerweise verwenden Sie ein Datenmodell pro Bericht. Sie können jedoch einen Bericht schreiben, der Daten aus mehreren Datenmodellen kombiniert.

Um einen Bericht zu schreiben, der Daten aus mehreren Datenmodellen kombiniert, wählen Sie eines der Datenmodelle als Basis aus und schreiben Sie dann SQL-Abfragen, um auf die Daten aus den zusätzlichen Data Marts zuzugreifen. Mit der SQL-Join-Funktion können Sie die Daten aus den verschiedenen Abfragen in einer einzigen Abfrage kombinieren, die Sie zum Schreiben des Berichts verwenden können.

Angenommen, Sie möchten die aktuelle Kapazität für jedes Speicherarray und benutzerdefinierte Anmerkungen zu den Arrays erfassen. Sie könnten den Bericht mithilfe des Datenmodells „Speicherkapazität“ erstellen. Sie könnten die Elemente aus den Tabellen „Aktuelle Kapazität“ und „Dimension“ verwenden und eine separate SQL-Abfrage hinzufügen, um auf die Anmerkungsinformationen im Inventardatenmodell zuzugreifen. Schließlich können Sie die Daten kombinieren, indem Sie die Inventarspeicherdaten mithilfe des Speichernamens und der Verknüpfungskriterien mit der Speicherdimensionstabelle verknüpfen.

Zugriff auf die Berichtsdatenbank über die API

Die leistungsstarke API von Data Infrastructure Insights ermöglicht es Benutzern, die Data Infrastructure Insights Reporting-Datenbank direkt abzufragen, ohne die Cognos Reporting-Umgebung zu durchlaufen.



Diese Dokumentation bezieht sich auf die Data Infrastructure Insights -Berichtsfunktion, die in der Data Infrastructure Insights Premium Edition verfügbar ist.

Odata

Die Data Infrastructure Insights Reporting API folgt dem "[OData v4](#)" (Open Data Protocol)-Standard für die Abfrage der Reporting-Datenbank. Weitere Informationen und weitere Informationen finden Sie unter "[dieses Tutorial](#)" auf OData.

Alle Anfragen beginnen mit der URL *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*

Generieren eines API-Schlüssels

Lesen Sie mehr über "[APIs für Data Infrastructure Insights](#)".

Gehen Sie wie folgt vor, um einen API-Schlüssel zu generieren:

- Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und wählen Sie **Admin > API-Zugriff**.
- Klicken Sie auf „+ API-Zugriffstoken“.
- Geben Sie einen Namen und eine Beschreibung ein.
- Wählen Sie als Typ „Data Warehouse“ aus.
- Legen Sie die Berechtigungen auf Lesen/Schreiben fest.
- Legen Sie ein gewünschtes Ablaufdatum fest.
- Klicken Sie auf „Speichern“, kopieren Sie dann den Schlüssel und speichern Sie ihn an einem sicheren Ort. Auf den vollständigen Schlüssel können Sie später nicht mehr 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 zu Anzeigezwecken auf *https://.../odata/* vereinfacht werden, anstatt auf die vollständige Version *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata/*

Versuchen Sie es mit einfachen Abfragen wie

- *https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_custom*
- *https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory*
- *https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/storage*
- *https://< URL der Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/disk*
- *https://.../odata/dwh_custom/custom_queries*

REST-API-Beispiele

Die URL für alle Aufrufe lautet *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*.

- GET */<schema>/*** – Ruft Daten aus der Berichtsdatenbank ab.

Format: *https://< Data Infrastructure 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 Hinweise

Beachten Sie beim Arbeiten mit Reporting-API-Abfragen Folgendes.

- Die Abfragenutzlast muss eine gültige JSON-Zeichenfolge sein
- Die Abfragenutzlast muss in einer einzigen Zeile enthalten sein
- Doppelte Anführungszeichen müssen maskiert werden, d. h. \"
- Tabs werden als \t unterstützt
- Vermeiden Sie Kommentare
- Tabellennamen in Kleinbuchstaben werden unterstützt

Zusätzlich:

- 2 Header sind erforderlich:
 - Name „X-CloudInsights-APIKey“
 - Attributwert „<apikey>“

Ihr API-Schlüssel ist spezifisch für Ihre Data Infrastructure Insights Umgebung.

Synchron oder asynchron?

Standardmäßig wird ein API-Befehl im *synchronen* Modus ausgeführt, d. h. Sie senden die Anfrage und die Antwort wird sofort zurückgegeben. Manchmal kann die Ausführung einer Abfrage jedoch sehr lange dauern, was zu einer Zeitüberschreitung der Anforderung führen kann. Um dies zu umgehen, können Sie eine Anfrage *asynchron* ausführen. Im asynchronen Modus gibt die Anfrage eine URL zurück, über die die Ausführung überwacht werden kann. Die URL gibt das Ergebnis zurück, wenn es fertig ist.

Um eine Abfrage im asynchronen Modus auszuführen, fügen Sie den Header hinzu **Prefer: respond-async** auf die Anfrage. Bei erfolgreicher Ausführung enthält die Antwort die folgenden Header:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

Bei der Abfrage der Standort-URL werden dieselben Header zurückgegeben, wenn die Antwort noch nicht bereit ist, oder der Status 200, wenn die Antwort bereit ist. Der Antwortinhalt ist vom Typ Text und enthält den HTTP-Status der ursprünglichen Abfrage und 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 und deren Bereitschaft anzuzeigen, verwenden Sie den folgenden Befehl:

```
GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
Die Antwort hat das folgende Format:
```

```
{
  "queries" : [
    {
      "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
      "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
      "Finished": false
    }
  ]
}
```

Veröffentlichung und Aufhebung der Veröffentlichung von Anmerkungen für Berichte

Veröffentlichung und Aufhebung der Veröffentlichung von Anmerkungen für Berichte

Erfahren Sie, wie Sie Anmerkungen zur Verwendung in Berichten und im Data Warehouse veröffentlichen und wie Sie Anmerkungen ordnungsgemäß wieder entfernen, wenn sie nicht mehr benötigt werden.

Veröffentlichung von Anmerkungen für Berichte

Nachdem Sie in Data Infrastructure Insights Annotationen erstellt haben, können Sie diese zur Verwendung in der Berichterstellung veröffentlichen.

Schritte zum Veröffentlichen von Anmerkungen

1. Navigieren Sie zur Seite **Observability > Enrich > Annotations** und wählen Sie die Registerkarte *Annotations for Reporting* aus.
2. Suchen Sie die Anmerkung, die Sie veröffentlichen möchten.
3. Wählen Sie die Anmerkung aus und wählen Sie *In Berichten veröffentlichen*. Sie können die Annotation auch auf historische Daten anwenden, sodass sie beim Ausführen von Verlaufsberichten verwendet werden kann.
4. Nach der Veröffentlichung steht die Annotation für die Verwendung in Berichten zur Verfügung.
5. Die Annotationen werden nach dem nächsten ETL-Lauf zur Verwendung in der Berichterstellung veröffentlicht.



Alle Berichte, die auf die Annotation Bezug nehmen, verwenden die veröffentlichten Werte. Wenn Sie eine Anmerkung nach der Veröffentlichung ändern, müssen Sie sie möglicherweise erneut veröffentlichen, damit diese Änderungen in den Berichten wirksam werden.

Veröffentlichung von Anmerkungen für die Berichterstellung aufheben

Es kann vorkommen, dass Sie Anmerkungen entfernen oder deren Veröffentlichung aufheben müssen, damit sie in der Berichterstellung nicht mehr verwendet werden. Beispielsweise kann eine Anmerkung nicht mehr

benötigt werden oder veraltete Informationen enthalten, die nicht in Berichten erscheinen sollten.

Schritte zum Aufheben der Veröffentlichung von Anmerkungen

Bevor Sie eine Anmerkung entfernen, beachten Sie bitte, dass diese Aktion Auswirkungen auf alle bestehenden Berichte hat, die diese Anmerkung verwenden. Berichte müssen gegebenenfalls redaktionell bearbeitet oder durch professionelle Dienstleistungen unterstützt werden, um die Anmerkungsverweise zu entfernen.

1. Navigieren Sie in der Benutzeroberfläche von Data Infrastructure Insights zur Registerkarte *Anmerkungen für die Berichterstellung*.
2. Suchen Sie die Anmerkung, die Sie entfernen möchten.
3. Für jedes Objekt, bei dem die Annotation veröffentlicht ist, deaktivieren Sie die Annotation und wählen Sie *Speichern*.
4. Entfernen Sie alle Abfragen oder Regeln, die noch auf die Annotation verweisen, um sicherzustellen, dass sie nicht als „in Verwendung“ markiert ist.
5. Die Annotationen werden nach dem nächsten ETL-Lauf wieder entfernt.
6. Nach Abschluss des ETL-Prozesses kann die Annotation aus der Liste der Annotationen gelöscht werden, wenn sie auf Mandantenseite nicht mehr benötigt wird.



Annotationen werden so lange im Data Warehouse angezeigt, bis sie ordnungsgemäß entfernt werden. Wenn man eine Anmerkung einfach von der Seite „Anmerkungen“ löscht, ohne sie vorher zu deaktivieren, bleiben veraltete Daten zurück, die möglicherweise in bestehenden Berichten erscheinen. Um eine vollständige Entfernung zu gewährleisten, befolgen Sie die oben beschriebenen Schritte zum Aufheben der Veröffentlichung.

Auswirkungen auf bestehende Berichte

Das Entfernen oder Aufheben der Veröffentlichung von Anmerkungen kann Änderungen an bestehenden Berichten erfordern, die auf diese Anmerkungen Bezug nehmen. Beachten Sie Folgendes:

- Berichte, die die Annotation als Filter oder Dimension verwenden, müssen aktualisiert werden.
- Wird eine Annotation entfernt, ohne die abhängigen Berichte zu aktualisieren, können diese Berichte Fehler oder unerwartete Ergebnisse liefern.
- Bei komplexen Szenarien können professionelle Dienstleistungen zur Unterstützung bei der Behebung von Mängeln im Bericht erforderlich sein.

Es wird empfohlen, alle Berichte, die auf einer Anmerkung basieren, vor der Deaktivierung zu überprüfen.

So werden historische Daten für die Berichterstellung aufbewahrt

Data Infrastructure Insights speichert historische Daten zur Verwendung in Berichten basierend auf den Data Marts und der Granularität der Daten, wie in der folgenden Tabelle gezeigt.

Datamart	Messobjekt	Granularität	Aufbewahrungsfrist
Performance-Märkte	Volumes und interne Volumes	Stündlich	14 Tage

Performance-Märkte	Volumes und interne Volumes	Täglich	13 Monate
Performance-Märkte	Anwendung	Stündlich	13 Monate
Performance-Märkte	Gastgeber	Stündlich	13 Monate
Performance-Märkte	Switch-Leistung für Port	Stündlich	35 Tage
Performance-Märkte	Switch-Leistung für Host, Speicher und Band	Stündlich	13 Monate
Performance-Märkte	Speicherknotten	Stündlich	14 Tage
Performance-Märkte	Speicherknotten	Täglich	13 Monate
Performance-Märkte	VM-Leistung	Stündlich	14 Tage
Performance-Märkte	VM-Leistung	Täglich	13 Monate
Performance-Märkte	Hypervisor-Leistung	Stündlich	35 Tage
Performance-Märkte	Hypervisor-Leistung	Täglich	13 Monate
Performance-Märkte	VMDK-Leistung	Stündlich	35 Tage
Performance-Märkte	VMDK-Leistung	Täglich	13 Monate
Performance-Märkte	Festplattenleistung	Stündlich	14 Tage
Performance-Märkte	Festplattenleistung	Täglich	13 Monate
Kapazitätsmärkte	Alle (außer Einzelbände)	Täglich	13 Monate
Kapazitätsmärkte	Alle (außer Einzelbände)	Monatsvertreter	14 Monate und darüber hinaus
Inventarmärkte	Einzelbände	Aktueller Stand	1 Tag (oder bis zum nächsten ETL)

Schemadiagramme für die Data Infrastructure Insights -Berichterstattung

Dieses Dokument enthält Schemadiagramme für die Berichtsdatenbank.

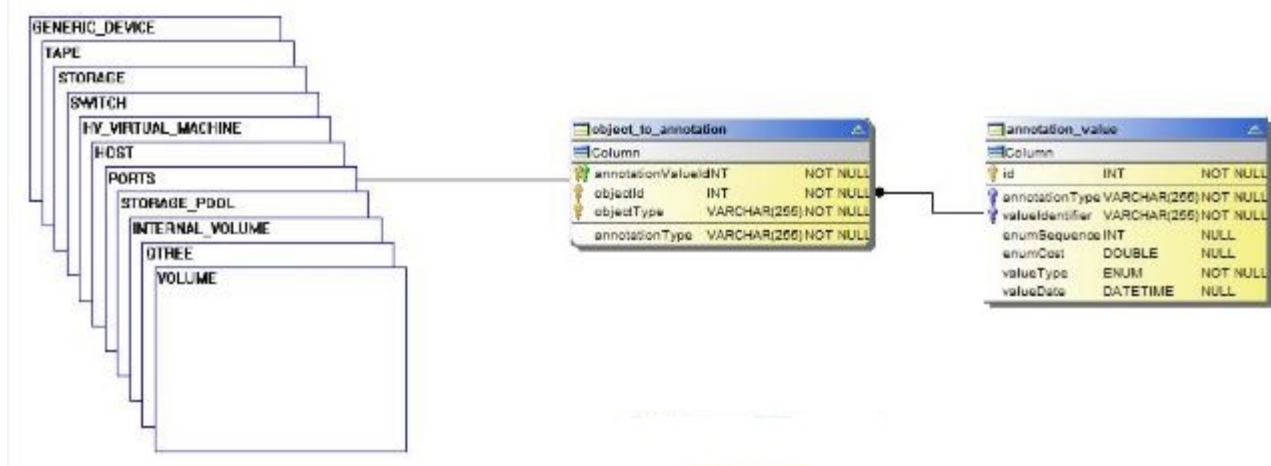


Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar "[Premium Edition](#)".

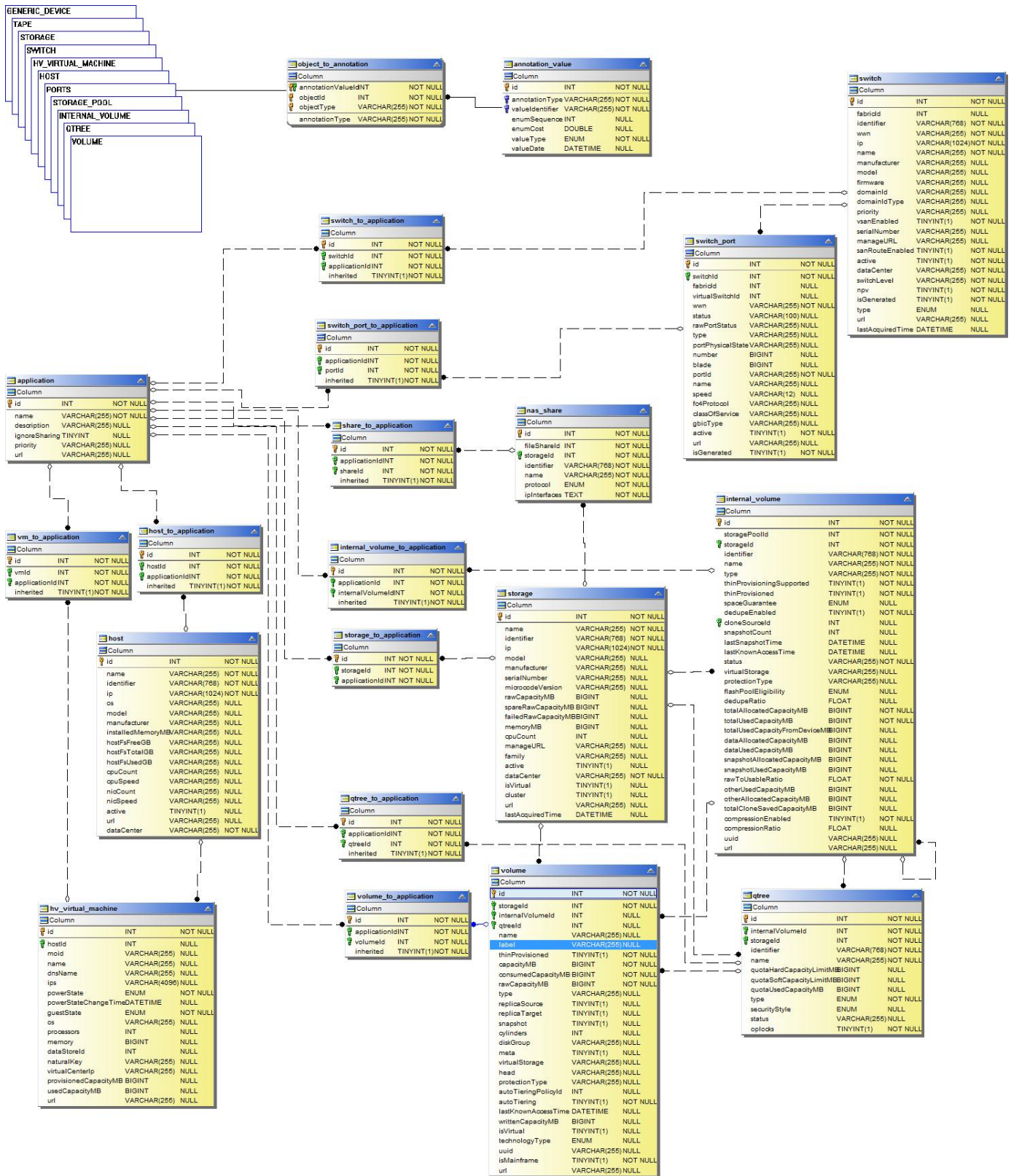
Inventar-Datamart

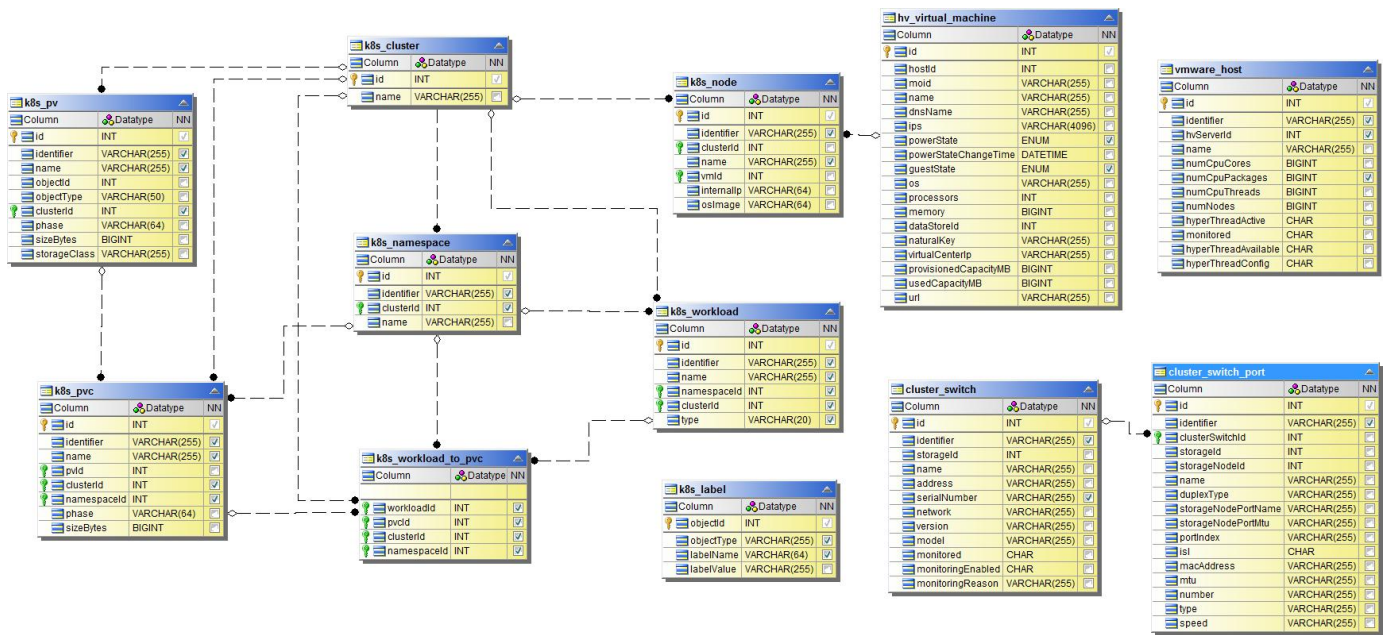
Die folgenden Bilder beschreiben den Inventar-Datamart.

Anmerkungen

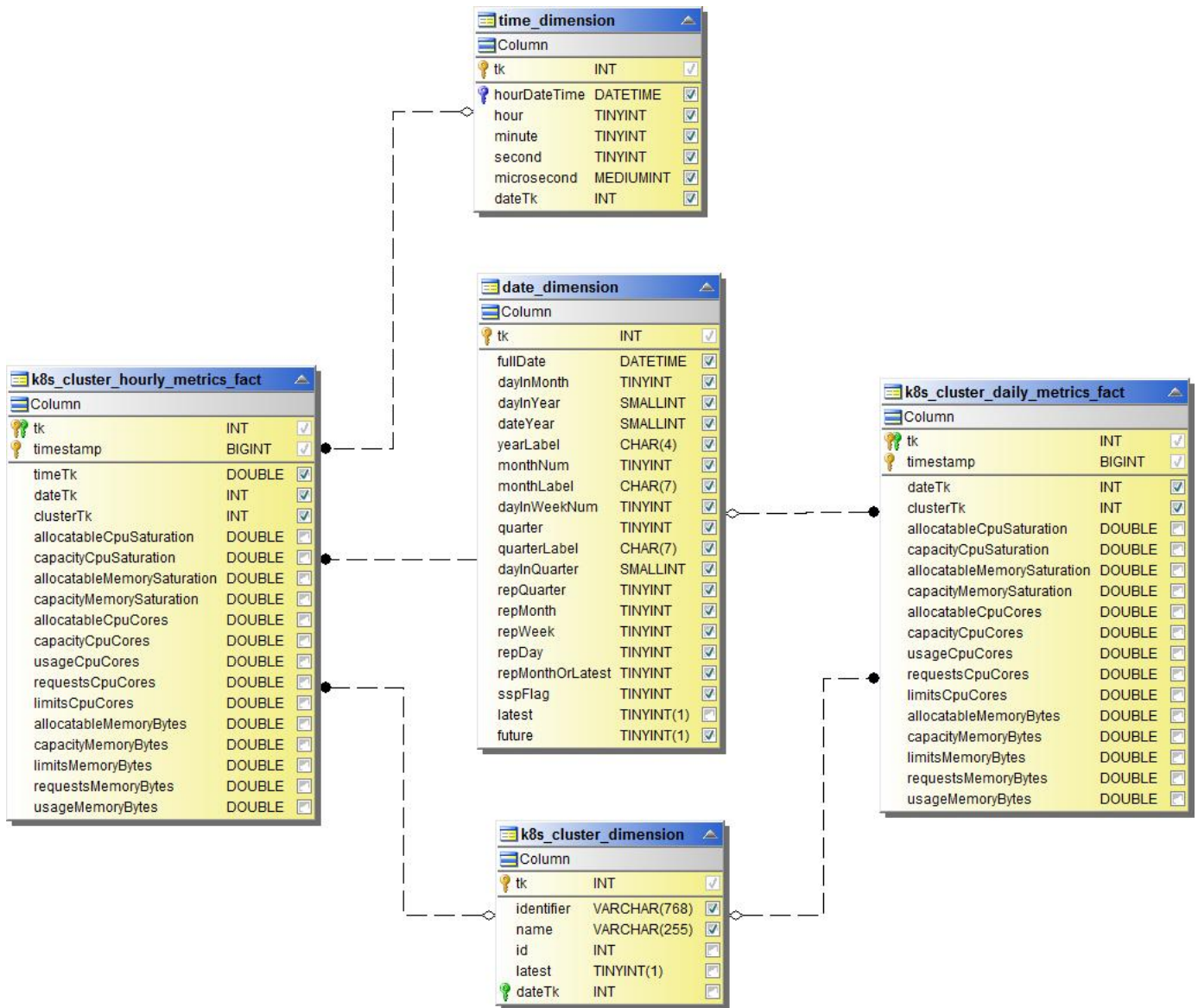


Anwendungen

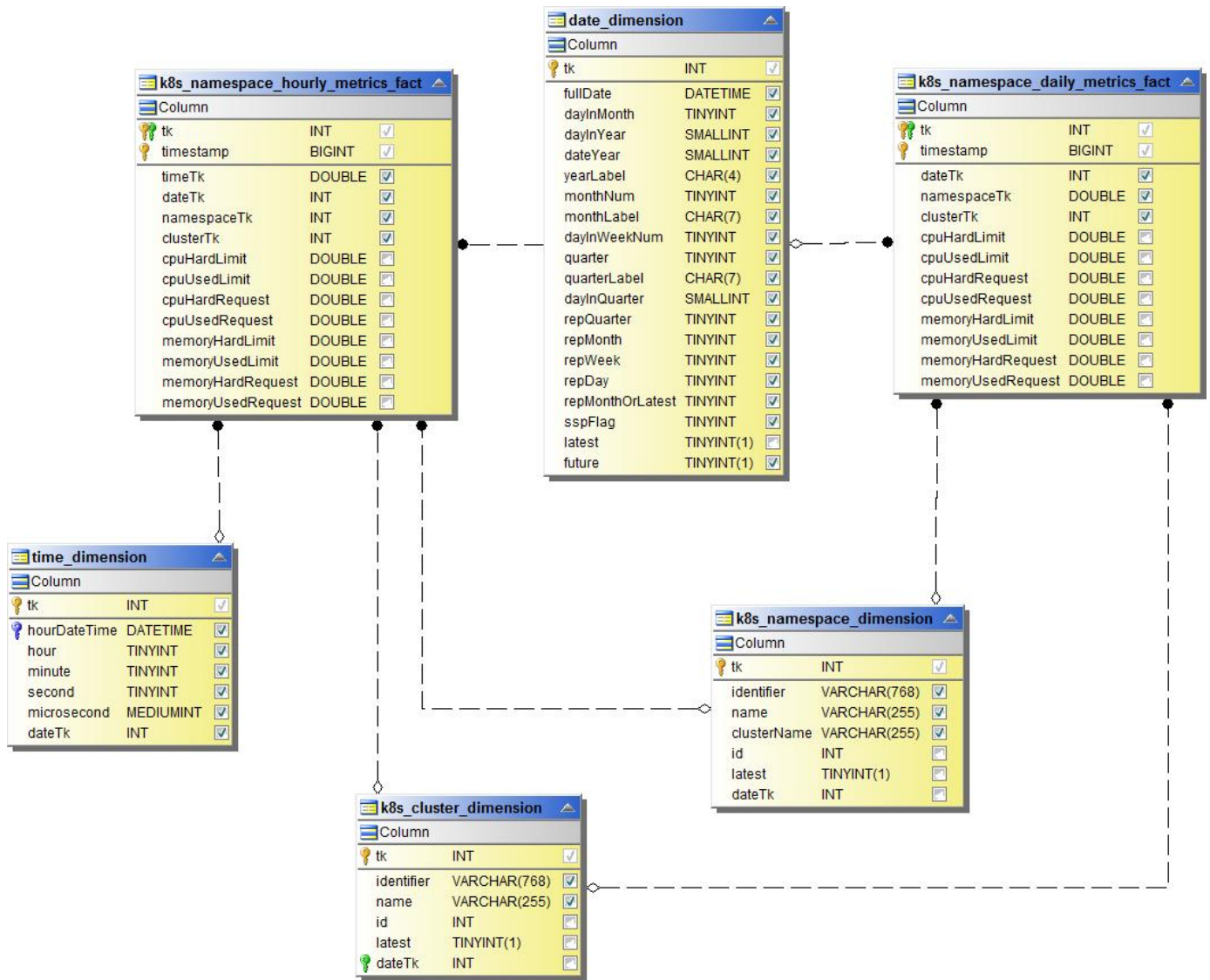




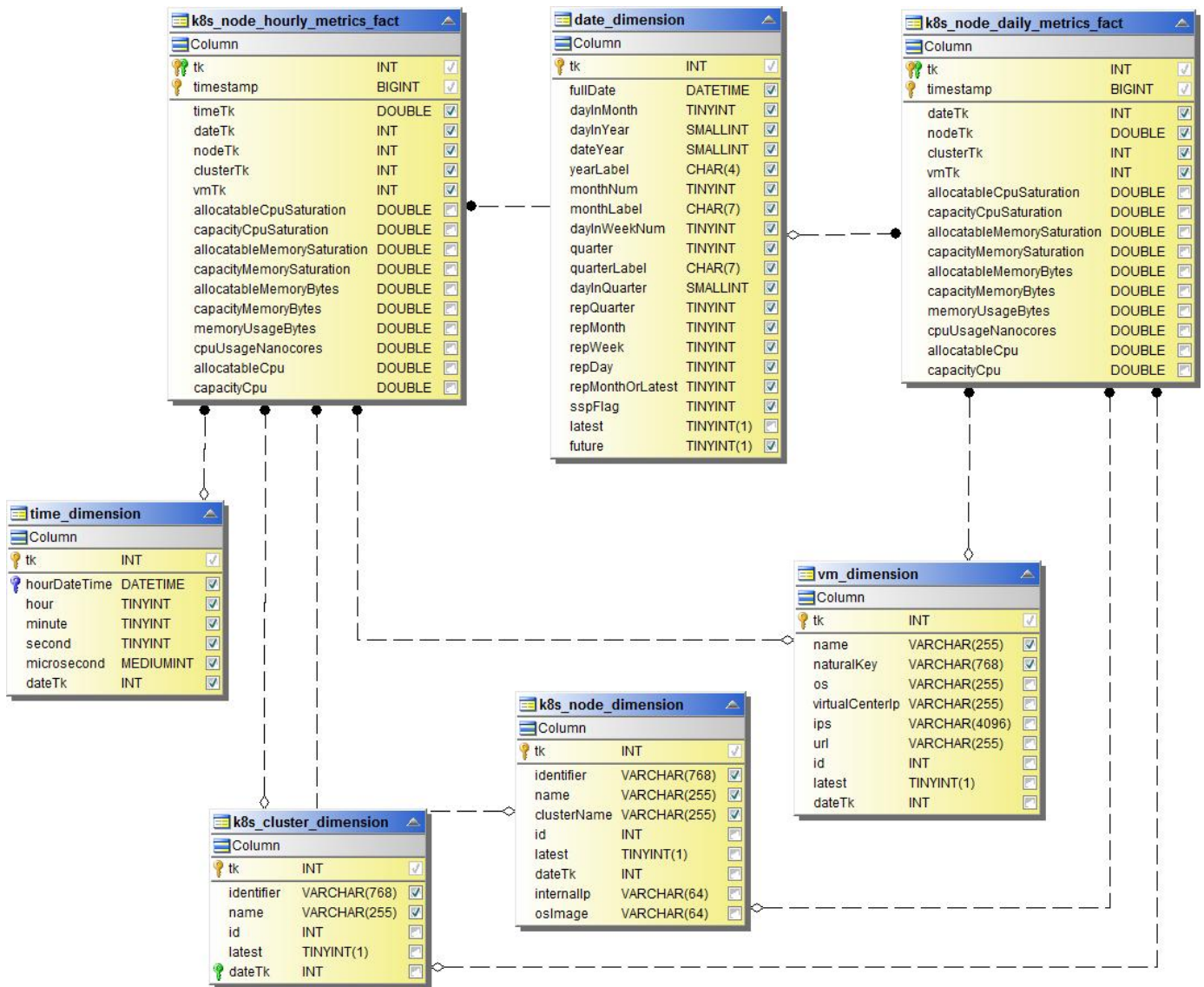
Kubernetes-Clustermetriken – Fakten



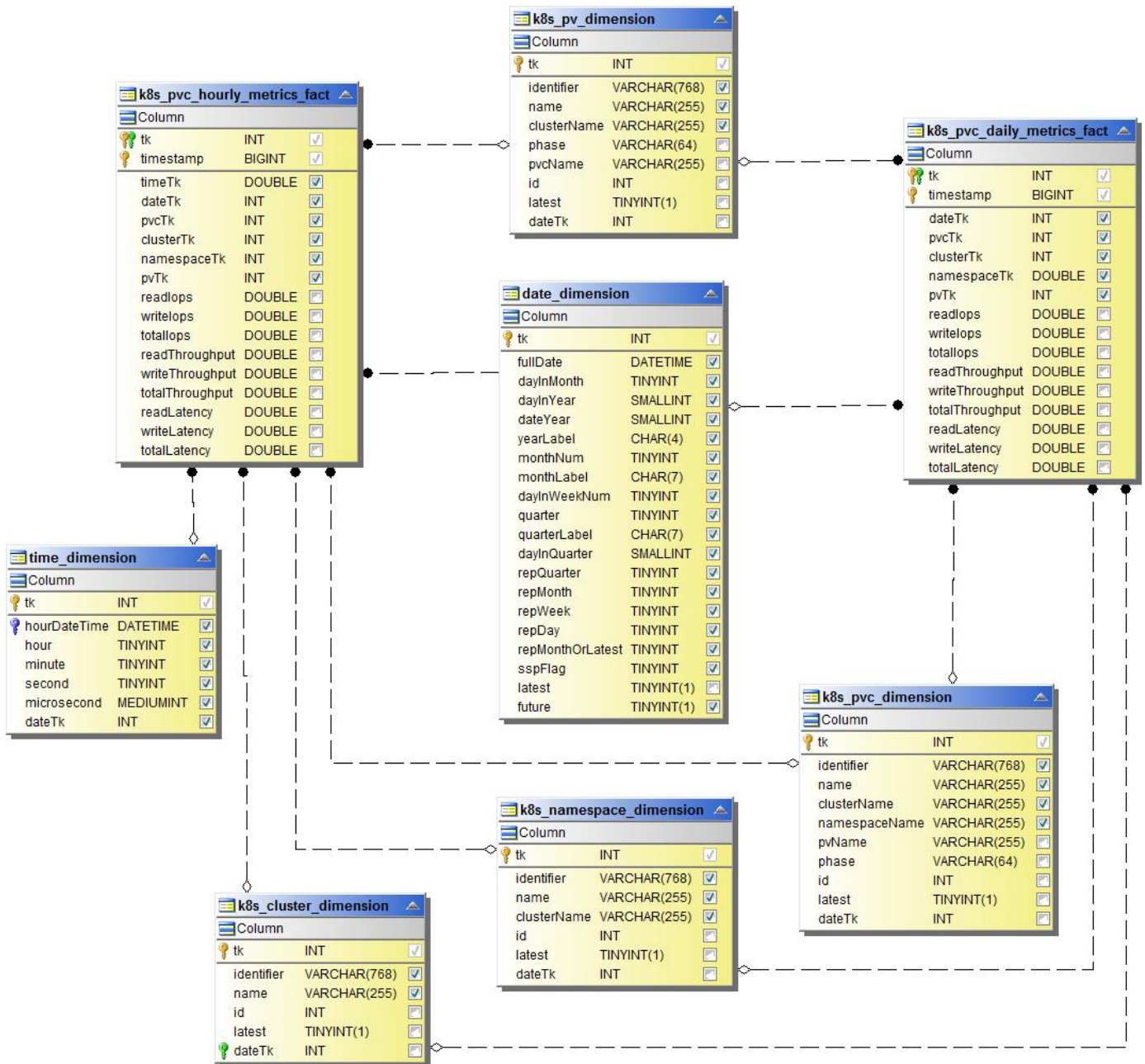
Kubernetes-Namespace-Metriken – Fakten



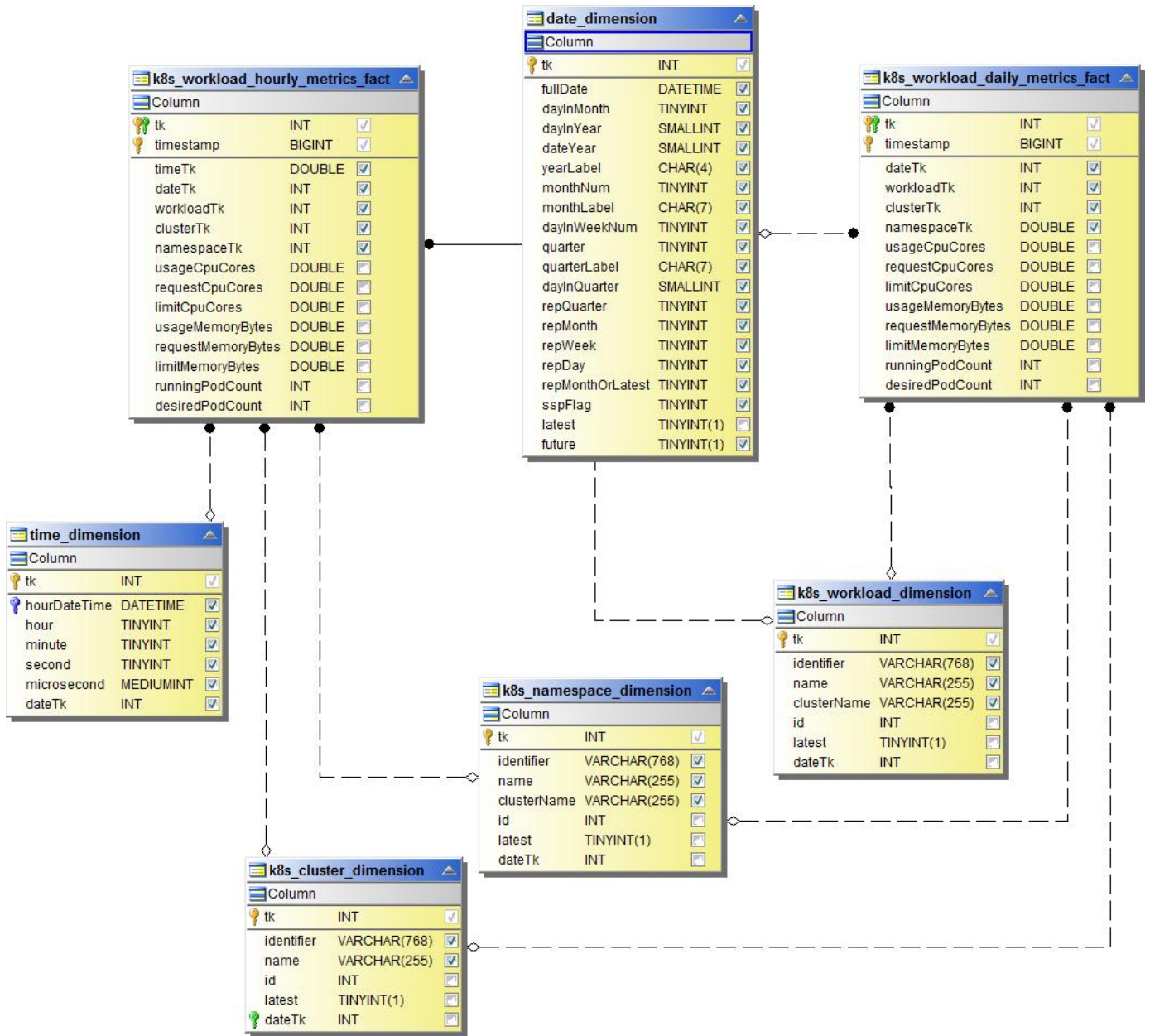
Kubernetes-Knotenmetriken – Fakten



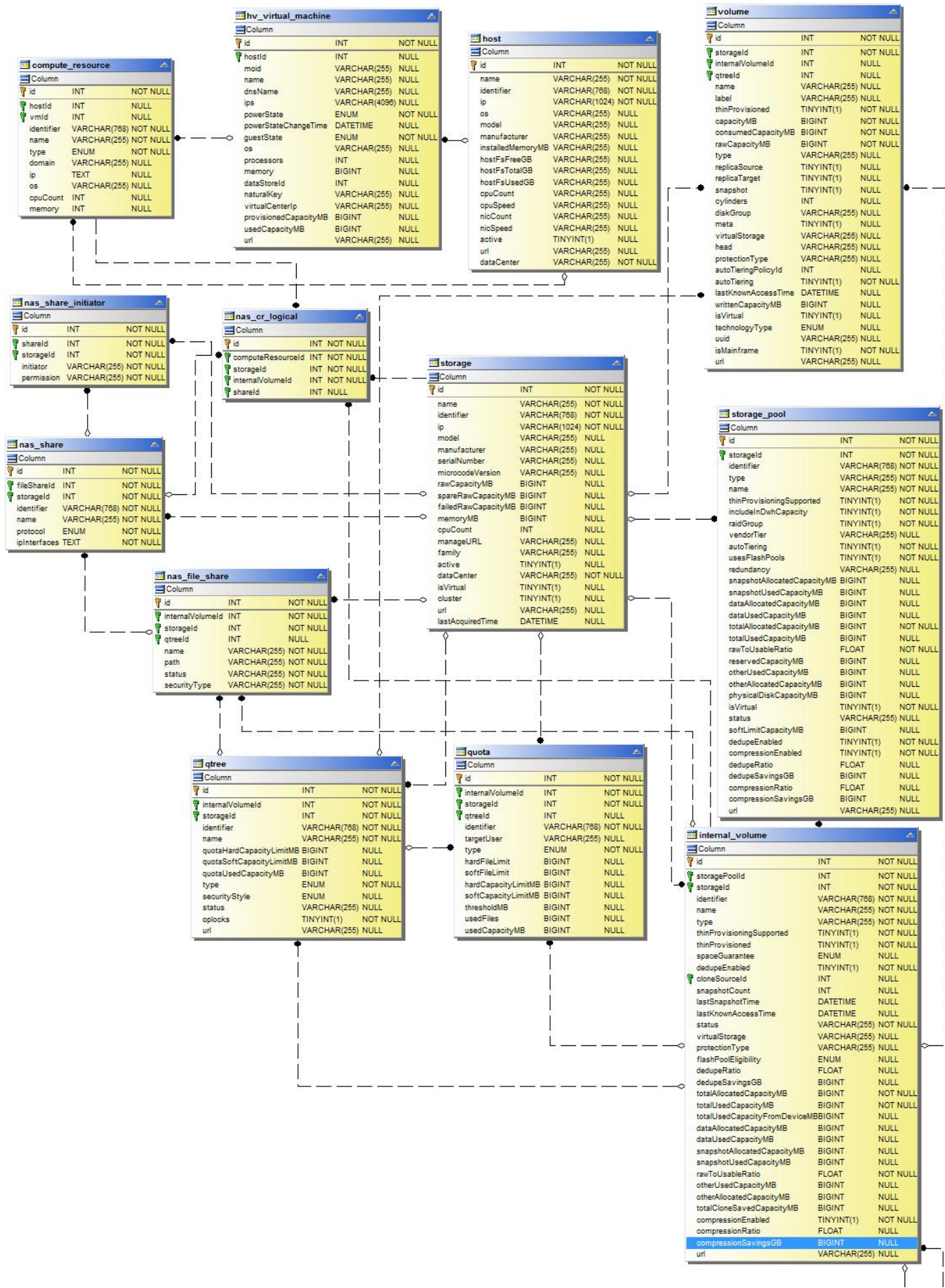
Kubernetes PVC-Metriken-Fakten

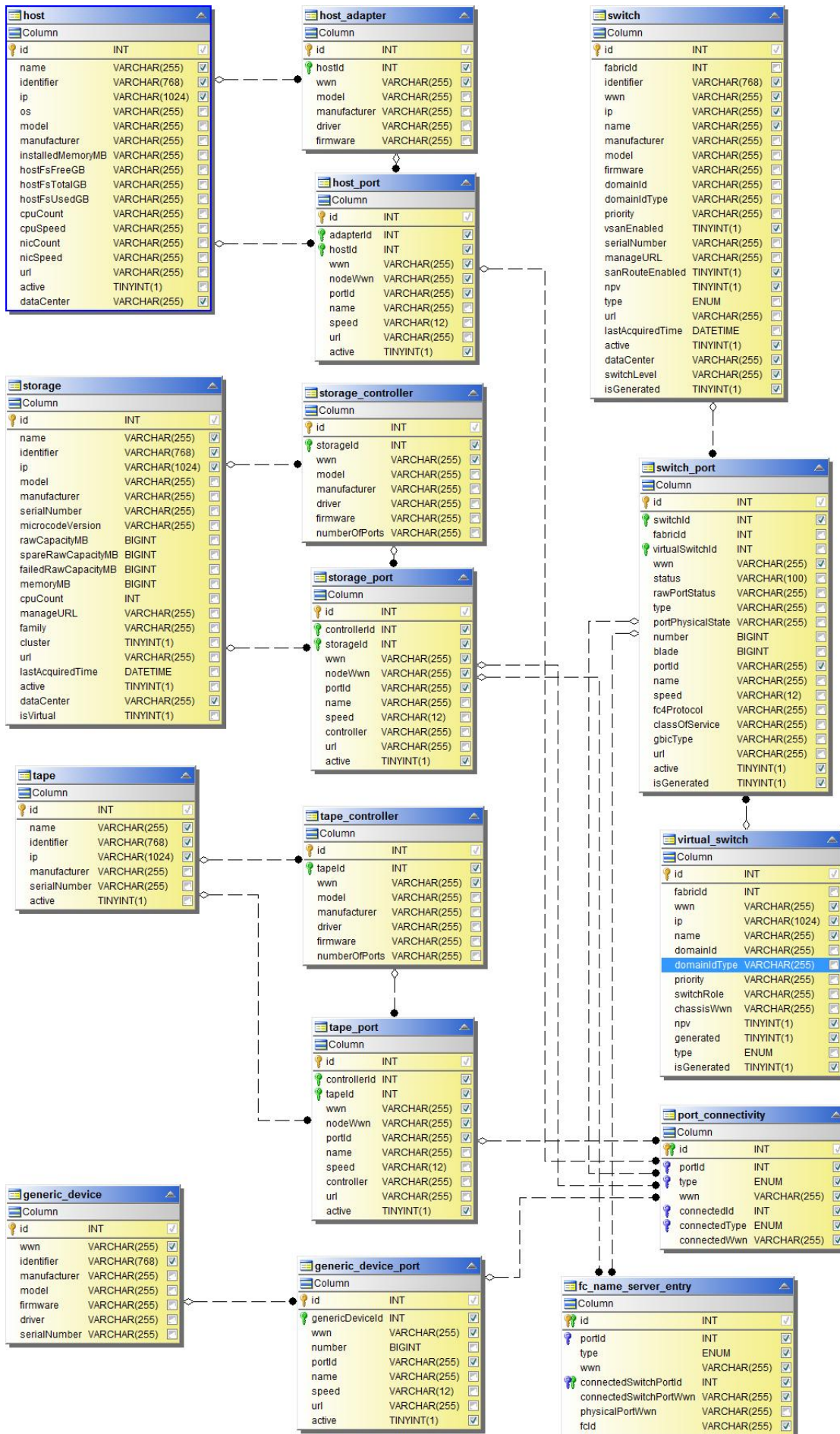


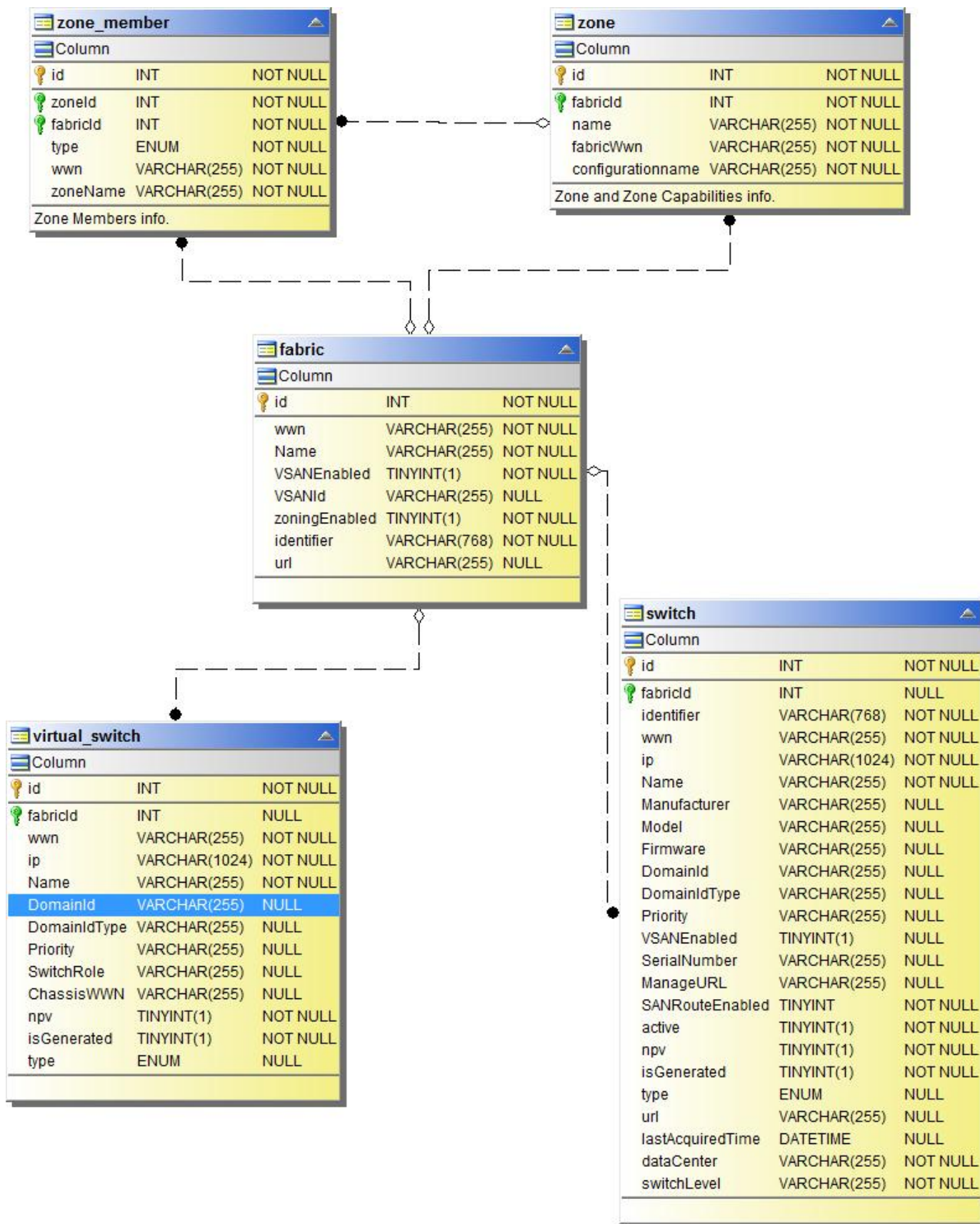
Fakten zu Kubernetes-Workload-Metriken



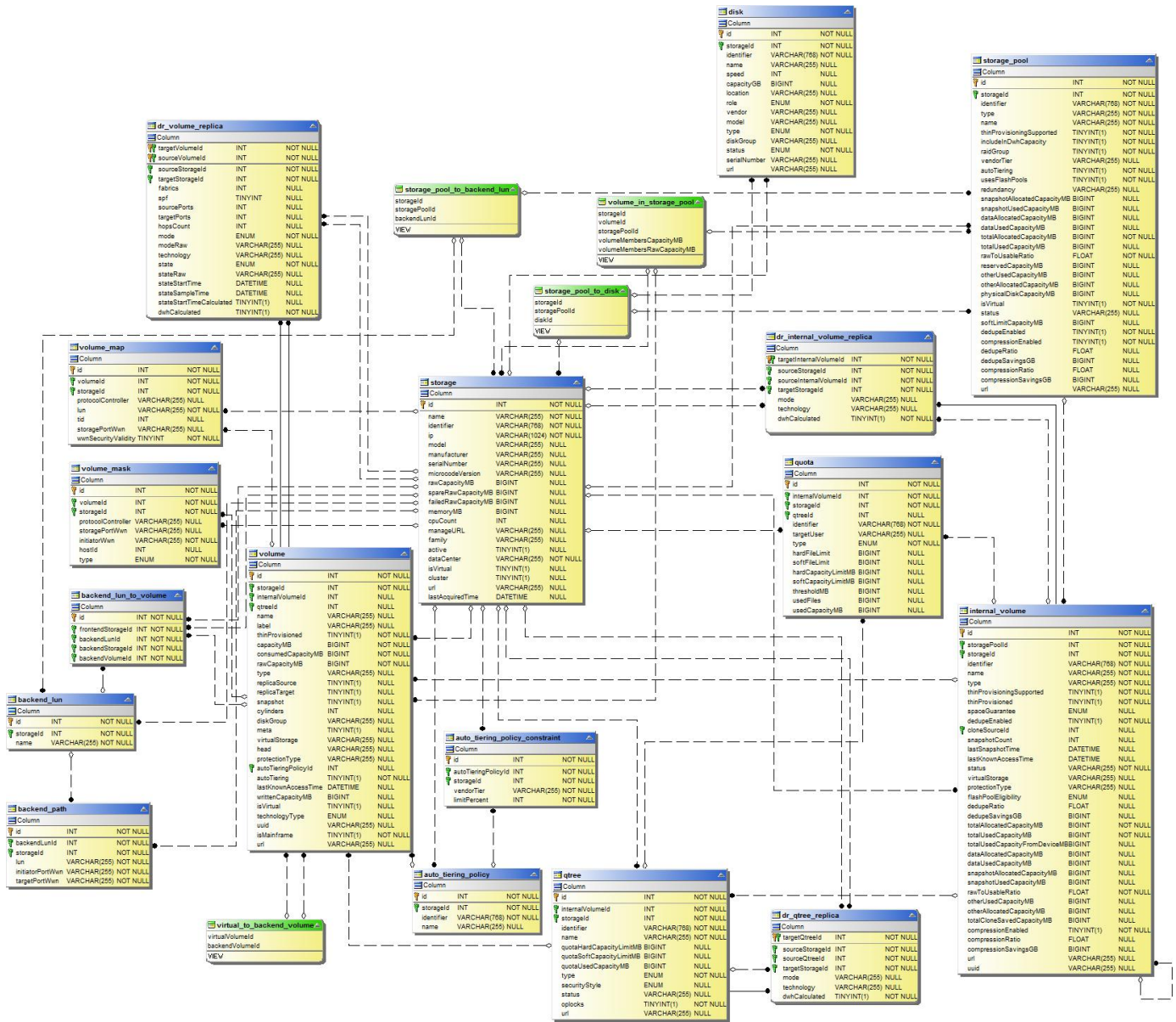
NAS



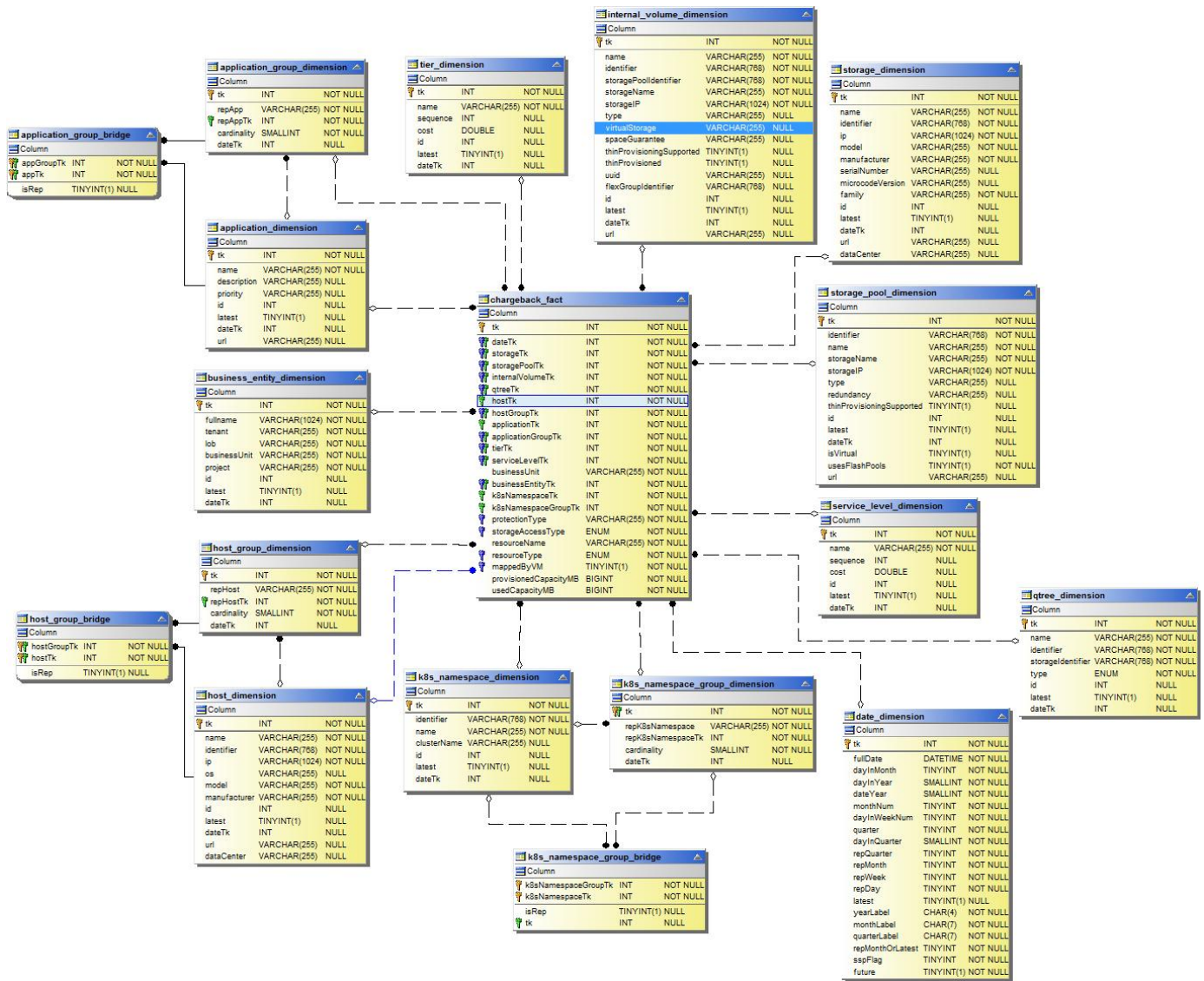




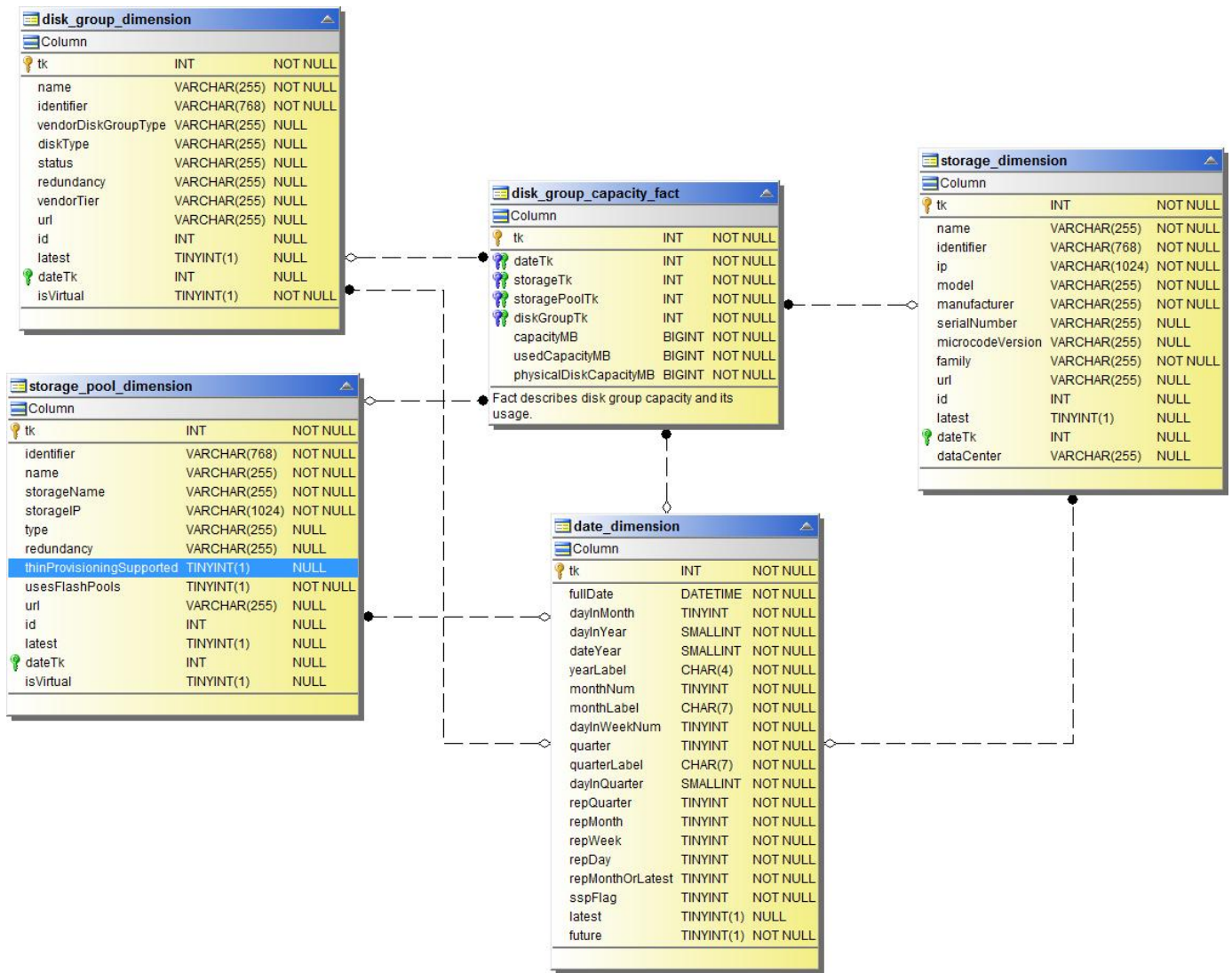
Storage



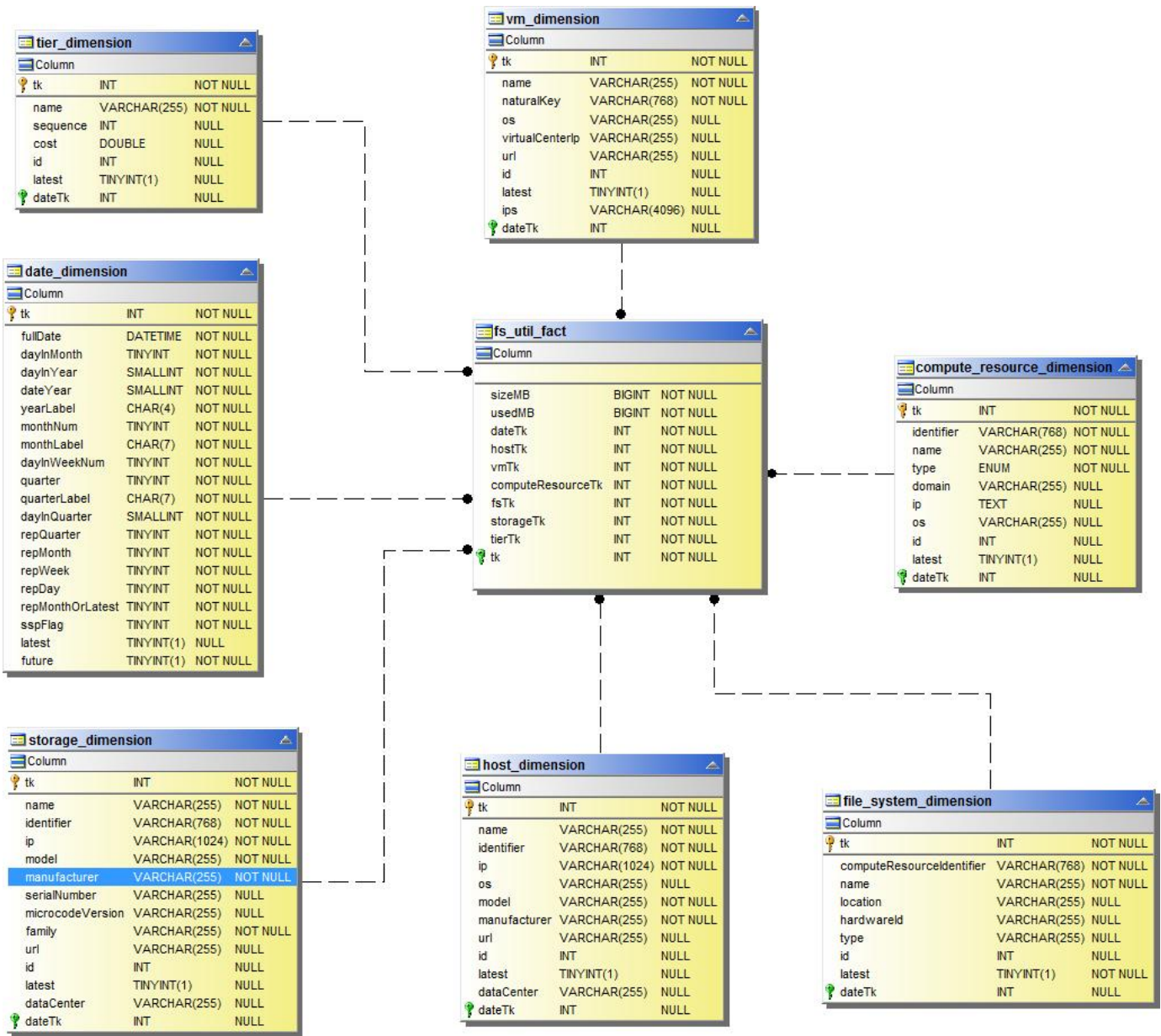
Speicherknoten



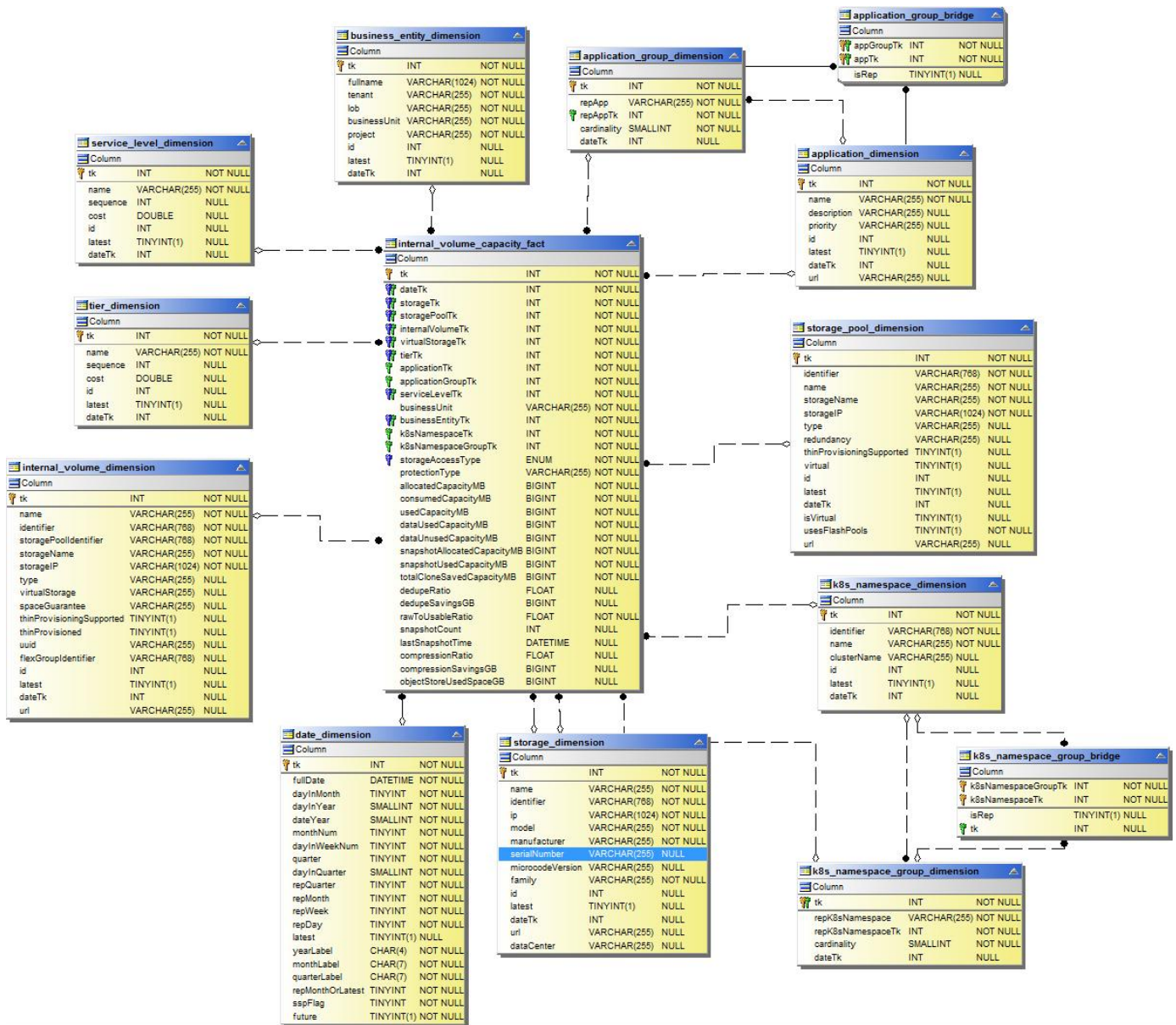
Kapazität der Datenträgergruppe



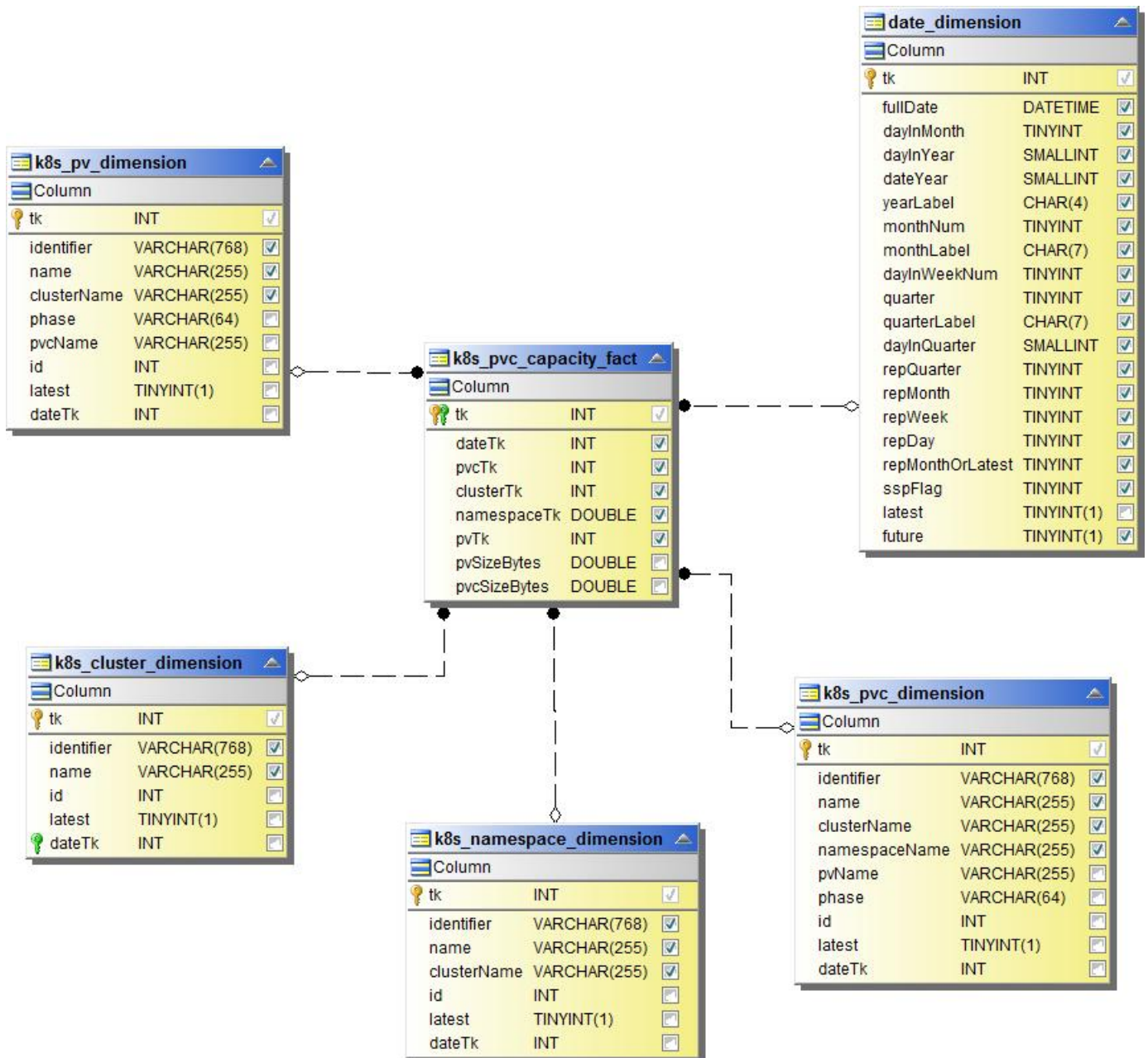
Dateisystemauslastung



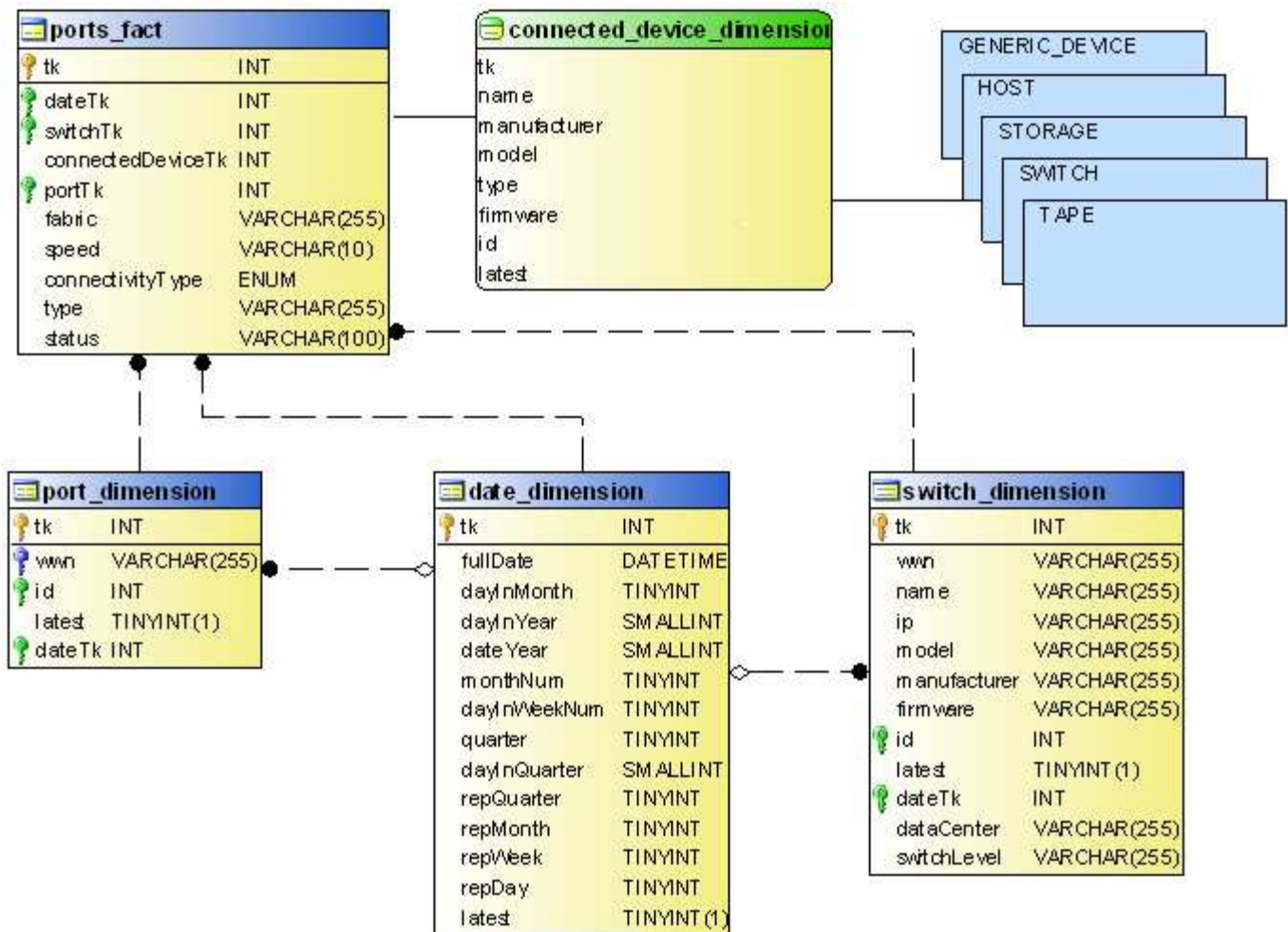
Interne Volumenkapazität



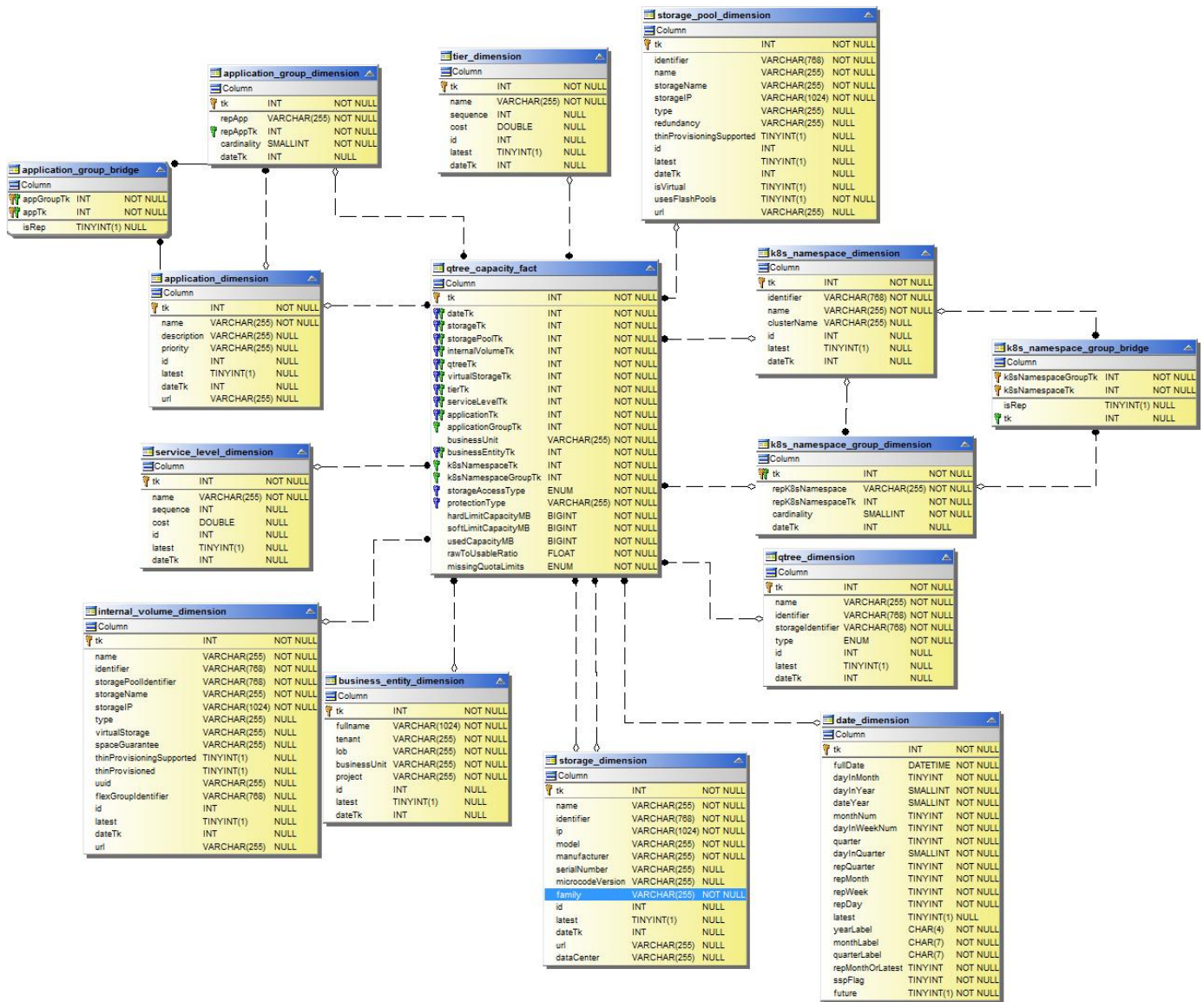
Kubernetes PV-Kapazität



Hafenkapazität



Qtree-Kapazität



Speicherkapazitätseffizienz

efficiency_fact			
Column			
tk	INT	NOT NULL	
dateTk	INT	NOT NULL	
storageTk	INT	NOT NULL	
rawCapacityMB	BIGINT	NOT NULL	
backendCapacityMB	BIGINT	NOT NULL	
storageTechnology	VARCHAR(255)	NULL	
gainMB	BIGINT	NOT NULL	
lossMB	BIGINT	NOT NULL	
potentialGainMB	BIGINT	NOT NULL	
potentialLossMB	BIGINT	NOT NULL	

date_dimension			
Column			
tk	INT	NOT NULL	
fullDate	DATETIME	NOT NULL	
dayInMonth	TINYINT	NOT NULL	
dayInYear	SMALLINT	NOT NULL	
dateYear	SMALLINT	NOT NULL	
monthNum	TINYINT	NOT NULL	
dayInWeekNum	TINYINT	NOT NULL	
quarter	TINYINT	NOT NULL	
dayInQuarter	SMALLINT	NOT NULL	
repQuarter	TINYINT	NOT NULL	
repMonth	TINYINT	NOT NULL	
repWeek	TINYINT	NOT NULL	
repDay	TINYINT	NOT NULL	
latest	TINYINT(1)	NULL	
yearLabel	CHAR(4)	NOT NULL	
monthLabel	CHAR(7)	NOT NULL	
quarterLabel	CHAR(7)	NOT NULL	
repMonthOrLatest	TINYINT	NOT NULL	
sspFlag	TINYINT	NOT NULL	
future	TINYINT(1)	NOT NULL	

storage_dimension			
Column			
tk	INT	NOT NULL	
name	VARCHAR(255)	NOT NULL	
identifier	VARCHAR(768)	NOT NULL	
ip	VARCHAR(1024)	NOT NULL	
model	VARCHAR(255)	NOT NULL	
manufacturer	VARCHAR(255)	NOT NULL	
serialNumber	VARCHAR(255)	NULL	
microcodeVersion	VARCHAR(255)	NULL	
family	VARCHAR(255)	NOT NULL	
id	INT	NULL	
latest	TINYINT(1)	NULL	
dateTk	INT	NULL	
url	VARCHAR(255)	NULL	
dataCenter	VARCHAR(255)	NULL	

Speicher- und Speicherpoolkapazität

date_dimension			
Column			
tk	INT	NOT NULL	
fullDate	DATETIME	NOT NULL	
dayInMonth	TINYINT	NOT NULL	
dayInYear	SMALLINT	NOT NULL	
dateYear	SMALLINT	NOT NULL	
monthNum	TINYINT	NOT NULL	
dayInWeekNum	TINYINT	NOT NULL	
quarter	TINYINT	NOT NULL	
dayInQuarter	SMALLINT	NOT NULL	
repQuarter	TINYINT	NOT NULL	
repMonth	TINYINT	NOT NULL	
repWeek	TINYINT	NOT NULL	
repDay	TINYINT	NOT NULL	
latest	TINYINT(1)	NULL	
yearLabel	CHAR(4)	NOT NULL	
monthLabel	CHAR(7)	NOT NULL	
quarterLabel	CHAR(7)	NOT NULL	
repMonthOrLatest	TINYINT	NOT NULL	
sspFlag	TINYINT	NOT NULL	
future	TINYINT(1)	NOT NULL	

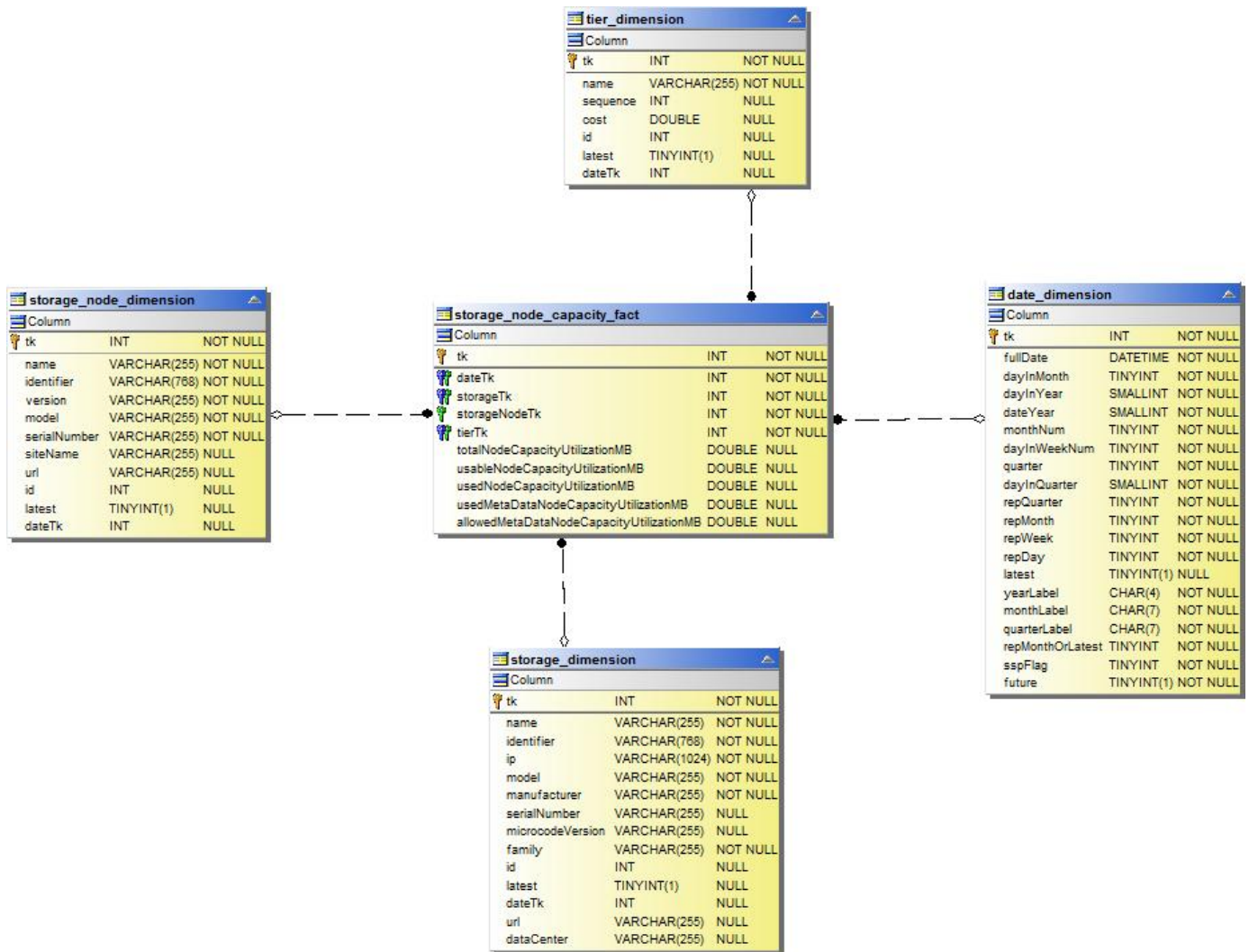
tier_dimension			
Column			
tk	INT	NOT NULL	
name	VARCHAR(255)	NOT NULL	
sequence	INT	NULL	
cost	DOUBLE	NULL	
id	INT	NULL	
latest	TINYINT(1)	NULL	
dateTk	INT	NULL	

storage_pool_dimension			
Column			
tk	INT	NOT NULL	
identifier	VARCHAR(768)	NOT NULL	
name	VARCHAR(255)	NOT NULL	
storageName	VARCHAR(255)	NOT NULL	
storageIP	VARCHAR(1024)	NOT NULL	
type	VARCHAR(255)	NULL	
redundancy	VARCHAR(255)	NULL	
thinProvisioningSupported	TINYINT(1)	NULL	
virtual	TINYINT(1)	NULL	
usesFlashPools	TINYINT(1)	NOT NULL	
id	INT	NULL	
latest	TINYINT(1)	NULL	
dateTk	INT	NULL	
isVirtual	TINYINT(1)	NULL	
url	VARCHAR(255)	NULL	

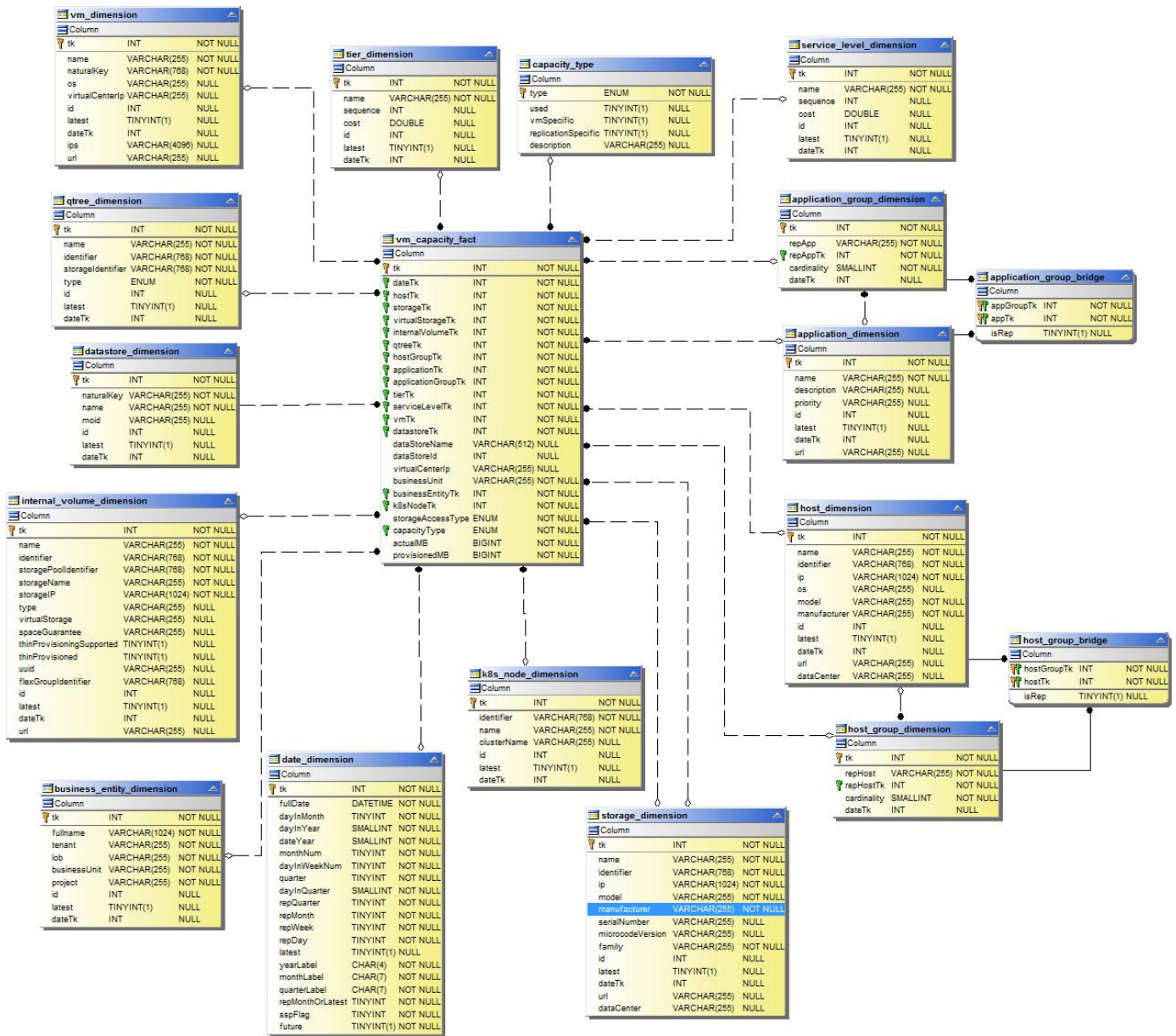
storage_dimension			
Column			
tk	INT	NOT NULL	
name	VARCHAR(255)	NOT NULL	
identifier	VARCHAR(768)	NOT NULL	
ip	VARCHAR(1024)	NOT NULL	
model	VARCHAR(255)	NOT NULL	
manufacturer	VARCHAR(255)	NOT NULL	
serialNumber	VARCHAR(255)	NULL	
microcodeVersion	VARCHAR(255)	NULL	
family	VARCHAR(255)	NOT NULL	
id	INT	NULL	
latest	TINYINT(1)	NULL	
dateTk	INT	NULL	
dataCenter	VARCHAR(255)	NULL	
url	VARCHAR(255)	NULL	

storage_and_storage_pool_capacity_fact			
Column			
tk	INT	NOT NULL	
dateTk	INT	NOT NULL	
storagePoolTk	INT	NOT NULL	
storageTk	INT	NOT NULL	
tierTk	INT	NOT NULL	
backend	TINYINT(1)	NOT NULL	
virtual	TINYINT(1)	NOT NULL	
capacityMB	BIGINT	NOT NULL	
rawCapacityMB	BIGINT	NOT NULL	
usedCapacityMB	BIGINT	NOT NULL	
usedRawCapacityMB	BIGINT	NOT NULL	
snapshotUsedCapacityMB	BIGINT	NOT NULL	
snapshotUsedRawCapacityMB	BIGINT	NOT NULL	
isVirtual	TINYINT(1)	NOT NULL	
softLimitCapacityMB	BIGINT	NULL	
unconfiguredRawCapacityMB	BIGINT	NOT NULL	
spareRawCapacityMB	BIGINT	NOT NULL	
failedRawCapacityMB	BIGINT	NOT NULL	
volumeCapacityMB	BIGINT	NOT NULL	
unusedVolumeCapacityMB	BIGINT	NOT NULL	
volumeConsumedCapacityMB	BIGINT	NOT NULL	
mappedVolumeCapacityMB	BIGINT	NOT NULL	
maskedVolumeCapacityMB	BIGINT	NOT NULL	
internalVolumeAllocatedCapacityMB	BIGINT	NOT NULL	
internalVolumeUsedCapacityMB	BIGINT	NOT NULL	
internalVolumeConsumedCapacityMB	BIGINT	NOT NULL	
dedupeRatio	FLOAT	NULL	
dedupeSavingsGB	BIGINT	NULL	
compressionRatio	FLOAT	NULL	
compressionSavingsGB	BIGINT	NULL	
compactionRatio	FLOAT	NULL	
compactionSavingsGB	BIGINT	NULL	
objectStoreUsedSpaceGB	BIGINT	NULL	

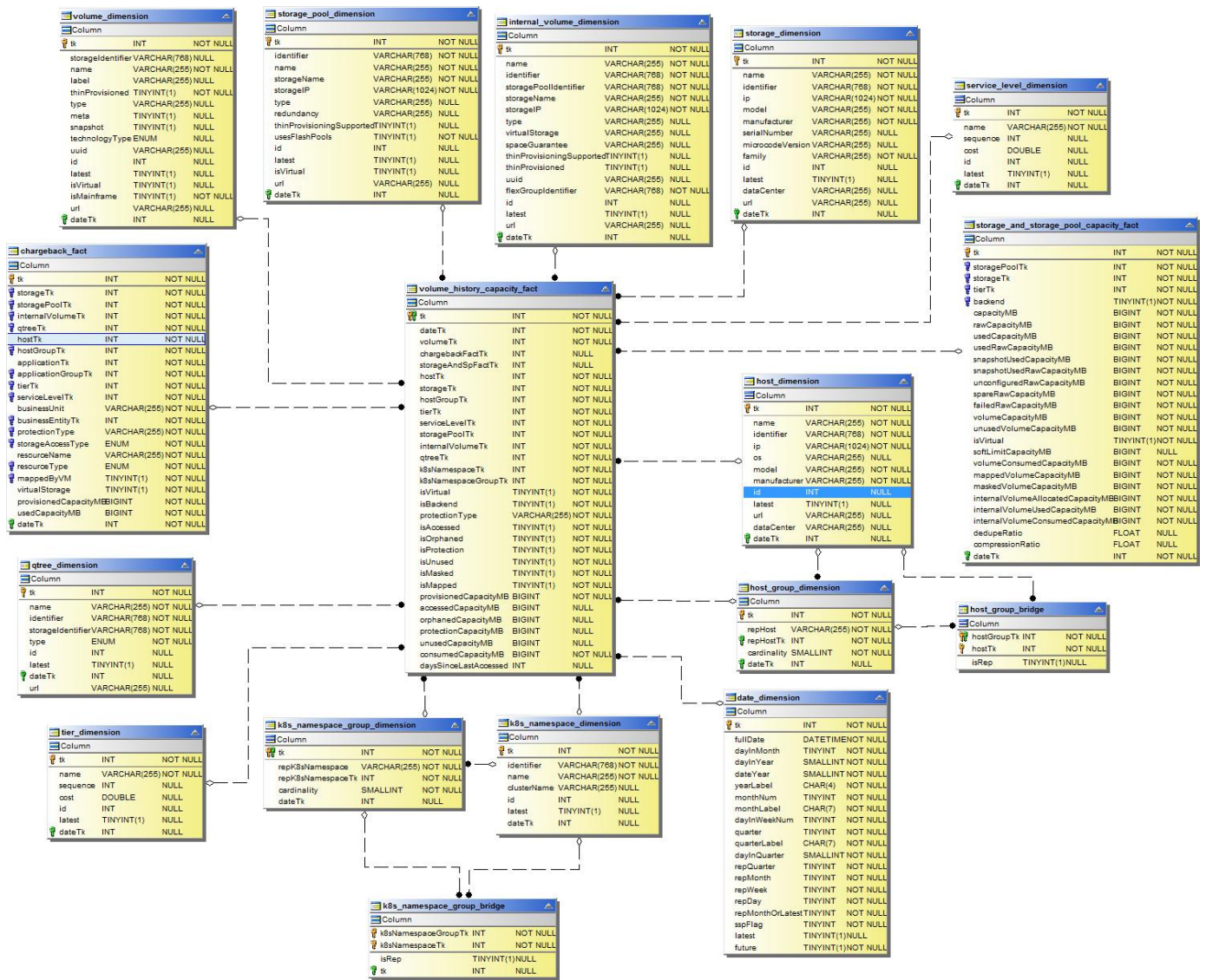
Speicherknotenkapazität



VM-Kapazität



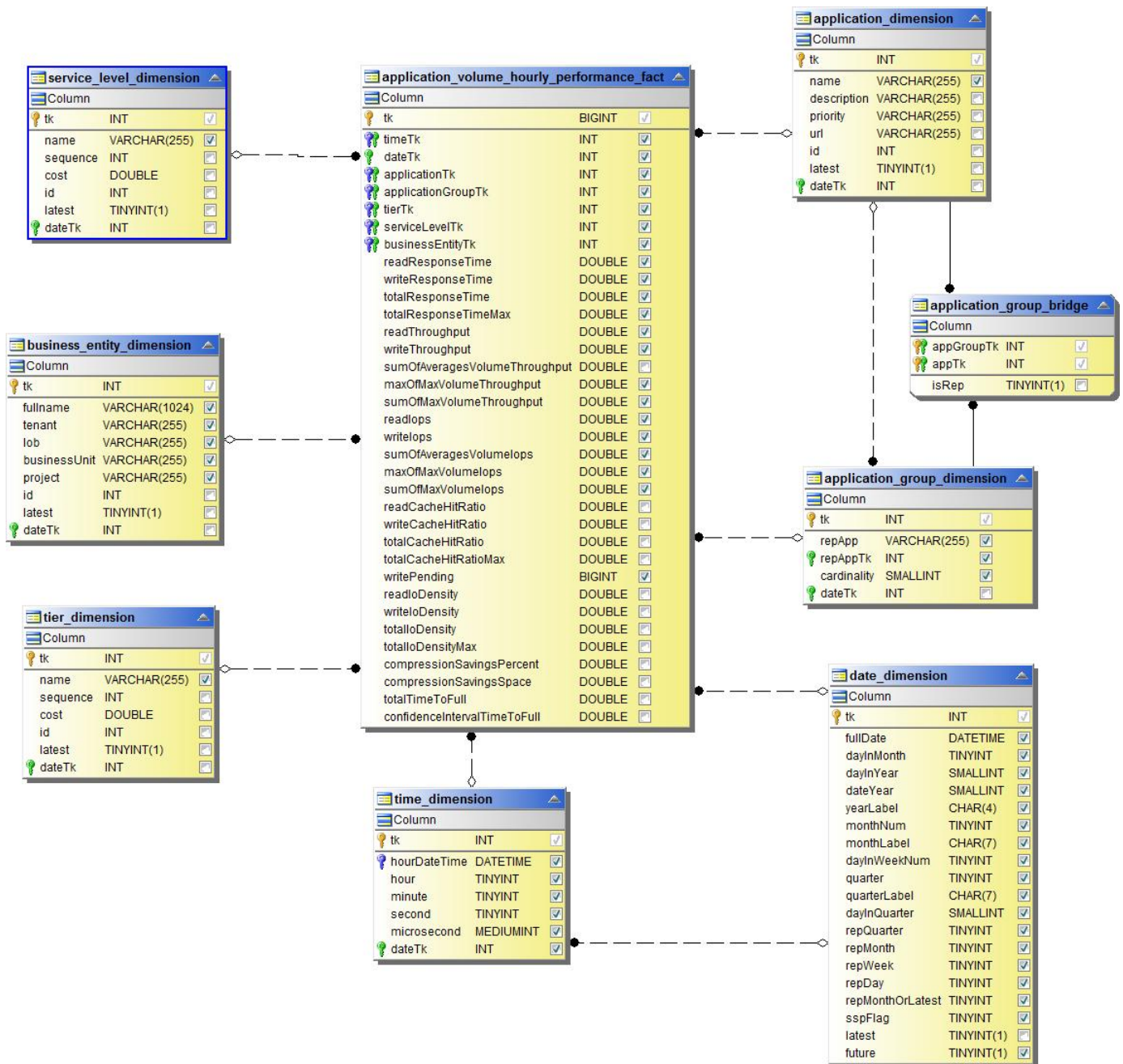
Volumenkapazität



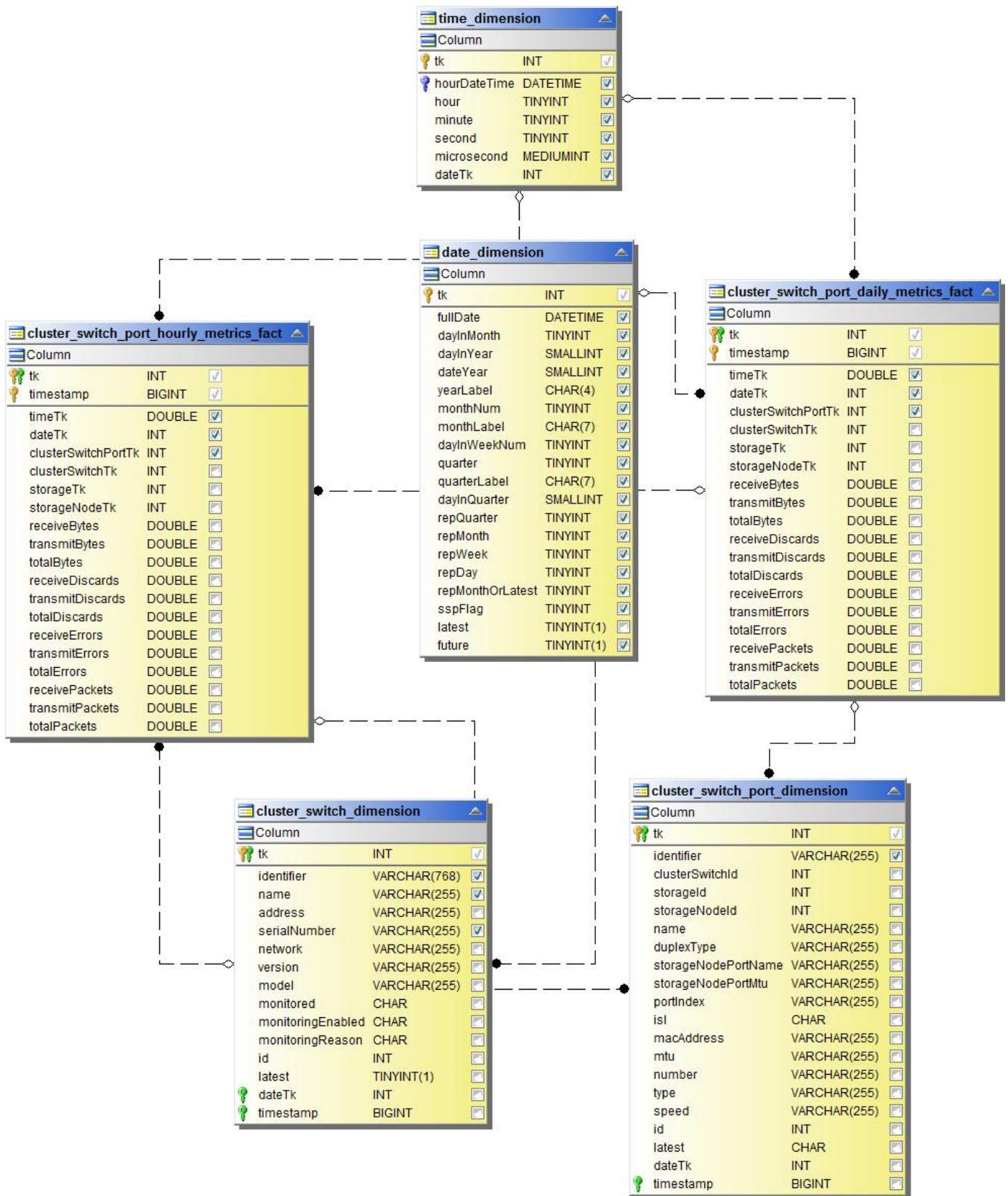
Leistungs-Datamart

Die folgenden Bilder beschreiben den Performance-Datamart.

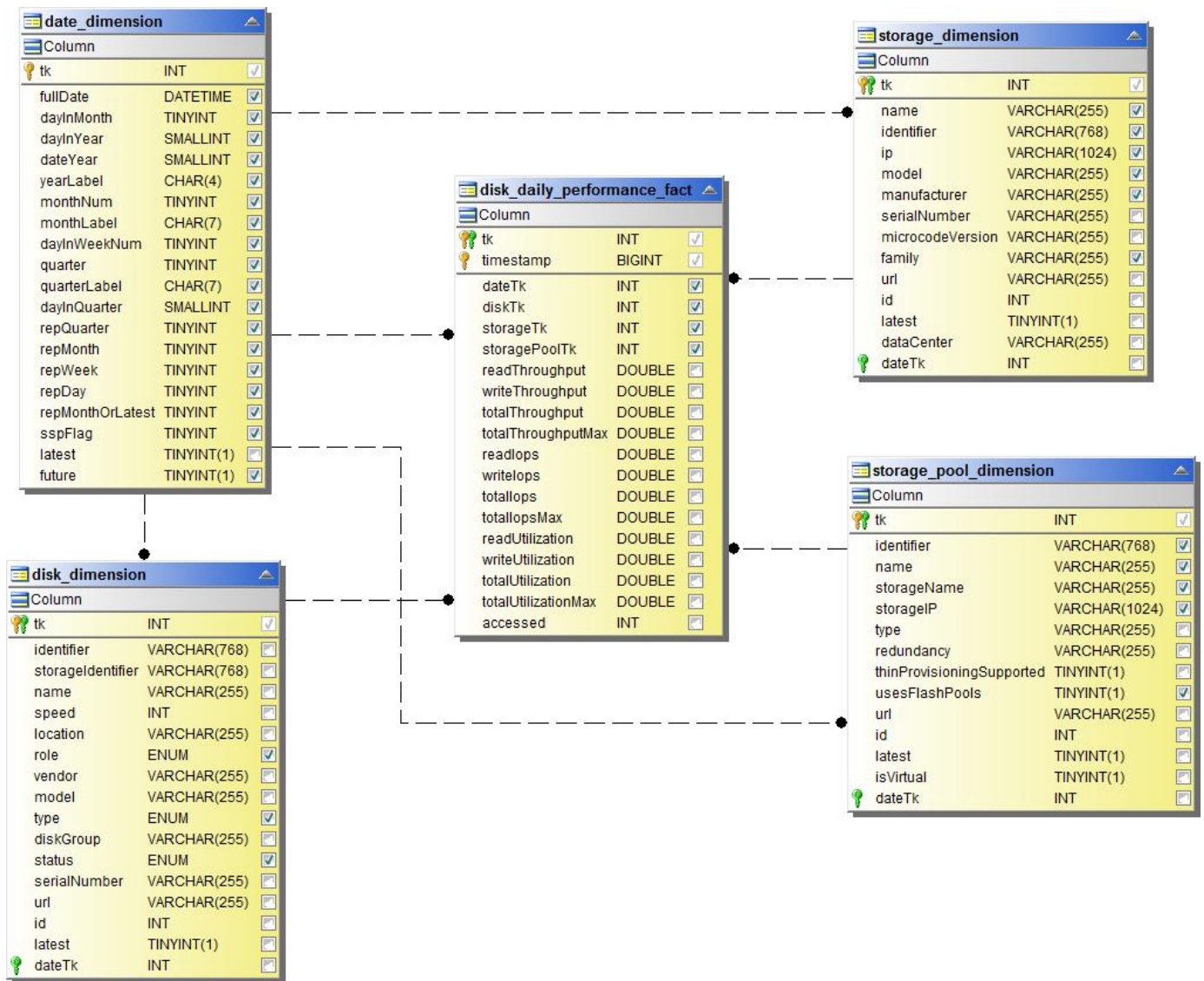
Anwendungsvolumen Stündliche Leistung



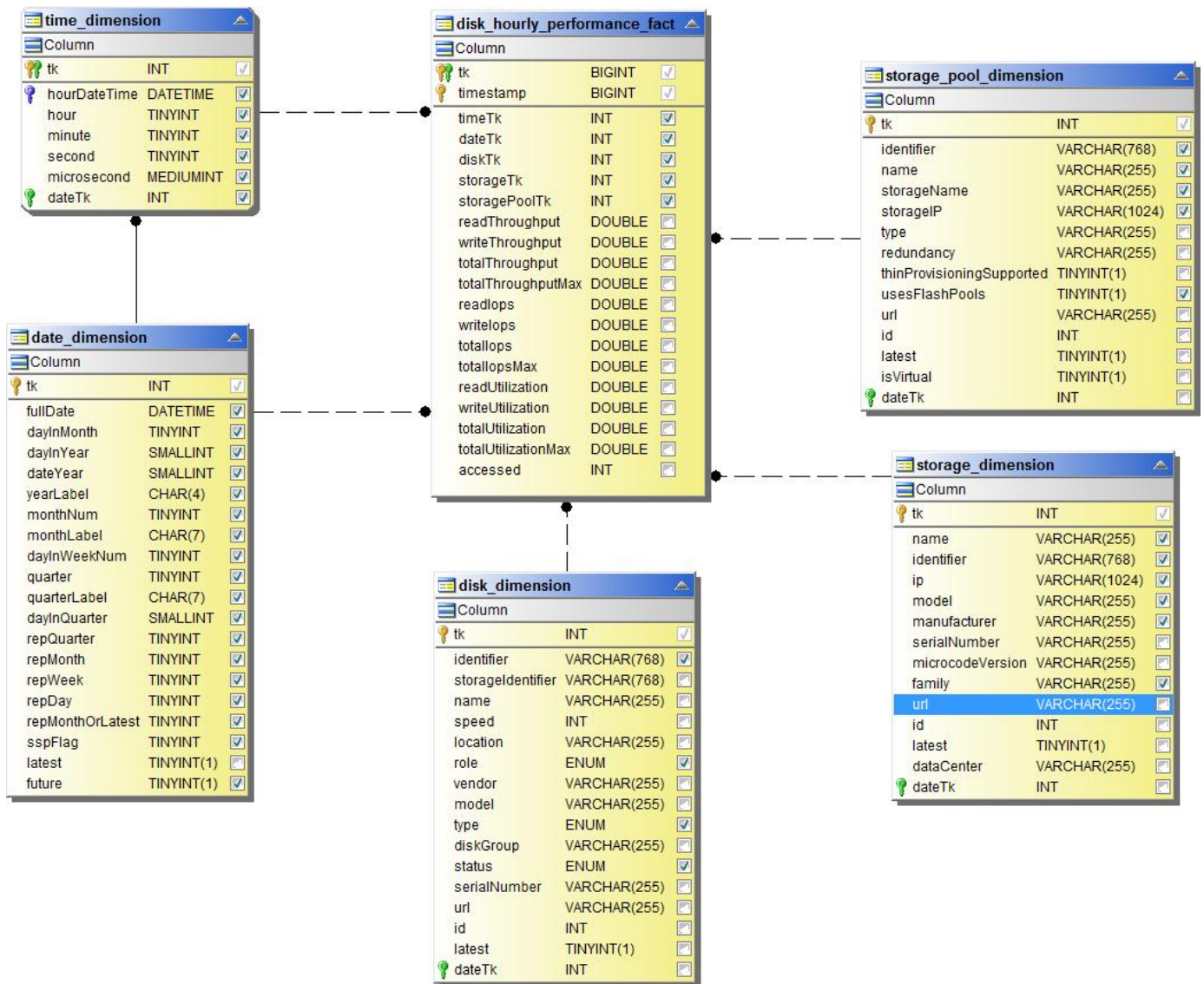
Cluster-Switch-Leistung



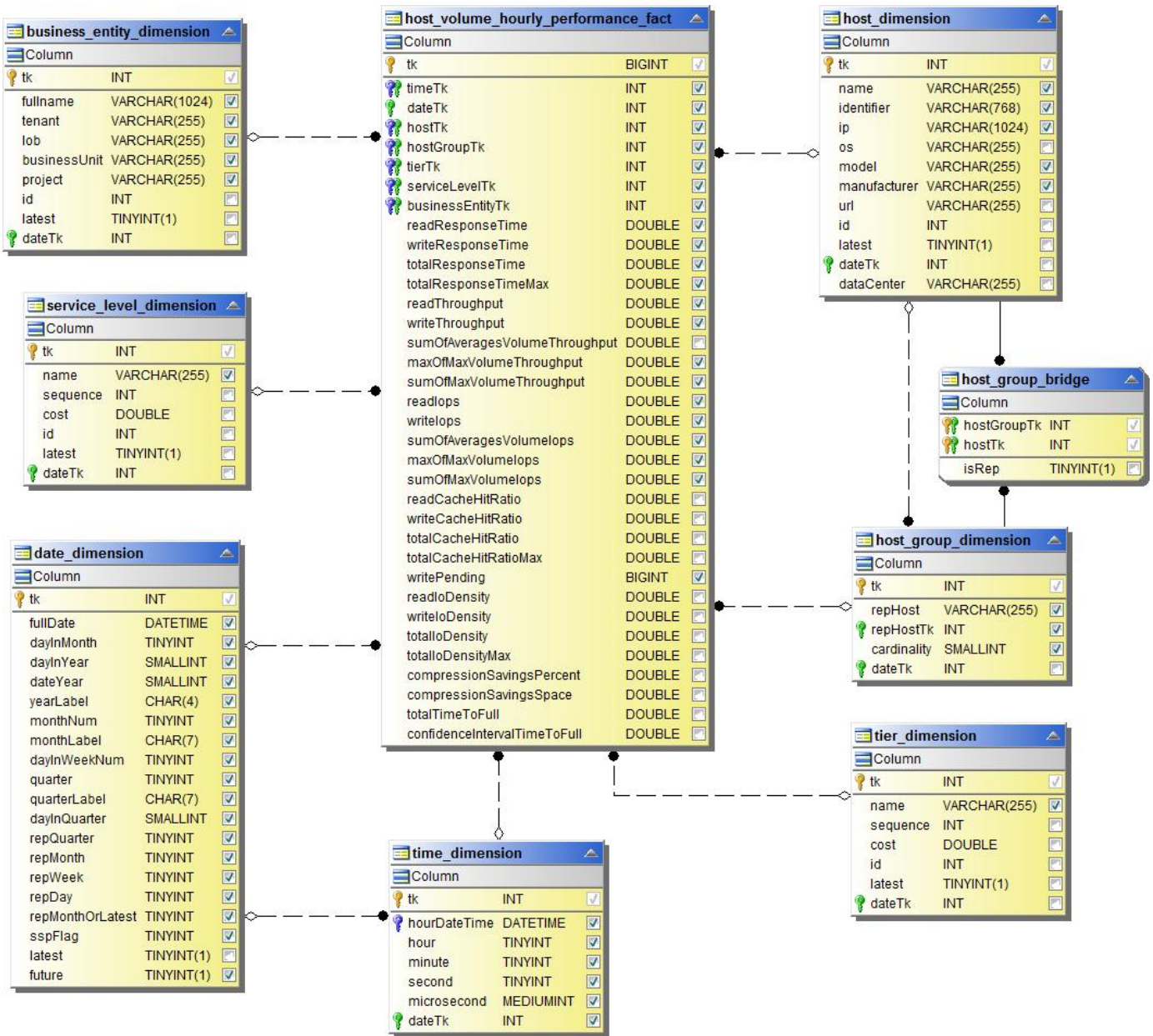
Tägliche Festplattenleistung



Stündliche Festplattenleistung



Host-Stundenleistung



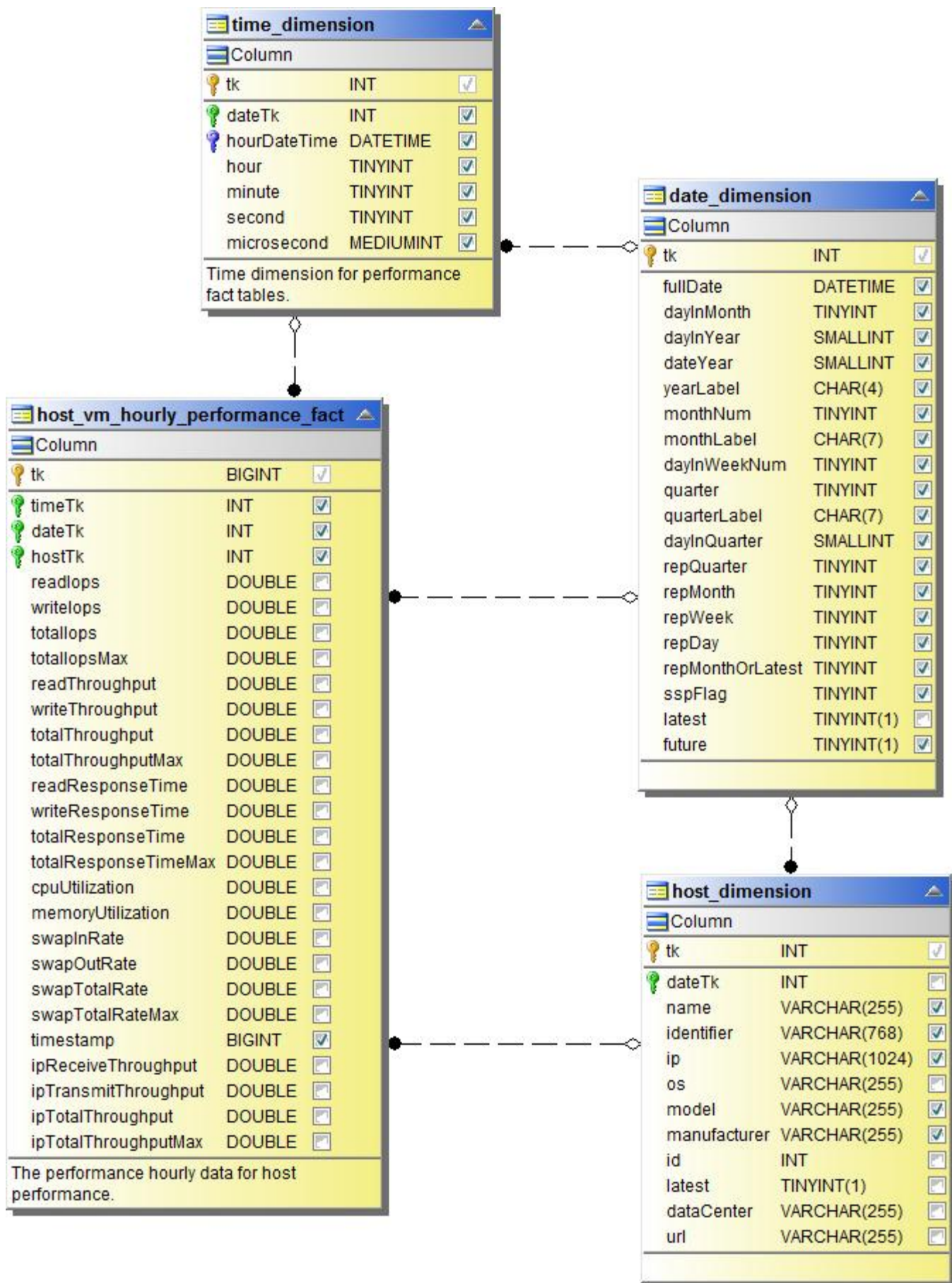
Tägliche Leistung der Host-VM

host_vm_daily_performance_fact		
Column		
tk	INT	<input checked="" type="checkbox"/>
dateTk	INT	<input checked="" type="checkbox"/>
hostTk	INT	<input checked="" type="checkbox"/>
readIops	DOUBLE	<input type="checkbox"/>
writeIops	DOUBLE	<input type="checkbox"/>
totalIops	DOUBLE	<input type="checkbox"/>
totalIopsMax	DOUBLE	<input type="checkbox"/>
readThroughput	DOUBLE	<input type="checkbox"/>
writeThroughput	DOUBLE	<input type="checkbox"/>
totalThroughput	DOUBLE	<input type="checkbox"/>
totalThroughputMax	DOUBLE	<input type="checkbox"/>
readResponseTime	DOUBLE	<input type="checkbox"/>
writeResponseTime	DOUBLE	<input type="checkbox"/>
totalResponseTime	DOUBLE	<input type="checkbox"/>
totalResponseTimeMax	DOUBLE	<input type="checkbox"/>
cpuUtilization	DOUBLE	<input type="checkbox"/>
maxOfAvgCpuUtilization	DOUBLE	<input type="checkbox"/>
memoryUtilization	DOUBLE	<input type="checkbox"/>
maxOfAvgMemoryUtilization	DOUBLE	<input type="checkbox"/>
swapInRate	DOUBLE	<input type="checkbox"/>
maxOfAvgSwapInRate	DOUBLE	<input type="checkbox"/>
swapOutRate	DOUBLE	<input type="checkbox"/>
maxOfAvgSWapOutRate	DOUBLE	<input type="checkbox"/>
swapTotalRate	DOUBLE	<input type="checkbox"/>
swapTotalRateMax	DOUBLE	<input type="checkbox"/>
timestamp	BIGINT	<input checked="" type="checkbox"/>
ipReceiveThroughput	DOUBLE	<input type="checkbox"/>
ipTransmitThroughput	DOUBLE	<input type="checkbox"/>
ipTotalThroughput	DOUBLE	<input type="checkbox"/>
ipTotalThroughputMax	DOUBLE	<input type="checkbox"/>
The performance daily data for host vm performance.		

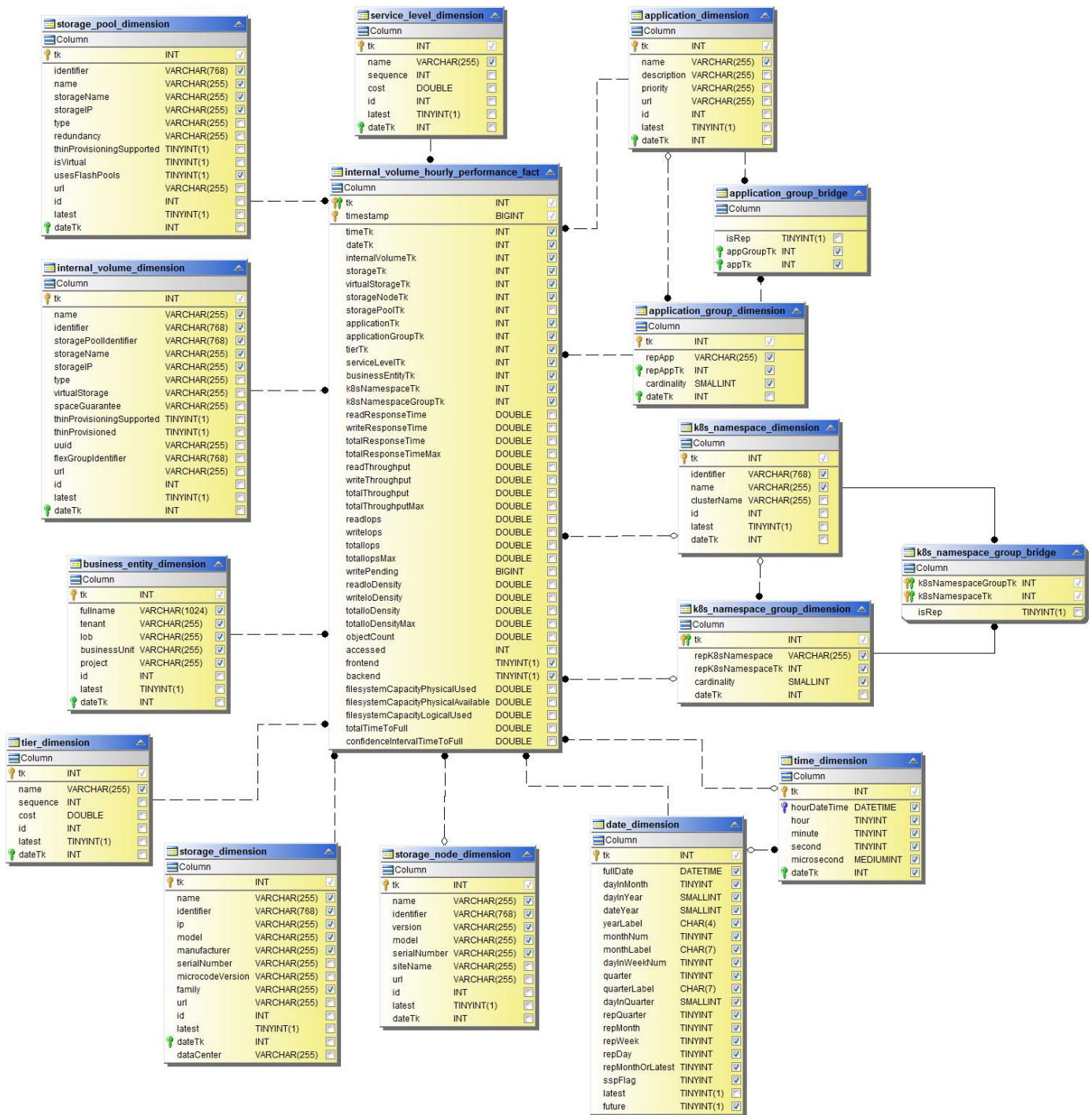
date_dimension		
Column		
tk	INT	<input checked="" type="checkbox"/>
fullDate	DATETIME	<input checked="" type="checkbox"/>
dayInMonth	TINYINT	<input checked="" type="checkbox"/>
dayInYear	SMALLINT	<input checked="" type="checkbox"/>
dateYear	SMALLINT	<input checked="" type="checkbox"/>
yearLabel	CHAR(4)	<input checked="" type="checkbox"/>
monthNum	TINYINT	<input checked="" type="checkbox"/>
monthLabel	CHAR(7)	<input checked="" type="checkbox"/>
dayInWeekNum	TINYINT	<input checked="" type="checkbox"/>
quarter	TINYINT	<input checked="" type="checkbox"/>
quarterLabel	CHAR(7)	<input checked="" type="checkbox"/>
dayInQuarter	SMALLINT	<input checked="" type="checkbox"/>
repQuarter	TINYINT	<input checked="" type="checkbox"/>
repMonth	TINYINT	<input checked="" type="checkbox"/>
repWeek	TINYINT	<input checked="" type="checkbox"/>
repDay	TINYINT	<input checked="" type="checkbox"/>
repMonthOrLatest	TINYINT	<input checked="" type="checkbox"/>
sspFlag	TINYINT	<input checked="" type="checkbox"/>
latest	TINYINT(1)	<input checked="" type="checkbox"/>
future	TINYINT(1)	<input checked="" type="checkbox"/>

host_dimension		
Column		
tk	INT	<input checked="" type="checkbox"/>
dateTk	INT	<input type="checkbox"/>
name	VARCHAR(255)	<input checked="" type="checkbox"/>
identifier	VARCHAR(768)	<input checked="" type="checkbox"/>
ip	VARCHAR(1024)	<input checked="" type="checkbox"/>
os	VARCHAR(255)	<input type="checkbox"/>
model	VARCHAR(255)	<input checked="" type="checkbox"/>
manufacturer	VARCHAR(255)	<input checked="" type="checkbox"/>
id	INT	<input type="checkbox"/>
latest	TINYINT(1)	<input type="checkbox"/>
dataCenter	VARCHAR(255)	<input type="checkbox"/>
url	VARCHAR(255)	<input type="checkbox"/>

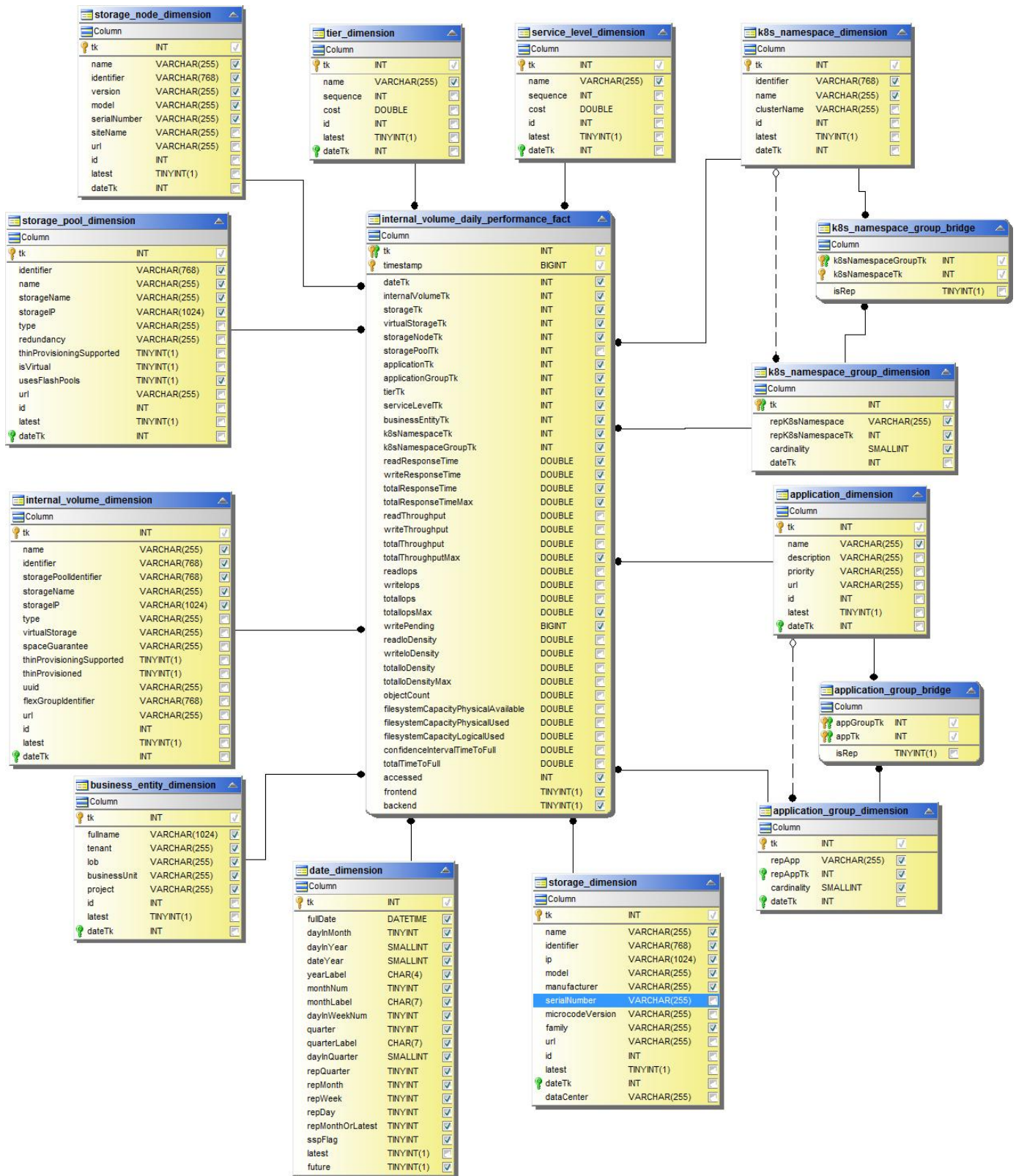
Host-VM-Stündliche Leistung



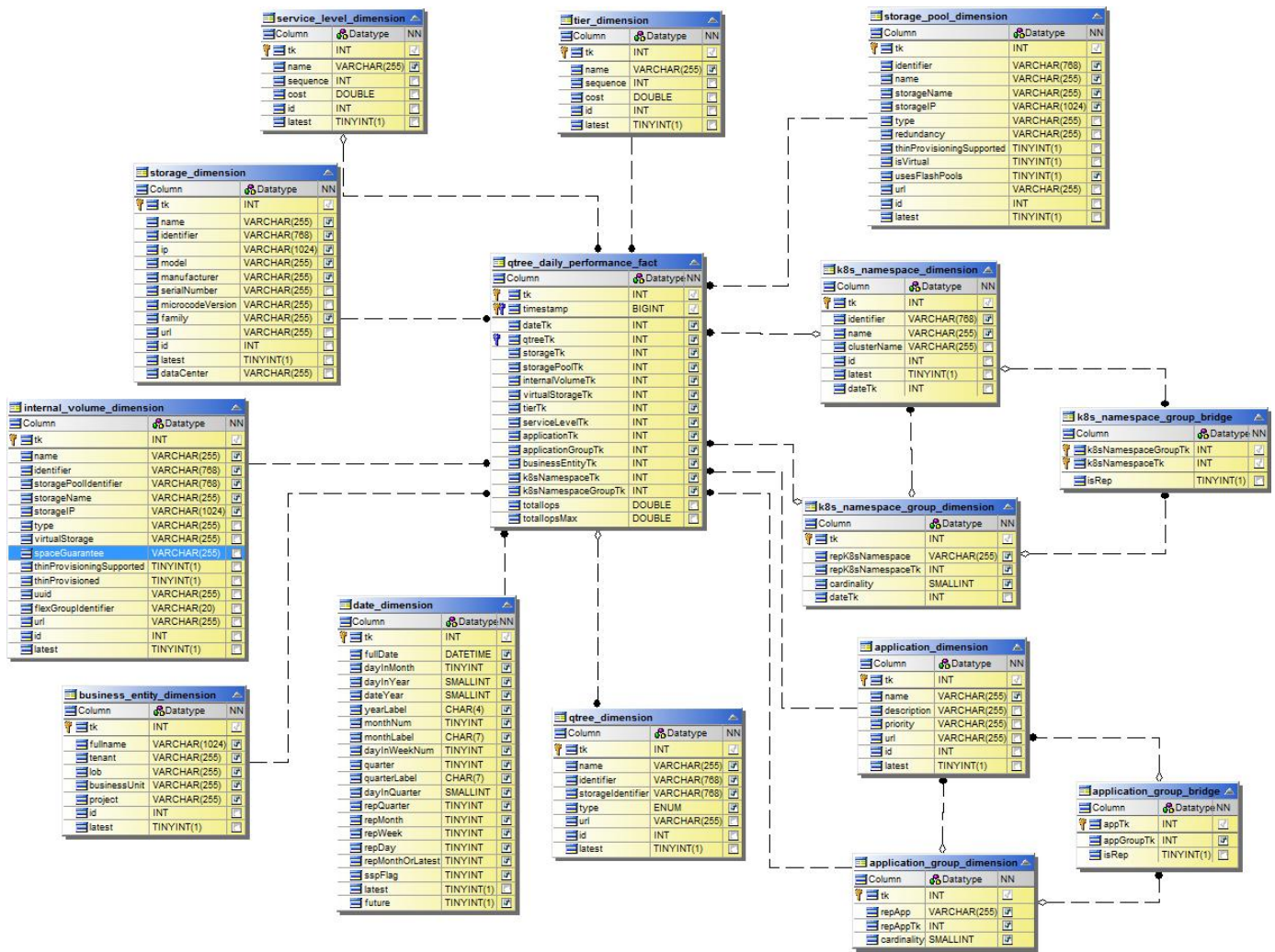
Internes Volumen, stündliche Leistung



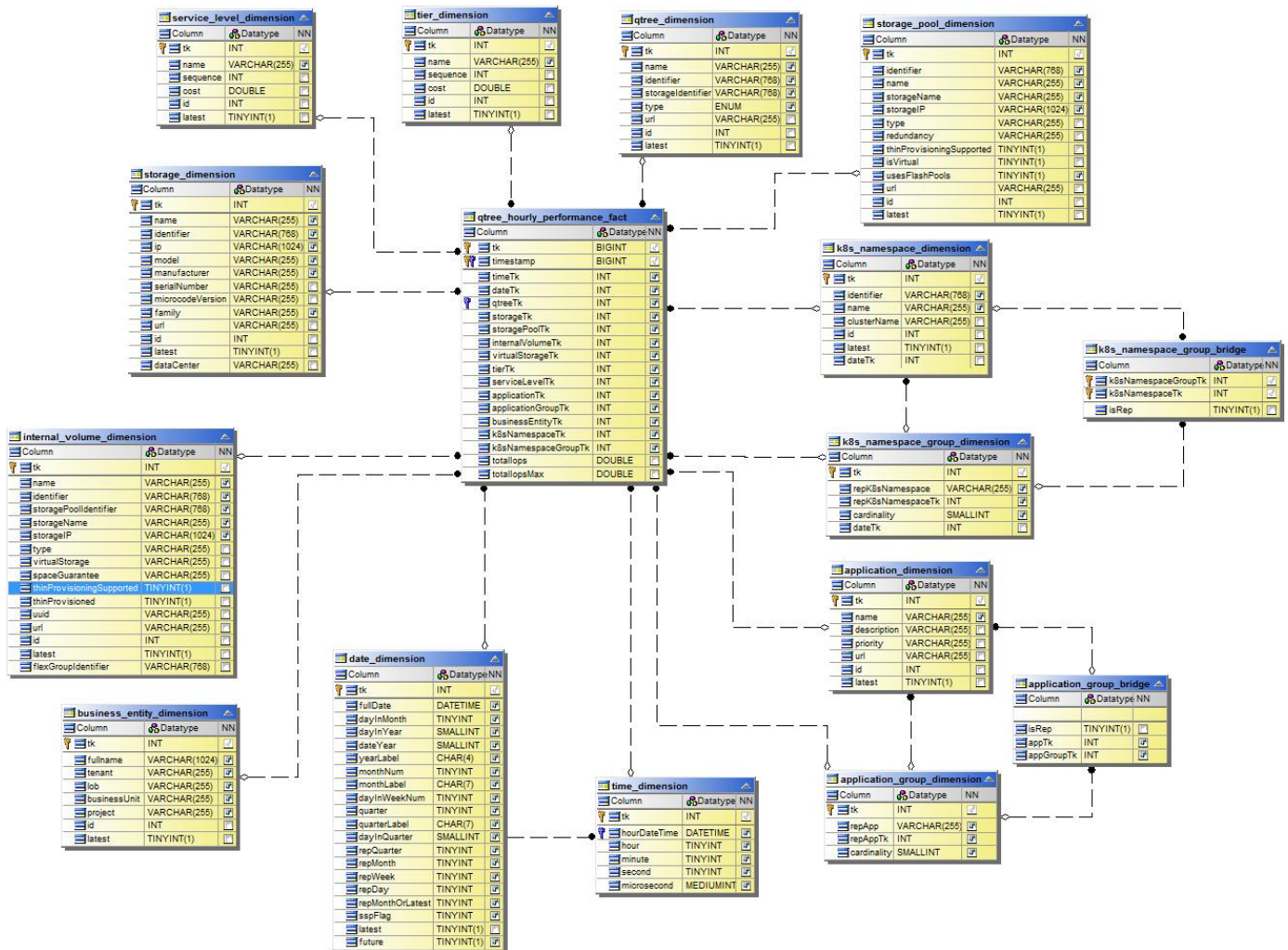
Internes Volumen – Tägliche Leistung



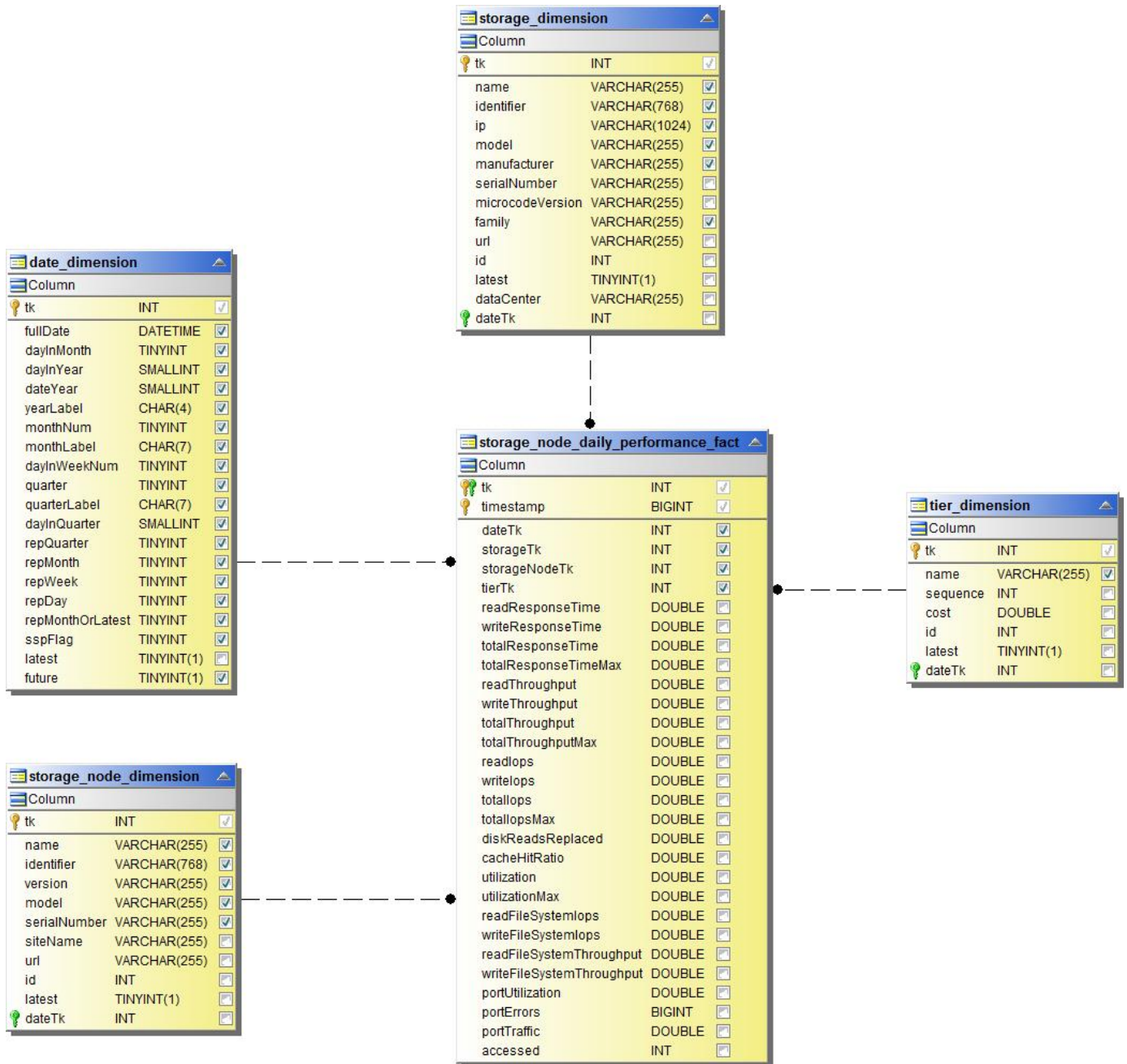
Qtree Tägliche Leistung



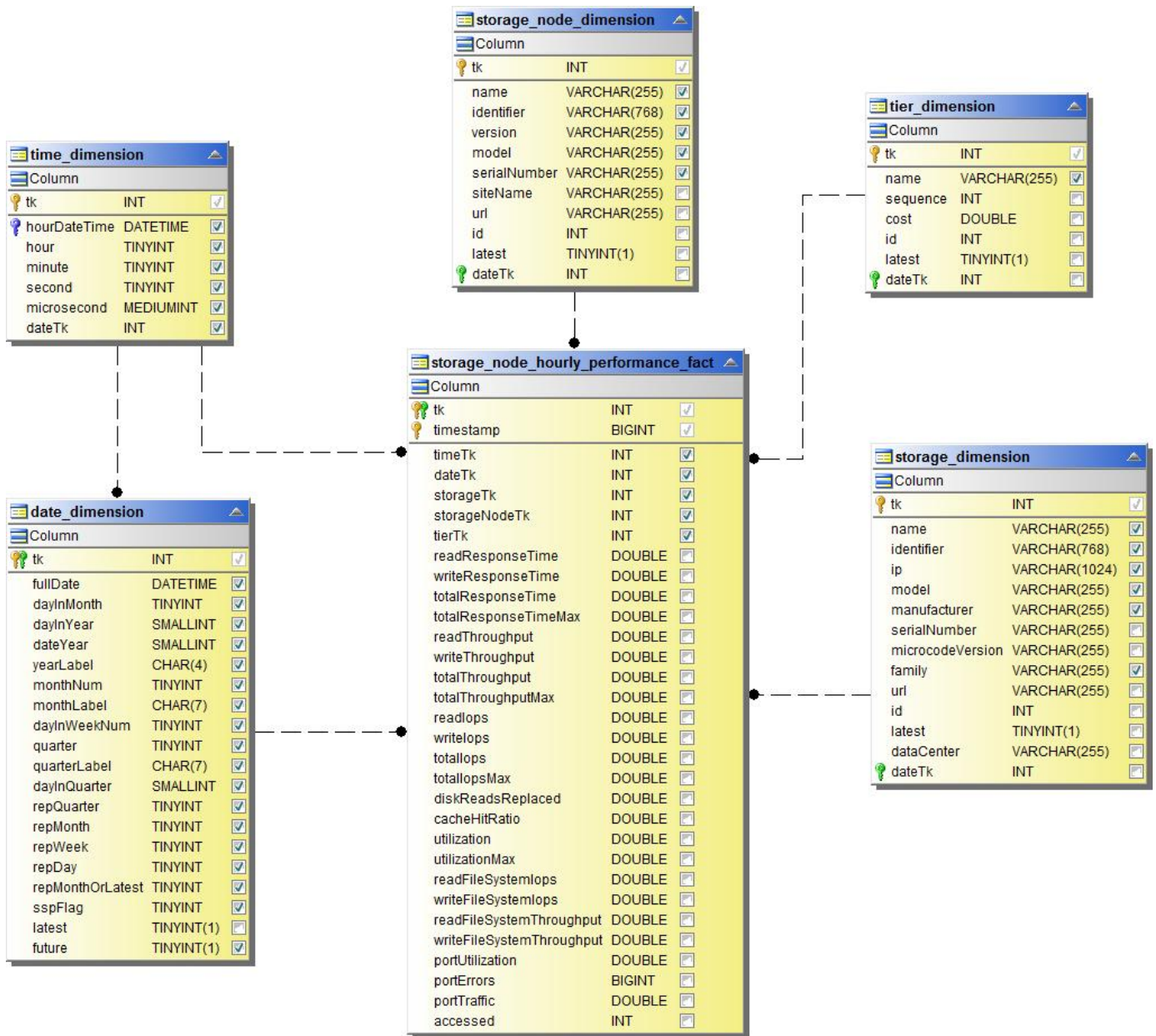
Qtree Stundenleistung



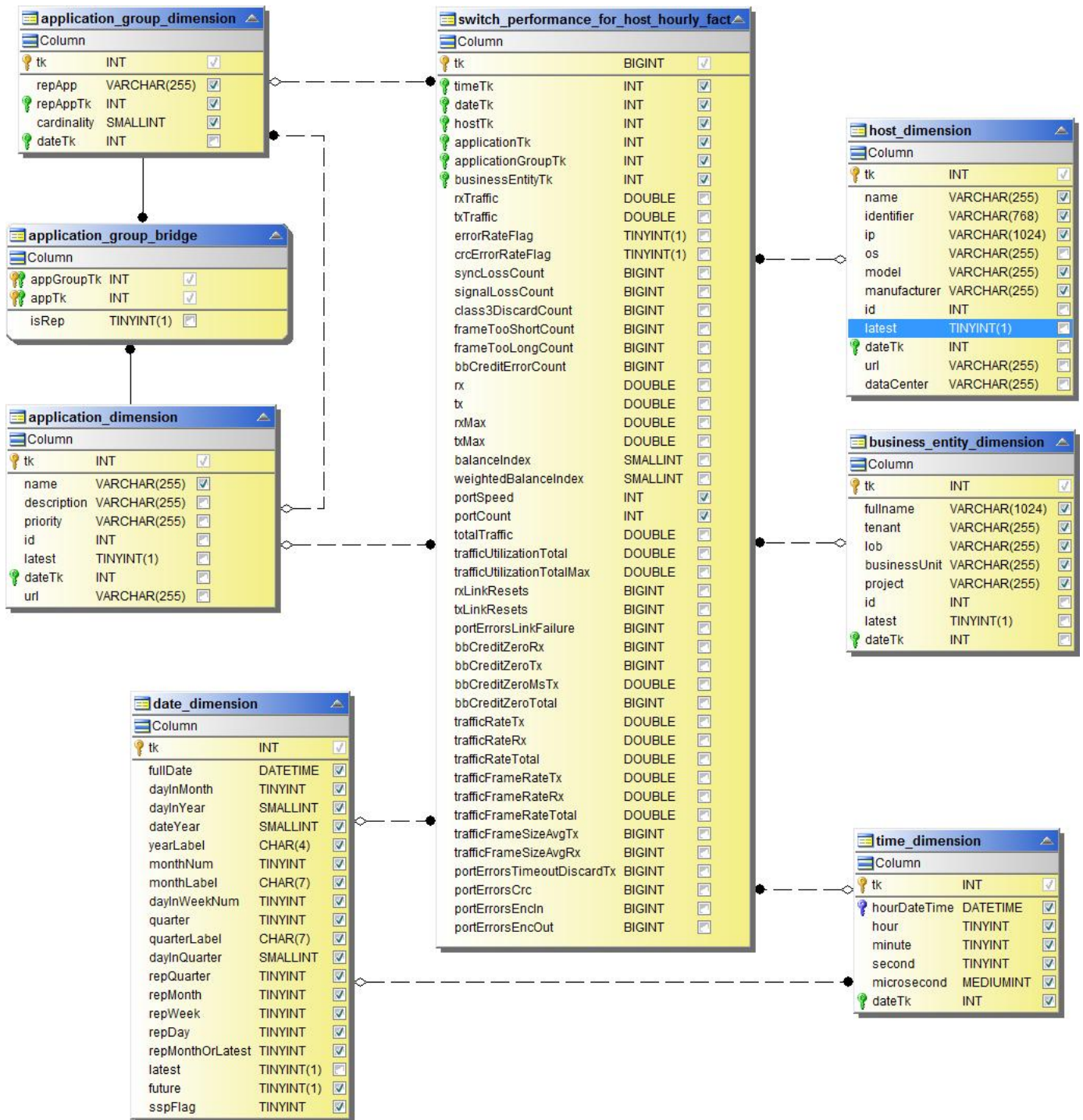
Tägliche Leistung des Speicherknotens



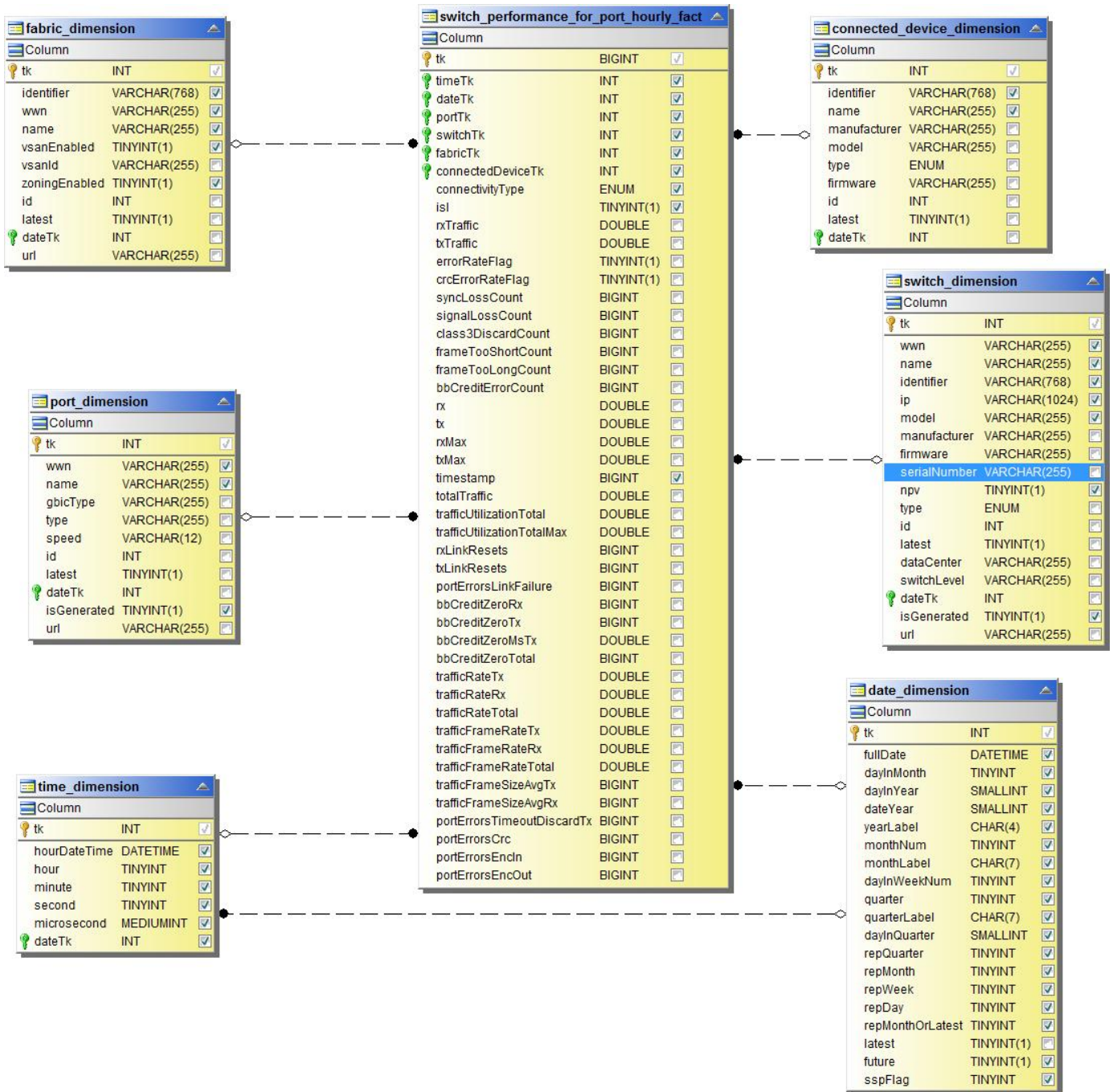
Stündliche Leistung des Speicherknotens



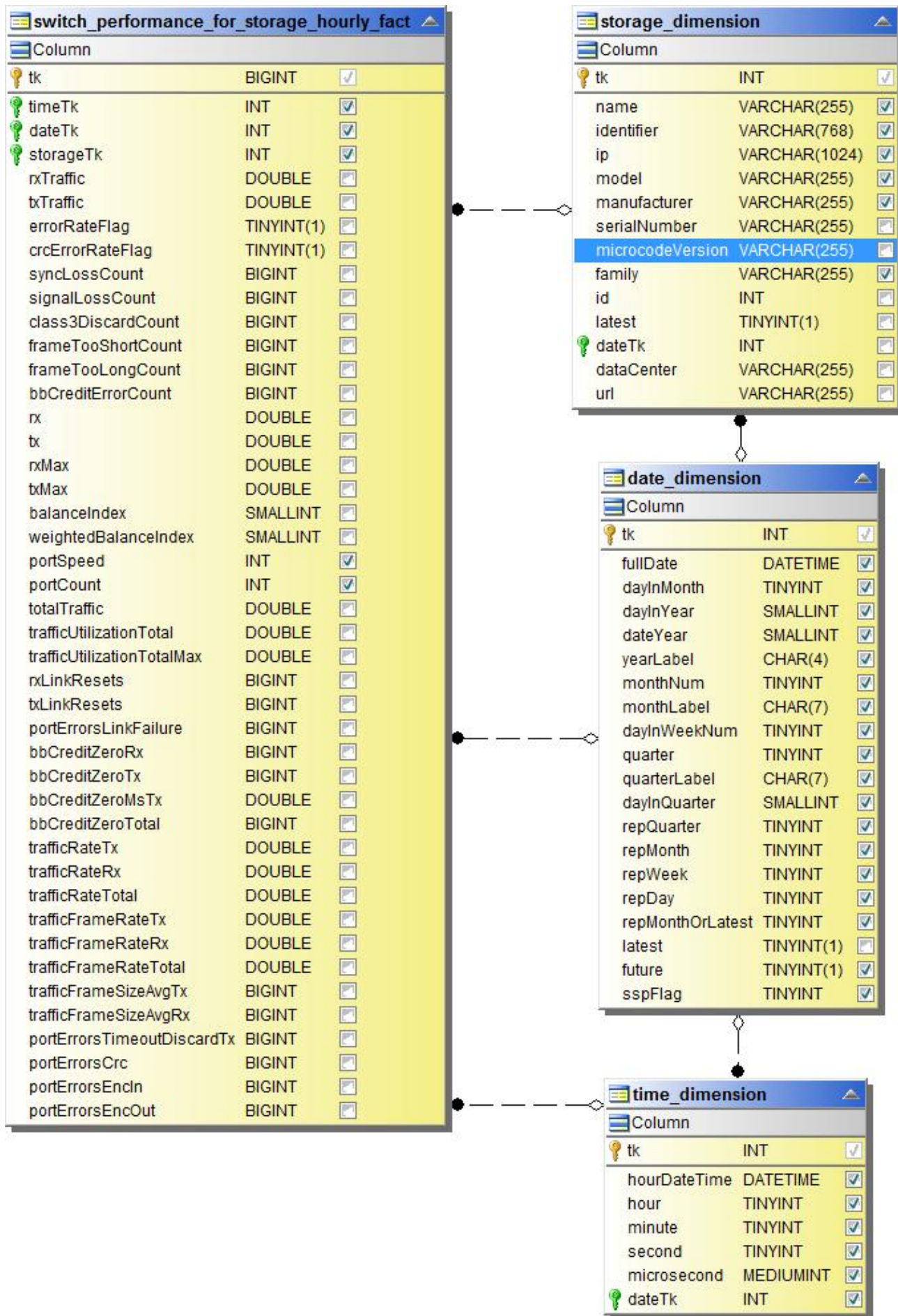
Switch-Stundenleistung für Host

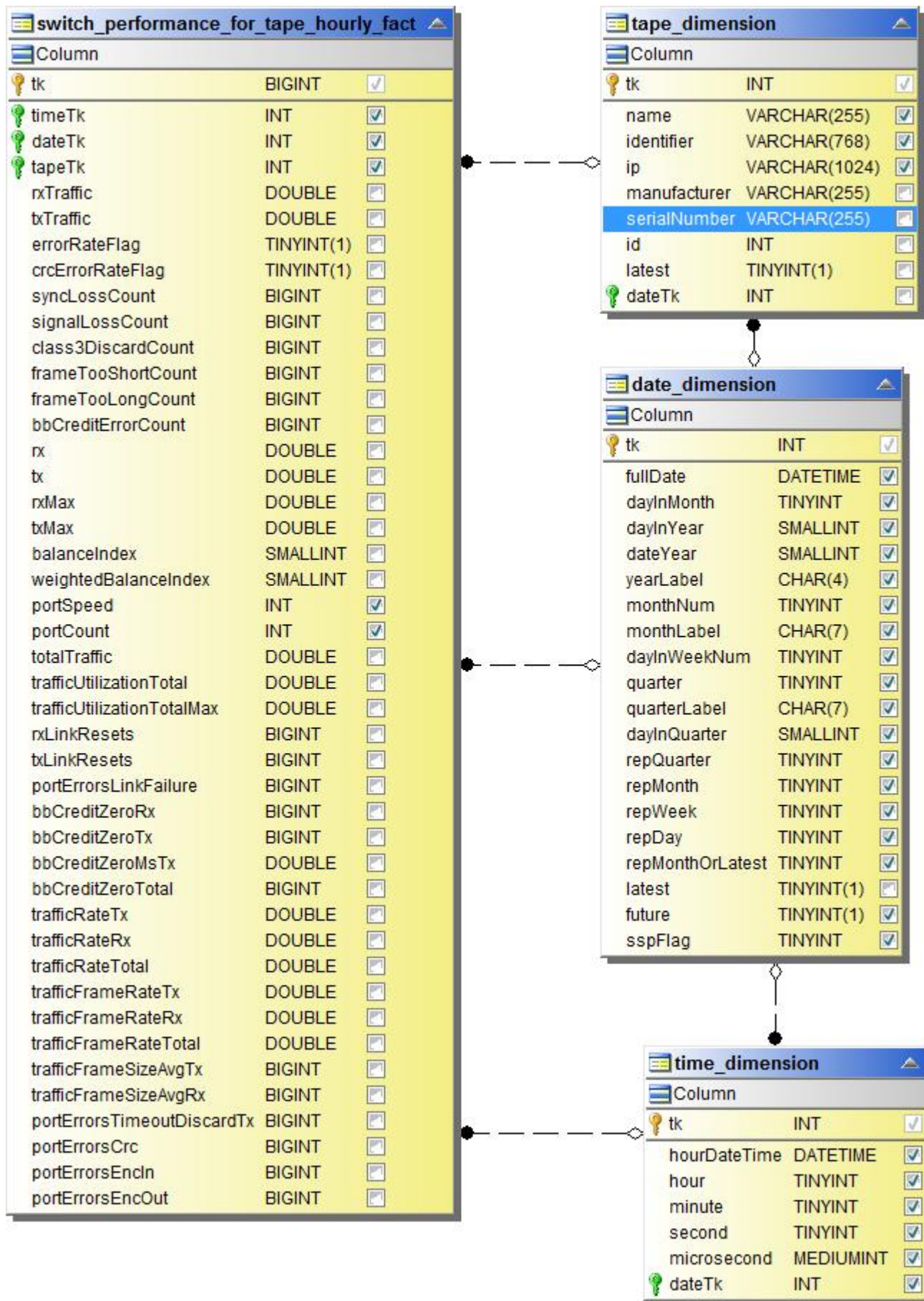


Switch-Stundenleistung für Port

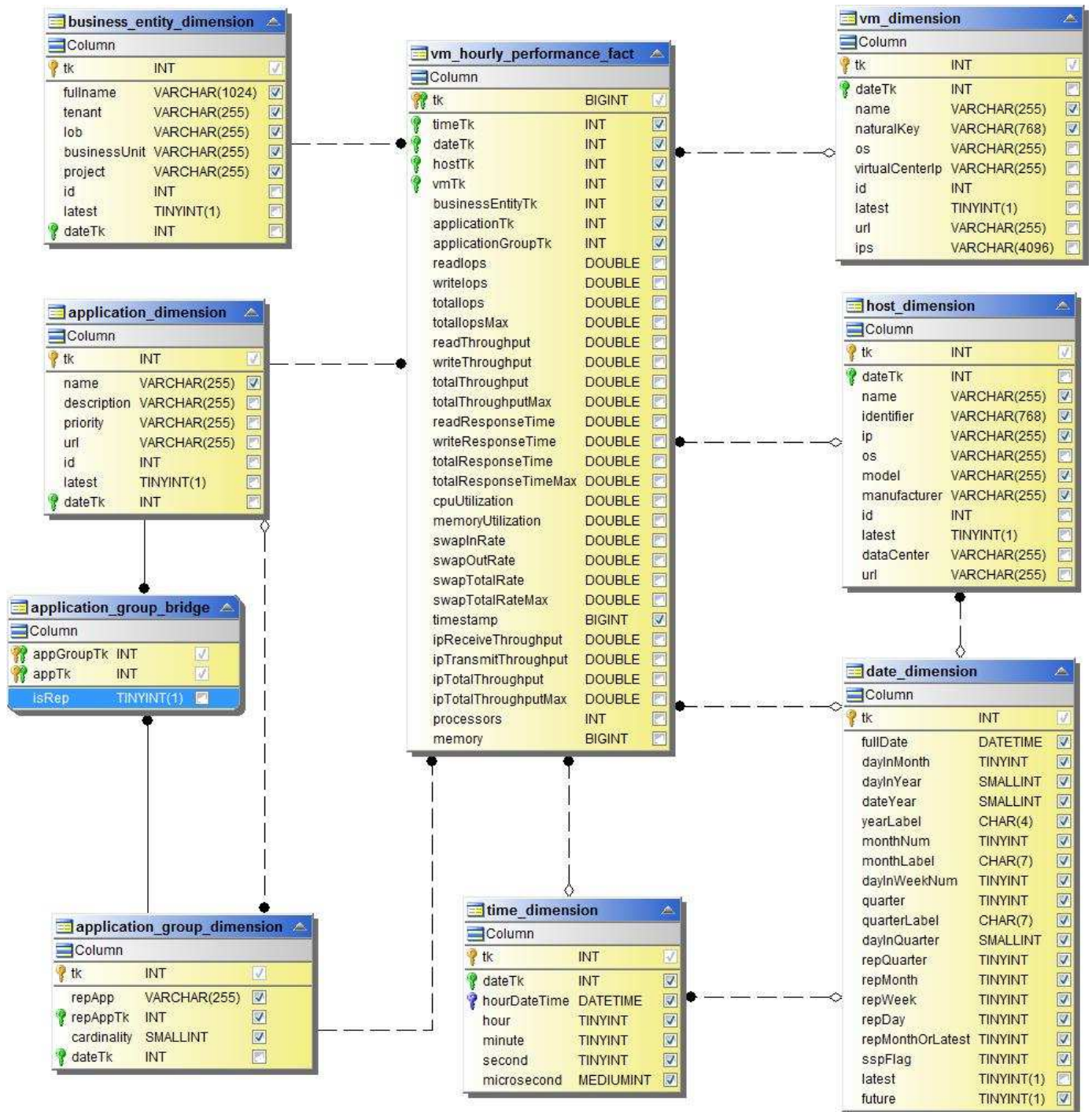


Switch-Stundenleistung für Speicher

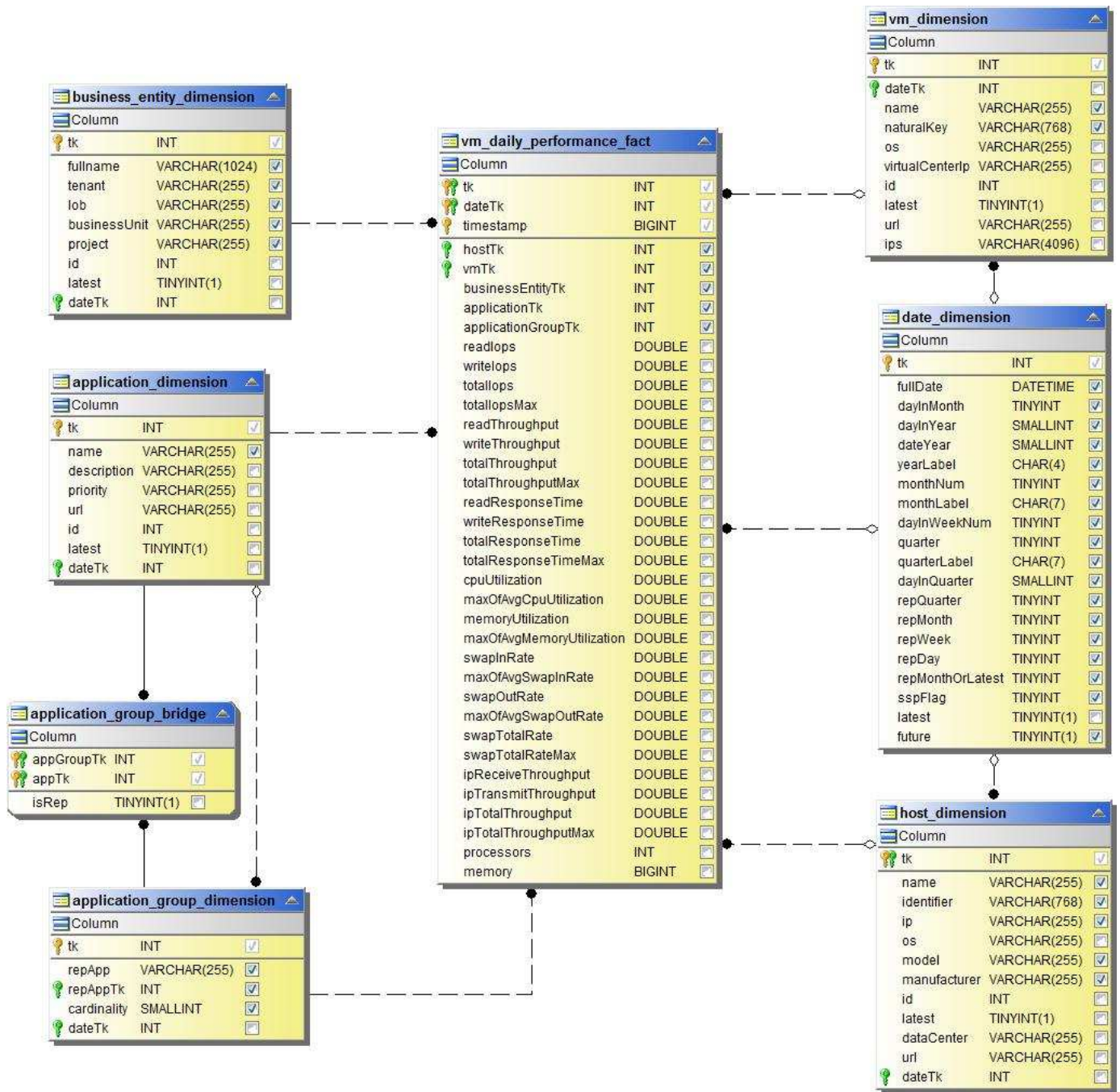




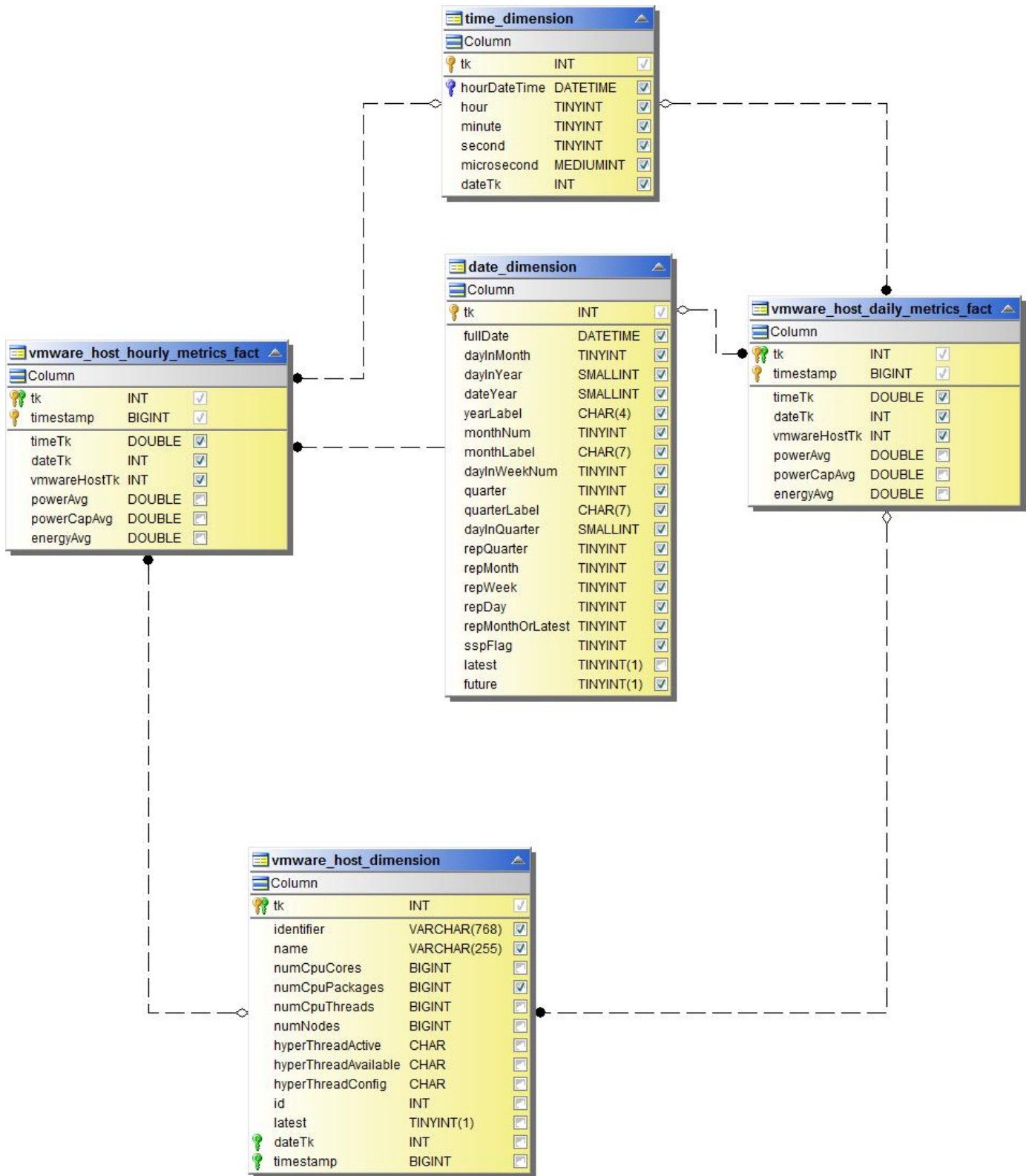
VM-Leistung



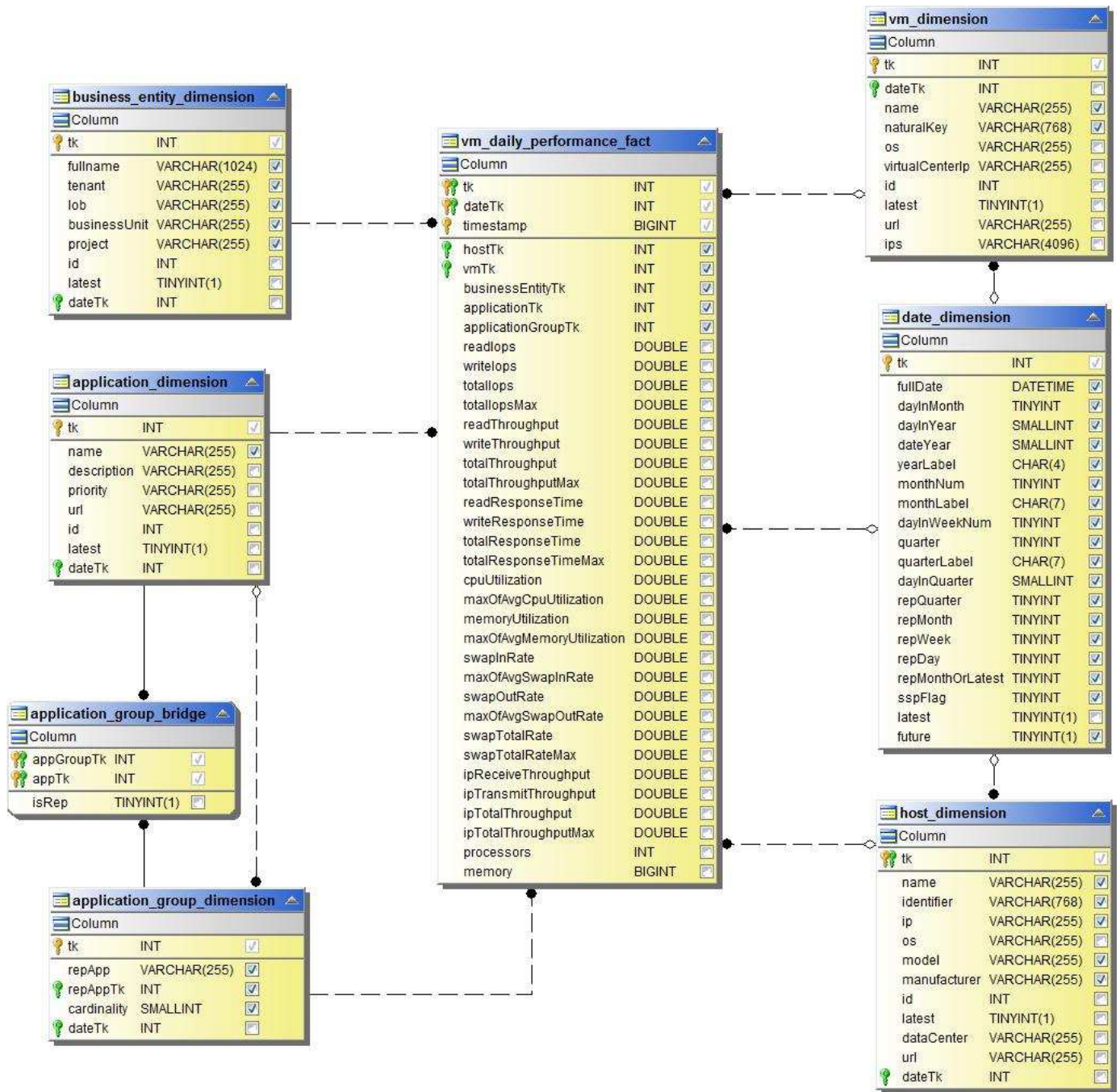
Tägliche VM-Leistung für Host



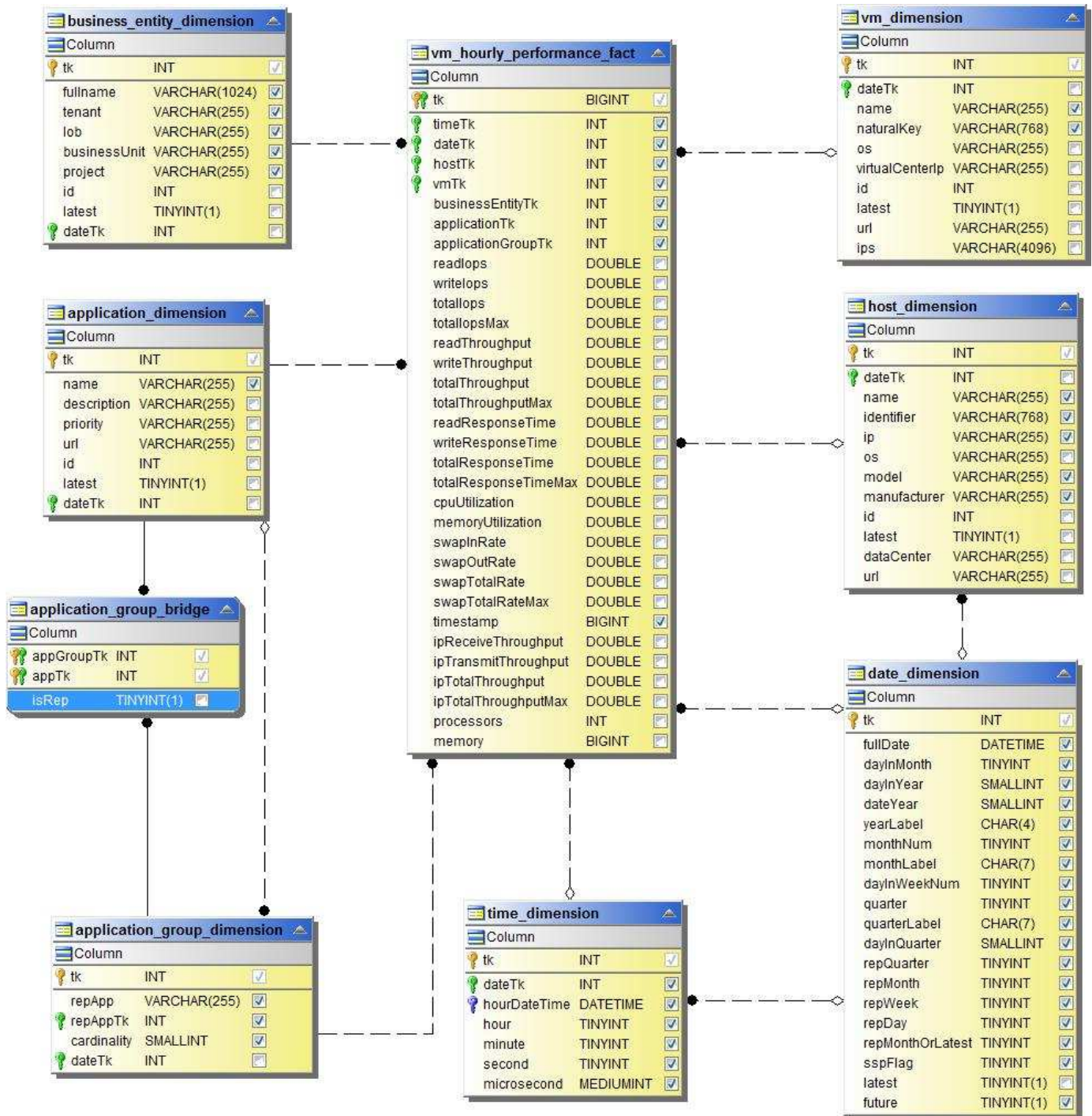
VM-Stundenleistung für Host



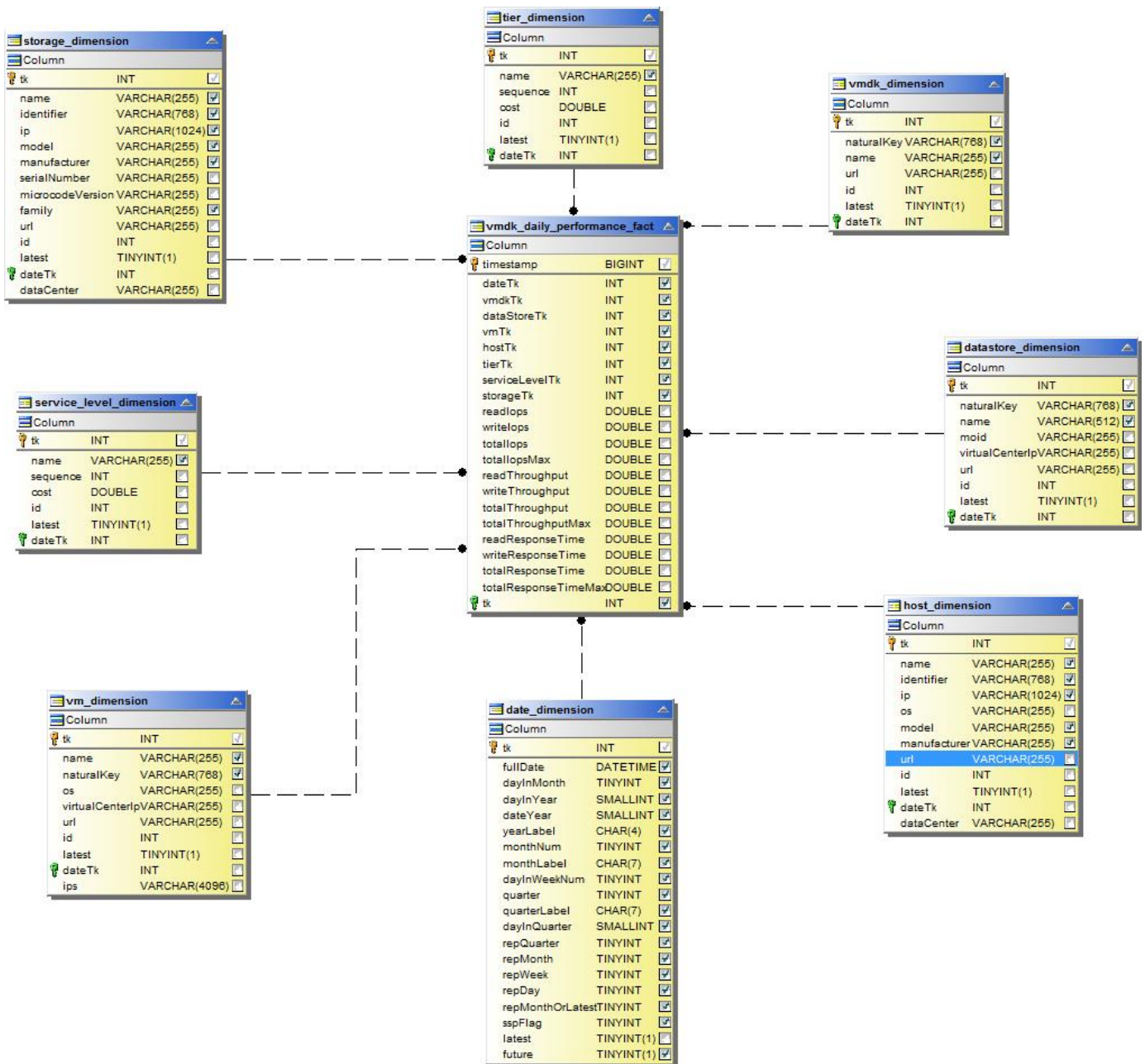
Tägliche VM-Leistung für Host



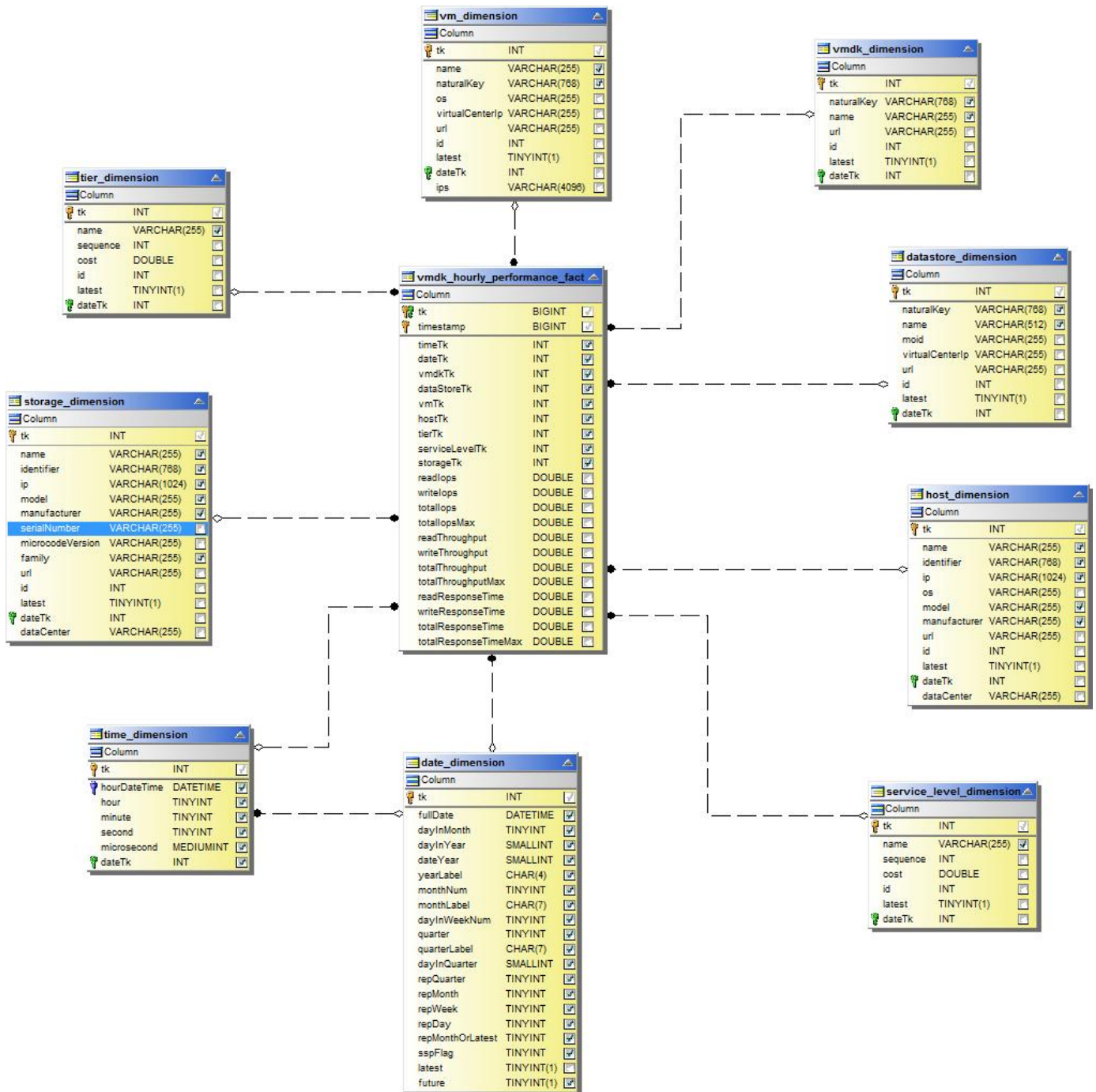
VM-Stundenleistung für Host



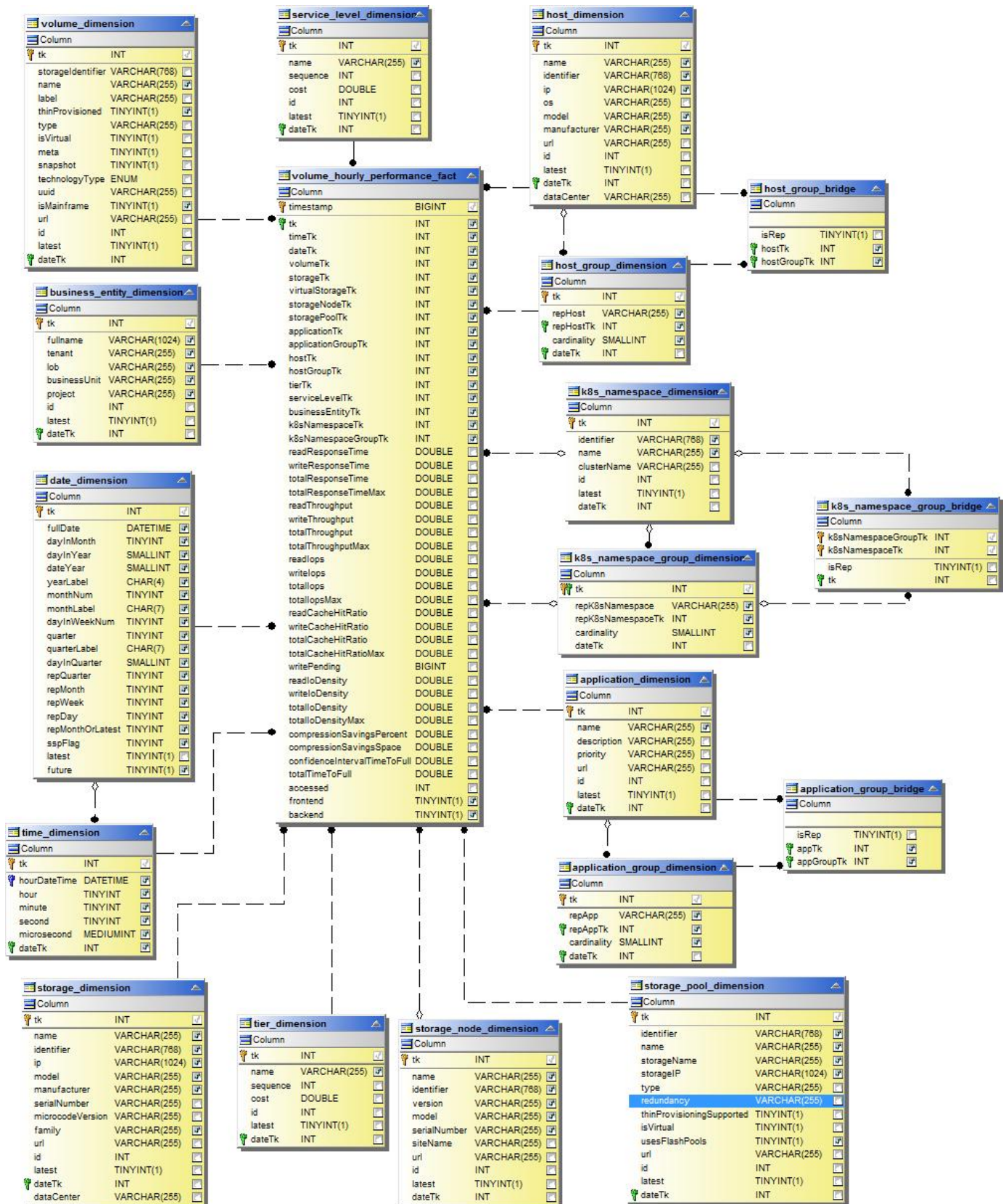
Tägliche VMDK-Leistung



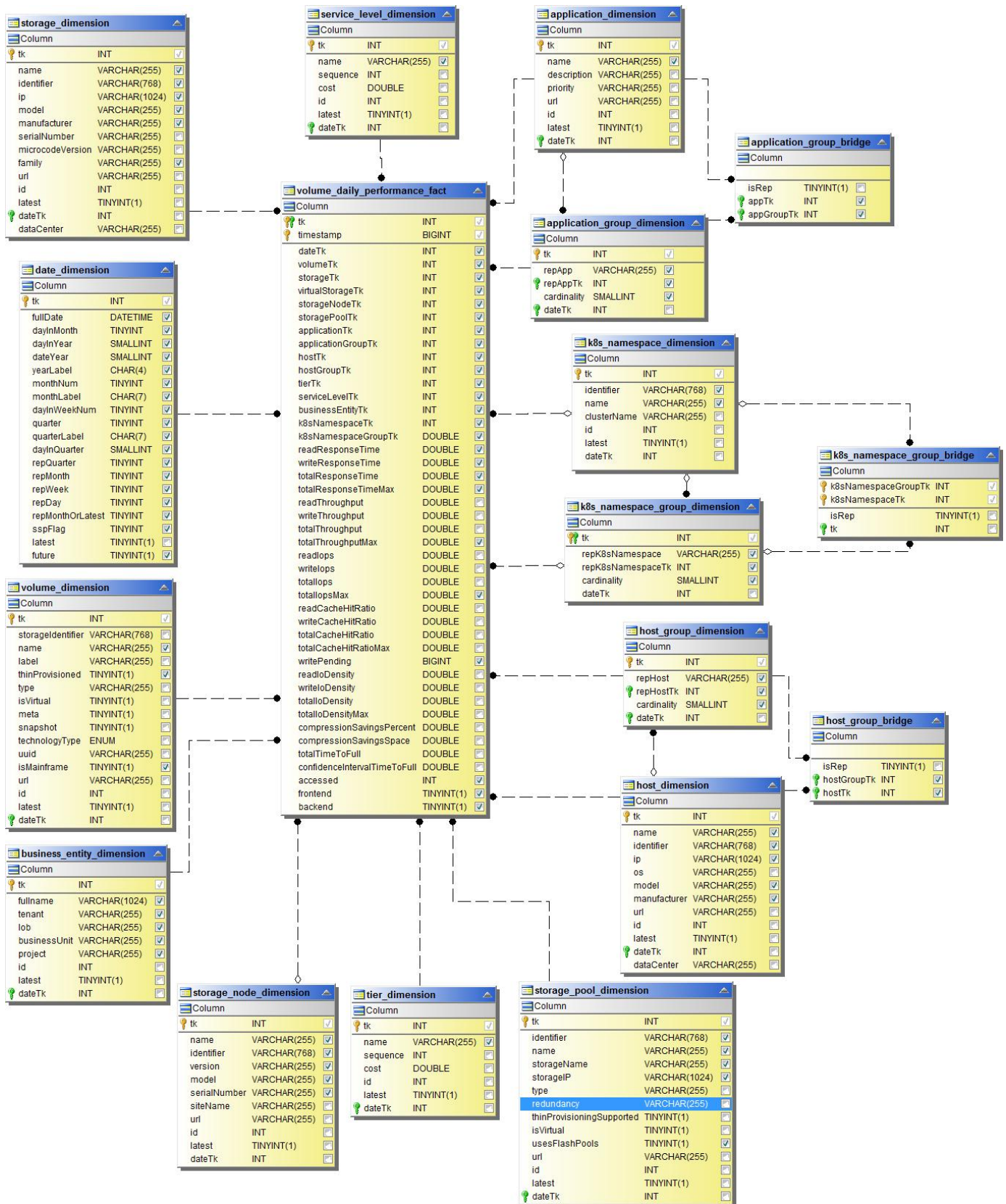
VMDK-Stundenleistung



Volumen Stündliche Leistung



Volumen Tägliche Leistung



Data Infrastructure Insights Schemas für die Berichterstellung

Diese Schematabellen und Diagramme werden hier als Referenz für Data Infrastructure Insights Reporting bereitgestellt.

"**Schematabellen**" im PDF-Format. Klicken Sie zum Öffnen auf den Link oder klicken Sie mit der rechten Maustaste und wählen Sie *Speichern unter...* zum Herunterladen.

"Schemadiagramme"



Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar "**Premium Edition**".

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.