Dokumentation zu Data Infrastructure Insights

Data Infrastructure Insights

NetApp
September 26, 2024

Inhalt

Dokumentation zu Data Infrastructure Insights

NetApp Data Infrastructure Insights (ehemals Cloud Insights) ist ein Cloud-Infrastruktur-Monitoring-Tool, mit dem Sie die gesamte Infrastruktur im Blick haben. Es überwacht nicht nur alle Ressourcen, die in Public Clouds und privaten Datacentern liegen, sondern hilft auch dabei, Fehler aufzuspüren und den Ressourceneinsatz zu optimieren.

Welche Vorteile bietet mir Dateninfrastruktur Insights?

Data Infrastructure Insights ermöglicht das Monitoring in der Hybrid-Multi-Cloud, wodurch Sie Infrastruktur und Workloads vollständig beobachten können.

- Datensammler für heterogene Infrastrukturen und Workloads einschließlich Kubernetes
- Offener Telegraf-Kollektor und offene APIs für eine einfache Integration
- Umfassende Warn- und Benachrichtigungen
- Maschinelles Lernen für intelligente Erkenntnisse
- Optimierte Ressourcenauslastung
- Integrierte oder anpassbare Dashboards mit erweiterten Filtern zur Reduzierung von Anzeigerauschen bei der Beantwortung von Fragen
- Der Zustand Ihrer ONTAP Storage-Vorgänge erkennen
- Schutz Ihrer wertvollsten Geschäftsdaten – Daten – vor Ransomware oder Datenvernichtung

---

Erste Schritte

- **"Start"**Welche Vorteile bietet Dateninfrastruktur Insights?
- Ich bin angemeldet. Was mache ich nun?"Erfassen Von Daten"
  "Benutzer einrichten"
- Genial! Nächste Schritte
  "Vorbereiten Von Ressourcen: Anmerkungen"
  "Suchen der gewünschten Assets: Abfragen"
  "Anzeigen der gewünschten Daten: Dashboards"
  "Monitoring und Alarme"
  "Sicherheit Der Daten"
- Das ist tolle Sache! Ich bin bereit **"Anmeldung"**.

Neuerungen bei Dateninfrastruktur Insights

NetApp verbessert seine Produkte und Services kontinuierlich. Im Folgenden finden Sie einige der neuesten Funktionen, die in Data Infrastructure Insights (ehemals Cloud Insights) verfügbar sind.

September 2024

Einführung in die Dateninfrastruktur – ehemals Cloud Insights

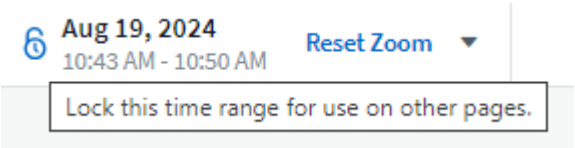
Am Dienstag, den 24. September 2024, hat NetApp den Namen Cloud Insights offiziell in **Data Infrastructure Insights** (DII) geändert. Dies wurde auf der Insight-Nutzerkonferenz von Haiyan Song in ihrer Keynote-Präsentation auf der Hauptbühne und in einer Produktpressemitteilung der Insight-Konferenz angekündigt.

Der DII-Dienst bleibt gleich; es gibt keine Änderungen oder Änderungen an den Funktionen. Dies ist eine Namensänderung, um den Namen des Service besser an seinen Möglichkeiten für die gesamte IT-Infrastruktur anzupassen.

August 2024

Anzeigen von Daten, die für Ihren Zeitbereich spezifisch sind

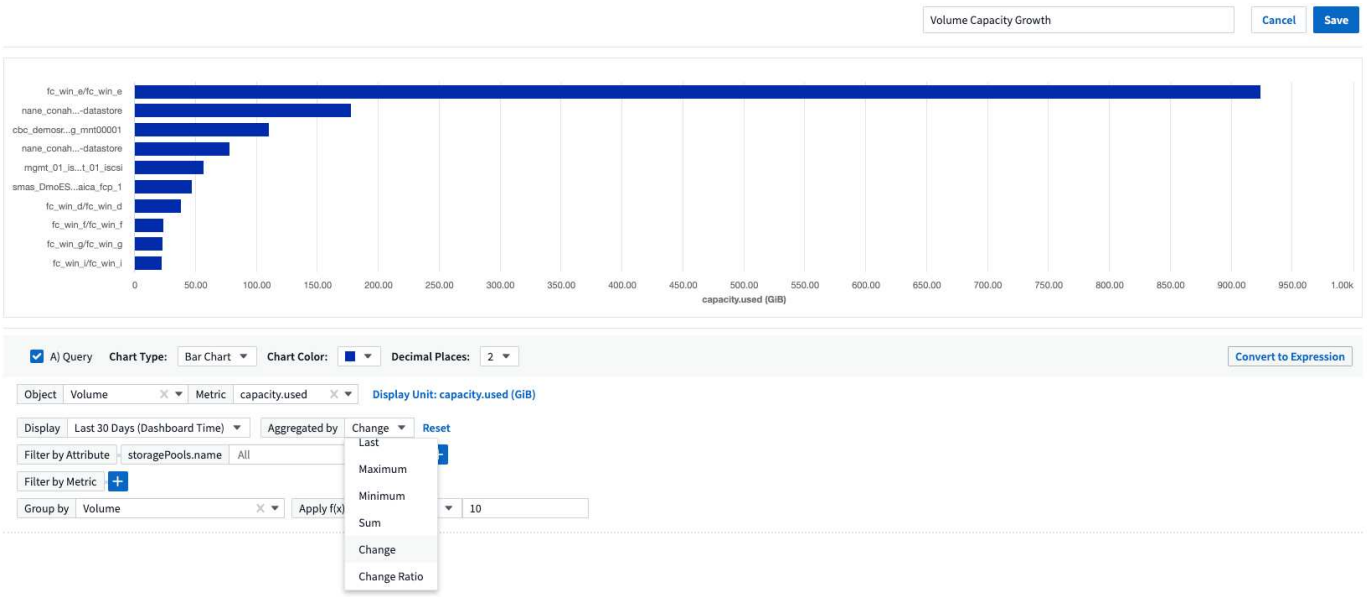
Sie suchen eine Meldung? Auf einem Diagramm vergrößert? Diese Aktionen ändern den Zeitbereich für diese Seiten. Jetzt können Sie diesen Zeitraum sperren, zu anderen Cloud Insights-Seiten navigieren und Daten anzeigen, die für diesen gesperrten Zeitraum spezifisch sind. Die Untersuchung und Fehlerbehebung ist jetzt viel einfacher!



Analyse der Änderungs- und Änderungsquote (%)

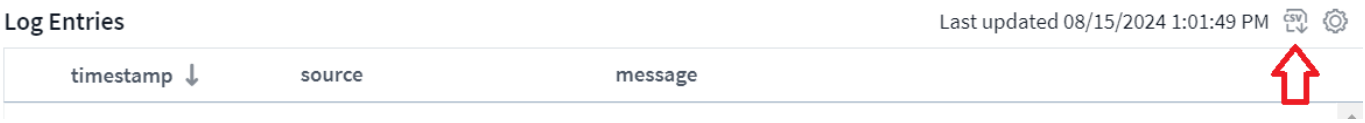
Mithilfe von Zeitaggregationen für das Change-Ratio können Sie signifikante Änderungen und Trends in metrischen Werten im Laufe der Zeit erkennen. Diese Erkenntnisse sind der Schlüssel zum Verständnis der Veränderungen, wie zum Beispiel ein beträchtliches Kapazitätswachstum für einen bestimmten Zeitraum oder eine Änderung der Leistung eines einzelnen Ports.

- **Änderung** - Beobachten Sie die Änderung in einer Metrik zwischen zwei Punkten innerhalb eines ausgewählten Zeitraums.
- **Veränderungsverhältnis** - Beobachten Sie die proportionale Veränderung in einer Metrik zwischen zwei Punkten, bezogen auf den Anfangspunkt, innerhalb eines ausgewählten Zeitraums.



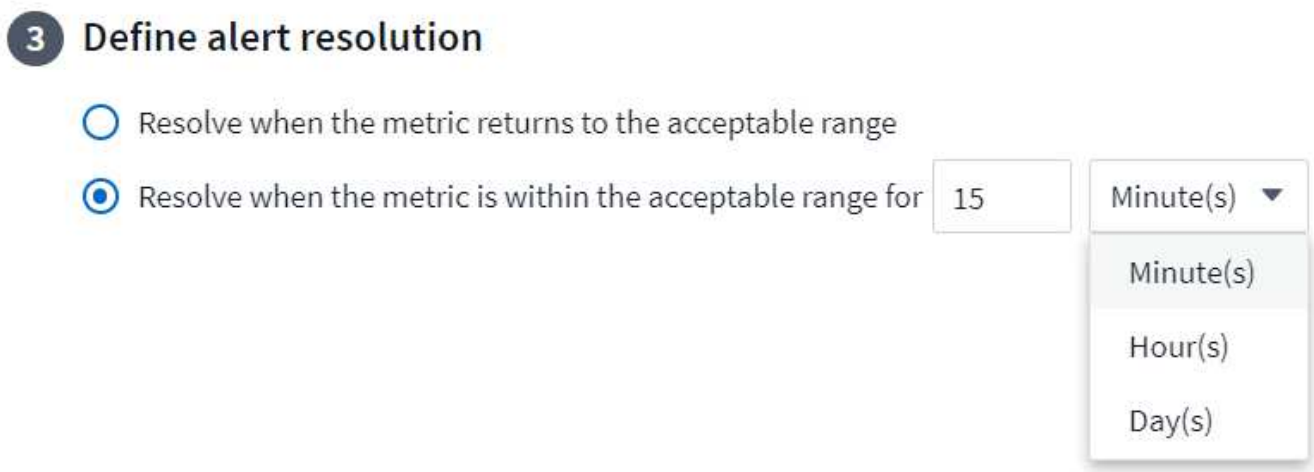
Protokollabfrageergebnisse in .CSV exportieren

Beim Anzeigen der Protokollabfrageergebnisse können Sie problemlos bis zu 10,000 Zeilen in .CSV exportieren, indem Sie auf die neue Schaltfläche „Exportieren“ klicken. Auf diese Weise wird die Datenverfügbarkeit verbessert, die Datenanalyse und die Berichterstellung vereinfacht und die nahtlose Integration in andere Data Processing-Tools ermöglicht.



Lösen Sie Warnmeldungen nach Zeit

Mit Cloud Insights haben Sie jetzt die Möglichkeit, eine Warnmeldung zu beheben, wenn die überwachte Kennzahl für einen bestimmten Zeitraum im zulässigen Bereich bleibt. So können Sie sich auf echte Probleme konzentrieren und die Störungen reduzieren, die mit der wiederholten Überschreitung definierter Schwellenwerte durch die Konsolidierung mehrerer Warnmeldungen zu einem verbunden sind.



Juli 2024

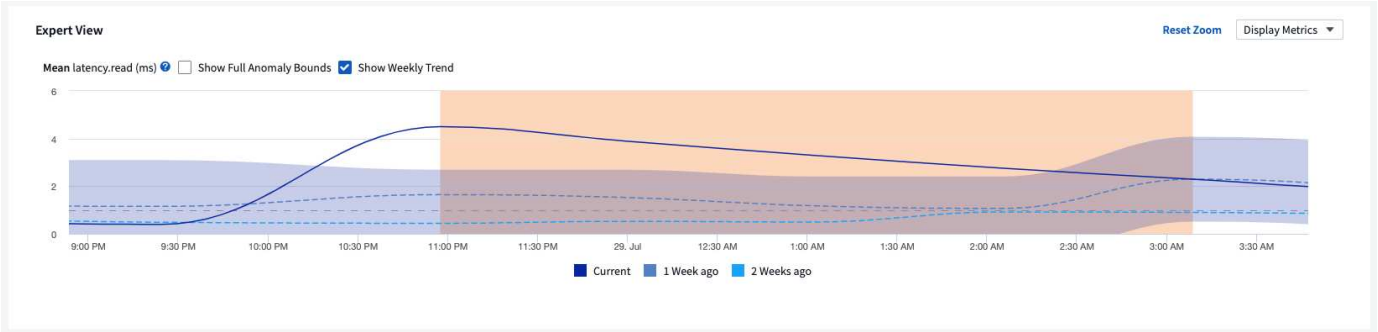
AIOPs: Anomalieerkennung

Cloud Insights nutzt Machine Learning, um unerwartete Änderungen in den Datenmustern in einer Kundenumgebung zu erkennen und proaktive Warnmeldungen zu erstellen, damit Probleme frühzeitig erkannt werden.

Ein Rechenzentrum verhält sich zu verschiedenen Tageszeiten und an verschiedenen Wochentagen unterschiedlich. Cloud Insights verwendet wöchentliche Saisonabhängigkeit, um das historische Verhalten für jeden Tag und jede Uhrzeit zu vergleichen.

Überwachung der Anomalieerkennung kann Warnungen für Situationen bereitstellen, z. B. wenn die Definition von „normal“ unklar ist, wenn sich das Verhalten im Laufe der Zeit ändert oder wenn mit großen Datenmengen gearbeitet wird, bei denen die manuelle Festlegung von Schwellenwerten unpraktisch ist.

Neue "Überwachung Der Anomalieerkennung" Warnmeldung bei Anomalien wie dieser bei ausgewählten Objektkennzahlen.



Verbesserungen Bei Der Workload-Sicherheit

Unterstützung für NFS 4.1

Der SVM Data Collector unterstützt jetzt NFS-Versionen bis einschließlich **NFS 4.1** mit ONTAP 9.15.1 oder höher.

Neue Forensics Activity API

Die forensische Aktivität "API" hat eine neue Version. Wenn Sie die API für Forensics Activity aufrufen, verwenden Sie die API **cloudSecure_forensics.activities.*v2***.

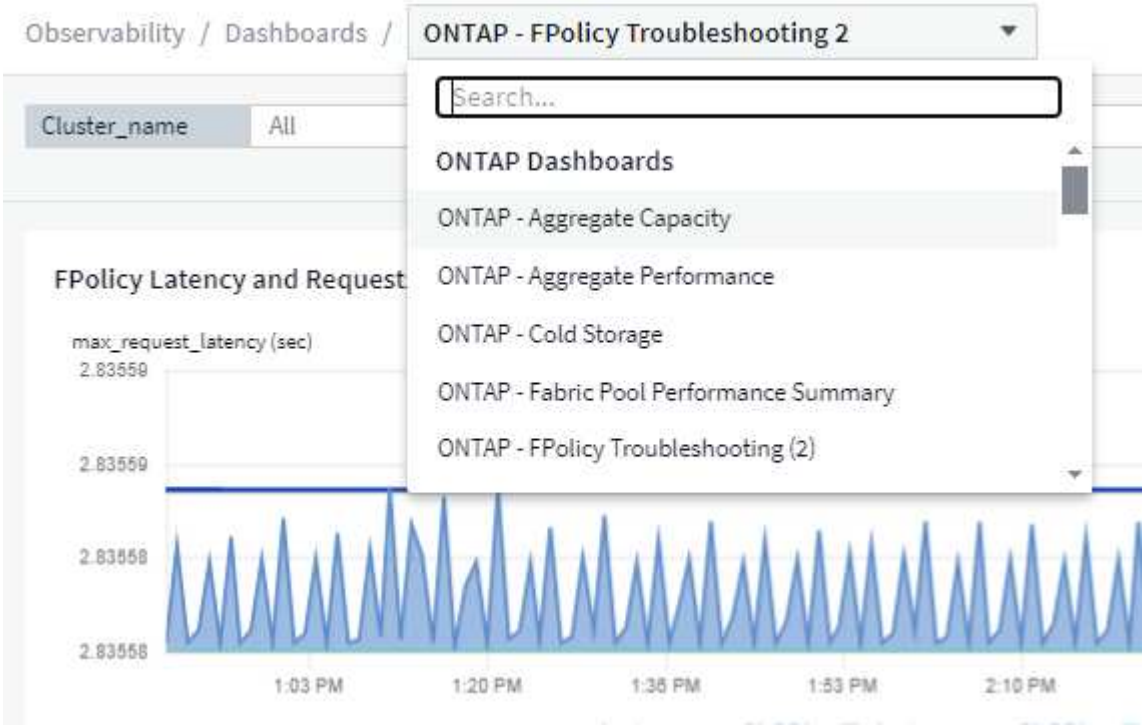
Wenn Sie mehrere Aufrufe an dieser API durchführen, stellen Sie für optimale Ergebnisse sicher, dass die Aufrufe nacheinander statt parallel stattfinden. Mehrere parallele Aufrufe können dazu führen, dass die API-Zeit abgeht.

Einfachere Dashboard-Navigation

Mit dieser Funktion wollen Sie Ihre betrieblichen Workflows optimieren und die Zusammenarbeit zwischen den Teams vereinfachen.

Durch die Gruppierung Ihrer Dashboards können Sie schnell die benötigten Informationen abrufen. Mit dem neuen Navigationsmenü können Sie zwischen verschiedenen Dashboards wechseln, ohne dabei Ihren Platz zu verlieren. So können Sie Ihre Infrastruktur einfach erkunden und managen. Richten Sie Dashboard-

Gruppen an Ihren Runbooks aus, um Ihre Benutzererfahrung weiter zu verbessern.



Juni 2024

Betriebssystemunterstützung

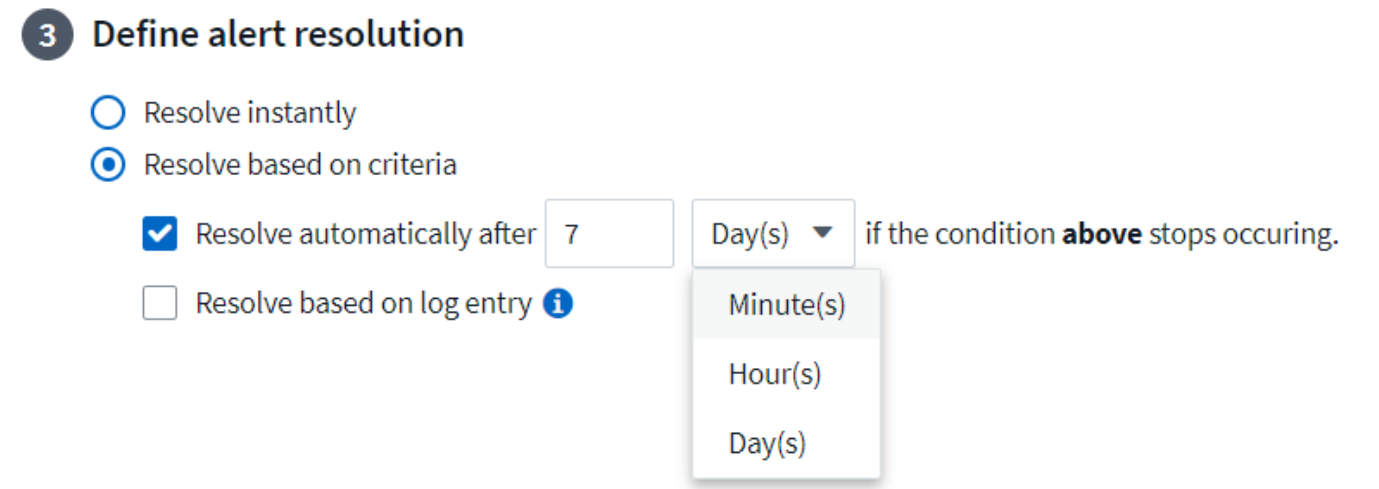
Zusätzlich zu diesen werden die folgenden Betriebssysteme mit Cloud Insights Acquisition Units unterstützt "Unterstützung bereits vorhanden":

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- Rocky 9.4
- AlmaLinux 9.3 und 9.4

Mai 2024

Automatische Problemlösung nach Zeitbasis

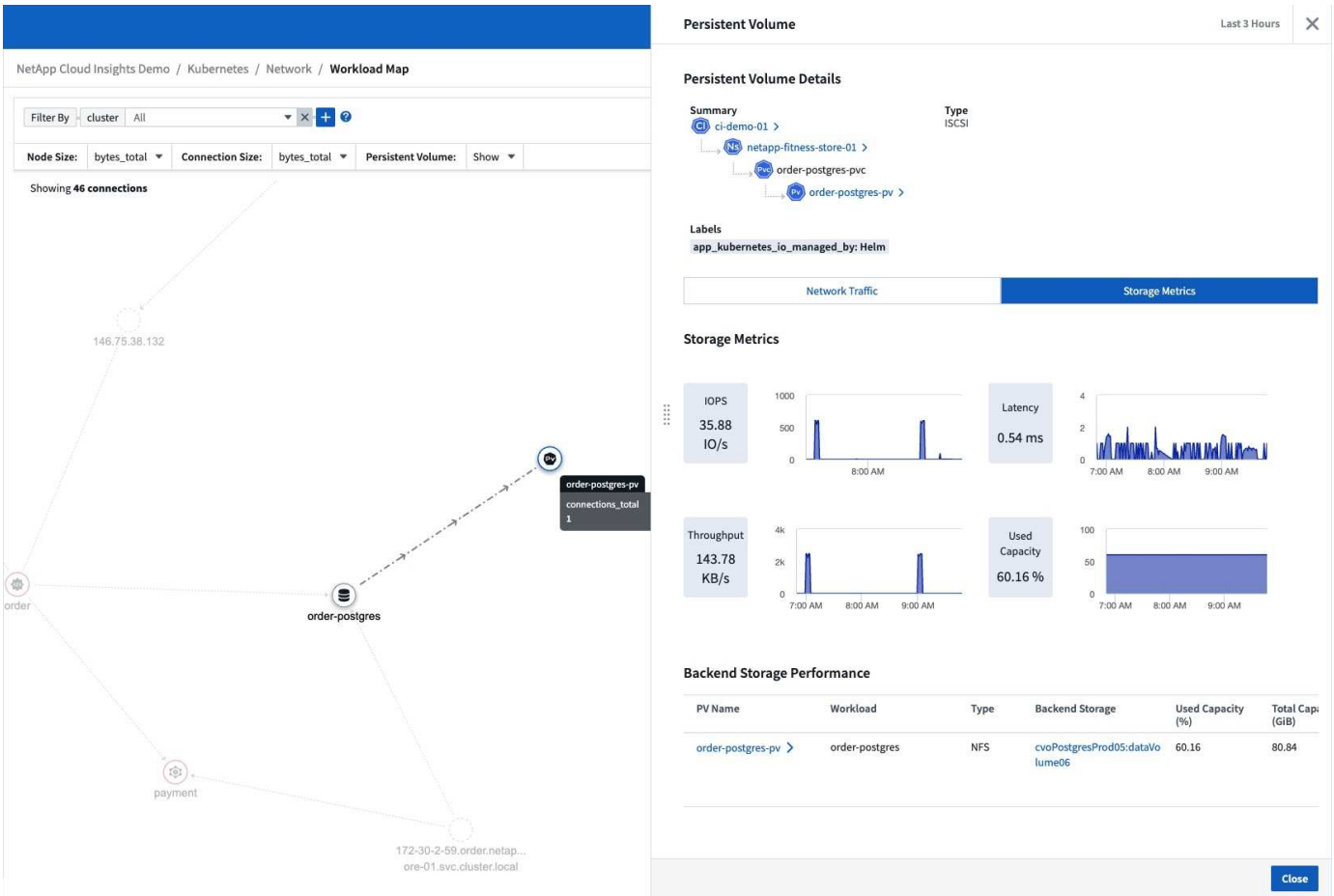
Protokollwarnungen können nun basierend auf der Zeit gelöst werden. Wenn die Alarmsituation nicht mehr auftritt, kann Cloud Insights die Warnmeldung nach Ablauf einer bestimmten Zeit automatisch beheben. Sie können die Warnmeldung in Minuten, Stunden oder Tagen beheben.



April 2024

ISCSI-Unterstützung für Kubernetes

Cloud Insights unterstützt jetzt die Zuordnung des iSCSI-Storage zu Kubernetes. Dadurch lässt sich eine schnellere Fehlerbehebung mithilfe der Kubernetes-Netzwerkzuordnung erreichen und es können Berichte zur Kostenverrechnung und Anzeige über Berichte erstellt werden.



Betriebssystemunterstützung

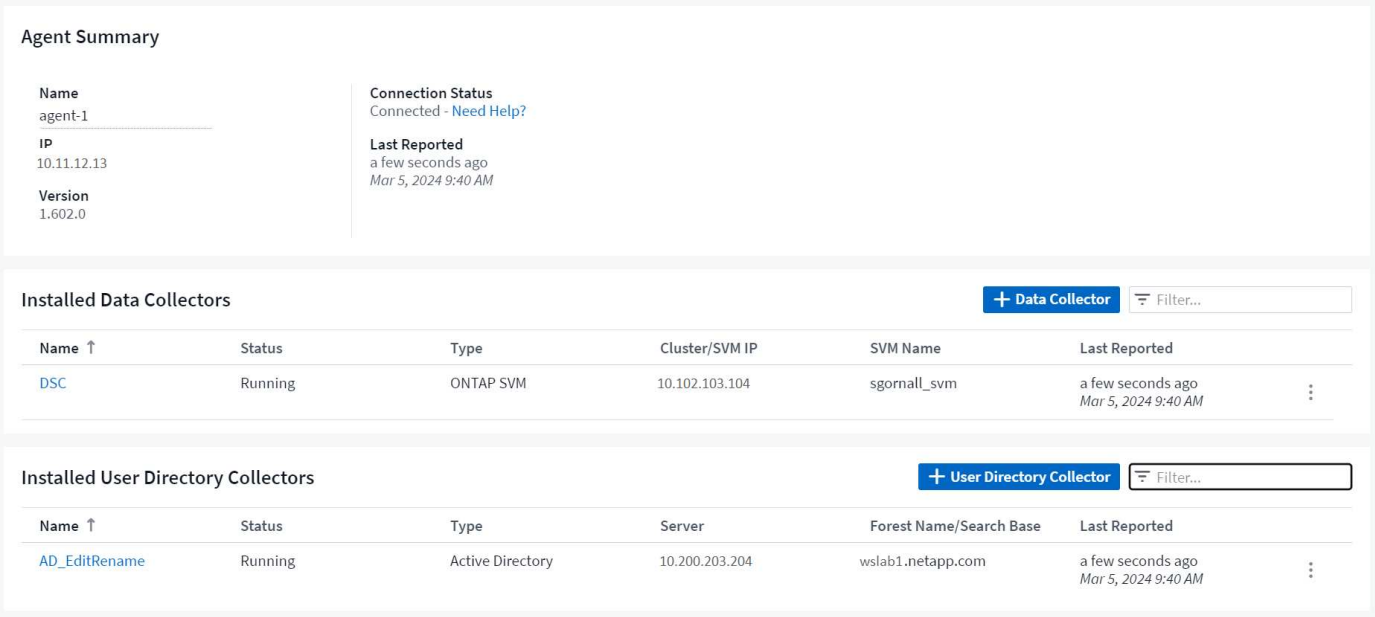
Zusätzlich zu diesen werden die folgenden Betriebssysteme mit Cloud Insights Acquisition Units unterstützt "Unterstützung bereits vorhanden":

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- Rocky 9.3
- OpenSUSE Leap 15.1 bis 15.5
- SUSE Enterprise Linux Server 15, 15 SP2 bis 15 SP5

März 2024

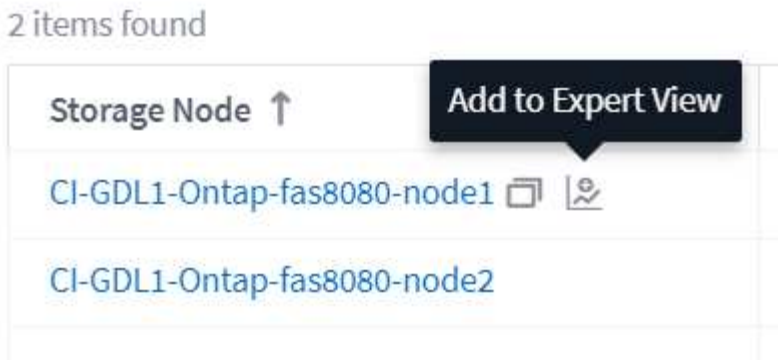
Details Zum Workload Security Agent

Jeder Ihrer Workload Security Agents verfügt über eine eigene Landing Page, auf der Sie leicht zusammenfassende Informationen über den Agenten sowie die mit diesem Agent verbundenen installierten Daten- und Benutzerverzeichnissammler sehen können.

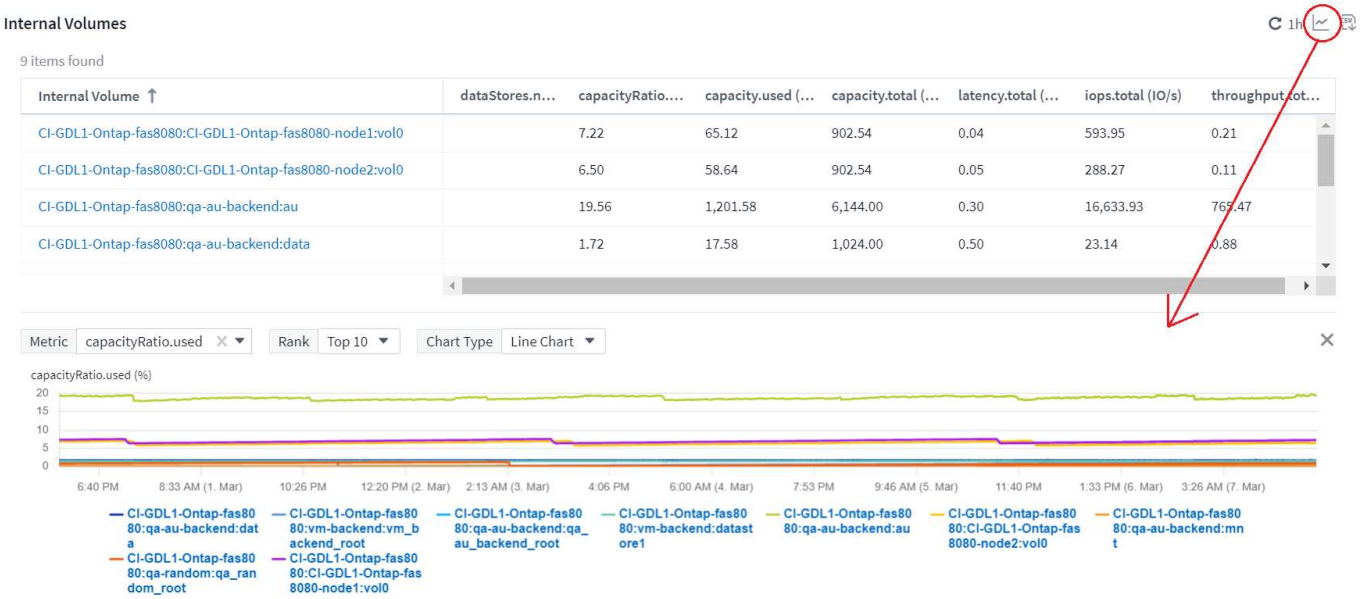


Schneller mehr Daten darstellen

Beim Analysieren von Daten auf der Landing Page eines Assets ist das Hinzufügen zusätzlicher Daten zu den Diagrammen der Expert View ein Kinderspiel. Wenn ein Objekttyp über relevante Daten verfügt, bewegen Sie den Mauszeiger für jede Tabelle auf der Landing Page über dieses Objekt, um das Symbol „zur Expertenansicht hinzufügen“ anzuzeigen. Durch Auswahl dieses Symbols wird das Objekt zu den zusätzlichen Ressourcen hinzugefügt und in den Diagrammen der Expertenansicht angezeigt.



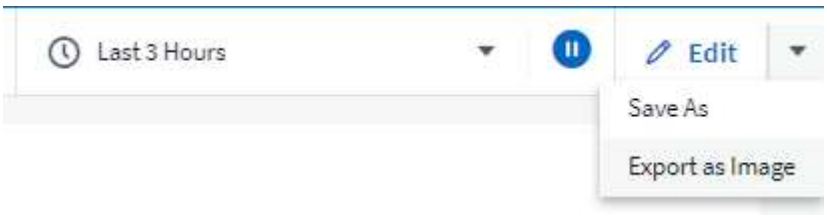
Oder vielleicht möchten Sie die Daten einer Landing Page-Tabelle in einem eigenen Diagramm sehen. Wählen Sie einfach das *Diagramm anzeigen* -Symbol, um das Diagramm unter der Tabelle zu öffnen:



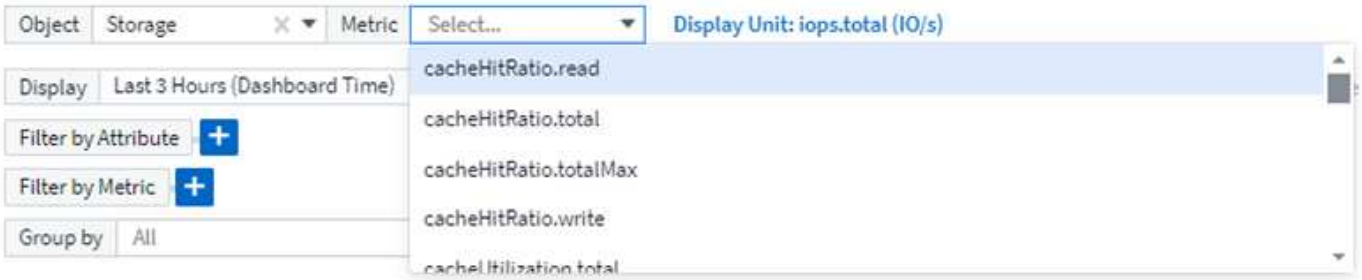
Februar 2024

Höhere Benutzerfreundlichkeit

Speichern Sie einen **Snapshot** Ihres aktuellen Dashboards, indem Sie in der Dropdown-Liste rechts *als Bild exportieren* auswählen. Cloud Insights erstellt eine .PNG-Datei der aktuellen Widget-Status.

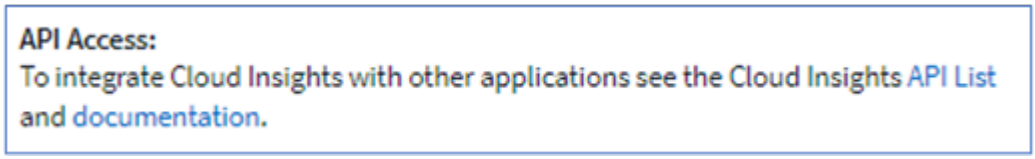


Objekt- und Metrikauswahl ist einfacher denn je für Widgets, Monitore, etc. Wählen Sie den gewünschten Objekttyp aus, und wählen Sie dann im separaten Dropdown-Menü eine für dieses Objekt relevante Metrik aus.



Export Data Collector and Acquisition Unit listet auf .CSV durch Auswahl des Symbols am oberen Rand dieser Seiten.

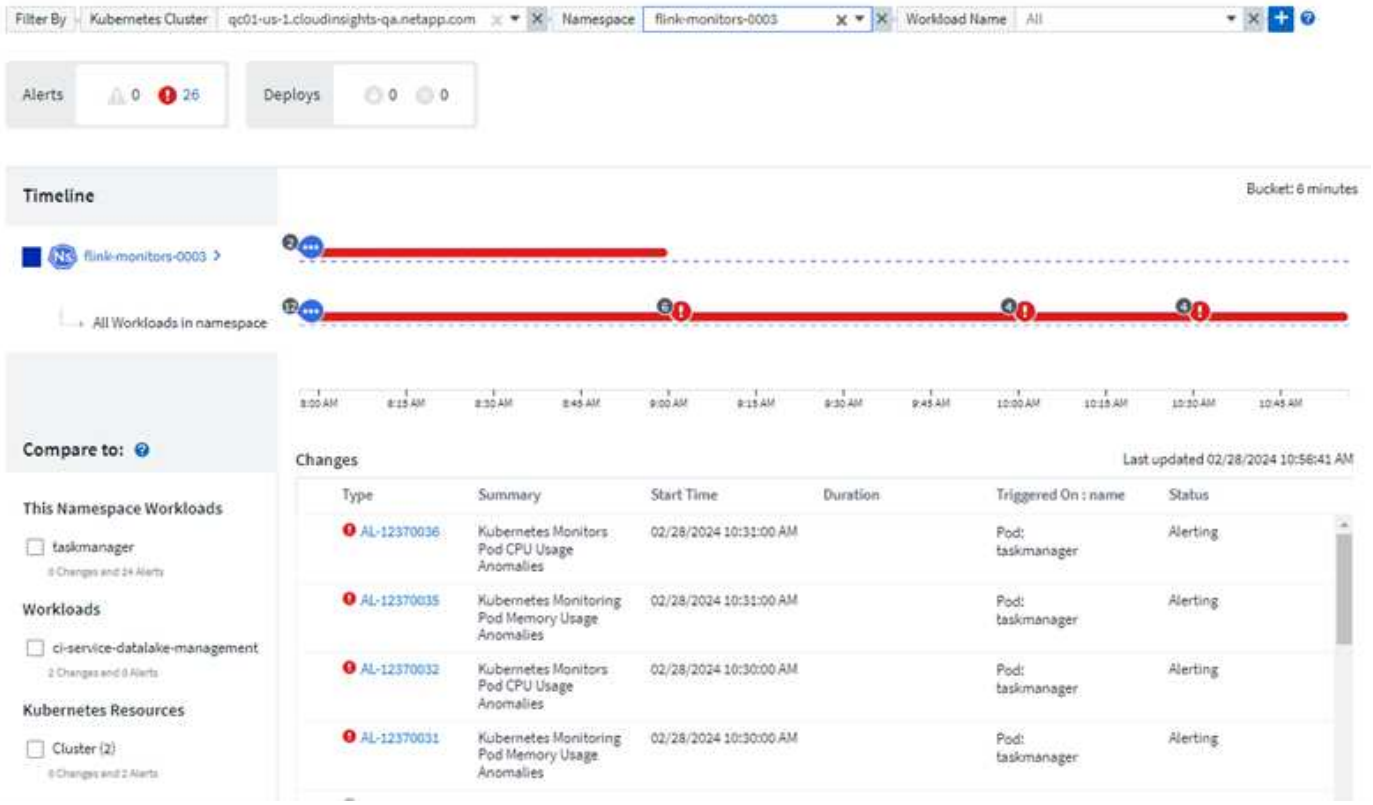
Wir haben die Hilfe > Support* Seite neu organisiert, damit es einfacher ist, das zu finden, wonach Sie suchen, und weil Sie danach gefragt haben, haben wir auf dieser Seite direkte Links zu **API Swagger** und Benutzerdokumentation hinzugefügt.



Links in der Spalte „triggeredOn“ auf der Seite Alerts list wird zur entsprechenden Landing Page navigieren, sofern für dieses Objekt eine Landing Page verfügbar ist.

Sehen Sie alle Änderungen in Ihrem Namespace

Mit der Kubernetes-Änderungsanalyse können Sie jetzt einen Überblick über die Änderungen bei der Auswahl von Cluster und Namespace erhalten. Zuvor muss auch Workload ausgewählt worden sein. Beim Filtern nach Cluster und Namespace wird die Chronik aller Workload-Änderungen in diesem Namespace auf einer Zeile angezeigt.



Verwandte Protokolle für Warnmeldungen

Beim Anzeigen einer Protokollwarnung werden die zugehörigen Protokolleinträge in einer neuen Tabelle angezeigt. Ein Protokolleintrag hängt zusammen, wenn er in derselben Quelle und demselben Zeitrahmen wie die Warnmeldung auftritt, und unterliegt denselben Bedingungen. Wählen Sie „Protokolle analysieren“, um weitere Informationen zu erhalten.

ONTAP-Switch-Daten erfassen

Cloud Insights kann Daten von den Back-End-Switches des ONTAP Systems erfassen; aktivieren Sie einfach die Erfassung im Abschnitt „*Advanced Configuration* “ des Datensammlers und stellen Sie sicher, dass das ONTAP-System so konfiguriert ist, dass es bereitgestellt wird "Switch-Informationen" Und hat das entsprechende "Berechtigungen" Einstellen.

Workload Security Data Collector API

In großen Umgebungen können Sie die Erstellung von Workload Security Collectors mithilfe der neuen Data Collectors API automatisieren. Navigieren Sie zu **Admin > API Access > API Documentation**, und wählen

Sie den API-Typ *Workload Security* aus, um weitere Informationen zu erhalten.

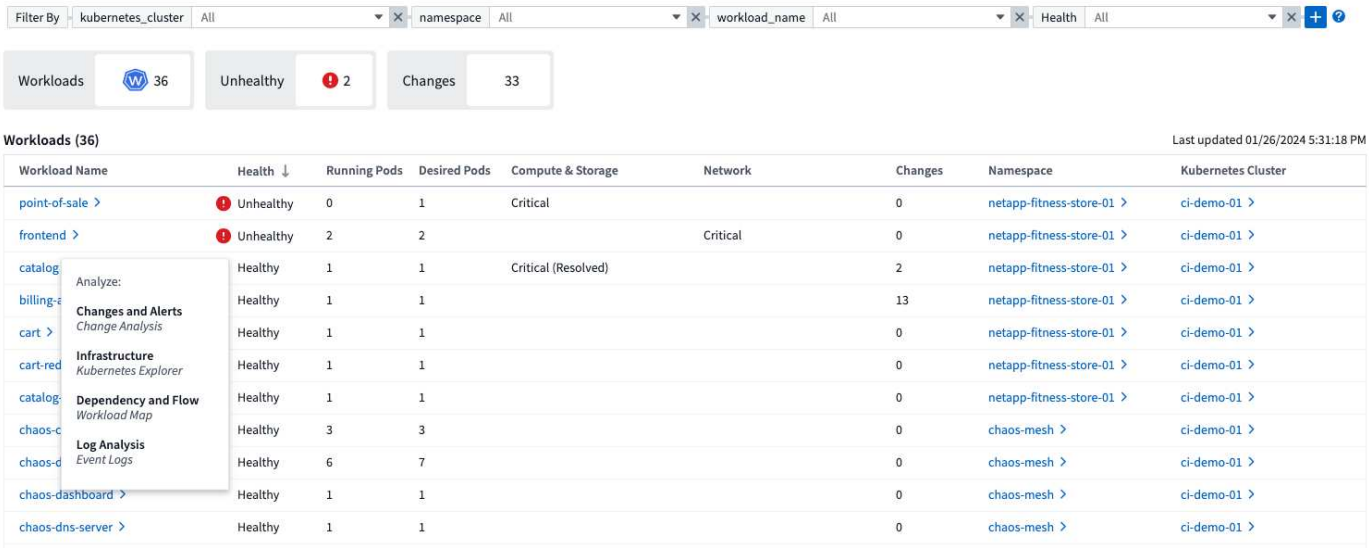
Januar 2024

Testen Sie die Cloud Insights Funktionen, die Sie noch nicht verwendet haben

Zusätzlich zu Ihrer ersten Testversion von Cloud Insights können Sie von diesen Funktionen profitieren "Modulbewertungen". Wenn Sie beispielsweise Cloud Insights abonniert haben und schon Storage und Virtual Machines überwacht haben, können Sie, wenn Sie Ihrer Umgebung Kubernetes hinzufügen, automatisch eine 30-Tage-Testversion von Kubernetes Observability starten. Die Nutzung der gemanagten Kubernetes Observability-Einheit wird erst nach Ende des Testzeitraums mit Ihren abonnierten Berechtigungen gerechnet.

Wie gut sind meine Workloads?

Der Workload-Status ist auf der Seite **Kubernetes > Explore > Workloads** auf einen Blick verfügbar. So können Sie schnell erkennen, welche Workloads eine gute Performance aufweisen und welche Unterstützung benötigen. Erkennen Sie auf einfache Weise, ob das Integritätsproblem mit Infrastruktur-, Netzwerk- oder Konfigurationsänderungen zusammenhängt, und analysieren Sie die Ursache im Detail.



Updates Für Data Collector

Data Domain-Identifizierung

Der Data Domain Collector wurde verbessert, um HA-Systeme für die Haltbarkeit bei Failover-Ereignissen besser zu identifizieren. Diese Änderung führt zu einer * einmaligen * Neuidentifikation von Data Domain-Appliances in HA-Systemen, was in der Folge dazu führt, dass alle Anmerkungen zu diesen Assets entfernt werden (da diese Arrays neu identifiziert werden). Sie müssen Anmerkungen erneut an Ihre Data Domain-Objekte anhängen.

Verbesserter ML-Algorithmus zur Erkennung von Ransomware

Workload Security umfasst einen neuen ML-Algorithmus zur Ransomware-Erkennung der zweiten Generation, der die anspruchsvollsten Angriffe schneller und exakter erkennt.

„Saisonalität“ von Verhaltensweisen: Das Verhalten am Wochenende kann sich an verschiedenen Mustern des Wochentags oder des morgendlichen Verhaltens vom Nachmittag anpassen. Bei Workload-Sicherheits-Algorithmen wird diese Saisonabhängigkeit berücksichtigt.

Veraltete Funktionalität

Gelegentlich ist die Funktionalität veraltet, wenn sich Funktionen entwickeln. Hier sind einige der Features und Funktionalitäten, die in Cloud Insights veraltet sind:

Workload Secure REST cloudSecure_forensics.activities.v1 API ist veraltet

Die *cloudSecure_forensics.activities.v1* API ist veraltet. Diese API gibt Informationen zu Aktivitäten zurück, die mit Entitäten in der Storage Workload Security-Umgebung verknüpft sind. Diese API wurde durch cloudSecure_forensics.activities ersetzt.*v2*_.

GET für diese API hat zuvor Folgendes zurückgegeben:

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

Diese API gibt jetzt Folgendes zurück:

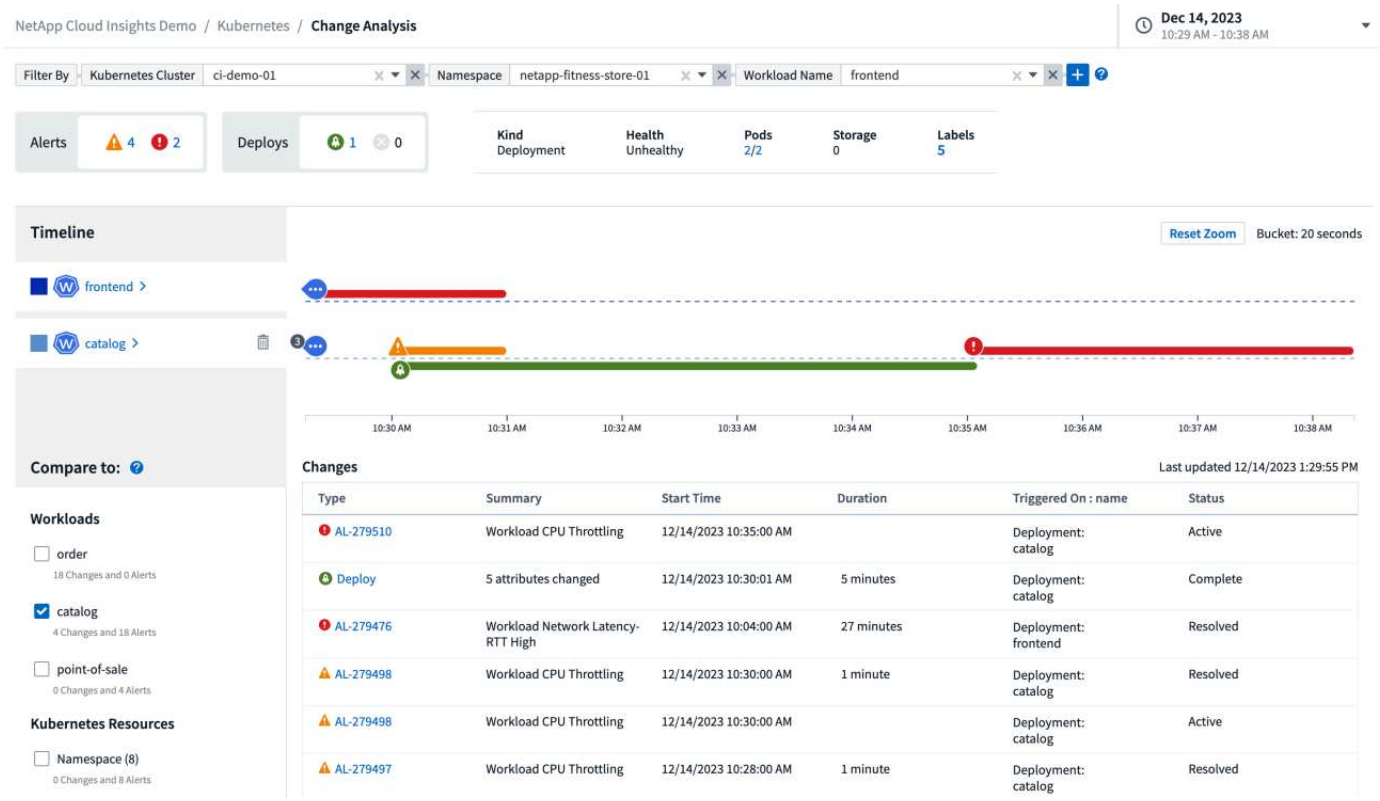
```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

Weitere Informationen finden Sie in der Dokumentation von Swagger unter „Admin > API-Zugriff > API-Dokumentation > Workload-Sicherheit“.

Dezember 2023

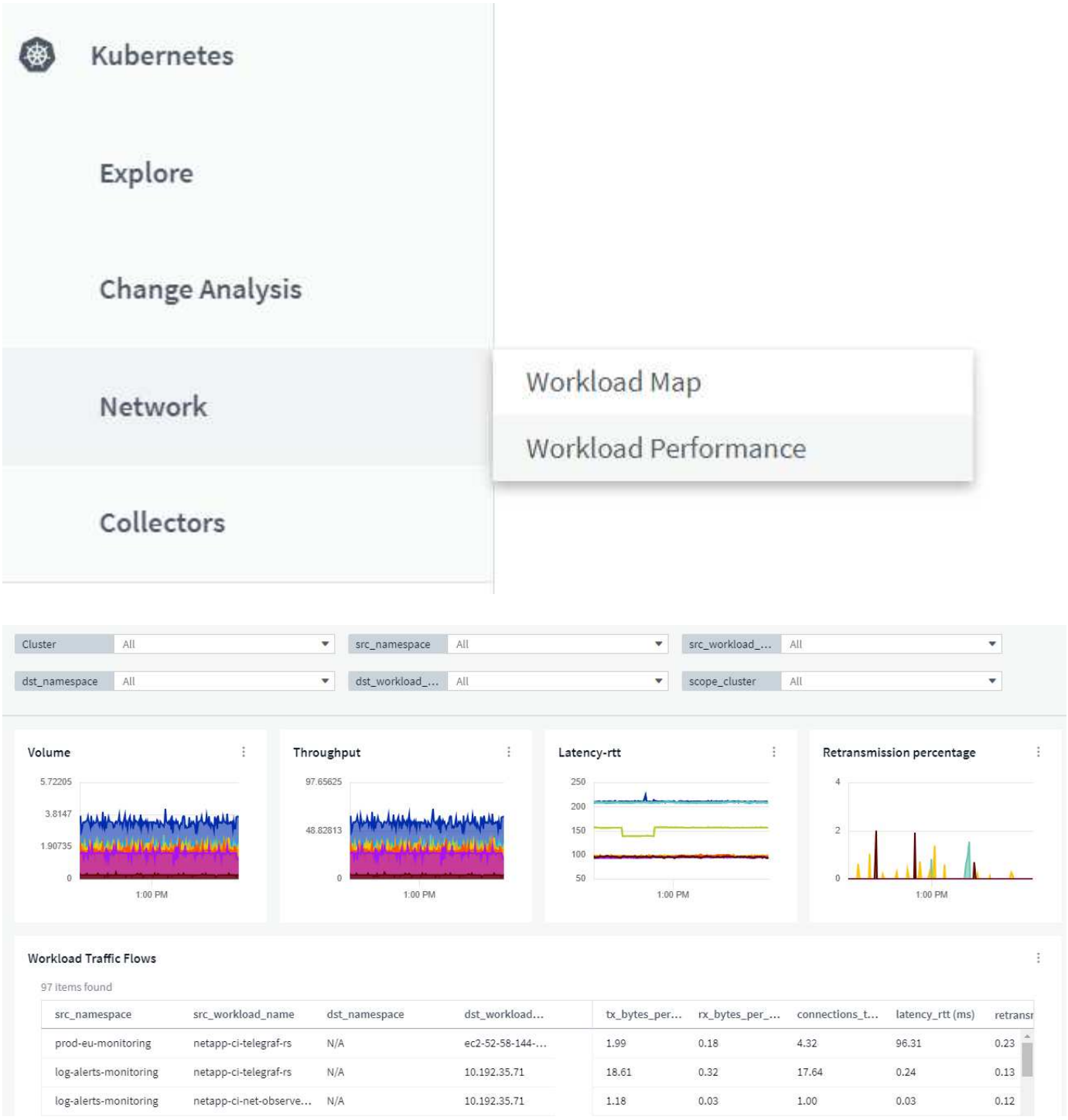
Change Analytics auf einen Blick

Kubernetes "Analyse Ändern" Sie erhalten einen All-in-One-Überblick über die neuesten Änderungen an Ihrer Kubernetes-Umgebung. Warnmeldungen und Bereitstellungsstatus stehen Ihnen jederzeit zur Verfügung. Mit Change Analytics lassen sich jede Implementierungs- und Konfigurationsänderung nachverfolgen und mit dem Zustand und der Performance von Kubernetes-Services, Infrastruktur und Clustern korrelieren.



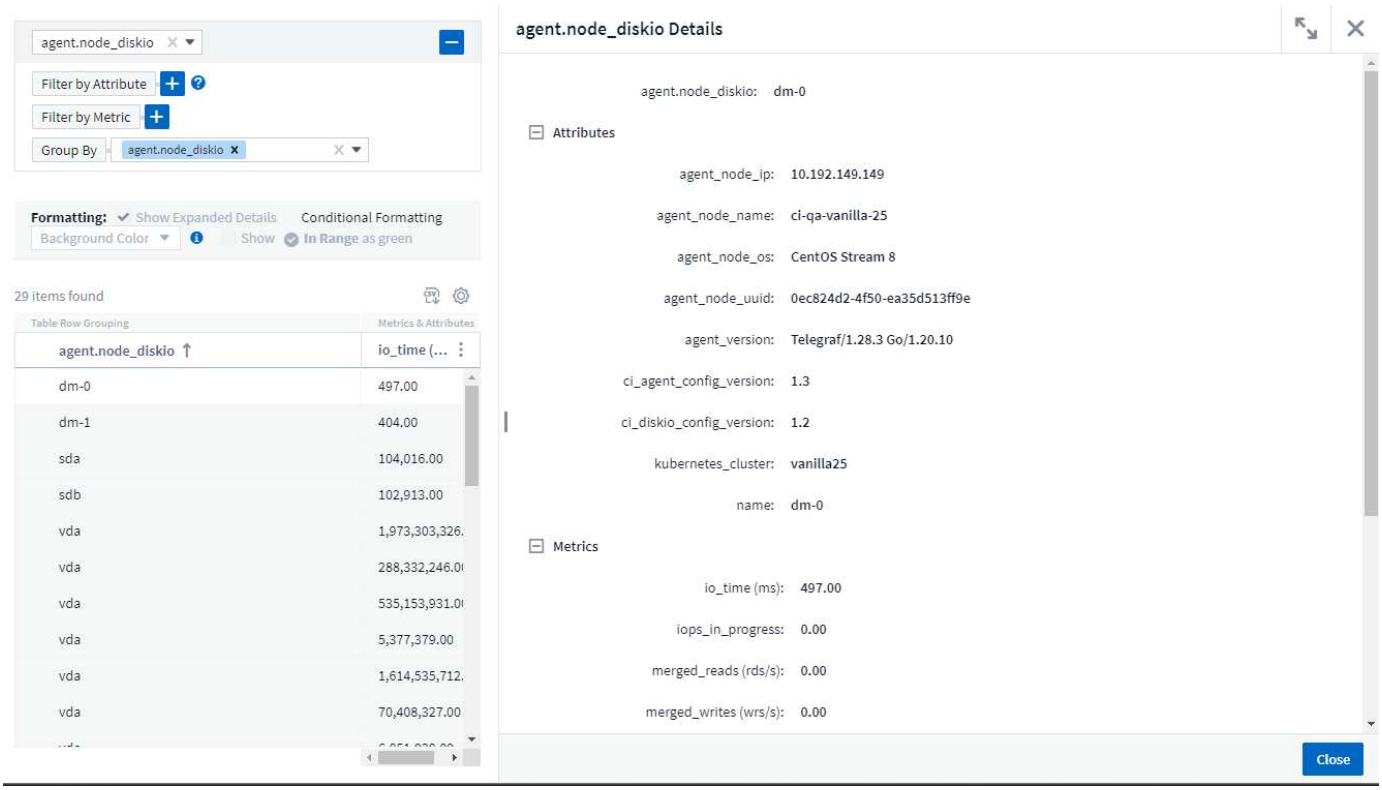
Kubernetes Workload Performance Dashboard

Die Workload-Performance ist im umfassenden Kubernetes Workload Performance Dashboard auf einen Blick verfügbar. Sehen Sie sich schnell Diagramme zu Volume-, Durchsatz-, Latenz- und Lösungstrends sowie eine Tabelle des Workload-Datenverkehrs für jeden Namespace in Ihrer Umgebung an. Filter ermöglichen eine einfache Fokussierung auf Bereiche, die von Interesse sind.



Abfragedetails auf einem Bildschirm

Wenn Sie in einer Abfrage eine Zeile auswählen, wird ein Seitenfenster geöffnet, in dem Attribut-, Anmerkungs- und Kennzahlendetails für die ausgewählte Zeile angezeigt werden. Dadurch erhalten Sie hilfreiche Informationen, ohne einen Drilldown auf die Zielseite des Objekts durchführen zu müssen. Links in der Reihe oder im Seitenbereich ermöglichen eine einfache Navigation.



Aktualisierungen des Data Collectors:

- **Brocade FOS REST**: Dieser Kollektor wird aus "Preview" entfernt und ist nun allgemein verfügbar. Einige Dinge zu beachten:
  - FOS führte seine REST API mit FOS 8.2 ein. Aber einige Funktionen wie Routing haben nur REST API-Fähigkeiten mit 9.0 erhalten.
  - Wenn Sie eine Fabric haben, die aus gemischten FOS-Assets 8.2 höher sowie einigen < 8.2 besteht, kann der Cloud Insights-FOS-REST-Collector diese älteren Assets nicht erkennen. Sie können den FOS-REST-Collector bearbeiten und eine kommagetrennte Liste der IPv4-Adresse dieser Geräte erstellen, um sie von diesem Collector auszuschließen.
- **SELinux**: Cloud Insights enthält Verbesserungen an der Erstinstallation der Linux Acquisition Unit, um die Robustheit des Betriebs in Linux-Umgebungen mit aktivierter SELinux Enforcement zu gewährleisten. Diese Verbesserungen wirken sich nur auf *New* AU-Bereitstellungen aus. Wenn Sie Probleme mit SELinux im Zusammenhang mit AU-Upgrades haben, wenden Sie sich an den NetApp-Support, um Ihre SELinux-Konfiguration zu beheben.

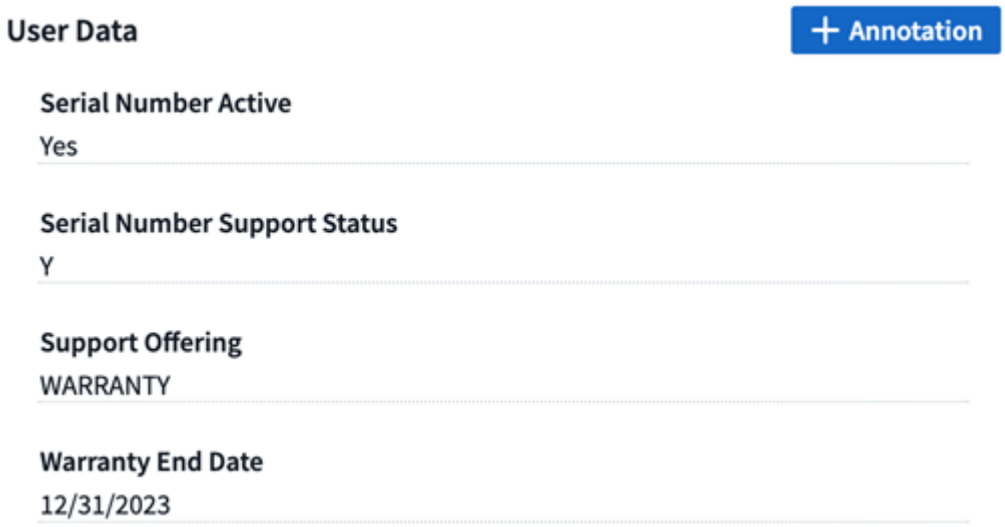
November 2023

Workload-Sicherheit: Anhalten/Fortsetzen eines Collectors

In Workload Security können Sie einen Data Collector anhalten, wenn sich der Collector im Status „*Running*“ befindet. Öffnen Sie das Menü „drei Punkte“ für den Collector und wählen Sie PAUSE. Während der Collector angehalten wird, werden keine Daten von ONTAP erfasst und keine Daten vom Collector an ONTAP gesendet. Wählen Sie Fortsetzen, um die Erfassung erneut zu starten.

Support-Informationen Zum Storage-Node

Auf einer Landing Page des Storage-Node finden Sie im Abschnitt *User Data* auf einen Blick Informationen zu Ihrem Supportangebot, dem aktuellen Status, dem Support-Status und dem Enddatum der Garantie. Beachten Sie, dass Cloud Insights diese Informationen derzeit nur automatisch für NetApp-Geräte veröffentlicht. Beachten Sie auch, dass diese Support-Felder Anmerkungen sind, sodass sie in Abfragen und Dashboards verwendet werden können.



Zuordnen von VMware-Tags zu Cloud Insights-Annotationen

Der "VMware" Mithilfe des Datensammlers können Sie Cloud Insights Textanmerkungen mit Tags mit demselben Namen ausfüllen, die auf VMware konfiguriert sind.

Verbesserungen der Brocade CLI-Collector-Zuverlässigkeit für FOS 9.1.1c und höhere Firmware

Bei einigen Brocade Fibre-Channel-Switches, auf denen die Firmware 9.1.1c ausgeführt wird, kann die Ausgabe bestimmter CLI-Befehle mit dem „motd“-Anmeldebannertext oder Warnungen für Benutzer, die Standardpasswörter ändern, vorangestellt werden. Der Brocade CLI-Collector wurde verbessert, um diese beiden Arten von überflüssigen Text zu ignorieren.

Vor dieser Verbesserung waren bei diesem Collector-Typ wahrscheinlich nur FOS 9.1.1c-Switches ohne vorhandene Virtual Fabrics erkennbar.

Oktober 2023

Verbesserte Workload-Sicherheit

Die Workload-Sicherheit wurde durch folgende Funktionen verbessert:

- **Zugriff verweigert**: Workload-Sicherheit integriert sich in ONTAP um zu empfangen "„Zugriff verweigert“-Ereignisse" Und bieten eine zusätzliche Schicht für Analysen und automatische Reaktionen.
- **Zulässige Dateitypen**: Wenn ein Ransomware-Angriff für eine bekannte Dateierweiterung erkannt wird,

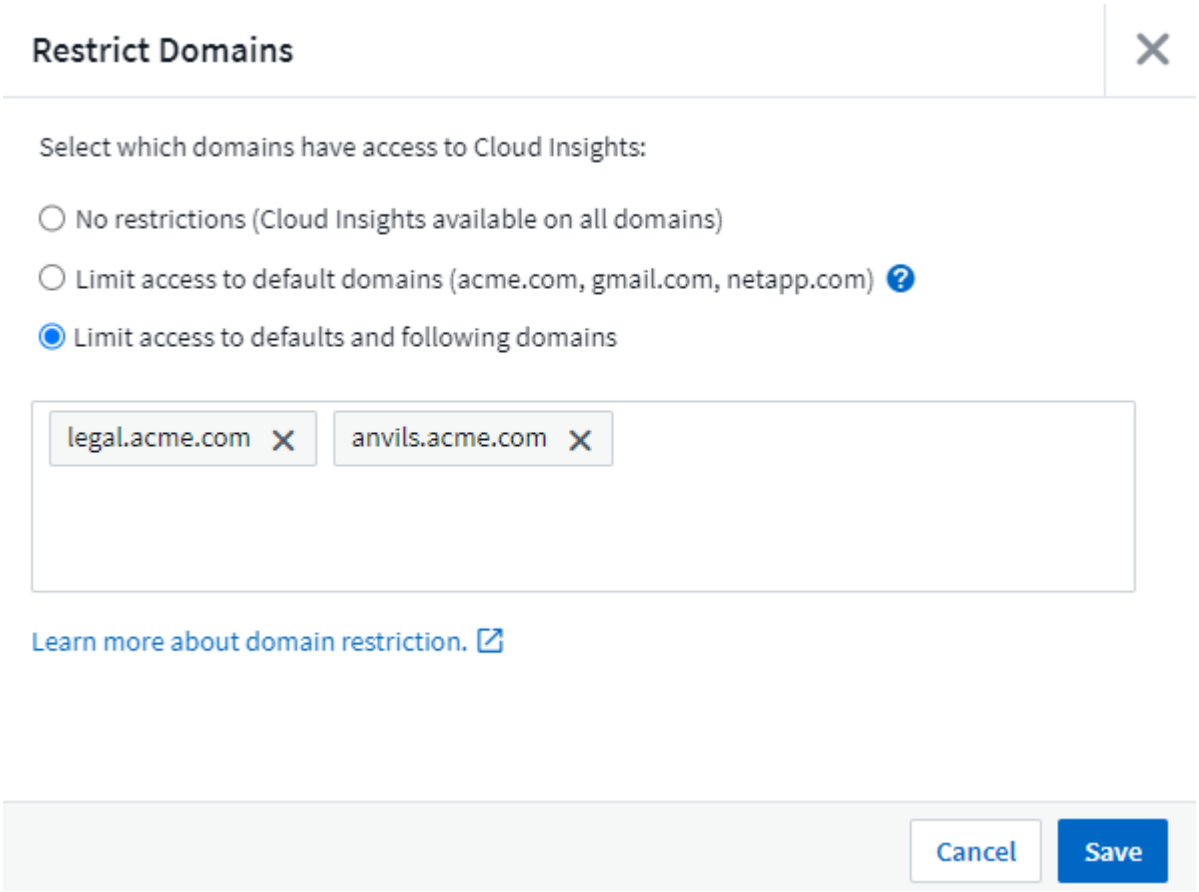
kann diese Dateierweiterung zu einem hinzugefügt werden "Zulässige Dateitypen" Liste, um unnötige Warnmeldungen zu vermeiden.

Modulversuche

Zusätzlich zu Ihrer ersten Testversion von Cloud Insights können Sie von diesen Funktionen profitieren "Modulbewertungen". Wenn Sie beispielsweise bereits Infrastruktur-Observability abonniert haben, aber Kubernetes in Ihre Umgebung integrieren möchten, können Sie automatisch für eine 30-Tage-Testversion von Kubernetes Observability starten. Ihnen wird am Ende des Evaluierungszeitraums nur die Nutzung Ihrer Kubernetes Observability-gemanagten Einheit in Rechnung gestellt.

Beschränken Sie den Zugriff auf bestimmte Domänen

Administratoren und Kontoinhaber haben jetzt die Möglichkeit, dies zu erreichen "Einschränken des Cloud Insights-Zugriffs" E-Mail-Domänen, die sie angeben. Gehen Sie zu **Admin > User Management** und wählen Sie die Schaltfläche *Domains einschränken*.



Updates Für Data Collector

Die folgenden Änderungen an der Data Collector/Acquisition Unit sind vorhanden:

- **Isilon / PowerScale REST**: Unter dem Namen *emc_isilon.node_pool.** wurden verschiedene neue Attribute und Kennzahlen zu den erweiterten Analysefunktionen von Cloud Insights hinzugefügt. Mit diesen Zählern und Attributen können Benutzer Dashboards und Monitore für den Kapazitätsverbrauch von *Node_Pool* erstellen. Benutzer mit Isilon-Clustern, die aus unterschiedlichen Hardware-Node-Modellen erstellt wurden, verfügen über mehrere Node-Pools. Das Verständnis der HDD-/SSD-/Gesamtkapazität auf Node-Pool-Ebene ist sowohl für die Überwachung als auch für die Planung von Nutzen.

- **Rubrik** "Dienstkonto" Authentifizierungsunterstützung: Cloud Insights' Rubik-Kollektor unterstützt jetzt sowohl die traditionelle HTTP-Basisauthentifizierung (Benutzername und Passwort), als auch den Dienst-Account-Ansatz von Rubrik, der einen Benutzernamen + Schlüssel + Organisations-ID erfordert.

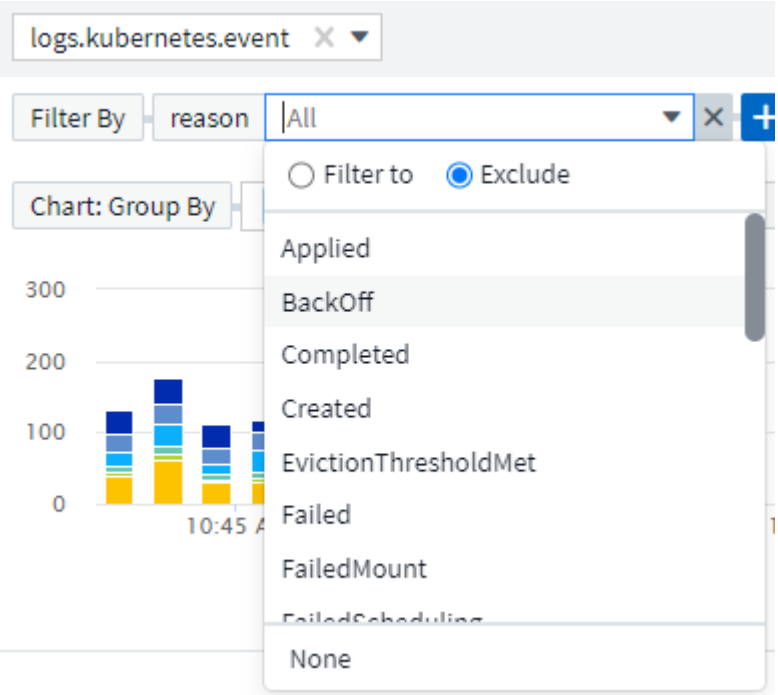
September 2023

In den Protokollen finden Sie ganz einfach, was Sie möchten

Log Query (**Observability > Log Queries > +New Log Query**) enthält eine Reihe von "Vorgestellt werden" Um die Protokollforschung einfacher und informativer zu machen.

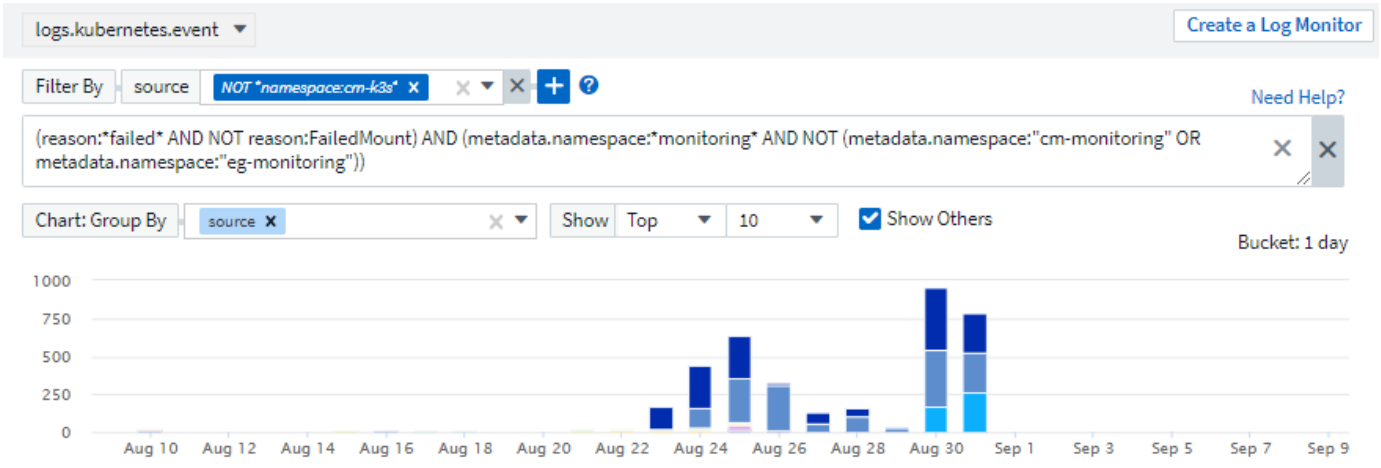
Ein-/Ausschließen

Beim Filtern nach einem Wert können Sie ganz einfach wählen, ob **include** oder **exclude** Ergebnisse dem Filter entsprechen. Durch Auswahl von „Exclude“ wird ein Filter „NOT <value>“ erstellt. Sie können die ein- und Ausschlusswerte in einem einzelnen Filter kombinieren.



Erweiterte Abfrage

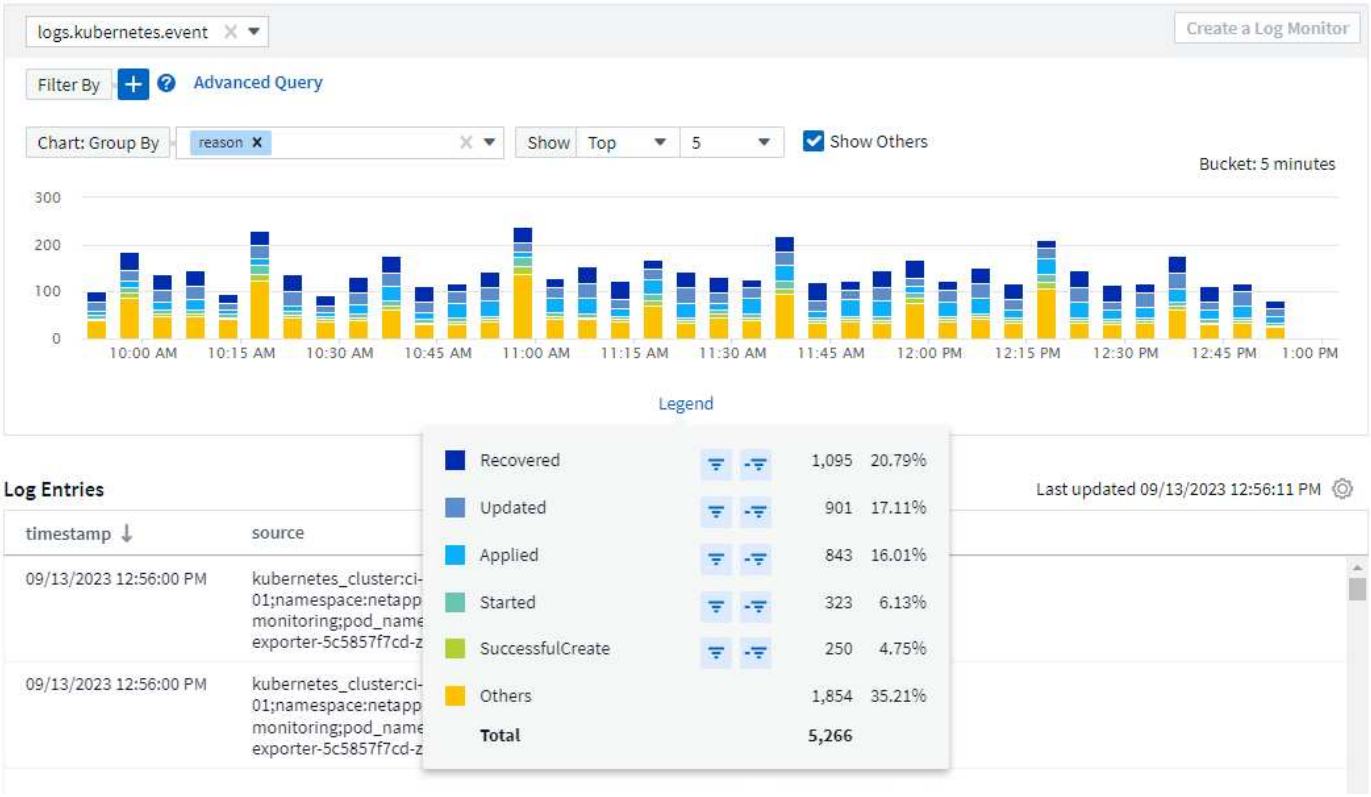
Advanced Querying gibt Ihnen die Möglichkeit, "freie Form"-Filter zu erstellen, indem Sie Werte mit AND, NOT, OR, Wildcards, etc. Kombinieren ODER ausschließen



Die Optionen „Filtern nach“ und „Erweiterte Abfrage“ werden zu einer einzigen Abfrage zusammengefasst. Die Ergebnisse werden in der Ergebnisliste und im Diagramm angezeigt.

Gruppierung im Diagramm

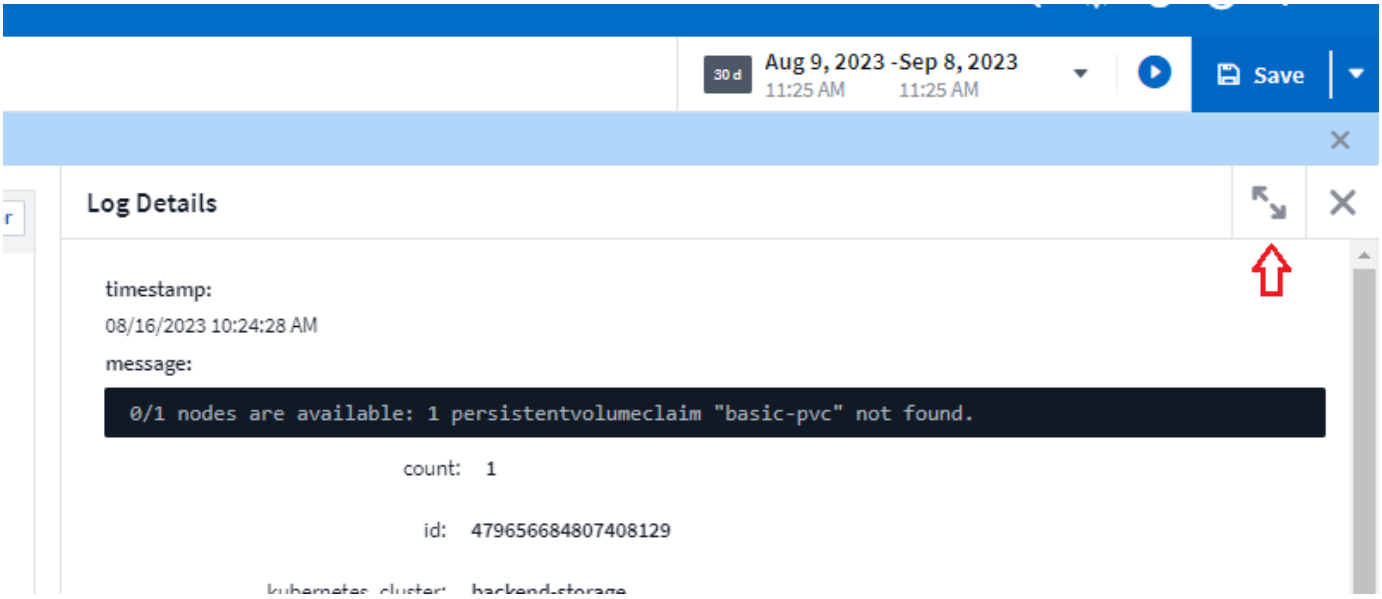
Wenn Sie ein Protokollattribut für **Gruppieren nach** auswählen, werden in der Liste und im Diagramm die Ergebnisse des aktuellen Filters angezeigt. Im Diagramm werden die Spalten in Farben gruppiert. Wenn Sie den Mauszeiger über eine Spalte im Diagramm bewegen, werden Details zu den spezifischen Einträgen angezeigt, ähnlich den allgemeinen Informationen, die beim erweitern der Diagrammlegende angezeigt werden. In der Legende können Sie auch festlegen, ob ein Filter ein- oder Ausschlussfilter für eine bestimmte Gruppierung verwendet werden soll.



Fenster „Schwebende“ Protokolldetails

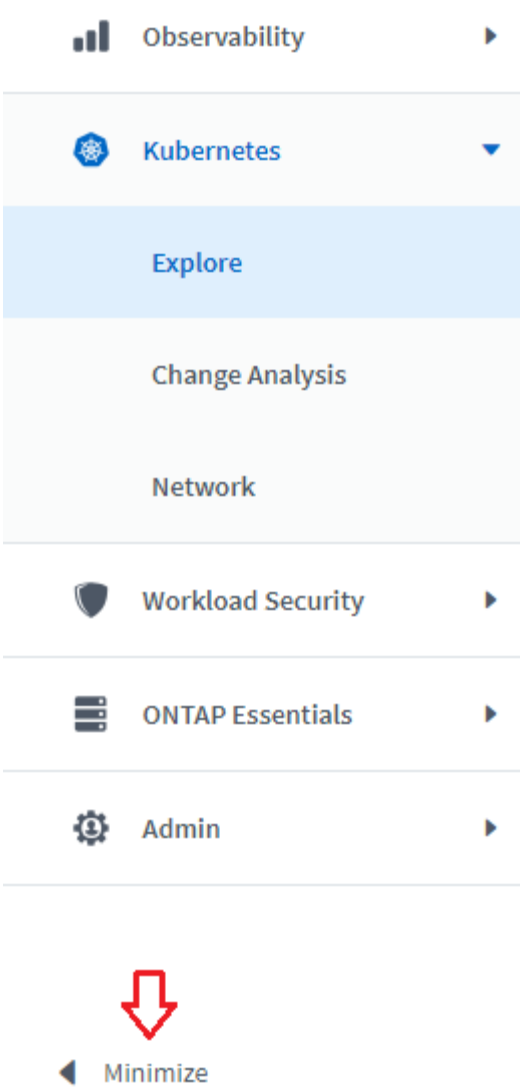
Wenn Sie Protokolle mithilfe der Protokollabfrage untersuchen, wird durch Auswahl eines Eintrags in der Liste

ein Detailfenster für diesen Eintrag geöffnet. Sie können nun wählen, ob das Schiebefenster „frei“ (d. h. über den Rest des Bildschirms angezeigt) oder „in Seite“ (d. h. als eigenen Rahmen auf der Seite angezeigt) angezeigt werden soll. Um zwischen diesen Ansichten zu wechseln, klicken Sie oben rechts im Bedienfeld auf die Schaltfläche „in Page / Floating“.



Schließen Sie das Menü ab

Sie können das linke Cloud Insights-Navigationsmenü durch Auswahl der Schaltfläche „Minimieren“ unter dem Menü ausblenden. Wenn das Menü minimiert ist, bewegen Sie den Mauszeiger über ein Symbol, um zu sehen, welcher Abschnitt geöffnet wird. Durch Auswahl des Symbols wird das Menü geöffnet und Sie gelangen direkt zu diesem Abschnitt.



Verbesserungen Des Data Collectors

Cloud Insights erleichtert das Anzeigen und Auffinden von Daten-Collector-Informationen:

- **Die Verarbeitung von Datensammlerlisten** ist effizienter, was bedeutet, dass die Zeit, die benötigt wird, um diese Listen anzuzeigen und zu navigieren, stark reduziert wird. Wenn Sie eine große Umgebung mit vielen Datensammlern haben, werden Sie eine deutliche Verbesserung bei der Auflistung Ihrer Datensammler sehen.
- Die **Data Collector Support Matrix** ist von einer .PDF-Datei auf eine .HTML-basierte Seite umgestiegen, schneller zu navigieren und einfacher zu warten. Schauen Sie sich die neue Matrix hier an: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

August 2023

Sammeln von Isilon/PowerScale-Protokollen und Advanced Analytics-Daten

Die Isilon REST- und PowerScale Rest-Collectors enthalten die folgenden Verbesserungen:

- Isilon-Protokollereignisse stehen zur Verwendung in Abfragen und Warnmeldungen zur Verfügung
- Isilon Advanced Analytic-Attribute stehen für Abfragen, Dashboards und Warnmeldungen zur Verfügung:
  - emc_isilon.Cluster
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

Diese sind standardmäßig für Benutzer der Isilon REST- und/oder PowerScale REST-Collectors aktiviert. NetApp empfiehlt Benutzern des CLI-basierten Collectors von Isilon dringend, zu dem neuen REST-API-basierten Collector zu migrieren, um Verbesserungen wie die oben genannten zu erhalten.

Verbesserte Workload-Map

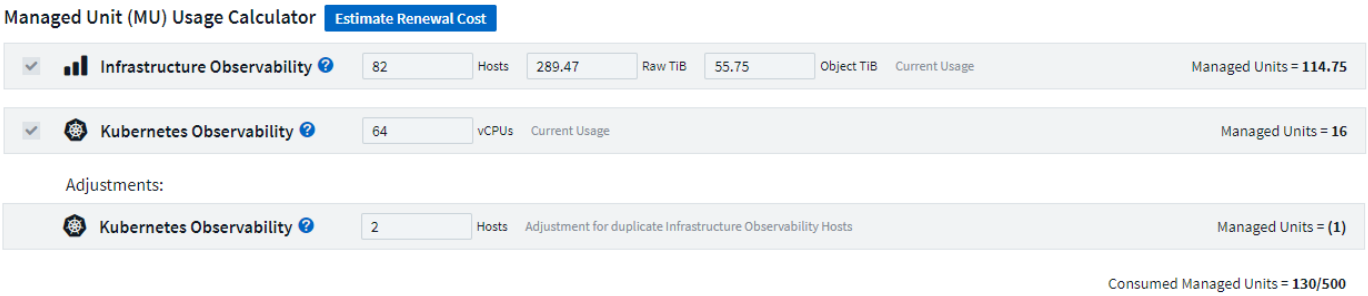
Die Workload-Zuordnung ist benutzerfreundlicher und weniger laut. Sie gruppiert alle ähnlichen externen Services zu einem Node, wenn sie mit denselben Workloads kommunizieren. Dadurch verringert sich die Komplexität der Grafik und es lässt sich leichter nachvollziehen, wie Services miteinander verbunden sind.

Wenn Sie einen gruppierten Knoten auswählen, wird eine detaillierte Tabelle mit den Kennzahlen für den Netzwerkverkehr für jeden externen Service angezeigt, der für diesen Knoten relevant ist.

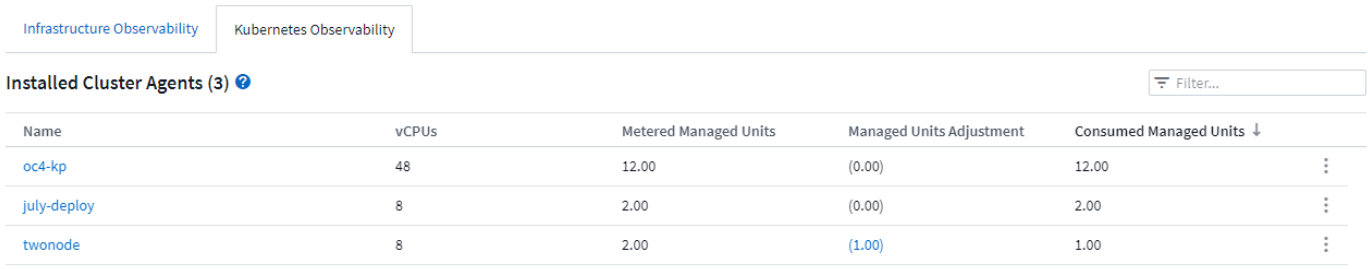
Anpassung der Nutzung von Kubernetes Managed Unit

Wenn eine Compute-Ressource in Ihrer Kubernetes-Cluster-Umgebung sowohl vom NetApp Kubernetes Monitoring Operator als auch vom zugrunde liegenden Datensammler für die Infrastruktur (z. B. VMware) gezählt wird, wird die Nutzung dieser Ressourcen angepasst, um eine möglichst effiziente Zählung der gemanagten Einheiten zu gewährleisten. Sie können die Kubernetes-MU-Anpassungen auf der Seite Admin > Subscription sowohl auf der Registerkarte Summary als auch Usage anzeigen.

Registerkarte „Zusammenfassung“:



Registerkarte „Verwendung“:



Änderungen bei der Erfassung/Erfassung:

Die folgenden Änderungen an der Data Collector/Acquisition Unit sind vorhanden:

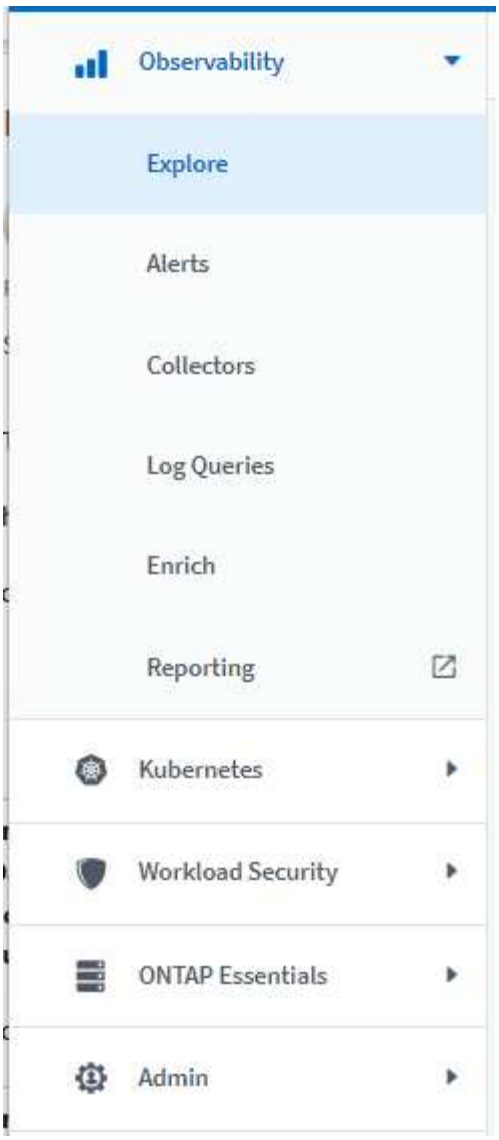
- Acquisition Units unterstützen jetzt RHEL 8.7.

Verbesserte Menüs

Wir haben das Navigationsmenü auf der linken Seite aktualisiert, um die Workflows unserer Kunden besser zu unterstützen. Neue Elemente der obersten Ebene wie *Kubernetes* ermöglichen beschleunigten Zugriff auf die Bedürfnisse des Kunden, und eine konsolidierte Administratorkonsole unterstützt die Rolle des Mandanten-Eigentümers.

Hier einige weitere Beispiele für die Änderungen:

- Im obersten *Observability*-Menü werden Datenerkennung, Warnmeldungen und Protokollabfragen angezeigt
- Die Funktionen von ‘API Access für Beobachtbarkeit und Workload-Sicherheit befinden sich unter einem Menü
- Ebenso für Observability und Workload Security ‘Benachrichtigungen’ Funktionalität, jetzt auch unter einem Menü



Hier ist eine kurze Liste der Funktionen, die Sie unter jedem Menü finden:

Beobachtbarkeit:

- Mehr Erfahren (Dashboards, Kennzahlen-Abfragen, Infrastruktureinblicke)
- Warnmeldungen (Monitore und Alarmfunktionen)
- Kollektoren (Datensammler und Erfassungseinheiten)
- Protokollabfragen
- Anreichern (Anmerkungs- und Anmerkungsregeln, Anwendungen, Geräteauflösung)
- Berichterstellung

Kubernetes:

- Cluster Exploration und Network Map

Workload-Sicherheit:

- Meldungen

- Forensik
- Kollektoren
- Richtlinien

Grundlagen von ONTAP:

- Datensicherung
- Sicherheit
- Meldungen
- Infrastruktur
- Netzwerkbetrieb
- Workloads
  *VMware

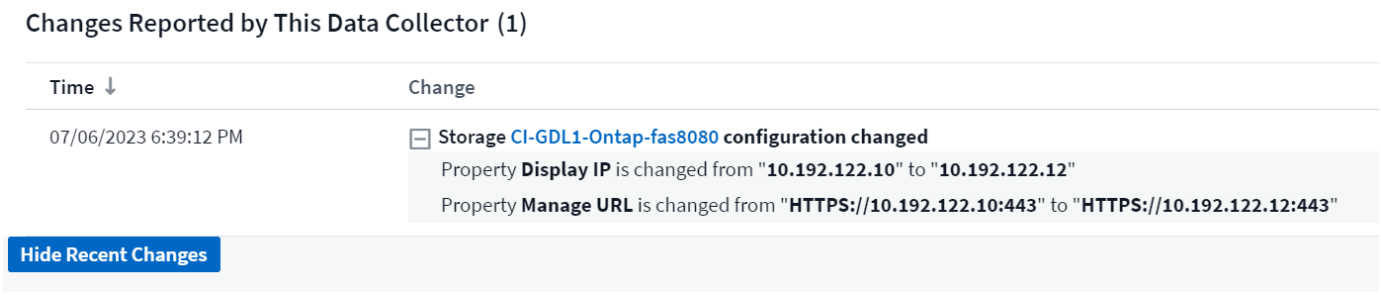
Admin.:

- API-Zugriff
- Prüfung
- Benachrichtigungen
- Abonnementinformationen
- Benutzerverwaltung

Juli 2023

Letzte Änderungen Anzeigen

Die Landing Pages des Data Collectors enthalten nun eine Liste der letzten Änderungen. Klicken Sie einfach auf die Schaltfläche „Letzte Änderungen“ unten auf einer beliebigen Landing Page für den Datensammler, um die letzten Änderungen an der Datensammlung anzuzeigen.



Verbesserungen Des Bedieners

Die folgenden Verbesserungen wurden an vorgenommen "Kubernetes Operator" Implementierung:

- Option zum Umgehen der metrischen Erfassung von Andockern
- Möglichkeit, telegraf-Demonsets und Replikasets Toleranzen hinzuzufügen und anzupassen

Einblick: Cold Storage-Lösung Zurückgewinnen

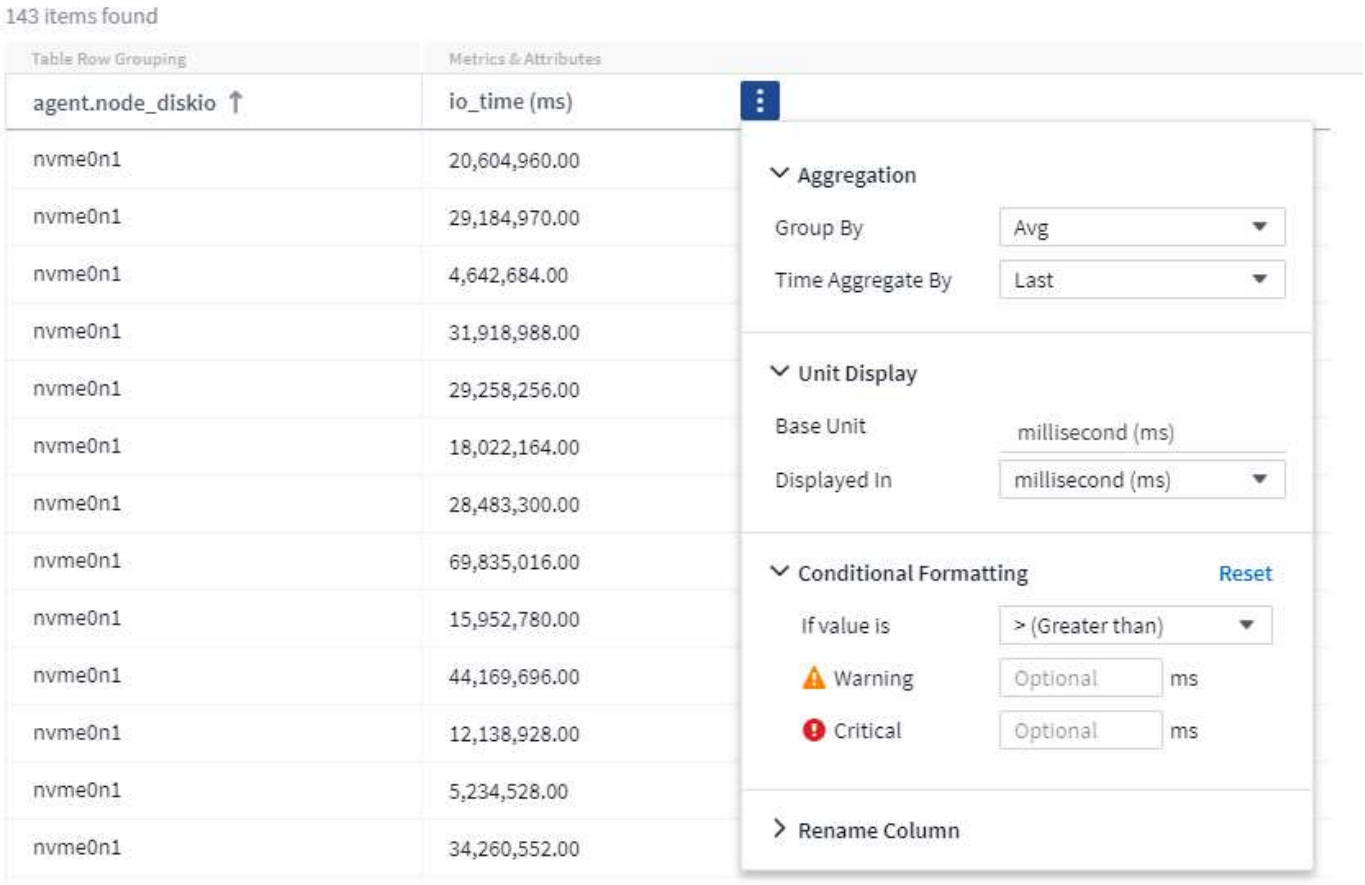
Der "Gewinnen Sie einen Einblick in ONTAP Cold Storage zurück" Unterstützt jetzt FlexGroups und ist jetzt für alle Kunden verfügbar.

Unterschrift Des Bedieners

Für Kunden, die ein privates Repository für ihren NetApp-Kubernetes-Überwachungsoperator verwenden, können Sie jetzt den öffentlichen Schlüssel für die Bildsignatur während der Installation des Bedieners kopieren, um die Authentizität der heruntergeladenen Software zu bestätigen. Wählen Sie während des optionalen Schritts die Schaltfläche *Copy Image Signature Public Key* aus, um das Bedienerbild in Ihr privates Projektarchiv zu laden.

Aggregation, bedingte Formatierung und mehr für Abfragen

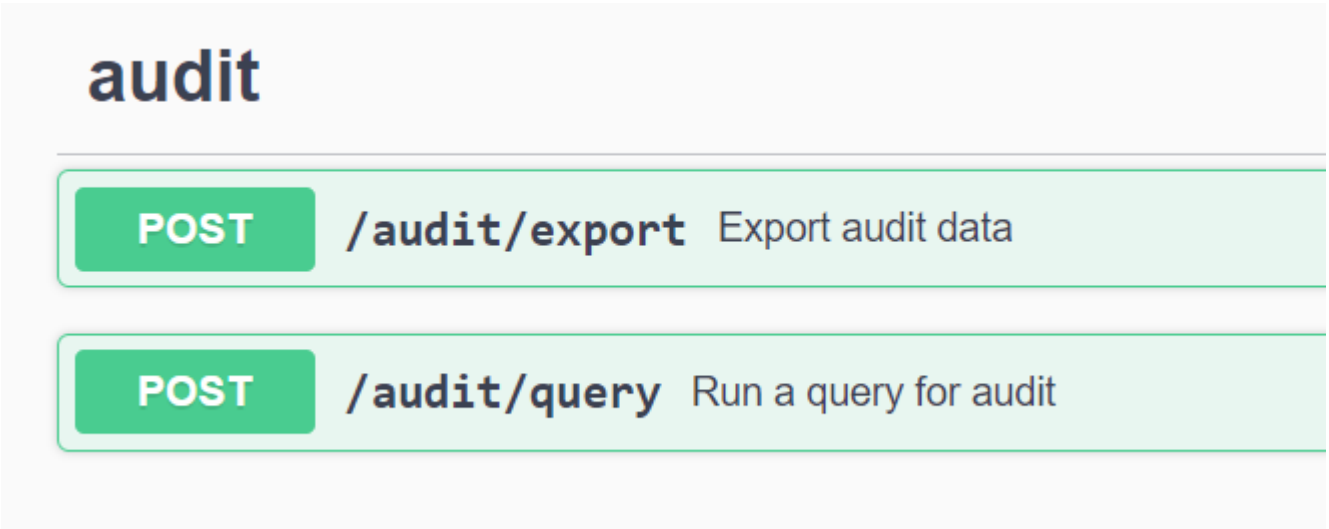
Aggregation, Einheitenauswahl, bedingte Formatierung und Spaltenumbenennung gehören zu den nützlichsten Funktionen eines Dashboard-Tabellen-Widgets, und jetzt sind dieselben Funktionen verfügbar "Abfragen".



Diese Funktionen sind jetzt für Integrationsdaten (Kubernetes, ONTAP Advanced Metrics usw.) verfügbar und werden in Kürze auch für Infrastrukturobjekte (Storage, Volume, Switch usw.) erhältlich sein.

API für Audit

Sie können jetzt eine API zum Abfragen oder Exportieren von überwachten Ereignissen verwenden. Gehen Sie zu Admin > API Access, und wählen Sie den Link *API Documentation*, um Informationen zu erhalten.



Data Collector: Trident Economy

Cloud Insights unterstützt jetzt den Trident-Wirtschaftstreiber und bietet damit folgende Vorteile:

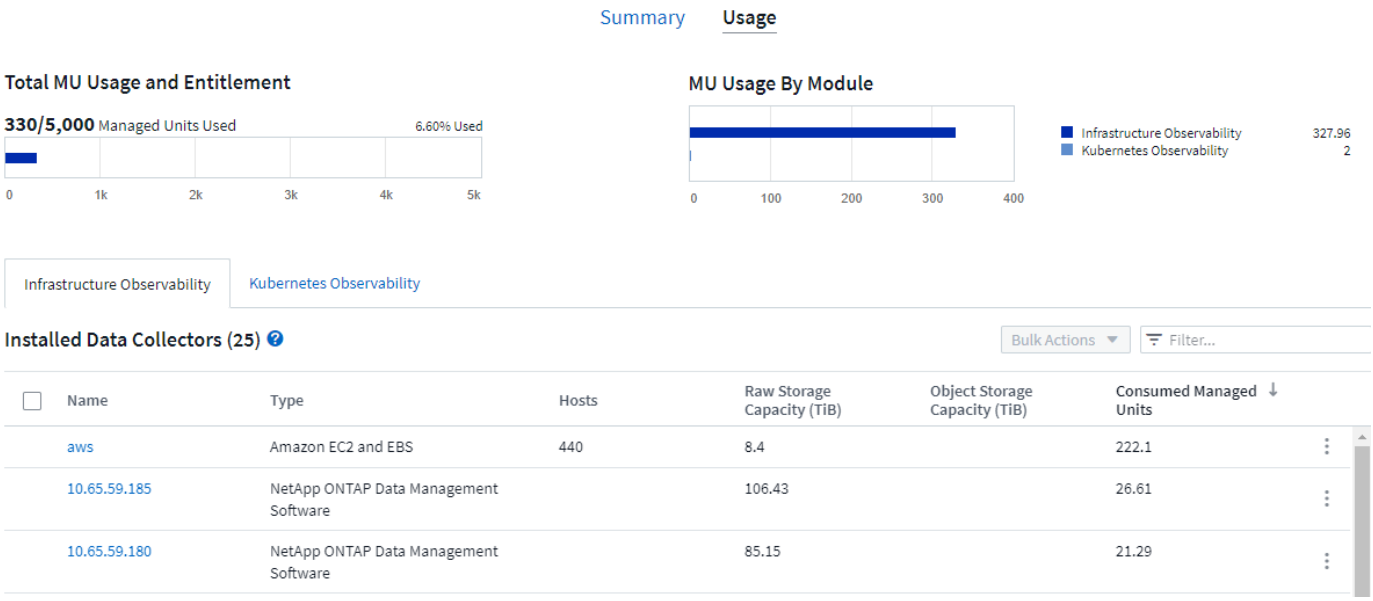
- Erhalten Sie Einblick in die Pod-zu-ONTAP Qtree-Zuordnung und Performance-Metriken.
- Sorgen Sie für eine nahtlose Fehlerbehebung und einfache Navigation von Kubernetes Pods zum Back-End-Storage
- Proaktive Erkennung von Back-End-Performance-Problemen mit Monitoren

---

Juni 2023

Überprüfen Sie Ihre Nutzung

Ab Juni 2023 bietet Cloud Insights eine Aufschlüsselung der Auslastung der verwalteten Einheiten basierend auf dem Funktionssatz. Sie können jetzt die Managed Unit (MU)-Nutzung für Ihre Infrastruktur sowie die MU-Nutzung in Verbindung mit Kubernetes schnell anzeigen und überwachen.



Kubernetes-Netzwerküberwachung und -Zuordnung ist für alle verfügbar

Der "*Kubernetes-Netzwerk-Performance und -Zuordnung*" Vereinfacht die Fehlerbehebung durch die Zuordnung von Abhängigkeiten zwischen Kubernetes-Workloads und bietet Echtzeiteinblick in die Latenzen und Anomalien der Kubernetes-Netzwerk-Performance. So können Performance-Probleme erkannt werden, bevor sie sich auf die Benutzer auswirken. Viele Kunden fanden es hilfreich während der Vorschau, und jetzt ist es für alle zu genießen.

Änderungen bei der Erfassung/Erfassung:

Die folgenden Änderungen an der Data Collector/Acquisition Unit sind vorhanden:

- Die Mus für Data Domain und Cohesity betragen 40 tib : 1 MU.
- Acquisition Units unterstützen jetzt RHEL und Rocky 9.0 und 9.1.

Neue ONTAP Essentials Dashboards

Die folgenden ONTAP Essentials Dashboards sind in Vorschauumgebungen verfügbar und jetzt für alle verfügbar:

- Sicherheits-Dashboard
- Data Protection Dashboard (einschließlich Überblick über den lokalen und den Remote-Schutz)

Zusätzliche Systemmonitore

Die folgenden Systemmonitore sind im Lieferumfang von Cloud Insights enthalten:

- Der FCP-Service für Storage-VM ist nicht verfügbar
- Speicher-VM iSCSI-Service nicht verfügbar

Mai 2023

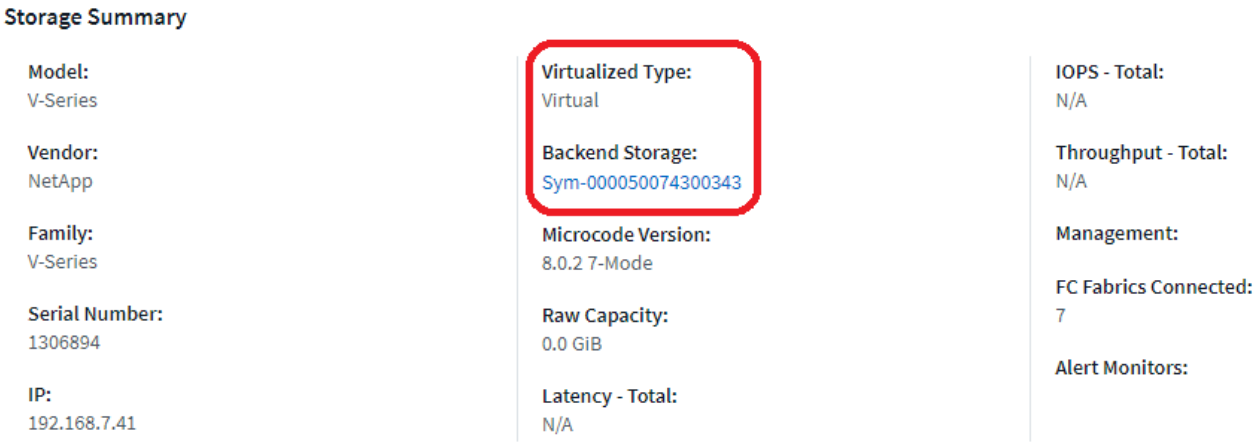
Verbesserte Installation Von Kubernetes Monitoring Operator

Installation und Konfiguration des "NetApp Kubernetes Monitoring Operator" Mit den folgenden Verbesserungen ist es einfacher denn je:

- Umgebung "Konfigurationseinstellungen" Werden in einer einzelnen, selbst dokumentierten Konfigurationsdatei gespeichert.
- Schritt-für-Schritt-Anleitung zum Hochladen von Kubernetes Monitoring Operator Images in Ihr privates Repository.
- Upgrades sind ganz einfach mit einem einzigen Befehl möglich. So können Sie Ihr Kubernetes-Monitoring aktualisieren und benutzerdefinierte Konfigurationen behalten.
- Sicherer: API-Schlüssel verwalten Geheimnisse sicher.
- Einfache Integration und Implementierung mit CI/CD-Automatisierungstools.

Storage-Virtualisierung

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



Neue Webhook-Parameter

Beim Erstellen eines "Webhook" Benachrichtigung können Sie diese Parameter nun in Ihre Webhook-Definition aufnehmen:

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%

Berichte zu Kubernetes-Daten

Von Cloud Insights gesammelte Kubernetes-Daten – einschließlich persistenter Volumes (PV), PVC, Workloads, Cluster und Namespaces – können jetzt in der Berichterstellung verwendet werden. Dies ermöglicht Chargeback, Trendanalysen, Prognosen, TTF-Berechnungen, Und andere Geschäftsberichte zu Kennzahlen für Kubernetes.

Standard-ONTAP-Systemmonitore für neue Kunden aktiviert

Viele ONTAP-Systemmonitore sind in neuen Cloud Insights-Umgebungen standardmäßig aktiviert (d. h. *reaktiviert*). Bisher haben die meisten Monitore den Standardstatus „*Paused*“. Da die geschäftlichen Anforderungen von Unternehmen zu Unternehmen variieren, empfehlen wir immer einen Blick auf die zu werfen "Systemmonitore" In Ihrer Umgebung vorhalten und je nach Alarmanforderungen wieder aufnehmen.

April 2023

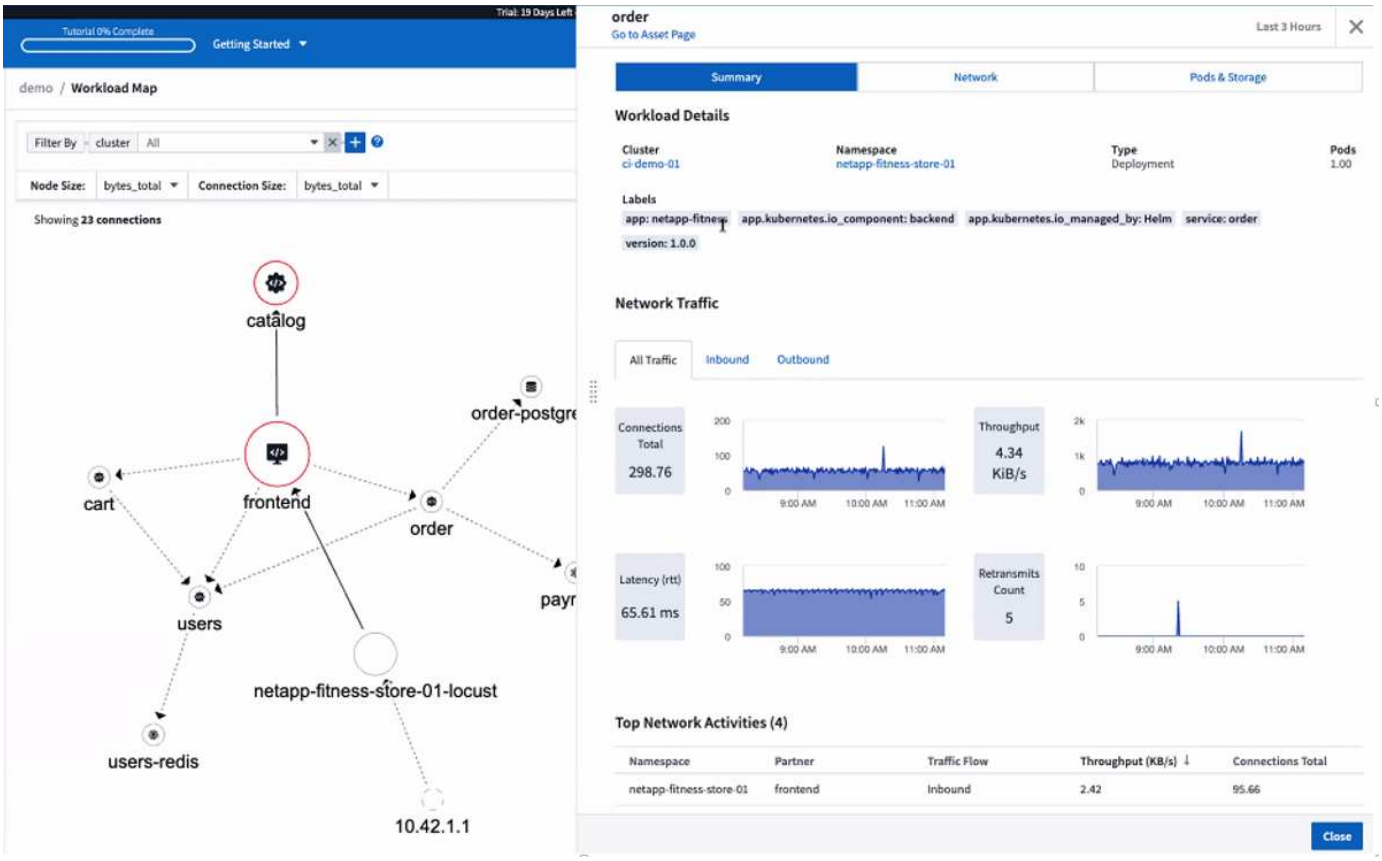
Performance-Monitoring und -Zuordnung von Kubernetes

Der "*Kubernetes-Netzwerk-Performance und -Zuordnung*" Die Funktion vereinfacht die Fehlerbehebung durch Zuordnen von Abhängigkeiten zwischen Kubernetes-Workloads. Es bietet Echtzeiteinblicke in Latenzen und Anomalien bei der Kubernetes-Netzwerk-Performance, um Performance-Probleme zu identifizieren, bevor sie sich auf die Benutzer auswirken. Diese Funktion hilft Unternehmen, durch Analyse und Prüfung des Kubernetes-Traffic-Flows die Gesamtkosten zu senken.

Die wichtigsten Funktionen • die Workload-Map präsentiert Kubernetes-Workload-Abhängigkeiten und -Abläufe und hebt Netzwerk- und Performance-Probleme hervor. • Monitoring des Netzwerkverkehrs zwischen Kubernetes-Pods, Workloads und Nodes; Ermittlung der Quelle von Traffic- und Latenzproblemen • Senkung

der Gesamtkosten durch Analyse des Ingress-, Egress-, Regions- und zonenübergreifenden Netzwerk-Traffics.

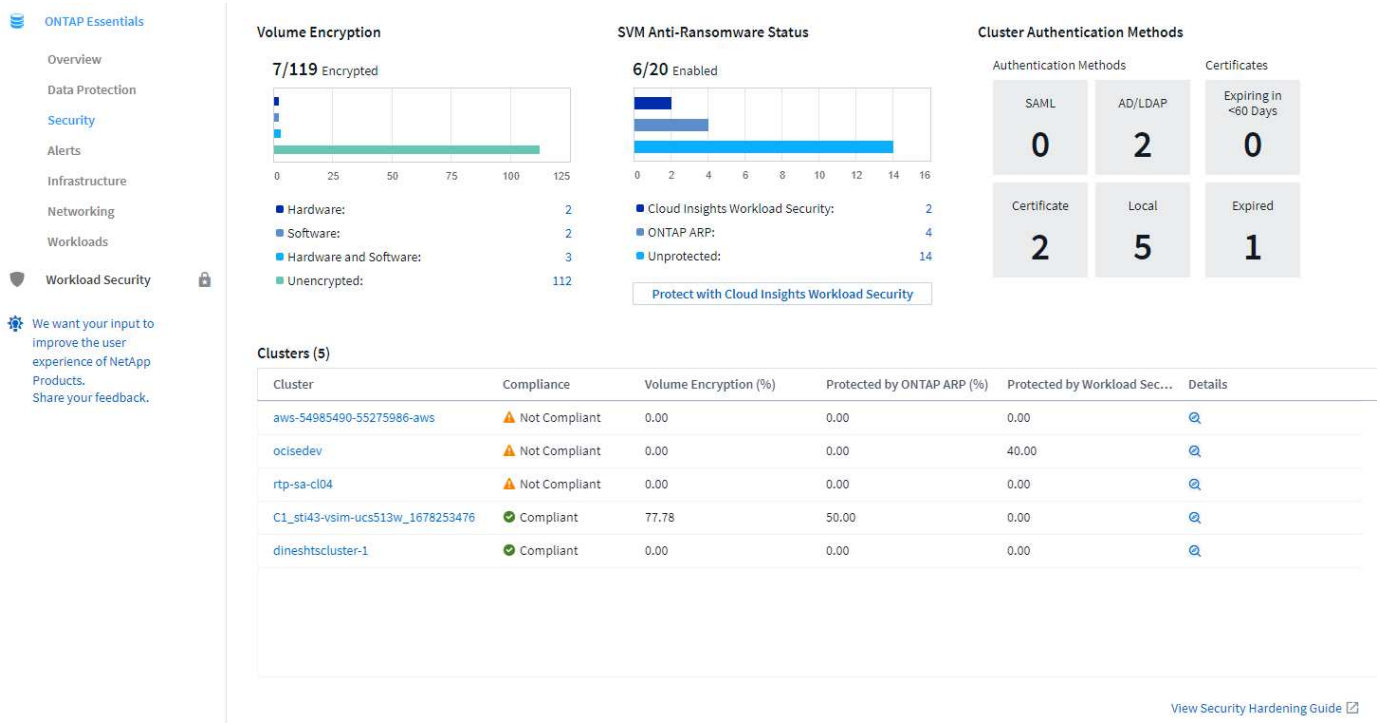
Workload-Zuordnung, die Details zum „Slideout“ anzeigt:



Kubernetes Performance Monitoring and Map ist als erhältlich "Vorschau" Merkmal:

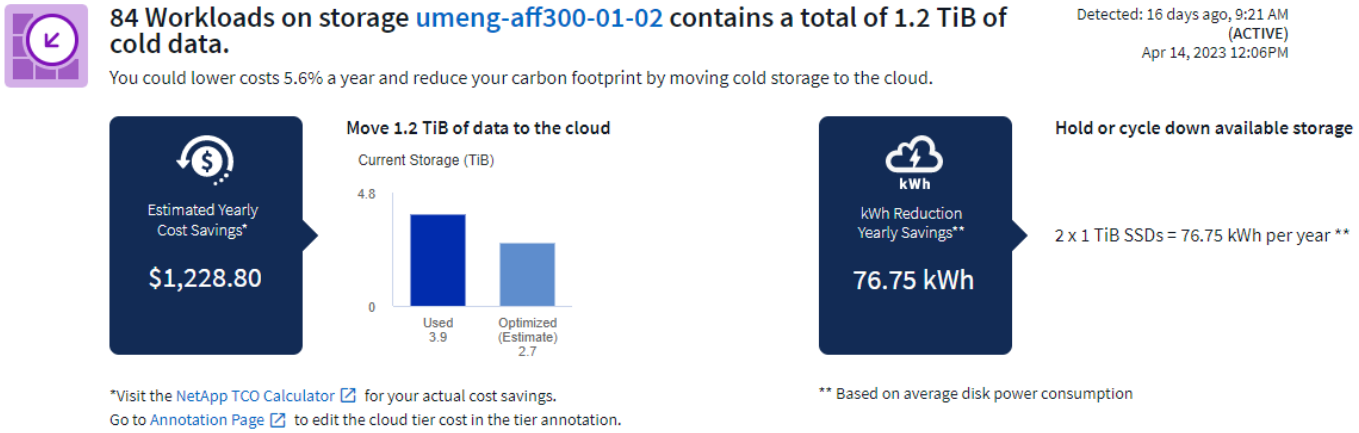
ONTAP Essentials Sicherheitskonsole

Der "Sicherheits-Dashboard" Bietet einen sofortigen Überblick über Ihre aktuelle Sicherheitssituation und zeigt Diagramme zur Verschlüsselung von Hardware- und Software-Volumes, zum Ransomware-Schutz und zu Clusterauthentifizierungsmethoden an. Das Security Dashboard ist als verfügbar "Vorschau" Merkmal:



Rückgewinnung von ONTAP Cold Storage

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



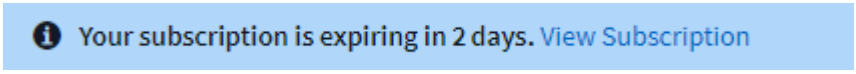
Mit dieser Insight können Sie Fragen wie:

- Welche Menge an kalten Daten in einem Storage Cluster befinden sich auf (a) kostenleistungsfähigen SSD-Festplatten, (b) HDD-Festplatten und (c) virtuellen Festplatten?
- Welche Workloads leisten in Bezug auf den nicht optimierten Storage die größten Beiträge?
- Wie lange (in Tagen) wurden die Daten für einen bestimmten Workload nicht genutzt?

Rückforderung ONTAP Cold Storage wird als A betrachtet "*Vorschau*" Feature und kann daher geändert werden.

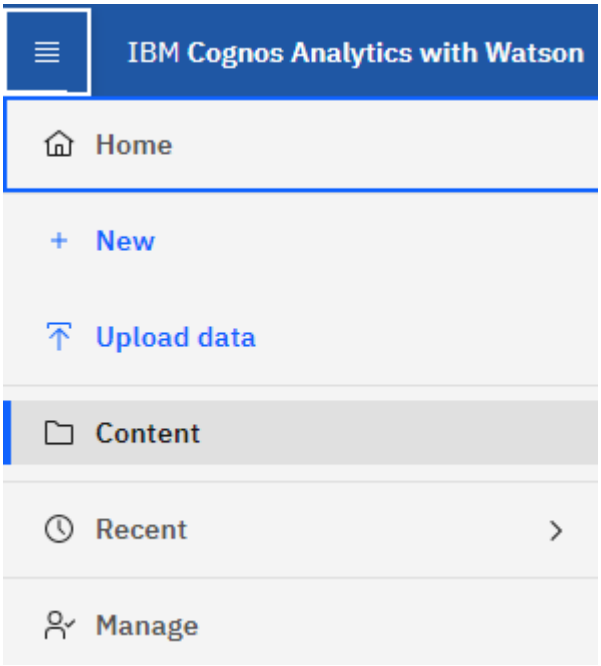
Die Abonnementbenachrichtigung steuert auch Banner-Meldungen

Durch das Festlegen von Empfängern für Abonnementbenachrichtigungen (Admin > Benachrichtigungen) wird jetzt auch festgelegt, wer abonnements in-Product-Banner-Benachrichtigungen sehen wird.



Reporting hat ein neues Aussehen

Sie werden feststellen, dass die Cloud Insights-Berichtsbildschirme ein neues Aussehen haben und dass sich einige der Menünavigation geändert haben. Diese Bildschirme und Navigationsänderungen wurden im aktuellen aktualisiert "Berichtsdokumentation".



Monitore standardmäßig angehalten

Denken Sie daran, sich für neue Cloud Insights-Umgebungen zu eignen "Systemdefinierte Monitore" Senden Sie keine Warnmeldungen standardmäßig. Sie müssen Benachrichtigungen für jeden Monitor aktivieren, den Sie benachrichtigen möchten, indem Sie eine oder mehrere Bereitstellungsmethoden für den Monitor hinzufügen. Für bestehende Cloud Insights-Umgebungen wurde die standardmäßige Empfängerliste *global* für alle systemdefinierten Monitore entfernt, die sich derzeit im Status *Paused* befinden. Benutzerdefinierte Benachrichtigungen bleiben unverändert, ebenso wie Benachrichtigungseinstellungen für aktuell aktive systemdefinierte Monitore.

Suchen Sie die Registerkarte API-Messung?

API Metering wurde von der Seite Abonnement auf die Seite **Admin > API Access** verschoben.

März 2023

Cloud-Anbindung für ONTAP 9.9+ veraltet

Die Cloud-Verbindung für den ONTAP 9.9+-Datensammler wird veraltet. Ab dem 4. April 2023 werden die Datensammler von Cloud Connection in Ihrer Umgebung keine Daten mehr sammeln, sondern beim Abrufen einen Fehler anzeigen. Der Datensammler der Cloud-Verbindung wird in einem späteren Update komplett aus Cloud Insights entfernt.

Vor dem 4. April 2023 ist die Konfiguration eines neuen Datensammlers für die NetApp ONTAP Datenmanagement-Software für alle ONTAP Systeme, die derzeit über Cloud Connection erfasst werden, erforderlich. "Weitere Informationen".

Januar 2023

Neue Protokollmonitore

Wir haben fast zwei Dutzend hinzugefügt "Zusätzliche Systemmonitore" Um bei unterbrochenen Interconnect-Links, Heartbeat-Problemen und vielem mehr eine Warnung zu erhalten. Darüber hinaus wurden drei neue Data Protection Log-Monitore hinzugefügt, um Änderungen bei der automatischen Neusynchronisierung von SnapMirror, der MetroCluster-Spiegelung und dem Resync von FabricPool-Spiegelung zu benachrichtigen.

Beachten Sie, dass einige dieser Monitore standardmäßig *aktiviert* sind. Sie müssen sie *Pause* ausführen, wenn Sie darauf nicht hinweisen möchten. Beachten Sie auch, dass diese Monitore nicht für die Übermittlung von Benachrichtigungen konfiguriert sind. Sie müssen Benachrichtigungsempfänger auf diesen Monitoren konfigurieren, wenn Sie Benachrichtigungen per E-Mail oder Webhook senden möchten.

.CSV-Export für alle Dashboard-TabellenWidgets

Den Zugriff auf Ihre Daten zu gewährleisten ist von entscheidender Bedeutung, deshalb haben wir . CSV-Export ist für alle Metrikabfragen, Dashboard-Tabellen-Widgets und Objekt-Landing-Pages verfügbar, unabhängig vom Datentyp (Asset oder Integration), den Sie abfragen.

Anpassungen von Daten wie Spaltenauswahl, Umbenennung von Spalten und Umbauten von Einheiten sind nun auch in der neuen Exportfunktion enthalten.

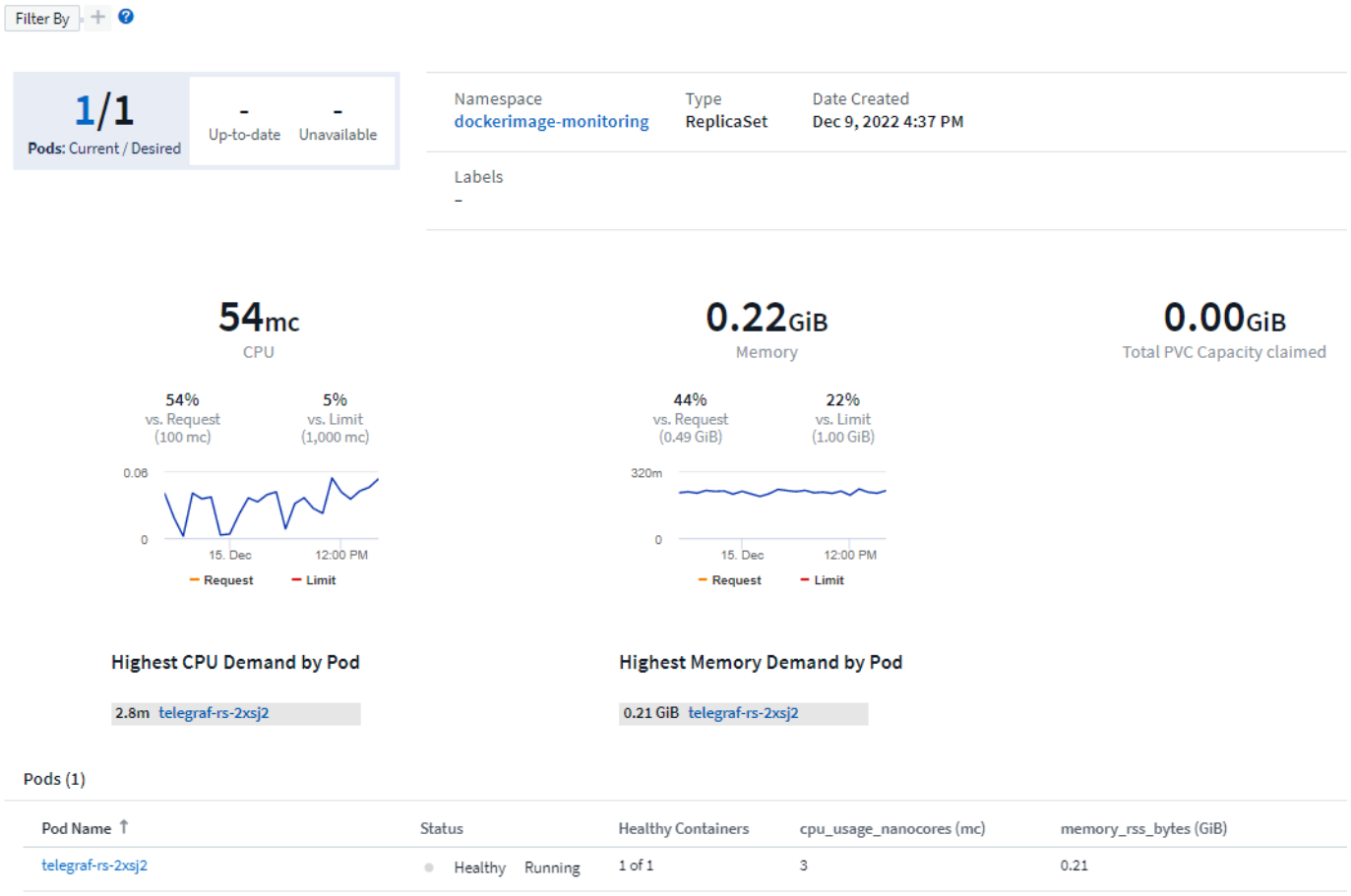
Dezember 2022

Entdecken Sie Ransomware-Schutz und andere Sicherheitsfunktionen während der Cloud Insights-Testversion

Wenn Sie sich ab heute für eine neue Testversion von Cloud Insights anmelden, können Sie sich über Sicherheitsfunktionen wie Ransomware-Erkennung und automatisierte benutzerblockierende Antwortrichtlinien informieren. Wenn Sie sich noch nicht für Ihren Testlauf angemeldet haben, tun Sie es noch heute!

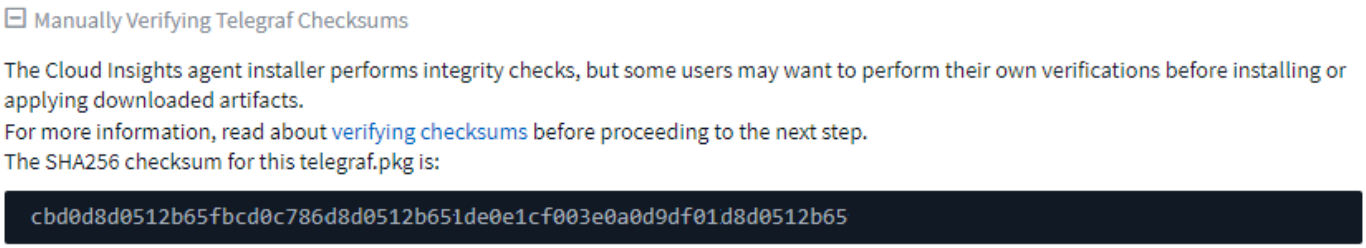
Kubernetes-Workloads verfügen über eine eigene Landing Page

Workloads sind eine wichtige Komponente in Ihrer Kubernetes-Umgebung. Cloud Insights bietet daher jetzt Landing Pages für diese Workloads. Hier können Sie Probleme anzeigen, untersuchen und beheben, die sich auf Ihre Kubernetes-Workloads auswirken.



Überprüfen Sie Ihre Prüfsummen

Sie haben uns gebeten, Ihnen während der Installation des Agenten für Windows und Linux Prüfsummenwerte bereitzustellen, und wir denken, dass das eine tolle Idee ist. Hier sind sie also:

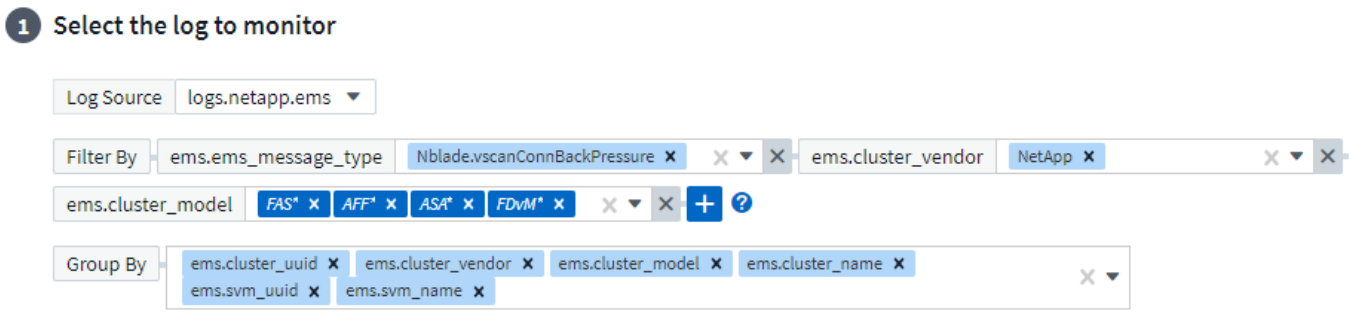


Verbesserungen Bei Der Protokollierung Von Warnmeldungen

Gruppieren Nach

Wenn Sie einen Protokollmonitor erstellen oder bearbeiten, können Sie jetzt Attribute „Gruppieren nach“ festlegen, um eine zielgerichteter Warnung zu ermöglichen. Suchen Sie nach den Attributen „Gruppieren nach“

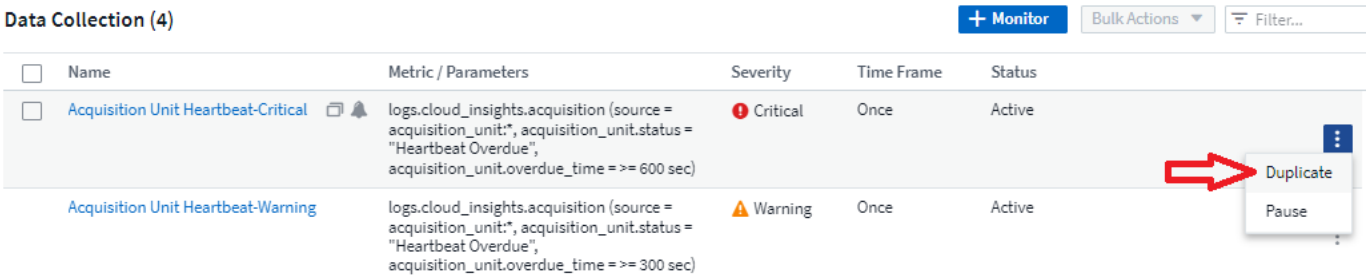
unter den „Filter“-Einstellungen in Ihrer Monitordefinition.



Diese Änderung bringt metrische Monitore und Log-Monitore in Funktionsparität durch Normalisierung des Aspekts „Gruppe nach“ der Monitor-Definitionen. Mit dieser Parität können Kunden zur weiteren Anpassung alle systemdefinierten Standardmonitore klonen/duplizieren.

Duplizieren

Sie können jetzt die Monitore Änderungsprotokoll, Kubernetes Log und Data Collector Log klonen (duplizieren). Dadurch wird ein neuer benutzerdefinierter Protokollmonitor erstellt, den Sie an Ihre spezifischen Definitionen anpassen können.



11 Neue Standard-ONTAP-Monitore für Business Continuity bei SnapMirror

Wir haben fast ein Dutzend neue hinzu "Systemmonitore" Für SnapMirror for Business Continuity (SMBC), die eine Warnung bei Änderungen an SMBC-Zertifikaten und ONTAP Mediatoren enthält.

November 2022

Mehr als 40 neue Sicherheits-, Datenerfassungs- und CVO-Monitore!

Es gibt Dutzende neue, systemdefinierte Monitore, um Sie bei potenziellen Problemen mit Cloud Volumes, Sicherheit und Datensicherung zu warnen. Weitere Informationen zu diesen Monitoren "Hier".

Oktober 2022

Bessere und genauere Ransomware-Erkennung mit ONTAP Integration Autonomer Ransomware-Schutz

Cloud Secure verbessert die Ransomware-Erkennung durch Integration mit ONTAP "Autonomer Schutz Durch Ransomware" (ARP).

Cloud Secure erhält ONTAP ARP-Ereignisse zu potenziellen Volume-Dateiverschlüsselungsaktivitäten und

- Korreliert Ereignisse der Volume-Verschlüsselung mit den Benutzeraktivitäten, um festzustellen, wer die Schäden verursacht,
- Implementiert automatische Antwortrichtlinien, um den Angriff zu blockieren,
- Ermittelt die betroffenen Dateien, was ein schnelleres Recovery ermöglicht und Untersuchungen zu Datenschutzverletzungen durchführt.

September 2022

Monitore in der Basic Edition verfügbar

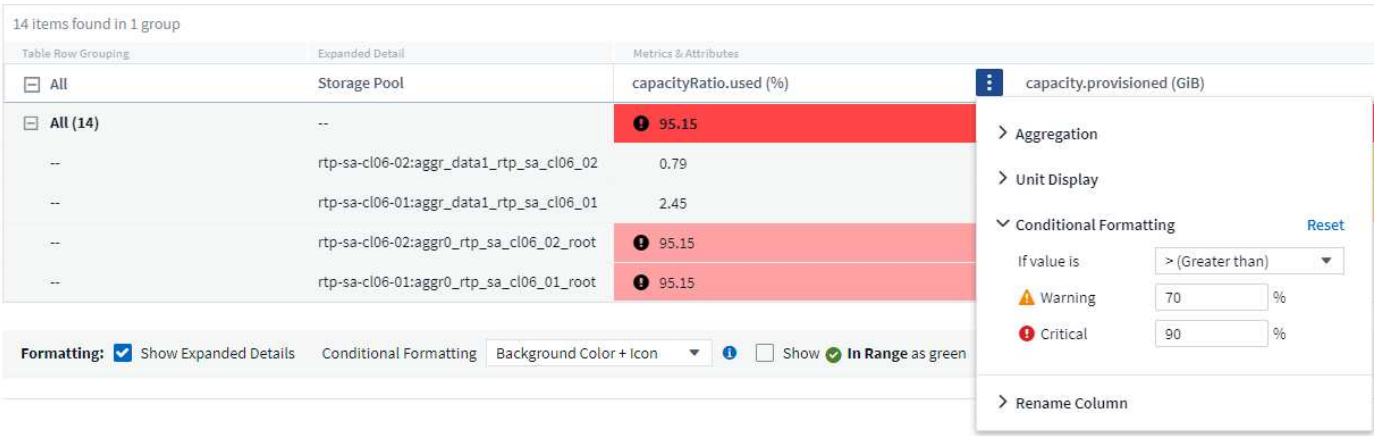
ONTAP "Standardmonitore" Jetzt für die Verwendung in der Cloud Insights Basic Edition verfügbar. Dies umfasst mehr als 70 Infrastrukturmonitore und 30 Workload-Beispiele.

ONTAP Power und StorageGRID Dashboards

Die Dashboard-Galerie enthält ein neues Dashboard für ONTAP-Stromversorgung und -Temperatur sowie vier Dashboards für StorageGRID. Wenn in Ihrer Umgebung ONTAP-Leistungskennzahlen und/oder StorageGRID-Daten erfasst werden, importieren Sie diese Dashboards, indem Sie **+aus Galerie** auswählen.

Übersichtlichkeit der Schwellenwerte auf einen Blick in Tabellen

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



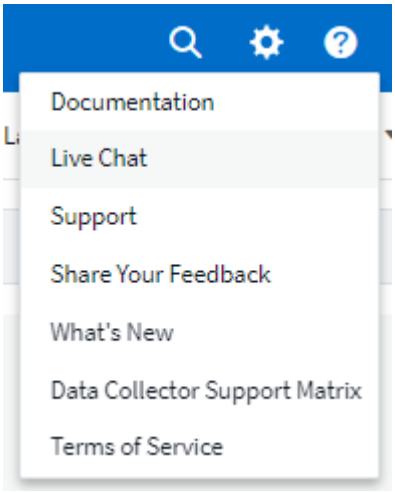
Sicherheitsmonitor

Cloud Insights gibt eine Warnmeldung aus, wenn erkannt wird, dass der FIPS-Modus auf dem ONTAP System

deaktiviert ist. Weitere Informationen "Systemmonitore", Und beobachten Sie diesen Raum für mehr Sicherheit Monitore, kommen bald!

Chat von überall

Chat mit einem NetApp Support-Experten auf jedem Cloud Insights-Bildschirm, indem Sie den neuen Link **Hilfe > Live Chat** auswählen. Hilfe ist über „?“ verfügbar. Symbol oben rechts auf dem Bildschirm.



Mehr sichtbare Einblicke

Wenn Ihre Umgebung eine hat "Insight" Beispielsweise *Shared Ressourcen unter Stress* oder _Kubernetes Namesaces, die nicht mehr über den Speicherplatz verfügen, umfassen Landing Pages für Ressourcen, die betroffen sind, jetzt Links zur Insight selbst und ermöglichen so eine schnellere Exploration und Fehlerbehebung.

Neue Datensammler

- Amazon S3 (als Vorschau verfügbar)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Andere Aktualisierungen Für Data Collector

Alle Datenquellen sind nun optimiert, um die Leistungsabfrage nach Aktualisierungen und/oder Patches der Erfassungseinheit fortzusetzen.

Betriebssystemunterstützung

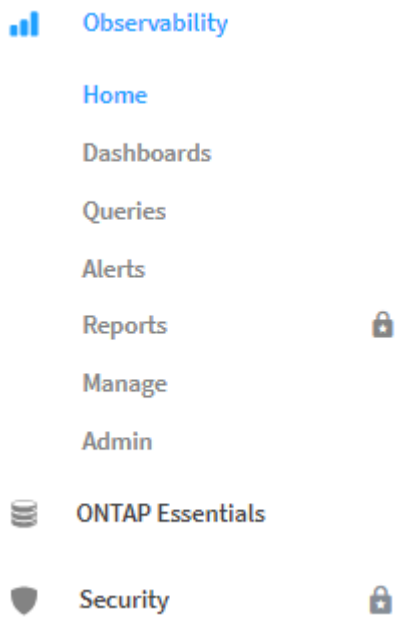
Zusätzlich zu diesen werden die folgenden Betriebssysteme mit Cloud Insights Acquisition Units unterstützt "Unterstützung bereits vorhanden":

- Red Hat Enterprise Linux 8.5, 8.6

August 2022

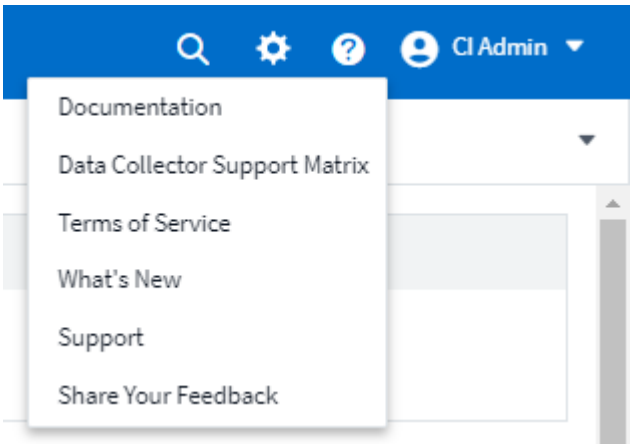
Cloud Insights hat einen neuen Look!

Ab diesem Monat wurde "Monitor and Optimize" umbenannt **Beobachtbarkeit**. Hier finden Sie alle Ihre Lieblingsfunktionen wie Dashboards, Abfragen, Warnmeldungen und Berichte. Suchen Sie darüber hinaus im neuen Menü **Sicherheit** nach Cloud Secure. Beachten Sie, dass sich nur die Menüs geändert haben; die Funktionsfunktionalität bleibt gleich.



Suchen Sie das Menü * Hilfe*?

Hilf jetzt lebt in der oberen rechten Seite des Bildschirms.

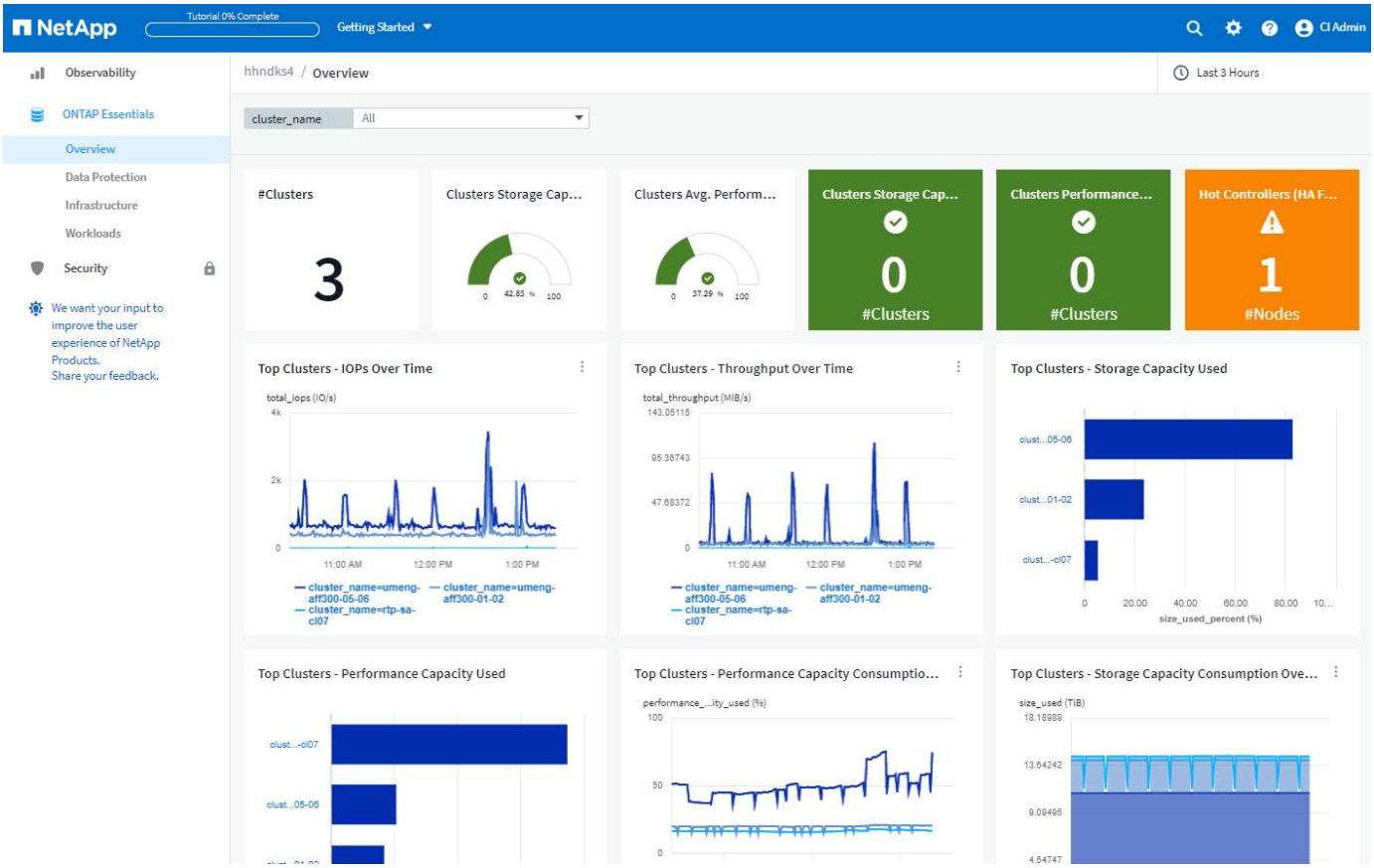


Sie sind nicht sicher, wo Sie anfangen sollen? Informieren Sie sich über die wichtigsten ONTAP-Funktionen.

"ONTAP-Grundlagen" Diese umfassen eine Reihe von Dashboards und Workflows, die detaillierte Einblicke in Ihre ONTAP-Bestände, Workloads und Datensicherung mit detaillierten Prognosen zur Storage-Kapazität und -Performance bieten. Sie sehen sogar, ob Controller mit hoher Auslastung arbeiten. ONTAP Essentials ist Ihr

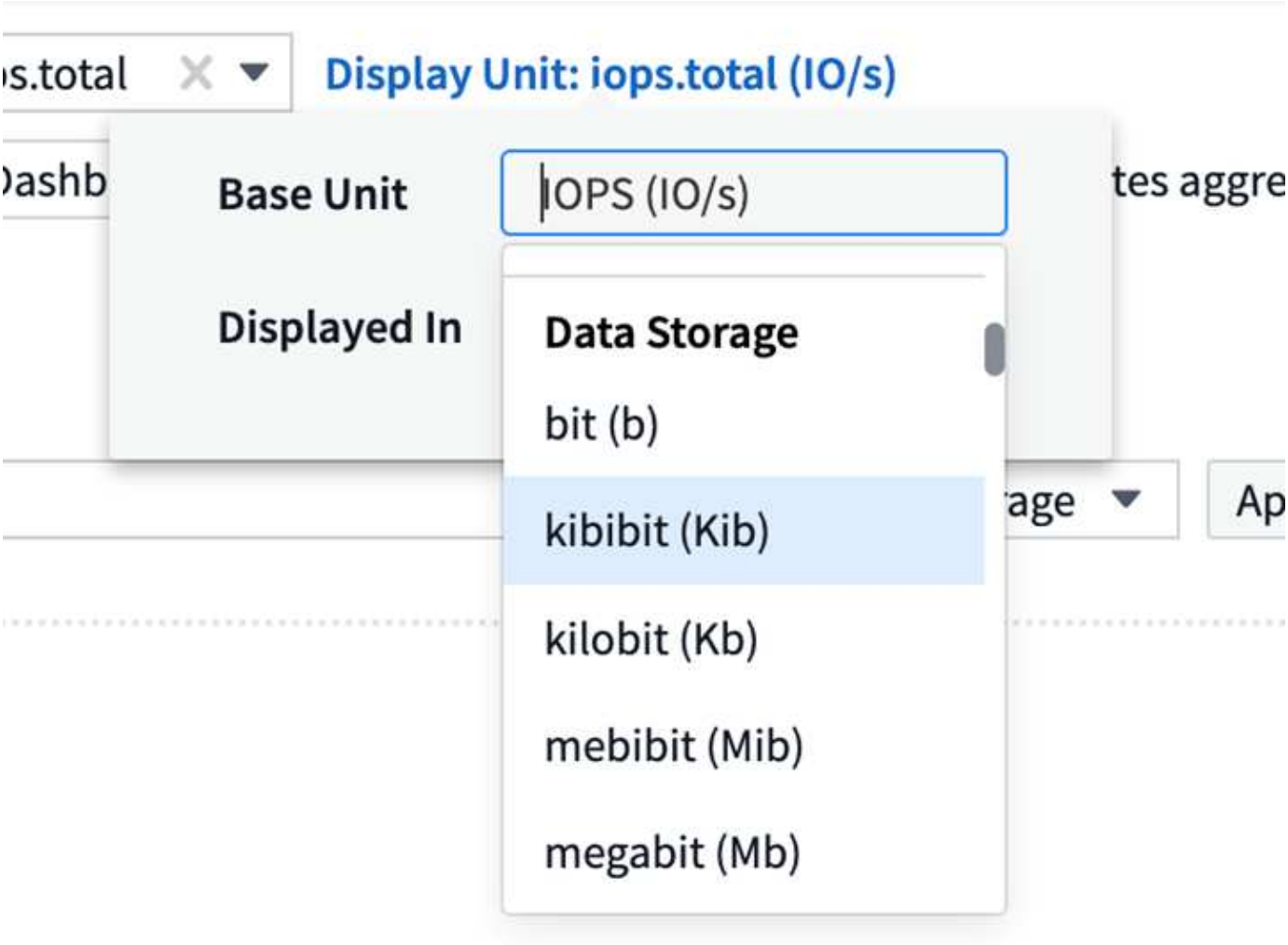
idealer Ort für alle Ihre NetApp ONTAP Monitoring-Anforderungen!

ONTAP Essentials – verfügbar in allen Editionen – ist für bestehende ONTAP-Betreiber und -Administratoren intuitiv gestaltet. Dadurch wird der Übergang von ActiveIQ Unified Manager zu Service-basierten Management-Tools erleichtert.



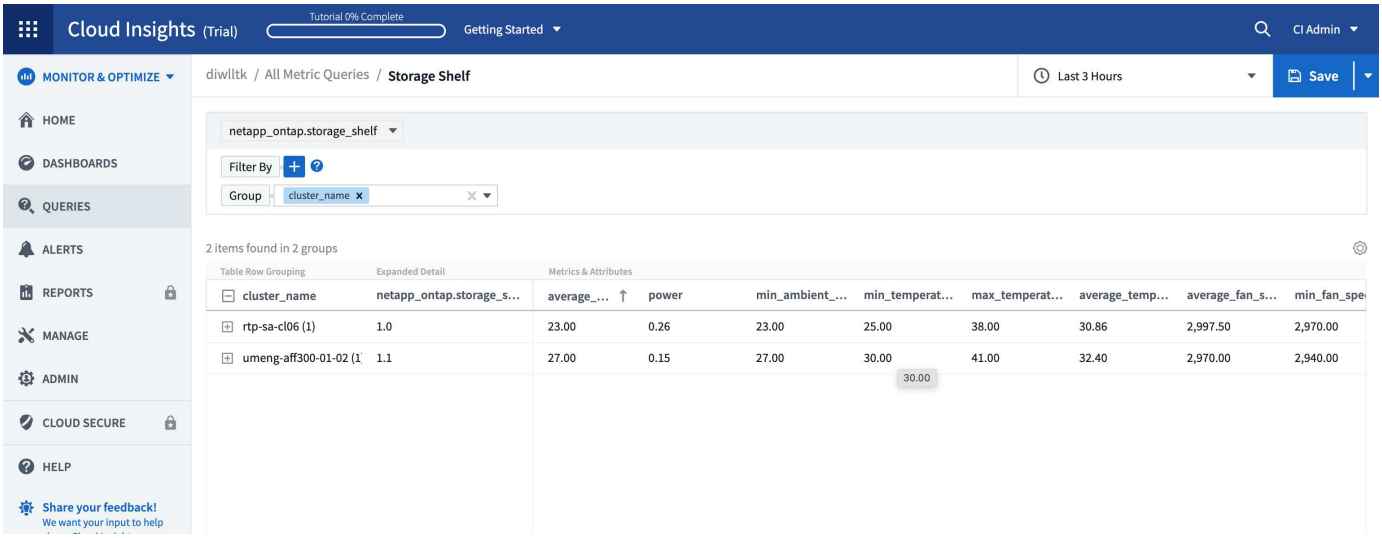
Speicherdatenfamilien werden zusammengeführt

Auf Nachfrage ist das nun ja. Die Dateneinheiten der Speicherbasis-2 und Base-10 werden jetzt in einer Produktfamilie zusammengefasst, von Bits und Bytes bis hin zu Tebits und Terabyte. Auf diese Weise können Sie Daten auf Ihren Dashboards einfacher anzeigen. Auch Datenraten sind jetzt eine große Familie von sich.



Wie viel Energie nutzt mein Storage?

Überwachen Sie Ihren Stromverbrauch, die Temperatur und die Lüftergeschwindigkeit für ein ONTAP Storage Shelf und Ihre Node-Nodes mit den Kennzahlen netapp_ontap.Storage_Shelf, netapp_ontap.System_Node und netapp_ontap.Cluster (nur Stromverbrauch).



Verfügt über abgestufte Funktionen von der Vorschau

Die folgenden Funktionen wurden aus der Vorschau entfernt und stehen nun allen Kunden zur Verfügung:

Funktion	Beschreibung
Kubernetes Namespaces sind nicht mehr platzsparend	Die _Kubernetes Namesaces sind nicht mehr genügend Speicherplatz. Insight bietet Ihnen eine Übersicht über Workloads auf Ihren Kubernetes-Namespaces, die Gefahr laufen, dass der Speicherplatz zu knapp wird. Eine Schätzung für die verbleibende Anzahl an Tagen bevor der Speicherplatz voll wird."Weitere Informationen"
Freigegebene Ressource Unter Stress	Die *Shared Ressource unter Stress* Insight ermittelt mithilfe von KI/ML automatisch, wo Ressourcenkonflikte in Ihrer Umgebung zu einer Performance-Verschlechterung führen, alle von der IT betroffenen Workloads werden hervorgehoben und bietet empfohlene Aktionen zur Behebung für eine schnellere Behebung von Performance-Problemen."Weitere Informationen"
Cloud Secure – Blockieren des Benutzerzugriffs bei Angriffen	Besserer Schutz für geschäftskritische Daten durch die Möglichkeit, Benutzerzugriff bei einem Angriff zu blockieren Der Zugriff kann mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden."Weitere Informationen"

Wie ist meine Datenerfassung Gesundheit?

Cloud Insights bietet zwei neue Heartbeat-Monitore für Ihre Erfassungseinheiten sowie zwei Monitore, um Sie auf Fehler bei der Datenerfassung zu warnen. Diese können verwendet werden, um Sie schnell auf Probleme bei der Datenerfassung zu benachrichtigen.

Die folgenden Monitore sind nun in der Monitorgruppe *Data Collection* verfügbar:

- Acquisition Unit Heartbeat-Critical
- Heartbeat-Warnung Für Erfassungseinheit
- Collector Fehlgeschlagen
- Sammlerwarnung

Beachten Sie, dass sich diese Monitore standardmäßig im Status *Paused* befinden. Aktivieren Sie sie, um über Probleme bei der Datenerfassung informiert zu werden.

Automatische Erneuerung von API-Tokens

API-Access-Token können jetzt für die automatische Erneuerung festgelegt werden. Wenn Sie diese Funktion aktivieren, werden neue/aktualisierte API-Zugriffs-Tokens automatisch für ablaufende Token generiert. Cloud Insights-Agenten, die ein ablaufender Token verwenden, werden automatisch aktualisiert, um das entsprechende neue/aktualisierte API-Zugriffstoken zu verwenden, sodass sie weiterhin reibungslos arbeiten können. Aktivieren Sie einfach das Kontrollkästchen „Token automatisch erneuern“, wenn Sie Ihr Token erstellen. Diese Funktion wird derzeit auf Cloud Insights-Agenten unterstützt, die auf der Kubernetes-Plattform

mit dem aktuellen NetApp Kubernetes Monitoring Operator ausgeführt werden.

Basic Edition bietet mehr als zuvor

Ihre Testversion wird beendet, aber Sie sind sich noch nicht sicher, ob ein Abonnement für Sie geeignet ist? Basic Edition bietet Ihnen schon immer die Möglichkeit, Cloud Insights mit Ihrem aktuellen ONTAP Datensammler weiter zu nutzen, aber jetzt können Sie auch VMware Version-, Topologie- und IOPS/Throughput/Latenz-Daten weiter erfassen. NetApp Kunden mit Premium-Support für ihre Storage-Systeme können auch Cloud Insights unterstützen.

Möchten Sie mehr erfahren?

Im Abschnitt * Learning Center* auf der Seite Hilfe > Support finden Sie Links zu den Cloud Insights Kursangeboten der NetApp University!

Betriebssystemunterstützung

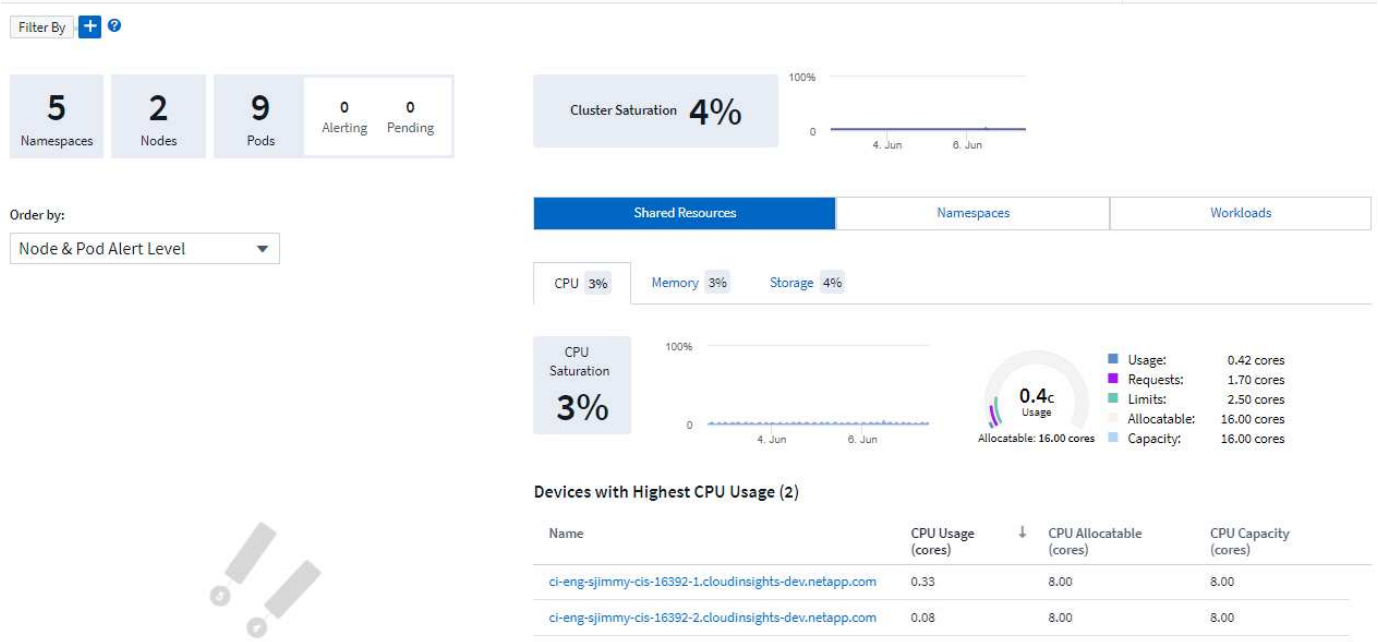
Zusätzlich zu diesen wird das folgende Betriebssystem mit Cloud Insights Acquisition Units unterstützt "Unterstützung bereits vorhanden":

- Windows 11

Juni 2022

Kubernetes-Cluster-Sättigung und andere Details

Mit Cloud Insights können Sie Ihre Kubernetes-Umgebung leichter als je zuvor erkunden. Die verbesserte Cluster-Detailseite bietet Sättigungsdetails, einen übersichtlicheren Überblick über Namespaces und Workloads.

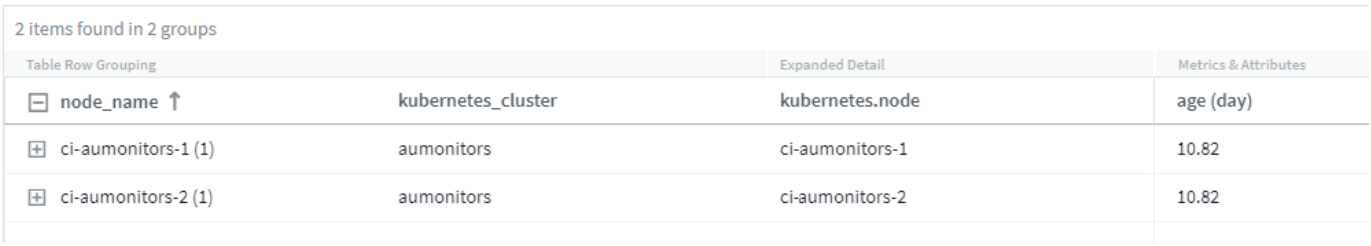


Auf der Seite „Cluster list“ erhalten Sie zusätzlich zu Node, Pod, Namespace und Workload-Anzahl außerdem

einen schnellen Überblick über Sättigung:

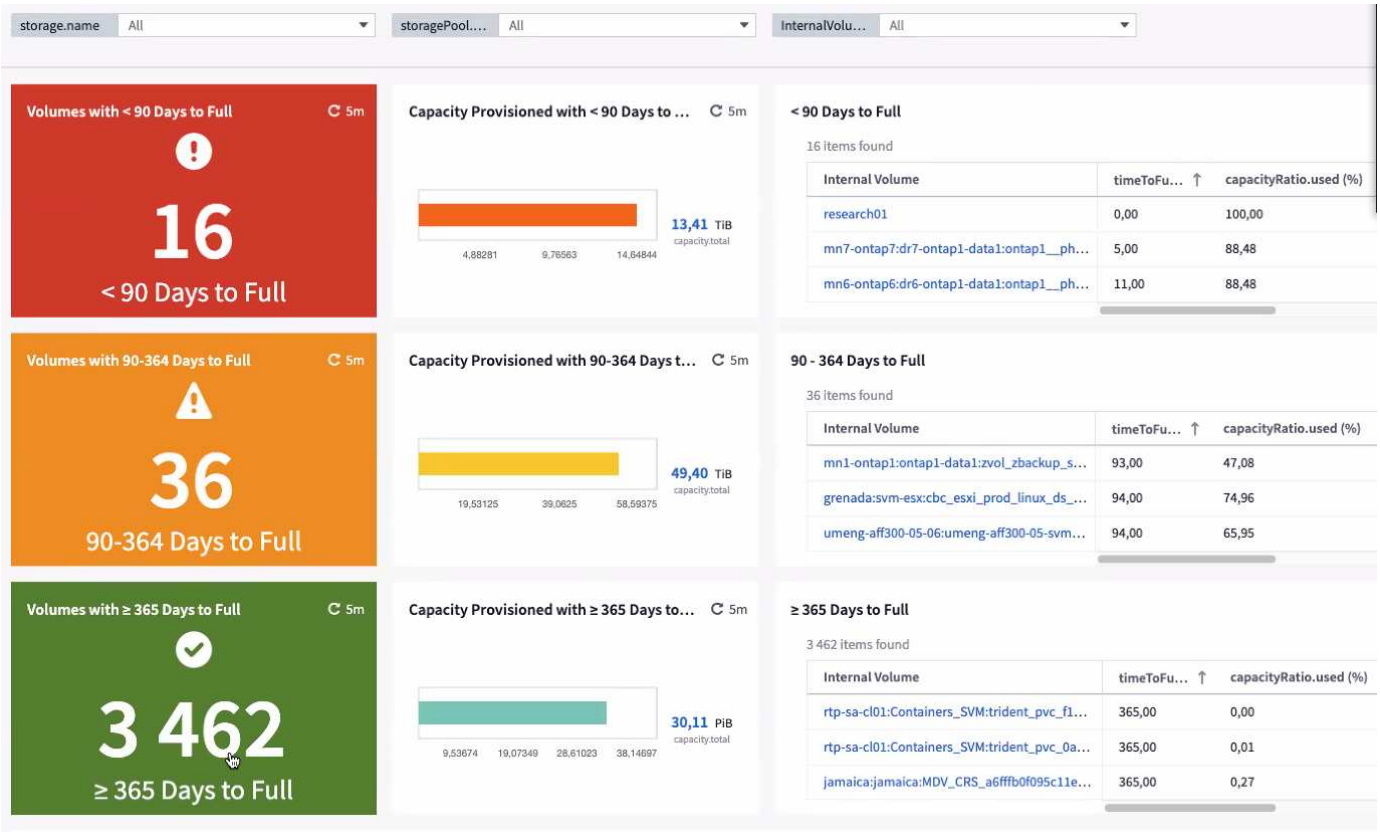
Wie alt ist Ihr Kubernetes Cluster?

Ist Ihr Cluster gerade erst auf der Welt gestartet, oder hat es ein langes digitales Leben erlebt? *Age* wurde als für Kubernetes Nodes gesammelte Zeitmetrik hinzugefügt.



Erstellung vollständiger Prognosen

Cloud Insights stellt ein Dashboard zur Verfügung, das die Anzahl der Tage prognostiziert, bis die Kapazität für jedes überwachte interne Volume erschöpft ist. Diese Werte verringern das Risiko eines Systemausfalls deutlich.

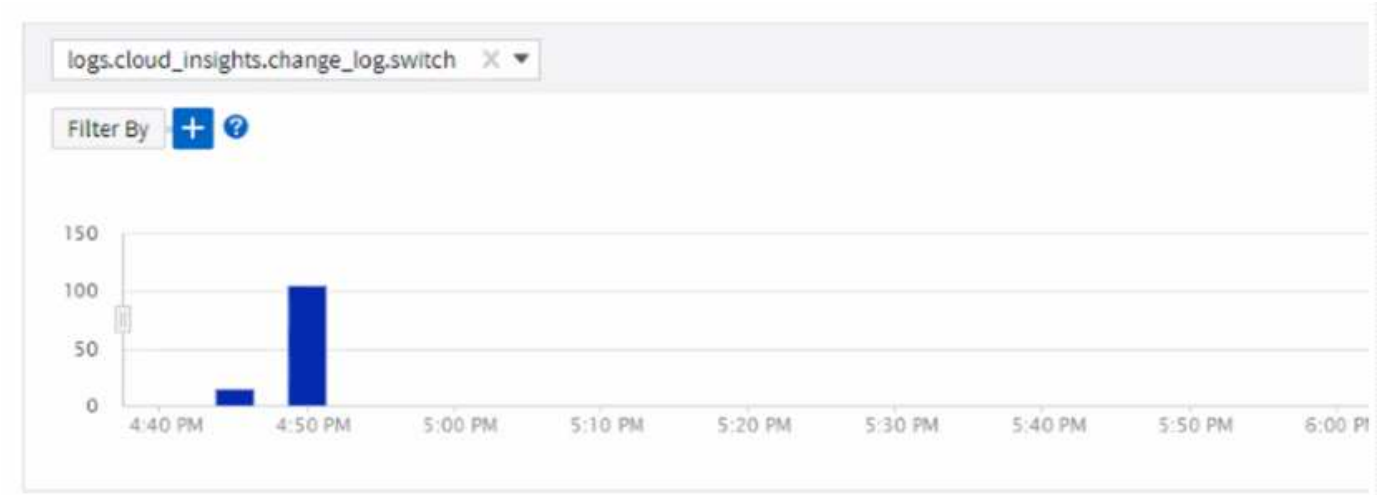


TTF-Zähler stehen auch für Speicher, Speicherpool und Volume zur Verfügung. Achten Sie darauf, dass diese Bereiche weitere Dashboards für diese Objekte enthalten.

Beachten Sie, dass die Time-to-Full-Prognosen sich aus_Preview_ abverlagert und für alle Kunden eingeführt werden.

Was hat sich in meiner Umgebung geändert?

Einträge im ONTAP Änderungsprotokoll können im Log Explorer angezeigt werden.



Log Entries

timestamp ↓	name	object_type	message
06/08/2022 4:52:51 PM	fc19	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	fc20	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	fc23	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	fc22	Port	Port with name:fc22 has been created

Betriebssystemunterstützung

Zusätzlich zu diesen werden die folgenden Betriebssysteme mit Cloud Insights Acquisition Units unterstützt "Unterstützung bereits vorhanden":

- CentOS Stream 9
- Windows 2022

Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf Version **1.22.3** aktualisiert, mit Verbesserungen bei Leistung und Sicherheit. Benutzer, die eine Aktualisierung durchführen möchten, können sich im entsprechenden Abschnitt zur Aktualisierung des s informieren "Agenteninstallation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass eine Benutzeraktion erforderlich ist.

Vorschaufunktionen

Cloud Insights weist regelmäßig eine Reihe von interessanten neuen Vorschaufunktionen auf. Wenn Sie eine oder mehrere dieser Funktionen anzeigen möchten, wenden Sie sich an Ihren "NetApp Vertriebsteam" Finden Sie weitere Informationen.

Funktion	Beschreibung
Kubernetes Namespaces sind nicht mehr platzsparend	Die _Kubernetes Namesaces sind nicht mehr genügend Speicherplatz. Insight bietet Ihnen eine Übersicht über Workloads auf Ihren Kubernetes-Namespaces, die Gefahr laufen, dass der Speicherplatz zu knapp wird. Eine Schätzung für die verbleibende Anzahl an Tagen bevor der Speicherplatz voll wird."Weitere Informationen"
Cloud Secure – Blockieren des Benutzerzugriffs bei Angriffen	Besserer Schutz für geschäftskritische Daten durch die Möglichkeit, Benutzerzugriff bei einem Angriff zu blockieren Der Zugriff kann automatisch mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden."Weitere Informationen"
Freigegebene Ressource Unter Stress	Die *Shared Ressource unter Stress* Insight ermittelt mithilfe von KI/ML automatisch, wo Ressourcenkonflikte in Ihrer Umgebung zu einer Performance-Verschlechterung führen, alle von der IT betroffenen Workloads werden hervorgehoben und bietet empfohlene Aktionen zur Behebung für eine schnellere Behebung von Performance-Problemen."Weitere Informationen"

Mai 2022

Live-Chat mit dem NetApp Support

Sie können jetzt mit Mitarbeitern des NetApp Supports live chatten! Klicken Sie auf der Seite Hilfe > Support einfach auf das Chat-Symbol oder klicken Sie im Abschnitt „Kontakt“ auf „ Chat_“, um eine Chat-Sitzung zu starten. Chat-Support ist an Wochentagen in den USA für Benutzer der Standard und Premium Edition verfügbar.

Kubernetes Operator

Mit der erweiterten Kubernetes-Überwachung und dem Cluster-Explorer von Cloud Insights haben wir es Ihnen leichter gemacht, Sie zum Laufen zu bringen.

Der "Kubernetes Monitoring Operator" (NKMO) ist die bevorzugte Methode für die Installation von Kubernetes für Cloud Insights Insights, für eine flexiblere Konfiguration der Überwachung in weniger Schritten und erweiterte Möglichkeiten zur Überwachung anderer Software, die im K8s-Cluster ausgeführt wird.

Weitere Informationen und Voraussetzungen erhalten Sie über den obigen Link

Benutzer verwalten und Einladungen mit API

Dank der leistungsstarken API von Cloud Insights können Benutzer und Einladungen jetzt gemanagt werden. Lesen Sie mehr im "API-Swagger-Dokumentation".

Warnmeldungen Zur Datenerfassung

Verpassen Sie nicht auf kritische Metriken wegen einem fehlgeschlagenen Sammler!

Es ist einfacher denn je, Ihre Datensammler mit neuen zu verfolgen "Meldungen" Bei Fehlern der Datensammler- und Erfassungseinheit.
Beachten Sie, dass diese Monitore standardmäßig *Paused* sind. Navigieren Sie zur Seite „Monitore“, und suchen Sie „Abschalten der Aufnahmeeinheit“ und „Collector failed“, und nehmen Sie sie wieder auf.

Warnmeldungen zu Änderungen am ONTAP Storage

Unerwartete Storage-Änderungen dürfen nicht zu Ausfällen führen!

Sie können Cloud Insights jetzt so konfigurieren, dass eine Warnmeldung ausgegeben wird, wenn FlexVols, Nodes und SVMs auf ONTAP Systemen erkannt werden.

Vorschaufunktionen

Cloud Insights weist regelmäßig eine Reihe von interessanten neuen Vorschaufunktionen auf. Wenn Sie eine oder mehrere dieser Funktionen anzeigen möchten, wenden Sie sich an Ihren "NetApp Vertriebsteam" Finden Sie weitere Informationen.

Funktion	Beschreibung
Kubernetes Namespaces sind nicht mehr platzsparend	Die _Kubernetes Namesaces sind nicht mehr genügend Speicherplatz. Insight bietet Ihnen eine Übersicht über Workloads auf Ihren Kubernetes-Namespaces, die Gefahr laufen, dass der Speicherplatz zu knapp wird. Eine Schätzung für die verbleibende Anzahl an Tagen bevor der Speicherplatz voll wird."Weitere Informationen"
Interne Volumen- und Volume-Kapazität: Erstellung vollständiger Prognosen	Cloud Insights kann die Anzahl der Tage prognosen, bis die Kapazität für jedes überwachte interne Volume und Volume erschöpft ist. Dieser Wert kann das Risiko eines Systemausfalls deutlich verringern.
Cloud Secure – Blockieren des Benutzerzugriffs bei Angriffen	Besserer Schutz für geschäftskritische Daten durch die Möglichkeit, Benutzerzugriff bei einem Angriff zu blockieren Der Zugriff kann automatisch mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden."Weitere Informationen"

Freigegebene Ressource Unter Stress	Die *Shared Ressource unter Stress* Insight ermittelt mithilfe von KI/ML automatisch, wo Ressourcenkonflikte in Ihrer Umgebung zu einer Performance-Verschlechterung führen, alle von der IT betroffenen Workloads werden hervorgehoben und bietet empfohlene Aktionen zur Behebung für eine schnellere Behebung von Performance-Problemen."Weitere Informationen"

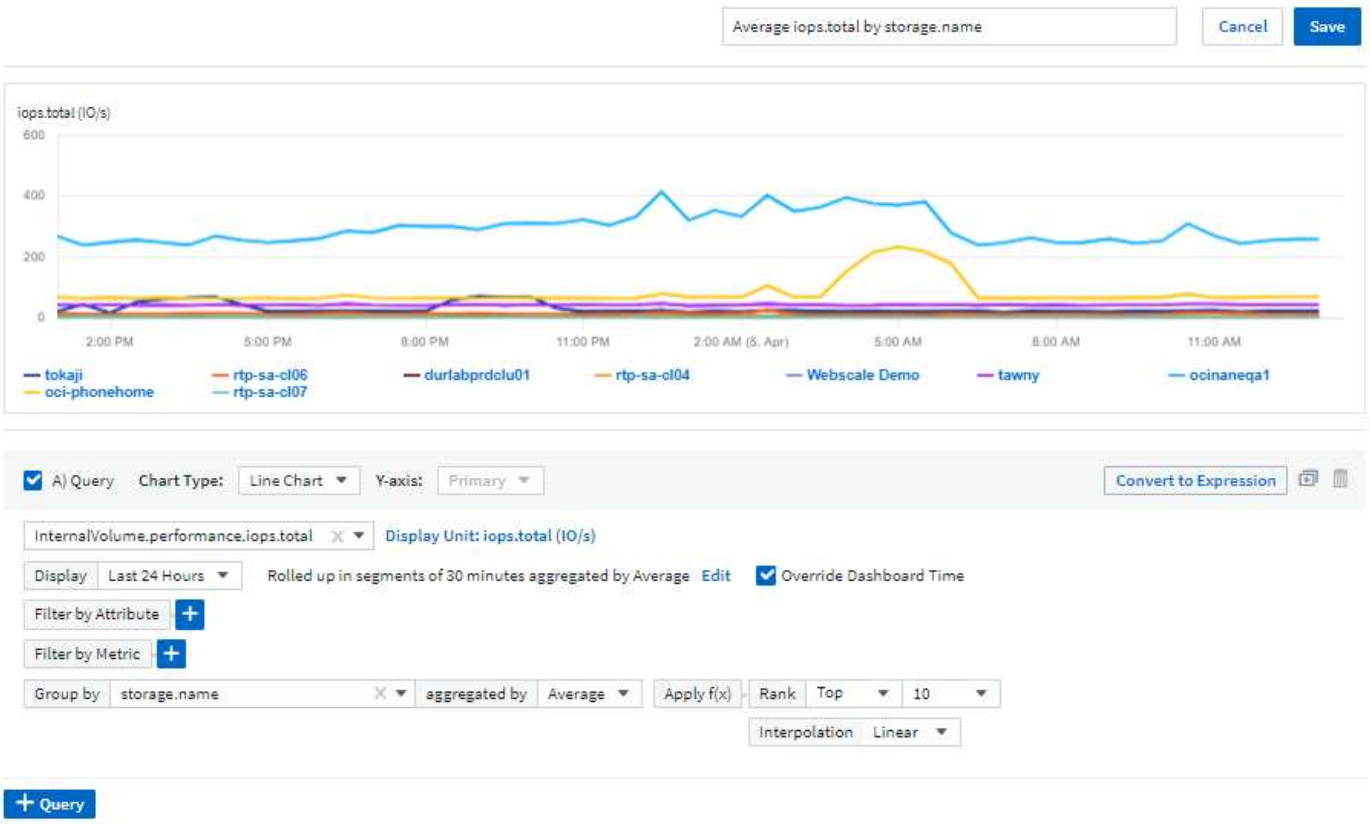
April 2022

Feedback geben!

Ihre Angaben sollen dazu beitragen, die Cloud Insights zu gestalten. Sammeln Sie Punkte und Preise durch die Teilnahme am NetApp Programm **Insights to Action**. **"Jetzt anmelden"**!

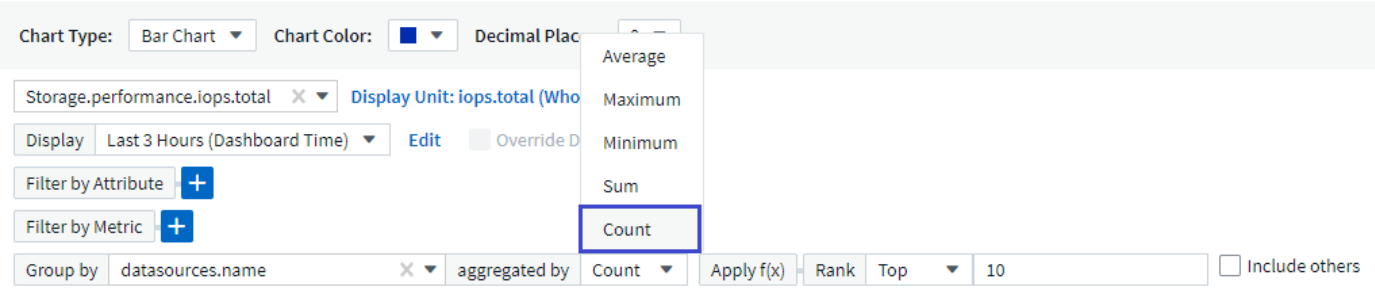
Dashboard-Editor Wurde Aktualisiert

Wir haben unsere Dashboard-Erstellungstools überarbeitet, damit Sie Ihre Daten noch schneller visualisieren können. Navigieren Sie zur Seite „Dashboards“ von Cloud Insights, um ein vorhandenes Dashboard zu bearbeiten, ein Dashboard aus unserer Dashboard-Galerie hinzuzufügen oder ein neues Dashboard von Ihrem eigenen zu erstellen, um es zu überprüfen.



Eine neue Methode zur Zählaggregation wurde ebenfalls eingeführt. Beim Gruppieren von Daten in Balkendiagrammen, Spaltendiagrammen und Kreisdiagrammen können Sie schnell und einfach die Anzahl der

relevanten Objekte für die ausgewählte Metrik anzeigen.



Darüber hinaus können Sie jetzt in Liniendiagrammen eine von drei auswählen "Interpolation" Methoden:

- Keine - Keine Interpolation erfolgt
- Linear - interpoliert einen Datenpunkt zwischen den vorhandenen Punkten
- Treir - verwendet den vorherigen Datenpunkt als interpolierten Datenpunkt

Verbessertes Monitoring Ihrer Kubernetes-Infrastruktur

Cloud Insights behält Sie auf Änderungen in Ihrer Kubernetes-Umgebung bei, indem Sie benachrichtigt werden, wenn Pods, Dämonen und Replikasets erstellt oder entfernt werden, sowie wenn neue Implementierungen erstellt werden. Kubernetes überwacht den Standardwert *pausiert* Status. Daher sollten Sie nur die spezifischen aktivieren, die Sie benötigen.

Vorschaufunktionen

Cloud Insights weist regelmäßig eine Reihe von interessanten neuen Vorschaufunktionen auf. Wenn Sie eine oder mehrere dieser Funktionen anzeigen möchten, wenden Sie sich an Ihren "NetApp Vertriebsteam" Finden Sie weitere Informationen.

Funktion	Beschreibung
Interne Volumen- und Volume-Kapazität: Erstellung vollständiger Prognosen	Cloud Insights kann die Anzahl der Tage prognosen, bis die Kapazität für jedes überwachte interne Volume und Volume erschöpft ist. Dieser Wert kann das Risiko eines Systemausfalls deutlich verringern.
Cloud Secure – Blockieren des Benutzerzugriffs bei Angriffen	Besserer Schutz für geschäftskritische Daten durch die Möglichkeit, Benutzerzugriff bei einem Angriff zu blockieren Der Zugriff kann automatisch mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden."Weitere Informationen"
Freigegebene Ressource Unter Stress	Die Shared-Ressource-Ressourcen unter Stressbewältigung setzt KI/ML ein, um automatisch zu erkennen, wo Ressourcenkonflikte in Ihrer Umgebung eine Performance-Verschlechterung verursachen, alle von der IT betroffenen Workloads hervorheben und empfohlene Aktionen zur Behebung bereitstellen und Performance-Probleme schneller lösen zu können."Weitere Informationen"

Neuer Data Collector

- **Cohesity SmartFiles** - dieser REST API-basierte Collector erwirbt einen Cohesity Cluster, der die „Ansichten“ (als CI-interne Volumes), die verschiedenen Nodes und das Sammeln von Performance-Kennzahlen ermittelt.

Andere Aktualisierungen Für Data Collector

Die Erfassung und Anzeige von Performancedaten wurde auf den folgenden Datensammlern verbessert:

- Brocade CLI
- Dell/EMC VPLEX, PowerStore, Isilon/PowerScale, VNX Block/CLARiiON CLI, XtremIO Unity/VNXe
- Pure FlashArray

Diese Performance-Verbesserungen sind bereits in allen NetApp Data Collectors sowie VMware und Cisco erhältlich und werden in den nächsten Monaten allen anderen Data Collectors eingeführt.

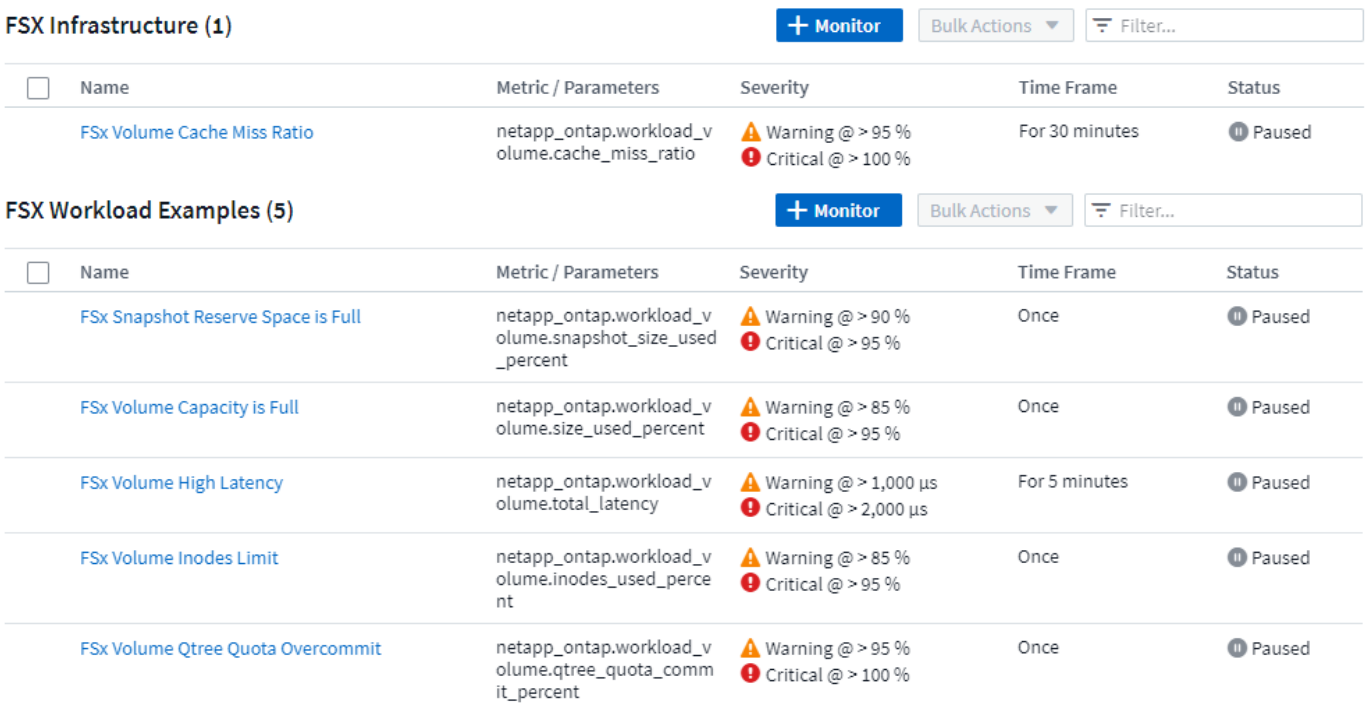
März 2022

Cloud-Anbindung für ONTAP 9.9 oder höher

Der "NetApp Cloud Connection für ONTAP 9.9 oder höher" Data Collector macht die Installation einer externen Erfassungseinheit überflüssig und vereinfacht so die Fehlersuche, die Wartung und die Erstbereitstellung.

Neue FSX für NetApp ONTAP-Monitore

Dank neuer Funktionen überwachen Sie Ihre FSX für NetApp ONTAP Umgebungen mühelos "Systemdefinierte Monitore" Sowohl für die Infrastruktur (Kennzahlen) als auch für Workloads (Protokolle).



Neue Cloud Secure Funktionen stehen allen zur Verfügung

Ihre Umgebung ist sicherer als je zuvor und bietet die folgenden Cloud Secure Funktionen, die nun allgemein verfügbar sind:

Funktion	Beschreibung
Datenvernichtung – Erkennung von Dateilöschung	Erkennen abnormaler Dateilösch-Aktivitäten, Blockieren schädlicher Dateizugriffe durch böswillige Benutzer und Erarbeiten automatischer Snapshots mit automatischen Antwortrichtlinien.
Separate Benachrichtigungen für Warnungen und Warnungen	Warn- und Alarmbenachrichtigungen können an separate Empfänger gesendet werden, um sicherzustellen, dass das richtige Team auf dem Laufenden bleiben kann

Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf Version **1.21.2** aktualisiert, mit Verbesserungen bei Leistung und Sicherheit. Benutzer, die eine Aktualisierung durchführen möchten, können sich im entsprechenden Abschnitt zur Aktualisierung des s informieren "Agenteninstallation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass eine Benutzeraktion erforderlich ist.

Updates Für Data Collector

- Der Datensammler der Broadcom Fibre Channel-Switches wurde optimiert, um die Anzahl der CLI-Befehle zu reduzieren, die bei jeder Bestandsabfrage ausgegeben werden.

Februar 2022

Cloud Insights behebt die Sicherheitsanfälligkeiten von Apache Log4j

Kundensicherheit hat bei NetApp höchste Priorität. Cloud Insights enthält Updates seiner Software-Bibliotheken, um die letzten Apache Log4j-Sicherheitsanfälligkeiten zu beheben.

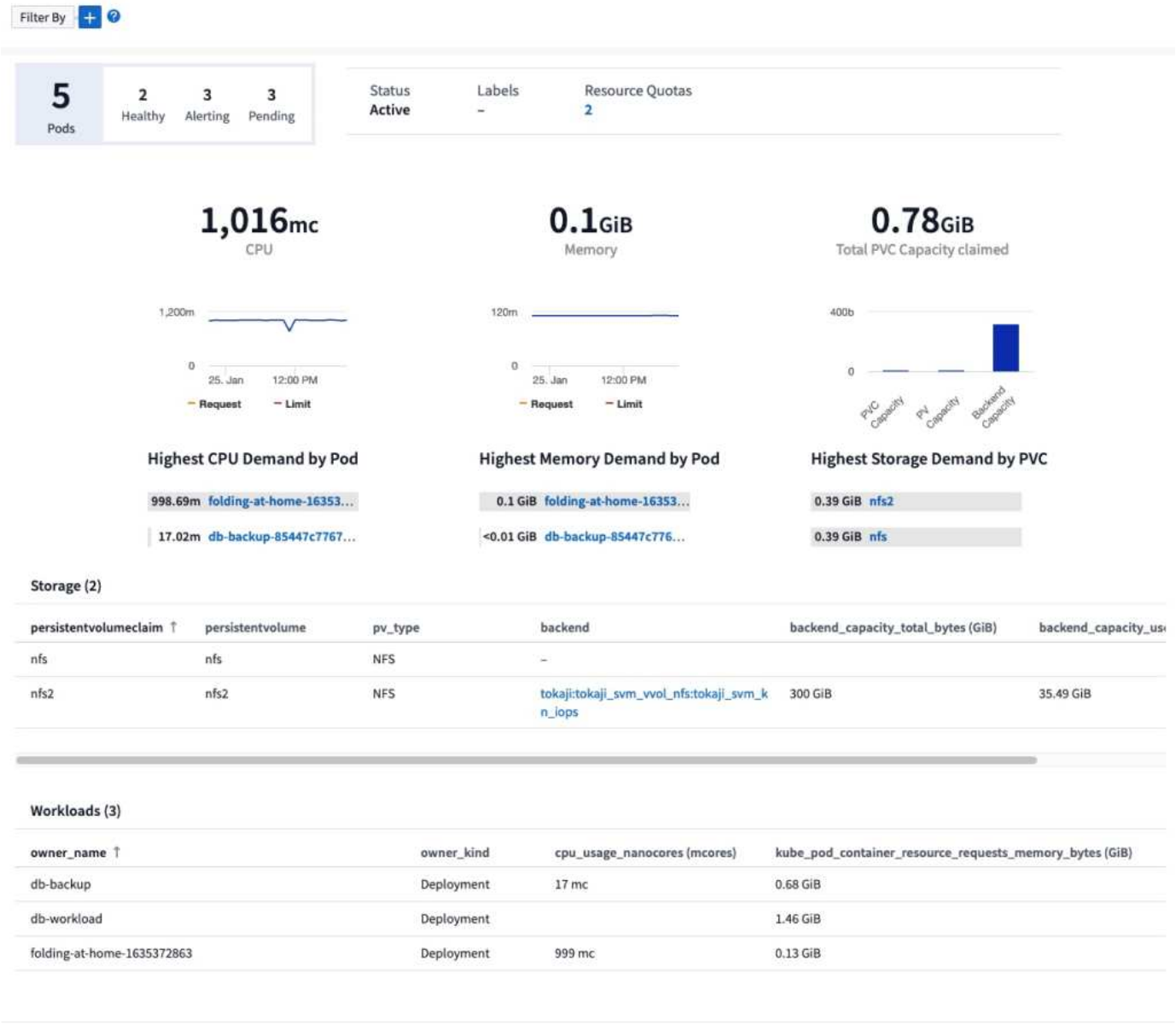
Auf der Product Security Advisory Website von NetApp finden Sie Folgendes:

"CVE-2021-44228"
"CVE-2021-45046"
"CVE-2021-45105"

Weitere Informationen zu diesen Schwachstellen und der Reaktion von NetApp finden Sie unter "NetApp Newsroom".

Detailseite Kubernetes Namespace

Die Erforschung Ihrer Kubernetes-Umgebung ist jetzt besser denn je, mit informativen Detailseiten für die Namespaces Ihres Clusters. Die Namespace-Detailseite bietet eine Zusammenfassung aller durch einen Namespace verwendeten Ressourcen, einschließlich aller Backend-Storage-Ressourcen und deren Kapazitätsnutzung.



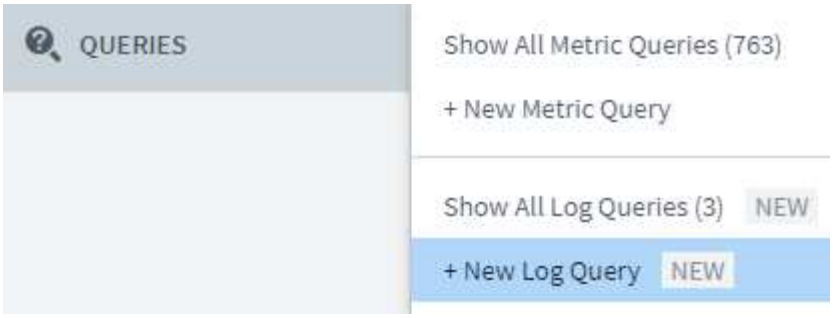
Dezember 2021

Enge Integration für ONTAP Systeme

Vereinfachen Sie die Alarmierung bei ONTAP Hardware-Ausfällen und vieles mehr durch neue Integration mit dem NetApp Event Management System (EMS)."Erkunden und warnen" Auf Low-Level ONTAP Meldungen in Cloud Insights, um Workflows zur Fehlerbehebung zu informieren und zu verbessern, und die Abhängigkeit von ONTAP Element Management Tools weiter zu reduzieren

Abfragen Von Protokollen

Für ONTAP Systeme bieten Cloud Insights-Anfragen eine leistungsstarke "Log-Explorer", So dass Sie leicht zu untersuchen und Fehler EMS-Log-Einträge.



Benachrichtigungen auf Data Collector-Ebene

Zusätzlich zu systemdefinierten und benutzerdefinierten Monitoren für Warnmeldungen können Sie auch Warnmeldungen für ONTAP-Datensammler einrichten. So können Sie Empfänger für Warnmeldungen auf Sammelebene festlegen, unabhängig von anderen Monitoralarme.

Höhere Flexibilität von Cloud Secure-Rollen

Benutzern kann auf Grundlage von Zugriff auf Cloud Secure-Funktionen gewährt werden "Rollen" Von einem Administrator festgelegt:

Rolle	Cloud Secure Zugriff
Verwalter	Alle Cloud Secure-Funktionen, einschließlich der Funktionen für Alarme, Forensik, Datensammler, automatisierte Antwortrichtlinien und APIs für Cloud Secure, können ausgeführt werden. Ein Administrator kann auch andere Benutzer einladen, kann aber nur Cloud Secure-Rollen zuweisen.
Benutzer	Kann Warnungen anzeigen und verwalten und Forensik anzeigen. Benutzerrolle kann den Alarmstatus ändern, eine Notiz hinzufügen, Snapshots manuell erstellen und den Benutzerzugriff blockieren.
Gast	Kann Warnungen und Forensik anzeigen. Gastrolle kann den Alarmstatus nicht ändern, Notizen hinzufügen, Snapshots manuell erstellen oder den Benutzerzugriff blockieren.

Betriebssystemunterstützung

CentOS 8.x Unterstützung wird durch **CentOS 8 Stream** Unterstützung ersetzt. CentOS 8.x wird das Ende des Lebens am 31. Dezember 2021 erreichen.

Updates Für Data Collector

Zur Berücksichtigung von Anbieteränderungen wurde eine Reihe von Cloud Insights Data Collector-Namen hinzugefügt:

Anbieter/Modell	Vorheriger Name
Dell EMC PowerScale	Isilon

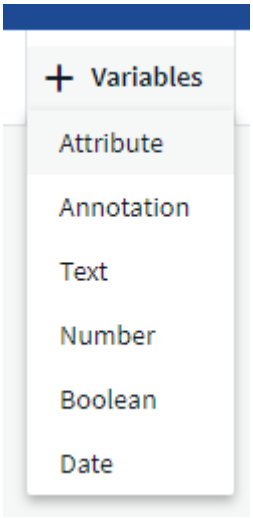
HPE Alletra 9000/Primera	3PAR
HPE Alletra 6000	Nimble

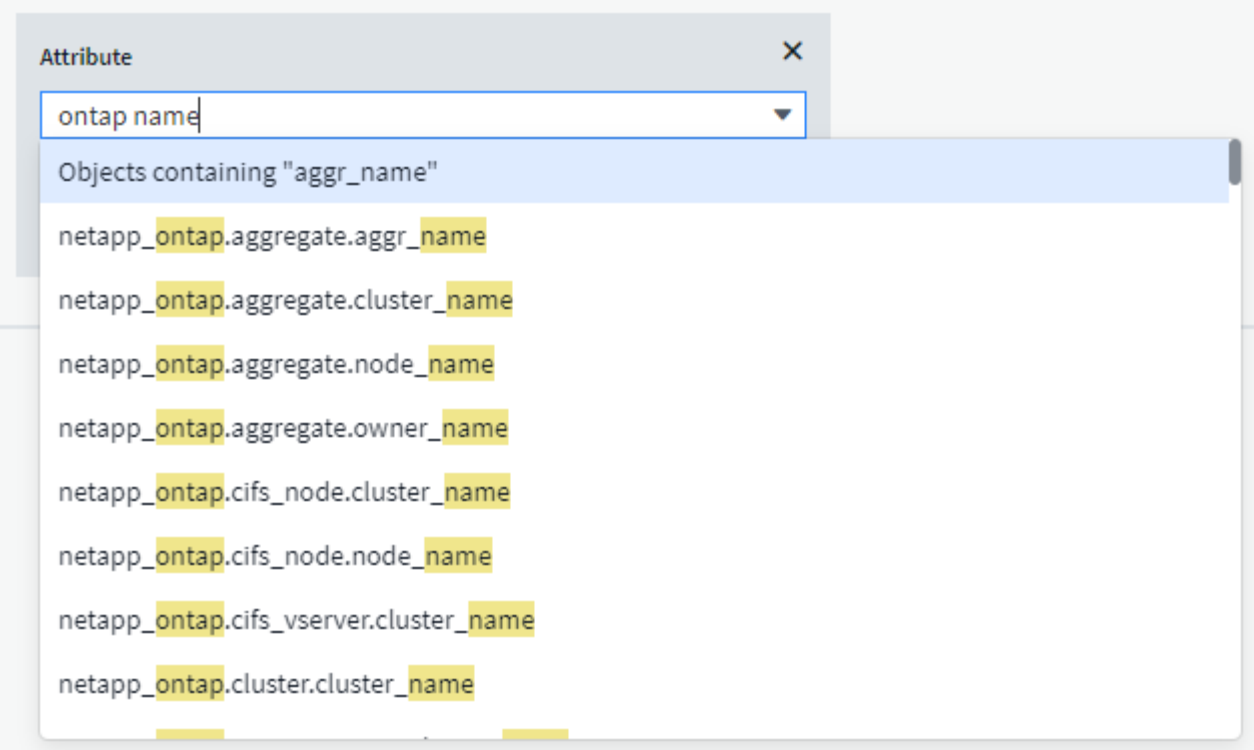
November 2021

Adaptive Dashboards

Neue Variablen für Attribute und die Fähigkeit, Variablen in Widgets zu verwenden.

Dashboards sind jetzt leistungsfähiger und flexibler als je zuvor. Erstellen Sie adaptive Dashboards mit Attributvariablen, um Dashboards schnell im laufenden Betrieb zu filtern. Mit diesen und anderen bereits vorhandenen "Variablen" Sie können jetzt ein Dashboard erstellen, das Kennzahlen für Ihre gesamte Umgebung anzeigt und reibungslos nach Ressourcenname, Typ, Standort usw. gefiltert wird. Verwenden Sie Zahlenvariablen in Widgets, um Rohdaten mit Kosten zu verknüpfen, z. B. Kosten pro GB für Speicher als Service.





Greifen Sie über die API auf die Berichtsdatenbank zu

Verbesserte Funktionen zur Integration in Berichterstellungs-, ITSM- und Automatisierungs-Tools von Drittanbietern – leistungsstarke Cloud Insights "API" Ermöglicht Benutzern, die Cloud Insights-Berichtsdatenbank direkt abzufragen, ohne die Cognos-Berichtsumgebung zu durchlaufen.

Pod-Tabellen auf der VM Landing Page

Nahtlose Navigation zwischen VMs und den Kubernetes Pods, bei denen sie verwendet werden: Für eine bessere Fehlerbehebung und Management von Performance-Reserven wird nun eine Tabelle mit Kubernetes Pods auf VM-Landing Pages angezeigt.

Updates Für Data Collector

- ECS meldet jetzt Firmware für Speicher und Knoten
- Isilon hat eine verbesserte Problemerkennung verbessert
- Azure NetApp Files erfasst Performance-Daten schneller
- StorageGRID unterstützt jetzt Single Sign On (SSO).
- Brocade CLI meldet ordnungsgemäß das Modell für X&-4

Weitere Betriebssysteme werden unterstützt

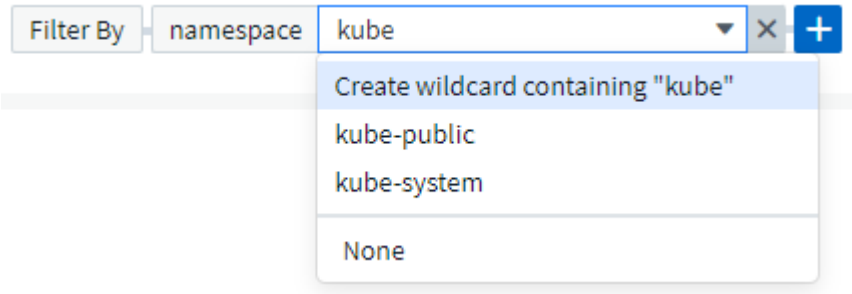
Die Cloud Insights-Erfassungseinheit unterstützt zusätzlich zu den bereits unterstützten Betriebssystemen die folgenden Betriebssysteme:

- CentOS (64 Bit) 8.4
- Oracle Enterprise Linux (64 Bit) 8.4
- Red hat Enterprise Linux (64-Bit) 8.4

Oktober 2021

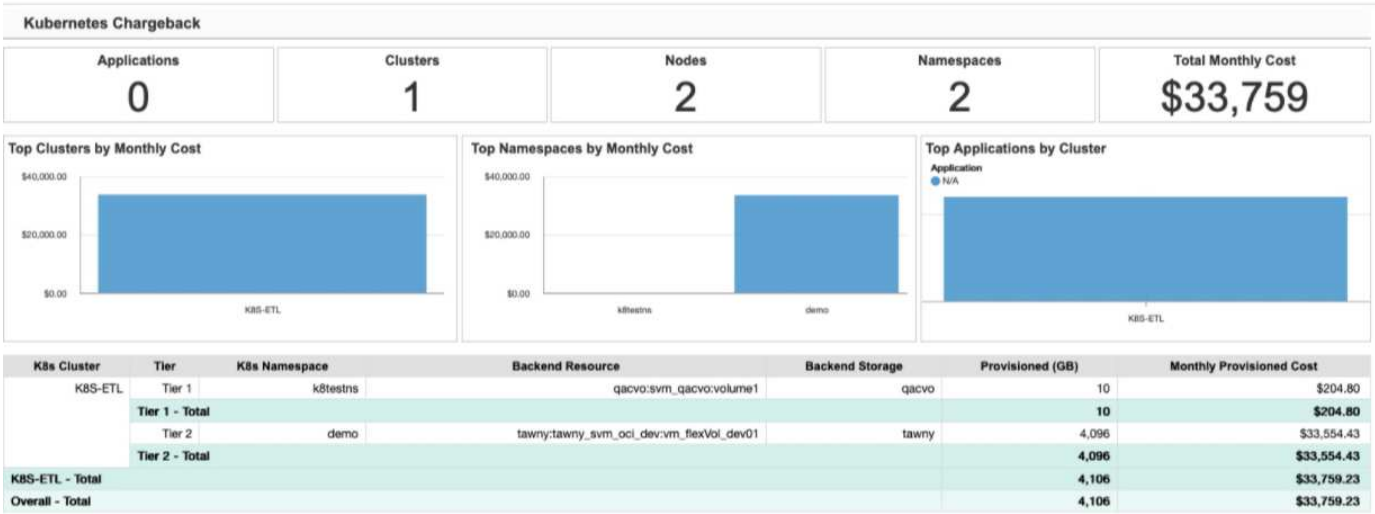
Filter auf K8S Explorer-Seiten

"Kubernetes Explorer" Mit Seitenfiltern können Sie die angezeigten Daten für Ihre Kubernetes-Cluster, Nodes und POD-Exploration im Fokus haben.



K8s-Daten für die Berichterstellung

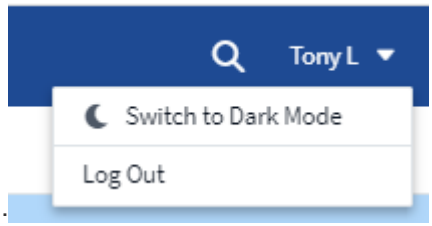
Kubernetes-Daten können jetzt in Reporting verwendet werden. Damit können Sie Chargeback oder andere Berichte erstellen. Damit Kubernetes-Kostenzuordnungsdaten an die Berichterstellung weitergeleitet werden können, ist eine aktive Verbindung zu erforderlich. Cloud Insights muss Daten von Ihrem Kubernetes-Cluster und dem Back-End-Storage erhalten. Wenn vom Back-End-Storage keine Daten empfangen werden, kann Cloud Insights Kubernetes-Objektdaten nicht an die Berichterstellung senden.



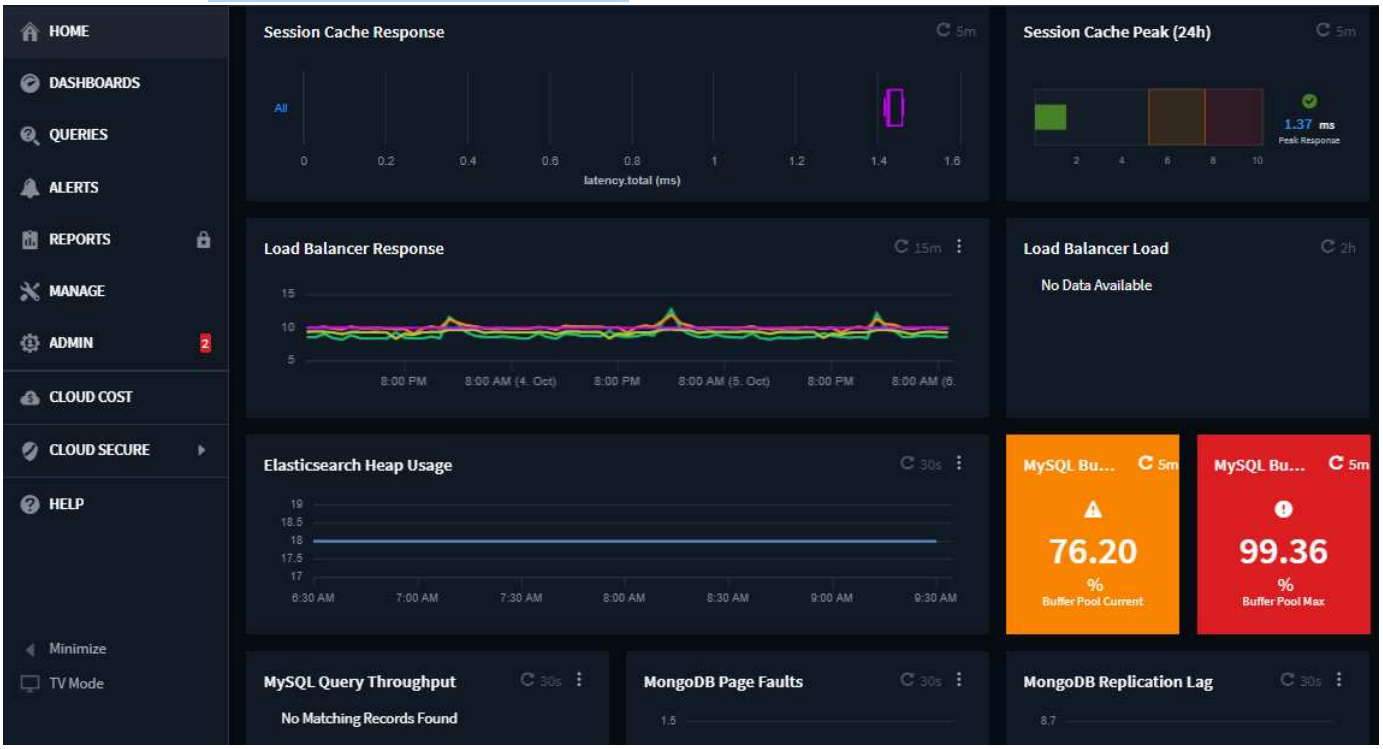
K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

Dunkles Thema ist angekommen

Viele von euch baten um ein dunkles Thema, und Cloud Insights hat geantwortet. Um zwischen hellen und dunklen Themen zu wechseln, klicken Sie auf das Dropdown-Menü neben Ihrem



Benutzernamen.



Data Collector-Unterstützung

Wir haben einige Verbesserungen bei Cloud Insights-Datensammlern vorgenommen. Hier einige Highlights:

- Neuer Kollektor für Amazon FSX für ONTAP

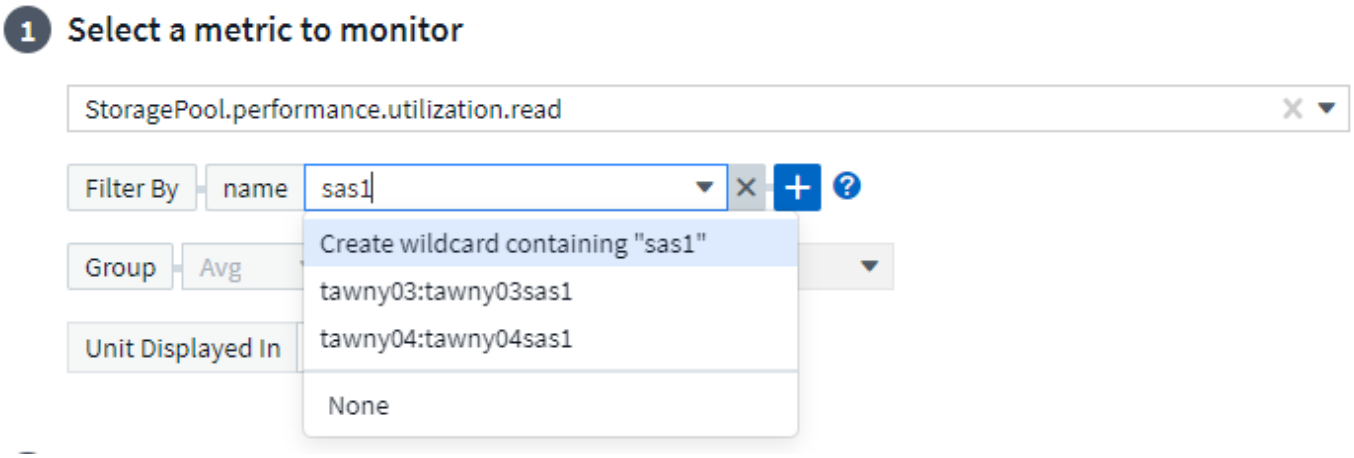
September 2021

Performancerichtlinien werden jetzt überwacht

Überwachung und Warnmeldungen haben Performance-Richtlinien und Verstöße im gesamten Cloud Insights ersetzt. "Warnfunktionen mit Monitoren" Sie erhalten mehr Flexibilität und einen besseren Einblick in potenzielle Probleme oder Trends in Ihrer Umgebung.

Automatische Fertigstellung von Vorschlägen, Wildcards und Ausdrücken in Monitoren

Wenn Sie einen Monitor für Warnungen erstellen, ist das Eingeben eines Filters jetzt vorausschauend, damit Sie ganz einfach nach Metriken oder Attributen Ihres Monitors suchen und diese finden können. Zusätzlich haben Sie die Möglichkeit, basierend auf dem von Ihnen angegebenen Text einen Platzhalter-Filter zu erstellen.



Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf Version **1.19.3** aktualisiert, mit Verbesserungen bei Leistung und Sicherheit. Benutzer, die eine Aktualisierung durchführen möchten, können sich im entsprechenden Abschnitt zur Aktualisierung des s informieren "Agenteninstallation" Dokumentation. Frühere Versionen des Agenten funktionieren weiterhin, ohne dass eine Benutzeraktion erforderlich ist.

Data Collector-Unterstützung

Wir haben einige Verbesserungen bei Cloud Insights-Datensammlern vorgenommen. Hier einige Highlights:

- Microsoft Hyper-V Collector verwendet jetzt PowerShell statt WMI
- Azure VMs und VHD Collector sind nun bis zu 10-mal schneller, da parallele Anrufe auch möglich sind
- HPE Nimble unterstützt jetzt föderierte und iSCSI-Konfigurationen

Und da wir immer verbessern Datensammlung, hier sind einige andere neue Änderungen der Anmerkung:

- Neuer Collector für EMC PowerStore
- Neuer Collector für Hitachi Ops Center
- Neuer Collector für Hitachi Content Platform
- Erweiterter ONTAP Collector zur Erstellung von Fabric Pools
- Verbesserter ANF mit Storage-Pool und Volume-Performance
- Erweitertes EMC ECS mit Speicherknoten und Speicherleistung sowie der Objektanzahl in Buckets
- Verbesserte EMC Isilon mit Storage-Knoten und Qtree-Kennzahlen
- Verbessertes EMC Symetrix mit Volume-QOS-Limits
- Verbesserte IBM SVC und EMC PowerStore mit der übergeordneten Seriennummer der Speicherknoten

August 2021

Neue Benutzeroberfläche Der Überwachungsseite

Der "Audit-Seite" Bietet eine übersichtlichere Schnittstelle und ermöglicht jetzt den Export von Audit-Ereignissen in .CSV-Datei.

Verbessertes Benutzerrollenmanagement

Cloud Insights bietet jetzt noch mehr Freiheit beim Zuweisen von Benutzerrollen und Zugriffskontrollen. Benutzern können nun granulare Berechtigungen für Monitoring, Berichterstellung und Cloud Secure separat zugewiesen werden.

Das bedeutet, dass Sie mehr Benutzern administrativen Zugriff auf Monitoring-, Optimierungs- und Reporting-Funktionen gewähren und gleichzeitig den Zugriff auf Ihre sensiblen Cloud Secure Audit- und Aktivitätsdaten nur auf diejenigen beschränken können, die sie benötigen.

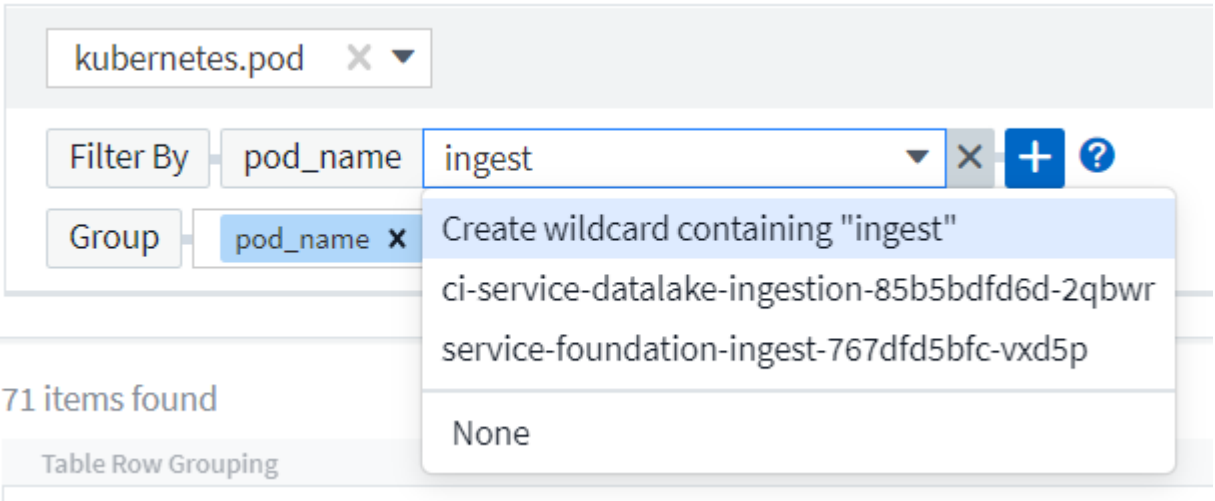
"Erfahren Sie mehr darüber" Über die verschiedenen Zugriffsebenen in der Cloud Insights-Dokumentation.

Juni 2021

Machen Sie Vorschläge, Wildcards und Ausdrücke in Filtern automatisch fertig

Mit dieser Version von Cloud Insights müssen Sie nicht mehr alle möglichen Namen und Werte kennen, nach denen Sie in einer Abfrage oder einem Widget filtern können. Beim Filtern können Sie einfach mit der Eingabe beginnen, und Cloud Insights schlägt Werte basierend auf Ihrem Text vor. Nicht mehr im Voraus nach Anwendungsnamen oder Kubernetes-Attributen suchen, nur um diejenigen zu finden, die in Ihrem Widget angezeigt werden sollen.

Wenn Sie einen Filter eingeben, zeigt der Filter eine intelligente Ergebnisliste an, aus der Sie auswählen können, sowie die Option, basierend auf dem aktuellen Text einen **Platzhalterfilter** zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse angezeigt, die dem Platzhalterausdruck entsprechen. Sie können natürlich auch mehrere einzelne Werte auswählen, die Sie dem Filter hinzufügen möchten.



Zusätzlich können Sie **Expressions** in einem Filter mit NOT oder oder erstellen, oder Sie können die Option

"Keine" auswählen, um nach Null-Werten im Feld zu filtern.

Weitere Informationen "Filteroptionen" In Abfragen und Widgets.

APIs von Edition erhältlich

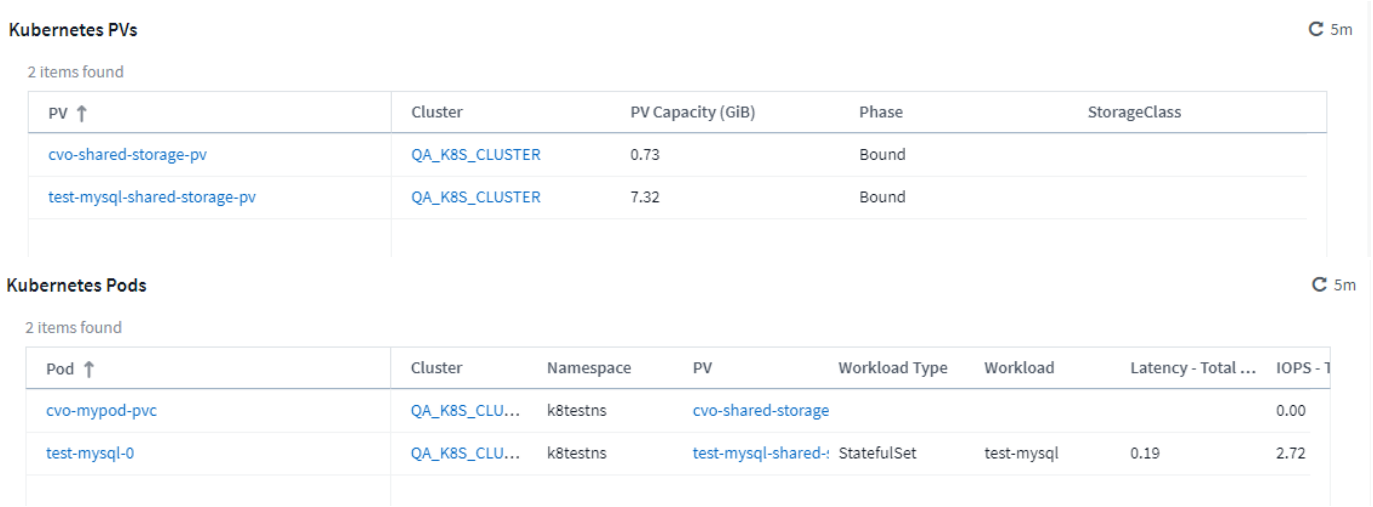
Die leistungsstarken APIs von Cloud Insights sind besser zugänglich als je zuvor. Alerts APIs sind jetzt in Standard- und Premium-Editionen verfügbar. Für jede Edition stehen folgende APIs zur Verfügung:

API-Kategorie	Basic	Standard	Premium
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Meldungen		✔	✔
Ressourcen		✔	✔
Datenaufnahme		✔	✔

Sichtbarkeit durch Kubernetes PV und Pod

Cloud Insights bietet einen Einblick in den Back-End Storage für Ihre Kubernetes-Umgebungen und gibt Ihnen einen Einblick in die Kubernetes Pods und PVS (Persistent Volumes). Sie können nun PV-Zähler wie IOPS, Latenz und Durchsatz von der Nutzung eines einzelnen Pods über einen PV-Zähler zu einem PV und bis zum Back-End-Speichergerät verfolgen.

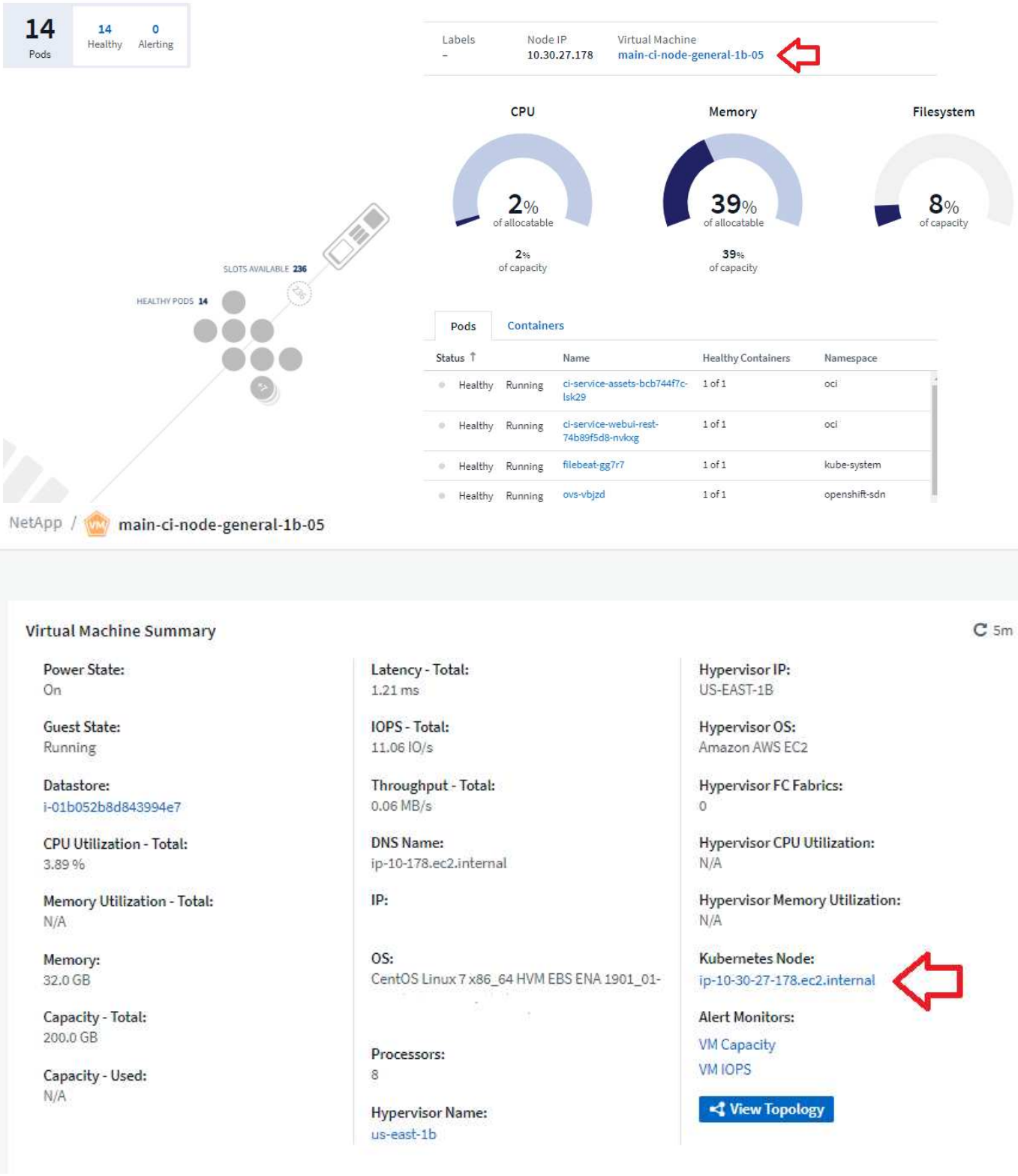
Auf einer Landing Page des Volume oder des internen Volume werden zwei neue Tabellen angezeigt:



Um die Vorteile dieser neuen Tabellen zu nutzen, wird empfohlen, Ihren aktuellen Kubernetes Agent zu deinstallieren und neu zu installieren. Sie müssen auch Kube-State-Metrics Version 2.1.0 oder höher installieren.

Kubernetes Node zu VM-Links

Sie können jetzt auf einer Kubernetes Node-Seite klicken, um die VM-Seite des Node zu öffnen. Die VM-Seite enthält auch einen Link zurück zum Node selbst.



Warnmeldungsüberwachung Ersetzen von Leistungsrichtlinien

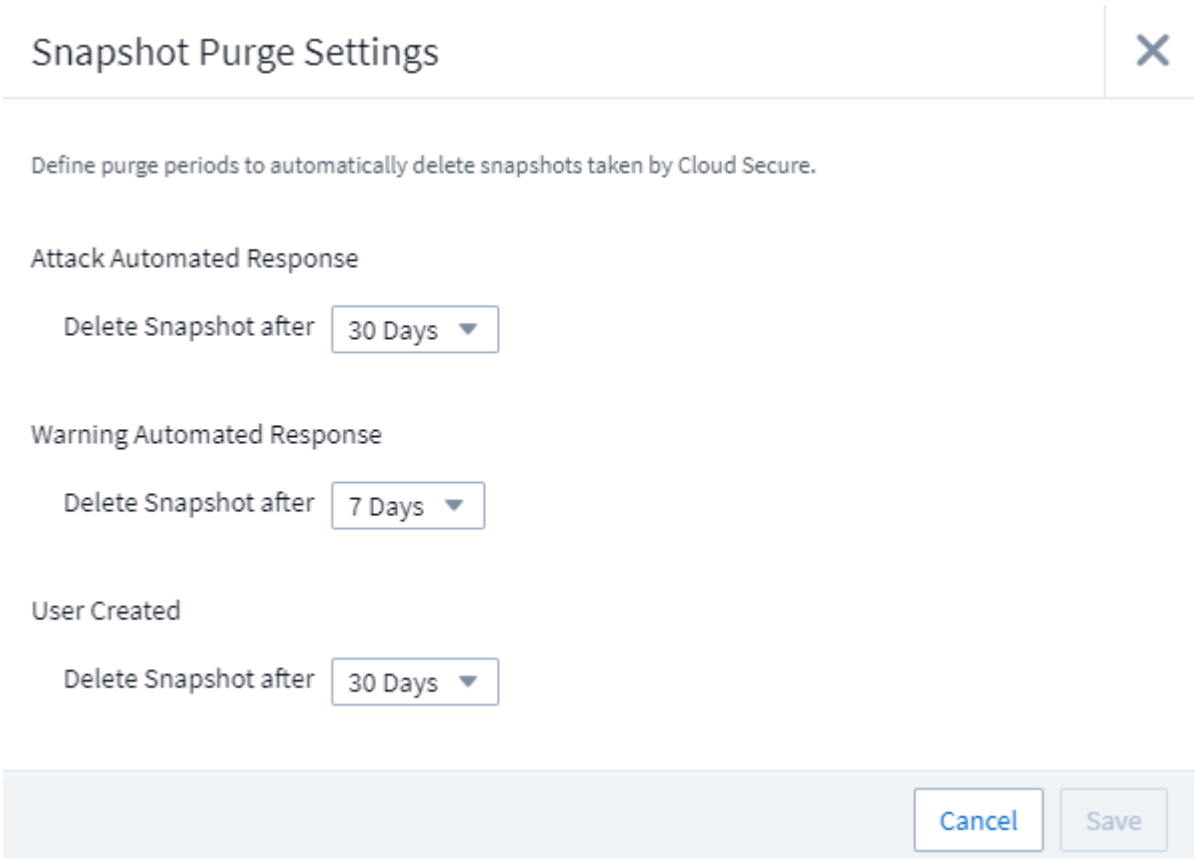
Um die zusätzlichen Vorteile mehrerer Schwellenwerte, Webhook- und E-Mail-Alarmauslieferung, Warnungen auf allen Kennzahlen über eine einzige Schnittstelle zu ermöglichen, wird Cloud Insights in den Monaten Juli und August 2021 Standard- und Premium Edition-Kunden von **Leistungsrichtlinien** in **Monitore** konvertieren. Weitere Informationen zu "Meldungen und Monitoring", Und bleiben Sie auf diesem spannenden Wandel abgestimmt.

Cloud Secure unterstützt NFS

Cloud Secure unterstützt jetzt die Datenerfassung per NFS für ONTAP. Schützen Sie Ihre Daten vor Ransomware-Angriffen durch SMB- und NFS-Benutzerzugriff. Darüber hinaus unterstützt Cloud Secure Active-Directory- und LDAP-Benutzerverzeichnisse zur Erfassung von NFS-Benutzerattributen.

Löschen von Cloud Secure Snapshots

Cloud Secure löscht automatisch Snapshots auf Basis der Einstellungen zum Löschen von Snapshots. So wird Speicherplatz eingespart und die Notwendigkeit zum manuellen Löschen von Snapshots verringert.



Geschwindigkeit der Cloud Secure Datenerfassung

Ein einzelnes Datensammler-Agent-System kann jetzt bis zu 20,000 Ereignisse pro Sekunde auf Cloud Secure posten.

Mai 2021

Im Folgenden einige Änderungen, die wir im April vorgenommen haben:

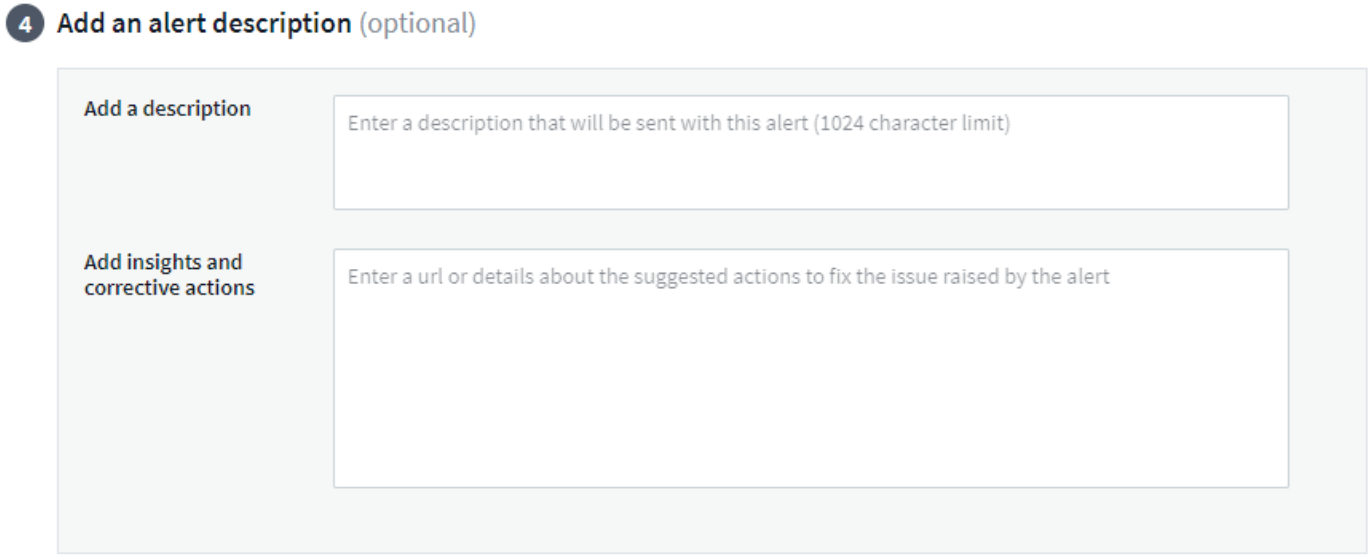
Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf Version 1.17.3 aktualisiert, mit Verbesserungen bei Leistung und Sicherheit. Benutzer, die eine Aktualisierung durchführen möchten, können sich im entsprechenden Abschnitt zur Aktualisierung des s informieren "Agenteninstallation" Dokumentation.

Frühere Versionen des Agenten funktionieren weiterhin, ohne dass eine Benutzeraktion erforderlich ist.

Fügen Sie Korrekturmaßnahmen zu einem Alarm hinzu

Sie können jetzt eine optionale Beschreibung sowie zusätzliche Erkenntnisse und/oder Korrekturmaßnahmen hinzufügen, wenn Sie einen Monitor erstellen oder ändern, indem Sie den Abschnitt **Alarmbeschreibung hinzufügen** ausfüllen. Die Beschreibung wird mit der Warnmeldung gesendet. Das Feld *insights and Corrective Actions* enthält ausführliche Schritte und Anleitungen zum Umgang mit Warnmeldungen und wird im Übersichtsbereich der Landing Page für Meldungen angezeigt.



Cloud Insights APIs für alle Editionen

API-Zugriff ist jetzt in allen Editionen von Cloud Insights verfügbar. Benutzer der Basic Edition können nun Aktionen für Erfassungseinheiten und Datensammler automatisieren, und Standard Edition Benutzer können Metriken abfragen und benutzerdefinierte Metriken erfassen. Die Premium Edition ermöglicht weiterhin die vollständige Nutzung aller API-Kategorien.

API-Kategorie	Basic	Standard	Premium
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Ressourcen		✔	✔
Datenaufnahme		✔	✔
Data Warehouse			✔

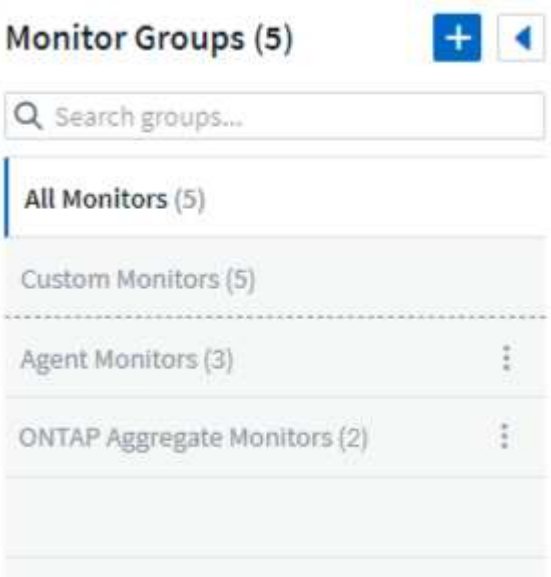
Details zur API-Verwendung finden Sie im "API-Dokumentation".

April 2021

Einfachere Verwaltung von Monitoren

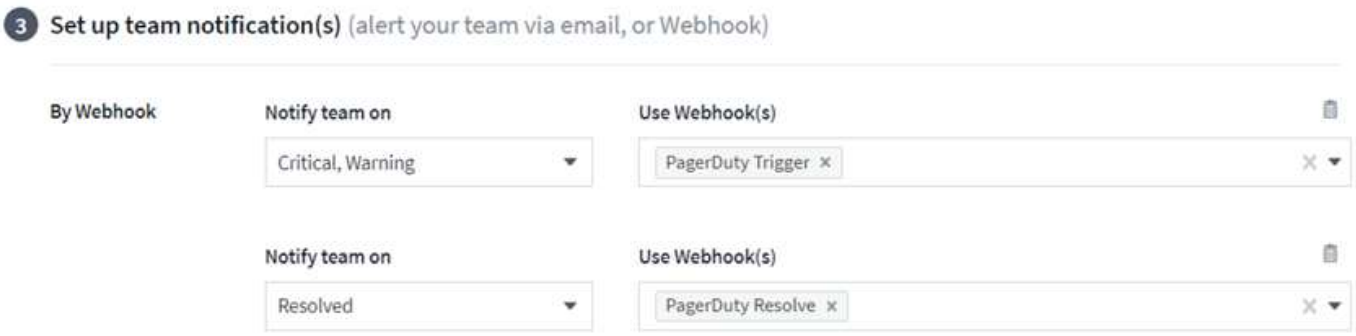
"Gruppierung Überwachen" Vereinfacht das Management von Monitoren in Ihrer Umgebung. Mehrere Monitore können jetzt zusammengefasst und als einen angehalten werden. Wenn beispielsweise ein Update zu einem Infrastruktur-Stack stattfindet, können Sie Warnmeldungen von allen diesen Geräten mit nur einem Klick unterbrechen.

Monitoring-Gruppen sind der erste Teil einer aufregenden neuen Funktion, die eine verbesserte Verwaltung von ONTAP-Geräten in Cloud Insights ermöglicht.



Erweiterte Alarmoptionen Mit Webhooks

Viele kommerzielle Anwendungen unterstützen "Webhaken" Als Standard-Eingangsschnittstelle. Cloud Insights unterstützt jetzt viele dieser Bereitstellungskanäle und stellt Standardvorlagen für Slack, PagerDuty, Teams und Discord zur Verfügung. Außerdem bietet er anpassbare generische Webhooks zur Unterstützung vieler anderer Anwendungen.



Verbesserte Geräteerkennung

Zur Verbesserung von Überwachung und Fehlerbehebung sowie zur Bereitstellung von präzisen Berichten ist es hilfreich, die Namen von Geräten zu verstehen und nicht ihre IP-Adressen oder andere Kennungen. Cloud Insights bietet jetzt eine automatische Möglichkeit, die Namen von Storage und physischen Hostgeräten in der Umgebung mit einem regelbasierten Ansatz zu identifizieren "* Geräteauflösung*", Im Menü * Verwalten* verfügbar.

Sie baten um mehr!

Eine beliebte Frage von Kunden war, dass es mehr Standardoptionen zur Visualisierung des Datenbereichs gibt. Daher haben wir die folgenden fünf neuen Optionen hinzugefügt, die nun über den Zeitbereich Picker im gesamten Service verfügbar sind:

- Letzte 30 Minuten
- Die Letzten 2 Stunden
- Letzte 6 Stunden
- Letzte 12 Stunden
- Letzte 2 Tage

Mehrere Abonnements in einer Cloud Insights-Umgebung

Ab dem 2. April unterstützt Cloud Insights für einen Kunden in einer einzelnen Cloud Insights-Instanz mehrere Abonnements desselben Edition-Typs. Kunden können so Teile ihres Cloud Insights Abonnements mit einem Infrastrukturkauf teilen. Wenden Sie sich an den NetApp Vertrieb, wenn Sie Unterstützung bei mehreren Abonnements benötigen.

Wählen Sie Ihren Pfad

Beim Einrichten von Cloud Insights können Sie nun entscheiden, ob Sie mit Monitoring und Alerting oder Ransomware und Insider Threat Detection beginnen möchten. Cloud Insights konfiguriert die Startumgebung auf der Grundlage des von Ihnen gewählten Pfads. Sie können den anderen Pfad jederzeit danach konfigurieren.

Einfachere Integration In Cloud Secure

Und der Einstieg in Cloud Secure ist leichter denn je, mit einer neuen Schritt-für-Schritt-Setup-Checkliste.

Wie immer hören wir gerne Ihre Vorschläge! Senden Sie sie an ng-cloudinsights-customerfeedback@netapp.com.

Februar 2021

Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf Version 1.17.0 aktualisiert, die Schwachstellen und Fehlerbehebungen umfasst.

Cloud Cost Analyse

Erleben Sie die Leistungsstärke von Spot by NetApp mit Cloud-Kosten. NetApp liefert eine detaillierte Kostenanalyse der vergangenen, aktuellen und geschätzten Ausgaben, die Ihnen Einblick in die Cloud-Nutzung in Ihrer Umgebung bietet. Die Cloud-Kostenkonsole bietet eine detaillierte Übersicht über die Cloud-Ausgaben und detaillierte Informationen zu einzelnen Workloads, Konten und Services.

Die Cloud-Kosten können die folgenden großen Herausforderungen bewältigen:

- Nachverfolgung und Überwachung Ihrer Cloud-Kosten
- Identifizierung von Abfall- und potenziellen Optimierungsbereichen
- Ausführbare Aktionselemente werden bereitgestellt

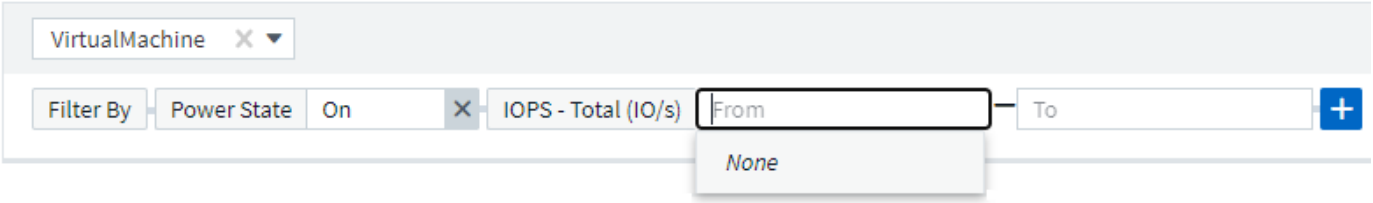
Cloud-Kosten konzentrieren sich auf Monitoring. Führen Sie ein Upgrade von NetApp Account an Spot durch, um automatische Kostenersparnisse und die Umgebung zu optimieren.

Abfrage nach Objekten mit Null-Werten unter Verwendung von Filtern

Cloud Insights ermöglicht jetzt die Suche nach Attributen und Metriken mit Null/keine Werten durch die Verwendung von Filtern. Sie können diese Filterung für alle Attribute/Metriken an folgenden Stellen durchführen:

- Auf der Seite Abfrage
- In Dashboard-Widgets und Seitenvariablen
- Auf der Liste „Meldungen“
- Beim Erstellen von Monitoren

Um nach Null/keine Werten zu filtern, wählen Sie einfach die Option *Keine* aus, wenn sie im entsprechenden Filter-Dropdown angezeigt wird.



Unterstützung In Mehreren Regionen

Ab heute bieten wir den Cloud Insights-Service in verschiedenen Regionen weltweit an, der für mehr Performance und mehr Sicherheit für Kunden außerhalb der USA sorgt. Cloud Insights/Cloud Secure speichert Informationen je nach Region, in der Ihre Umgebung erstellt wird.

Klicken Sie Auf "Hier" Finden Sie weitere Informationen.

Januar 2021

Zusätzliche ONTAP-Kennzahlen umbenannt

Im Rahmen unserer kontinuierlichen Bemühungen, die Effizienz des Datenerfassens aus ONTAP Systemen zu verbessern, wurden die folgenden ONTAP-Kennzahlen umbenannt.

Wenn Sie über vorhandene Dashboard-Widgets oder Abfragen mit einer dieser Kennzahlen verfügen, müssen Sie diese bearbeiten oder neu erstellen, um die neuen metrischen Namen verwenden zu können.

Vorheriger Metrischer Name	Neuer Metrischer Name
netapp_ontap.Disk_conentkomponente.total_Transfers	netapp_ontap.Disk_constituto.total_iops
netapp_ontap.Disk.total_Transfers	netapp_ontap.Disk.total_iops
netapp_ontap.fcp_lif.read_Data	netapp_ontap.fcp_lif.read_Throughput

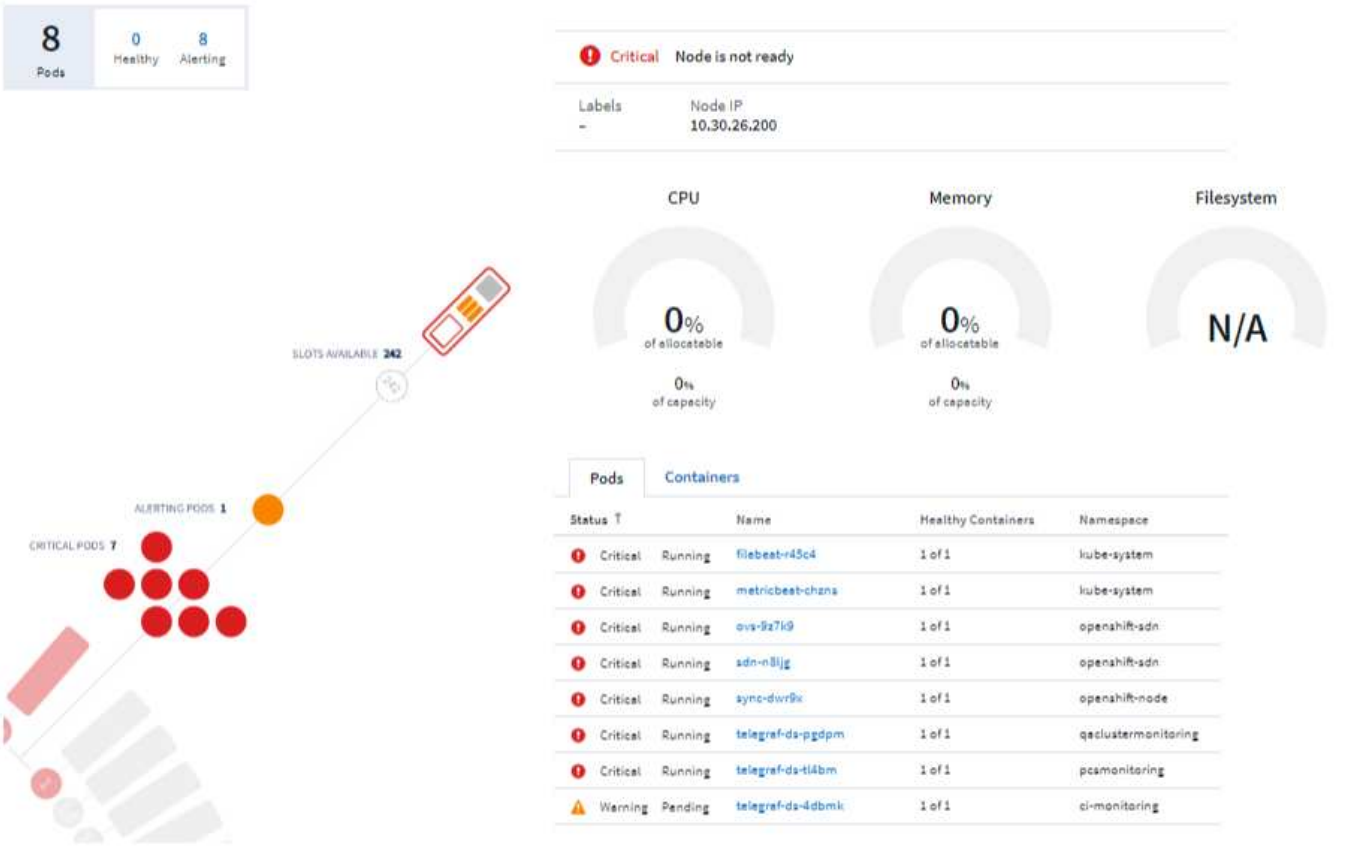
Vorheriger Metrischer Name	Neuer Metrischer Name
netapp_ontap.fcp_lif.write_Data	netapp_ontap.fcp_lif.write_Throughput
netapp_ontap.iscsi_lif.read_Data	netapp_ontap.iscsi_lif.read_Throughput
netapp_ontap.iscsi_lif.write_Data	netapp_ontap.iscsi_lif.write_Throughput
netapp_ontap.lif.recv_Data	netapp_ontap.lif.recv_Throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_Data	netapp_ontap.lun.read_Throughput
netapp_ontap.lun.write_Data	netapp_ontap.lun.Write_Throughput
netapp_ontap.nic_common.rx_Byte	netapp_ontap.nic_common.rx_Throughput
netapp_ontap.nic_common.tx_Bytes	netapp_ontap.nic_common.tx_Throughput
netapp_ontap.path.read_Data	netapp_ontap.path.read_Throughput
netapp_ontap.path.write_Data	netapp_ontap.path.write_Throughput
netapp_ontap.path.total_Data	netapp_ontap.path.total_Throughput
netapp_ontap.Policy_Group.read_Data	netapp_ontap.Policy_Group.read_Throughput
netapp_ontap.Policy_Group.write_Data	netapp_ontap.Policy_Group.write_Throughput
netapp_ontap.Policy_Group.other_Data	netapp_ontap.Policy_Group.other_Throughput
netapp_ontap.Policy_Group.total_Data	netapp_ontap.Policy_Group.total_Throughput
netapp_ontap.System_Node.Disk_Data_read	netapp_ontap.System_Node.Disk_Throughput_read
netapp_ontap.System_Node.Disk_Data_written	netapp_ontap.System_Node.Disk_Throughput_written
netapp_ontap.System_Node.hdd_Data_read	netapp_ontap.System_Node.hdd_Throughput_read
netapp_ontap.System_Node.hdd_Data_written	netapp_ontap.System_Node.hdd_Throughput_written
netapp_ontap.System_Node.ssd_Data_read	netapp_ontap.System_Node.ssd_Throughput_read
netapp_ontap.System_Node.ssd_Data_written	netapp_ontap.System_Node.ssd_Throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.System_Node.fcp_Data_rev	netapp_ontap.System_Node.fcp_Throughput_recv
netapp_ontap.System_Node.fcp_Data_sent	netapp_ontap.System_Node.fcp_Throughput_sent
netapp_ontap.Volume_Node.cifs_read_Data	netapp_ontap.Volume_Node.cifs_read_Throughput
netapp_ontap.Volume_Node.cifs_write_Data	netapp_ontap.Volume_Node.cifs_write_Throughput
netapp_ontap.Volume_Node.nfs_read_Data	netapp_ontap.Volume_Node.nfs_read_Throughput
netapp_ontap.Volume_Node.nfs_write_Data	netapp_ontap.Volume_Node.nfs_Write_Throughput
netapp_ontap.Volume_Node.iscsi_read_Data	netapp_ontap.Volume_Node.iscsi_read_Throughput
netapp_ontap.Volume_Node.iscsi_write_Data	netapp_ontap.Volume_Node.iscsi_Write_Throughput
netapp_ontap.Volume_Node.fcp_read_Data	netapp_ontap.Volume_Node.fcp_read_Throughput

Vorheriger Metrischer Name	Neuer Metrischer Name
netapp_ontap.Volume_Node.fcp_write_Data	netapp_ontap.Volume_Node.fcp_Write_Throughput
netapp_ontap.Volume.read_Data	netapp_ontap.Volume.read_Throughput
netapp_ontap.Volume.write_Data	netapp_ontap.Volume.write_Throughput
netapp_ontap.Workload.read_Data	netapp_ontap.Workload.read_Throughput
netapp_ontap.Workload.write_Data	netapp_ontap.Workload.Write_Throughput
netapp_ontap.Workload_Volume.read_Data	netapp_ontap.Workload_Volume.read_Throughput
netapp_ontap.Workload_Volume.write_Data	netapp_ontap.Workload_Volume.write_Throughput

Neuer Kubernetes Explorer

Der "Kubernetes Explorer" Bietet eine einfache Topologieansicht von Kubernetes-Clustern. So können selbst nicht-Experten Probleme und Abhängigkeiten schnell erkennen – von der Cluster-Ebene bis hin zu Container und Storage.

Mithilfe der Drill-Down-Details des Kubernetes Explorers können Sie zahlreiche Informationen zu Status, Verwendung und Zustand der Cluster, Nodes, Pods, Container und Storage in Ihrer Kubernetes-Umgebung untersuchen.



Dezember 2020

Vereinfachte Kubernetes-Installation

Die Installation von Kubernetes Agent wurde optimiert, damit weniger Benutzerinteraktionen erforderlich sind. "Installieren des Kubernetes Agent" Umfasst jetzt die Kubernetes-Datenerfassung.

November 2020

Zusätzliche Dashboards

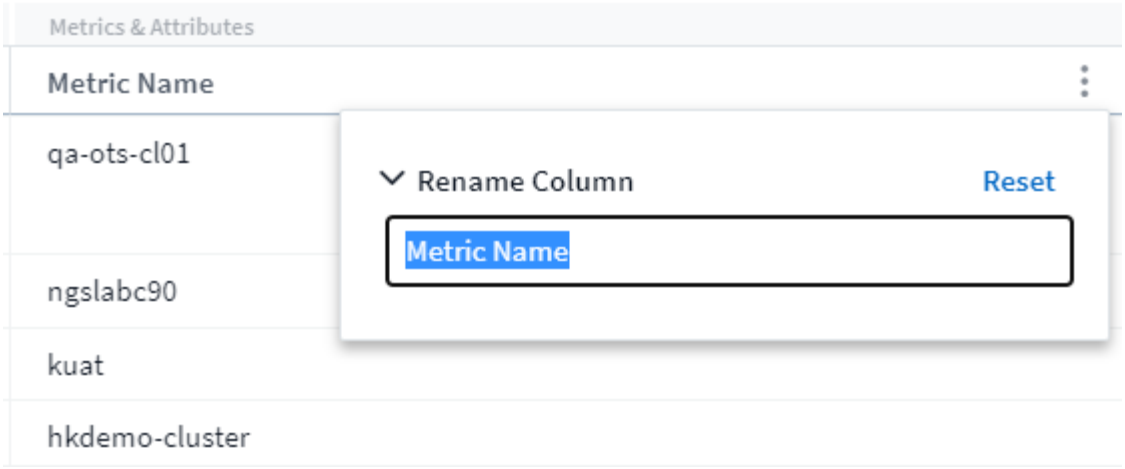
Die folgenden neuen Dashboards auf ONTAP wurden in die Galerie hinzugefügt und sind für den Import verfügbar:

- ONTAP: Aggregierte Performance und Kapazität
- ONTAP FAS/AFF – Kapazitätsauslastung
- ONTAP FAS/All Flash FAS – Cluster-Kapazität
- ONTAP FAS/ALL FLASH FAS – EFFIZIENZ
- ONTAP FAS/All Flash FAS – FlexVol-Performance
- ONTAP FAS/All Flash FAS – betriebliche/optimale Node-Punkte
- ONTAP FAS/All Flash FAS: Kapazitätseffizienz in Vorbereitung auf den Beitrag
- ONTAP: Netzwerkanschlussaktivität
- ONTAP: Performance der Node-Protokolle
- ONTAP: Node-Workload-Performance (Frontend)
- ONTAP: Prozessor
- ONTAP: SVM Workload-Performance (Frontend)
- ONTAP: Volume Workload Performance (Frontend)

Spaltenumbenennung in TabellenWidgets

Sie können Spalten im Abschnitt „*Metrics and Attributes*“ eines Tabellenwidgets umbenennen, indem Sie das Widget im Bearbeitungsmodus öffnen und oben in der Spalte auf das Menü klicken. Geben Sie den neuen Namen ein und klicken Sie auf *Save*, oder klicken Sie auf *Reset*, um die Spalte wieder auf den ursprünglichen Namen zu setzen.

Beachten Sie, dass sich dies nur auf den Anzeigenamen der Spalte im TabellenWidget auswirkt; der Name der Metrik/des Attributs ändert sich nicht in den zugrunde liegenden Daten selbst.



Oktober 2020

Standardmäßige Erweiterung der Integrationsdaten

Durch die Gruppierung von Tabellen-Widget können jetzt Standarderweiterungen für Kubernetes, erweiterte ONTAP-Daten und Agent-Node-Metriken vorgenommen werden. Wenn Sie beispielsweise Kubernetes *Nodes* von *Cluster* gruppieren, wird für jeden Cluster eine Zeile in der Tabelle angezeigt. Anschließend könnten Sie jede Cluster-Zeile erweitern, um eine Liste der Node-Objekte anzuzeigen.

Basic Edition: Technischer Support

Der technische Support steht ab sofort für Abonnenten der Cloud Insights Basic Edition sowie der Standard- und Premium-Editionen zur Verfügung. Darüber hinaus hat Cloud Insights den Workflow zur Erstellung eines NetApp Support-Tickets vereinfacht.

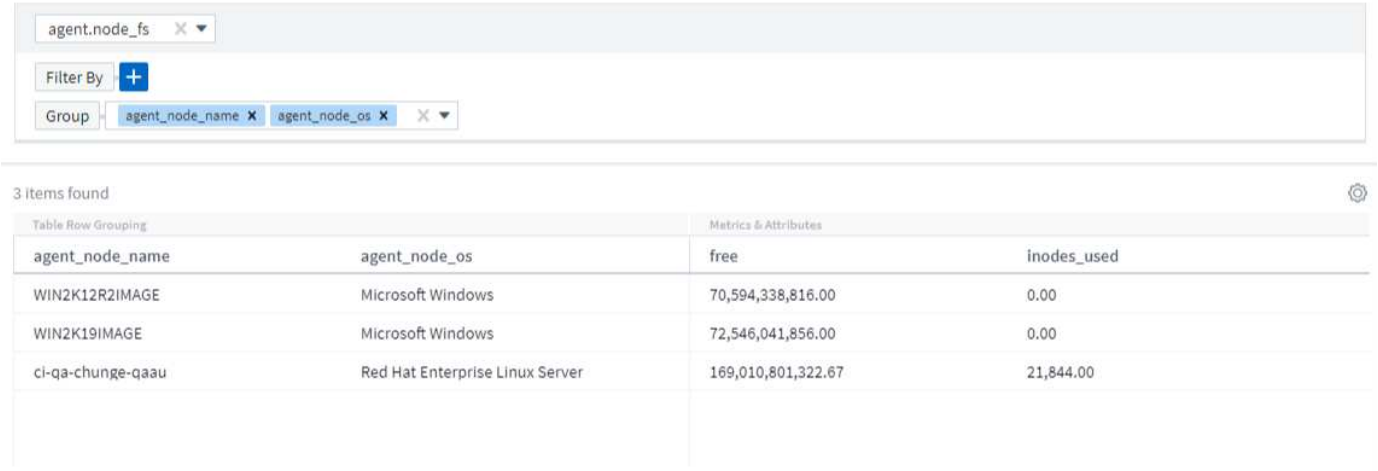
Öffentliche API von Cloud Secure

Cloud Secure unterstützt "Rest-APIs" Für den Zugriff auf Informationen zu Aktivitäten und Warnmeldungen. Dies geschieht mithilfe von API-Zugriffstoken, die über die Cloud Secure Admin-Benutzeroberfläche erstellt wurden und dann für den Zugriff auf DIE REST-APIs verwendet werden. Die Swagger-Dokumentation für diese REST-APIs ist in Cloud Secure integriert.

September 2020

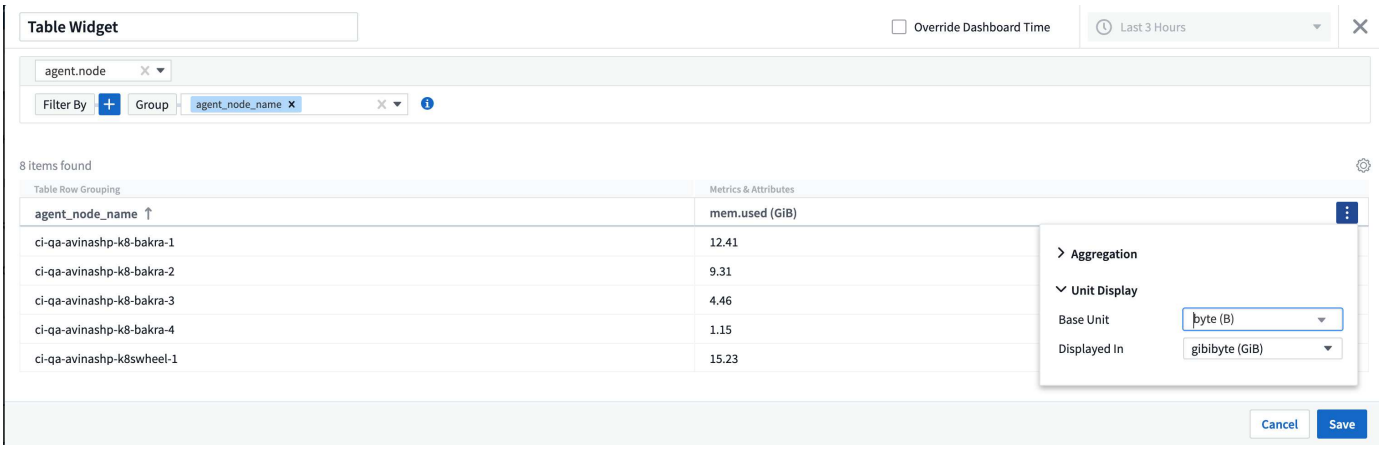
Seite mit Integrationsdaten abfragen

Die Seite „Cloud Insights Query“ unterstützt Integrationsdaten (z. B. von Kubernetes, erweiterten ONTAP Metriken usw.). Beim Arbeiten mit Integrationsdaten zeigt die Ergebnistabelle der Abfrage eine Ansicht „Split-Screen“ mit Objekt/Gruppierung auf der linken Seite und Objektdaten (Attribute/Metriken) auf der rechten Seite an. Sie können auch mehrere Attribute für die Gruppierung von Integrationsdaten auswählen.



Formatierung der Einheitenanzeige in TabellenWidget

Die Formatierung der Anzeige von Einheiten ist jetzt in den TabellenWidgets für Spalten verfügbar, in denen metrische/Zählerdaten angezeigt werden (z. B. Gigabyte, MB/Sekunde usw.). Um die Anzeigeeinheit einer Metrik zu ändern, klicken Sie in der Spaltenüberschrift auf das Menü „drei Punkte“ und wählen Sie „Anzeige der Einheit“. Sie können aus einer der verfügbaren Einheiten wählen. Die verfügbaren Einheiten variieren je nach Art der metrischen Daten in der Anzeigesäule.



Detailseite Der Erfassungseinheit

Akquisitionseinheiten verfügen nun über eine eigene Landing Page, die Ihnen nützliche Details für jede AU sowie Informationen zur Fehlerbehebung bietet. Der "AU Detailseite" Enthält Links zu Datensammlern der AU sowie hilfreiche Statusinformationen.

Die Abhängigkeit Von Cloud Secure Docker Wurde Entfernt

Die Abhängigkeit von Docker von Cloud Secure wurde entfernt. Docker wird für die Installation des Cloud Secure Agent nicht mehr benötigt.

Benutzerrollen Melden

Wenn Sie über Cloud Insights Premium Edition mit Reporting verfügen, verfügt jeder Cloud Insights-Benutzer in Ihrer Umgebung auch über eine SSO-Anmeldung bei der Reporting-Anwendung (d. h. Cognos); durch Klicken auf den Link **Berichte** im Menü werden sie automatisch bei Reporting angemeldet.

Die Benutzerrolle in Cloud Insights legt ihre fest "Benutzerrolle für die Berichterstellung":

Cloud Insights Rolle	Berichtsrolle	Reporting-Berechtigungen
Gast	Verbraucher	Es können Berichte angezeigt, geplant und erstellt sowie persönliche Einstellungen wie z. B. für Sprachen und Zeitzonen festgelegt werden. Verbraucher können keine Berichte erstellen oder administrative Aufgaben ausführen.
Benutzer	Autor	Kann alle Funktionen des Verbrauchers ausführen sowie Berichte und Dashboards erstellen und verwalten.
Verwalter	Verwalter	Kann alle Author-Funktionen sowie alle administrativen Aufgaben wie die Konfiguration von Berichten und das Herunterfahren und Neustarten von Reporting-Aufgaben ausführen.

Cloud Insights-Berichte sind für Umgebungen mit mindestens 500 MUs verfügbar.

Wenn Sie bereits Kunde von Premium Edition sind und Ihre Berichte behalten möchten, lesen Sie dies "Wichtiger Hinweis für Bestandskunden".

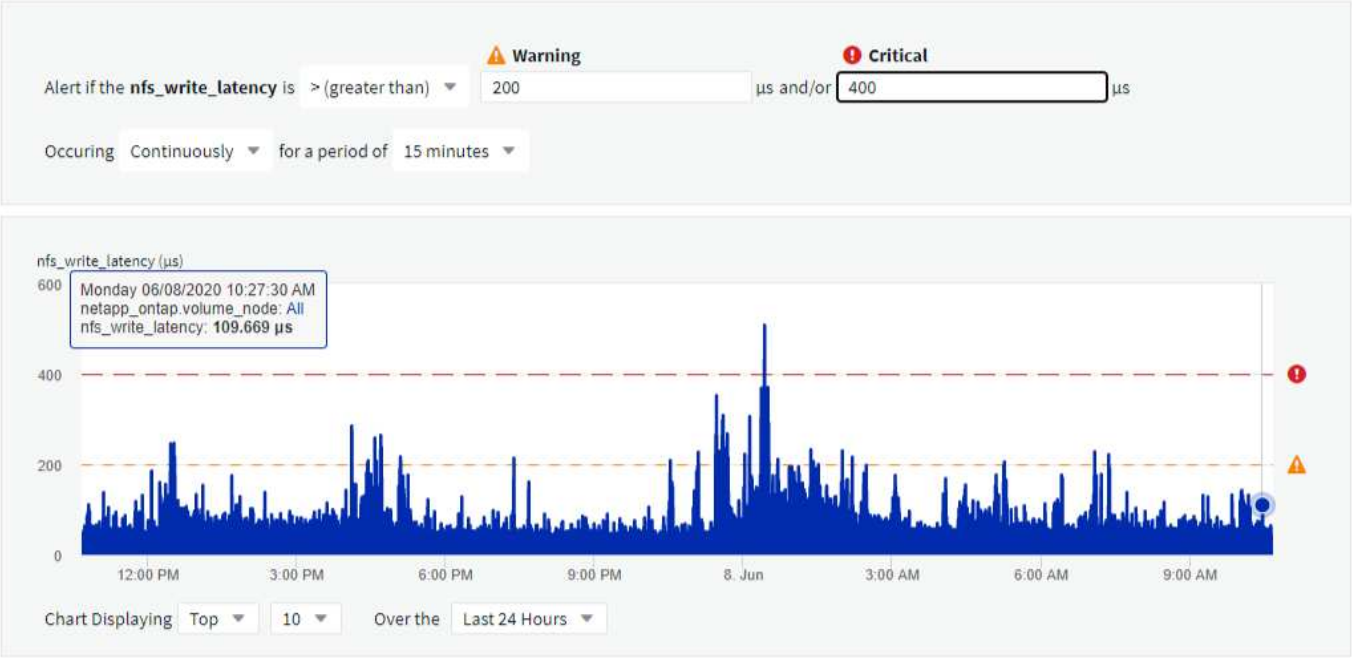
Neue API-Kategorie für die Datenaufnahme

Cloud Insights hat eine API-Kategorie mit **Datenaufnahme** hinzugefügt, die Ihnen eine bessere Kontrolle über benutzerdefinierte Daten und Agenten ermöglicht. Detaillierte Dokumentation zu dieser und anderen API-Kategorien finden Sie in Cloud Insights, indem Sie zu **Admin > API Access** navigieren und auf den Link *API Documentation* klicken. Sie können auch einen Kommentar an die AU im Feld Notiz anhängen, das auf der AU Detailseite sowie auf der AU-Listenseite angezeigt wird.

August 2020

Monitoring und Alarmfunktionen

Neben der derzeit festgelegten Performance-Richtlinien für Storage-Objekte, VMs, EC2 und Ports bietet Cloud Insights Standard Edition jetzt auch die Möglichkeit zur "Konfigurieren von Monitoren" Für Schwellenwerte über Integrationsdaten für Kubernetes, erweiterte Kennzahlen von ONTAP und Telegraf-Plug-ins. Sie erstellen einfach einen Monitor für jede Objektmetrik, die Sie Warnmeldungen auslösen, die Bedingungen für Schwellenwerte auf Warn- oder kritischen Ebene festlegen und die gewünschten E-Mail-Empfänger für jede Stufe angeben. Das können Sie dann "Anzeigen und Verwalten von Warnmeldungen" Um Trends zu verfolgen oder Probleme zu beheben.



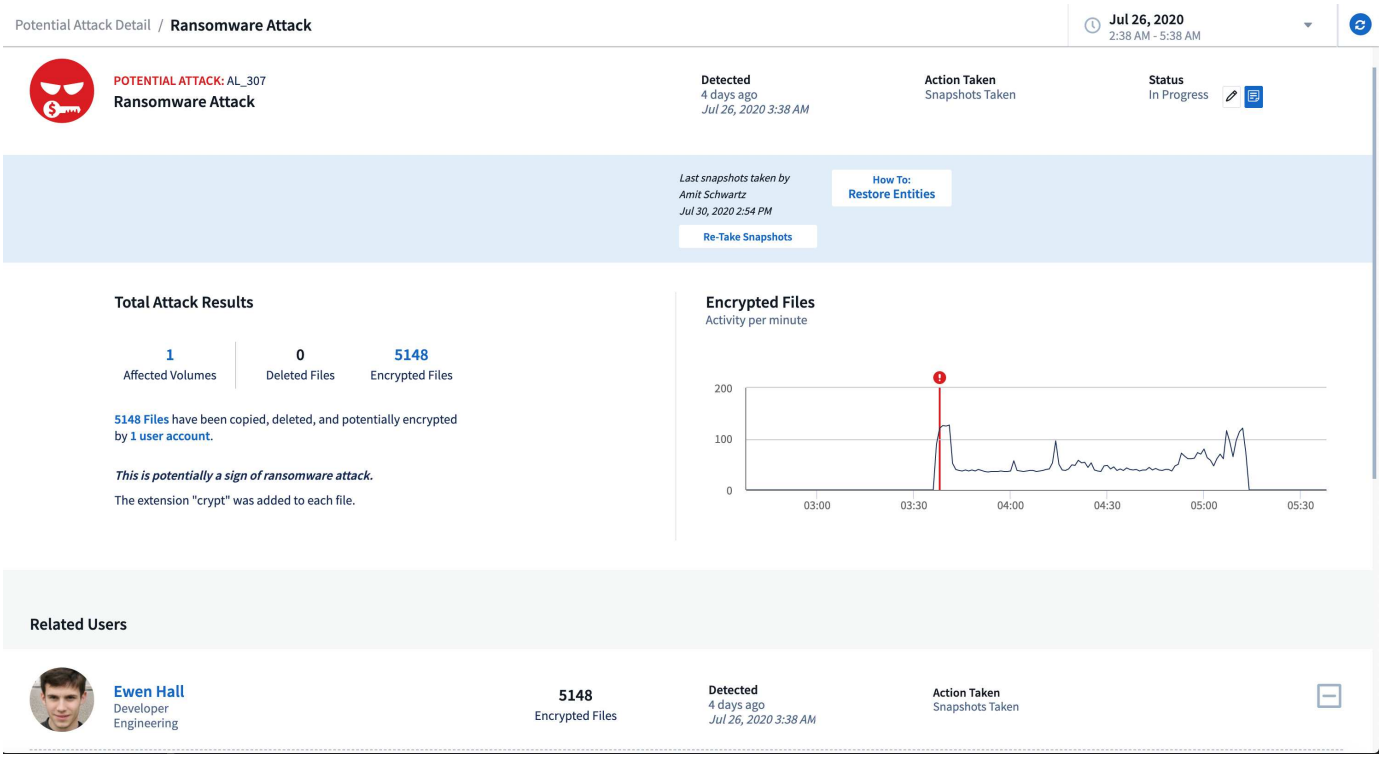
Juli 2020

Cloud Secure *Snapshot* Aktion starten

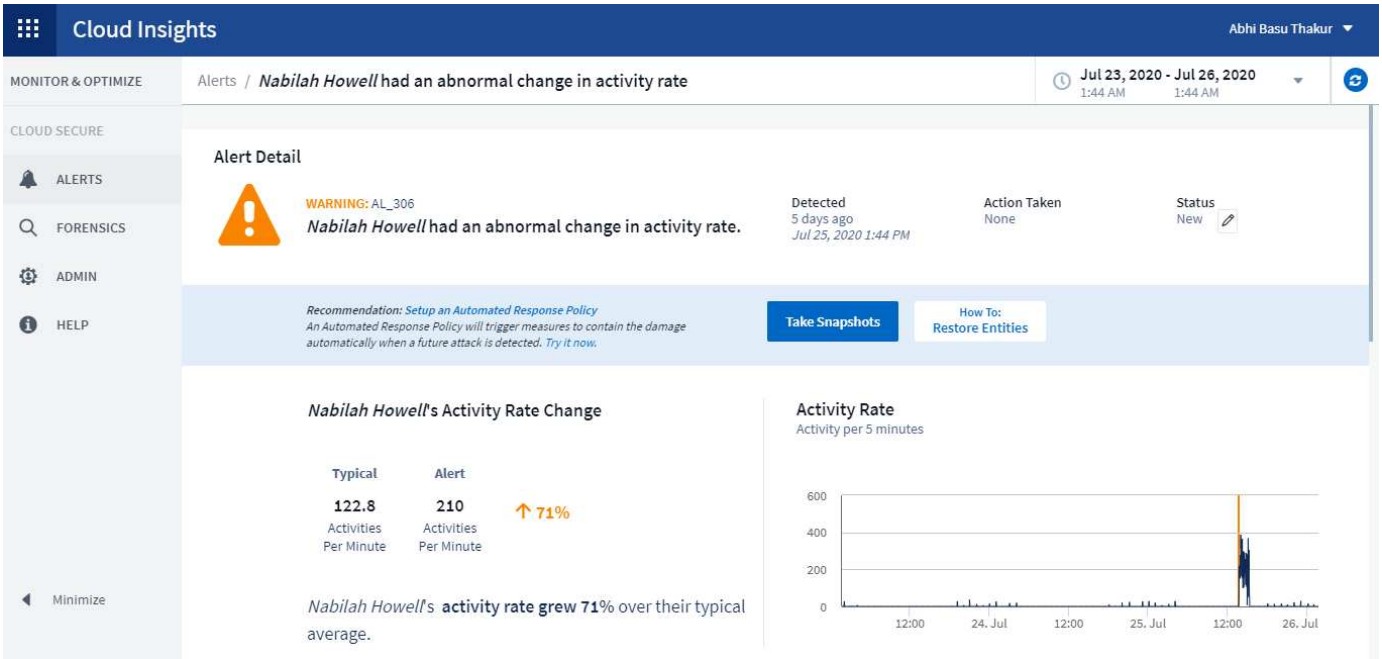
Cloud Secure schützt Ihre Daten, indem bei der Erkennung schädlicher Aktivitäten automatisch Snapshots erstellt werden. So wird sichergestellt, dass Ihre Daten sicher gesichert werden.

Sie können automatisierte Antwortrichtlinien festlegen, die einen Snapshot erstellen, wenn Ransomware-Angriff oder andere anormale Benutzeraktivitäten erkannt werden. Sie können einen Snapshot auch manuell von der Warnungsseite aus erstellen.

Automatische
Momentaufnahme:



Manuelle Momentaufnahme:



Aktualisierungen von Metrik/Zählzahlen

Die folgenden Kapazitätszähler sind für die Verwendung in der Cloud Insights-UI und DER REST-API verfügbar. Bisher waren diese Zähler nur für das Data Warehouse / Reporting verfügbar.

Objekttyp	Zähler
Storage	Kapazität - Spare Raw Capacity - Failed Raw

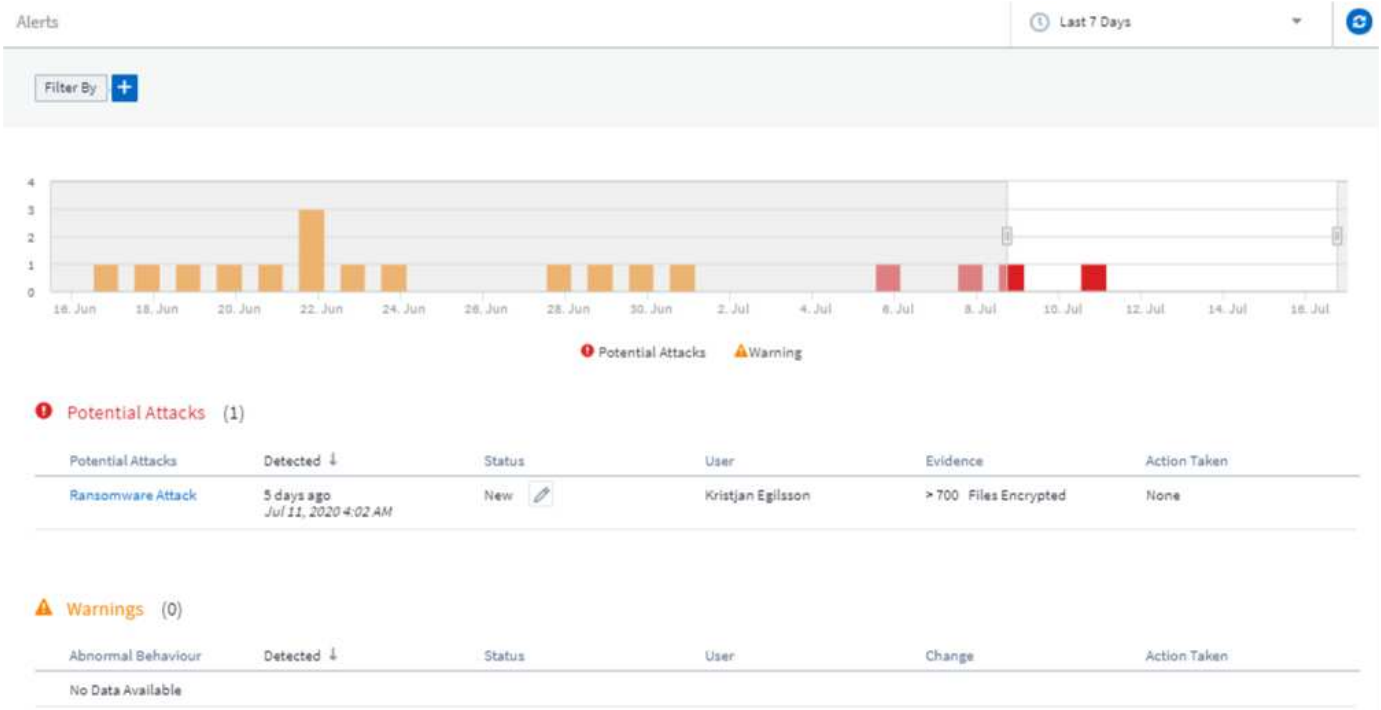
Objekttyp	Zähler
Storage-Pool	Datenkapazität - Genutzte Datenkapazität - Gesamte Sonstige Kapazität - Genutzte Sonstige Kapazität - Gesamtkapazität - Rohkapazität - Weiche Grenze
Internes Volumen	Datenkapazität - Verwendete Datenkapazität - Gesamte Sonstige Kapazität - Genutzte Andere Kapazität - Insgesamt Eingesparte Clone-Kapazität - Summe

Cloud Secure-Erkennung Potenzieller Angriffe

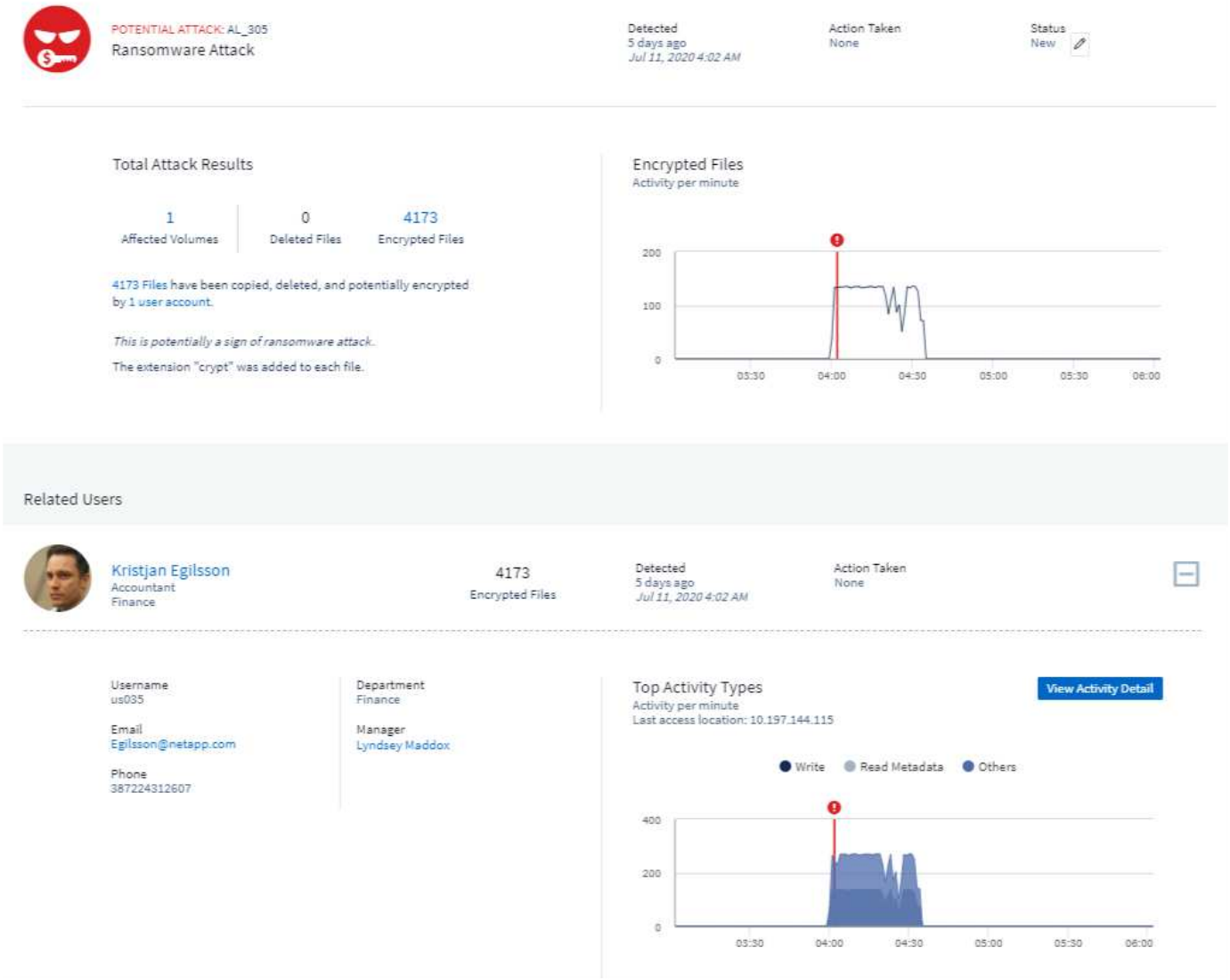
Cloud Secure erkennt jetzt potenzielle Angriffe wie Ransomware. Klicken Sie auf der Listenseite Meldungen auf eine Warnmeldung, um eine Detailseite mit den folgenden Informationen zu öffnen:

- Zeitpunkt des Angriffs
- Zugeordnete Benutzer- und Dateiaktivitäten
- Maßnahmen ergriffen
- Weitere Informationen, die Ihnen helfen, mögliche Sicherheitsverstöße nachzuverfolgen

Warneseite mit potenziellen Ransomware-Angriffen:



Detailseite zu potenziellen Ransomware-Angriffen:



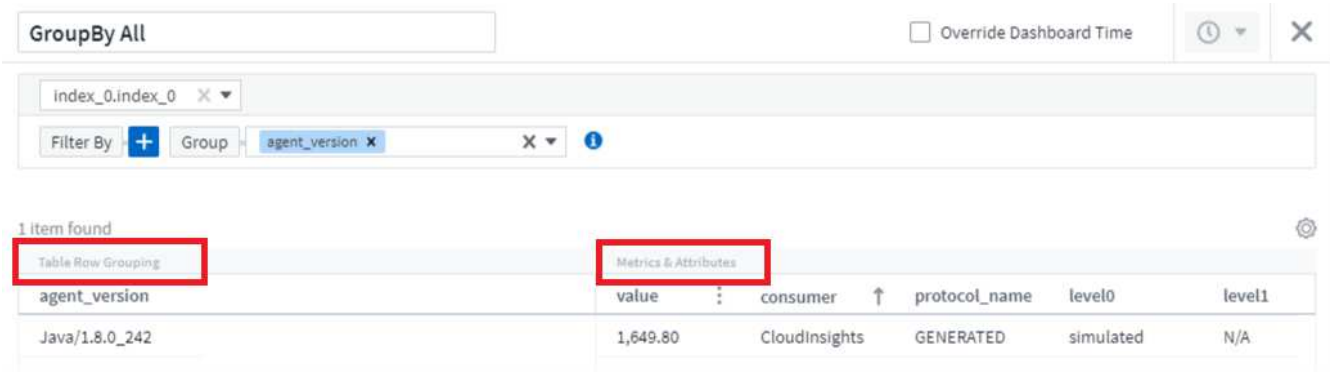
Abonnieren Sie Premium Edition über AWS

Können Sie während der Testversion von Cloud Insights "Self-Subscribe" AWS Marketplace für Cloud Insights Standard Edition oder Premium Edition. Bisher war es nur möglich, sich über AWS Marketplace eigenständig für Standard Edition anzumelden.

Erweitertes Tabellenwidget

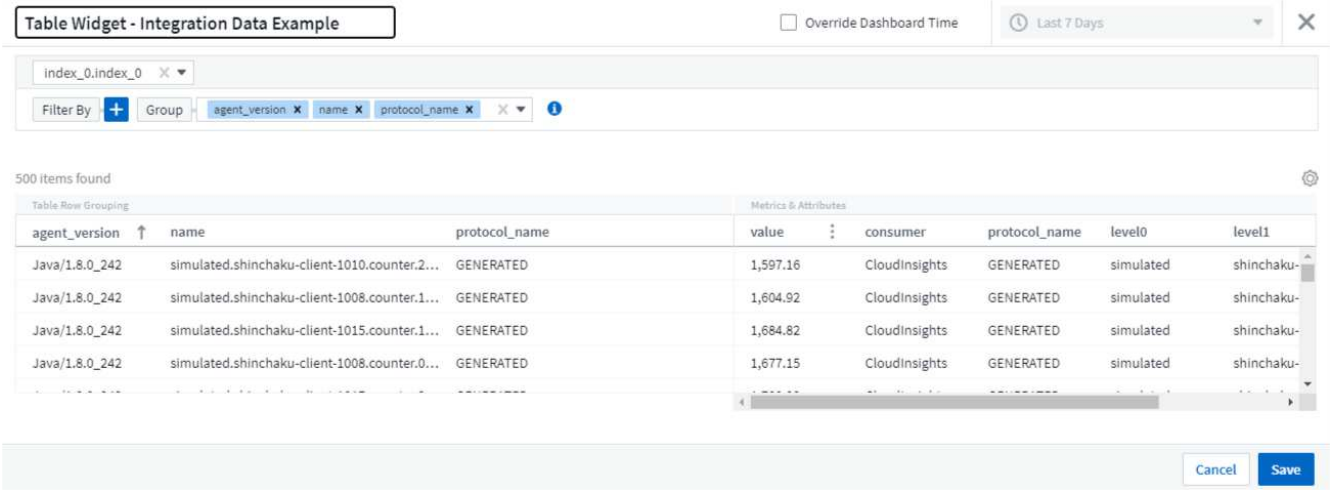
Das Widget „Dashboard/Asset Page Table“ umfasst die folgenden Verbesserungen:

- Ansicht "Split-Screen": Tabelle Widgets zeigen das Objekt/die Gruppierung auf der linken Seite und die Objektdaten (Attribute/Metriken) auf der rechten Seite an.



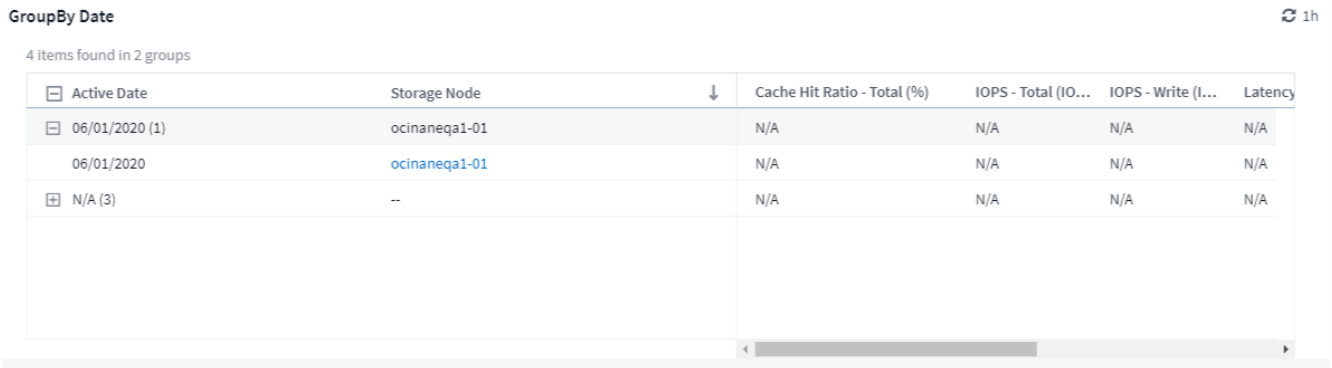
- Gruppierung mehrerer Attribute: Für Integrationsdaten (Kubernetes, ONTAP Advanced Metrics, Docker usw.) können mehrere Attribute zur Gruppierung ausgewählt werden. Die Daten werden entsprechend den Gruppierungsattributen angezeigt/ausgewählt.

  Gruppierung mit Integrationsdaten (dargestellt im Bearbeitungsmodus):



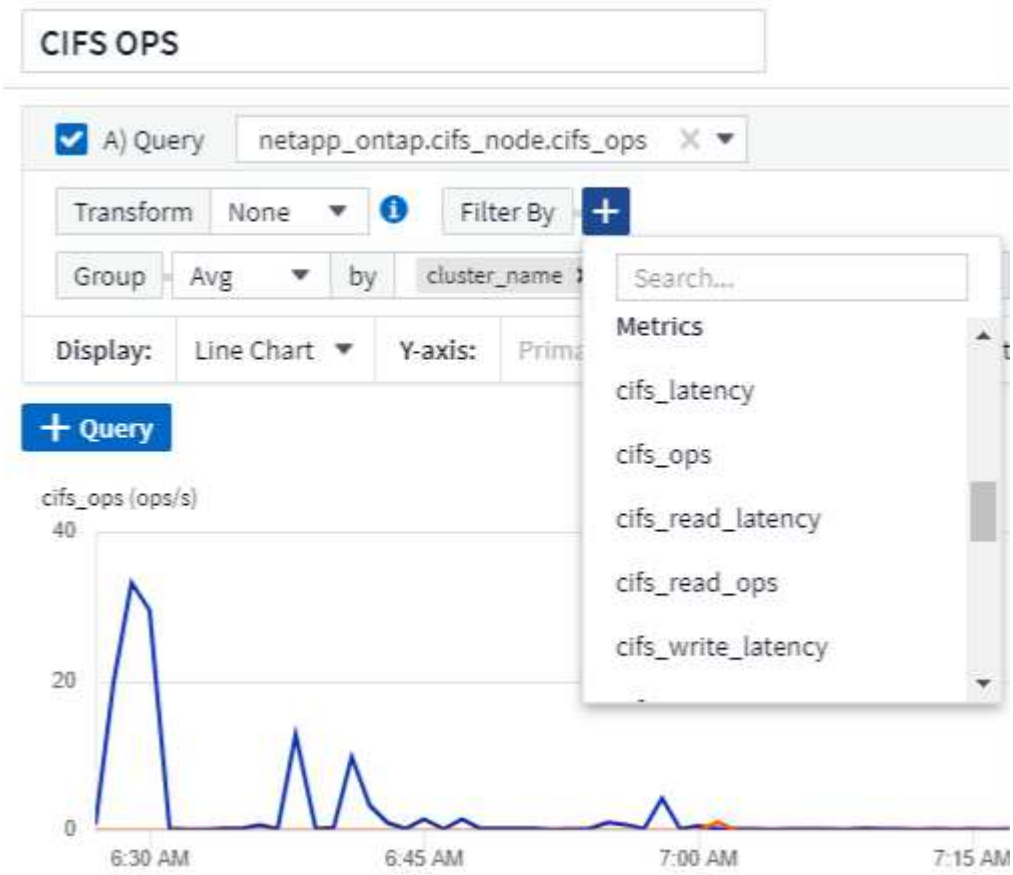
- Die Gruppierung von Infrastrukturdaten (Storage, EC2, VM, Ports usw.) erfolgt wie zuvor durch ein einzelnes Attribut. Wenn Sie nach einem Attribut gruppieren, das nicht das Objekt ist, können Sie in der Tabelle die Gruppenzeile erweitern, um alle Objekte in der Gruppe anzuzeigen.

  Gruppierung mit Infrastrukturdaten (im Anzeigemodus angezeigt):

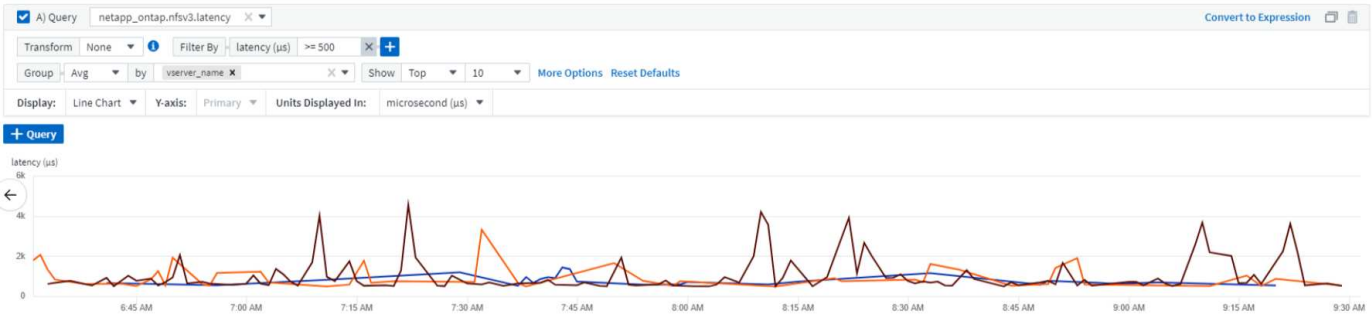


Filtern Von Metriken

Neben der Filterung von Objektattributen in einem Widget können Sie jetzt auch nach Metriken filtern.



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

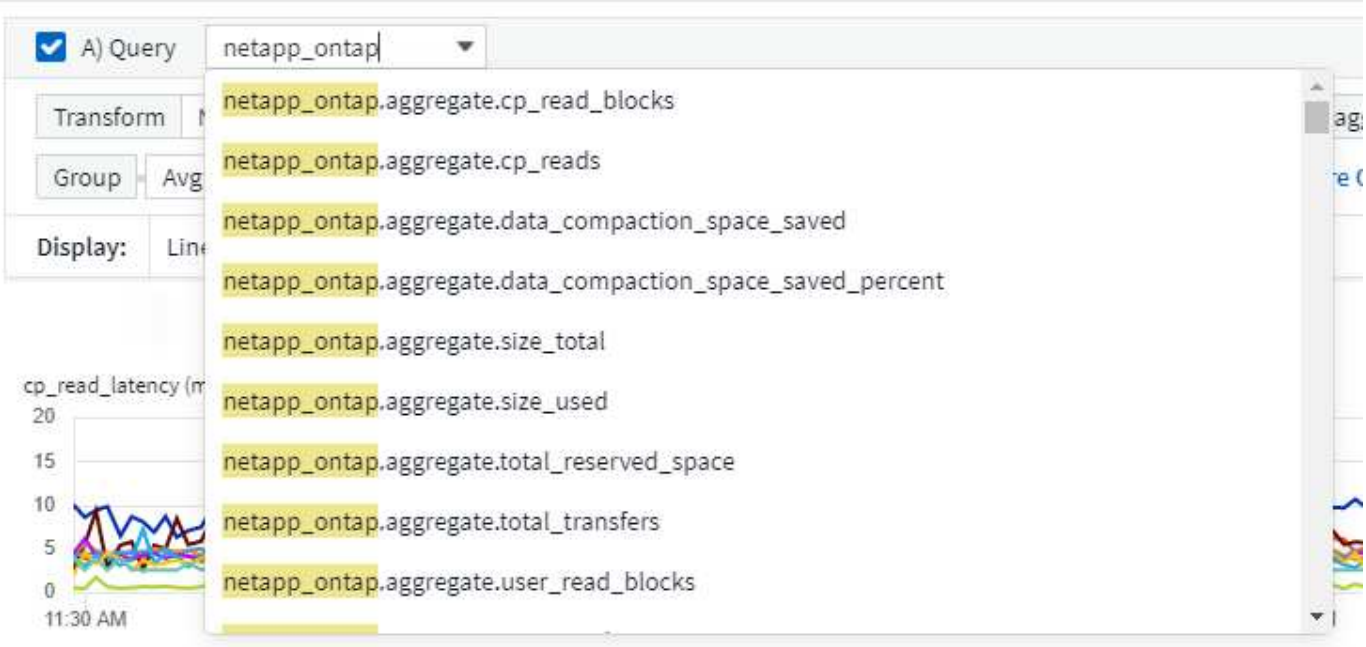


ONTAP Advanced Counter Data

Cloud Insights nutzt die ONTAP-spezifischen **Advanced Counter Data** von NetApp, die über eine Vielzahl von Zählern und Kennzahlen von ONTAP-Geräten erfasst werden. ONTAP Advanced Counter Data steht allen NetApp ONTAP Kunden zur Verfügung. Diese Kennzahlen ermöglichen eine individuelle und breit gefächerte Visualisierung in Cloud Insights Widgets und Dashboards.

ONTAP Advanced Counters finden Sie, indem Sie in der Widgets Abfrage nach „netapp_ontap“ suchen und

zwischen den Zählern auswählen.



Sie können Ihre Suche verfeinern, indem Sie zusätzliche Teile des Zählernamens eingeben. Beispiel:

- *Lif*
- *Aggregat*
- *Offbox_vscan_Server*
- Und vieles mehr

Bitte beachten Sie Folgendes:

- Die erweiterte Datensammlung wird standardmäßig für neue ONTAP-Datensammler aktiviert. Um die erweiterte Datensammlung für Ihre vorhandenen ONTAP-Datensammler zu aktivieren, bearbeiten Sie den Datensammler und erweitern Sie den Abschnitt *Erweiterte Konfiguration*.
- Die erweiterte Datenerfassung ist für ONTAP im 7-Mode nicht verfügbar.

Moderne Counter-Dashboards

Cloud Insights verfügt über eine Vielzahl an vordefinierten Dashboards, um Ihnen die Visualisierung erweiterter ONTAP-Zähler für Themen wie *Aggregate Performance*, *Volume Workload*, *Processor Activity* usw. zu erleichtern. Wenn mindestens ein ONTAP-Datensammler konfiguriert ist, können diese aus der Dashboard-Galerie auf einer beliebigen Dashboard-Listenseite importiert werden.

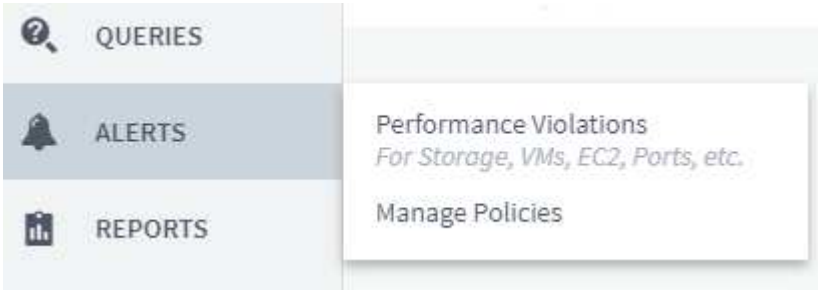
Weitere Informationen

Weitere Informationen zu erweiterten ONTAP Daten finden Sie unter folgenden Links:

- https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest (Hinweis: Sie müssen sich beim NetApp Support anmelden.)
- https://nabox.org/faq/

Menü „Richtlinien und Verstöße“

Performancerichtlinien und -Verstöße finden Sie jetzt im Menü **Alarme**. Funktionen für Richtlinien und Verstöße bleiben unverändert.



Telegraf Agent Aktualisiert

Der Agent für die Aufnahme von telegraf-Integrationsdaten wurde auf aktualisiert "Version 1.14", Die Bugs Fixes, Security Fixes und neue Plug-ins beinhaltet.

Hinweis: Wenn Sie einen Kubernetes Data Collector auf der Kubernetes-Plattform konfigurieren, wird möglicherweise ein Fehler „HTTP Status 403 Forbidden“ im Protokoll angezeigt, da die Berechtigungen im Attribut „clusterrole“ nicht ausreichen.

Um dieses Problem zu umgehen, fügen Sie dem Abschnitt *rules:* der clusterrolle für Endpunktzugriff folgende hervorgehobene Zeilen hinzu und starten Sie dann die Telegraf-Pods neu.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

Juni 2020

Vereinfachte Fehlerberichterstattung Für Data Collector

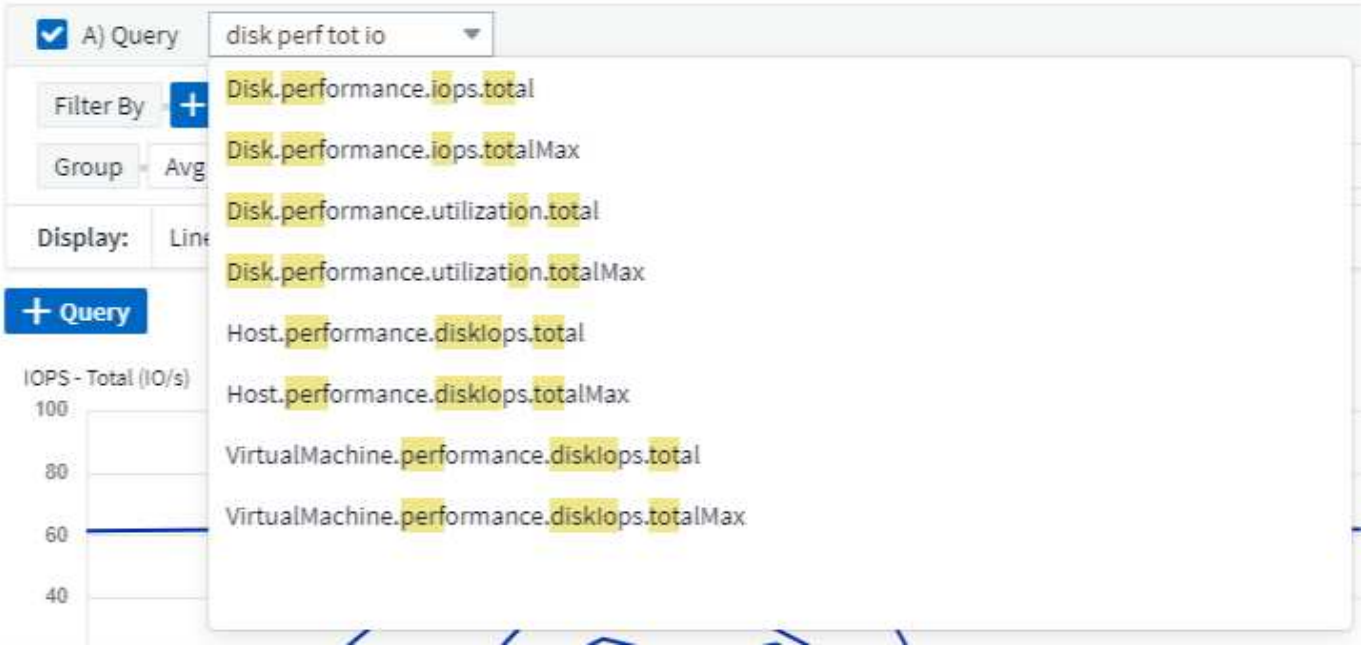
Die Meldung eines Datensammlungsfehlers ist mit der Schaltfläche *Fehlerbericht senden* auf der Seite Datensammler einfacher. Durch Klicken auf die Schaltfläche werden grundlegende Informationen zum Fehler an NetApp gesendet und eine Aufforderung zur Untersuchung des Problems angezeigt. Sobald Cloud Insights gedrückt wurde, bestätigt dieser NetApp eine entsprechende Benachrichtigung. Die Schaltfläche „Fehlerbericht“ ist deaktiviert, um anzugeben, dass ein Fehlerbericht für die entsprechende Datenerfassung gesendet wurde. Die Schaltfläche bleibt deaktiviert, bis die Browserseite aktualisiert wird.

Widget-Verbesserungen

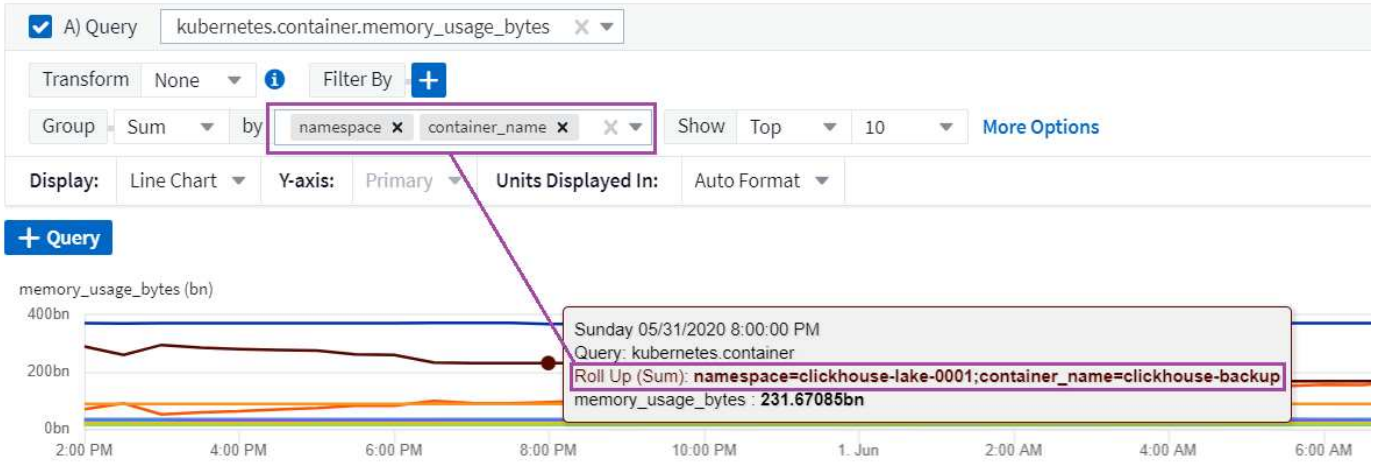
Die folgenden Verbesserungen wurden in Dashboard-Widgets vorgenommen: Diese Verbesserungen gelten als Vorschau-Funktionalität und stehen möglicherweise nicht für alle Cloud Insights-Umgebungen zur Verfügung.

- Neue Auswahl von Objekten/Kennzahlen: Objekte (Storage, Festplatte, Ports, Nodes usw.) und die zugehörigen Metriken (IOPS, Latenz, CPU-Anzahl usw.) stehen jetzt in einem Dropdown-Menü mit

umfassender Suchfunktion in Widgets zur Verfügung. Im Dropdown-Menü können Sie mehrere Teilbegriffe eingeben, und Cloud Insights führt alle Objektmetriken auf, mit denen diese Begriffe erfüllt werden.



- Gruppierung mehrerer Tags: Beim Arbeiten mit Integrationsdaten (Kubernetes, etc.) können Sie die Daten nach mehreren Tags/Attributen gruppieren. Fassen Sie beispielsweise die Speichernutzung nach Kubernetes Namespace und Container-Name zusammen.



Mai 2020

Benutzerrollen Melden

Folgende Rollen wurden für Reporting hinzugefügt:

- Cloud Insights-Nutzer: Können Berichte ausführen und anzeigen
- Cloud Insights-Autoren: Kann die Kundenfunktionen ausführen sowie Berichte und Dashboards erstellen und verwalten

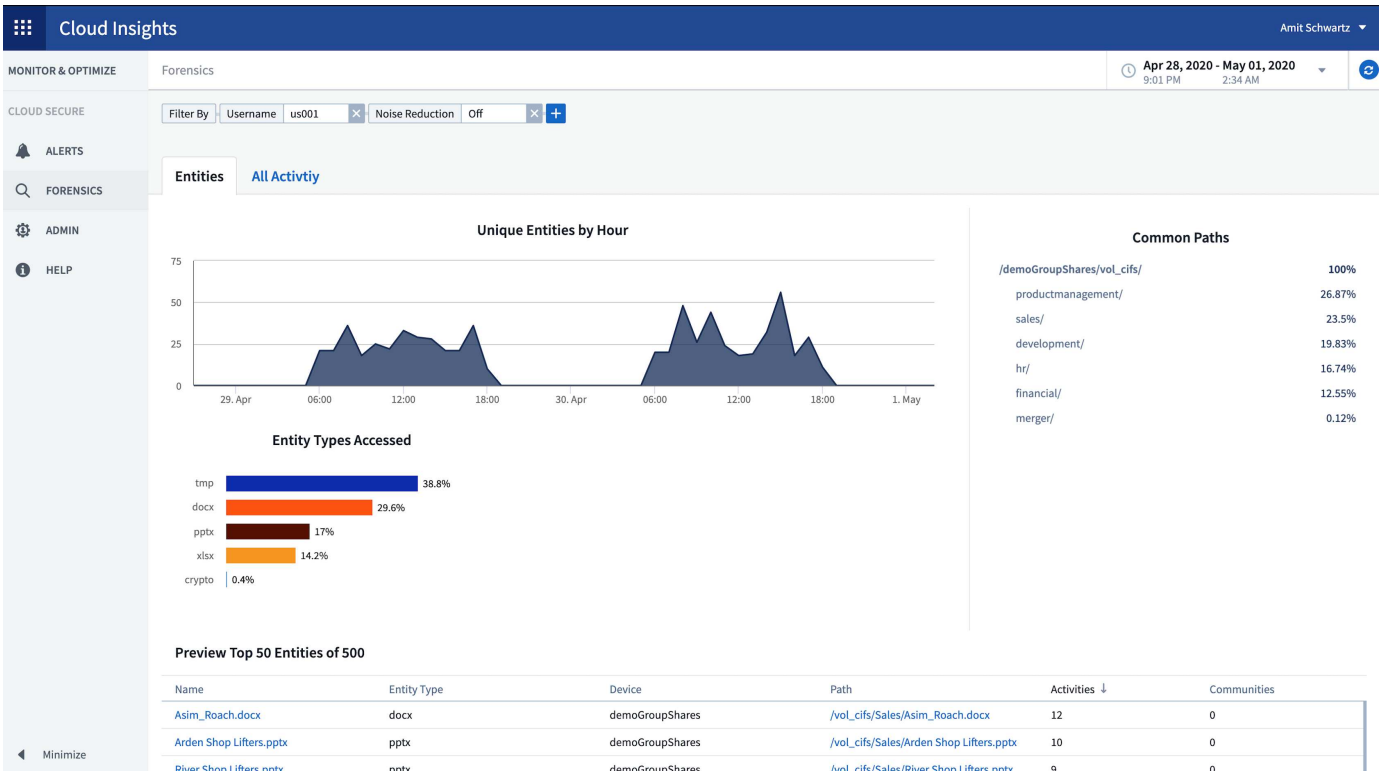
- Cloud Insights-Administratoren: Kann die Autorenfunktionen sowie alle administrativen Aufgaben ausführen

Cloud Secure-Updates

Cloud Insights umfasst die folgenden letzten Cloud Secure Änderungen.

Auf der Seite Forensics > Activity Forensics stellen wir zwei Ansichten zur Analyse und Untersuchung von Benutzeraktivitäten zur Verfügung:

- Aktivitätsansicht mit Schwerpunkt auf Benutzeraktivität (welche Operation? Wo durchgeführt?)
- Entities zeigen auf, auf welche Dateien der Benutzer zugegriffen hat.

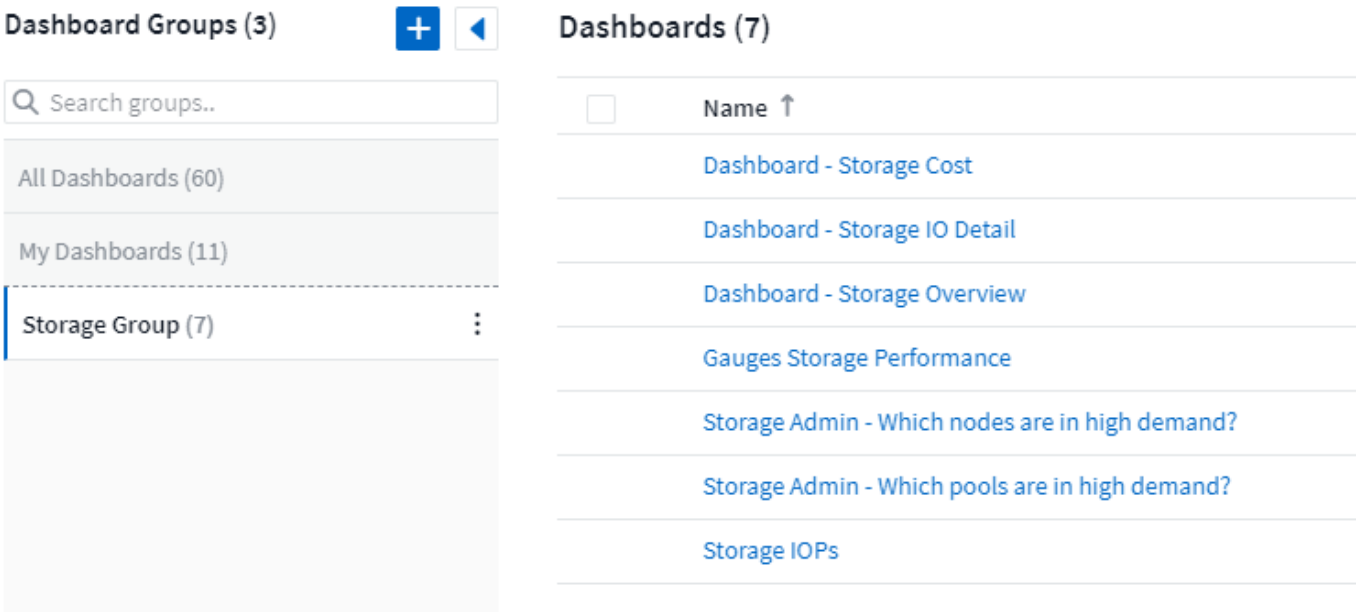


Darüber hinaus enthält die Benachrichtigung per E-Mail jetzt einen direkten Link zur Alarmseite.

Dashboard-Gruppierung

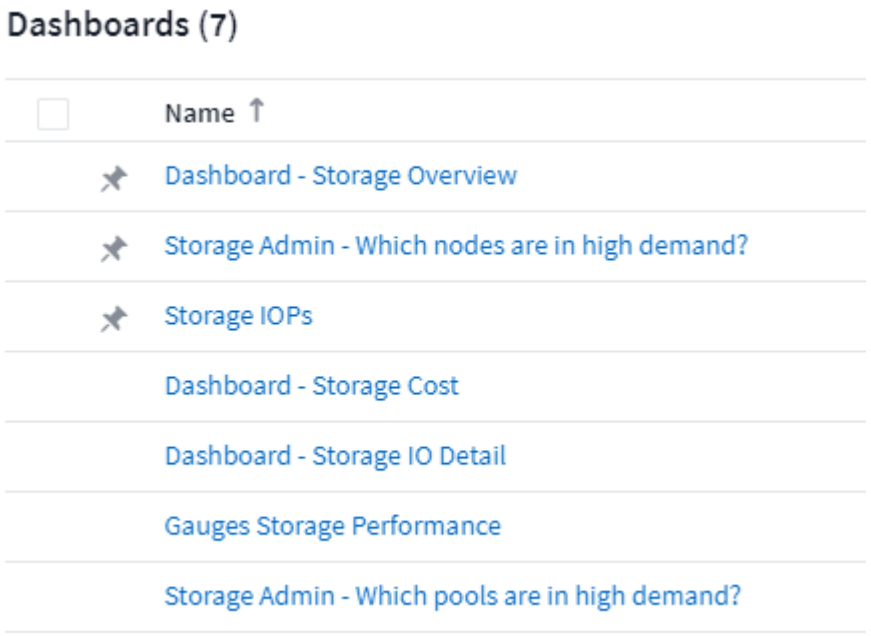
Dank der Gruppierung des Dashboards ist es besser möglich "Management von Dashboards" Die für Sie relevant sind. Sie können einer Gruppe entsprechende Dashboards für die „One-Stop“-Verwaltung von beispielsweise Ihrem Speicher oder virtuellen Maschinen hinzufügen.

Gruppen werden pro Benutzer individuell angepasst, sodass die Gruppen einer Person sich von anderen unterscheiden können. Sie können beliebig viele Gruppen mit so wenigen oder so vielen Dashboards in jeder Gruppe haben, wie Sie möchten.



Dashboard-Pinning

Sie können Dashboards anheften, sodass Favoriten immer oben in der Liste angezeigt werden.



TV-Modus und automatische Aktualisierung

"TV-Modus und automatische Aktualisierung" Anzeige von Daten nahezu in Echtzeit auf einem Dashboard oder einer Asset-Seite zulassen:

- **TV-Modus** bietet ein übersichtliches Display; das Navigationsmenü ist ausgeblendet und bietet mehr Platz auf dem Bildschirm für Ihre Datenanzeige.
- Daten in Widgets auf Dashboards und Asset Landing Pages **Auto-Refresh** gemäß einem Aktualisierungsintervall (alle 10 Sekunden), das vom ausgewählten Dashboard-Zeitbereich (oder Widget-

Zeitbereich, falls die Dashboard-Zeit außer Kraft gesetzt wird) bestimmt wird.

Der TV-Modus und die automatische Aktualisierung sorgen für eine Live-Ansicht Ihrer Cloud Insights-Daten, die sich perfekt für eine nahtlose Vorführung oder interne Überwachung eignet.

April 2020

Neue Optionen Für Den Zeitbereich Auf Dem Dashboard

Für Dashboards und andere Cloud Insights-Seiten stehen jetzt *Letzte 1 Stunde* und *Letzte 15 Minuten* zur Auswahl.

Cloud Secure-Updates

Cloud Insights umfasst die folgenden letzten Cloud Secure Änderungen.

- Bessere Datei- und Ordnermetadaten ändern die Erkennung, um festzustellen, ob der Benutzer die Berechtigung, den Eigentümer oder die Gruppeneigentümer geändert hat.
- Benutzeraktivitätsbericht in CSV exportieren.

Cloud Secure überwacht und prüft alle Vorgänge für den Benutzerzugriff auf Dateien und Ordner. Durch die Prüfung von Aktivitäten können Unternehmen interne Sicherheitsrichtlinien einhalten, externe Compliance-Anforderungen wie PCI, DSGVO und HIPAA erfüllen und Verletzungen von Datensicherheitsverletzungen durchführen.

Standard-Dashboard-Zeit

Der Standardzeitbereich für Dashboards beträgt jetzt 3 Stunden statt 24 Stunden.

Optimierte Aggregationszeiten

Optimiert "Zeitaggregation" Intervalle in Zeitreihen-Widgets (Linien-, Spline-, Bereich- und gestapelte Flächendiagramme) sind häufiger für 3-Stunden- und 24-Stunden-Dashboard-/Widget-Zeitbereiche, was eine schnellere Datenaufstellung ermöglicht.

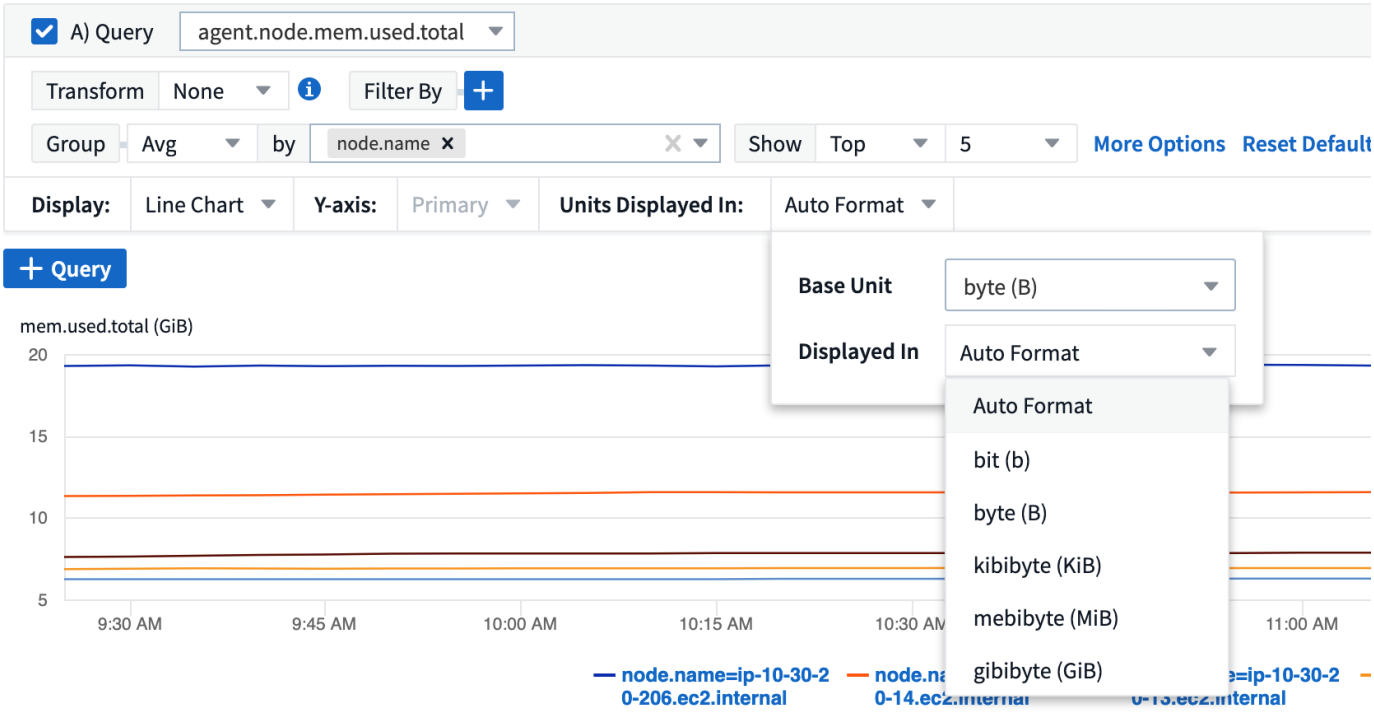
- Der Zeitbereich von 3 Stunden optimiert bis zu einem Aggregationsintervall von 1 Minute. Vorher waren es 5 Minuten.
- Der Zeitbereich von 24 Stunden optimiert bis zu einem 30-minütigen Aggregationsintervall. Vorher war dies 1 Stunde.

Sie können die optimierte Aggregation dennoch überschreiben, indem Sie ein benutzerdefiniertes Intervall festlegen.

Anzeige Des Automatischen Formats Der Einheit

In den meisten Widgets kennt Cloud Insights die Basiseinheit, in der Werte angezeigt werden sollen, z. B. *Megabyte*, *Tausende*, *Prozentsatz*, *Millisekunden (ms)*, Usw. und jetzt "Formate werden automatisch formatiert" Das Widget zur am meisten lesbaren Einheit. Beispielsweise würde ein Datenwert von 1,234,567,890 Byte automatisch auf 1.23 Gibibyte formatiert werden. In vielen Fällen kennt Cloud Insights das beste Format für die zu erschaffenden Daten. Wenn das beste Format nicht bekannt ist oder in Widgets, in

denen Sie die automatische Formatierung überschreiben möchten, können Sie das gewünschte Format auswählen.

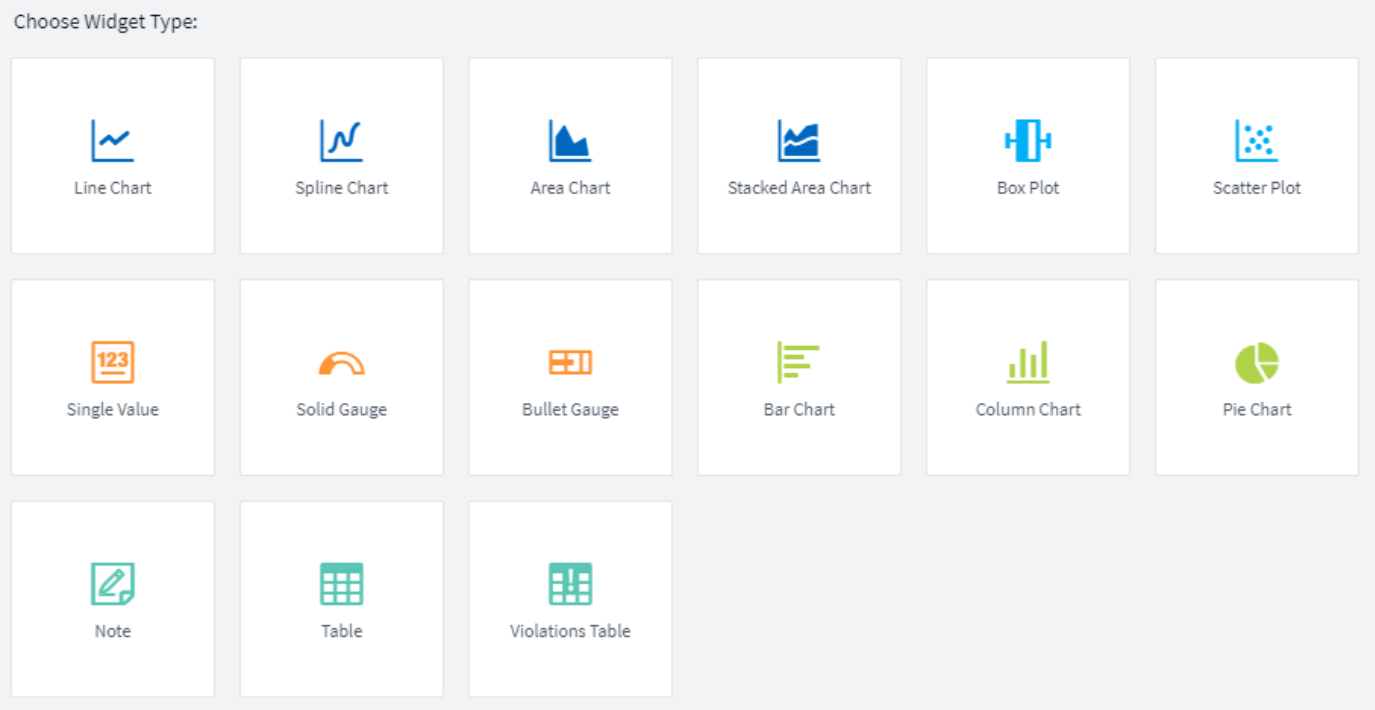


Anmerkungen mit API importieren

Die leistungsstarke API der Cloud Insights Premium Edition bietet Ihnen jetzt Möglichkeiten "Anmerkungen importieren" Und weisen Sie sie mithilfe einer .CSV-Datei Objekten zu. Sie können auch Anwendungen importieren und Geschäftseinheiten auf die gleiche Weise zuweisen.

Einfachere Widget-Auswahl

Das Hinzufügen von Widgets zu Dashboards und Asset-Landing-Seiten ist mit einem neuen Widget-Selektor einfacher, der alle Widgets in einer einzelnen All-at-once-Ansicht anzeigt, sodass der Benutzer nicht mehr durch eine Liste von Widget-Typen scrollen muss, um das zu erweitere Widget zu finden. Verwandte Widgets sind farblich koordiniert und nach Nähe in der neuen Auswahl gruppiert.



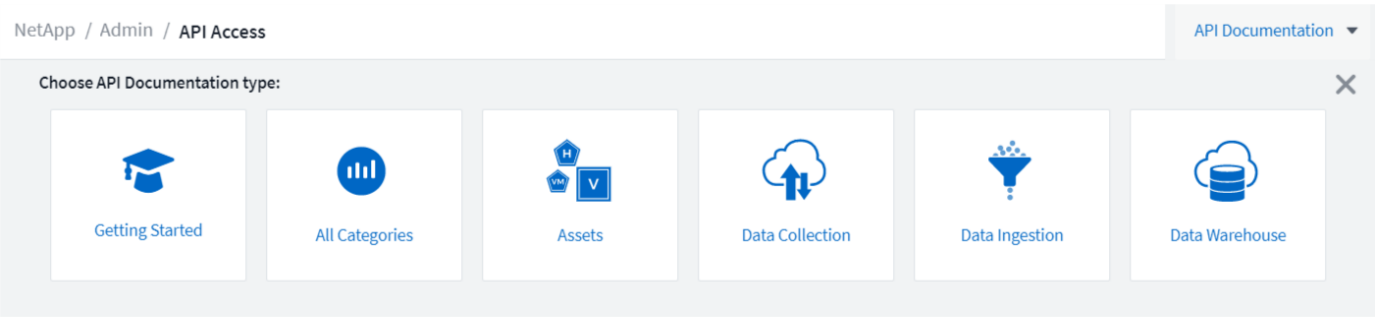
Februar 2020

API mit Premium Edition

Die Cloud Insights Premium Edition ist mit einer Lieferung erhältlich "Leistungsstarke API" Das verwendet werden kann, um Cloud Insights in andere Anwendungen wie CMDB oder andere Ticketsysteme zu integrieren.

Detaillierte, auf Swagger basierende Informationen finden Sie unter **Admin > API Acccess** unter dem Link **API Documentation**. Swagger bietet eine kurze Beschreibung und Informationen zur Verwendung der API und ermöglicht es Ihnen, jede API in Ihrer Umgebung auszuprobieren.

Die Cloud Insights-API verwendet Zugriffstoken, um auf Zugriffsberechtigungen basierenden Zugriff auf API-Kategorien wie Z. B. RESSOURCEN oder SAMMLUNGEN zu gewähren.



Erste Abfrage nach Hinzufügen Eines Data Collectors

Zuvor, nach der Konfiguration eines neuen Datensammlers, Cloud Insights fragt den Datensammler sofort, um *Inventory*-Daten zu sammeln, aber würde warten, bis das konfigurierte Performance-Abfrageintervall (in der

Regel 15 Minuten) erste *Performance*-Daten zu sammeln. Es wartete dann noch ein anderes Intervall, bevor die zweite Performance-Umfrage gestartet wurde, was bedeutete, dass es bis zu *30 Minuten* dauern würde, bevor aussagekräftige Daten von einem neuen Datensammler erfasst wurden.

Datensammler "Umfrage" Wurde stark verbessert, so dass die anfängliche Performance-Umfrage unmittelbar nach der Bestandsabfrage erfolgt, wobei die zweite Performance-Umfrage innerhalb weniger Sekunden nach Abschluss der ersten Performance-Umfrage stattfindet. So kann Cloud Insights innerhalb kürzester Zeit nützliche Daten zu Dashboards und Diagrammen anzeigen.

Dieses Abfrageverhalten tritt auch nach der Bearbeitung der Konfiguration eines vorhandenen Datensammlers auf.

Vereinfachte Duplizierung Von Widget

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

Single Sign On (SSO)

Mit Cloud Insights Premium Edition können Administratoren * aktivieren"Single Sign On"* (SSO) Zugriff auf Cloud Insights für alle Benutzer in ihrer Unternehmensdomäne, ohne sie einzeln einladen zu müssen. Wenn SSO aktiviert ist, kann sich jeder Benutzer mit derselben Domänen-E-Mail-Adresse mithilfe seiner Unternehmensdaten bei Cloud Insights anmelden.

SSO ist nur in der Cloud Insights Premium Edition verfügbar und muss konfiguriert werden, bevor SSO für Cloud Insights aktiviert werden kann. SSO-Konfiguration umfasst "Identitätsföderation" Über NetApp Cloud Central. Mit Single Sign-On-Benutzern im Unternehmensverzeichnis können Benutzer auf NetApp Cloud Central-Konten zugreifen.

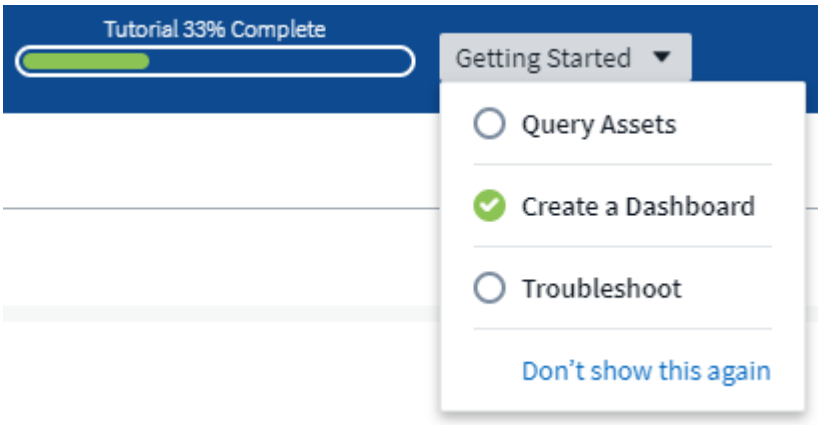
Januar 2020

Swagger-Dokumentation für REST-API

Swagger erklärt jede verfügbare REST-API in Cloud Insights sowie deren Verwendung und Syntax. Informationen über Cloud Insights-APIs finden Sie in "Dokumentation".

Fortschrittsleiste Für Die Funktion „Tutorials“

Die Checkliste für die Funktionanleitungen wurde in den oberen Banner verschoben und verfügt nun über eine Fortschrittsanzeige. Bis zum Abweisen sind für jeden Benutzer Tutorials verfügbar und sind immer in Cloud Insights verfügbar "Dokumentation".



Änderungen An Der Erfassungseinheit

Bei der Installation einer Akquisitionseinheit (AU) auf einem Host oder einer VM mit demselben Namen wie eine bereits installierte AU garantiert Cloud Insights einen eindeutigen Namen, indem er den AU-Namen mit „_1“, „_2“ anhängt. Usw. das ist auch der Fall, wenn eine AU-Deinstallation und Neuinstallation von der gleichen VM durchgeführt wird, ohne dass Sie sie zuerst aus Cloud Insights entfernen. Wollen Sie einen anderen AU-Namen zusammen? Kein Problem; AU’s können nach der Installation umbenannt werden.

Optimierte Zeitaggregation in Widgets

In Widgets können Sie zwischen einem *optimierten* Zeitintervall oder einem von Ihnen festgelegten *Custom* Intervall wählen. Die optimierte Aggregation wählt automatisch das richtige Zeitintervall basierend auf dem ausgewählten Dashboard-Zeitbereich (oder Widget-Zeitbereich, wenn die Dashboard-Zeit überschrieben wird) aus. Das Intervall ändert sich dynamisch, wenn der Zeitbereich des Dashboards oder Widgets geändert wird.

Vereinfachung des Prozesses „erste Schritte mit Cloud Insights“

Der Prozess für die ersten Schritte mit Cloud Insights wurde vereinfacht, damit das erstmalige Setup reibungsloser und einfacher wird. Wählen Sie einfach einen ersten Datensammler aus und folgen Sie den Anweisungen. Cloud Insights führt Sie durch die Konfiguration des Datensammlers und aller benötigten Agenten oder Erfassungseinheiten. In den meisten Fällen wird sogar ein oder mehrere anfängliche Dashboards importiert, sodass Sie schnell Einsichten in Ihre Umgebung erhalten können (Cloud Insights erfasst jedoch bis zu 30 Minuten.)

Zusätzliche Verbesserungen:

- Die Installation der Akquisitionseinheit ist einfacher und läuft schneller.
- Alphabetische Datensammler-Optionen erleichtern es Ihnen, die gesuchte zu finden.
- Verbesserte Anweisungen zur Einrichtung von Data Collector sind einfacher zu befolgen.
- Erfahrene Benutzer können den Prozess „erste Schritte“ mit nur einem Mausklick überspringen.
- Eine neue Statusleiste zeigt Ihnen an, wo Sie sich gerade befinden.

Dezember 2019

Business Entity kann in Filtern verwendet werden

Anmerkungen zur Geschäftseinheit können in Filtern für Abfragen, Widgets, Leistungsrichtlinien und Landing Pages verwendet werden.

Drilldown verfügbar für Widgets mit einem Wert und Anzeige, und alle Widgets, die von „Alle“ gerollt werden

Wenn Sie auf den Wert in einem Widget mit einem einzelnen Wert oder einem Messwert klicken, wird eine Abfrageseite geöffnet, auf der die Ergebnisse der ersten Abfrage angezeigt werden, die im Widget verwendet wird. Durch Klicken auf die Legende für ein beliebiges Widget, dessen Daten durch "Alle" gerollt werden, wird außerdem eine Abfrageseite geöffnet, auf der die Ergebnisse der ersten Abfrage angezeigt werden, die im Widget verwendet wird.

Testzeitraum verlängert

Neue Benutzer, die sich für eine kostenlose Testversion von Cloud Insights anmelden, haben jetzt 30 Tage Zeit, das Produkt zu testen. Dies ist ein Anstieg gegenüber dem letzten 14-Tage-Testzeitraum.

Berechnung der verwalteten Einheiten

Die Berechnung der verwalteten Einheiten (MUs) in Cloud Insights wurde in folgende Werte geändert:

- 1 Managed Unit = 2 Hosts (jede virtuelle oder physische Maschine)
- 1 Managed Unit = 4 TB unformatierte Kapazität physischer oder virtueller Festplatten

Mit dieser Änderung wird die Umgebungskapazität, die Sie mit Ihrem vorhandenen Cloud Insights-Abonnement überwachen können, verdoppelt.

November 2019

Oktober 2019

Berichterstellung

"Cloud Insights-Berichterstattung" Ist ein Business-Intelligence-Tool, mit dem Sie vordefinierte Berichte anzeigen oder benutzerdefinierte Berichte erstellen können. Mit Reporting können Sie die folgenden Aufgaben ausführen:

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

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

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

Die Berichterstellung ist mit Cloud Insights **Premium Edition** verfügbar.

Verbesserungen von Active IQ

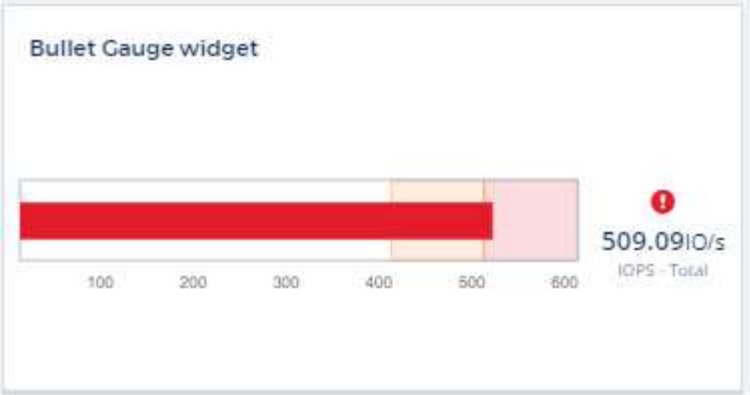
"Active IQ Risiken" Sind nun als Objekte verfügbar, die abgefragt werden können, sowie in Dashboard-Tabellen-Widgets verwendet werden können. Folgende Objektattribute für Risikoprobjekte sind enthalten: * Kategorie * Mitigation Kategorie * potenzielle Auswirkungen * Risikodetails * Schweregrad * Quelle * Storage * Storage-Node * UI-Kategorie

---

September 2019

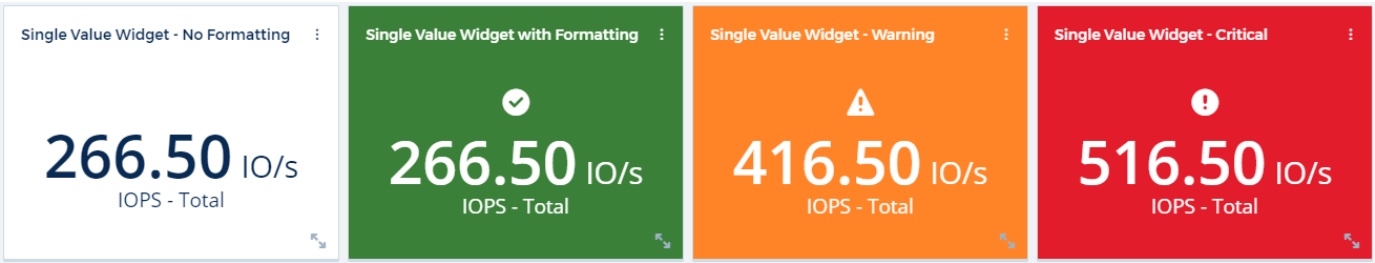
Neue Messbreiteanzeigen

Es stehen zwei neue Widgets zur Anzeige von Einzelwertdaten auf Ihren Dashboards in auffälligen Farben auf der Grundlage der von Ihnen festgelegten Schwellenwerte zur Verfügung. Sie können Werte entweder mit einer **Messanzeige** oder mit einer **Bullet-Anzeige** anzeigen. Werte, die im Warnungsbereich landen, werden orange angezeigt. Die Werte im kritischen Bereich werden rot angezeigt. Werte unterhalb des Warnschwellenwerts werden grün angezeigt.



Bedingte Farbformatierung für ein einzelnes Widget

Sie können nun das Widget „Single Value“ mit einem farbigen Hintergrund anzeigen, der auf den von Ihnen festgelegten Schwellenwerten basiert.



Benutzer Während Der Einschiffung Einladen

Sie können während des Onboarding-Prozesses jederzeit auf Admin > Benutzerverwaltung > +Benutzer klicken, um weitere Benutzer zu Ihrer Cloud Insights-Umgebung einzuladen. Beachten Sie, dass Benutzer mit *Guest* oder *User*-Rollen größere Vorteile erzielen, sobald das Onboarding abgeschlossen ist und Daten gesammelt wurden.

Detailseite des Data Collectors verbessert

Die Datensammler-Detailseite wurde verbessert, um Fehler in einem lesbaren Format anzuzeigen. Fehler werden nun in einer separaten Tabelle auf der Seite angezeigt, wobei jeder Fehler in einer separaten Zeile bei mehreren Fehlern für den Datensammler angezeigt wird.

August 2019

Alle vs Verfügbare Datensammler

Wenn Sie Ihrer Umgebung Datensammler hinzufügen, können Sie einen Filter festlegen, um nur die Datensammler anzuzeigen, die Ihnen auf der Grundlage Ihrer Abonnementstufe oder aller Datensammler zur Verfügung stehen.

Integration mit ActiveIQ

Cloud Insights sammelt Daten von NetApp ActiveIQ, das NetApp Kunden und ihren Hardware-/Softwaresystemen eine Reihe von Visualisierungen, Analysen und anderen Support-Services bietet. Cloud Insights lässt sich in ONTAP Datenmanagementsysteme integrieren. Siehe "Active IQ" Finden Sie weitere Informationen.

Juli 2019

Dashboard-Verbesserungen

Dashboards und Widgets wurden durch folgende Änderungen verbessert:

- Zusätzlich zu Summe, Min, Max und Mittelwert ist **Count** nun eine Option für Roll Up in Single-Value Widgets. Beim Rolling Up durch „Count“ überprüft Cloud Insights, ob ein Objekt aktiv ist oder nicht, und fügt nur die aktiven zu dem Zähler hinzu. Die resultierende Zahl unterliegt der Aggregation und den Filtern.
- Im Widget „Single-Value“ können Sie die resultierende Zahl nun mit 0-, 1-, 2-, 3- oder 4 Dezimalstellen anzeigen.
- Liniendiagramme zeigen eine Achsenbeschriftung und -Einheiten an, wenn ein einzelner Zähler gezeichnet wird.
- **Transform** Option ist für die Service Integration Data jetzt in allen ZeitreihenWidgets für alle Metriken verfügbar. Für alle Services Integration (Telegraf) Zähler oder Metrik in Zeitreihen Widgets (Linie, Spline, Bereich, gestapelte Bereich), werden Sie eine Auswahl an, wie Sie wollen "Transformieren Sie die Werte". Keine (Anzeigewert AS-IS), Summe, Delta, kumulative usw.

Herabstufung auf Basic Edition

Die Downgrade auf Basic Edition schlägt mit einer Fehlermeldung fehl, wenn kein NetApp Gerät verfügbar ist, das in den letzten 7 Tagen erfolgreich eine Umfrage abgeschlossen hat.

Erfassung Von Kube-State-Metrics

Der "Kubernetes Data Collector" Jetzt sammelt Objekte und Zähler aus dem kube-State-Metriken-Plugin, wodurch die Anzahl und der Umfang der Metriken, die für die Überwachung in Cloud Insights verfügbar sind, stark erweitert werden.

Juni 2019

Cloud Insights Editionen

Cloud Insights ist in verschiedenen Editionen erhältlich, um Ihr Budget und Ihre Geschäftsanforderungen zu erfüllen. Bestehende NetApp Kunden mit einem aktiven NetApp Support Account erhalten mit der kostenlosen **Basic Edition** 7 Tage Datenaufbewahrung und Zugriff auf NetApp Datensammler. Sie erhalten aber auch mehr Datenhaltung, Zugang zu allen unterstützten Datensammlern, technischen Support durch Experten und mehr mit **Standard Edition**. Weitere Informationen über verfügbare Funktionen erhalten Sie auf der NetApp "Einblicke in die Cloud" Standort.

Neuer Infrastruktur-Data Collector: NetApp HCI

- "NetApp HCI Virtual Center" Wurde als Infrastrukturdatensammler hinzugefügt. Der Datensammler HCI Virtual Center erfasst Informationen zum NetApp HCI Host und benötigt schreibgeschützten Berechtigungen für alle Objekte im Virtual Center.

Beachten Sie, dass der HCI Data Collector nur vom HCI Virtual Center übernommen wird. Um Daten aus dem Storage-System zu erfassen, müssen Sie außerdem NetApp konfigurieren "SolidFire" Datensammler.

Mai 2019

Neuer Service Data Collector: Kapacitor

- "Kapacitor" Wurde als Datensammler für Dienste hinzugefügt.

Einbindung in Services über Telegraf

Neben der Erfassung von Daten von Infrastrukturgeräten wie Switches und Storage erfasst Cloud Insights jetzt mithilfe verschiedener Betriebssysteme und Services Daten "Telegraf als Agent" Zur Erfassung von Integrationsdaten. Telegraf ist ein Plug-in-Agent, der zum Sammeln und Berichten von Kennzahlen verwendet werden kann. Mit Input-Plug-ins werden die gewünschten Informationen in den Agent erfasst, indem direkt auf das System/Betriebssystem zugegriffen wird, APIs von Drittanbietern angerufen werden oder konfigurierte Streams angehört werden.

Dokumentation für aktuell unterstützte Integrationen finden Sie im Menü links unter **Referenz und Support**.

Ressourcen Für Storage Virtual Machines

- Storage Virtual Machines (SVMs) sind als Assets in Cloud Insights verfügbar. SVMs verfügen über eigene Asset Landing Pages, die in Suchvorgängen, Abfragen und Filtern angezeigt und verwendet werden können. SVMs können auch in den Dashboard-Widgets verwendet werden und mit Annotationen verknüpft werden.

Niedrigere Systemanforderungen Für Die Akquisitionseinheit

- Die CPU- und Speicheranforderungen des Systems für die Software Acquisition Unit (AU) wurden reduziert. Die neuen Anforderungen sind:

* Komponente*	* Alte Anforderung*	**Neue Anforderung**

CPU-Kerne	4	2
Speicher	16 GB	8 GB

Weitere Plattformen Werden Unterstützt

- Die folgenden Plattformen wurden diesen derzeit hinzugefügt "Unterstützt für Cloud Insights":

Linux	Windows
CentOS 7.3 64-Bit CentOS 7.4 64-Bit CentOS 7.6 64-Bit Debian 9 64-Bit Red hat Enterprise Linux 7.3 64-Bit Red hat Enterprise Linux 7.4 64-Bit Red hat Enterprise Linux 7.6 64-Bit Ubuntu Server 18.04 LTS	Microsoft Windows 10 64-Bit Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019

April 2019

Filtern Sie virtuelle Maschinen nach Tags

Wenn Sie die folgenden Datensammler konfigurieren, können Sie filtern, virtuelle Maschinen nach ihren Tags oder Labels in die Datensammlung einzuschließen oder auszuschließen.

- "Amazon EC2"
- "Azure"
- "Google Cloud Platform"

März 2019

E-Mail-Benachrichtigungen für abonnementbezogene Ereignisse

- Sie können Empfänger für E-Mail auswählen "Benachrichtigungen" Wenn Veranstaltungen mit Abonnements auftreten, z. B. Änderungen an einem Testlauf oder an einem abonnierten Konto. Sie können Empfänger für diese Benachrichtigungen aus folgenden Optionen auswählen:
  - Alle Account-Inhaber
  - Alle Administratoren
  - Zusätzliche E-Mail-Adressen, die Sie angeben

Zusätzliche Dashboards

- Mit dem folgenden neuen AWS-orientierten Storage "Dashboards" Wurden in die Galerie hinzugefügt und sind für den Import verfügbar:
  - AWS Admin - welche EC2 sind in großen Anforderungen?
  - Performance der AWS EC2 Instanz nach Region

Februar 2019

Erfassung über AWS Child-Konten

- Cloud Insights unterstützt "Erfassung aus AWS Child-Konten" In einem einzelnen Datensammler gespeichert werden. Ihre AWS-Umgebung muss so konfiguriert sein, dass Cloud Insights den Abholung von untergeordneten Konten ermöglicht.

Benennung Des Data Collectors

- Data Collector-Namen können jetzt auch Punkte (.), Bindestriche (-) und Leerzeichen ( ) sowie Buchstaben, Zahlen und Unterstriche enthalten. Namen dürfen nicht mit Leerzeichen, Punkt oder Bindestrich beginnen oder enden.

Erfassungseinheit für Windows

- Sie können eine Cloud Insights-Erfassungseinheit auf einem Windows-Server/einer Windows-VM konfigurieren. Überprüfen Sie die Windows "Voraussetzungen" Vor der Installation des "Software für Akquisitionseinheiten".

Januar 2019

Das Feld „Eigentümer“ ist besser lesbar

- In Dashboard- und Abfragelisten waren die Daten für das Feld „Eigentümer“ zuvor eine Autorisierungs-ID-Zeichenfolge anstelle eines benutzerfreundlichen inhabernamens. Das Feld „Eigentümer“ zeigt jetzt einen einfacheren und leserteren Namen des Eigentümers.

Aufschlüsselung der verwalteten Einheiten auf der Abonnementseite

- Für jeden Datensammler, der auf der Seite **Admin > Subscription** aufgeführt ist, können Sie jetzt eine Aufschlüsselung der Anzahl der verwalteten Einheiten (ME) für Hosts und Speicher sowie die Summe anzeigen.

Dezember 2018

Verbesserung der UI-Ladezeit

- Die anfängliche Ladezeit für die Cloud Insights-Benutzeroberfläche (UI) wurde deutlich verbessert. Auch die Aktualisierungszeit für die Benutzeroberfläche profitiert von der Verbesserung unter Umständen, wenn Metadaten geladen werden.

Datensammler Zur Massenbearbeitung

- Sie können Informationen für mehrere Datensammler gleichzeitig bearbeiten. Wählen Sie auf der Seite **Observability > Collectors** die zu ändernden Datensammler aus, indem Sie das Kontrollkästchen links von jedem aktivieren und auf die Schaltfläche **Massenaktionen** klicken. Wählen Sie **Bearbeiten** und

ändern Sie die erforderlichen Felder.

Die ausgewählten Datensammler müssen derselbe Anbieter und dasselbe Modell sein und sich auf derselben Akquisitionseinheit befinden.

Während der Einschiffung stehen Support- und Abonnementseiten zur Verfügung

- Während des Onboarding Workflows können Sie zu den Seiten **Hilfe > Support** und **Admin > Abonnement** navigieren. Wenn Sie von diesen Seiten zurückkehren, kehren Sie zum Onboarding-Workflow zurück, sofern Sie die Registerkarte Browser nicht geschlossen haben.

November 2018

Abonnieren Sie unseren Newsletter über NetApp Sales oder AWS Marketplace

- Das Cloud Insights Abonnement und die Abrechnung stehen jetzt direkt über NetApp zur Verfügung. Dies ist eine Ergänzung zum Self-Service-Abonnement, das über AWS Marketplace verfügbar ist. Auf der Seite **Admin > Subscription** wird ein neuer Link für den **Contact Sales** angezeigt. Für Kunden mit Umgebungen, in denen 1,000 oder mehr Managed Units (MUs) vorhanden sind oder erwartet werden, empfiehlt es sich, über den Link „Vertrieb kontaktieren“ den NetApp Vertrieb zu kontaktieren.

Textanmerkung Hyperlinks

- Textanmerkungen können nun Hyperlinks enthalten.

Onboarding – Rundgang

- Cloud Insights bietet jetzt einen Onboarding-Schritt für den ersten Benutzer (Administrator oder Account-Inhaber), der sich in einer neuen Umgebung einloggen kann. Der Rundgang führt Sie durch die Installation einer Erfassungseinheit, die Konfiguration eines ersten Datensammlers und die Auswahl eines oder mehrerer nützlicher Dashboards.

Importieren Sie Dashboards aus der Galerie

- Zusätzlich zur Auswahl von Dashboards während des Onboarding können Sie Dashboards über **Dashboards > Alle Dashboards anzeigen** importieren und auf **+aus Galerie** klicken.

Duplizieren Von Dashboards

- Die Möglichkeit, ein Dashboard zu duplizieren, wurde der Dashboard-Listenseite als eine Auswahl im Optionsmenü für jedes Dashboard und auf der Hauptseite eines Dashboards selbst aus dem Menü „*Save*“ hinzugefügt.

Produktmenü von Cloud Central

- Das Menü, über das Sie zu anderen NetApp Cloud Central Produkten wechseln können, ist jetzt in die obere rechte Ecke des Bildschirms verschoben.

Einblicke Aus Die Dateninfrastruktur

Bevor Sie mit der Arbeit mit Data Infrastructure Insights beginnen können, müssen Sie sich im **NetApp BlueXP** -Portal anmelden. Wenn Sie bereits über ein NetApp BlueXP Login verfügen, können Sie mit ein paar schnellen Schritten eine kostenlose Testversion von Data Infrastructure Insights starten.

Sie erstellen Ihr NetApp BlueXP Konto

Erste Schritte mit NetApp Cloud-Services finden Sie unter "NetApp BlueXP" Und klicken Sie auf **erste Schritte**.

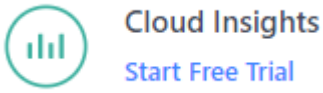
- Wenn Sie sich noch nicht angemeldet haben, wählen Sie **Anmelden**
- Geben Sie eine gültige geschäftliche E-Mail-Adresse ein und wählen Sie ein Passwort.
- Geben Sie Ihren Firmennamen und Ihren vollständigen Namen ein.
- Akzeptieren Sie die Geschäftsbedingungen und wählen Sie **Weiter**.
- BlueXP zeigt Ihnen die ersten Schritte auf.

Was ist, wenn ich bereits über einen NetApp BlueXP Login spreche?

Sobald Sie über einen NetApp BlueXP Account verfügen, wählen Sie **Anmelden** auf der "NetApp BlueXP" Portalseite.

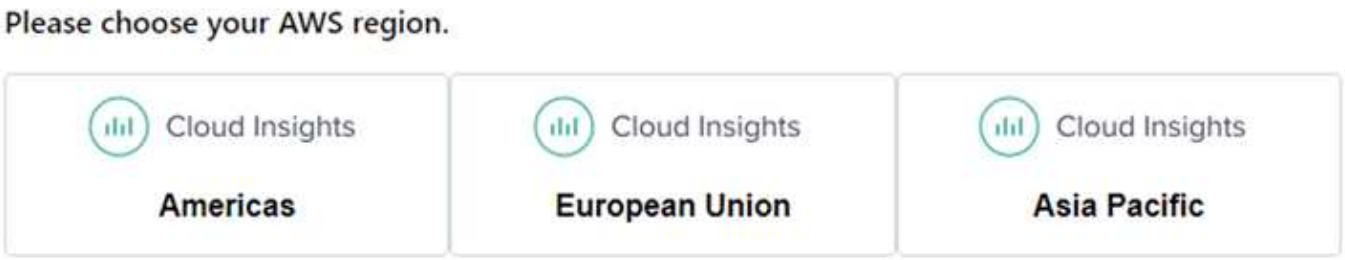
Geben Sie Ihre E-Mail-Adresse und Ihr Kennwort ein. Anschließend gelangen Sie zu den Cloud-Angeboten von NetApp.

Wählen Sie Dateninfrastruktur Insights.



Starten Sie Ihre Data Infrastructure Insights kostenlos

Wenn Sie sich zum ersten Mal bei Data Infrastructure Insights anmelden, klicken Sie unter Data Infrastructure Insights auf **kostenlose Testversion starten**. Data Infrastructure Insights unterstützt Sie beim Aufbau Ihrer Unternehmensumgebung und zeigt Ihnen, welche Region Sie für die gewünschte Umgebung auswählen.



Nach Abschluss der Erstellung Ihrer Umgebung können Sie Ihre BlueXP Zugangsdaten verwenden, um sich

anzumelden und Ihre kostenlose 30-Tage-Testversion von Data Infrastructure Insights zu starten. Entdecken Sie bei diesem Testlauf die Features, die Data Infrastructure Insights zu bieten hat.

Während der kostenlosen Testversion können Sie "Starten Sie Ihr Abonnement"Data Infrastructure Insights jederzeit zur Verfügung stellen. Nach dem Abonnement können Sie die Funktionen von Data Infrastructure Insights basierend auf Ihrem aktuellen Abonnement nutzen.

Melden Sie sich an und gehen Sie

Sobald Ihre Umgebung erstellt wurde, können Sie sich jederzeit einfach im NetApp BlueXP -Portal anmelden und auf **Gehe zu Dateninfrastrukturinformationen** klicken. Sie gelangen direkt zu Ihrer Data Infrastructure Insights Umgebung.

Sie können einen Browser auch direkt öffnen, um die URL Ihrer Data Infrastructure Insights Umgebung aufzurufen, zum Beispiel:

```
 \https://<environment-prefix>.c01.cloudinsights.netapp.com/
Die URL wird auch in die Einladungs-E-Mail jedes Benutzers für einfachen
Zugriff und Lesezeichen enthalten. Wenn der Benutzer noch nicht bei BlueXP
angemeldet ist, wird er zur Anmeldung aufgefordert.
```

Neue Benutzer müssen sich nach wie vor für den Zugriff auf BlueXP registrieren, bevor sie auf die URL ihrer Umgebung zugreifen können.

Wenn Sie sich zum ersten Mal in einer neuen Umgebung anmelden, werden Sie durch die Einrichtung bis geleitet **"Datensammlung beginnen"**.

Abmelden

Um sich bei Data Infrastructure Insights abzumelden, klicken Sie auf Ihren **Benutzernamen** und wählen **Abmelden**. Sie werden zurück zum Anmeldefenster von BlueXP angezeigt.

Wenn Sie von Dateninfrastruktur Insights abmelden, werden Sie von BlueXP abgebloggt. Sie werden außerdem von anderen NetApp-Cloud-Services, die die BlueXP-Anmeldung verwenden, abgemeldet.

Zeitüberschreitung Bei Inaktivität

BlueXP meldet einen Benutzer standardmäßig ab, wenn sechs Stunden (360 Minuten) keine Aktivitäten bestehen. Unabhängig von der Aktivität werden Benutzer nach sieben Tagen abgemeldet.

Sicherheit

Einblicke In Die Dateninfrastruktur, Sicherheit

Die Datensicherheit bei Produkten und Kunden ist bei NetApp von größter Bedeutung. Data Infrastructure Insights befolgt während des gesamten Release-Lebenszyklus sicherheitstechnisch bewährte Verfahren, damit Kundeninformationen und -Daten bestmöglich geschützt werden.

Sicherheit – Überblick

Physische Sicherheit

Die Produktionsinfrastruktur von Data Infrastructure Insights wird auf Amazon Web Services (AWS) gehostet. Physische und umgebungsbezogene Sicherheitskontrollen für Data Infrastructure Insights Produktions-Server, einschließlich Gebäude sowie Schlösser oder Schlüssel, die an Türen verwendet werden, werden von AWS gemanagt. Gemäß AWS: „Der physische Zugang wird sowohl am Perimeter als auch an Einbruchstellen durch professionelles Sicherheitspersonal mithilfe von Videoüberwachung, Intrusion Detection Systemen und anderen elektronischen Mitteln gesteuert. Autorisierte Mitarbeiter nutzen Multi-Faktor-Authentifizierungsmechanismen für den Zugriff auf Datacenter-Stockwerke.“

Data Infrastructure Insights folgt den Best Practices"Modell der gemeinsamen Verantwortung", die von AWS beschrieben werden.

Produktsicherheit

Data Infrastructure Insights folgt einem Entwicklungslebenszyklus nach den Prinzipien von Agile. So können wir sicherheitsbezogene Softwarefehler im Vergleich zu Methoden zur Entwicklung eines längeren Release-Zyklus schneller beheben. Mithilfe von Methoden zur kontinuierlichen Integration sind wir in der Lage, schnell sowohl auf funktionale als auch auf Sicherheitsänderungen zu reagieren. Die Änderungsmanagementverfahren und -Richtlinien legen fest, wann und wie Änderungen vorgenommen werden, und tragen dazu bei, die Stabilität der Produktionsumgebung zu erhalten. Alle wirkungsvollen Änderungen werden formal kommuniziert, koordiniert, richtig überprüft und vor ihrer Veröffentlichung in der Produktionsumgebung genehmigt.

Netzwerksicherheit

Der Netzwerkzugriff auf Ressourcen in der Data Infrastructure Insights Umgebung wird über Host-basierte Firewalls gesteuert. Jede Ressource (wie z. B. ein Load Balancer oder eine virtuelle Maschineninstanz) verfügt über eine hostbasierte Firewall, die den eingehenden Datenverkehr auf nur die Ports beschränkt, die für die Ausführung ihrer Funktion benötigt werden.

Data Infrastructure Insights nutzt verschiedene Mechanismen wie Intrusion Detection Services, um die Produktionsumgebung auf Sicherheitsanomalien zu überwachen.

Risikoeinschätzung

Das Data Infrastructure Insights-Team folgt einem formalisierten Risikobewertungsprozess, um eine systematische, wiederholbare Methode zur Identifizierung und Bewertung der Risiken bereitzustellen, damit diese durch einen Risikobehandlungsplan angemessen gemanagt werden können.

Datensicherung

Die Produktionsumgebung von Data Infrastructure Insights wird in einer hochredundanten Infrastruktur eingerichtet, in der für alle Services und Komponenten mehrere Verfügbarkeitszonen genutzt werden. Neben einer hochverfügbaren und redundanten Computing-Infrastruktur werden wichtige Daten in regelmäßigen Abständen gesichert und Restores regelmäßig getestet. Formelle Backup-Richtlinien und -Verfahren minimieren die Auswirkungen von Unterbrechungen von Geschäftsaktivitäten und schützen Unternehmensprozesse gegen die Auswirkungen von Fehlern in Informationssystemen oder -Ausfällen und stellen einen zeitnahen und adäquaten Wiederaufnahme sicher.

Authentifizierung und Zugriffsmanagement

Der gesamte Zugriff von Kunden auf Data Infrastructure Insights erfolgt über Interaktionen auf der Browser-Benutzeroberfläche über HTTPS. Die Authentifizierung erfolgt über den Dienst Auth0 eines Drittanbieters. NetApp hat hier als Authentifizierungsebene für alle Cloud-Datenservices zentralisiert.

Data Infrastructure Insights befolgt branchenübliche Best Practices, einschließlich „Least Privilege“ und „rollenbasierte Zugriffssteuerung“ beim logischen Zugriff auf die Produktionsumgebung von Data Infrastructure Insights. Der Zugriff wird streng nach Anforderungen kontrolliert und nur ausgewählten autorisierten Mitarbeitern mit Multi-Faktor-Authentifizierungsmechanismen gewährt.

Erhebung und Schutz von Kundendaten

Alle Kundendaten werden während der Übertragung über öffentliche Netzwerke verschlüsselt und im Ruhezustand verschlüsselt. Data Infrastructure Insights nutzt Verschlüsselung an verschiedenen Stellen im System zum Schutz von Kundendaten. Dazu kommen Technologien wie Transport Layer Security (TLS) und der branchenübliche AES-256-Algorithmus.

Kundendeprovisionierung

E-Mail-Benachrichtigungen werden in verschiedenen Abständen versendet, um dem Kunden mitzuteilen, dass das Abonnement abläuft. Nach Ablauf des Abonnements wird die UI eingeschränkt und eine Kulanzzeit beginnt für die Datenerfassung. Der Kunde wird dann per E-Mail benachrichtigt. Bei Testabonnements besteht eine Frist von 14 Tagen. Im Rahmen der bezahlten Abonnements haben Sie eine Frist von 28 Tagen. Nach Ablauf der Kulanzzeit wird der Kunde per E-Mail darüber informiert, dass das Konto innerhalb von 2 Tagen gelöscht wird. Ein zahlter Kunde kann auch direkt beantragen, dass er nicht im Service ist.

Abgelaufene Mandanten und alle zugehörigen Kundendaten werden vom Data Infrastructure Insights Operations (SRE) Team am Ende der Gnadenfrist oder nach Bestätigung der Kontoersatzanfrage eines Kunden gelöscht. In beiden Fällen führt das SRE-Team einen API-Aufruf aus, um das Konto zu löschen. Der API-Aufruf löscht die Mandanteninstanz und alle Kundendaten. Die Löschung durch den Kunden wird durch den Aufruf derselben API überprüft und überprüft, ob der Kunde den Status „GELÖSCHT“ hat.

Management von Sicherheitsproblemen

Dateninfrastruktur Insights ist in den PSIRT-Prozess (Product Security Incident Response Team) von NetApp integriert, um bekannte Schwachstellen zu finden, zu bewerten und zu beheben. PSIRT nutzt Informationen zu Schwachstellen über mehrere Kanäle, darunter Kundenberichte, interne technische Informationen und allgemein anerkannte Quellen wie die CVE-Datenbank.

Wenn ein Problem vom Data Infrastructure Insights Engineering-Team erkannt wird, leitet das Team den PSIRT-Prozess ein, bewertet und Behebung des Problems.

Es ist auch möglich, dass ein Kunde oder Wissenschaftler bei Data Infrastructure Insights ein Sicherheitsproblem beim Data Infrastructure Insights Produkt identifiziert und das Problem dem technischen

Support oder direkt dem NetApp Incident Response-Team meldet. In diesen Fällen leitet das Team von Data Infrastructure Insights den PSIRT-Prozess ein, bewertet und beseitigt das Problem möglicherweise.

Schwachstellen- und Penetrationstests

Data Infrastructure Insights befolgt branchenübliche Best Practices und führt regelmäßig Schwachstellen- und Penetrationstests durch, bei denen sowohl interne als auch externe Sicherheitsexperten und Unternehmen zum Einsatz kommen.

Schulung zur Sensibilisierung für die Sicherheit

Alle Mitarbeiter von Data Infrastructure Insights werden gemäß dem Sicherheitstraining für individuelle Rollen entwickelt, um sicherzustellen, dass jeder Mitarbeiter in der Lage ist, mit den spezifischen sicherheitsorientierten Herausforderungen seiner Rolle umzugehen.

Compliance

Data Infrastructure Insights führt unabhängige Audits und Validierungen der Sicherheitsmaßnahmen, Prozesse und Services durch anerkannte externe Prüfer durch. Zu den Prüfungen zählen auch SOC 2-Audits.

NetApp-Sicherheitsempfehlungen

Sehen Sie sich die verfügbaren Sicherheitsempfehlungen von NetApp an "Hier".

Informationen und Region

NetApp nimmt die Sicherheit von Kundeninformationen sehr ernst. Hier erfahren Sie, wie und wo Data Infrastructure Insights Ihre Informationen speichert.

Welche Informationen werden in Data Infrastructure Insights gespeichert?

Data Infrastructure Insights speichert folgende Informationen:

- Performance-Daten

  Performancedaten sind Zeitreihendaten, die Informationen zur Leistung des überwachten Geräts/der überwachten Quelle liefern. Dazu zählen beispielsweise die Anzahl der von einem Speichersystem bereitgestellten iOS, der Durchsatz eines FibreChannel-Ports, die Anzahl der von einem Webserver bereitgestellten Seiten, die Reaktionszeit einer Datenbank und vieles mehr.

- Bestandsdaten

  Bestandsdaten bestehen aus Metadaten, die das überwachte Gerät/die Quelle beschreiben und wie es konfiguriert wird. Dazu gehören beispielsweise installierte Hardware- und Softwareversionen, Festplatten und LUNs in einem Storage-System, CPU-Kerne, RAM und Festplatten einer Virtual Machine, die Tabellen einer Datenbank, die Anzahl und die Art der Ports auf einem SAN Switch, Verzeichnis-/Dateinamen (bei aktivierter Storage Workload Security) usw.

- Konfigurationsdaten

  Dies fasst vom Kunden bereitgestellte Konfigurationsdaten zusammen, die zur Verwaltung von Kundeninventar und -Vorgängen verwendet werden, z. B. Hostnamen oder IP-Adressen der überwachten Geräte, Abfrageintervalle, Zeitlimits usw.

- Secrets

  Geheimnisse umfassen die Anmeldeinformationen, die von der Data Infrastructure Insights Acquisition Unit für den Zugriff auf Kundengeräte und -Services verwendet werden. Diese Anmeldeinformationen werden mit einer starken asymmetrischen Verschlüsselung verschlüsselt, und die privaten Schlüssel werden nur auf den Akquisitionseinheiten gespeichert und verlassen nie die Kundenumgebung. Selbst privilegierte Data Infrastructure Insights SRES können aufgrund dieses Designs nicht auf Kundengeheimnisse im Klartext zugreifen.

- Funktionale Daten

  Diese Daten werden durch die Bereitstellung des Cloud Data Service durch NetApp generiert, der NetApp über die Entwicklung, Implementierung, den Betrieb, die Wartung und die Sicherung des Cloud Data Service informiert. Funktionale Daten enthalten weder Kundendaten noch personenbezogene Daten.

- Benutzerdaten

  Authentifizierungs- und Zugriffsinformationen, die es NetApp BlueXP ermöglichen, mit regionalen Dateninfrastrukturen Insights zu kommunizieren, einschließlich Daten zur Benutzerautorisierung.

- Sicherheitsdaten Des Benutzerverzeichnisses Für Storage-Workloads

  In Fällen, in denen die Workload-Sicherheitsfunktion aktiviert ist UND der Kunde den Benutzer-Directory-Collector aktivieren möchte, speichert das System Anzeigenamen, Unternehmens-E-Mail-Adressen und andere Informationen, die aus Active Directory gesammelt wurden.

Benutzerverzeichnisdaten beziehen sich auf Benutzerverzeichnisinformationen, die vom Datensammler Workload Security User Directory erfasst werden, nicht auf Daten über die Benutzer von Data Infrastructure Insights/Workload Security selbst.

Es werden keine expliziten personenbezogenen Daten aus Infrastruktur- und Dienstleistungsressourcen erhoben. Die erfassten Daten bestehen aus Performance-Kennzahlen, Konfigurationsdaten und Infrastrukturmetadaten, ähnlich wie viele Telefonanbieter mit NetApp Auto-Support und ActiveIQ. Abhängig von den Namenskonventionen des Kunden werden jedoch Daten für Shares, Volumes, VMs, qtrees, Anwendungen usw. können personenbezogene Informationen enthalten.

Wenn Workload Security aktiviert ist, untersucht das System außerdem Datei- und Verzeichnisnamen auf SMB- oder anderen Freigaben, die personenbezogene Informationen enthalten können. Wenn Kunden den Workload Security User Directory Collector aktivieren (der Windows SIDs im Wesentlichen über Active Directory Benutzernamen zuordnet), werden der Anzeigename, die Unternehmens-E-Mail-Adresse und alle zusätzlich ausgewählten Attribute von Data Infrastructure Insights erfasst und gespeichert.

Darüber hinaus werden Zugriffsprotokolle zu Data Infrastructure Insights verwaltet und enthalten die IP- und E-Mail-Adressen der Benutzer, die zur Anmeldung beim Service verwendet werden.

Wo werden meine Informationen gespeichert?

Data Infrastructure Insights speichert Informationen entsprechend der Region, in der Ihre Umgebung erstellt wird.

Folgende Informationen werden in der Host-Region gespeichert:

- Telemetrie- und Asset-/Objektdaten, einschließlich Zähler und Performance-Kennzahlen

- Informationen zu den Erfassungseinheiten
- Funktionale Daten
- Audit-Informationen zu Benutzeraktivitäten innerhalb von Data Infrastructure Insights
- Active Directory-Informationen zu Workload-Sicherheit
- Informationen zur Workload Security Audit

Die folgenden Informationen verbleiben in den USA, unabhängig von der Region, in der Ihre Data Infrastructure Insights Umgebung gehostet wird:

- Angaben zum Umgebungsstandort (manchmal auch „Mandant“ genannt), z. B. Standort-/Kontoinhaber.
- Informationen, die es NetApp BlueXP ermöglichen, mit regionalen Einsichten zu Dateninfrastrukturen zu kommunizieren, einschließlich aller Vorgänge, die mit der Benutzerautorisierung ausgeführt werden.
- Informationen im Zusammenhang mit der Beziehung zwischen dem Benutzer Data Infrastructure Insights und dem Mandanten.

Host-Regionen

Host-Regionen sind:

- USA: USA-Osten-1
- EMEA: EU-Mitte-1
- APAC: ap-Südost-2

Weitere Informationen

Weitere Informationen zu Datenschutz und Sicherheit von NetApp finden Sie unter folgenden Links:

- "Trust Center"
- "Grenzüberschreitende Datenübertragungen"
- "Binding Corporate Rules"
- "Reaktion auf Datenanfragen von Drittanbietern"
- "NetApp Datenschutzgrundsätze"

Sicherheitstool

Dateninfrastruktur Insights umfasst Sicherheitsfunktionen, mit denen Ihre Umgebung sicherer betrieben werden kann. Die Funktionen umfassen Verbesserungen bei der Verschlüsselung, Passwort-Hashing und die Fähigkeit, interne Benutzerpasswörter zu ändern sowie Schlüsselpaare, die Kennwörter verschlüsseln und entschlüsseln.

Zum Schutz sensibler Daten empfiehlt NetApp, nach einer Installation oder einem Upgrade die Standardschlüssel und das Benutzerpasswort „*Acquisition*“ zu ändern.

Verschlüsselte Passwörter der Datenquelle werden in Data Infrastructure Insights gespeichert, das einen öffentlichen Schlüssel verwendet, um Passwörter zu verschlüsseln, wenn ein Benutzer sie auf einer Konfigurationsseite für den Datensammler eingibt. Data Infrastructure Insights verfügt nicht über die privaten Schlüssel, die zum Entschlüsseln der Datensammlerkennwörter erforderlich sind. Nur Acquisition Units (aus)

verfügen über den privaten Datensammlerschlüssel, der zum Entschlüsseln der Datensammlerkennwörter erforderlich ist.

Überlegungen zu Upgrades und Installationen

Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (d. h. Sie haben ein rekeyed Kennwort), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen eines Software-Upgrades wird das System auf eine Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System auf die Standardkonfiguration zurückgesetzt wird, müssen Sie die nicht voreingestellte Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Sicherheitsverwaltung auf der Akquisitionseinheit

Mit dem SecurityAdmin-Tool können Sie die Sicherheitsoptionen für Data Infrastructure Insights verwalten und wird auf dem Erfassungssystem ausgeführt. Die Sicherheitsverwaltung umfasst das Verwalten von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen von Sicherheitskonfigurationen, die Sie erstellen oder auf die Standardeinstellungen wiederherstellen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte auf dem AU-System verfügen, um die Acquisition Unit-Software (die das SecurityAdmin-Tool enthält) installieren zu können.
- Wenn Sie nicht-Admin-Benutzer haben, die anschließend auf das SecurityAdmin-Tool zugreifen müssen, müssen diese zur *cisys*-Gruppe hinzugefügt werden. Die *cisys*-Gruppe wird während der AU-Installation erstellt.

Nach der AU-Installation befindet sich das SecurityAdmin-Tool auf dem Erfassungseinheitssystem an einem der folgenden Standorte:

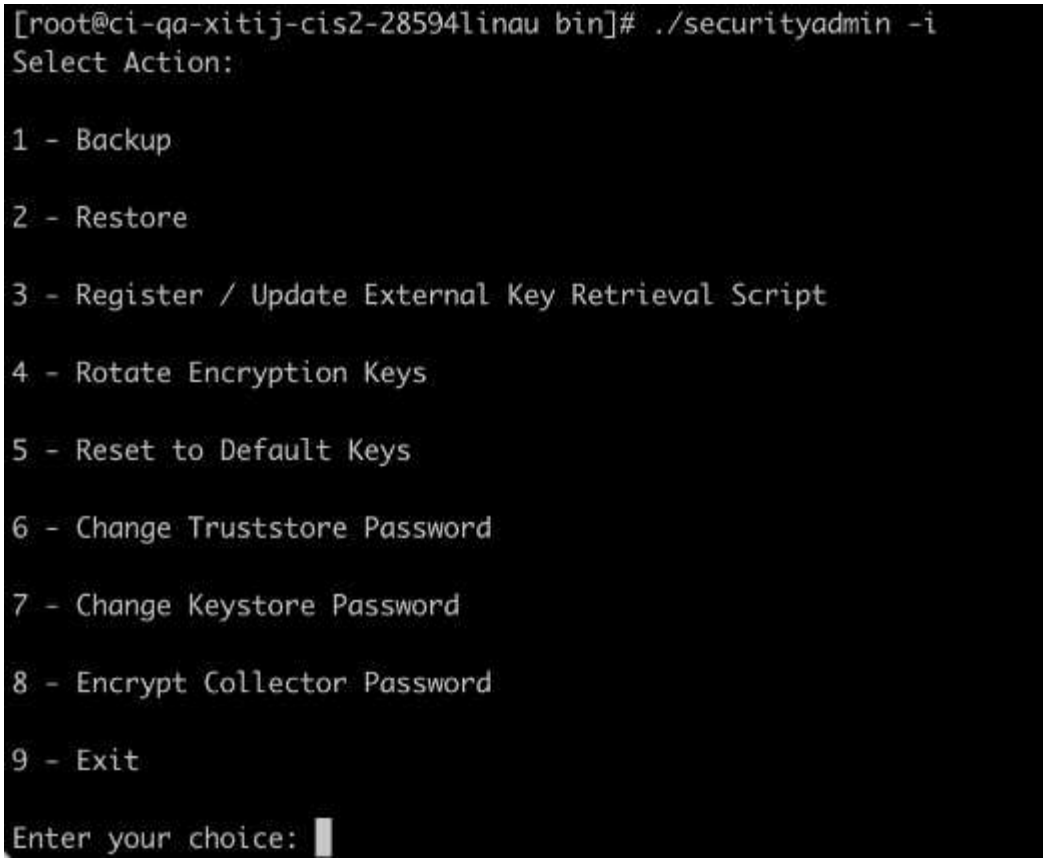
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Verwenden des SecurityAdmin-Tools

Starten Sie das SecurityAdmin-Tool im interaktiven Modus (-i).

Es wird empfohlen, das SecurityAdmin-Tool im interaktiven Modus zu verwenden, um das Übergeben von Geheimnissen in der Befehlszeile zu vermeiden, die in Protokollen erfasst werden können.

Folgende Optionen werden angezeigt:



1. **Backup**

   Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

   ```
   Windows - C:\Program Files\SANscreen\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Es wird empfohlen, Vault-Backups sicher zu halten, da sie vertrauliche Informationen enthalten.

2. **Wiederherstellen**

   Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

   Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel mit den folgenden Schritten: 1) Ändern der Verschlüsselungsschlüssel auf der AU. 2) Erstellen Sie eine Sicherung des Tresors. 3) Stellen Sie die Vault-Sicherung auf jedem der aus wieder her.

3. **Skript Zum Abrufen Des Externen Schlüssels Registrieren/Aktualisieren**

   Verwenden Sie ein externes Skript, um die AU-Verschlüsselungsschlüssel zu registrieren oder zu ändern, die zum Verschlüsseln oder Entschlüsseln von Gerätekennwörtern verwendet werden.

   Wenn Sie Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

Beachten Sie, dass diese Option nur unter Linux verfügbar ist.

Wenn Sie Ihr eigenes Schlüsselabruf-Skript mit dem SecurityAdmin-Tool verwenden, beachten Sie Folgendes:

- Der aktuell unterstützte Algorithmus ist RSA mit mindestens 2048 Bit.
- Das Skript muss die privaten und öffentlichen Schlüssel im Klartext zurückgeben. Das Skript darf keine verschlüsselten privaten und öffentlichen Schlüssel zurückgeben.
- Das Skript sollte rohe, codierte Inhalte zurückgeben (nur PEM-Format).
- Das externe Skript muss über *execute* Berechtigungen verfügen.

4. **Verschlüsselungstasten Drehen**

   Drehen Sie die Verschlüsselungsschlüssel (heben Sie die Registrierung der aktuellen Schlüssel auf und registrieren Sie neue Schlüssel). Um einen Schlüssel aus einem externen Schlüsselverwaltungssystem zu verwenden, müssen Sie die ID des öffentlichen Schlüssels und die ID des privaten Schlüssels angeben.

5. **Auf Standardschlüssel zurücksetzen**

   Setzt das Erfassungs-Benutzerpasswort und die Erfassungs-Benutzerverschlüsselungsschlüssel auf die Standardwerte zurück. Bei der Installation werden die Standardwerte angegeben.

6. **Passwort Des Truststore Ändern**

   Ändern Sie das Passwort des Truststore.

7. **Passwort Des Keystore Ändern**

   Ändern Sie das Passwort des Keystore.

8. **Passwort Des Verschlüsselten Collectors**

   Kennwort für den Datensammler verschlüsseln.

9. **Ausgang**

   Beenden Sie das SecurityAdmin-Tool.

Wählen Sie die Option, die Sie konfigurieren möchten, und befolgen Sie die Anweisungen.

Festlegen eines Benutzers, der das Tool ausführen soll

Wenn Sie sich in einer kontrollierten, sicherheitsbewussten Umgebung befinden, verfügen Sie möglicherweise nicht über die *cisys*-Gruppe, möchten aber möglicherweise, dass bestimmte Benutzer das SecurityAdmin-Tool ausführen.

Sie können dies erreichen, indem Sie die AU-Software manuell installieren und den Benutzer/die Gruppe angeben, für den Sie Zugriff haben möchten.

- Laden Sie den CI Installer mithilfe der API auf das AU-System herunter, und entpacken Sie ihn.
  - Sie benötigen ein einmaliger Autorisierungstoken. Siehe API Swagger Dokumentation (*Admin > API Access* und wählen Sie den Link *API Documentation*) und finden Sie den Abschnitt *GET /au/oneTimeToken* API.

    - Sobald Sie das Token haben, verwenden Sie die *GET /au/Installers/{Platform}/{Version}* API, um die Installer-Datei herunterzuladen. Sie müssen sowohl die Plattform (Linux oder Windows) als auch die Installer-Version bereitstellen.
- Kopieren Sie die heruntergeladene Installationsdatei auf das AU-System, und entpacken Sie sie.
- Navigieren Sie zu dem Ordner, der die Dateien enthält, und führen Sie das Installationsprogramm als root aus. Geben Sie dabei den Benutzer und die Gruppe an:

```
./cloudinsights-install.sh <User> <Group>
```

Wenn der angegebene Benutzer und/oder die angegebene Gruppe nicht vorhanden ist, werden diese erstellt. Der Benutzer hat Zugriff auf das SecurityAdmin-Tool.

Proxy wird aktualisiert oder entfernt

Mit dem SecurityAdmin-Tool können Proxy-Informationen für die Acquisition Unit festgelegt oder entfernt werden, indem das Tool mit dem Parameter *-PR* ausgeführt wird:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Um den Proxy beispielsweise zu entfernen, führen Sie folgenden Befehl aus:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Sie müssen die Erfassungseinheit neu starten, nachdem Sie den Befehl
ausgeführt haben.
```

Um einen Proxy zu aktualisieren, lautet der Befehl

```
./securityadmin -pr -upr <arg>
```

Externer Schlüsselabruf

Wenn Sie ein UNIX-Shell-Skript bereitstellen, kann es von der Erfassungseinheit ausgeführt werden, um den **privaten Schlüssel** und den **öffentlichen Schlüssel** von Ihrem Schlüsselverwaltungssystem abzurufen.

Um den Schlüssel abzurufen, führt Data Infrastructure Insights das Skript aus und gibt zwei Parameter an: *Key id* und *key type*. *Key id* kann verwendet werden, um den Schlüssel in Ihrem Key Management System zu identifizieren. *Schlüsseltyp* ist entweder "öffentlich" oder "privat". Wenn der Schlüsseltyp „public“ ist, muss das Skript den öffentlichen Schlüssel zurückgeben. Wenn der Schlüsseltyp „privat“ ist, muss der private Schlüssel zurückgegeben werden.

Um den Schlüssel an die Erfassungseinheit zurücksenden zu können, muss das Skript den Schlüssel auf die Standardausgabe drucken. Das Skript muss *only* den Schlüssel zur Standardausgabe drucken; kein anderer Text muss in der Standardausgabe gedruckt werden. Sobald der angeforderte Schlüssel in die Standardausgabe gedruckt wurde, muss das Skript mit einem Exit-Code von 0 beendet werden. Jeder andere Rückgabewert wird als Fehler angesehen.

Das Skript muss mit der Erfassungseinheit mit dem SecurityAdmin-Tool registriert werden, das das Skript zusammen mit der Erfassungseinheit ausführt. Das Skript muss über *read* und *execute* Berechtigungen für den Root- und „cisys“-Benutzer verfügen. Wenn das Shell-Skript nach der Registrierung geändert wird, muss das geänderte Shell-Skript erneut bei der Erfassungseinheit registriert werden.

Eingabeparameter: Schlüssel-id	Schlüsselkennung zur Identifizierung des Schlüssels im Verschlüsselungsmanagement-System des Kunden
Eingabeparameter: Schlüsseltyp	Public oder Private Cloud.
Ausgang	Die angeforderte Taste muss in der Standardausgabe ausgedruckt werden. 2048-Bit RSA-Schlüssel wird derzeit unterstützt. Schlüssel müssen im folgenden Format kodiert und gedruckt werden: Privates Schlüsselformat - PEM, DER-encoded PKCS8 PrivateKeyInfo RFC 5958 Public Key Format - PEM, DER-encoded X.509 SubjectPublicKeyInfo RFC 5280
Exit-Code	Der Exit-Code von Null wird erfolgreich ausgeführt. Alle anderen Exit-Werte gelten als fehlgeschlagen.
Skriptberechtigungen	Das Skript muss über Lese- und Ausführungsberechtigungen für den Root- und „cisys“-Benutzer verfügen.
Protokolle	Skriptausführungen werden protokolliert. Protokolle finden Sie in - /Var/log/netapp/Cloudinsights/securityadmin/securityadmin.log /Var/log/netapp/Cloudinsights/acq/acq.log

Verschlüsseln eines Kennworts für die Verwendung in API

Mit Option 8 können Sie ein Passwort verschlüsseln, das Sie dann per API an einen Datensammler weiterleiten können.

Starten Sie das SecurityAdmin-Tool im interaktiven Modus und wählen Sie Option 8: *Encrypt Password*.

```
 securityadmin.sh -i
Sie werden aufgefordert, das Kennwort einzugeben, das Sie verschlüsseln
möchten. Beachten Sie, dass die von Ihnen eingegebenen Zeichen nicht auf
dem Bildschirm angezeigt werden.  Geben Sie das Passwort erneut ein, wenn
Sie dazu aufgefordert werden.
```

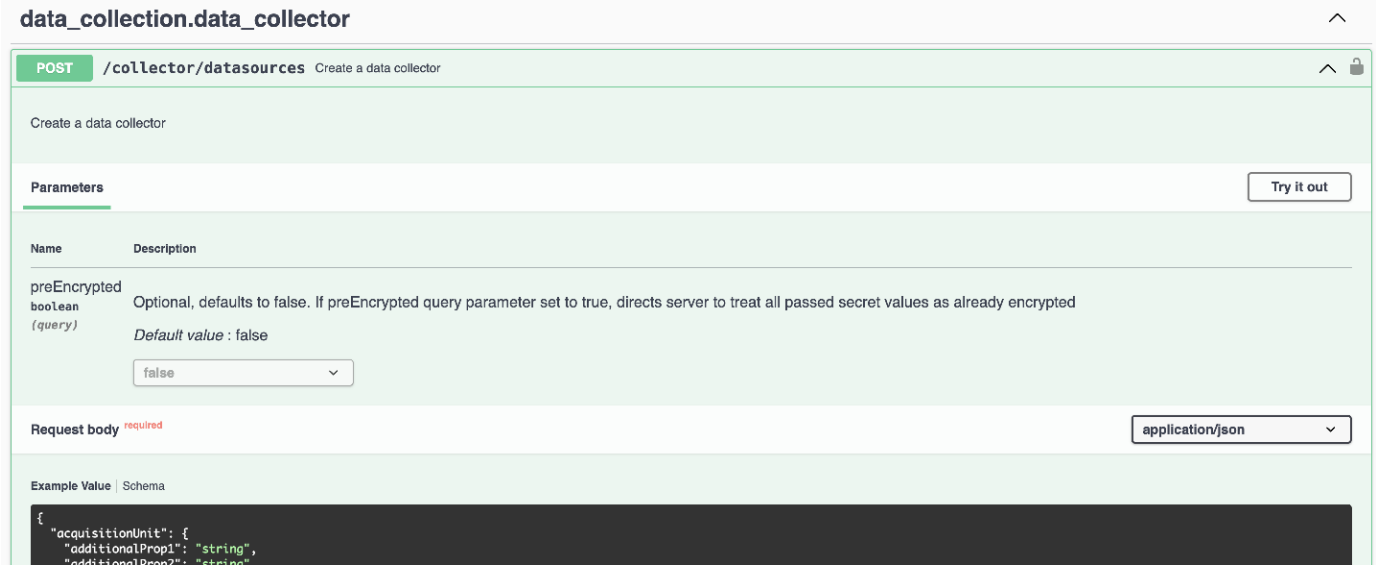
Wenn Sie den Befehl in einem Skript verwenden, verwenden Sie alternativ auf einer Befehlszeile *securityadmin.sh* mit dem Parameter "-enc" und geben Ihr unverschlüsseltes Passwort ein:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Beispiel für CLI"]
```

Das verschlüsselte Passwort wird auf dem Bildschirm angezeigt. Kopieren Sie die gesamte Zeichenfolge einschließlich aller führenden oder nachgestellten Symbole.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Um das verschlüsselte Passwort an einen Datensammler zu senden, können Sie die Data Collection API verwenden. Der Swagger für diese API ist unter **Admin > API Access** zu finden und auf den Link "API Documentation" zu klicken. Wählen Sie den API-Typ „Data Collection“ aus. Wählen Sie unter der Überschrift *Data_Collection.Data_Collector* die API */Collector/Datasources* POST für dieses Beispiel aus.



Wenn Sie die Option *preEncrypted* auf *true* setzen, wird jedes Passwort, das Sie über den API-Befehl übergeben, als **bereits verschlüsselt** behandelt; die API verschlüsselt das/die Passwort(e) nicht neu. Wenn Sie Ihre API erstellen, fügen Sie einfach das zuvor verschlüsselte Passwort an der entsprechenden Stelle ein.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```


Verschlüsseln eines Kennworts für die Verwendung in API

Mit Option 8 können Sie ein Passwort verschlüsseln, das Sie dann per API an einen Datensammler weiterleiten können.

Starten Sie das SecurityAdmin-Tool im interaktiven Modus und wählen Sie Option 8: *Encrypt Password*.

```
 securityadmin.sh -i
Sie werden aufgefordert, das Kennwort einzugeben, das Sie verschlüsseln
möchten. Beachten Sie, dass die von Ihnen eingegebenen Zeichen nicht auf
dem Bildschirm angezeigt werden.  Geben Sie das Passwort erneut ein, wenn
Sie dazu aufgefordert werden.
```

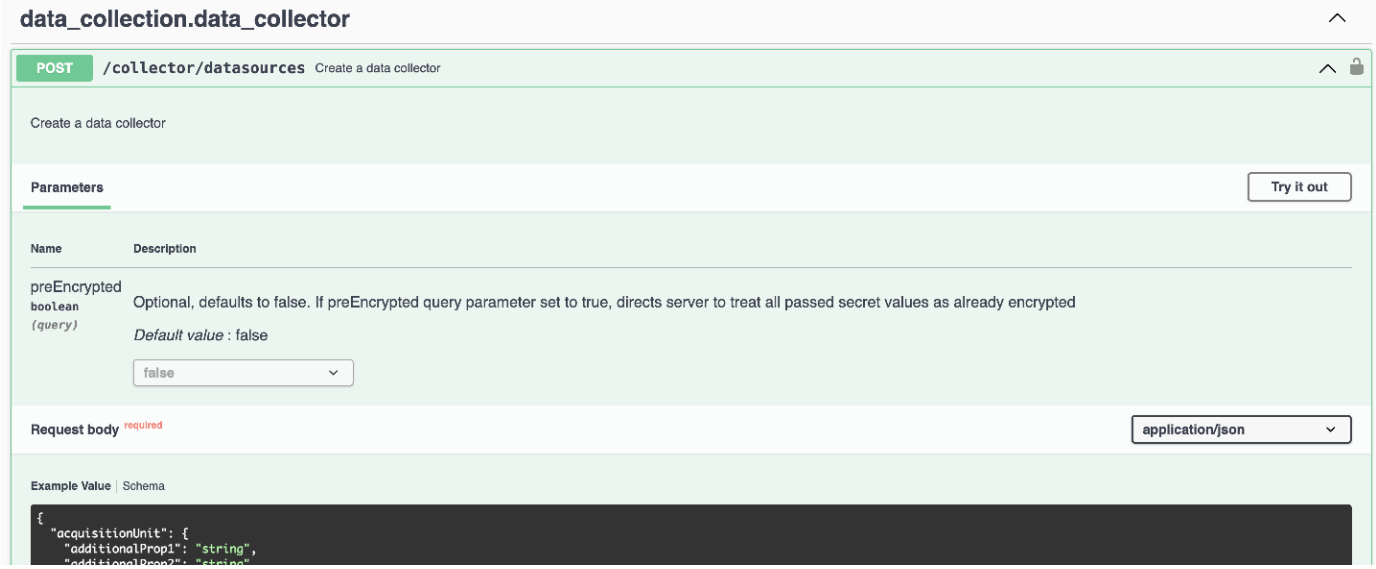
Wenn Sie den Befehl in einem Skript verwenden, verwenden Sie alternativ auf einer Befehlszeile *securityadmin.sh* mit dem Parameter "-enc" und geben Ihr unverschlüsseltes Passwort ein:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Beispiel für CLI"]
```

Das verschlüsselte Passwort wird auf dem Bildschirm angezeigt. Kopieren Sie die gesamte Zeichenfolge einschließlich aller führenden oder nachgestellten Symbole.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Um das verschlüsselte Passwort an einen Datensammler zu senden, können Sie die Data Collection API verwenden. Der Swagger für diese API ist unter **Admin > API Access** zu finden und auf den Link "API Documentation" zu klicken. Wählen Sie den API-Typ „Data Collection“ aus. Wählen Sie unter der Überschrift *Data_Collection.Data_Collector* die API */Collector/Datasources* POST für dieses Beispiel aus.



Wenn Sie die Option *preEncrypted* auf *true* setzen, wird jedes Passwort, das Sie über den API-Befehl übergeben, als **bereits verschlüsselt** behandelt; die API verschlüsselt das/die Passwort(e) nicht neu. Wenn Sie Ihre API erstellen, fügen Sie einfach das zuvor verschlüsselte Passwort an der entsprechenden Stelle ein.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

Erste Schritte

Lernprogramme Zu Funktionen

Data Infrastructure Insights enthält viele nützliche Funktionen, mit denen Sie Daten schnell und einfach finden, Probleme beheben und Einblicke in Ihre Unternehmensumgebung erhalten. Nutzen Sie leistungsstarke Abfragen, visualisieren Sie Daten in Dashboards und senden Sie E-Mail-Benachrichtigungen für die von Ihnen festgelegten Datenschwellenwerte.

Data Infrastructure Insights enthält eine Reihe von Video-Tutorials, die Ihnen dabei helfen, diese Funktionen zu verstehen und Ihre Business-Insight-Strategien besser zu implementieren. Diese Tutorials nutzen alle Benutzer, die Zugriff auf Ihre Data Infrastructure Insights Umgebung haben.

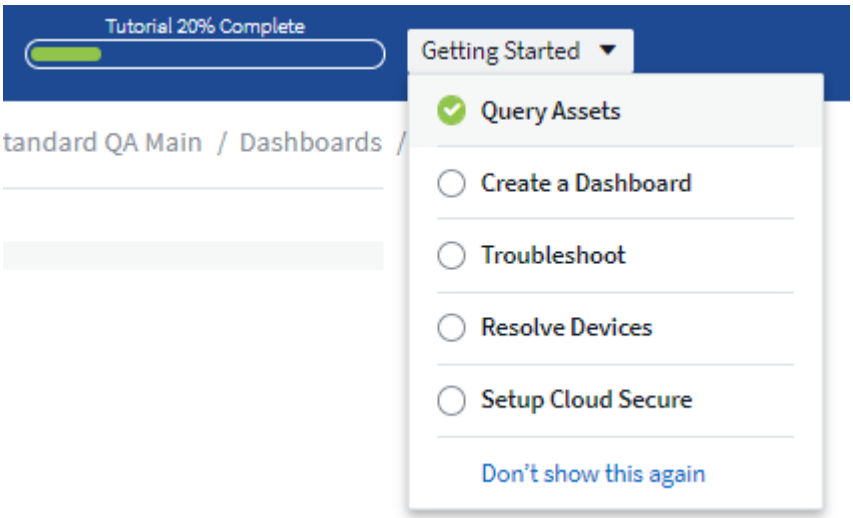
Einführung

Sehen Sie sich ein kurzes Tutorial an, das erklärt, wie Data Infrastructure Insights funktioniert.

► https://docs.netapp.com/de-de/cloudinsights//media/howTo.mp4 *(video)*

Checkliste und Video Tutorials

Die **Startup Checklist**, die auf Ihrer Data Infrastructure Insights Seite angezeigt wird, enthält eine Liste mit mehreren nützlichen Aufgaben und Konzepten. Durch Auswahl eines Elements in der Checkliste gelangen Sie zur entsprechenden Seite „Einblicke in die Dateninfrastruktur“ für dieses Konzept. Wenn Sie beispielsweise auf das Element *Create a Dashboard* klicken, wird die Seite Data Infrastructure Insights **Dashboards** geöffnet.



Oben auf der Seite befindet sich ein Link zu einem Video-Tutorial, das zeigt, wie ein Dashboard erstellt wird. Sie können das Video so oft ansehen, wie Sie möchten, bis Sie auf das *Got klicken! Diesen Link nicht mehr anzeigen* für dieses Video. Das Video ist jedes Mal verfügbar, wenn Sie die Seite Dashboards aufrufen, bis Sie es verwerfen.

Nachdem Sie sich das Video mindestens einmal angesehen haben, wird die Option *Dashboard erstellen* in der Checkliste deaktiviert, was darauf hinweist, dass Sie das Tutorial abgeschlossen haben. Sie können dann mit dem nächsten Tutorial fortfahren.

Sie können die Tutorials in jeder beliebigen Reihenfolge anzeigen, die Sie mögen, so oft wie Sie mögen, bis Sie entlassen.

Die Checkliste nicht ausfüllen

Die Startup-Checkliste wird auf Ihrer Site angezeigt, bis Sie unten in der Checkliste auf den Link *Do't Show This* klicken. Selbst wenn Sie die Checkliste nicht mehr verwenden, sind die Tutorials immer noch auf jeder entsprechenden Seite „Data Infrastructure Insights“ verfügbar, bis Sie sie in der Kopfzeile der Nachricht verwerfen.

Tutorials anzeigen

Abfragen Von Daten

► https://docs.netapp.com/de-de/cloudinsights//media/Queries.mp4 *(video)*

Erstellen eines Dashboards

► https://docs.netapp.com/de-de/cloudinsights//media/Dashboards.mp4 *(video)*

Fehlerbehebung

► https://docs.netapp.com/de-de/cloudinsights//media/Troubleshooting.mp4 *(video)*

Auflösen Von Geräten

► https://docs.netapp.com/de-de/cloudinsights//media/AHR_small.mp4 *(video)*

Daten Werden Erfasst

Erste Schritte zum Sammeln von Daten

Nachdem Sie sich bei Data Infrastructure Insights angemeldet und sich zum ersten Mal in Ihrer Umgebung angemeldet haben, werden Sie durch die folgenden Schritte geführt, um mit der Erfassung und dem Management von Daten zu beginnen.

Datensammler erkennen Informationen aus Ihren Datenquellen, wie Speichergeräte, Netzwerk-Switches und virtuelle Maschinen. Die erfassten Informationen werden für Analysen, Validierung, Monitoring und Fehlerbehebung verwendet.

Data Infrastructure Insights bietet drei Arten von Datensammlern:

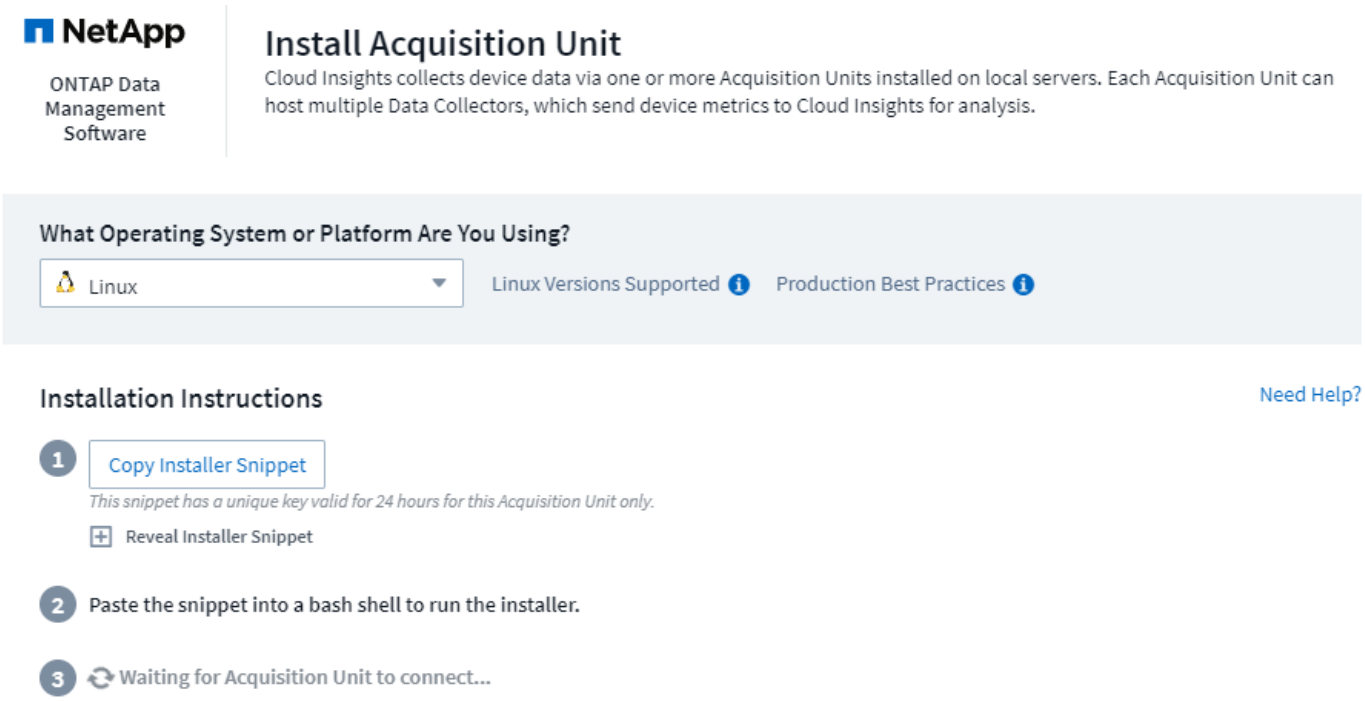
- Infrastruktur (Storage-Geräte, Netzwerk-Switches, Computing-Infrastruktur)
- Betriebssysteme (wie VMware oder Windows)
- Services (wie Kafka)

Wählen Sie Ihren ersten Datensammler von den unterstützten Anbietern und Modellen aus. Sie können später

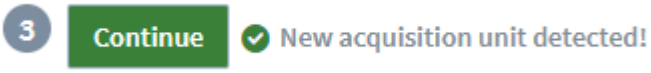
ganz einfach weitere Datensammler hinzufügen.

Installieren Sie eine Akquisitionseinheit

Wenn Sie einen *Infrastructure*-Datensammler ausgewählt haben, ist eine Acquisition Unit erforderlich, um Daten in Data Infrastructure Insights zu integrieren. Sie müssen die Software Acquisition Unit auf einem Server oder einer VM auf dem Rechenzentrum herunterladen und installieren, von dem aus Sie die Software erfassen. Eine einzelne Erfassungseinheit kann für mehrere Datensammler verwendet werden.



- Folgen Sie den "Anweisungen" Wird angezeigt, um Ihre Akquisitionseinheit zu installieren. Sobald die Software für die Erfassungseinheit installiert ist, wird die Schaltfläche Weiter angezeigt, und Sie können mit dem nächsten Schritt fortfahren.



Sie können bei Bedarf später weitere Akquisitionseinheiten einrichten. So können Sie beispielsweise unterschiedliche Erfassungseinheiten wünschen, die Informationen aus Datacentern in verschiedenen Regionen erfassen.

Konfigurieren Sie den Data Collector - Infrastruktur

Für *Infrastructure* Datensammler werden Sie aufgefordert, die präsentierten Datensammler-Felder auszufüllen:

- Geben Sie dem Datensammler einen eindeutigen und aussagekräftigen Namen.
- Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) ein, um eine Verbindung zum Gerät herzustellen.
- Füllen Sie alle anderen Pflichtfelder in den Abschnitten_Configuration_ und_Advanced Configuration_ aus.
- Klicken Sie auf **Collector hinzufügen**, um den Datensammler zu speichern.

Sie können später zusätzliche Datensammler konfigurieren.

Konfigurieren Sie den Data Collector - Betriebssysteme und Dienste

Betriebssystem:

Wählen Sie für *Operating System*-Datensammler eine Plattform (Linux, Windows) aus, um einen Data Infrastructure Insights Agent zu installieren. Sie müssen mindestens einen Agenten haben, um Daten von Services zu erfassen. Der Agent sammelt außerdem Daten vom Host selbst, um sie in Data Infrastructure Insights zu verwenden. Diese Daten werden in Widgets usw. als „Knoten“-Daten kategorisiert

- Öffnen Sie ein Terminal- oder Befehlsfenster auf dem Agent-Host oder der VM, und fügen Sie den angezeigten Befehl ein, um den Agenten zu installieren.
- Klicken Sie nach Abschluss der Installation auf **Setup abschließen**.

Dienste:

Für *Service* Datensammler, klicken Sie auf eine Kachel, um die Instructions-Seite für diesen Dienst zu öffnen.

- Wählen Sie eine Plattform und einen Agent Access Key.
- Wenn auf dieser Plattform kein Agent installiert ist, befolgen Sie die Anweisungen, um den Agent zu installieren.
- Klicken Sie auf **Weiter**, um die Seite mit den Anweisungen für den Datensammler zu öffnen.
- Befolgen Sie die Anweisungen, um den Datensammler zu konfigurieren.
- Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Setup abschließen**.

Dashboards Hinzufügen

Je nach Art des ersten zu konfigurierenden Datensammlers (Speicher, Switch usw.) wird ein oder mehrere relevante Dashboards importiert. Wenn Sie beispielsweise einen Speicherdatensammler konfiguriert haben, wird ein Satz speicherbezogener Dashboards importiert, und eines wird als Data Infrastructure Insights-Startseite festgelegt. Sie können die Startseite über die Liste **Dashboards > Alle Dashboards anzeigen** ändern.

Sie können später weitere Dashboards importieren, oder "Erstellen Sie Ihre eigene".

Mehr ist nicht nötig

Nach Abschluss des anfänglichen Einrichtungsvorgangs beginnt Ihre Umgebung mit der Erfassung der Daten.

Wenn der anfängliche Setup-Vorgang unterbrochen wird (z. B. wenn Sie das Browser-Fenster schließen), müssen Sie die folgenden Schritte manuell ausführen:

- Wählen Sie einen Data Collector aus
- Installieren Sie einen Agenten oder eine Akquisitionseinheit, wenn Sie dazu aufgefordert werden
- Konfigurieren Sie den Data Collector

Nützliche Definitionen

Die folgenden Definitionen können hilfreich sein, wenn es um Datensammler oder Funktionen von Data Infrastructure Insights geht:

- Kollektorlebenszyklus: Ein Sammler wird zu einem der folgenden Zustände in seinem Lebenszyklus gehören:

- **Vorschau**: Verfügbar in begrenzter Kapazität oder für ein begrenztes Publikum. "Vorschaufunktionen" Und Datensammler werden nach dem Vorschauzeitraum voraussichtlich GA werden. Die Vorschauzeiträume variieren je nach Zielgruppe oder Funktion.
- **GA**: Ein Feature oder Datensammler, der allgemein für alle Kunden verfügbar ist, basierend auf Edition oder Feature Set.
- **Deparated**: Gilt für Datensammler, die funktionell nicht mehr nachhaltig sind oder werden sollen. Veraltete Datensammler werden häufig durch neuere, funktional aktualisierte Datensammler ersetzt.
- **Gelöscht**: Ein Datensammler, der entfernt wurde und nicht mehr verfügbar ist.

- Acquisition Unit: Ein Computer, der Datensammler hostet, typischerweise eine virtuelle Maschine. Dieser Computer befindet sich in der Regel im selben Rechenzentrum/VPC wie die überwachten Objekte.
- Datenquelle: Ein Modul zur Kommunikation mit einem Hardware- oder Software-Stack. Es besteht aus einer Konfiguration und einem Code, der auf dem AU-Computer ausgeführt wird, um mit dem Gerät zu kommunizieren.

Anforderungen An Die Erfassungseinheit

Sie müssen eine Acquisition Unit (AU) installieren, um Informationen aus Ihren Infrastrukturdatenkollektoren (Speicher, VM, Port, EC2 usw.) zu erhalten. Bevor Sie die Acquisition Unit installieren, sollten Sie sicherstellen, dass Ihre Umgebung den Anforderungen für Betriebssystem, CPU, Arbeitsspeicher und Festplattenspeicher entspricht.

Anforderungen

Komponente	Linux-Anforderungen Erfüllt	Windows Anforderungen

Betriebssystem	Ein Computer, auf dem eine lizenzierte Version einer der folgenden Versionen ausgeführt wird: * CentOS (64 Bit): 7.2 bis 7.9, 8.1 bis 8.4, Stream 8, Stream 9 * AlmaLinux 9.3 und 9.4 * Debian (64-bit): 9 und 10 * OpenSUSE Leap 15.1 bis 15.5 * Oracle Enterprise Linux (64 Bit): 7.5 bis 7.9, 8.1 bis 8.8 * Red hat Enterprise Linux (64 Bit): 7.2 bis 7.9, 8.1 bis 8.10, 9.1 bis 9.4 * Rocky 9.0 bis 9.4 * SUSE Enterprise Linux Server 15, 15 SP2 bis 15 SP5 * Ubuntu Server: 18.04, 20.04, 22.04 LTS * SELinux auf den oben genannten Plattformen Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen. Wenn Sie mit SELinux arbeiten, wird empfohlen, die folgenden Befehle auf dem Erfassungseinheitssystem auszuführen: Sudo semanage fcontext -a -t usr_t "/opt/netapp/Cloudinsights(/.*)?“ Sudo restorecon -R /opt/netapp/Cloud Insights	Ein Computer mit einer lizenzierten Version von einer der folgenden Komponenten: * Microsoft Windows 10 64-Bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen.
CPU	2 CPU-Kerne	Gleich
Speicher	8 GB RAM	Gleich
Verfügbarer Festplattenspeicher	50 GB (100 GB empfohlen) Bei Linux sollte der Speicherplatz folgendermaßen zugewiesen werden: /Opt/netapp 10 GB (20 GB für große Umgebungen) /Var/log/netapp 40 GB (80 GB für große Umgebungen) /Tmp mindestens 1 GB während der Installation verfügbar	50 GB

Netzwerk	Ethernet-Verbindung mit 100 Mbit/s/1 Gbit/s, statische IP-Adresse und Anschluss 80 oder 443 von Acquisition Unit zu *.cloudinsights.NetApp.com oder Ihrer Data Infrastructure Insights-Umgebung (d. h. https://<environment_id>.c01.cloudinsights.NetApp.com) sind erforderlich. Informationen zu Anforderungen zwischen der Erfassungseinheit und jedem Data Collector finden Sie in den Anweisungen für "Data Collector". Wenn Ihr Unternehmen die Proxy-Nutzung für den Internetzugang benötigt, müssen Sie möglicherweise das Proxy-Verhalten Ihres Unternehmens kennen und bestimmte Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Blockiert Ihr Unternehmen beispielsweise standardmäßig den Zugriff und gewährt ausnahmsweise nur Zugriff auf bestimmte Websites/Domänen? In diesem Fall müssen Sie die folgende Domain zur Ausnahmeliste hinzufügen: *.cloudinsights.NetApp.com Weitere Informationen finden Sie unter Proxies "Hier (Linux)" oder "Hier (Windows)".	Gleich
Berechtigungen	Sudo-Berechtigungen auf dem Akquisitionsgruppenserver. /Tmp muss mit exec-Funktionen montiert werden.	Administratorberechtigungen auf dem Akquisitionsbereiches-Server
Virenscan		Während der Installation müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die Pfade, die von der Software Acquisition Unit verwendet werden, vom Virenscan ausgeschlossen werden.

Zusätzliche Empfehlungen

- Für eine genaue Audit- und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Acquisition Unit-Rechner mit **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Bezüglich Der Größenanpassung

Beginnen Sie mit einer Data Infrastructure Insights Acquisition Unit mit nur 8 GB Arbeitsspeicher und 50 GB Festplattenspeicher. In größeren Umgebungen sollten Sie sich jedoch folgende Fragen stellen:

Vorteile:

- Mehr als 2500 virtuelle Maschinen oder 10 große (> 2 Nodes) ONTAP-Cluster, Symmetrix oder HDS/HPE VSP/XP-Arrays auf dieser Acquisition Unit ermitteln?
- 75 oder mehr Datensammler auf dieser Akquisitionseinheit bereitstellen?

Für jede „Ja“ Antwort oben empfiehlt es sich, 8 GB Arbeitsspeicher und 50 GB Festplattenspeicher zur AU hinzuzufügen. Wenn Sie also beispielsweise beide Fragen mit „Ja“ beantwortet haben, sollten Sie ein 24-GB-Speichersystem mit 150 GB oder mehr Festplattenspeicher implementieren. Unter Linux wird der Speicherplatz, der dem Protokollverzeichnis hinzugefügt werden soll, hinzugefügt.

Wenn Sie weitere Fragen zur Dimensionierung benötigen, wenden Sie sich an den NetApp Support.

Zusätzliche Federal Edition-Anforderung

- Für Acquisition Unit-Installationen in Data Infrastructure Insights Federal Edition-Clustern muss das zugrunde liegende Betriebssystem über eine gute Entropiequelle verfügen. Auf Linux-Systemen erfolgt dies typischerweise durch die Installation von *rng-Tools* oder durch die Hardware-Zufallszahlengenerierung (RNG). Es liegt in der Verantwortung des Kunden, sicherzustellen, dass diese Anforderung auf der Maschine der Erfassungseinheit erfüllt wird.

Konfigurieren Von Akquisitionseinheiten

Data Infrastructure Insights erfasst Gerätedaten mithilfe einer oder mehrerer auf lokalen Servern installierten Acquisition Units. Jede Erfassungseinheit kann mehrere Datensammler hosten, die Gerätekennzahlen zur Analyse an Data Infrastructure Insights senden.

In diesem Thema wird beschrieben, wie Sie Akquisitionseinheiten hinzufügen und zusätzliche Schritte beschrieben, die erforderlich sind, wenn in Ihrer Umgebung ein Proxy verwendet wird.

> Für eine genaue Audit- und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Acquisition Unit-Rechner mit **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Erfahren Sie mehr über Data Infrastructure Insights Security "Hier".

Hinzufügen einer Linux-Akquisitionseinheit

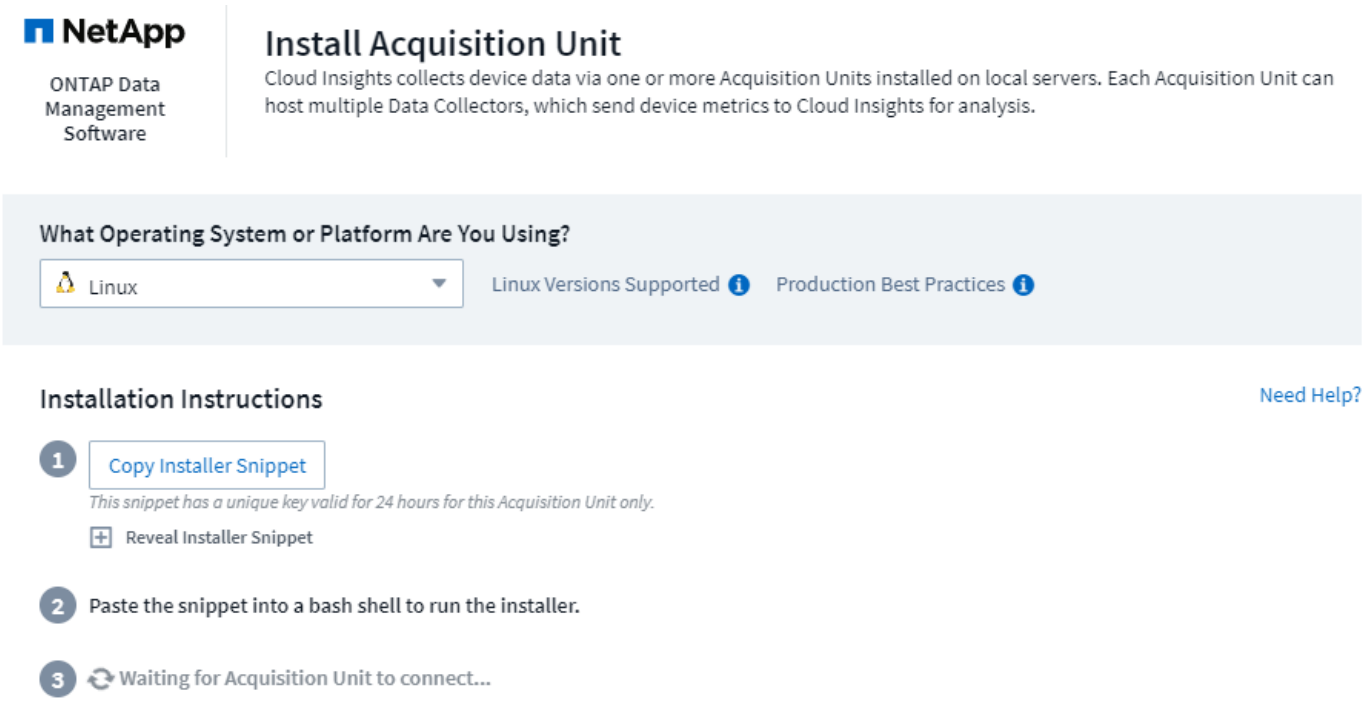
Bevor Sie beginnen

- Wenn Ihr System einen Proxy verwendet, müssen Sie die Proxy-Umgebungsvariablen festlegen, bevor die Erfassungseinheit installiert wird. Weitere Informationen finden Sie unter Festlegen von Proxy-Umgebungsvariablen.

Schritte für die Installation der Linux-Erfassungseinheit

1. Melden Sie sich als Administrator oder Account Owner bei Ihrer Data Infrastructure Insights-Umgebung an.
2. Klicken Sie Auf **Observability > Collectors > Acquisition Units > +Acquisition Unit**

Das Dialogfeld „_Erfassungseinheit installieren “ wird angezeigt. Wählen Sie Linux.



1. Vergewissern Sie sich, dass der Server oder die VM, auf dem die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
2. Vergewissern Sie sich, dass auf dem Server eine unterstützte Linux-Version ausgeführt wird. Klicken Sie auf *OS-Versionen supported (i)*, um eine Liste der unterstützten Versionen anzuzeigen.
3. Kopieren Sie den Befehl Installation snippet im Dialogfeld in ein Terminal-Fenster auf dem Server oder der VM, auf dem die Erfassungseinheit gehostet wird.
4. Fügen Sie den Befehl in die Bash-Shell ein und führen Sie ihn aus.

Nachdem Sie fertig sind

- Klicken Sie auf **Observability > Collectors > Acquisition Units**, um den Status von Acquisition Units zu überprüfen.
- Die Protokolle der Acquisition Unit finden Sie unter /var/log/netapp/nebinsights/acq/acq.log
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu steuern:
  - cloudinsights-service.sh (Stopp, Start, Neustart, Status überprüfen)
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu deinstallieren:
  - cloudinsights-uninstall.sh

Festlegen von Proxy-Umgebungsvariablen

Für Umgebungen, die einen Proxy verwenden, müssen Sie die Variablen für die Proxy-Umgebung festlegen, bevor Sie die Akquisitionseinheit hinzufügen. Die Anweisungen zur Konfiguration des Proxy finden Sie im Dialogfeld „*Acquisition Unit*“.

1. Klicken Sie auf + in *Proxy Server?*
2. Kopieren Sie die Befehle in einen Texteditor und legen Sie die Proxyvariablen nach Bedarf fest.

Hinweis: Beachten Sie die Beschränkungen für Sonderzeichen in den Feldern Proxy-Benutzername und Passwort: '%' und '!' Sind im Feld Benutzername zulässig. ':', '%' und '!' Sind im Feld Passwort zulässig.

3. Führen Sie den bearbeiteten Befehl in einem Terminal mit der Bash-Shell aus.
4. Installieren Sie die Software Acquisition Unit.

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights Server herzustellen. Das Clientzertifikat muss an den Data Infrastructure Insights-Server übergeben werden, um authentifiziert zu werden. Dazu muss der Proxy so eingerichtet sein, dass er die HTTPS-Anforderung an den Data Infrastructure Insights Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights festzulegen, z. B.:

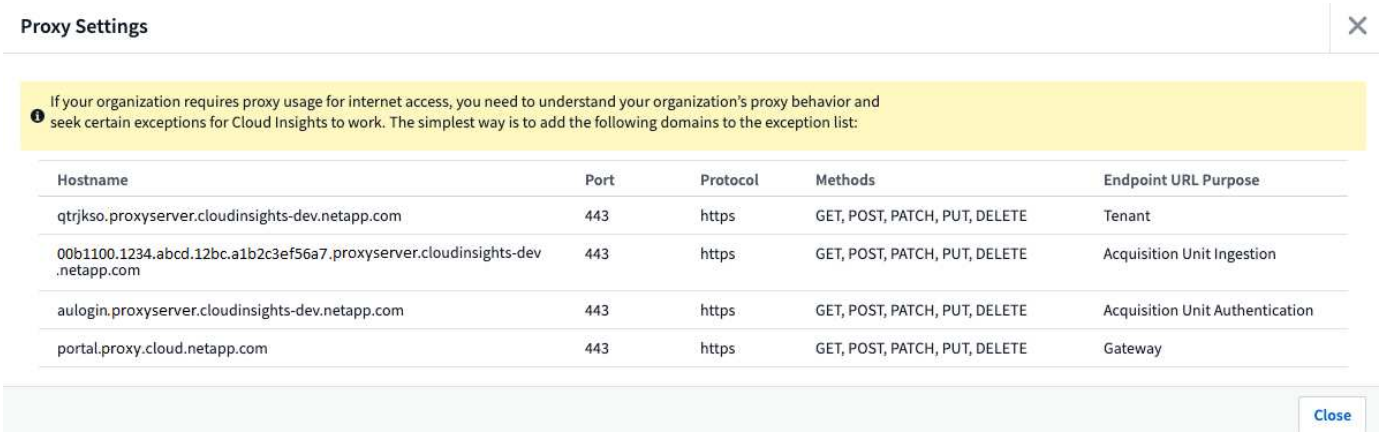
```
*.cloudinsights.netapp.com
```

Die Verwendung eines Sternchen (*) für Platzhalter ist üblich, aber Ihre Proxy-/Firewall-Konfiguration kann ein anderes Format verwenden. Fragen Sie in Ihrer Proxy-Dokumentation nach, um die korrekte Platzhalterspezifikation in Ihrer Umgebung sicherzustellen.

Weitere Informationen zur Proxy-Konfiguration finden Sie im NetApp "Wissensdatenbank".

Anzeigen von Proxy-URLs

Sie können Ihre Proxy-Endpunkt-URLs anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboarding auf den Link **Proxy-Einstellungen** klicken oder auf der Seite **Hilfe > Support** den Link unter *Proxy-Einstellungen*. Eine Tabelle wie die folgende wird angezeigt.



Wenn Sie Workload Security in Ihrer Umgebung haben, werden auch die konfigurierten Endpunkt-URLs in dieser Liste angezeigt.

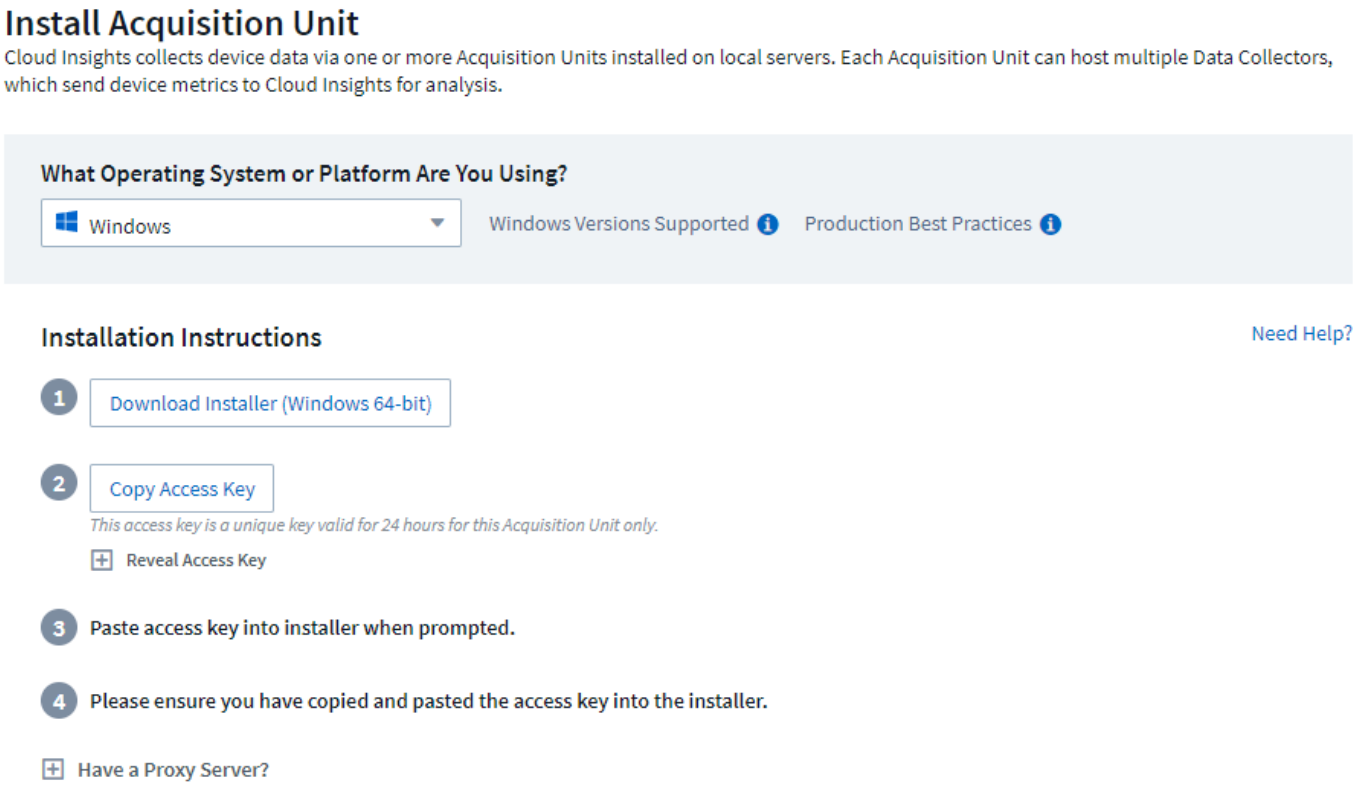
Hinzufügen einer Windows-Erfassungseinheit

Schritte für die Installation der Windows-Erfassungseinheit

1. Melden Sie sich als Benutzer mit Administratorrechten beim Server/der VM der Erfassungseinheit an.

2. Öffnen Sie auf diesem Server ein Browserfenster, und melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights-Umgebung an.
3. Klicken Sie Auf **Observability > Collectors > Acquisition Units > +Acquisition Unit** .

   Das Dialogfeld „_Erfassungseinheit installieren “ wird angezeigt. Wählen Sie Windows.



1. Vergewissern Sie sich, dass der Server oder die VM, auf dem die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
2. Überprüfen Sie, ob auf dem Server eine unterstützte Windows-Version ausgeführt wird. Klicken Sie auf *OS-Versionen supported (i)*, um eine Liste der unterstützten Versionen anzuzeigen.
3. Klicken Sie auf die Schaltfläche **Download Installer (Windows 64-bit)**.
4. Kopieren Sie den Zugriffsschlüssel. Sie benötigen diese während der Installation.
5. Führen Sie auf dem Erfassungseinheit-Server/VM das heruntergeladene Installationsprogramm aus.
6. Fügen Sie den Zugriffsschlüssel bei Aufforderung in den Installationsassistenten ein.
7. Während der Installation erhalten Sie die Möglichkeit, Ihre Proxy-Server-Einstellungen vorzunehmen.

Nachdem Sie fertig sind

- Klicken Sie auf * > Observability > Collectors > Acquisition Units*, um den Status von Acquisition Units zu überprüfen.
- Sie können das Protokoll der Erfassungseinheit in <install dir>\Cloud Insights\Acquisition Unit\log\acq.log aufrufen
- Verwenden Sie das folgende Skript, um den Status der Erfassungseinheit zu beenden, zu starten, neu zu starten oder zu überprüfen:

```
cloudinsights-service.sh
```

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights Server herzustellen. Das Clientzertifikat muss an den Data Infrastructure Insights-Server übergeben werden, um authentifiziert zu werden. Dazu muss der Proxy so eingerichtet sein, dass er die HTTPS-Anforderung an den Data Infrastructure Insights Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights festzulegen, z. B.:

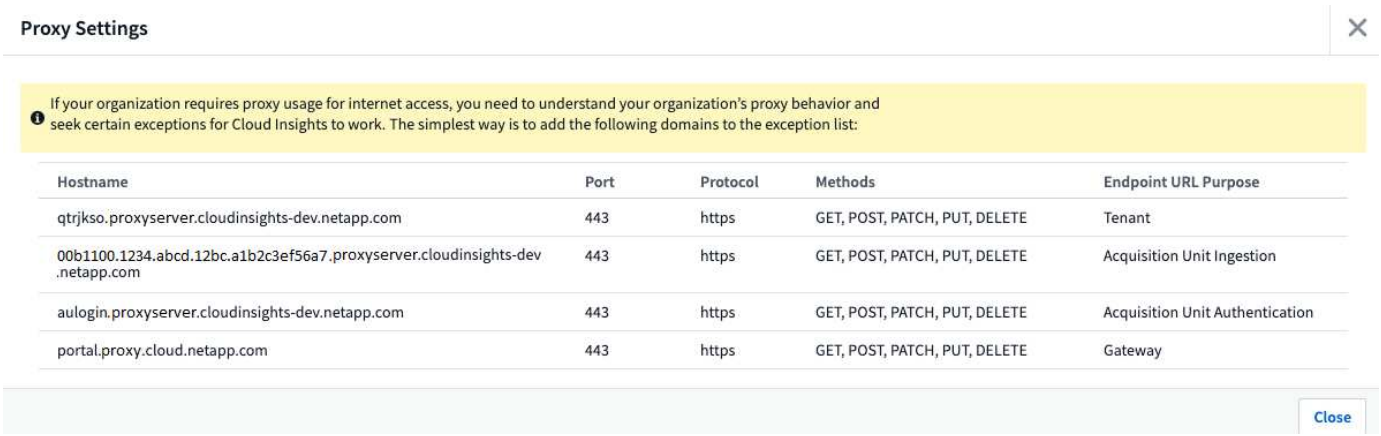
```
*.cloudinsights.netapp.com
```

Die Verwendung eines Sternchen (*) für Platzhalter ist üblich, aber Ihre Proxy-/Firewall-Konfiguration kann ein anderes Format verwenden. Fragen Sie in Ihrer Proxy-Dokumentation nach, um die korrekte Platzhalterspezifikation in Ihrer Umgebung sicherzustellen.

Weitere Informationen zur Proxy-Konfiguration finden Sie im NetApp "Wissensdatenbank".

Anzeigen von Proxy-URLs

Sie können Ihre Proxy-Endpunkt-URLs anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboarding auf den Link **Proxy-Einstellungen** klicken oder auf der Seite **Hilfe > Support** den Link unter *Proxy-Einstellungen*. Eine Tabelle wie die folgende wird angezeigt.



Wenn Sie Workload Security in Ihrer Umgebung haben, werden auch die konfigurierten Endpunkt-URLs in dieser Liste angezeigt.

Deinstallation einer Akquisitionseinheit

Gehen Sie zum Deinstallieren der Software Acquisition Unit wie folgt vor:

Windows:

Wenn Sie eine **Windows**-Erfassungseinheit deinstallieren:

1. Öffnen Sie auf dem Acquisition Unit Server/VM die Systemsteuerung und wählen Sie **Programm deinstallieren**. Wählen Sie das Programm Data Infrastructure Insights Acquisition Unit aus, das Sie entfernen möchten.
2. Klicken Sie auf Deinstallieren, und befolgen Sie die Anweisungen.

Linux:

Wenn Sie eine **Linux**-Erfassungseinheit deinstallieren:

1. Führen Sie auf dem Server/VM der Acquisition Unit den folgenden Befehl aus:

```
 sudo cloudinsights-uninstall.sh -p
. Um Hilfe bei der Deinstallation zu erhalten, führen Sie folgende
Schritte aus:
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows und Linux:

Nach die AU deinstallieren:

1. Gehen Sie in Data Infrastructure Insights zu **Observability > Collectors und wählen Sie die Registerkarte *Acquisition Units** aus.
2. Klicken Sie rechts neben der zu deinstallierenden Erfassungseinheit auf die Schaltfläche Optionen, und wählen Sie *Löschen*. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.

> Eine Acquisition Unit (AU), mit der Datensammler verbunden sind, kann nicht gelöscht werden. Verschieben Sie alle AU Datensammler auf eine andere AU (bearbeiten Sie den Sammler und wählen Sie einfach eine andere AU), bevor Sie die ursprüngliche AU löschen.

Für die Geräteauflösung wird eine Akquisitionseinheit mit einem Stern daneben verwendet. Bevor Sie diese AU entfernen, müssen Sie ein anderes AU auswählen, das für die Geräteauflösung verwendet werden soll. Bewegen Sie den Mauszeiger über eine andere AU, und öffnen Sie das Menü „drei Punkte“, um „für Geräteauflösung verwenden“ auszuwählen.

Erneutes Installieren einer Erfassungseinheit

Um eine Erfassungseinheit auf demselben Server/derselben VM neu zu installieren, müssen Sie folgende Schritte ausführen:

Bevor Sie beginnen

Sie müssen eine temporäre Erfassungseinheit auf einem separaten Server/einer separaten VM konfigurieren, bevor Sie eine Akquisitionseinheit neu installieren.

Schritte

1. Melden Sie sich beim Server/VM der Acquisition Unit an und deinstallieren Sie die AU-Software.
2. Melden Sie sich bei Ihrer Data Infrastructure Insights-Umgebung an, und rufen Sie **Observability > Collectors** auf.
3. Klicken Sie für jeden Datensammler rechts auf das Menü Optionen, und wählen Sie *Bearbeiten*. Weisen Sie den Datensammler der temporären Erfassungseinheit zu und klicken Sie auf **Speichern**.

   Sie können auch mehrere Datensammler desselben Typs auswählen und auf die Schaltfläche **Massenaktionen** klicken. Wählen Sie *Bearbeiten* und weisen Sie die Datensammler der temporären Erfassungseinheit zu.

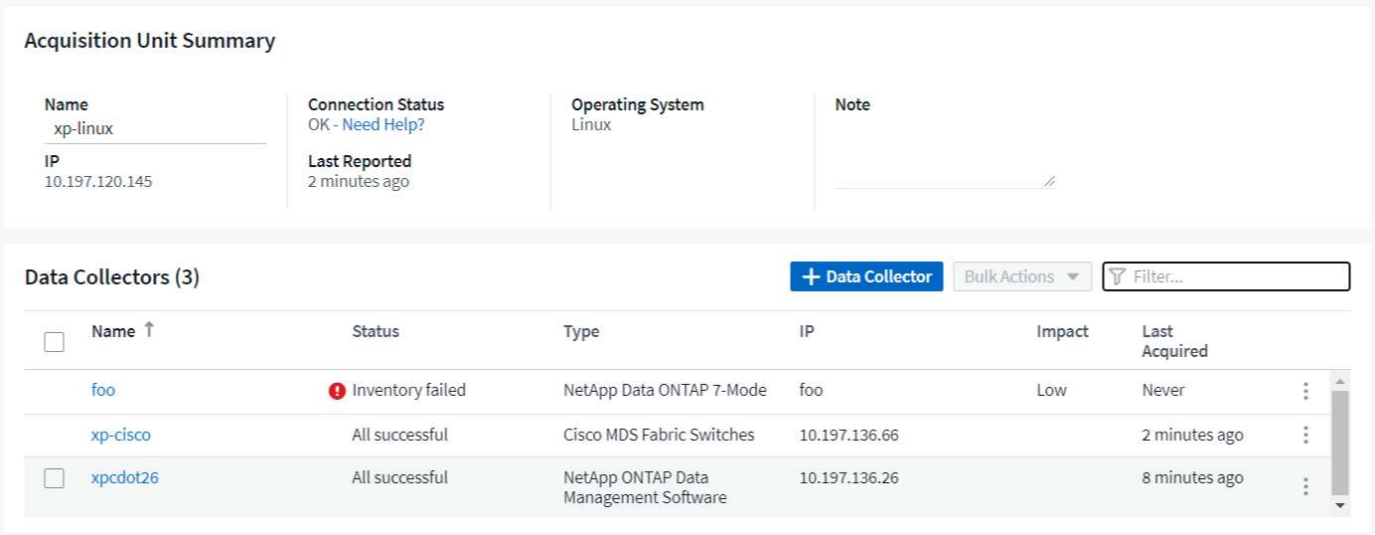
4. Nachdem alle Datensammler in die temporäre Erfassungseinheit verschoben wurden, gehen Sie zu **Observability > Collectors** und wählen Sie die Registerkarte **Erfassungseinheiten**.
5. Klicken Sie auf die Schaltfläche Optionen rechts neben der Erfassungseinheit, die Sie neu installieren möchten, und wählen Sie *Löschen*. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.
6. Sie können die Software Acquisition Unit jetzt auf dem ursprünglichen Server/VM neu installieren. Klicken Sie auf **+Acquisition Unit**, und befolgen Sie die Anweisungen oben, um die Acquisition Unit zu installieren.
7. Sobald die Erfassungseinheit neu installiert wurde, weisen Sie Ihre Datensammler der Akquisitionseinheit zu.

Anzeigen von AU-Details

Die Seite Acquisition Unit (AU) enthält nützliche Details für eine AU sowie Informationen zur Fehlerbehebung. Die AU-Detailseite enthält die folgenden Abschnitte:

- Ein Abschnitt **Zusammenfassung** mit folgenden Informationen:
  - **Name** und **IP** der Akquisitionseinheit
  - Aktuelle Verbindung **Status** der AU
  - **Zuletzt berichtet** erfolgreiche Datensammler-Abfragzeit
  - Das **Betriebssystem** der AU Maschine
  - Alle aktuellen **Hinweis** für die AU. Verwenden Sie dieses Feld, um einen Kommentar für die AU einzugeben. Das Feld zeigt die zuletzt hinzugefügte Notiz an.
- Eine Tabelle der AU's **Data Collectors** für jeden Datensammler:
  - **Name** - Klicken Sie auf diesen Link, um die Detailseite des Datensammlers mit zusätzlichen Informationen aufzurufen
  - **Status** - Erfolg- oder Fehlerinformationen
  - **Typ** - Hersteller/Modell

- **IP** Adresse des Datensammlers
- Aktuelle * Auswirkung*-Stufe
- **Zuletzt erfasste** Zeit - als der Datensammler zuletzt erfolgreich abgefragt wurde



Für jeden Datensammler können Sie auf das Menü „drei Punkte“ klicken, um den Datensammler zu klonen, zu bearbeiten, abzuspeichern oder zu löschen. Sie können auch mehrere Datensammler in dieser Liste auswählen, um Massenaktionen auf ihnen durchzuführen.

Um die Akquisitionseinheit neu zu starten, klicken Sie oben auf der Seite auf die Schaltfläche **Neustart**. Klicken Sie auf diese Schaltfläche, um zu versuchen, im Falle eines Verbindungsproblems eine Verbindung* mit der AU herzustellen.

Konfigurieren eines Agenten zur Datenerfassung (Windows/Linux)

Data Infrastructure Insights verwendet "Telegraf" als Agent für die Erfassung von Integrationsdaten. Telegraf ist ein Plug-in-gestützter Server-Agent, mit dem Kennzahlen, Ereignisse und Protokolle erfasst und protokolliert werden können. Input-Plugins werden verwendet, um die gewünschten Informationen in den Agenten zu sammeln, indem Sie direkt auf das System/Betriebssystem zugreifen, indem Sie APIs von Drittanbietern aufrufen oder konfigurierte Streams (d. h. anhören Kafka, StatsD usw.). Output-Plug-ins werden verwendet, um die vom Agenten gesammelten Kennzahlen, Ereignisse und Protokolle an Data Infrastructure Insights zu senden.

Die aktuelle Telegraf Version für Data Infrastructure Insights ist **1.24.0**.

Informationen zur Installation auf Kubernetes finden Sie im "NetApp Kubernetes Monitoring Operator" Seite.

Für eine genaue Audit- und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Rechner mit **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Wenn Sie die Installationsdateien überprüfen möchten, bevor Sie den Agent installieren, lesen Sie den Abschnitt unten auf Prüfsummen Werden Überprüft.

Installieren eines Agenten

Wenn Sie einen Service Data Collector installieren und noch keinen Agent konfiguriert haben, werden Sie aufgefordert, zuerst einen Agent für das entsprechende Betriebssystem zu installieren. Dieses Thema enthält Anweisungen zur Installation des Telegraf-Agenten auf folgenden Betriebssystemen:

- Windows
- RHEL und CentOS
- Ubuntu und Debian

Um einen Agent zu installieren, müssen Sie, unabhängig von der verwendeten Plattform, zunächst die folgenden Schritte ausführen:

1. Melden Sie sich beim Host an, den Sie für Ihren Agenten verwenden werden.
2. Melden Sie sich in Ihrer Data Infrastructure Insights-Umgebung an, und navigieren Sie zu **Observability > Collectors**.
3. Klicken Sie auf **+Data Collector** und wählen Sie einen zu installierenden Datensammler aus.
4. Wählen Sie die passende Plattform für Ihren Host (Windows, Linux)
5. Befolgen Sie die verbleibenden Schritte für jede Plattform.

Sobald Sie einen Agent auf einem Host installiert haben, müssen Sie auf diesem Host keinen Agenten mehr installieren.

Sobald Sie einen Agenten auf einem Server/einer VM installiert haben, erfasst Data Infrastructure Insights neben der Erfassung von Daten aus dem System auch Kennzahlen aus dem System. Diese Kennzahlen werden als gesammelt"Node-Metriken".

Wenn Sie einen Proxy verwenden, lesen Sie die Proxy-Anweisungen für Ihre Plattform, bevor Sie den Telegraf-Agent installieren.

Speicherorte Protokollieren

Telegraf-Protokollmeldungen werden von stdout zu den folgenden Standardprotokolldateien umgeleitet:

- RHEL/CentOS: /Var/log/telegraf/telegraf.log
- Ubuntu/Debian: /Var/log/telegraf/telegraf.log
- Windows: C:\Programme\telegraf\telegraf.log

Windows

Voraussetzungen:

- PowerShell muss installiert sein
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt * Proxy-Unterstützung für Windows konfigurieren* befolgen.

Proxy-Unterstützung für Windows wird konfiguriert

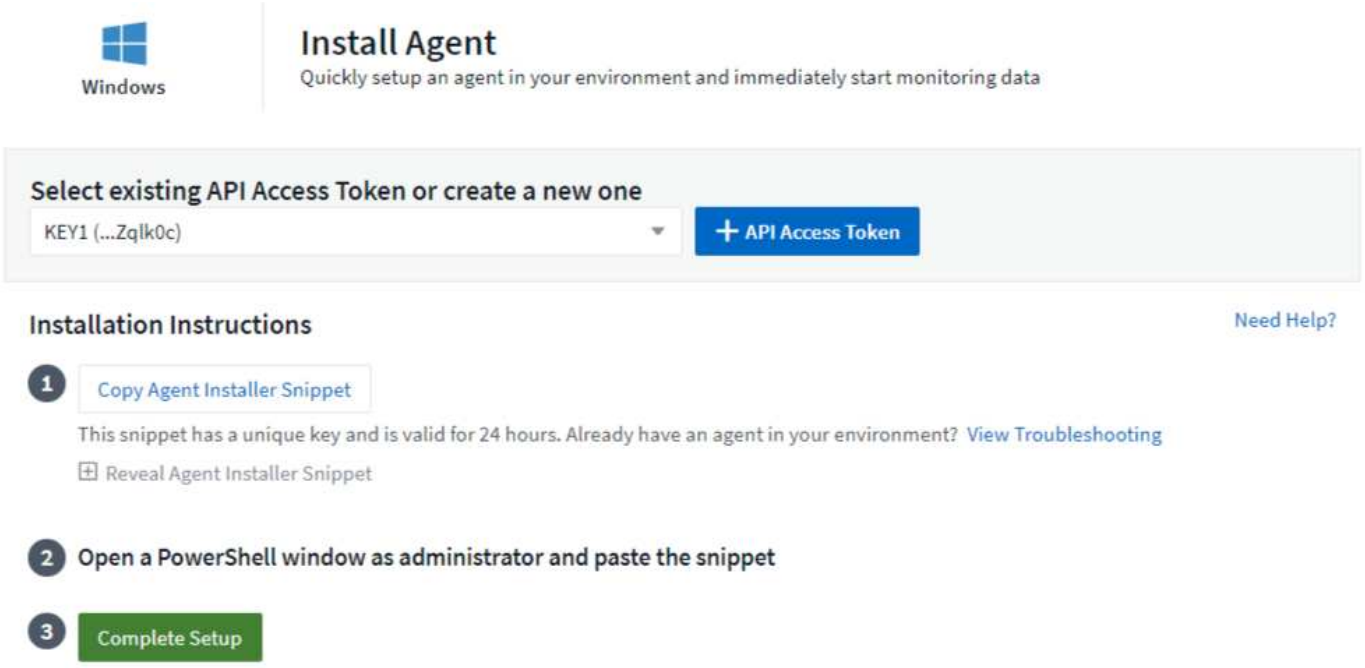
Wenn in Ihrer Umgebung ein Proxy verwendet wird, lesen Sie diesen Abschnitt vor der Installation.

In den folgenden Schritten werden die Aktionen beschrieben, die zum Festlegen der Umgebungsvariablen *http_Proxy/HTTPS_Proxy* erforderlich sind. In einigen Proxyumgebungen müssen Benutzer möglicherweise auch die Variable *no_Proxy-Umgebung* einstellen.

Führen Sie für Systeme, die sich hinter einem Proxy befinden, folgende Schritte aus, um die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* vor der Installation des Telegraf-Agenten festzulegen:

```
[System.Environment]::SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>",
[System.EnvironmentVariableTarget]::Machine)
```

Installieren des Agenten



Schritte zur Installation von Agent unter Windows:

1. Wählen Sie einen Agent-Zugriffsschlüssel aus.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Clipboard-Symbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein PowerShell-Fenster
4. Fügen Sie den Befehl in das PowerShell Fenster ein, und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Nach Abschluss des Vorgangs wird der Agent-Service neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nach der Installation des Agent können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

```
Start-Service telegraf
Stop-Service telegraf
```

Deinstallieren des Agenten

Gehen Sie zum Deinstallieren des Agent unter Windows in einem PowerShell-Fenster wie folgt vor:

1. Stoppen und löschen Sie den Telegraf-Dienst:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Entfernen Sie das Zertifikat aus dem trustore:

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Löschen Sie den Ordner *C:\Programme\telegraf*, um die Binärdateien, Protokolle und Konfigurationsdateien zu entfernen
4. Entfernen Sie den Schlüssel *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* aus der Registrierung

Aktualisieren des Agenten

Um den telegraf-Agent zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen und löschen sie den telegraf-Dienst:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Löschen Sie den Schlüssel *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* aus der Registrierung
3. Löschen *C:\Programme\telegraf\telegraf.conf*
4. Löschen Sie *C:\Programme\telegraf\telegraf.exe*
5. "Installieren Sie den neuen Agenten".

RHEL und CentOS

Voraussetzungen:

- Folgende Befehle müssen verfügbar sein: Curl, sudo, ping, sha256sum, openssl, Und Dmidecode
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt * Proxy-

Unterstützung für RHEL/CentOS* befolgen.

Proxy-Unterstützung für RHEL/CentOS wird konfiguriert

Wenn in Ihrer Umgebung ein Proxy verwendet wird, lesen Sie diesen Abschnitt vor der Installation.

In den folgenden Schritten werden die Aktionen beschrieben, die zum Festlegen der Umgebungsvariablen *http_Proxy/HTTPS_Proxy* erforderlich sind. In einigen Proxyumgebungen müssen Benutzer möglicherweise auch die Variable *no_Proxy-Umgebung* einstellen.

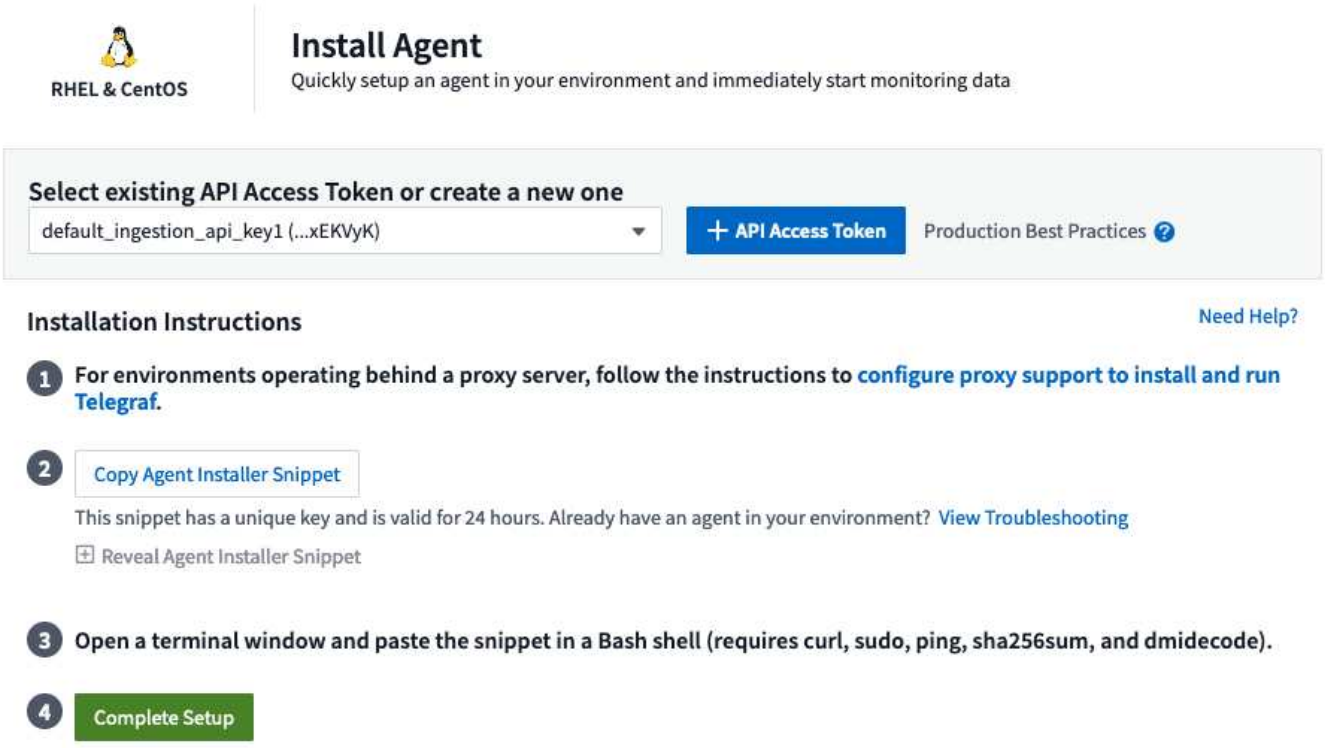
Führen Sie für Systeme, die sich hinter einem Proxy befinden, die folgenden Schritte vor der Installation des Telegraf-Agenten durch:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:

```
 export https_proxy=<proxy_server>:<proxy_port>
. _/etc/default/telegraf_ erstellen und Definitionen für die
Variable(en) _https_Proxy_ und/oder _http_Proxy_ einfügen:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installieren des Agenten



Schritte zum Installieren von Agent auf RHEL/CentOS:

1. Wählen Sie einen Agent-Zugriffsschlüssel aus.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Clipboard-Symbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein Fenster „Bash“
4. Fügen Sie den Befehl in das Fenster „Bash“ ein, und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Nach Abschluss des Vorgangs wird der Agent-Service neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nach der Installation des Agent können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

Wenn Ihr Betriebssystem systemd (CentOS 7+ und RHEL 7+) verwendet:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Wenn Ihr Betriebssystem keine systemd verwendet (CentOS 7+ und RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Deinstallieren des Agenten

Gehen Sie zum Deinstallieren des Agent auf RHEL/CentOS in einem Bash Terminal wie folgt vor:

1. Stoppen Sie den Telegraf-Service:

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Entfernen Sie den Telegraf-Agent:

   ```
    yum remove telegraf
   . Entfernen Sie alle Konfigurations- oder Protokolldateien, die
   zurückgelassen werden können:
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Aktualisieren des Agenten

Um den telegraf-Agent zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen sie den telegraf-Service:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den vorherigen telegraf-Agent:

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Installieren Sie den neuen
Agenten"].
```

Ubuntu und Debian

Voraussetzungen:

- Folgende Befehle müssen verfügbar sein: Curl, sudo, ping, sha256sum, openssl, Und Dmidecode
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt * Proxy-Unterstützung für Ubuntu/Debian* befolgen.

Proxy-Unterstützung für Ubuntu/Debian konfigurieren

Wenn in Ihrer Umgebung ein Proxy verwendet wird, lesen Sie diesen Abschnitt vor der Installation.

In den folgenden Schritten werden die Aktionen beschrieben, die zum Festlegen der Umgebungsvariablen *http_Proxy/HTTPS_Proxy* erforderlich sind. In einigen Proxyumgebungen müssen Benutzer möglicherweise auch die Variable *no_Proxy-Umgebung* einstellen.

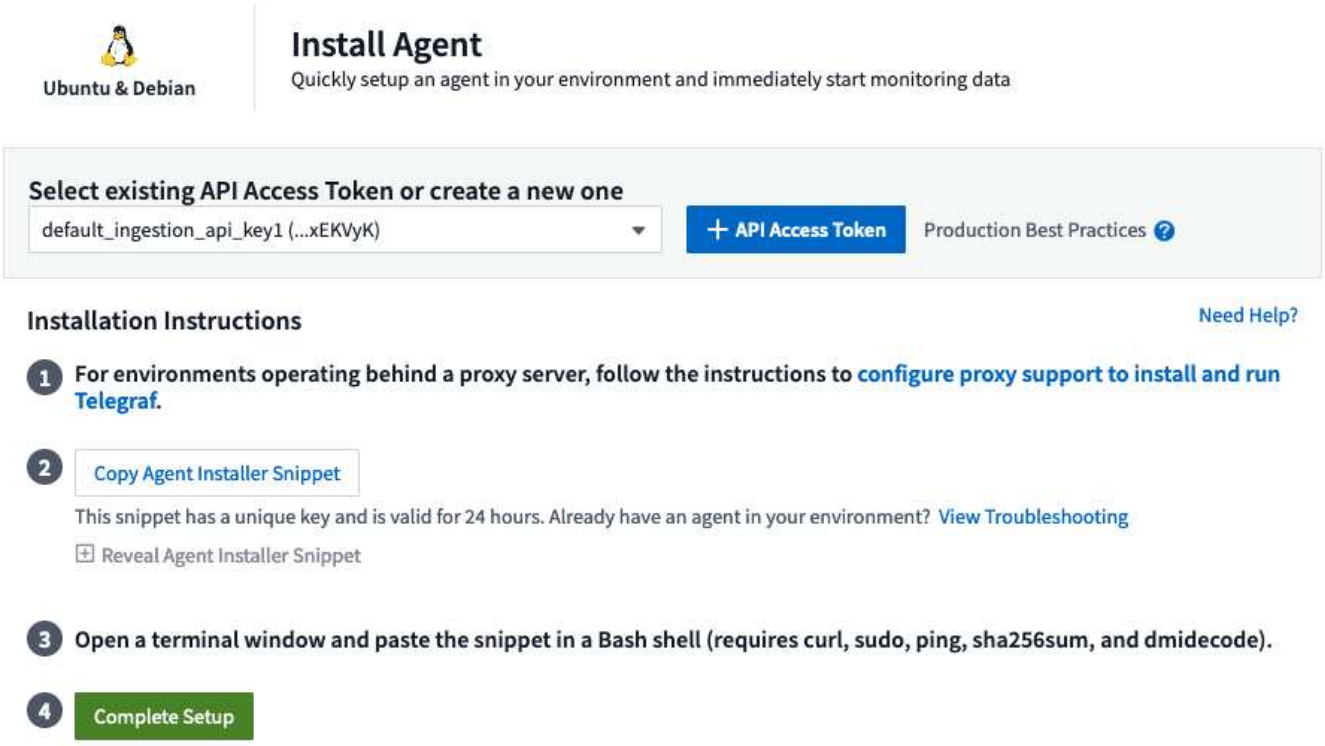
Führen Sie für Systeme, die sich hinter einem Proxy befinden, die folgenden Schritte vor der Installation des Telegraf-Agenten durch:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Erstellen Sie /etc/default/telegraf und fügen Sie Definitionen für die
Variable(en) _https_Proxy_ und/oder _http_Proxy_ ein:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installieren des Agenten



Schritte zur Installation von Agent auf Debian oder Ubuntu:

1. Wählen Sie einen Agent-Zugriffsschlüssel aus.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Clipboard-Symbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein Fenster „Bash“
4. Fügen Sie den Befehl in das Fenster „Bash“ ein, und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Nach Abschluss des Vorgangs wird der Agent-Service neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nach der Installation des Agent können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

Wenn Ihr Betriebssystem systemd verwendet:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Wenn Ihr Betriebssystem keine systemd verwendet:

```
sudo service telegraf start
sudo service telegraf stop
```

Deinstallieren des Agenten

Um den Agent auf Ubuntu/Debian zu deinstallieren, führen Sie in einem Bash-Terminal Folgendes aus:

1. Stoppen Sie den Telegraf-Service:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den Telegraf-Agent:

```
 dpkg -r telegraf
. Entfernen Sie alle Konfigurations- oder Protokolldateien, die
zurückgelassen werden können:
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Aktualisieren des Agenten

Um den telegraf-Agent zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen sie den telegraf-Service:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Entfernen Sie den vorherigen telegraf-Agent:

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Installieren Sie den neuen
Agenten"].
```

Prüfsummen Werden Überprüft

Das Installationsprogramm von Data Infrastructure Insights Agent führt Integritätsprüfungen durch, einige Benutzer möchten jedoch möglicherweise ihre eigenen Überprüfungen durchführen, bevor heruntergeladene Artefakte installiert oder angewendet werden. Dazu können Sie das Installationsprogramm herunterladen und eine Prüfsumme für das heruntergeladene Paket erstellen. Anschließend wird die Prüfsumme mit dem in der Installationsanleitung angegebenen Wert verglichen.

Laden Sie das Installationspaket herunter, ohne es zu installieren

Um einen ausschließlich herunterladbaren Vorgang durchzuführen (im Gegensatz zum Standard-Download-and-install), können Benutzer den Agent-Installationbefehl von der UI erhalten bearbeiten und die nachgestellte Option „install“ entfernen.

Führen Sie hierzu folgende Schritte aus:

1. Kopieren Sie das Agent Installer-Snippet wie angewiesen.
2. Anstatt das Snippet in ein Befehlsfenster einzufügen, fügen Sie es in einen Texteditor ein.
3. Entfernen Sie die nachstehende „--install“ (Linux) oder „-install“ (Windows) aus dem Befehl.
4. Kopieren Sie den gesamten Befehl aus dem Texteditor.
5. Fügen Sie es nun in Ihr Befehlsfenster ein (in einem Arbeitsverzeichnis) und führen Sie es aus.

Nicht-Windows (diese Beispiele gelten für Kubernetes; die tatsächlichen Skriptnamen können variieren):

- Download und Installation (Standard):

```
 installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download --install
* Nur Download:
```

```
installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download
```

Windows:

- Download und Installation (Standard):

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download -install)
* Nur Download:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download)
```

Mit dem Befehl „nur herunterladen“ werden alle erforderlichen Artefakte aus Data Infrastructure Insights in das Arbeitsverzeichnis heruntergeladen. Die Artefakte umfassen, dürfen aber nicht beschränkt sein auf:

- Ein Installationsskript
- Einer Umgebungsdatei
- YAML-Dateien
- Eine Prüfsummendatei (endet mit sha256.signed oder sha256.ps1)

Das Installationsskript, die Umgebungsdatei und die YAML-Dateien können mittels Sichtprüfung verifiziert werden.

Prüfsummenwert generieren

Um den Prüfsummenwert zu generieren, führen Sie für die entsprechende Plattform den folgenden Befehl aus:

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* Windows:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Überprüfen Sie die Prüfsumme

Extrahieren Sie die erwartete Prüfsumme aus der Prüfsummendatei

- Nicht Windows:

```
 openssl smime -verify -in telegraf*.sha256.signed -CAfile
netapp_cert.pem -purpose any -nosigs -noverify
* Windows:
```

```
(Get-Content telegraf.zip.sha256.ps1 -First 1).toUpper()
```

Installieren Sie das heruntergeladene Paket

Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die Agenteninstallation durch Ausführen von gestartet werden:

Nicht Windows:

```
 sudo -E -H ./<installation_script_name> --install
Windows:
```

```
.\cloudinsights-windows.ps1 -install
```

Fehlerbehebung

Einige Dinge, die Sie versuchen können, wenn Probleme beim Einrichten eines Agenten auftreten:

Problem:	Versuchen Sie dies:
Nach der Konfiguration eines neuen Plugins und dem Neustart von Telegraf startet Telegraf Telegraf nicht. Die Protokolle zeigen an, dass ein Fehler wie folgt auftritt: "[telegraf] Fehler laufende Agent: Fehler beim Laden der Konfigurationsdatei /etc/telegraf/telegraf.d/cloudinsights-default.conf: Plugin Outputs.http: Line <linenumber>: Configuration specified the fields ["use_System_Proxy"], they were't used"	Die installierte Telegraf-Version ist veraltet. Befolgen Sie die Schritte auf dieser Seite, um **Upgrade the Agent** für Ihre entsprechende Plattform.
Ich habe das Installer-Skript auf einer alten Installation ausgeführt und jetzt sendet der Agent keine Daten	Deinstallieren Sie den telegraf-Agent und führen Sie dann das Installationsskript erneut aus. Folgen Sie den Schritten **Upgrade the Agent** auf dieser Seite für Ihre entsprechende Plattform.
Ich habe bereits einen Agenten installiert, der Data Infrastructure Insights verwendet	Wenn Sie bereits einen Agent auf Ihrem Host/VM installiert haben, müssen Sie den Agent nicht erneut installieren. Wählen Sie in diesem Fall im Bildschirm Agenteninstallation einfach die entsprechende Plattform und die entsprechende Taste aus und klicken Sie auf **Weiter** oder **Fertig**.
Ich habe bereits einen Agenten installiert, aber nicht mit dem Data Infrastructure Insights Installer	Entfernen Sie den vorherigen Agent, und führen Sie die Installation von Data Infrastructure Insights Agent aus, um sicherzustellen, dass die Standardeinstellungen für die Konfigurationsdatei korrekt sind. Klicken Sie nach Abschluss auf **Weiter** oder **Fertig**.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren Von Datensammlern

Sie konfigurieren Data Collectors in Ihrer Data Infrastructure Insights-Umgebung, um Daten von Geräten im Rechenzentrum zu erfassen.

Bevor Sie beginnen

- Sie müssen eine Erfassungseinheit konfiguriert haben, bevor Sie mit dem Erfassen von Daten beginnen können.
- Sie benötigen Anmeldedaten für die Geräte, von denen Sie Daten erfassen.
- Für alle Geräte, von denen Sie Daten erfassen, sind Netzwerkadressen, Kontoinformationen und Passwörter erforderlich.

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**

   Das System zeigt die verfügbaren Datensammler an, die nach Hersteller geordnet sind.

2. Klicken Sie auf **+ Collector**, und wählen Sie den zu konfigurierenden Data Collector aus.

   Im Dialogfeld können Sie den Datensammler konfigurieren und eine Erfassungseinheit hinzufügen.

3. Geben Sie einen Namen für den Datensammler ein.
4. Klicken Sie auf **Erweiterte Konfiguration**, um weitere Konfigurationsfelder hinzuzufügen. (Nicht alle Datensammler benötigen erweiterte Konfiguration.)
5. Klicken Sie auf **Testkonfiguration**, um zu überprüfen, ob der Datensammler ordnungsgemäß konfiguriert ist.
6. Klicken Sie auf **Add Collector**, um die Konfiguration zu speichern und den Data Collector zu Ihrem Data Infrastructure Insights-Mandanten hinzuzufügen.

Es kann bis zu zwei Abfrageperioden dauern, bis die Daten aus dem Dienst in Dashboards angezeigt oder für die Abfrage verfügbar sind.

- 1. Bestandsabfrage: Sofort
- Erste Leistungsdatenabfrage, um eine Basislinie zu erstellen: Unmittelbar nach Bestandsabfrage
- 2. Leistungsumfrage: Innerhalb von 15 Sekunden nach Abschluss der 1. Leistungsumfrage

Die Abfrage erfolgt dann nach den konfigurierten Abfrageintervallen für Bestand und Leistung.

Bestimmen des Erfassungsstatus der Datensammlung

Da Datensammler die primäre Informationsquelle für Einblicke in die Dateninfrastruktur sind, muss sichergestellt werden, dass der Betrieb auch weiterhin gewährleistet ist.

Der Datenerfassungsstatus wird in der rechten oberen Ecke einer beliebigen Asset-Seite als Meldung „Erfasste N Minuten zuvor“ angezeigt, wobei N die letzte Erfassungszeit des Datensammlers des Assets angibt. Die Aufnahmezeit/das Erfassungsdatum wird ebenfalls angezeigt.

Durch Klicken auf die Meldung wird eine Tabelle mit dem Namen, dem Status und der letzten erfolgreichen Aufnahmezeit angezeigt. Wenn Sie als Administrator angemeldet sind, klicken Sie auf den Link für den Namen des Datensammlers in der Tabelle, um die Detailseite für diesen Datensammler aufzurufen.

Verwalten von konfigurierten Datensammlern

Die Seite installierte Datensammler bietet Zugriff auf die Datensammler, die für Data Infrastructure Insights konfiguriert wurden. Auf dieser Seite können Sie vorhandene Datensammler ändern.

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**

   Der Bildschirm Verfügbare Datensammler wird angezeigt.

2. Klicken Sie Auf **Installierte Datensammler**

   Eine Liste aller installierten Datensammler wird angezeigt. Die Liste enthält den Sammlungsnamen, den Status, die IP-Adresse, auf die der Sammler zugreift, und den Zeitpunkt, zu dem Daten vom Gerät erfasst wurden. Zu den Aktionen, die auf diesem Bildschirm ausgeführt werden können, gehören:

   - Kontrolle der Abfrage
   - Ändern der Zugangsdaten für die Datensammlung
   - Datensammler klonen

Kontrollieren der Data Collector-Umfrage

Nachdem Sie eine Änderung an einem Datensammler vorgenommen haben, können Sie es möglicherweise sofort abfragen, um Ihre Änderungen zu überprüfen, oder Sie möchten die Datenerfassung auf einem Datensammler um ein, drei oder fünf Tage verschieben, während Sie an einem Problem arbeiten.

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**
2. Klicken Sie Auf **Installierte Datensammler**
3. Aktivieren Sie das Kontrollkästchen links neben dem zu ändernden Data Collector
4. Klicken Sie auf **Massenaktionen** und wählen Sie die Abfrageraktion aus, die Sie durchführen möchten.

   Massenaktionen können gleichzeitig auf mehreren Datensammlern durchgeführt werden. Wählen Sie die Datensammler aus, und wählen Sie die Aktion aus dem Menü **Massenaktion** aus.

Bearbeiten von Daten-Collector-Informationen

Sie können vorhandene Daten-Collector-Setup-Informationen bearbeiten.

So bearbeiten Sie einen einzelnen Datensammler:

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**, um die Liste der installierten Data Collectors zu öffnen.
2. Klicken Sie im Optionsmenü rechts neben dem Datensammler, den Sie ändern möchten, auf **Bearbeiten**.

   Das Dialogfeld Collector bearbeiten wird geöffnet.

3. Geben Sie die Änderungen ein und klicken Sie auf **Testkonfiguration**, um die neue Konfiguration zu testen, oder klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Sie können auch mehrere Datensammler bearbeiten:

1. Aktivieren Sie das Kontrollkästchen links von jedem Datensammler, den Sie ändern möchten.
2. Klicken Sie auf die Schaltfläche **Massenaktionen** und wählen Sie **Bearbeiten**, um das Dialogfeld „Data Collector bearbeiten“ zu öffnen.
3. Ändern Sie die Felder wie oben beschrieben.

   Die ausgewählten Datensammler müssen derselbe Anbieter und dasselbe Modell sein und sich auf derselben Akquisitionseinheit befinden.

   Beim Bearbeiten mehrerer Datensammler zeigt das Feld Name des Data Collectors „gemischt“ an und kann nicht bearbeitet werden. Andere Felder wie Benutzername und Passwort zeigen „gemischt“ und können bearbeitet werden. Felder, die denselben Wert in den ausgewählten Datenkollektoren haben, zeigen die aktuellen Werte an und können bearbeitet werden.

   Wenn Sie mehrere Datensammler bearbeiten, steht die Schaltfläche **Testkonfiguration** nicht zur Verfügung.

Klonen von Datensammlern

Mit der Clone Facility können Sie schnell eine Datenquelle hinzufügen, die dieselben Anmeldedaten und

Attribute wie eine andere Datenquelle enthält. Klonen ermöglicht Ihnen die einfache Konfiguration mehrerer Instanzen desselben Gerätetyps.

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**.
2. Klicken Sie Auf **Installierte Datensammler**.
3. Klicken Sie auf das Kontrollkästchen links neben dem zu kopierenden Datensammler.
4. Klicken Sie im Optionsmenü rechts neben dem ausgewählten Datensammler auf **Clone**.

   Das Dialogfeld Data Collector klonen wird angezeigt.

5. Geben Sie die neuen Informationen in die erforderlichen Felder ein.
6. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Der Klonvorgang kopiert alle anderen Attribute und Einstellungen, um den neuen Datensammler zu erstellen.

Ausführen von Massenaktionen auf Datensammlern

Sie können gleichzeitig einige Informationen für mehrere Datensammler bearbeiten. Mit dieser Funktion können Sie eine Umfrage starten, Abfragen verschieben und das Abfragen für mehrere Datensammler fortsetzen. Außerdem können Sie mehrere Datensammler löschen.

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Collectors**
2. Klicken Sie Auf **Installierte Datensammler**
3. Klicken Sie auf das Kontrollkästchen links neben den Datensammlern, die Sie ändern möchten.
4. Klicken Sie im Optionsmenü rechts auf die gewünschte Option.

Nachdem Sie fertig sind

Die ausgewählte Operation wird auf den Datensammlern durchgeführt. Wenn Sie Datensammler löschen möchten, wird ein Dialogfeld angezeigt, in dem Sie die Aktion anpassen müssen.

Recherchieren eines fehlgeschlagenen Datensammlers

Wenn ein Datensammler über eine Fehlermeldung und eine hohe oder mittlere Auswirkung verfügt, müssen Sie dieses Problem anhand der Datensammler-Übersichtsseite mit den verknüpften Informationen untersuchen.

Gehen Sie wie folgt vor, um die Ursache für fehlgeschlagene Datensammler zu ermitteln. Fehlermeldungen der Datensammler werden im Menü **Admin** und auf der Seite **installierte Datensammler** angezeigt.

Schritte

1. Klicken Sie Auf **Admin** > **Datensammler** > **Installierte Datensammler**.
2. Klicken Sie auf den verknüpften Namen des defekten Datensammlers, um die Seite Zusammenfassung zu öffnen.
3. Auf der Seite Zusammenfassung können Sie im Bereich Kommentare alle Hinweise lesen, die von einem anderen Techniker hinterlassen wurden, der möglicherweise auch diesen Fehler untersucht hat.

4. Notieren Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniskleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unter der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol Fehlerdetails rechts neben der Meldung.

   Die Fehlerdetails enthalten den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, die verwendeten Informationen und Vorschläge, was versucht werden kann, das Problem zu beheben.

7. Im Bereich Geräte, die von diesem Data Collector gemeldet werden, können Sie die Liste filtern, um nur Geräte von Interesse anzuzeigen. Sie können dann auf den verknüpften **Name** eines Geräts klicken, um die Asset-Seite für dieses Gerät anzuzeigen.
8. Wenn Sie zur Übersichtsseite des Datensammlers zurückkehren, überprüfen Sie im Bereich **Letzte Änderungen anzeigen** unten auf der Seite, um zu sehen, ob die letzten Änderungen das Problem verursacht haben könnten.

Import aus der Dashboard-Galerie

Data Infrastructure Insights bietet eine Reihe empfohlener Dashboards, die Ihnen Einblick in Ihre Daten geben. Jedes Dashboard enthält Widgets, die dazu dienen, eine bestimmte Frage zu beantworten oder ein bestimmtes Problem zu lösen, das für die aktuell erfassten Daten in Ihrer Umgebung relevant ist.

So importieren Sie ein Dashboard aus der Galerie:

1. Wählen Sie **Dashboards > Dashboards**
2. Klicken Sie auf **+aus Galerie**

   Es wird eine Liste von **Empfohlene Dashboards** angezeigt. Jedes Dashboard enthält eine bestimmte Frage, die Sie mithilfe des Dashboards lösen können. Dashboards bieten Unterstützung bei der Beantwortung von Fragen zu verschiedenen Objekttypen, wie AWS, NetApp, Storage, VMware, Und anderen

3. Wählen Sie ein oder mehrere Dashboards aus der Liste aus und klicken Sie auf **Dashboards hinzufügen**. Diese Dashboards werden jetzt in Ihrer Dashboard-Liste angezeigt.

Zusätzlich zu den empfohlenen Dashboards können Sie auch **zusätzliche Dashboards** importieren, die für Ihre aktuellen Daten nicht relevant sind. Wenn Sie beispielsweise derzeit keine Speicherdatensammler installiert haben, aber zukünftig einige konfigurieren möchten, können Sie die speicherrelevanten Dashboards trotzdem importieren. Diese Dashboards sind zwar für die Anzeige verfügbar, zeigen jedoch möglicherweise keine relevanten Daten an, bis mindestens ein Speicherdatensammler konfiguriert ist.

Der Import von der Dashboard-Galerie ist für Benutzer mit Administrator- oder Kontoinhaber-Rolle verfügbar.

Benutzerkonten und Rollen

Data Infrastructure Insights bietet bis zu vier Benutzerkontorollen: Kontoinhaber, Administrator, Benutzer und Gast. Jedem Konto werden bestimmte Berechtigungsebenen zugewiesen, wie in der folgenden Tabelle angegeben. Benutzer werden entweder "Eingeladen"Data Infrastructure Insights zugewiesen und haben eine bestimmte Rolle

zugewiesen, oder sie können sich über "SSO-Autorisierung (Single Sign On)" mit einer Standardrolle anmelden. SSO-Autorisierung ist als Funktion in Data Infrastructure Insights Premium Edition verfügbar.

Berechtigungsstufen

Sie verwenden ein Konto mit Administratorrechten zum Erstellen oder Ändern von Benutzerkonten. Jedem Benutzerkonto wird anhand der folgenden Berechtigungsstufen für jede Funktion „Data Infrastructure Insights“ eine Rolle zugewiesen.

Rolle	Beobachtbarkeit	Workload-Sicherheit	Berichterstellung	Admin
Kontoinhaber	Wie Administrator	Wie Administrator	Wie Administrator	Wie Administrator, sowie Verwaltung der SSO-Authentifizierung und der Identity Federation-Konfiguration. Kann auch weitere Eigentümer zuweisen.
Verwalter	Kann alle Observability-Funktionen und das Management von Datensammlern ausführen	Alle Sicherheitsfunktionen, einschließlich der Funktionen für Alarme, Forensics, Datensammler, automatisierte Antwortrichtlinien und API Tokens für Sicherheit, sind möglich. Ein Administrator kann auch andere Benutzer einladen, kann aber nur Sicherheitsrollen zuweisen.	Alle Benutzer-/Author-Funktionen, einschließlich der Verwaltung von Reporting-API-Tokens, sowie alle administrativen Aufgaben wie die Konfiguration von Berichten und das Herunterfahren und Neustarten von Reporting-Aufgaben ausführen. Ein Administrator kann auch andere Benutzer einladen, kann aber nur Berichtsrollen zuweisen.	Kann andere Benutzer einladen, kann aber nur Observability-Rollen zuweisen. SSO-Konfiguration kann angezeigt, aber nicht geändert werden. Kann API-Zugriffstoken erstellen und verwalten. Kann Audit-Informationen anzeigen. Kann Abonnementinformationen, Nutzung und Verlauf anzeigen. Globale Benachrichtigungen und Empfängerlisten für Abonnementbenachrichtigungen können verwaltet werden.

Rolle	Beobachtbarkeit	Workload-Sicherheit	Berichterstellung	Admin
Benutzer	Kann Dashboards, Abfragen, Warnmeldungen, Anmerkungen, Anmerkungsregeln anzeigen und ändern. Und Applikationen managen, und die Geräterauflösung managen.	Kann Warnungen anzeigen und verwalten und Forensik anzeigen. Benutzer können den Meldungsstatus ändern, Notizen hinzufügen, Snapshots manuell erstellen und den Benutzerzugriff einschränken.	Kann alle Gast-/Consumer-Funktionen ausführen sowie Berichte und Dashboards erstellen und verwalten.	Nicht verfügbar
Gast	Schreibgeschützter Zugriff auf Asset-Seiten, Dashboards, Warnmeldungen und Abfragen können angezeigt und ausgeführt werden.	Kann Warnungen und Forensik anzeigen. Gastrolle kann den Alarmstatus nicht ändern, Notizen hinzufügen, Snapshots manuell erstellen oder den Benutzerzugriff einschränken.	Es können Berichte angezeigt, geplant und erstellt sowie persönliche Einstellungen wie z. B. für Sprachen und Zeitzonen festgelegt werden. Gäste/Verbraucher können keine Berichte erstellen oder administrative Aufgaben ausführen.	Nicht verfügbar

Die beste Vorgehensweise besteht darin, die Anzahl der Benutzer mit Administratorberechtigungen zu begrenzen. Die größte Anzahl von Konten sollte Benutzer- oder Gastkonten sein.

Dateninfrastrukturberechtigungen nach Benutzerrolle

Die folgende Tabelle zeigt die Berechtigungen von Data Infrastructure Insights, die jeder Benutzerrolle gewährt werden.

Merkmal	Administrator/Kontoinhaber	Benutzer	Gast
Erfassungseinheiten: Hinzufügen/Ändern/Löschen	Y	N	N
Alerts*: Erstellen/Ändern/Löschen	Y	Y	N
Alarme*: Anzeigen	Y	Y	Y
Anmerkungsregeln: Erstellen/Ausführen/Ändern/Löschen	Y	Y	N

Anmerkungen: Erstellen/Ändern/Zuweisen/Anzeigen/Entfernen/Löschen	Y	Y	N
API-Zugriff*: Erstellen/Umbenennen/Deaktivieren/Widerruf	Y	N	N
Anwendungen: Erstellen/Anzeigen/Ändern/Löschen	Y	Y	N
Asset-Seiten: Ändern	Y	Y	N
Asset-Seiten: Anzeigen	Y	Y	Y
Audit: Anzeigen	Y	N	N
Cloud-Kosten	Y	N	N
Sicherheit	Y	N	N
Dashboards: Erstellen/Ändern/Löschen	Y	Y	N
Dashboards: Anzeigen	Y	Y	Y
Datensammler: Hinzufügen/Ändern/Poll/Löschen	Y	N	N
Benachrichtigungen: Anzeigen	Y	Y	Y
Benachrichtigungen: Ändern	Y	N	N
Abfragen: Erstellen/Ändern/Löschen	Y	Y	N
Abfragen: Anzeigen/Ausführen	Y	Y	Y
Geräteauflösung	Y	Y	N
Berichte*: Anzeigen/Ausführen	Y	Y	Y
Berichte*: Erstellen/Ändern/Löschen/Zeitplan	Y	Y	N
Abonnement: Anzeigen/Ändern	Y	N	N
Benutzerverwaltung: Laden/Hinzufügen/Ändern/Deaktivieren	Y	N	N

*Erfordert Premium Edition

Erstellen von Konten durch Einladen von Benutzern

Die Erstellung eines neuen Benutzerkontos erfolgt über BlueXP. Ein Benutzer kann auf die per E-Mail gesendete Einladung antworten. Wenn der Benutzer jedoch kein Konto bei BlueXP hat, muss er sich bei BlueXP registrieren, damit er die Einladung annehmen kann.

Bevor Sie beginnen

- Der Benutzername ist die E-Mail-Adresse der Einladung.
- Verstehen Sie die Benutzerrollen, die Sie zuweisen möchten.
- Während der Anmeldung werden Passwörter vom Benutzer definiert.

Schritte

1. Melden Sie sich bei Dateninfrastruktur Insights an
2. Klicken Sie im Menü auf **Admin > Benutzerverwaltung**

   Der Bildschirm Benutzerverwaltung wird angezeigt. Der Bildschirm enthält eine Liste aller Konten im System.

3. Klicken Sie Auf **+ Benutzer**

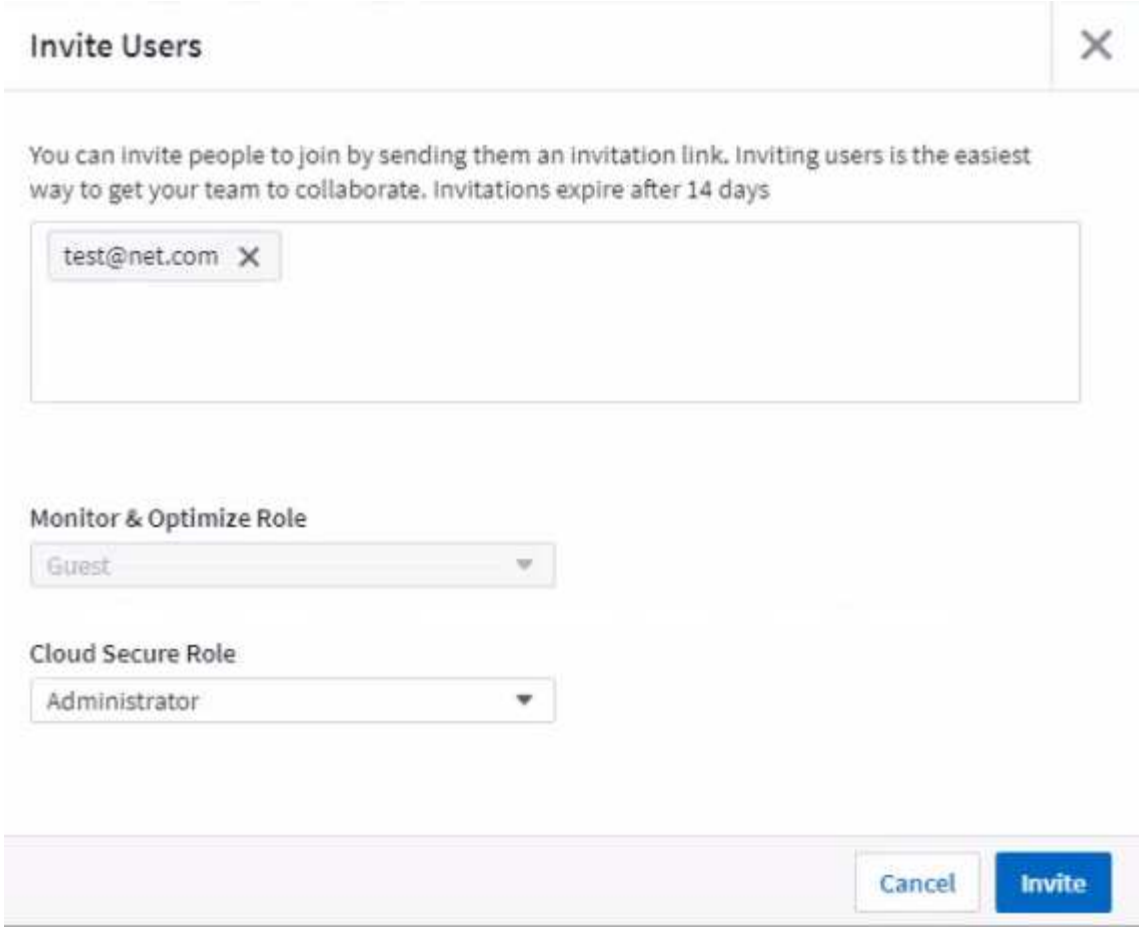
   Der Bildschirm * Benutzer einladen* wird angezeigt.

4. Geben Sie eine E-Mail-Adresse oder mehrere Adressen für Einladungen ein.

   Hinweis: Wenn Sie mehrere Adressen eingeben, werden sie alle mit derselben Rolle erstellt. Sie können nur mehrere Benutzer auf dieselbe Rolle festlegen.

5. Wählen Sie die Benutzerrolle für die einzelnen Funktionen von Data Infrastructure Insights aus.

   Welche Funktionen und Rollen Sie wählen können, hängt davon ab, auf welche Funktionen Sie in Ihrer speziellen Administratorrolle zugreifen können. Wenn Sie beispielsweise nur für Berichte eine Administratorrolle haben, können Sie Benutzer einer beliebigen Rolle in der Berichterstattung zuweisen, können aber keine Rollen für Beobachtbarkeit oder Sicherheit zuweisen.



6. Klicken Sie Auf **Einladung**

   Die Einladung wird an den Benutzer gesendet. Der Benutzer hat 14 Tage Zeit, die Einladung anzunehmen. Sobald ein Benutzer die Einladung akzeptiert hat, wird er an das NetApp Cloud Portal geschickt und dort unter Verwendung der E-Mail-Adresse in der Einladung registriert. Wenn der Kunde bereits über ein Konto für diese E-Mail-Adresse verfügt, kann er sich einfach anmelden und hat dann Zugriff auf seine Data Infrastructure Insights Umgebung.

Ändern der Rolle eines vorhandenen Benutzers

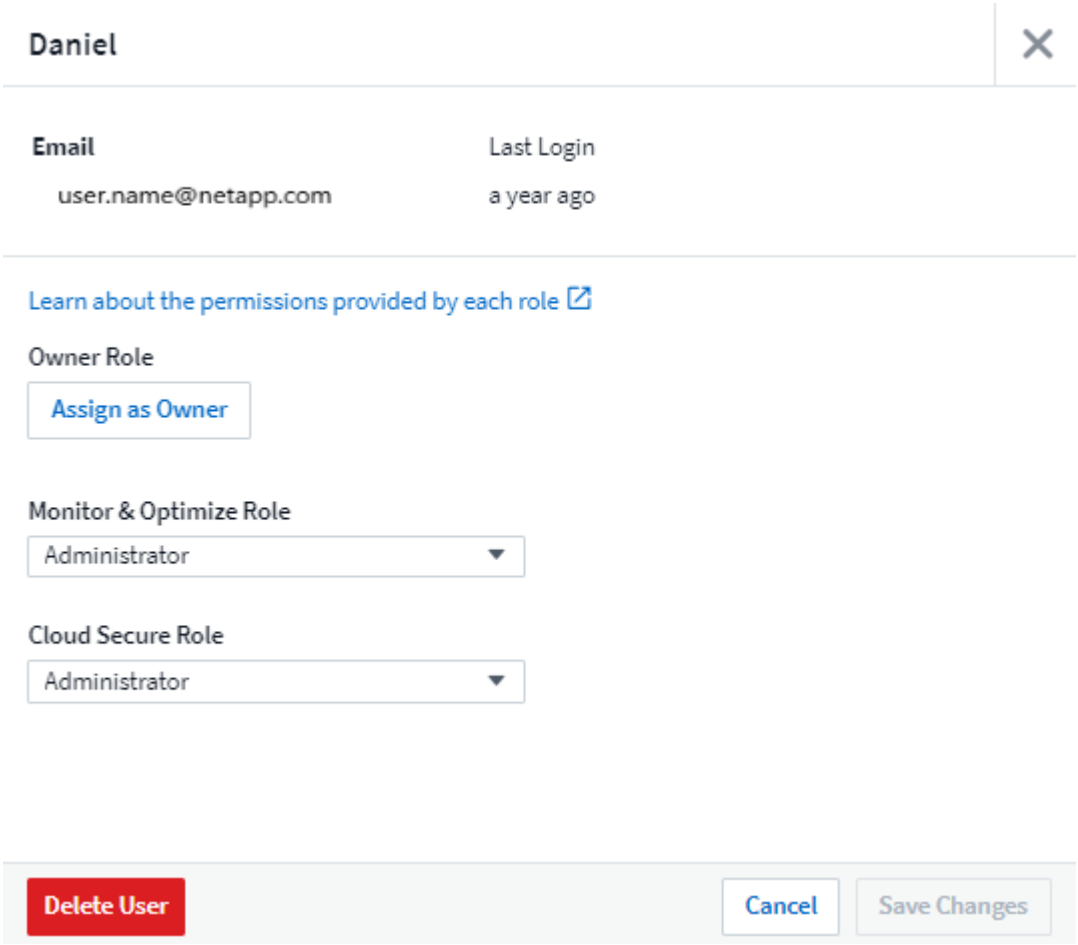
Gehen Sie folgendermaßen vor, um die Rolle eines vorhandenen Benutzers zu ändern, einschließlich der Hinzufügung als **sekundärer Kontoinhaber**.

1. Klicken Sie Auf **Admin > Benutzerverwaltung**. Auf dem Bildschirm wird eine Liste aller Konten im System angezeigt.
2. Klicken Sie auf den Benutzernamen des Kontos, das Sie ändern möchten.
3. Ändern Sie die Benutzerrolle in den einzelnen Funktionen von Data Infrastructure Insights nach Bedarf.
4. Klicken Sie Auf *Änderungen Speichern*.

So weisen Sie einen sekundären Kontoeigentümer zu

Sie müssen zur Beobachtung als Kontoinhaber angemeldet sein, um die Rolle eines Kontoinhabers einem anderen Benutzer zuzuweisen.

1. Klicken Sie Auf **Admin > Benutzerverwaltung**.
2. Klicken Sie auf den Benutzernamen des Kontos, das Sie ändern möchten.
3. Klicken Sie im Dialogfeld Benutzer auf **als Eigentümer zuweisen**.
4. Speichern Sie die Änderungen.



Sie können so viele Kontoinhaber haben, wie Sie möchten, aber Best Practice ist, die Rolle des Eigentümers beschränken, um nur Personen auszuwählen.

Benutzer Werden Gelöscht

Ein Benutzer mit der Administratorrolle kann einen Benutzer löschen (z. B. jemand, der nicht mehr mit dem Unternehmen ist), indem er auf den Namen des Benutzers klickt und im Dialogfeld auf „_Benutzer löschen “ klickt. Der Benutzer wird aus der Data Infrastructure Insights-Umgebung entfernt.

Beachten Sie, dass alle vom Benutzer erstellten Dashboards, Abfragen usw. auch nach dem Entfernen des Benutzers in der Data Infrastructure Insights-Umgebung verfügbar bleiben.

Single Sign On (SSO) und Identity Federation

Was ist Identity Federation?

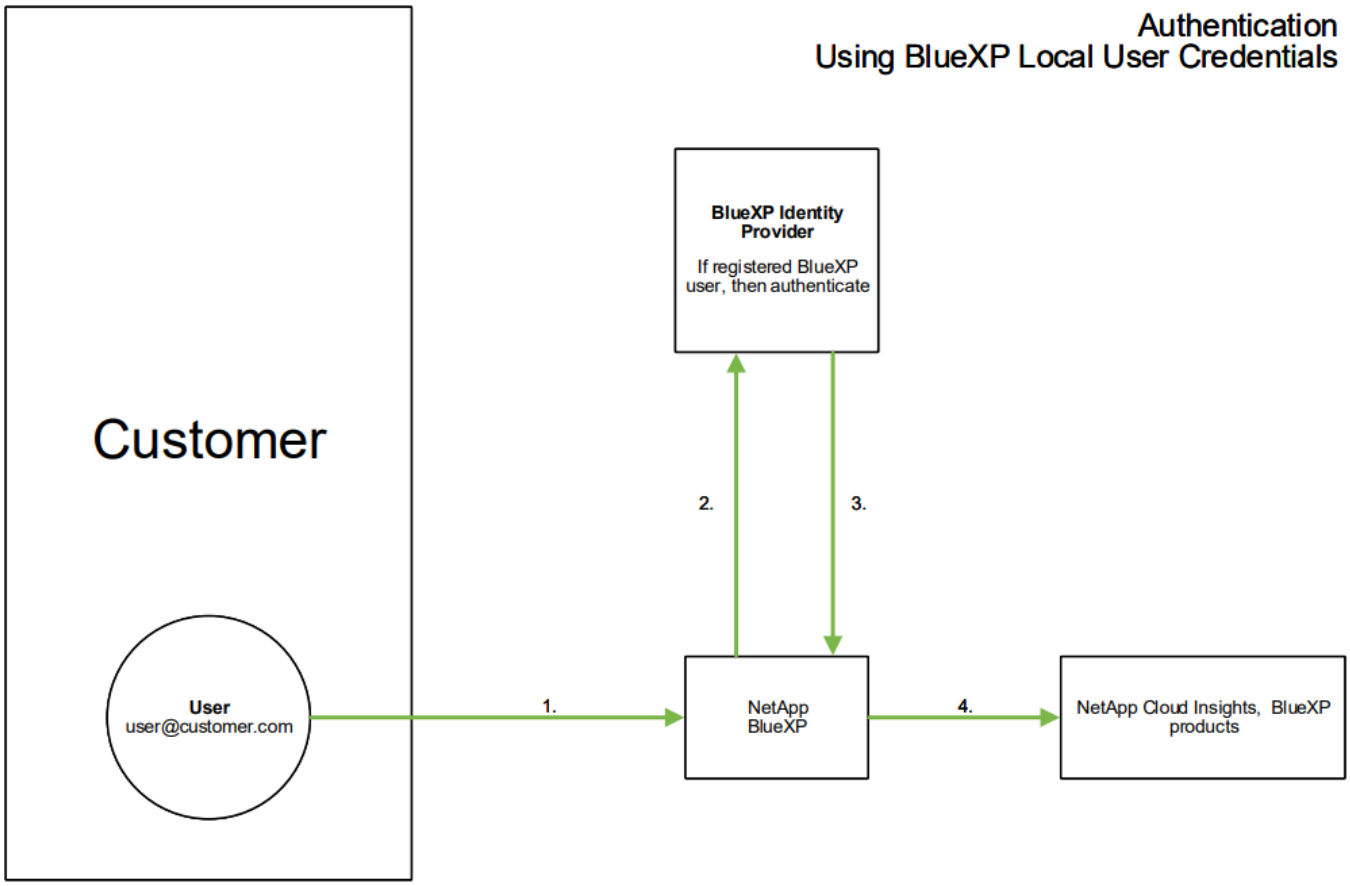
Mit Identity Federation:

- Die Authentifizierung wird an das Identitätsmanagement-System des Kunden unter Verwendung der

Anmeldeinformationen des Kunden aus Ihrem Firmenverzeichnis und der Automatisierungsrichtlinien wie Multi-Faktor Authentication (MFA) delegiert.

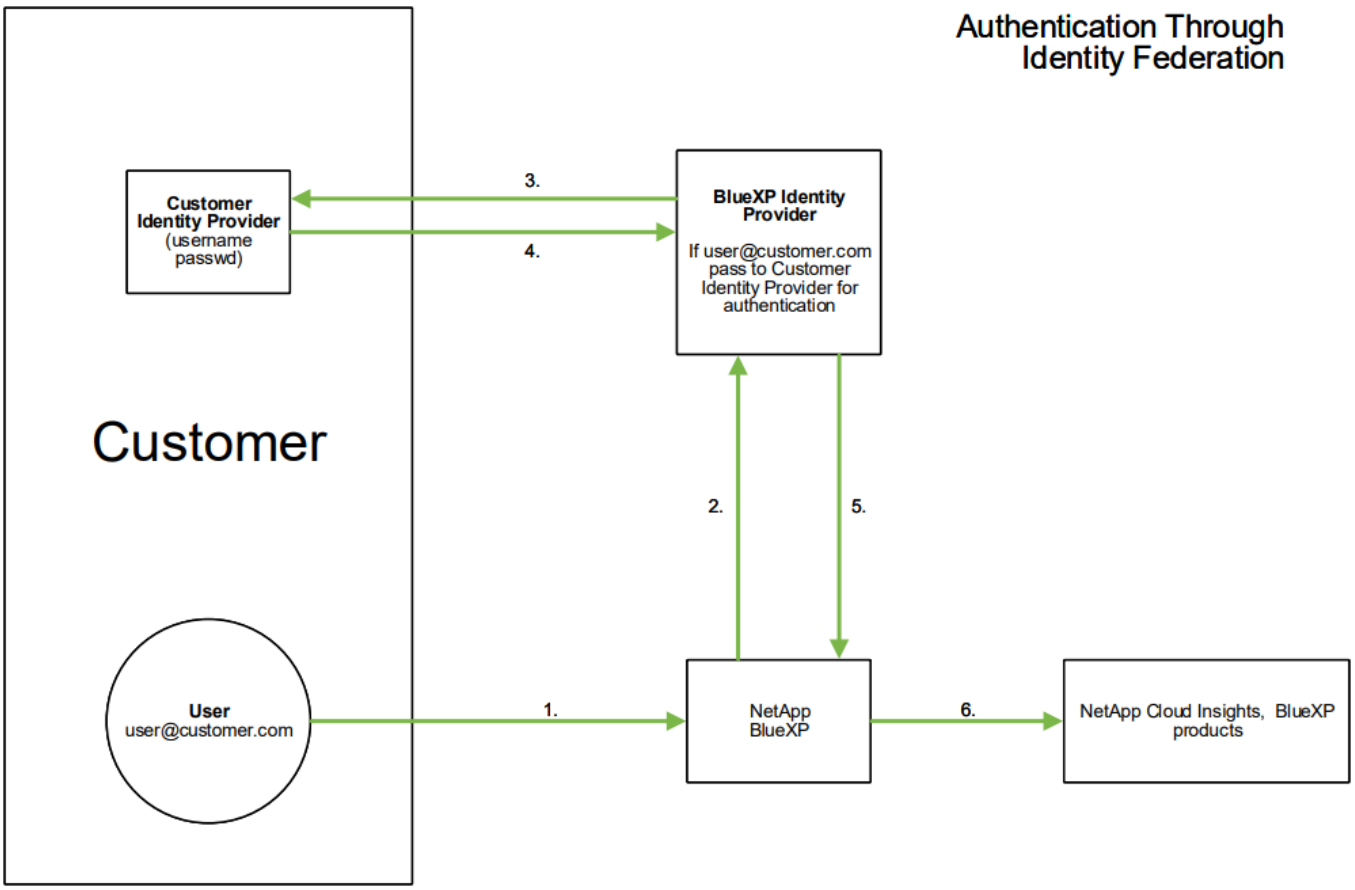
- Benutzer melden sich einmalig bei allen NetApp BlueXP Services an (Single Sign On).

Benutzerkonten werden für alle Cloud-Services in NetApp BlueXP gemanagt. Standardmäßig erfolgt die Authentifizierung über ein lokales BlueXP Benutzerprofil. Im Folgenden finden Sie eine vereinfachte Übersicht über diesen Prozess:



Einige Kunden möchten jedoch ihren eigenen Identitätsanbieter verwenden, um ihre Benutzer für Dateninfrastrukturanalysen und ihre anderen NetApp BlueXP -Services zu authentifizieren. NetApp BlueXP Konten werden mithilfe von Zugangsdaten aus Ihrem Unternehmensverzeichnis authentifiziert.

Im Folgenden finden Sie ein vereinfachtes Beispiel für diesen Prozess:



Wenn ein Benutzer im obigen Diagramm auf Data Infrastructure Insights zugreift, wird dieser Benutzer zur Authentifizierung an das Identitätsmanagementsystem des Kunden weitergeleitet. Nachdem das Konto authentifiziert wurde, wird der Benutzer zur Mandanten-URL von Data Infrastructure Insights weitergeleitet.

Aktivieren Der Identitätsföderation

BlueXP verwendet Auth0 für die Implementierung der Identity Federation und die Integration in Services wie Active Directory Federation Services (ADFS) und Microsoft Azure Active Directory (AD). Informationen zum Konfigurieren der Identity Federation finden Sie im "Anweisungen zur BlueXP Federation".

Sie müssen die BlueXP -Identitätsföderation konfigurieren, bevor Sie SSO mit der Dateninfrastrukturerkennung verwenden können.

Es ist wichtig zu wissen, dass die Änderung der Identitätsföderation in BlueXP nicht nur für Einblicke in die Dateninfrastruktur, sondern auch für alle NetApp BlueXP Services gilt. Der Kunde sollte diese Änderung mit dem NetApp Team für jedes seiner BlueXP Produkte besprechen, um sicherzustellen, dass die von ihm verwendete Konfiguration mit der Identity Federation funktioniert oder wenn Kundenkonten angepasst werden müssen. Der Kunde muss auch sein internes SSO-Team an die Änderung der Identitätsföderation einbinden.

Zudem ist zu beachten, dass nach Aktivierung des Identitätsverbunds für Änderungen am Identitätsanbieter des Unternehmens (beispielsweise beim Wechsel von SAML zu Microsoft AD) wahrscheinlich eine Fehlerbehebung/Änderung/Aufmerksamkeit in BlueXP erforderlich ist, um die Benutzerprofile zu aktualisieren.

Für dieses oder andere Verbundprobleme können Sie ein Support-Ticket unter öffnen https://mysupport.netapp.com/site/help Und wählen Sie die Kategorie **bluexp.netapp.com › Federation Ausgaben**.

Automatische Benutzerbereitstellung mit Single Sign On (SSO

Zusätzlich zur Einladung von Benutzern können Administratoren den **Single Sign-On (SSO) User Auto-Provisioning**-Zugriff auf Data Infrastructure Insights für alle Benutzer in ihrer Unternehmensdomäne aktivieren, ohne sie einzeln einladen zu müssen. Wenn SSO aktiviert ist, können sich alle Benutzer mit derselben Domain-E-Mail-Adresse unter Verwendung ihrer Anmeldedaten bei Data Infrastructure Insights anmelden.

> *SSO User Auto-Provisioning* ist in Data Infrastructure Insights Premium Edition verfügbar und muss konfiguriert werden, bevor es für Data Infrastructure Insights aktiviert werden kann. Die SSO-Konfiguration für die automatische Bereitstellung von Benutzern umfasst "Identitätsföderation"NetApp BlueXP , wie im obigen Abschnitt beschrieben. Verbund ermöglicht Benutzern mit einfacher Anmeldung den Zugriff auf Ihre NetApp BlueXP Konten mithilfe von Anmeldeinformationen aus Ihrem Unternehmensverzeichnis unter Verwendung offener Standards wie Security Assertion Markup Language 2.0 (SAML) und OpenID Connect (OIDC).

Um *SSO User Auto-Provisioning* auf der Seite **Admin > User Management** zu konfigurieren, müssen Sie zunächst BlueXP Identity Federation eingerichtet haben. Wählen Sie den Link **Verbindung einrichten** im Banner aus, um zur BlueXP Federation zu gelangen. Sobald diese Konfiguration abgeschlossen ist, können Administratoren von Data Infrastructure Insights die SSO-Benutzeranmeldung aktivieren. Wenn ein Administrator *SSO User Auto-Provisioning* aktiviert, wählen er eine Standardrolle für alle SSO-Benutzer (z. B. Gast oder Benutzer) aus. Benutzer, die sich über SSO anmelden, verfügen über diese Standardrolle.

Gelegentlich möchte ein Administrator einen einzelnen Benutzer aus der Standard-SSO-Rolle heraufstufen (um ihn zum Beispiel zu einem Administrator zu machen). Sie können dies auf der Seite **Admin > Benutzerverwaltung** durch Klicken auf das rechte Menü für den Benutzer und die Auswahl *Rolle zuweisen* erreichen. Benutzer, denen auf diese Weise eine explizite Rolle zugewiesen wird, haben weiterhin Zugriff auf Data Infrastructure Insights, selbst wenn *SSO User Auto-Provisioning* anschließend deaktiviert wird.

Wenn der Benutzer die erhöhte Rolle nicht mehr benötigt, können Sie auf das Menü klicken, um Benutzer zu entfernen_. Der Benutzer wird aus der Liste entfernt. Wenn *SSO User Auto-Provisioning* aktiviert ist, kann der Benutzer sich mit der Standardrolle weiterhin über SSO bei Data Infrastructure Insights anmelden.

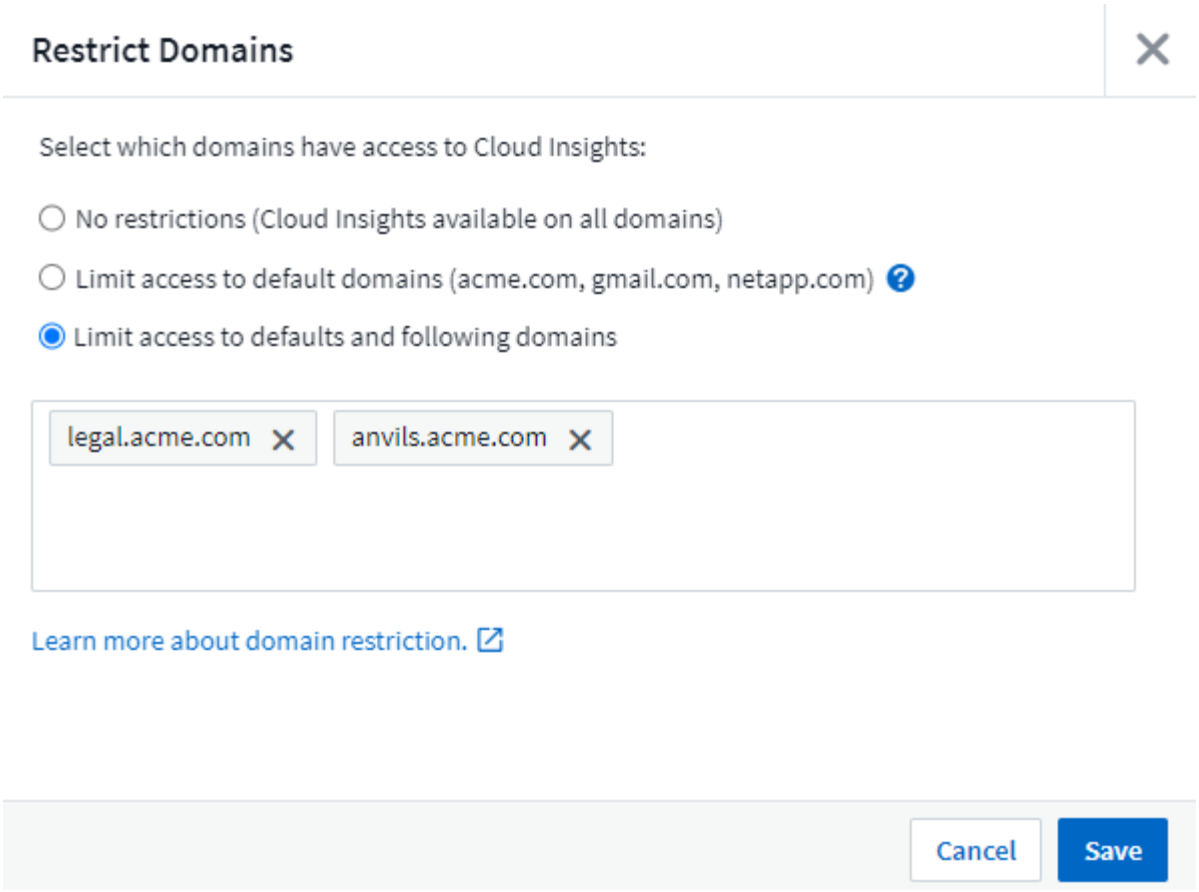
Sie können SSO-Benutzer ausblenden, indem Sie das Kontrollkästchen **SSO-Benutzer anzeigen** deaktivieren.

Aktivieren Sie jedoch die automatische Bereitstellung von *SSO-Benutzern* nicht, wenn eine der folgenden Optionen zutrifft:

- Ihr Unternehmen nutzt mehr als einen Data Infrastructure Insights Mandanten
- Ihr Unternehmen möchte nicht, dass jeder Benutzer in der föderierten Domäne über eine bestimmte Ebene des automatischen Zugriffs auf den Mandanten von Data Infrastructure Insights verfügt. *Zu diesem Zeitpunkt verfügen wir nicht über die Möglichkeit, Gruppen zu nutzen, um den Rollenzugriff mit dieser Option* zu steuern.

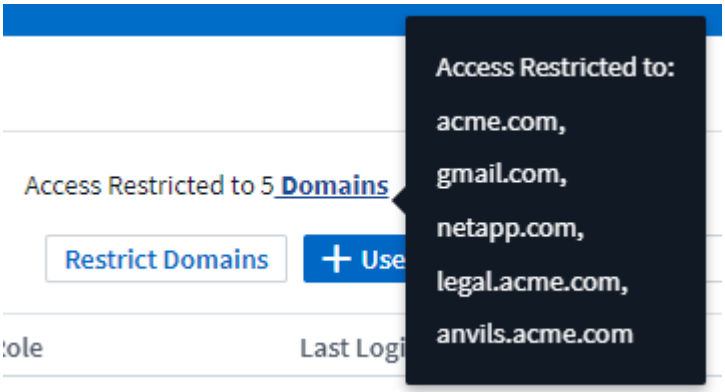
Einschränken des Zugriffs nach Domäne

Data Infrastructure Insights kann den Benutzerzugriff auf die von Ihnen angegebenen Domänen beschränken. Wählen Sie auf der Seite **Admin > User Management** die Option "Domains einschränken" aus.



Ihnen werden folgende Auswahlmöglichkeiten angezeigt:

- Keine Einschränkungen: Data Infrastructure Insights bleibt für Benutzer unabhängig von ihrer Domain verfügbar.
- Beschränken Sie den Zugriff auf Standarddomänen: Standarddomänen sind die Domänen, die von den Kontoeigentümern Ihrer Data Infrastructure Insights-Umgebung verwendet werden. Diese Domains sind immer zugänglich.
- Beschränken Sie den Zugriff auf die von Ihnen angegebenen Standardwerte und Domänen. Führen Sie alle Domänen auf, die zusätzlich zu den Standarddomänen für den Zugriff auf die Data Infrastructure Insights Umgebung benötigt werden.



Data Infrastructure Insights Data Collector List

Data Infrastructure Insights unterstützt eine Vielzahl von Datensammlern von verschiedenen Anbietern und Services.

Datensammler sind nach folgenden Typen kategorisiert:

- Infrastruktur: Von Anbietergeräten wie Storage-Arrays, Switches, Hypervisoren oder Backup-Geräten übernommen
- Service: Erworben durch Services wie Kubernetes oder Docker Auch *Integration* genannt.

Alphabetische Liste der von Data Infrastructure Insights unterstützten Data Collectors:

Data Collector	Typ
"Amazon EC2 und EBS"	Infrastruktur
"AWS S3 als Storage"	Infrastusture
"Amazon FSX für NetApp ONTAP"	Infrastruktur
"Apache"	Service
"Azure NetApp Dateien"	Infrastruktur
"Azure VMs und VHD"	Infrastruktur
"Brocade Network Advisor (BNA)"	Infrastruktur
"Brocade Fibre Channel Switches"	Infrastruktur
"Brocade FOS REST "	Infrastruktur
"Cisco MDS Fabric Switches"	Infrastruktur
"Konsul"	Service
"Couchbase"	Service
"CouchDB"	Service
"Cohesity SmartFiles"	Infrastruktur
"Dell EMC Data Domain"	Infrastruktur
"Dell EMC ECS"	Infrastruktur
"Dell EMC PowerScale (vormals Isilon)"	Infrastruktur
"Dell EMC Isilon/PowerScale REST"	Infrastruktur
"Dell EMC PowerStore"	Infrastruktur
"Dell EMC RecoverPoint"	Infrastruktur
"Dell EMC ScaleIO/PowerFlex "	Infrastruktur
"Dell EMC Unity"	Infrastruktur
"Dell EMC Unisphere REST"	Infrastruktur
"Dell EMC VMAX/PowerMax Produktfamilie"	Infrastruktur

Data Collector	Typ
"Dell EMC VNX Block Storage"	Infrastruktur
"Dell EMC VNX-Datei"	Infrastruktur
"Dell EMC VNX Unified"	Infrastruktur
"Dell EMC VPLEX"	Infrastruktur
"Dell EMC XtremIO"	Infrastruktur
"Dell XC-Serie"	Infrastruktur
"Docker"	Service
"Elasticsearch"	Service
"Knick"	Service
"Fujitsu ETERNUS DX"	Infrastruktur
"Google Compute und Storage"	Infrastruktur
"Hadoop"	Service
"HAProxy"	Service
"Hitachi Content Platform (HCP)"	Infrastruktur
"Hitachi Vantara Command Suite"	Infrastruktur
"Hitachi Vantara NAS-Plattform"	Infrastruktur
"Hitachi Ops Center (Hds)"	Infrastruktur
"HP Enterprise Alletra 6000 Storage (ehemals Nimble"	Infrastruktur
"HP Enterprise Alletra 9000 / Primera (vormals 3PAR) Storage"	Infrastruktur
"HP Enterprise Command View"	Infrastruktur
"Huawei OceanStor und Dorado Geräte"	Infrastruktur
"IBM Cleversafe"	Infrastruktur
"IBM CS Serie"	Infrastruktur
"IBM PowerVM"	Infrastruktur
"IBM SAN Volume Controller (SVC)"	Infrastruktur
"IBM System Storage DS8000 Serie"	Infrastruktur
"IBM XIV und A9000 Storage"	Infrastruktur
"Infiniat InfiniBox"	Infrastruktur
"Java"	Service
"Kafka"	Service
"Kapacitor"	Service
"Kibana"	Service

Data Collector	Typ
"Kubernetes"	Service
"Lenovo HX-Serie"	Infrastruktur
"Gememcachte"	Service
"Microsoft Azure NetApp Files"	Infrastruktur
"Microsoft Hyper-V"	Infrastruktur
"MongoDB"	Service
"MySQL"	Service
"NetApp Cloud Volumes ONTAP"	Infrastruktur
"NetApp Cloud Volumes Services für AWS"	Infrastruktur
"NetApp Cloud Connection für ONTAP 9.9 oder höher"	Infrastruktur
"NetApp Data ONTAP 7-Mode"	Infrastruktur
"NetApp E-Series"	Infrastruktur
"NetApp E-Series REST "	Infrastruktur
"Amazon FSX für NetApp ONTAP"	Infrastruktur
"NetApp HCI Virtual Center"	Infrastruktur
"NetApp ONTAP Datenmanagement-Software"	Infrastruktur
"NetApp ONTAP-REST-Kollektor "	Infrastruktur
"NetApp ONTAP Select"	Infrastruktur
"NetApp SolidFire All-Flash-Array"	Infrastruktur
"NetApp StorageGRID"	Infrastruktur
"Netstat"	Service
"Nginx"	Service
"Knoten"	Service
"Nutanix NX-Serie"	Infrastruktur
"OpenStack"	Infrastruktur
"OpenZFS"	Service
"Oracle ZFS Storage Appliance"	Infrastruktur
"PostgreSQL"	Service
"Puppet Agent"	Service
"Pure Storage FlashArray"	Infrastruktur
"Red Hat Virtualization"	Infrastruktur
"Redis"	Service

Data Collector	Typ
"RethinkDB"	Service
"RHEL CentOS"	Service
"Rubrik CDM Storage"	Infrastruktur
"Ubuntu Debian"	Service
"VMware vSphere"	Infrastruktur
"Windows"	Service
"ZooKeeper"	Service

Abonnieren von Data Infrastructure Insights

Der Einstieg in Data Infrastructure Insights ist mit drei einfachen Schritten ganz einfach:

- Melden Sie sich für ein Konto bei an **"NetApp BlueXP"** Zugang zu allen Cloud-Angeboten von NetApp.
- Melden Sie sich für eine **"Kostenlose Testversion"**Data Infrastructure Insights an, um mehr über die verfügbaren Funktionen zu erfahren.
- **Abonnieren** Data Infrastructure Insights für den kontinuierlichen, unterbrechungsfreien Zugriff auf Ihre Daten über "NetApp Vertrieb" direkt oder "AWS Marketplace".

Während des Registrierungsprozesses können Sie die globale Region auswählen, um Ihre Data Infrastructure Insights Umgebung zu hosten. Weitere Informationen finden Sie unter Dateninfrastruktureinblicke "Informationen und Region".

Einen vollständigen Vergleich der in Data Infrastructure Insights Basic und Premium Edition verfügbaren Funktionen finden Sie auf der "Preise Für Einblicke In Die Dateninfrastruktur" Seite.

Inaktive Data Infrastructure Insights Basic Edition-Umgebungen werden gelöscht und ihre Ressourcen zurückgewonnen. Eine Umgebung gilt als inaktiv, wenn 30 aufeinander folgende Tage keine Benutzeraktivität zur Verfügung steht, wenn 7 aufeinanderfolgende Tage keine Daten aufgenommen wurden. Data Infrastructure Insights sendet eine Benachrichtigung und gewährt eine Kulanzzeit von vier Tagen, bevor eine Umgebung gelöscht wird.

Wenn Sie bei der Verwendung von Data Infrastructure Insights ein Vorhängeschloss  -Symbol sehen, bedeutet dies, dass die Funktion in Ihrem aktuellen Abonnement nicht verfügbar ist oder in begrenzter Form verfügbar ist. Abonnieren Sie diese Funktion, um vollen Zugriff zu erhalten. Einige Funktionen sind vor dem Abonnieren als verfügbar Modulbewertung .

Testversion

Wenn Sie sich bei Data Infrastructure Insights anmelden und Ihre Umgebung aktiv ist, können Sie Data Infrastructure Insights kostenlos und 30 Tage testen. Entdecken Sie bei diesem Testlauf die Funktionen, die Data Infrastructure Insights in Ihrer eigenen Umgebung zu bieten hat.

Sie können Data Infrastructure Insights während Ihres Testzeitraums jederzeit abonnieren. Das Abonnement von Data Infrastructure Insights gewährleistet einen unterbrechungsfreien Zugriff auf Ihre Daten sowie erweiterte **"Produktsupport"** Optionen.

Data Infrastructure Insights zeigt ein Banner an, wenn sich Ihre kostenlose Testversion dem Ende nähert Innerhalb dieses Banners befindet sich ein *View Subscription* Link, der die Seite **Admin → Abonnement** öffnet. Nicht-Admin-Benutzer sehen das Banner, können aber nicht zur Abonnementseite gehen.

Wenn Sie zusätzliche Zeit benötigen, um Data Infrastructure Insights zu testen, und Ihre Testversion in 4 Tagen oder weniger abläuft, können Sie Ihre Testversion um weitere 30 Tage verlängern. Sie können die Testversion nur einmal verlängern. Sie können nicht verlängern, wenn Ihre Testversion abgelaufen ist.

Testversion über AWS Marketplace

Sie können sich zudem über den AWS Marketplace für eine kostenlose Testversion anmelden. Mit der

kostenlosen Testversion von AWS Marketplace haben Sie 33 Tage lang Zugriff auf Data Infrastructure Insights und können bis zu 499 Verwaltete Einheiten (Mus) testen.

Hinweis: Wenn Sie mehr als 499 MUs konfigurieren, geben Sie den Status „missachtet“ ein. Während der Testphase verlieren Sie den Zugriff auf einige Data Infrastructure Insights-Funktionen, bis die Sicherheitsverletzung behoben ist, indem Sie entweder die Anzahl der konfigurierten Mus reduzieren oder Data Infrastructure Insights abonnieren.

Die kostenlose Testversion von AWS Marketplace kann nicht erweitert werden. Sie können jederzeit während der Testversion auf ein Data Infrastructure Insights Basic Edition-Abonnement herunterstufen oder auf ein kostenpflichtiges Data Infrastructure Insights-Abonnement wechseln, indem Sie die Seite **Admin → Abonnement** aufrufen.

Was ist, wenn meine Testversion abgelaufen ist?

Wenn Ihre kostenlose Testversion abgelaufen ist und Sie Data Infrastructure Insights noch nicht abonniert haben, haben Sie eingeschränkte Funktionen, bis Sie sich anmelden. Die Datenaufnahme kann eingestellt werden, und nach einigen Wochen werden Ihre Daten gemäß unserer Datenaufbewahrungsrichtlinie gelöscht.

Was passiert, wenn mein Abonnement abgelaufen ist?

Wenn Sie ein Abonnement von Data Infrastructure Insights haben, dieses Abonnement jedoch abgelaufen ist, haben Sie eine Frist von fünf Tagen, um Ihr Abonnement zu verlängern. Während dieser Gnadenfrist bleiben alle Funktionen Data Infrastructure Insights aktiv.

Nach Ablauf der Gnadenfrist wird die Funktion Data Infrastructure Insights bis zur Erneuerung unterbrochen. Informationen zur Verlängerung finden Sie auf der Seite **Admin > Abonnement**, oder wenden Sie sich an den NetApp-Vertrieb.

Ihre Dateninfrastruktur Insights Daten, die Sie nach Ende der Gnadenfrist sammeln, bleiben nach der Gnadenfrist 30 Tage lang intakt. Wenn Sie Ihr Abonnement innerhalb dieser Zeit verlängern, stehen Ihnen alle Ihre Daten bis zu der verstrichenen Kulanzzeit zur Verfügung.

Was ist, wenn mein Abonnement abgelaufen ist?

Wenn Sie ein Abonnement von Data Infrastructure Insights haben, dieses Abonnement jedoch abgelaufen ist, haben Sie eine Frist von fünf Tagen, um Ihr Abonnement zu verlängern. Während dieser Gnadenfrist bleiben alle Funktionen Data Infrastructure Insights aktiv.

Nach Ablauf der Gnadenfrist wird die Funktion Data Infrastructure Insights bis zur Erneuerung unterbrochen. Informationen zur Verlängerung finden Sie auf der Seite **Admin > Abonnement**, oder wenden Sie sich an den NetApp-Vertrieb.

Ihre Daten aus Data Infrastructure Insights bleiben nach der Gnadenfrist 30 Tage lang erhalten. Wenn Sie Ihr Abonnement innerhalb dieser Zeit verlängern, stehen Ihnen alle Ihre Daten bis zu der verstrichenen Kulanzzeit zur Verfügung.

Modulbewertung

Sie können auch von **Module Evaluations** profitieren. Wenn Sie beispielsweise bereits Infrastruktur-Observability abonniert haben, aber Kubernetes zu Ihrer Umgebung hinzufügen, erhalten Sie automatisch eine 30-Tage-Evaluierung von Kubernetes Observability, beginnend mit der Installation des NetApp Kubernetes

Monitoring Operator. Ihnen wird am Ende des Evaluierungszeitraums nur die Nutzung Ihrer Kubernetes Observability-gemanagten Einheit in Rechnung gestellt.

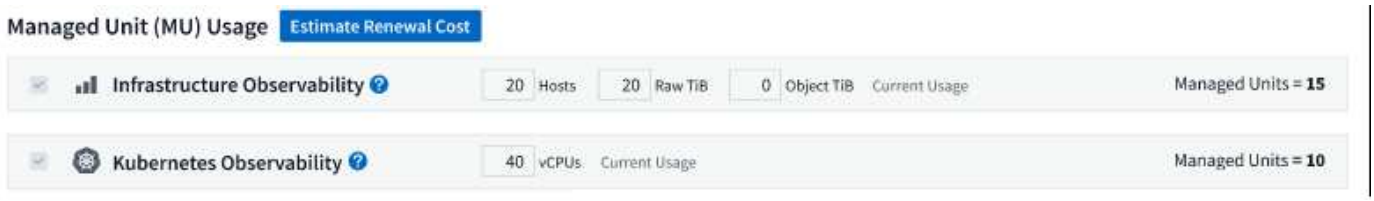
Denken Sie daran, dass Ihnen nach der Bewertung die Kosten für die Verwendung neuer verwalteter Einheiten (Managed Unit, MU) in Rechnung gestellt werden. Planen Sie daher entsprechend. Wenn Ihre Modulbewertung beendet ist, werden Sie benachrichtigt, wenn Sie weitere Mus hinzufügen müssen, um Serviceunterbrechungen zu vermeiden.

Sie können die Nutzung Ihrer verwalteten Einheit auf der Seite **Admin > Abonnement** auf der Registerkarte **Nutzung** überwachen.

Eine *Modulbewertung* ist keine *Testversion* - wir verwenden den Begriff Testversion, wenn wir Kunden eine kostenlose Testphase zur Nutzung des Data Infrastructure Insights Service zur Bestätigung der Eignung und Aktivierung des Kaufs anbieten. Eine Modulbewertung ist anders. Dies ist der Fall, wenn wir einem zahlenden Kunden ermöglichen, ein Modul von Data Infrastructure Insights auszuprobieren, das er in den letzten Monaten seines kostenpflichtigen Abonnements nicht verwendet hat. Wenn die Evaluierung aktiv ist, werden die Kosten für das neu konfigurierte Modul aufgehoben. Die Arbeitsumgebung des Kunden ist noch nicht abonniert und hat sich nicht auf kostenlose Testversion zurückgesetzt. Das Abonnement hat sich nicht geändert.

Kalkulator

Während einer Modulbewertung wird die ME-Auslastung für Ressourcen, die für das Modul verbraucht werden, nicht geändert. aber Sie können den **Estimator** (auf der *Summary* Registerkarte) öffnen, um zu sehen, wie MUs nach der Auswertung berechnet werden, sowie mit "Was wäre wenn"-Szenarien mit der Anzahl der Mus spielen, die Sie in Zukunft benötigen. Setzen Sie die Zahlen zurück, indem Sie den Kalkulator beenden.



Aktivieren Sie das Kontrollkästchen neben einem Modul, um die gesamten ME des Moduls zu den geschätzten Kosten hinzuzufügen oder zu entfernen.

Mit dem Kalkulator können Sie außerdem sehen, wie die Zahlen für ein Add-On, bei dem Sie Ihre aktuelle Abonnementdauer beibehalten und die Anzahl der lizenzierten verwalteten Einheiten erhöhen, oder für ein Verlängerungsabonnement, das Sie beim Kauf Ihres aktuellen Abonnements erwerben würden, gestapelt werden Laufzeit endet.

Beachten Sie, dass Kunden nur einmal pro Abonnement für eine Modulbewertung berechtigt sind.

Abonnementoptionen

Um sich zu registrieren, gehen Sie zu **Admin** → **Abonnement**. Zusätzlich zu den **Abonnieren** Buttons können Sie Ihre installierten Datensammler sehen und Ihre geschätzte Zählung berechnen. In einer typischen Umgebung können Sie auf die Schaltfläche Self-Service AWS Marketplace klicken. Wenn in Ihrer Umgebung 1,000 oder mehr Managed Units enthalten sind oder davon erwartet werden, haben Sie ein Anrecht auf Volume Pricing.

Observability-Messung

Einblicke in die Dateninfrastruktur die Beobachtbarkeit der Infrastruktur von Data Infrastructure und die Beobachtbarkeit von Kubernetes werden pro **gemanagter Einheit** gemessen. Die Nutzung Ihrer verwalteten Einheiten wird anhand der Anzahl der **Hosts oder virtuellen Maschinen** und der Menge der **unformatierten Kapazität** berechnet, die in Ihrer Infrastrukturumgebung verwaltet wird.

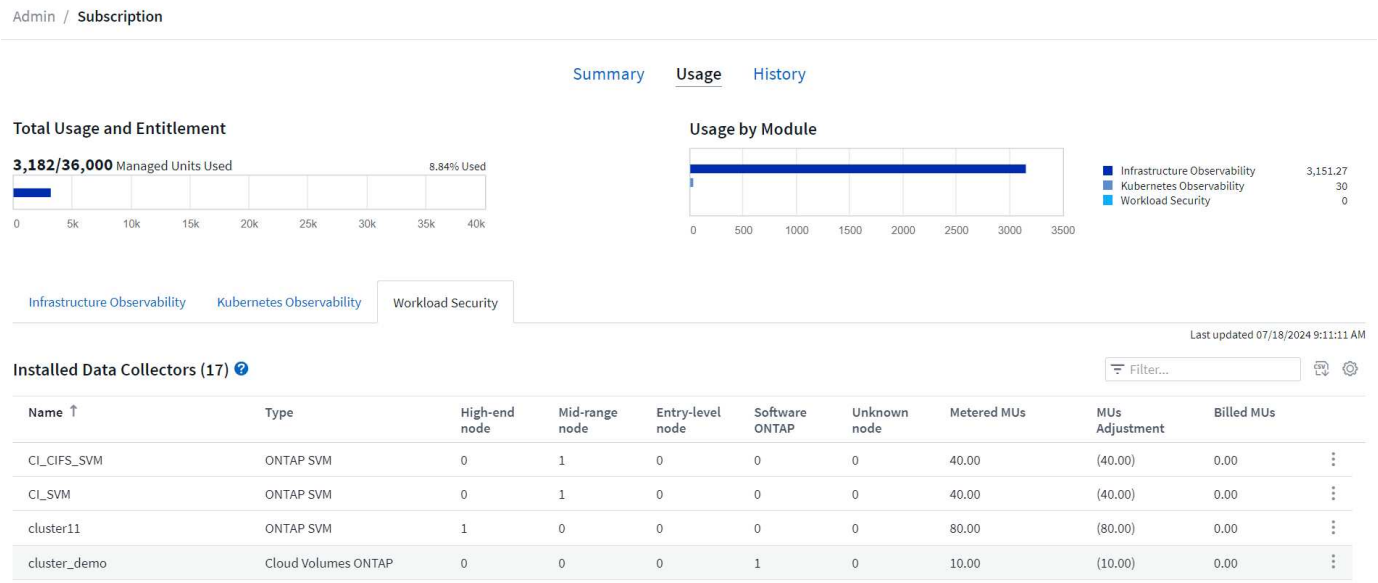
- 1 Managed Unit = 2 Hosts (jede virtuelle oder physische Maschine)
- 1 Managed Unit = 4 tib unformatierte Kapazität physischer oder virtueller Festplatten
- 1 Managed Unit = 40 tib unformatierte Kapazität ausgewählter sekundärer Speicher: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik:
- 1 Managed Unit = 4 vCPUs von Uberentes.
    - 1 Managed Unit K8s Adjustment = 2 Nodes oder Hosts, die auch von der Infrastruktur überwacht werden.

Wenn in Ihrer Umgebung 1,000 oder mehr Managed Units enthalten sind oder erwartet werden, haben Sie Anspruch auf **Volumenrabatte** und werden dazu aufgefordert, sich an den NetApp Vertrieb zu wenden. Siehe Unten Entnehmen.

Messung Der Workload-Sicherheit

Die Workload-Sicherheit wird nach Cluster gemessen und verwendet denselben Ansatz wie die Observability-Messung.

Sie können Ihre Workload Security-Nutzung auf der Seite **Admin > Abonnement** auf der Registerkarte **Workload Security** anzeigen.



Bei bestehenden Workload Security-Abonnements wird die MU-Nutzung angepasst, sodass die Node-Nutzung keine verwalteten Einheiten verbraucht. Data Infrastructure Insights misst die Nutzung von Messgeräten, um die Compliance mit der lizenzierten Nutzung sicherzustellen.

Wie kann ich mich anmelden?

Wenn die Anzahl Ihrer Managed Units kleiner als 1,000 ist, können Sie sich auch über den NetApp Vertrieb anmelden oder Self-Subscribe Über AWS Marketplace:

Abonnieren Sie NetApp Sales Direct

Wenn die erwartete Anzahl der verwalteten Einheiten 1,000 oder höher beträgt, klicken Sie auf das **"Vertrieb Kontaktieren"** Taste um das NetApp Sales Team zu abonnieren.

Sie müssen Ihrem NetApp Vertriebsmitarbeiter Ihre Data Infrastructure Insights **Seriennummer** zur Verfügung stellen, damit Ihr bezahltes Abonnement auf Ihre Data Infrastructure Insights-Umgebung angewendet werden kann. Die Seriennummer identifiziert eindeutig Ihre Data Infrastructure Insights-Testumgebung und ist auf der Seite **Admin > Abonnement** zu finden.

Self-Subscribe über AWS Marketplace

Sie müssen Kontoinhaber oder Administrator sein, um ein AWS Marketplace Abonnement auf Ihr vorhandenes Data Infrastructure Insights Testkonto anwenden zu können. Zusätzlich ist ein Amazon Web Services (AWS) Konto erforderlich.

Durch Klicken auf den Link Amazon Marketplace wird die AWS- "Einblicke In Die Dateninfrastruktur"Abonnementseite geöffnet, auf der Sie Ihr Abonnement abschließen können. Beachten Sie, dass die Werte, die Sie im Rechner eingegeben haben, nicht auf der AWS-Abonnementseite ausgefüllt sind. Sie müssen auf dieser Seite die Gesamtzahl der verwalteten Einheiten eingeben.

Nachdem Sie die Gesamtzahl der verwalteten Einheiten eingegeben und entweder 12 Monate oder 36 Monate Abonnement-Laufzeit gewählt haben, klicken Sie auf **Konto einrichten**, um den Abonnementprozess abzuschließen.

Sobald das AWS Abonnement abgeschlossen ist, werden Sie zurück in die Data Infrastructure Insights Umgebung versetzt. Wenn die Umgebung nicht mehr aktiv ist (Sie haben sich z. B. abgemeldet), werden Sie zur Anmeldeseite von NetApp BlueXP weitergeleitet. Wenn Sie sich erneut bei Data Infrastructure Insights anmelden, ist Ihr Abonnement aktiv.

Nachdem Sie auf der AWS Marketplace Seite auf **Konto einrichten** geklickt haben, müssen Sie den AWS Abonnementprozess innerhalb einer Stunde abschließen. Wenn Sie den Vorgang nicht innerhalb einer Stunde abschließen, müssen Sie erneut auf **Konto einrichten** klicken, um den Vorgang abzuschließen.

Wenn ein Problem auftritt und der Abonnementprozess nicht korrekt abgeschlossen werden kann, sehen Sie beim Anmelden in Ihrer Umgebung weiterhin das Banner „Testversion“. In diesem Fall können Sie zu **Admin > Abonnement** gehen und den Abonnementprozess wiederholen.

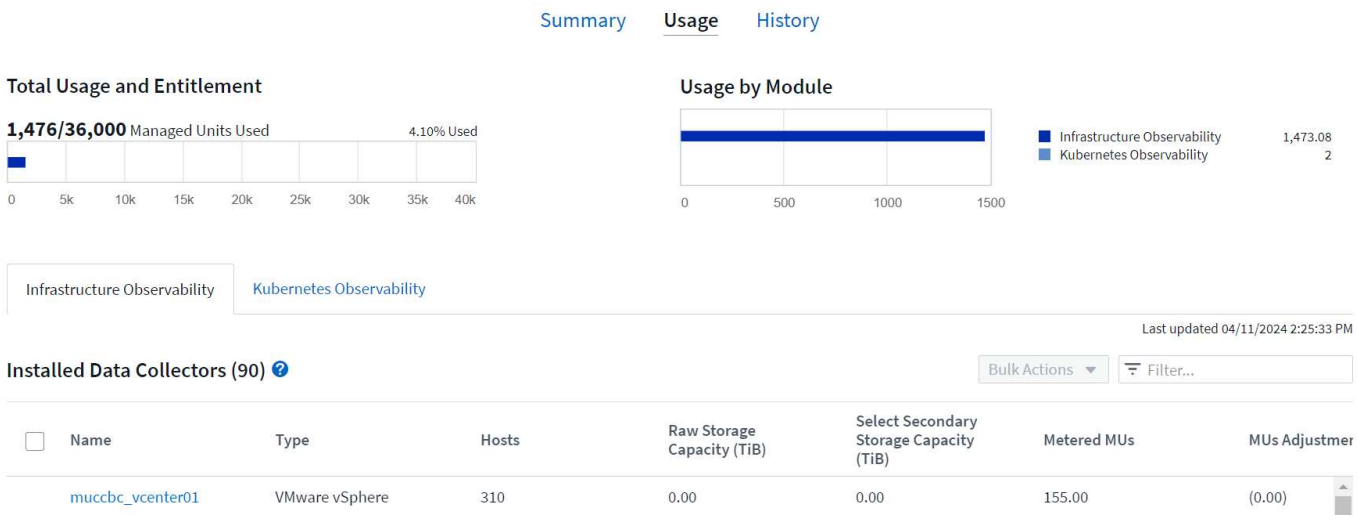
Ihren Abonnementstatus Anzeigen

Sobald Ihr Abonnement aktiv ist, können Sie Ihren Abonnementstatus und die Nutzung der verwalteten Einheit über die Seite **Admin > Abonnement** anzeigen.

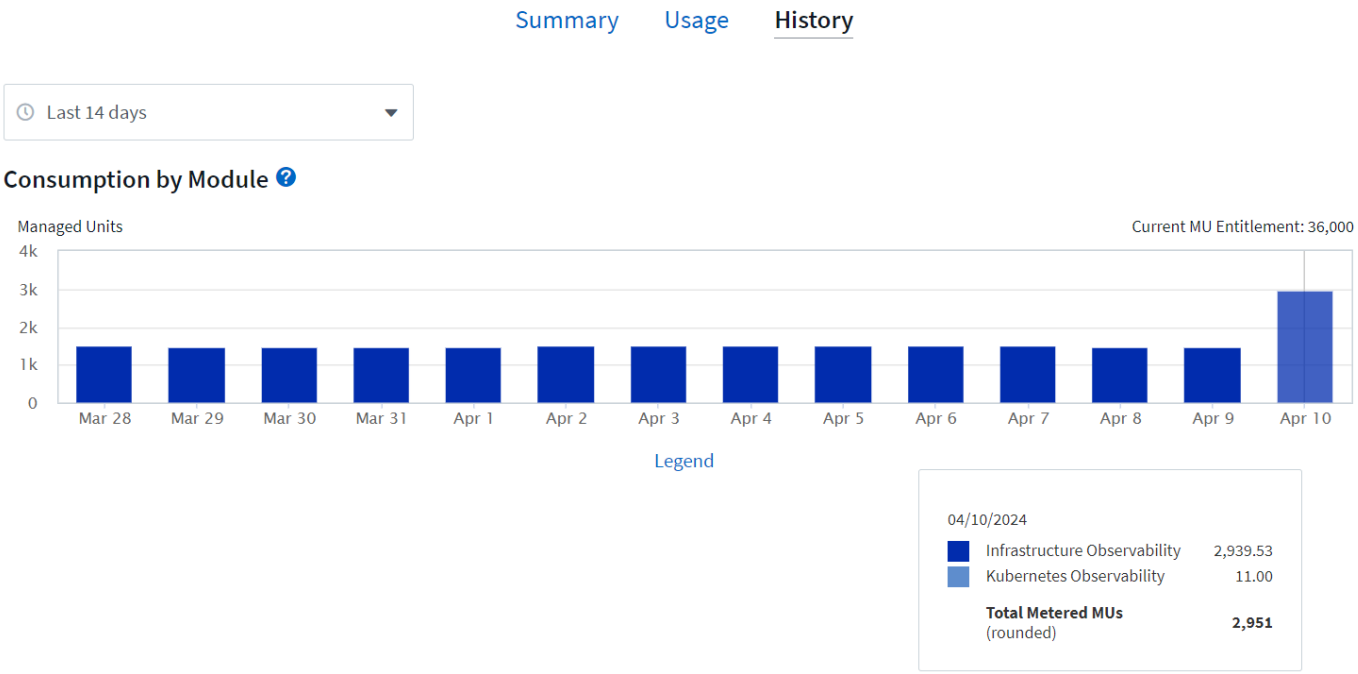
Auf der Registerkarte Subscription **Summary** werden folgende Elemente angezeigt:

- Aktuelle Ausgabe
- Seriennummer Des Abonnements
- Aktuelle ME-Berechtigung

Die Registerkarte **Usage** zeigt Ihnen Ihre aktuelle MU-Nutzung und wie diese Nutzung nach Datensammler unterteilt wird.



Die Registerkarte **Verlauf** gibt Ihnen einen Einblick in Ihre MU-Nutzung in den letzten 7 bis 90 Tagen. Wenn Sie den Mauszeiger über eine Spalte im Diagramm halten, werden Sie nach Modul aufgeschlüsselt (z. B. Observability, Kubernetes).



Ihr Nutzungsmanagement anzeigen

Auf der Registerkarte Usage Management wird eine Übersicht über die Auslastung der verwalteten Einheiten sowie Registerkarten angezeigt, die den Verbrauch der verwalteten Einheiten nach Collector oder Kubernetes Cluster aufschlüsselung.

Die Anzahl der nicht formatierten Einheiten für die verwaltete Kapazität entspricht einer Summe der gesamten Rohkapazität in der Umgebung und wird auf die nächste verwaltete Einheit aufgerundet.

Die Summe der verwalteten Einheiten kann sich leicht von der Datensammler-Anzahl im Zusammenfassungsbereich unterscheiden. Dies liegt daran, dass die Anzahl der verwalteten Einheiten auf die nächste verwaltete Einheit aufgerundet wird. Die Summe dieser Zahlen in der Datensammler-Liste kann etwas höher sein als die Summe der verwalteten Einheiten im Statusbereich. Im Übersichtsbereich finden Sie die tatsächliche Anzahl der verwalteten Einheiten für Ihr Abonnement.

Falls sich Ihre Nutzung dem abonnierten Betrag nähert oder diesen überschreitet, können Sie die Nutzung verringern, indem Sie Datensammler löschen oder die Überwachung von Kubernetes-Clustern stoppen. Löschen Sie einen Eintrag in dieser Liste, indem Sie auf das Menü „drei Punkte“ klicken und *Löschen* wählen.

Was passiert, wenn ich meine abonnierte Nutzung überüberschreitung?

Warnungen werden angezeigt, wenn die Nutzung der verwalteten Einheiten 80 %, 90 % und 100 % Ihres abonnierten Gesamtbetrags überschreitet:

Bei mehr als:	Dies passiert / Empfohlene Aktion:
80%	Ein Informationsbanner wird angezeigt. Es ist keine Aktion erforderlich.

Bei mehr als:	Dies passiert / Empfohlene Aktion:
90%	Ein Warnbanner wird angezeigt. Sie können die Anzahl Ihrer abonnierten verwalteten Einheiten erhöhen.
100%	Ein Fehlerbanner wird angezeigt, bis Sie einen der folgenden Schritte ausführen: • Entfernen Sie Data Collectors, damit Ihre Managed Unit-Nutzung Ihren abonnierten Betrag erreicht oder darunter liegt • Ändern Sie Ihr Abonnement, um die Anzahl der abonnierten verwalteten Einheiten zu erhöhen

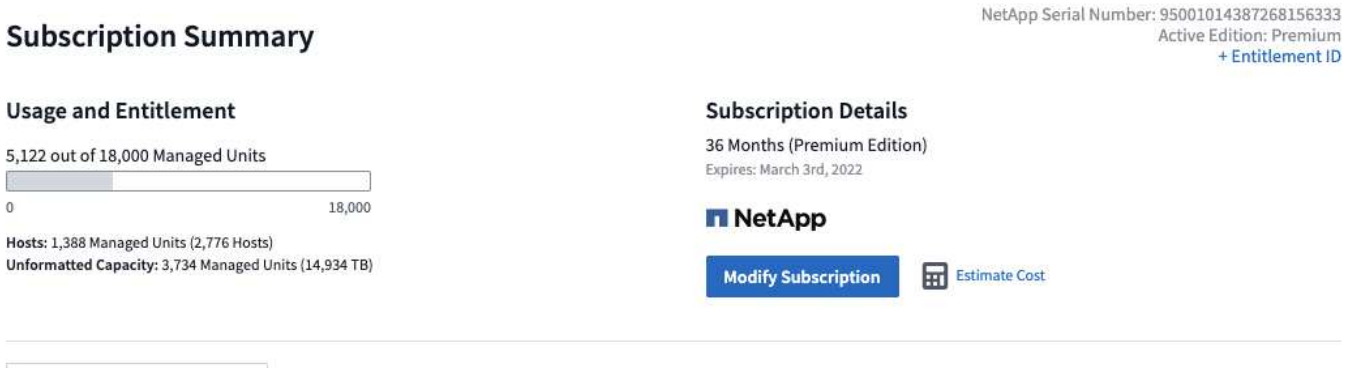
Melden Sie sich direkt an und überspringen Sie die Testversion

Sie können Data Infrastructure Insights auch direkt aus dem abonnieren "AWS Marketplace", ohne zuvor eine Testumgebung zu erstellen. Sobald Ihr Abonnement abgeschlossen und Ihre Umgebung eingerichtet ist, werden Sie umgehend abonniert.

Hinzufügen einer Berechtigungs-ID

Wenn Sie ein gültiges NetApp Produkt besitzen, das im Paket mit Data Infrastructure Insights erhältlich ist, können Sie dieses Produktseriennummer zu Ihrem bestehenden Abonnement von Data Infrastructure Insights hinzufügen. Wenn Sie beispielsweise NetApp Astra Control Center erworben haben, können Sie mithilfe der Astra Control Center Lizenzseriennummer das Abonnement unter Data Infrastructure Insights identifizieren. Dateninfrastruktur Insights bezeichnet dies als *Entitlement ID*.

Um Ihrem Data Infrastructure Insights-Abonnement eine Berechtigungskennung hinzuzufügen, klicken Sie auf der Seite **Admin > Abonnement** auf *+Berechtigungskennung*.



Beobachtbarkeit

Dashboards Werden Erstellt

Übersicht Über Dashboards

Data Infrastructure Insights bietet den Benutzern die Flexibilität, Betriebsansichten von Infrastrukturdaten zu erstellen, indem Sie benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen können, von denen jede ein hohes Maß an Flexibilität bei der Anzeige und Dokumentation Ihrer Daten bietet.

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

Erstellen eines Dashboards

Sie erstellen ein neues Dashboard an einem von zwei Stellen:

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

Dashboard-Steuerelemente

Der Dashboard-Bildschirm verfügt über mehrere Bedienelemente:

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

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

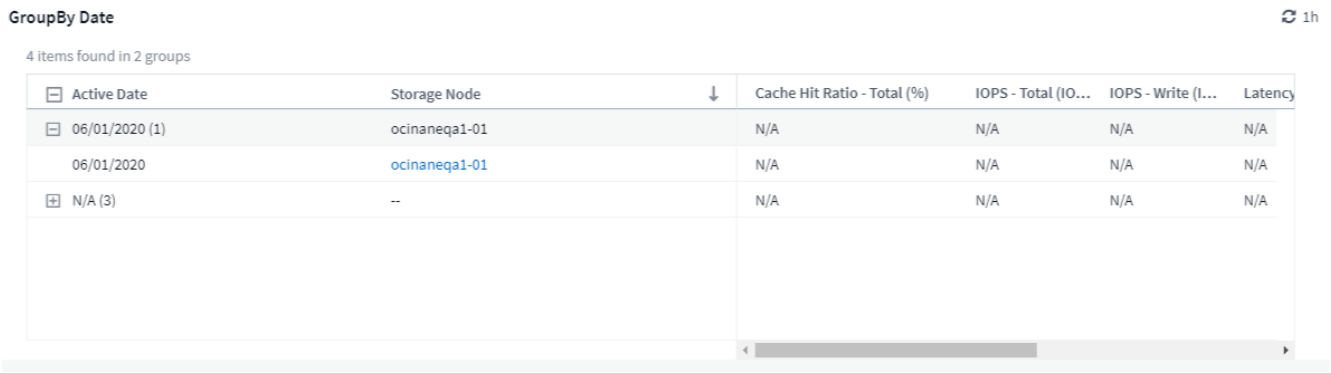
- **Widget**-Schaltfläche hinzufügen, mit der Sie eine beliebige Anzahl von Tabellen, Diagrammen oder anderen Widgets zum Dashboard hinzufügen können.

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

Widget-Typen

Sie können aus den folgenden Widgets wählen:

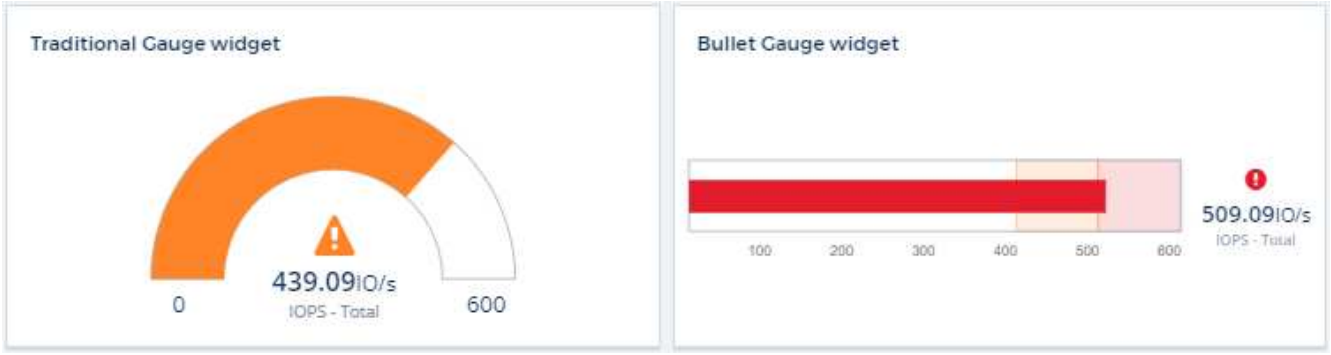
- **Tabelle Widget**: Eine Tabelle, die Daten nach den gewählten Filtern und Spalten anzeigt. Tabellendaten können in Gruppen zusammengefasst werden, die ausgeblendet und erweitert werden können.



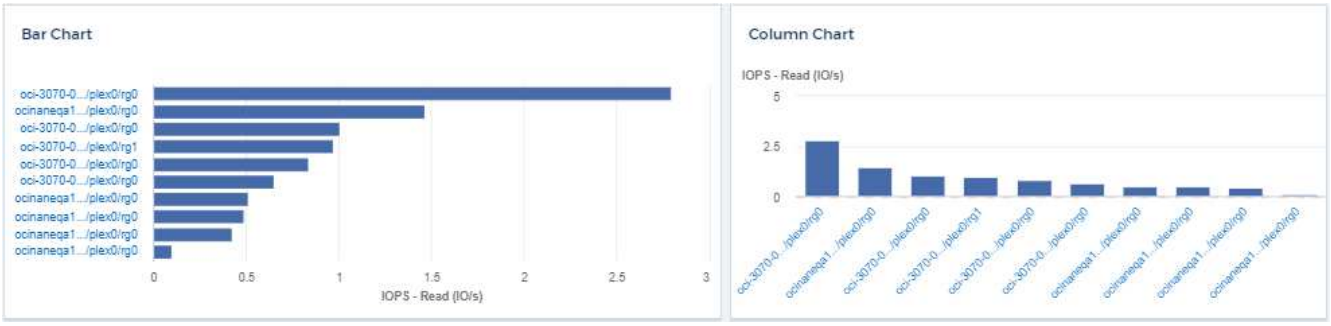
- **Linie, Spline, Bereich, gestapelte Flächendiagramme**: Dies sind Zeitreihenkarten-Widgets, auf denen Sie Leistung und andere Daten über die Zeit anzeigen können.

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

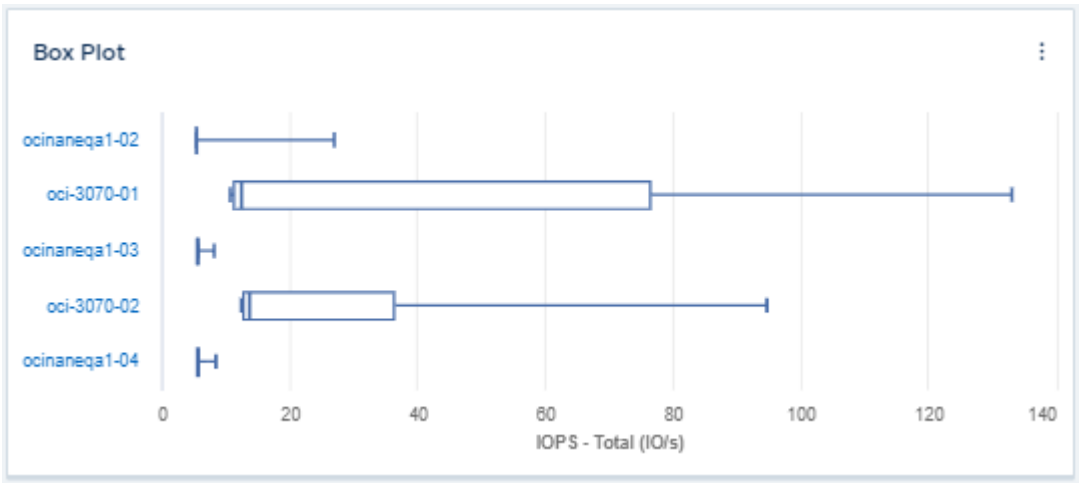
- **Widget messen**: Zeigt Daten mit einem einzigen Wert in einem herkömmlichen (festen) Manometer oder einer Kugel an, mit Farben, die auf "Warnung" oder "kritische" Werte basieren "Anpassen".



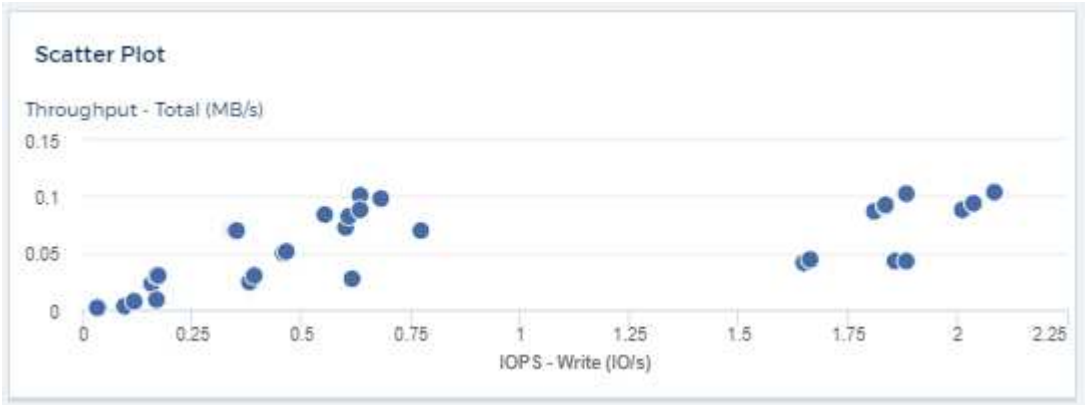
- **Balken, Spaltendiagramme**: Zeigt die oberen oder unteren N-Werte an, z. B. die Top 10-Storage nach Kapazität oder die unteren 5-Volumes nach IOPS.



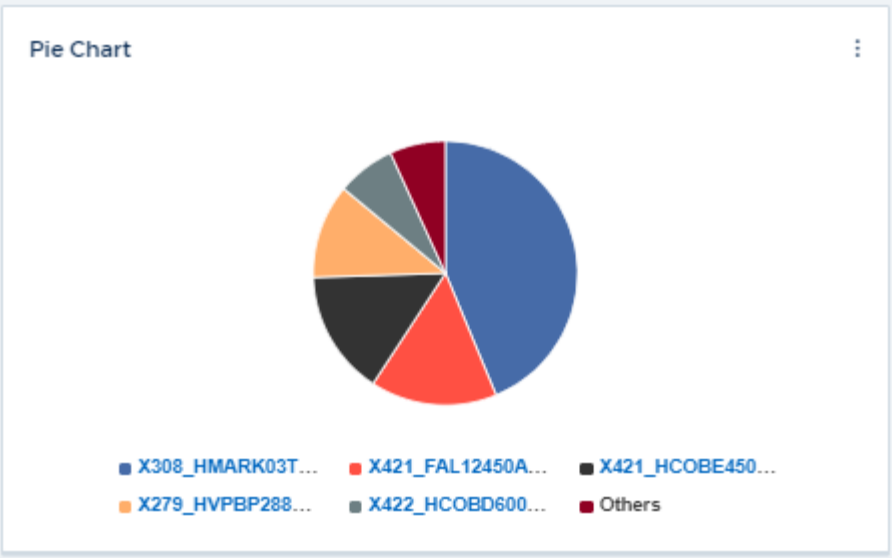
- **Box Plot Chart**: Eine Darstellung des min., max., Median und des Bereichs zwischen dem unteren und dem oberen Quartil der Daten in einem einzigen Diagramm.



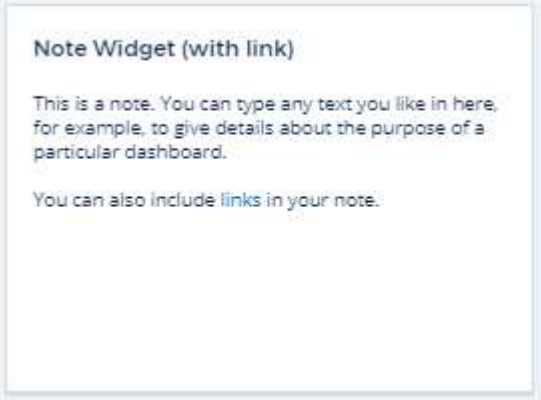
- **Scatter Plot Chart**: Zeichnet verwandte Daten als Punkte, zum Beispiel IOPS und Latenz. In diesem Beispiel sind Assets mit hohem Durchsatz und niedrigen IOPS schnell zu finden.



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



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



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

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

Einrichten eines Dashboards als Startseite

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

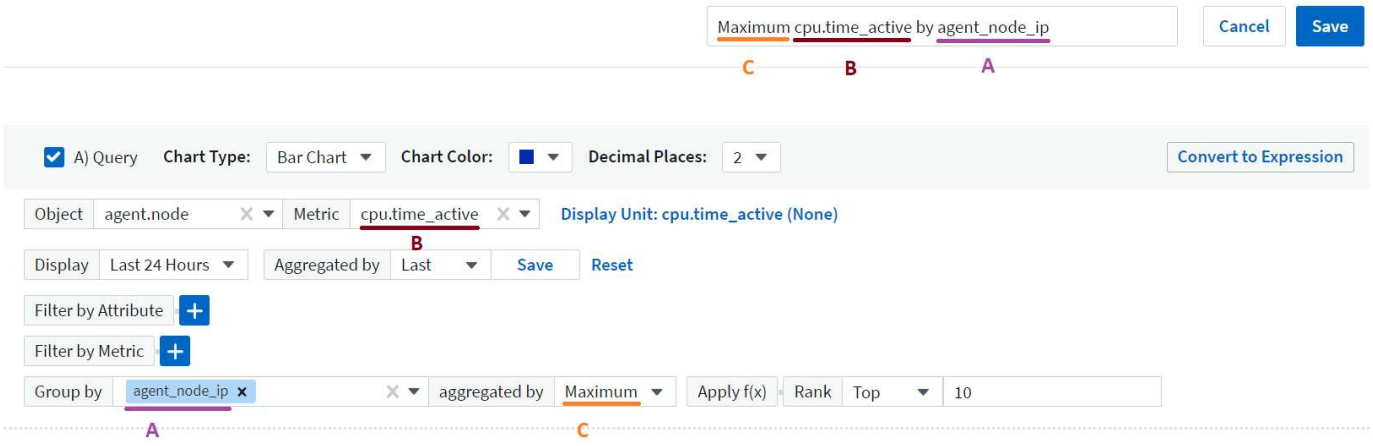
- Gehen Sie zu **Dashboards > Alle Dashboards anzeigen**, um die Liste der Dashboards in Ihrer Umgebung anzuzeigen. Klicken Sie auf das Optionsmenü rechts neben dem gewünschten Dashboard und wählen Sie **als Startseite festlegen**.
- Klicken Sie in der Liste auf ein Dashboard, um das Dashboard zu öffnen.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

Dashboard-Funktionen

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

Widget-Naming

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



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

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

Widget-Platzierung und -Größe

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

Duplizieren eines Widgets

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

Widget-Legenden Werden Angezeigt

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

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

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

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

Neue Metriken

Data Infrastructure Insights bietet verschiedene **transform**-Optionen für bestimmte Kennzahlen in Widgets (insbesondere die Kennzahlen, die als „Benutzerdefinierte“ oder „Integrationsmetriken“ bezeichnet werden, wie z. B. von Kubernetes, ONTAP Advanced Data, Telegraf-Plug-ins usw.), so dass Sie die Daten auf verschiedene Arten anzeigen können. Beim Hinzufügen transformbarer Metriken zu einem Widget werden Sie mit einem Dropdown-Menü mit den folgenden Optionen zur Transformation angezeigt:

Keine
: Die Daten werden ohne Manipulation als IS angezeigt.

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

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

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

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

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

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

Anfragen und Filter für das Dashboard-Widget

Abfragen

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

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

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

Die folgenden Widget-Typen können mehrere Abfragen haben:

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

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

- Tabelle
- Balkendiagramm
- Box-Darstellung
- Streudiagramm

Filtern in Dashboard-Widget-Abfragen

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

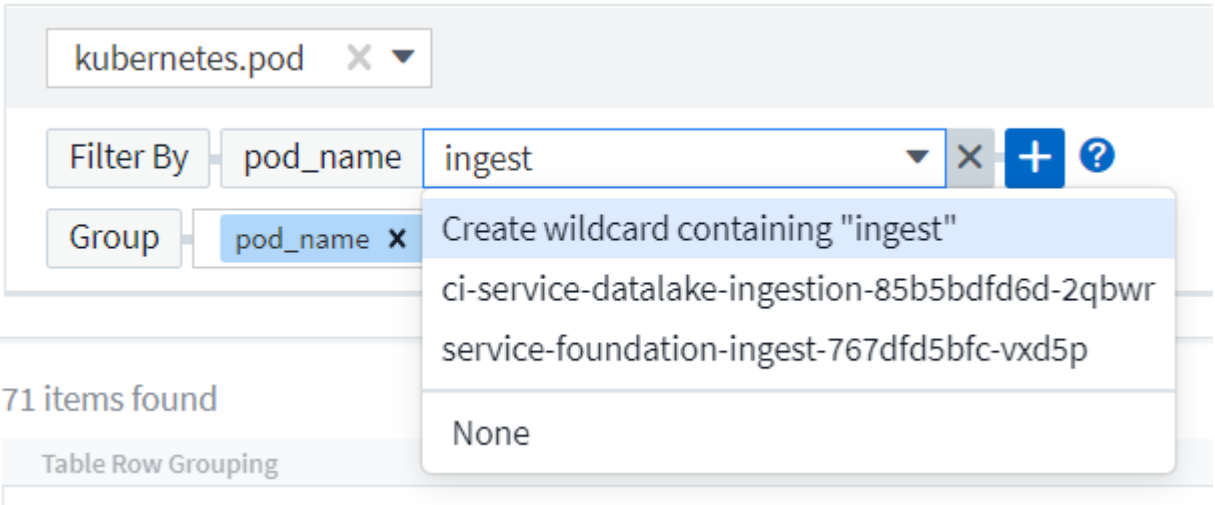
Filter Für Exakte Übereinstimmung

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

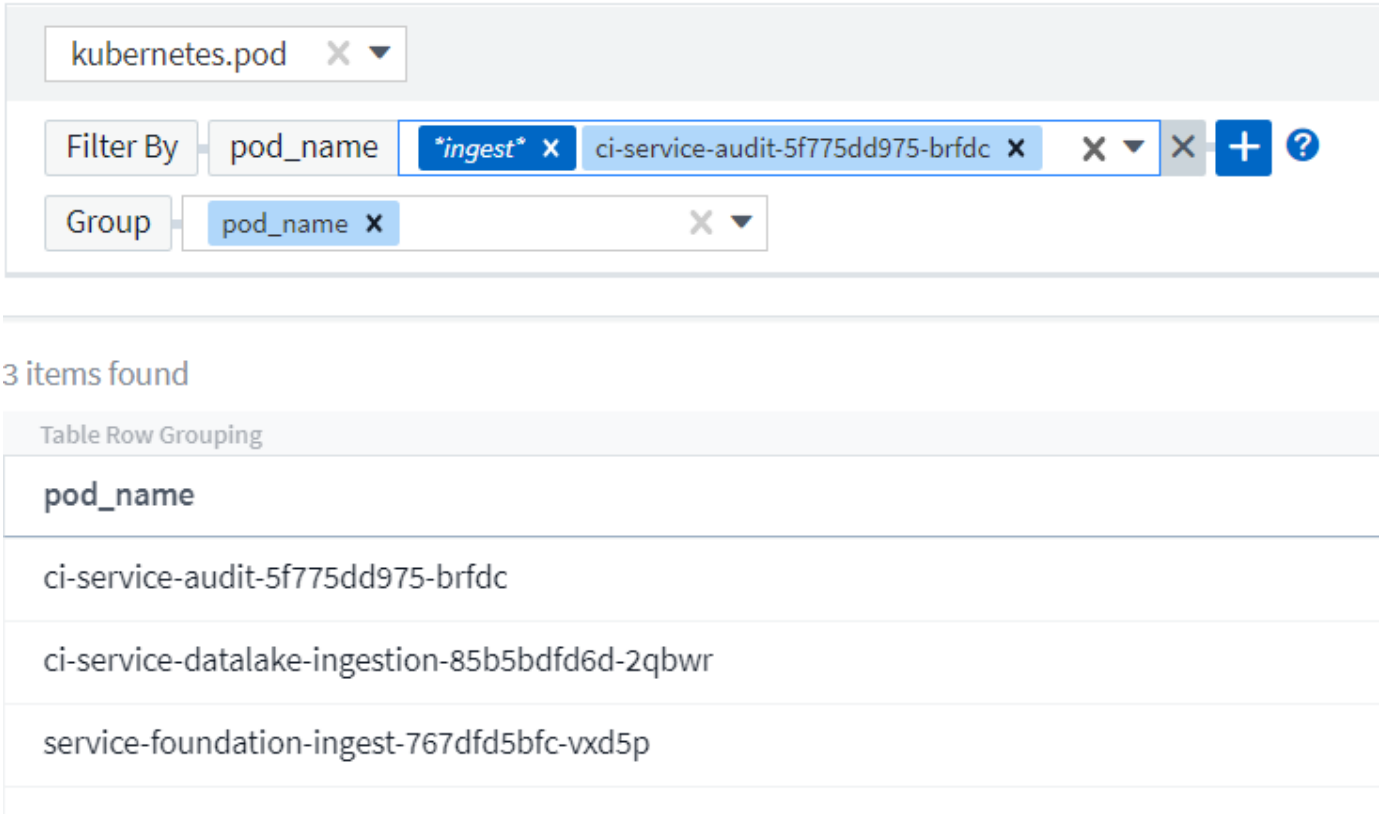
Sie können mithilfe von „Exact Match“-Filtern nach bestimmten Ressourcen suchen, z. B. nach Hostnamen. Wenn Sie nur den Hostnamen 'Marketing' finden möchten, aber 'Marketings-boston' ausschließen möchten, schließen Sie einfach den Namen "Marketing" in doppelte Anführungszeichen ein.

Platzhalter und Ausdrücke

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



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



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

Erweiterte Textfilterung mit Vorschlägen zum Kontexttyp

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

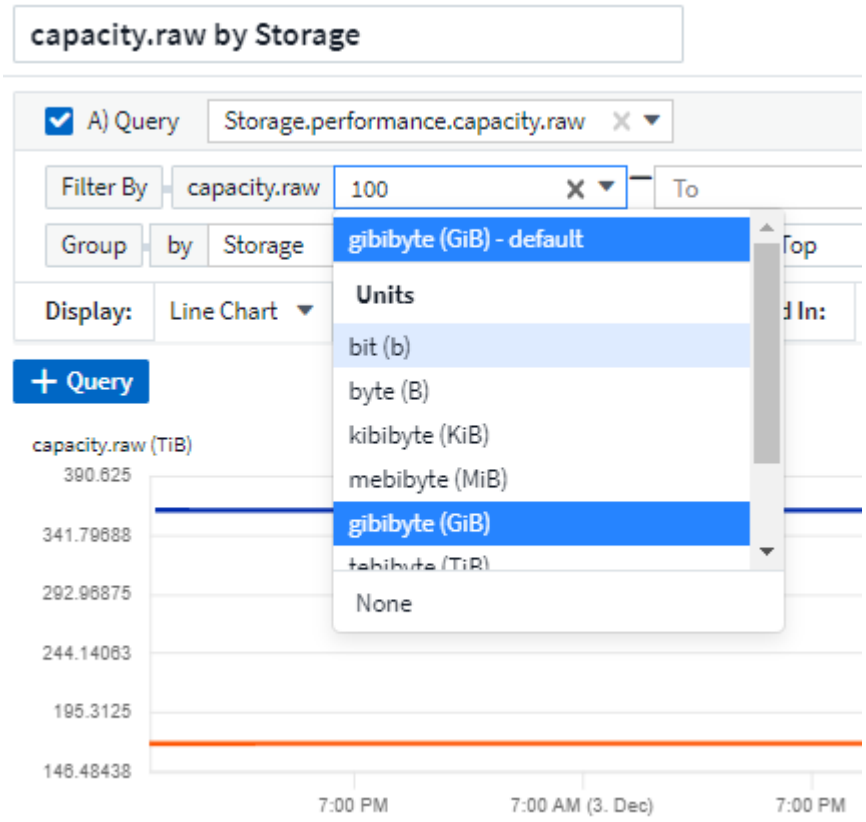
Kontextbezogene Filterung gilt auch für Dashboard-Seitenvariablen (nur Textattribute oder Anmerkungen). Wenn Sie einen Filer-Wert für eine Variable auswählen, werden bei allen anderen Variablen, die verwandte Objekte verwenden, nur mögliche Filterwerte auf der Grundlage dieser verwandten Variablen angezeigt.

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

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

Auswählen der Filtereinheiten

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



Zusätzliche Filterveredlungen

Mit den folgenden Optionen können Sie Ihre Filter weiter verfeinern.

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

  ```
  vol*rhel
  ```

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

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

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

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

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

  ```
  FAS2240 OR CX600 OR FAS3270
  ```

  Findet mehrere Storage-Modelle

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

```
NOT EMC*
```

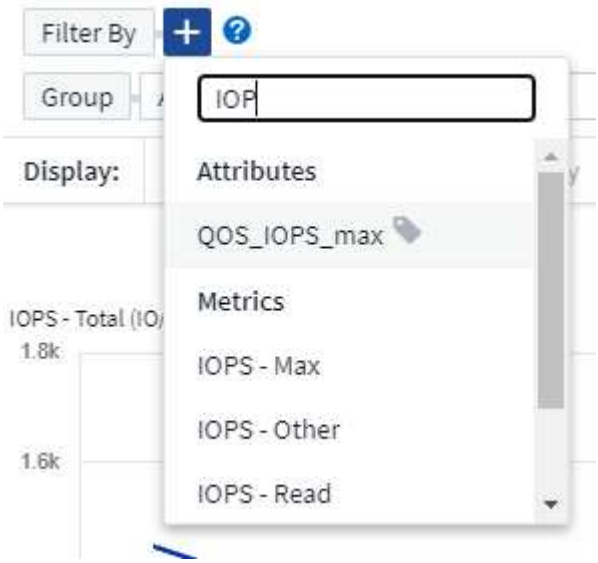
Findet alles, was nicht mit „EMC“ beginnt. Verwenden Sie können

```
NOT *
```

So zeigen Sie Felder an, die keinen Wert enthalten.

Identifizieren von Objekten, die von Abfragen und Filtern zurückgegeben werden

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



Gruppierung und Aggregation

Gruppierung (Rolling Up)

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

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

Schritte

Gehen Sie wie folgt vor, um die Gruppierungsmethode festzulegen.

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

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

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

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

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

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

Aggregation von Daten

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

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

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

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

Anzeige Der Oberen/Unteren Ergebnisse

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

Diagramm-Widget oben/unten

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

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

Tabelle Widget zeigt Einträge an

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

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

Gruppierung in TabellenWidget

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

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

Die Gruppierung ist nur im Widget-Typ Tabelle verfügbar.

Beispiel für Gruppierung (mit Rollup-Erklärung)

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

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

Schritte

1. Erstellen oder öffnen Sie ein Dashboard, und fügen Sie ein Widget mit * Table* hinzu.
2. Wählen Sie *Virtual Machine* als Asset-Typ für dieses Widget aus.
3. Klicken Sie auf die Spaltenauswahl und wählen Sie *Hypervisor Name* und *IOPS - Total*.

   Diese Spalten werden jetzt in der Tabelle angezeigt.

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

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

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

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

   In jedem Spaltenkopf für eine Leistungskennzahl wird ein Menü „drei Punkte“ mit einer Option **Roll Up** angezeigt. Die Standard-Rollup-Methode lautet *Average*. Das bedeutet, dass die für die Gruppe

angezeigte Zahl der Durchschnitt aller gesamten IOPS ist, die für jede VM innerhalb der Gruppe gemeldet wurden. Sie können diese Spalte um *Durchschnitt, Summe, Minimum* oder *Maximum* nach oben Rollen. Alle angezeigten Spalten mit Performance-Metriken können individuell aufgerollt werden.

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

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

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

Aufkommen von Performance-Daten

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

Dashboard-Zeitbereich – Auswahl

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

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Die Letzten 2 Stunden
- Die letzten 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden

- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

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

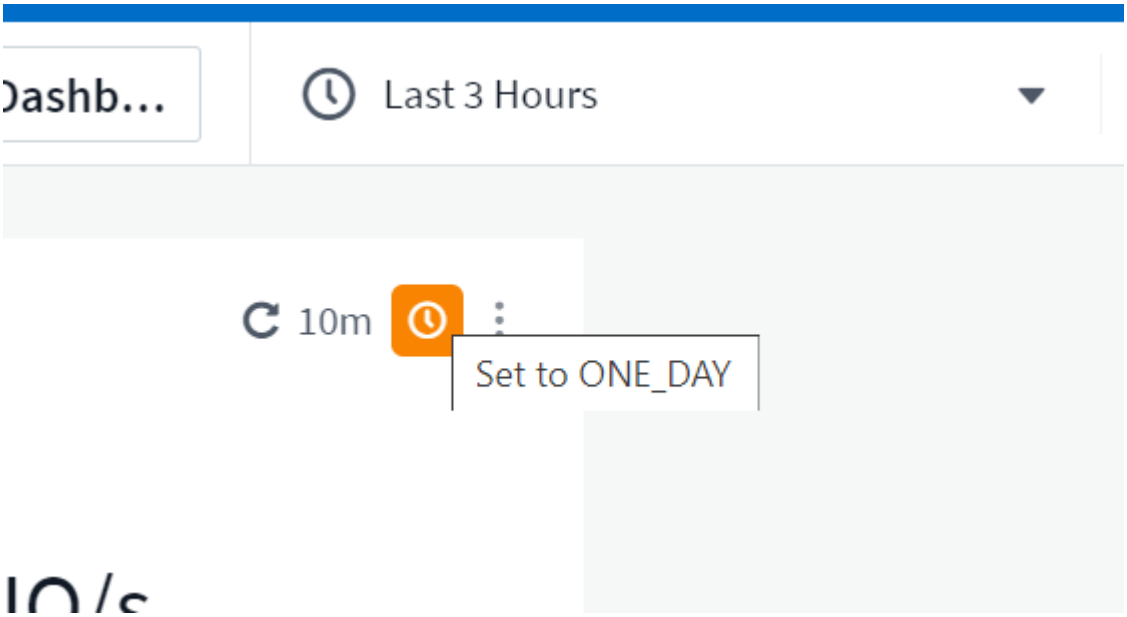
Dashboard-Zeit in einzelnen Widgets außer Kraft setzen

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

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

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

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



Primäre und sekundäre Achse

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

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

Schritte

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

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

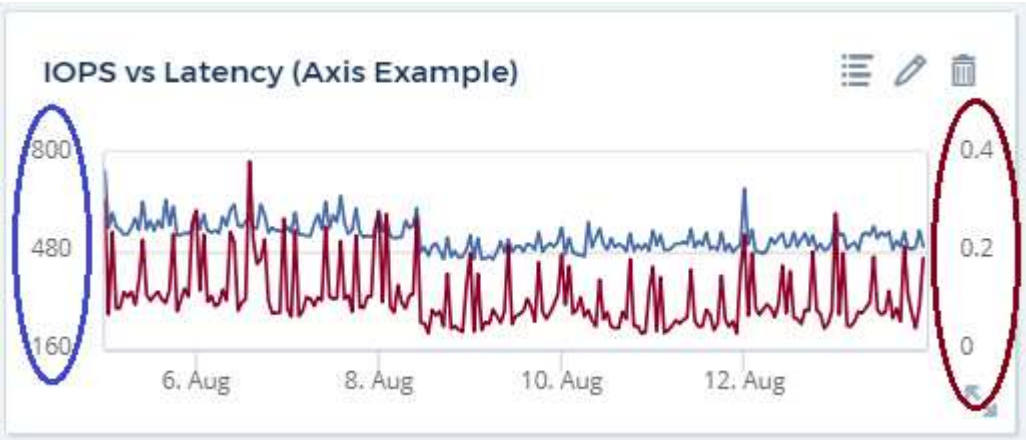
   Die IOPS-Linie wird auf dem Diagramm angezeigt, wobei ihre Skalierung auf der linken Seite dargestellt ist.

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

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

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

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



Ausdrücke in Widgets

In einem Dashboard können Sie mit einem Widget für Zeitreihen (Linie, Spline, Bereich, gestapelter Bereich), einem Balkendiagramm, einem Säulendiagramm, einem Kreisdiagramm oder einem Widget für Tabellen

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

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

Ausdrücke Beispiel: Lese-IOPS in Prozent

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

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

Schritte

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

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

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

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

   Bleiben Sie jetzt im Expression-Modus.

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

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

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

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

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

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

Ausdrücke Beispiel: "System" I/O

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

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

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

Schritte

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

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

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

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

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

   Ein Duplikat der Abfrage wird unterhalb des Originals hinzugefügt.

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

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

   Bleiben Sie jetzt im Expression-Modus.

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

   ```
   a + b
   ```

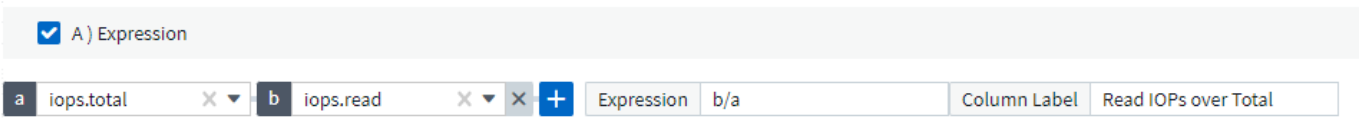
   Wählen Sie im Bereich Anzeige für diesen Ausdruck die Option **Flächendiagramm** aus.
9. Das Feld **Beschriftung** kennzeichnet den Ausdruck. Ändern Sie das Label in „System IOPS“ oder etwas, das für Sie gleichbedeutend ist.

   Im Diagramm wird die IOPS insgesamt als Liniendiagramm angezeigt. In einem Flächendiagramm wird die Kombination aus Lese- und Schreib-IOPS unterhalb dieser Werte angezeigt. Die Lücke zwischen den beiden gibt die IOPS an, die nicht direkt mit Lese- oder Schreibvorgängen verbunden sind. Das sind Ihre „System“ IOPS.
10. Klicken Sie auf **Speichern**, um das Diagramm auf Ihrem Dashboard zu speichern.

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

Ausdrücke in einem TabellenWidget

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



Variablen

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

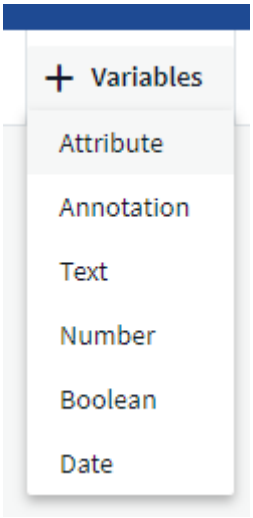
Dashboard-Variablen enthalten verschiedene Typen, können in verschiedenen Feldern verwendet werden und müssen Regeln für die Benennung befolgen. Diese Konzepte werden hier erläutert.

Variabentypen

Eine Variable kann einen der folgenden Typen sein:

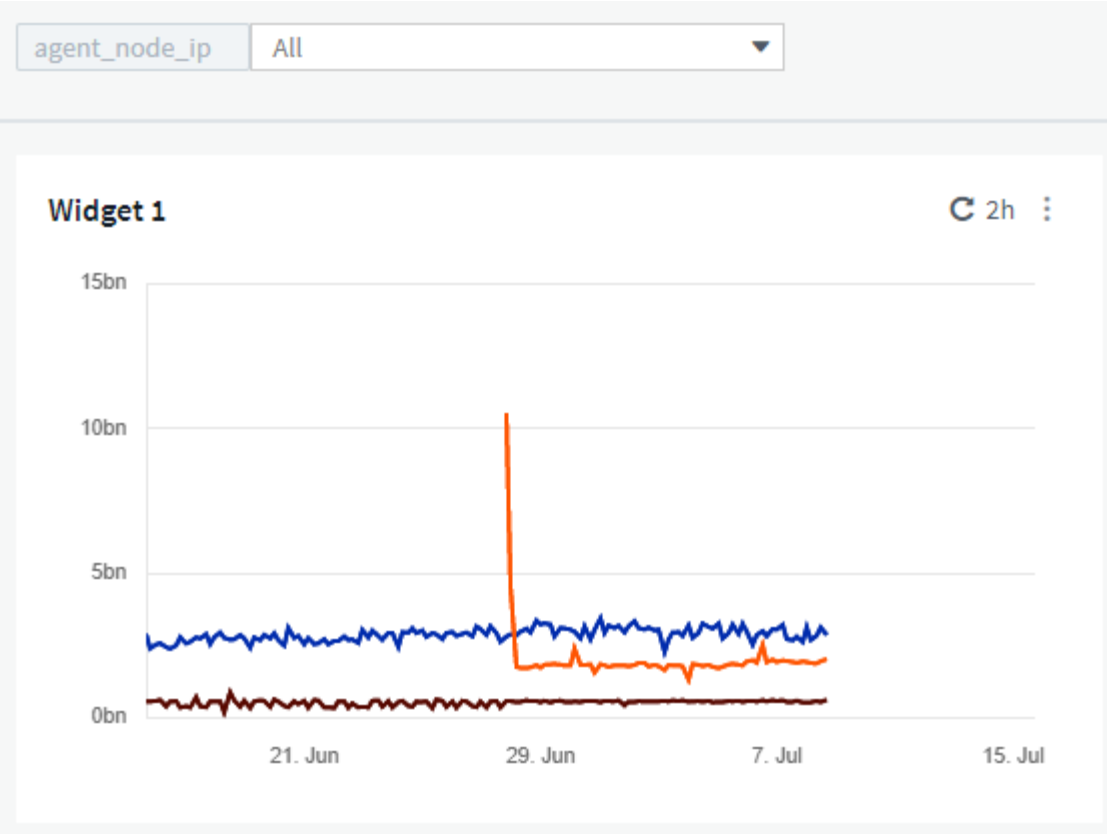
- **Attribut**: Verwenden Sie die Attribute oder Metriken eines Objekts, um sie zu filtern
- **Anmerkung**: Verwenden Sie eine vordefinierte "Anmerkung" Widget-Daten filtern.

- **Text**: Eine alphanumerische Zeichenfolge.
- **Numerisch**: Ein Zahlenwert. Sie können je nach Widget-Feld entweder selbst oder als „von“- oder „nach“-Wert verwenden.
- **Boolean**: Verwenden Sie für Felder mit Werten True/False, Yes/No, etc. Für die boolesche Variable stehen die Optionen Ja, Nein, Keine, Any.
- **Datum**: Ein Datumswert. Verwenden Sie je nach Konfiguration Ihres Widgets als „von“ oder „nach“-Wert.

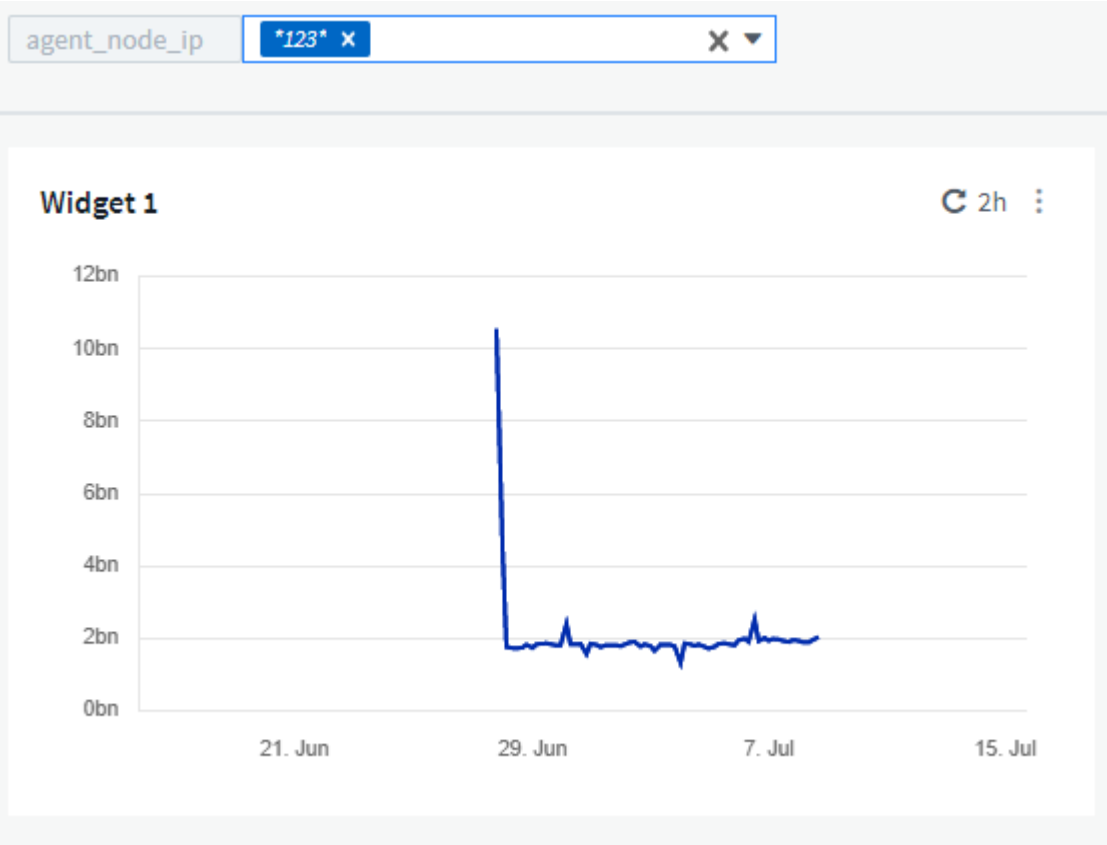


Attributvariablen

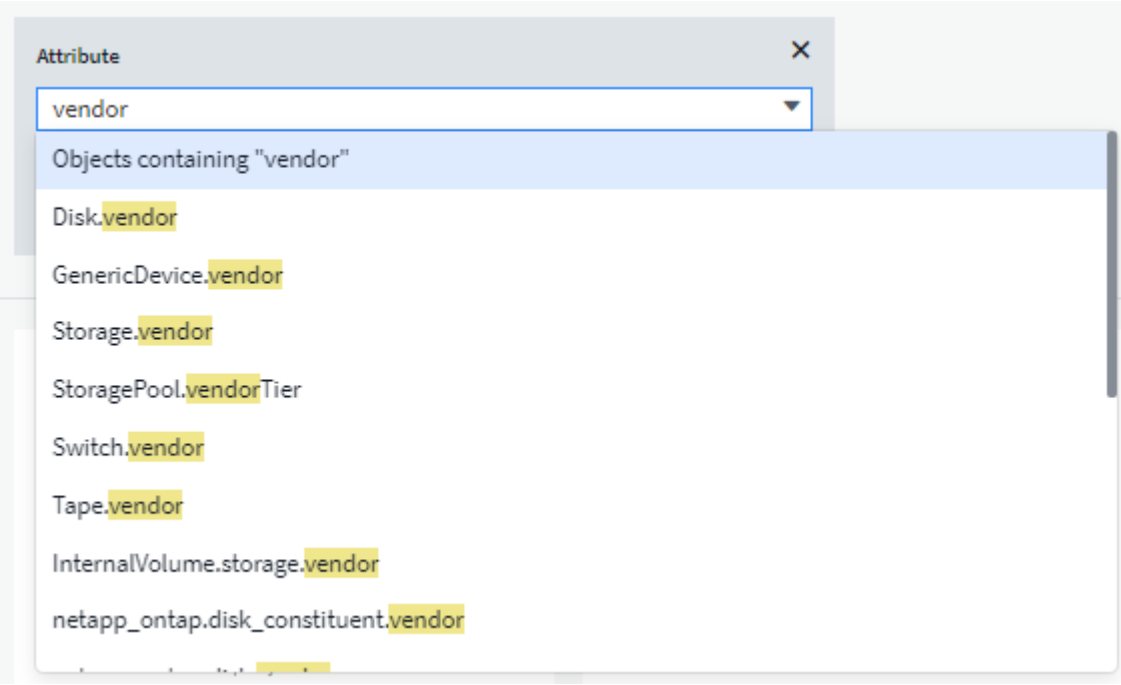
Durch die Auswahl einer Attributtypvariable können Sie nach Widget-Daten filtern, die den angegebenen Attributwert oder die angegebenen Werte enthalten. Das folgende Beispiel zeigt ein Line-Widget mit freien Speichertrends für Agent-Knoten. Wir haben eine Variable für Agent-Node-IPs erstellt, die derzeit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



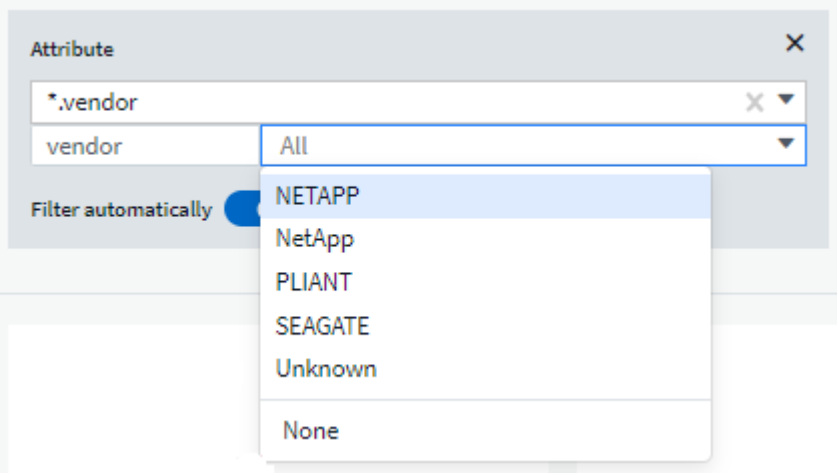
Wenn Sie jedoch vorübergehend nur Nodes in einzelnen Subnetzen in Ihrer Umgebung sehen möchten, können Sie die Variable in eine bestimmte Agent-Node-IP oder IPs einstellen oder ändern. Hier sehen wir nur die Knoten auf dem „123“ Subnetz:



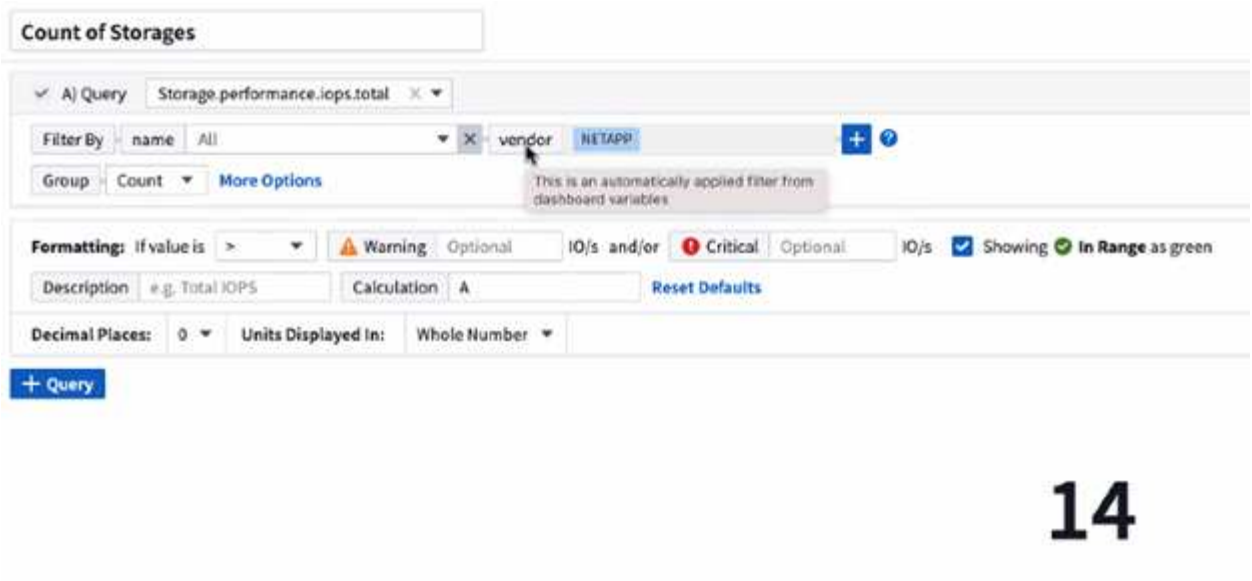
Sie können auch eine Variable festlegen, um unabhängig vom Objekttyp auf *all* Objekte mit einem bestimmten Attribut zu filtern, zum Beispiel Objekte mit einem Attribut "Anbieter", indem Sie **.Vendor* im Feld Variable angeben. Sie müssen kein „*.“ eingeben; Data Infrastructure Insights liefert dies, wenn Sie die Platzhalteroption auswählen.



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



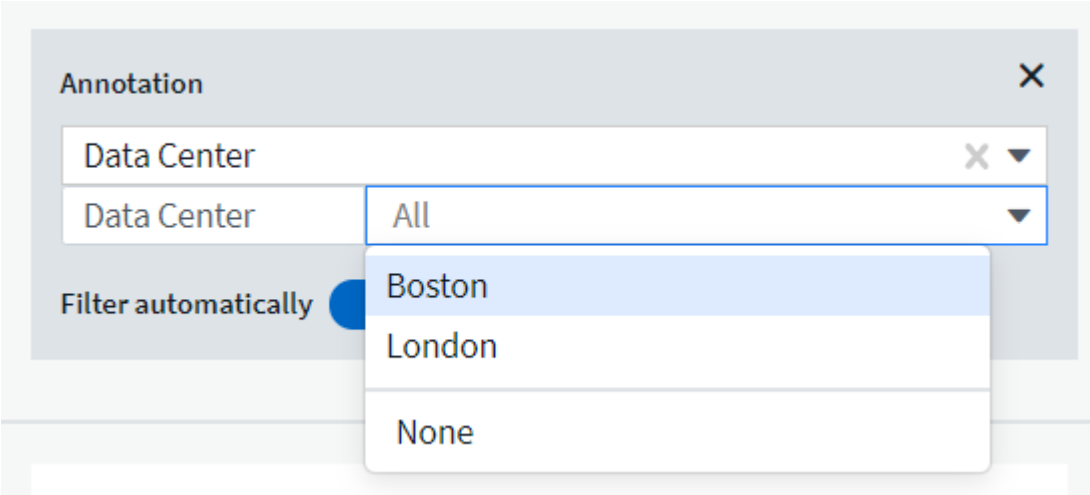
Wenn Sie ein Widget in Ihrem Dashboard bearbeiten, in dem der Attributfilter relevant ist (d. h. die Objekte des Widgets enthalten ein beliebiges **.Vendor-Attribut*), zeigt es Ihnen an, dass der Attributfilter automatisch angewendet wird.



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

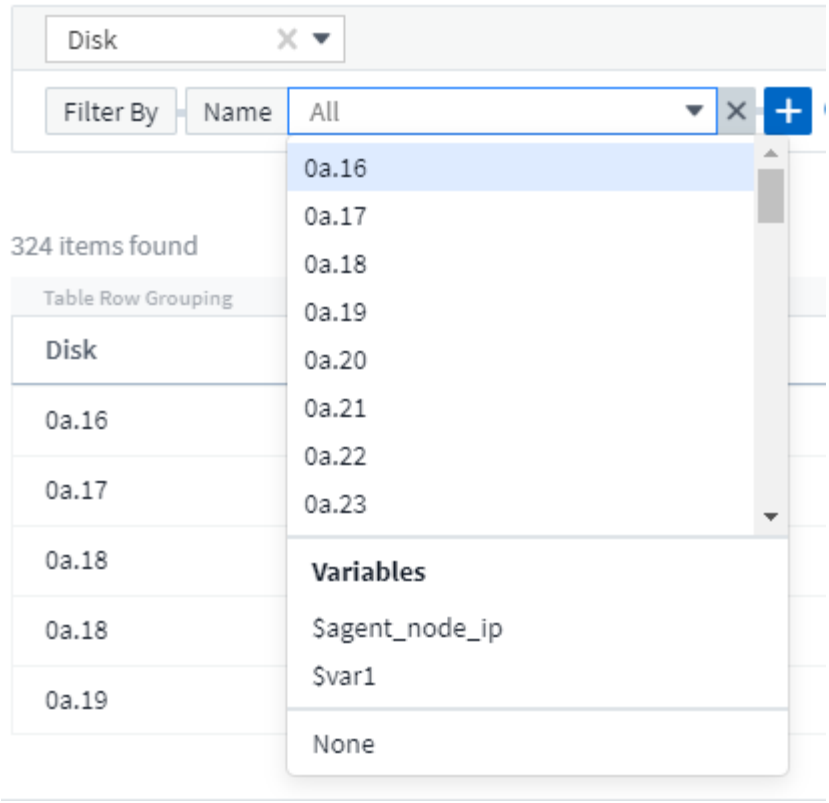
Anmerkungsvariablen

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



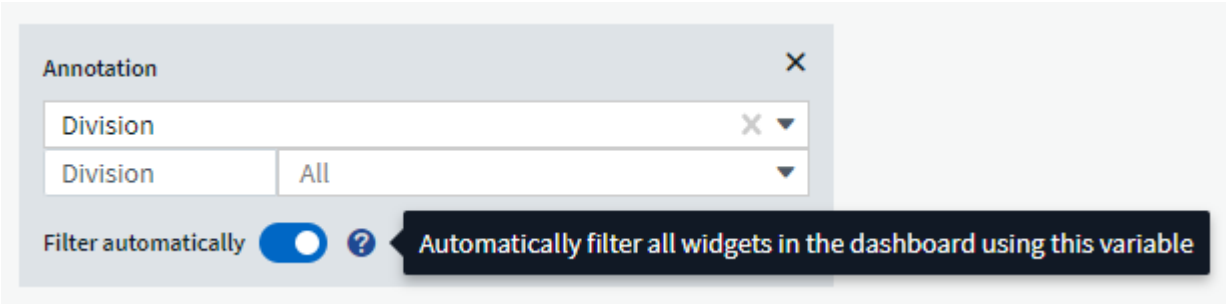
Text, Nummer, Datum oder Boolesche Variable

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



Bereich Für Variablenfilter

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



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

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

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

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

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

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

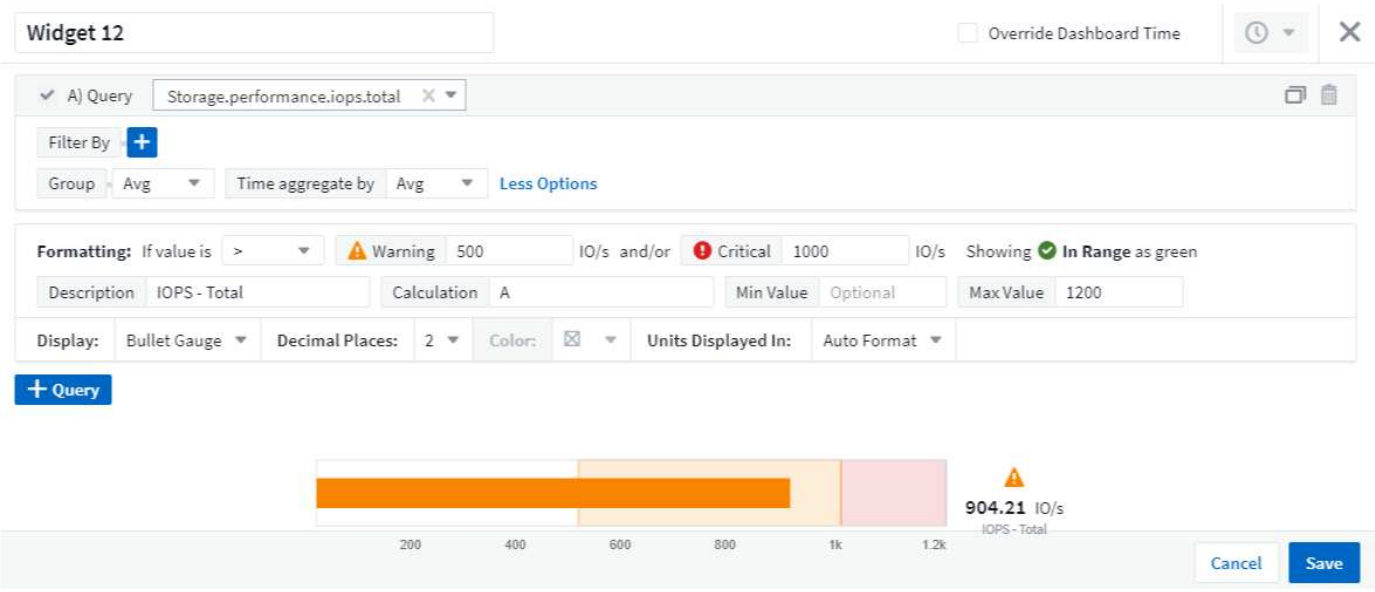
Variablenbenennung

Variablennamen:

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

Formatieren Von Messbreitewidgets

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



So legen Sie die Formatierung für diese Widgets fest:

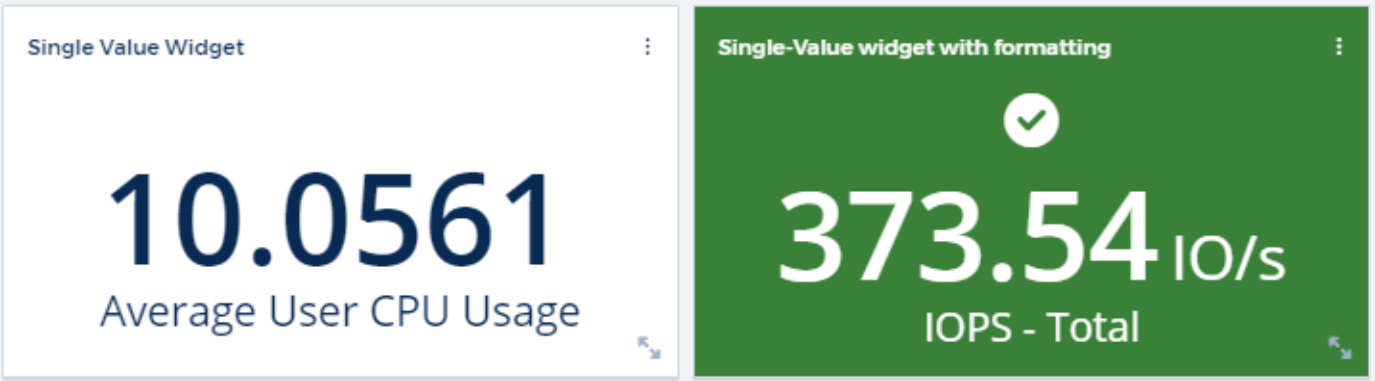
1. Wählen Sie aus, ob Sie Werte größer als (>) oder kleiner als (<) Ihre Schwellenwerte markieren möchten. In diesem Beispiel werden Werte hervorgehoben, die größer sind als (>) die Schwellwerte.

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

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

Formatieren Eines Single-Value-Widgets

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



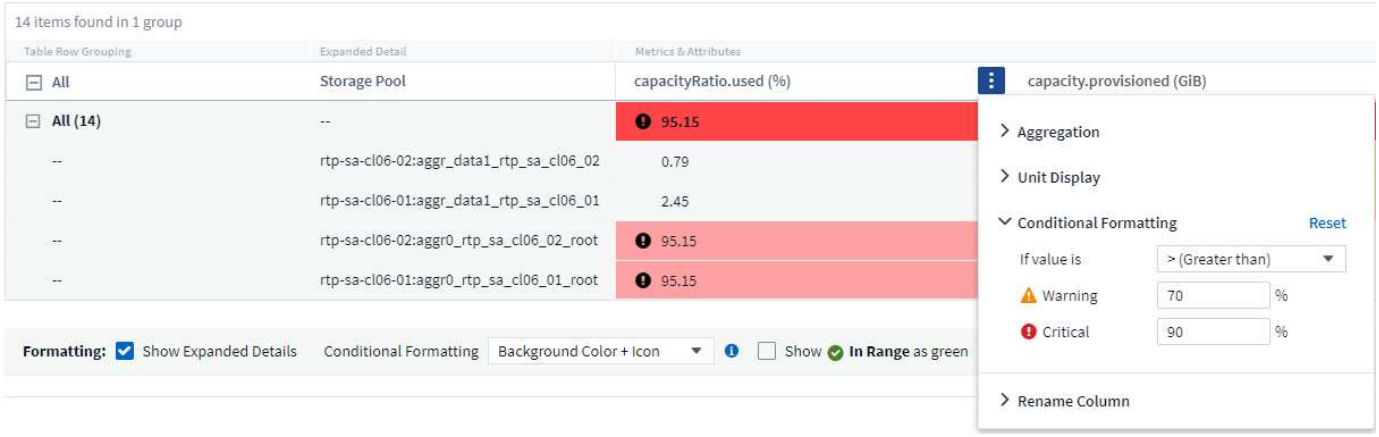
Wenn Sie auf den Link in einem Widget mit einem Wert oder einem Gauge-Widget klicken, wird eine Abfrageseite angezeigt, die der ersten Abfrage im Widget entspricht.

Formatieren Von Tabellenwidgets

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

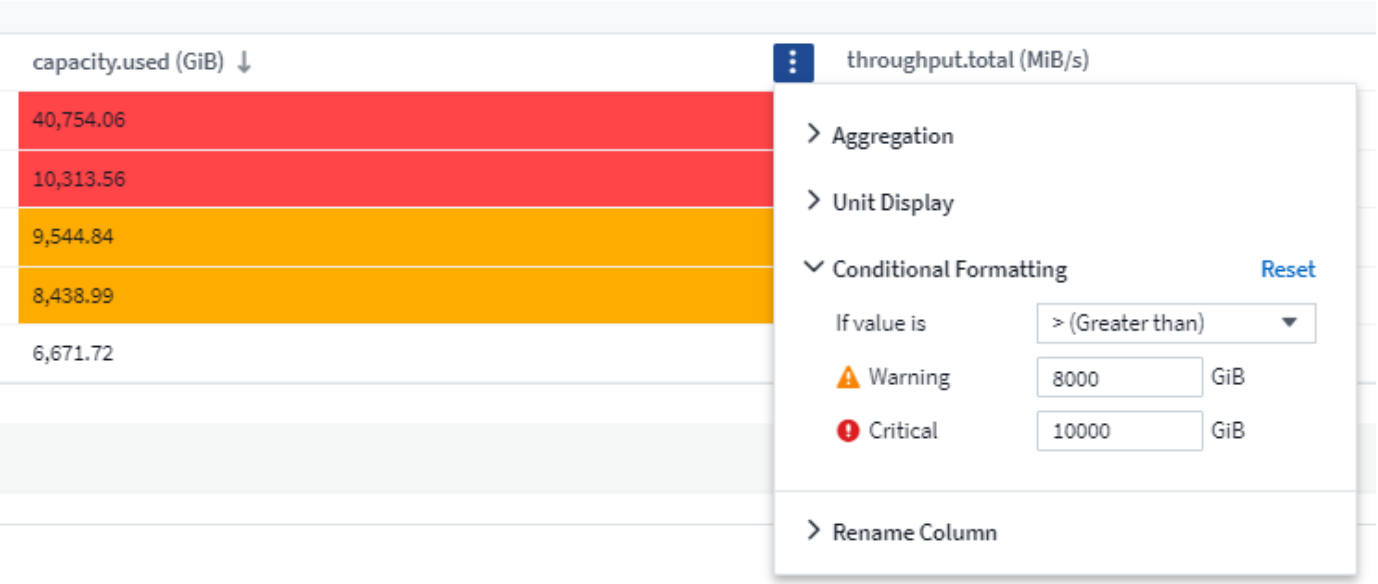
Bedingte Formatierung ist derzeit in Data Infrastructure Insights Federal Edition nicht verfügbar.

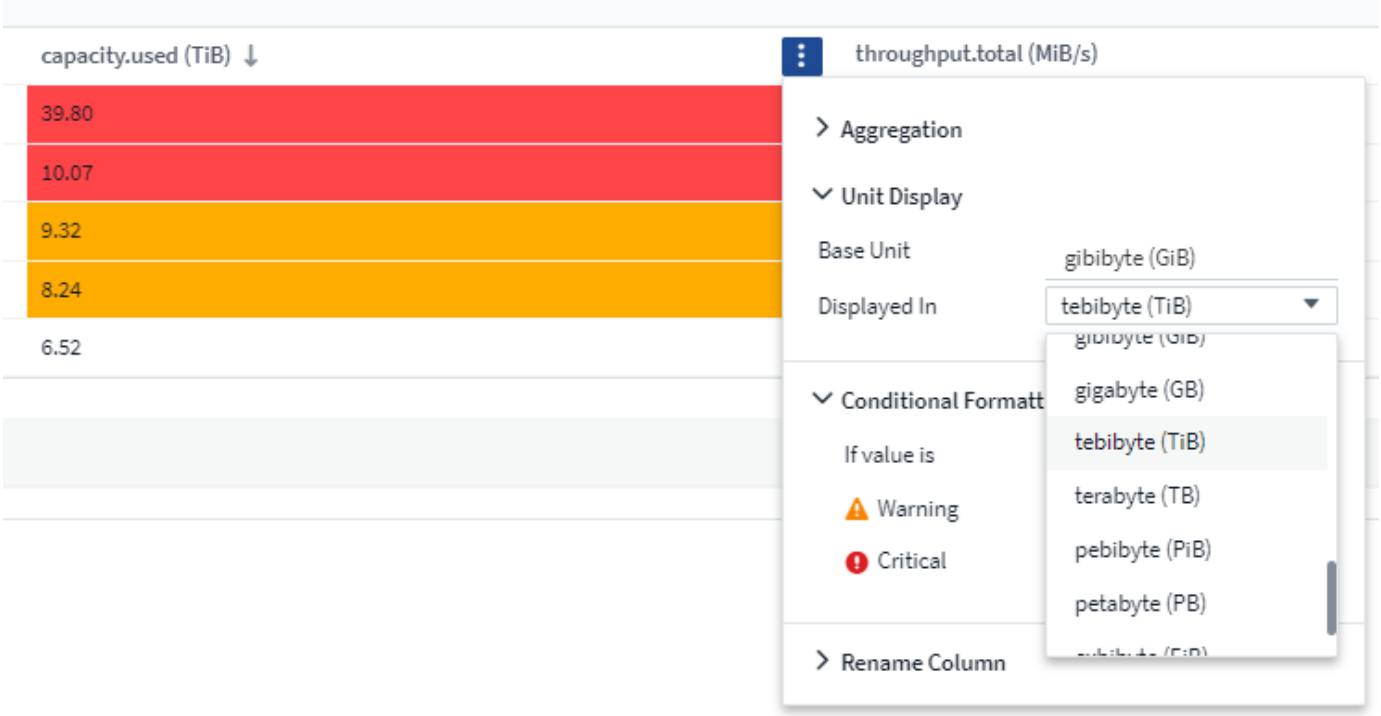
Mit Conditional Formatting können Sie Schwellenwerte auf Warnebene und kritische Ebene in den TabellenWidgets festlegen und hervorheben. Dadurch erhalten Sie sofortige Sichtbarkeit für Ausreißer und außergewöhnliche Datenpunkte.



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

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



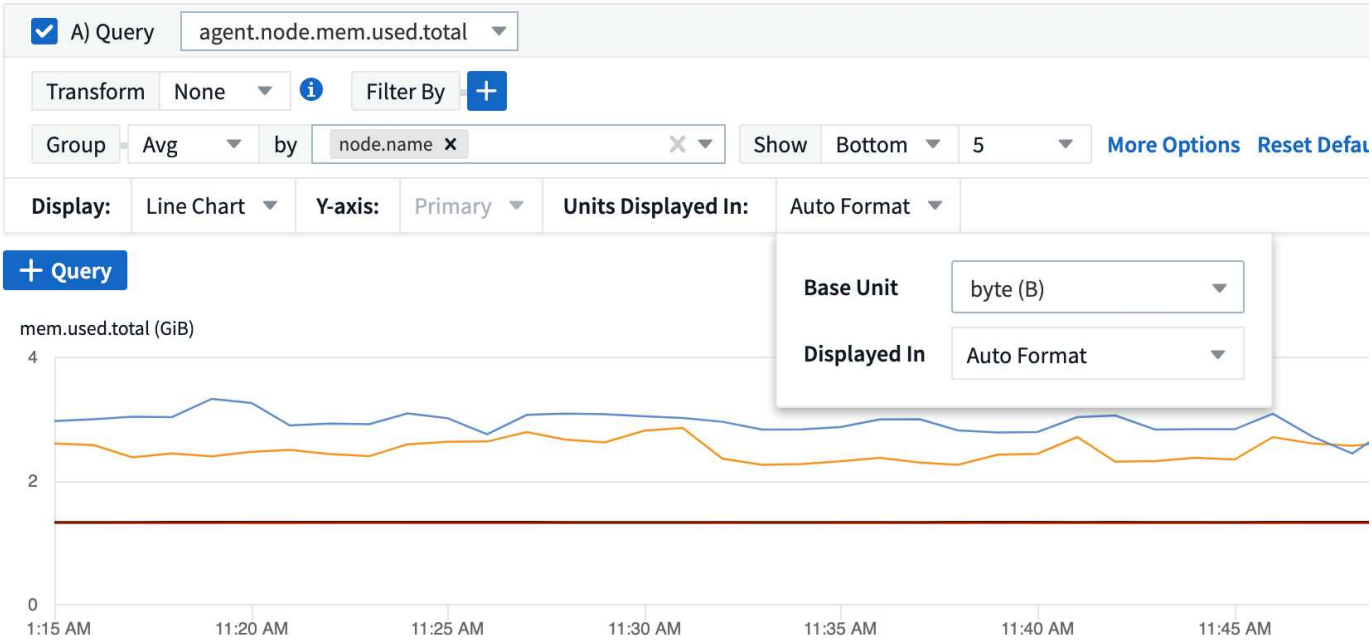


Sie können festlegen, ob die Zustandsformatierung als Farbe, Symbole oder beides angezeigt werden soll.

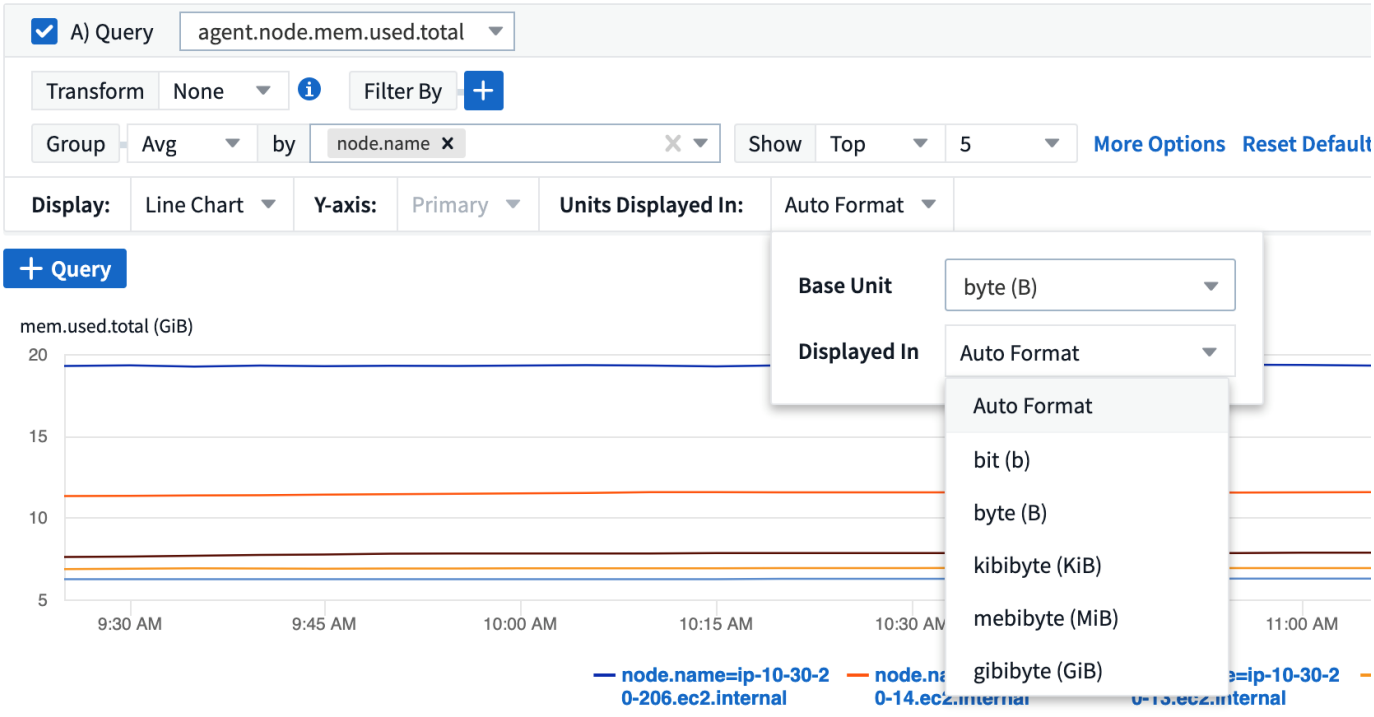
Auswählen des Geräts für die Datenanzeigen(Anzeige

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

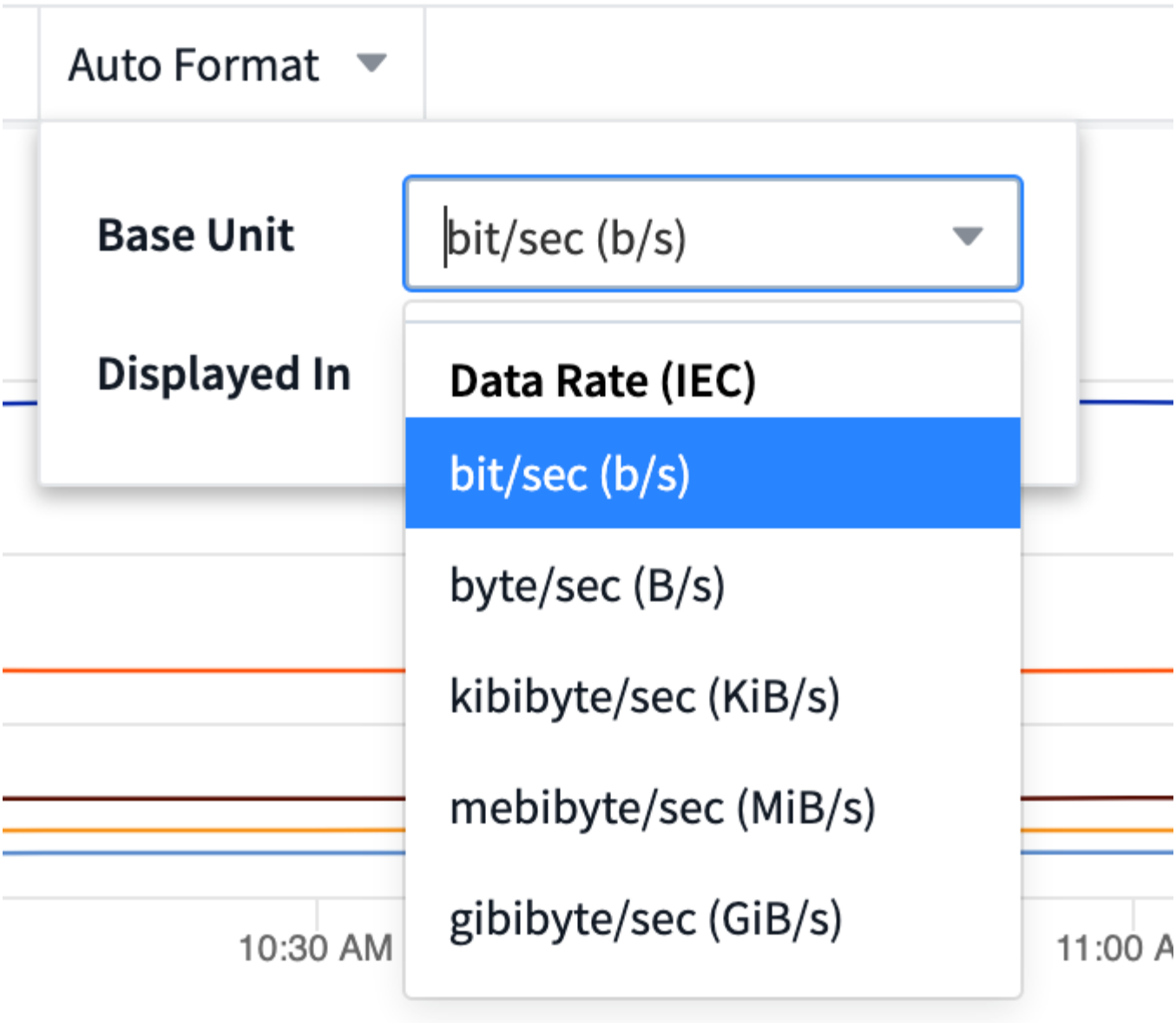
Im nachstehenden Liniendiagramm sind die für das Widget ausgewählten Daten in *Bytes* (die Basiseinheit IEC-Daten: Siehe Tabelle unten) angegeben, sodass die Basiseinheit automatisch als 'Byte (B)' ausgewählt wird. Die Datenwerte sind jedoch groß genug, um als Gibibyte (gib) dargestellt zu werden. Daher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



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



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



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

Ein Wort zu Auto-Format

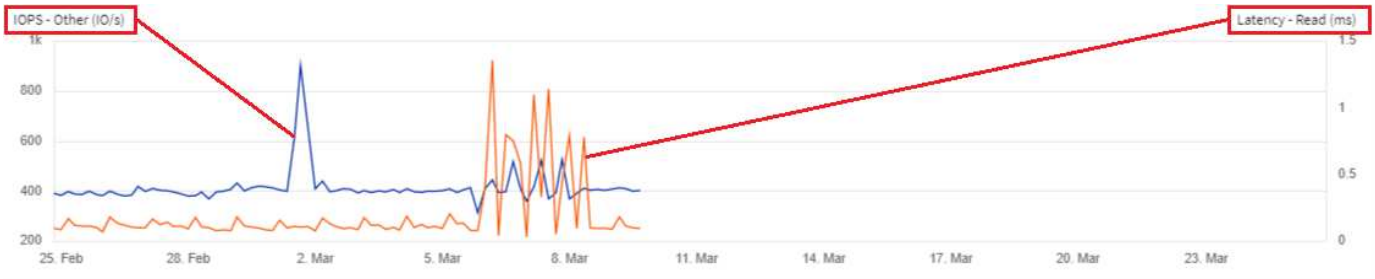
Die meisten Metriken werden von Datensammlern in der kleinsten Einheit berichtet, beispielsweise als ganze Zahl wie 1,234,567,890 Bytes. Standardmäßig formatiert Data Infrastructure Insights den Wert für die am besten lesbare Anzeige automatisch. Beispielsweise würde ein Datenwert von 1,234,567,890 Byte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

Data Infrastructure Insights verwendet amerikanische Standards für die Nummernbenennung. Die amerikanische "Milliarde" entspricht "tausend Millionen".

Widgets mit mehreren Abfragen

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

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



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

Verfügbare Einheiten

Die folgende Tabelle zeigt alle verfügbaren Einheiten nach Kategorie.

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

TV-Modus und automatische Aktualisierung

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

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

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

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

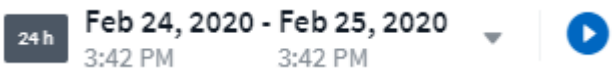
Die automatische Aktualisierung ist für den benutzerdefinierten Zeitbereich des Dashboards nicht verfügbar.

In Kombination mit **TV-Modus** ermöglicht die automatische Aktualisierung die Anzeige von Daten auf einem Dashboard oder einer Asset-Seite nahezu in Echtzeit. Der TV-Modus bietet ein übersichtliches Display. Das Navigationsmenü ist ausgeblendet und bietet so mehr Platz für Ihre Datenanzeige, wie die Schaltfläche Bearbeiten. Im TV-Modus werden typische Daten-Infrastruktur-Insights-Timeouts ignoriert. Die Anzeige bleibt so lange aktiv, bis sie manuell oder automatisch über Sicherheitsprotokolle der Autorisierung abgemeldet wird.

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

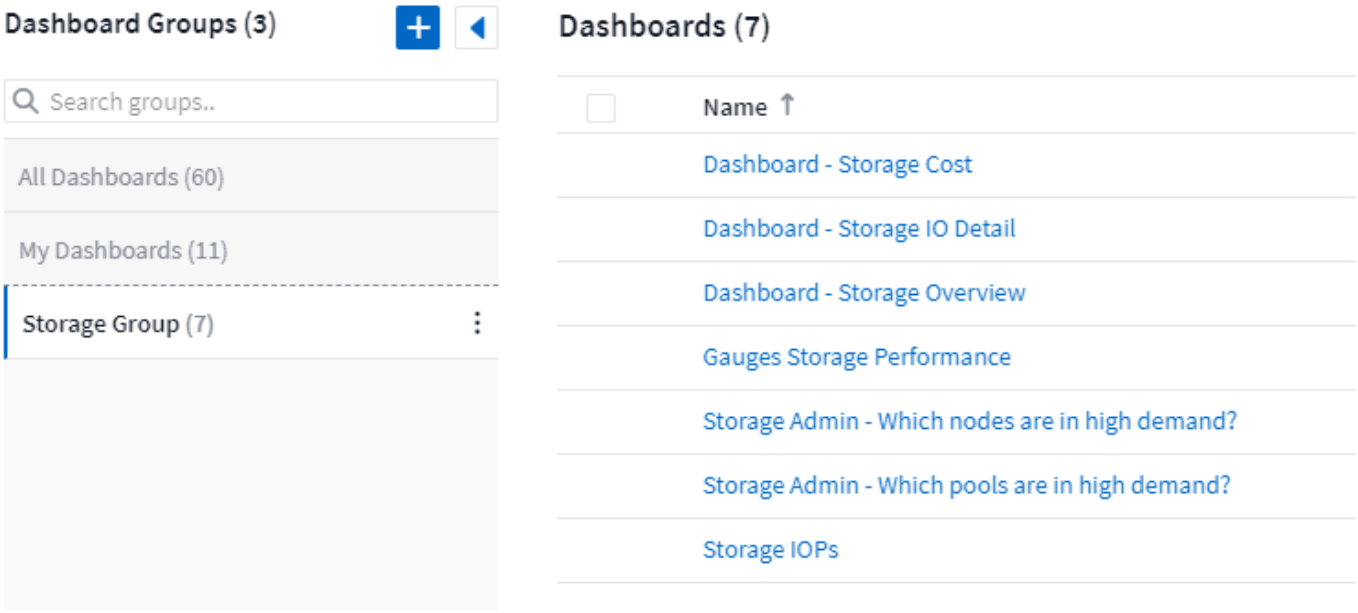
- Um den TV-Modus zu aktivieren, klicken Sie auf die Schaltfläche TV-Modus.
- Um den TV-Modus zu deaktivieren, klicken Sie oben links auf dem Bildschirm auf die Schaltfläche **Beenden**.

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



Dashboard-Gruppen

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



Standardmäßig werden zwei Gruppen angezeigt:

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

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

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

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

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

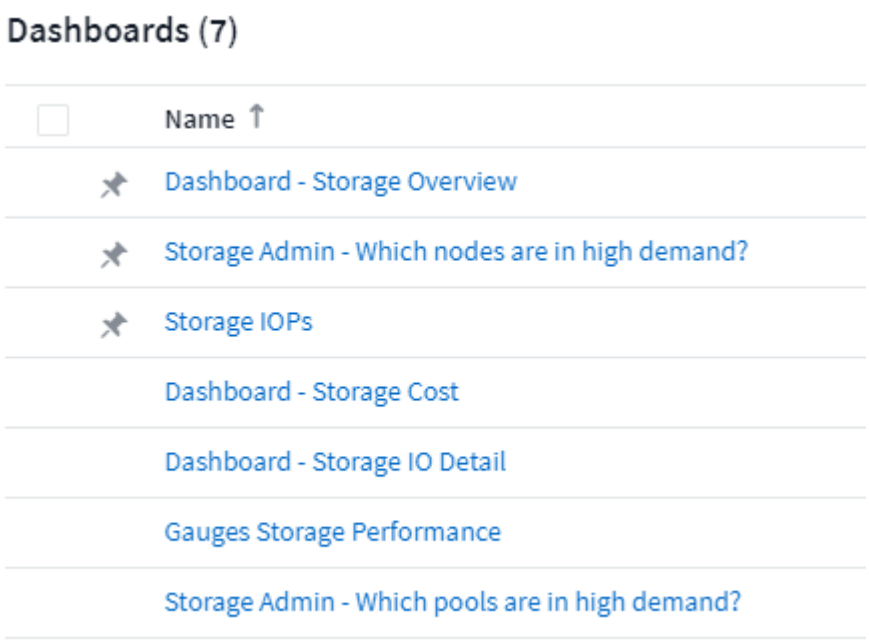
Entfernen Sie Dashboards auf dieselbe Weise aus der aktuellen Gruppe, indem Sie *aus Gruppe* entfernen auswählen. Sie können Dashboards nicht aus der Gruppe *Alle Dashboards* oder *Meine Dashboards* entfernen.

Durch 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 er von allen Gruppen entfernt, zu denen er gehört hat und für keinen Benutzer mehr verfügbar ist.

PIN für Ihre Lieblings-Dashboards

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

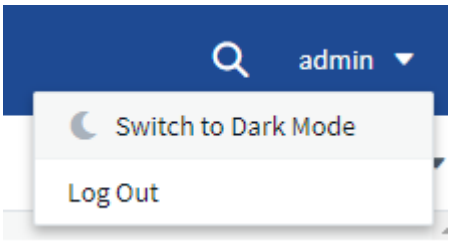
Dashboard PIN/Unpin ist eine individuelle Benutzerpräferenz und unabhängig von der Gruppe (oder Gruppen), zu der das Dashboard gehört.



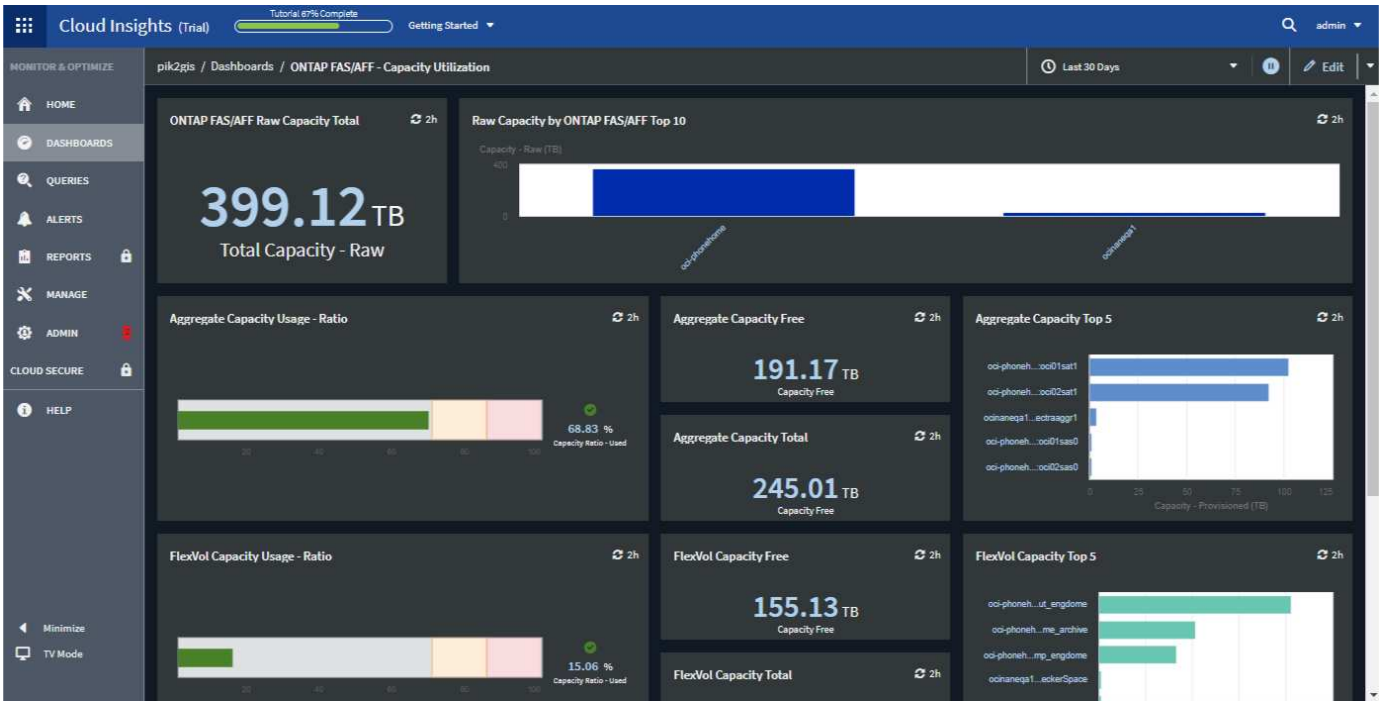
Dunkles Thema

Sie können Daten-Infrastruktur-Insights entweder mit einem hellen Thema (der Standard) anzeigen, das die meisten Bildschirme mit einem hellen Hintergrund mit dunklem Text anzeigt, oder mit einem dunklen Thema, das die meisten Bildschirme mit einem dunklen Hintergrund mit hellem Text anzeigt.

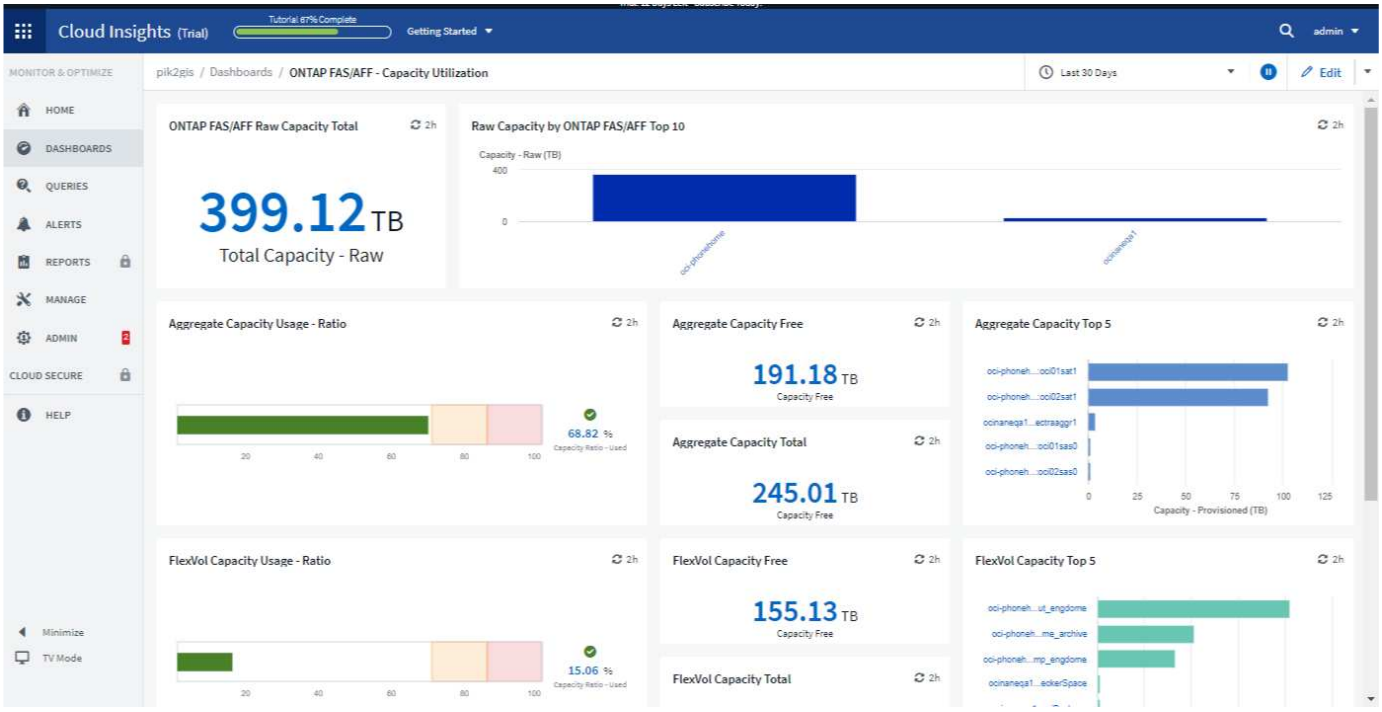
Um zwischen hellen und dunklen Themen zu wechseln, klicken Sie auf die Schaltfläche Benutzername in der oberen rechten Ecke des Bildschirms und wählen Sie das gewünschte Thema.



Dashboard-Ansicht „Dark Theme“:



Dashboard-Ansicht „Light Theme“:



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

Zeilendiagramm-Interpolation

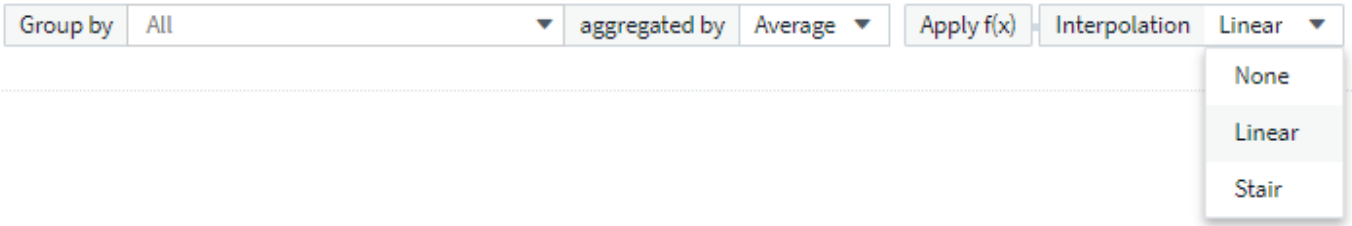
Unterschiedliche Datensammler stellen ihre Daten häufig in unterschiedlichen Intervallen in Frage. Zum Beispiel kann Datensammler A alle 15 Minuten abfragen, während Datensammler B alle fünf Minuten abfragt. Wenn ein Liniendiagramm-Widget (auch Spline-, Bereich- und gestapelte Flächendiagramme) diese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

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

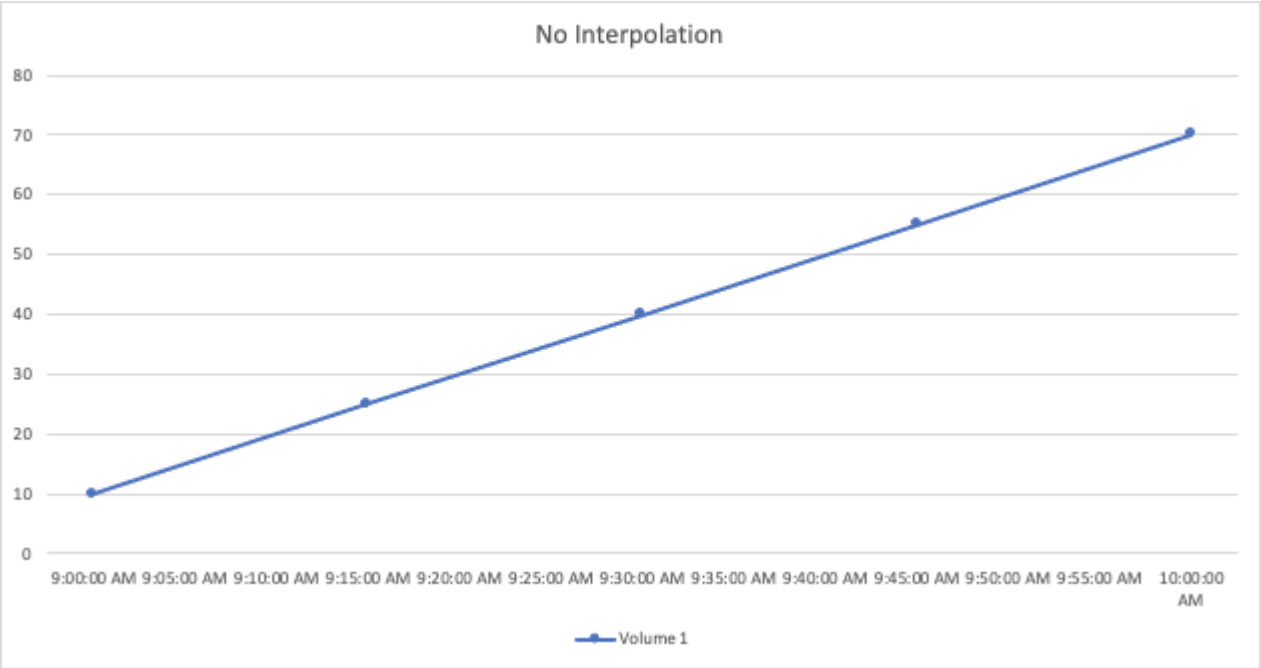
Um dies zu verringern, interpoliert Data Infrastructure Insights Daten bei der Aggregation und nutzt die umliegenden Datenpunkte, um eine „Best Guess“ an Daten zu nehmen, bis die Datensammler wieder abfragen. Sie können die Objektdaten jedes Datensammlers immer einzeln anzeigen, indem Sie die Gruppierung des Widgets anpassen.

Interpolationsmethoden

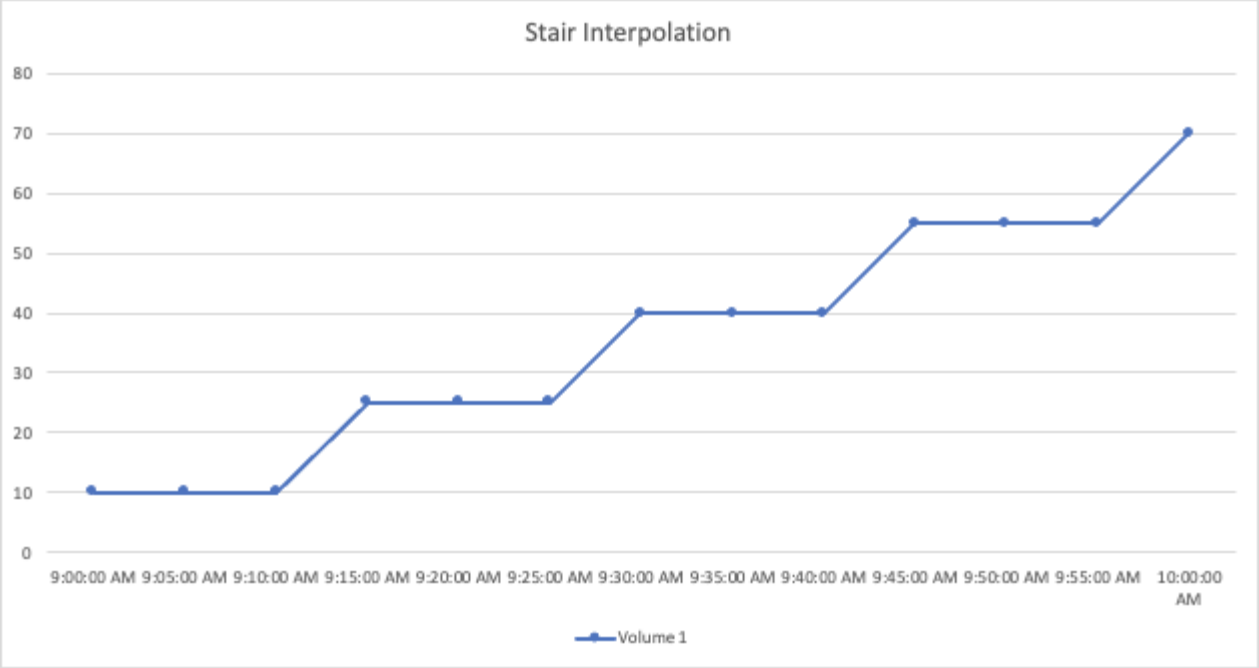
Wenn Sie ein Liniendiagramm (oder ein Spline-, Bereich- oder Stapeldiagramm) erstellen oder ändern, können Sie die Interpolationsmethode auf einen von drei Typen festlegen. Wählen Sie im Abschnitt „Gruppieren nach“ die gewünschte Interpolation aus.



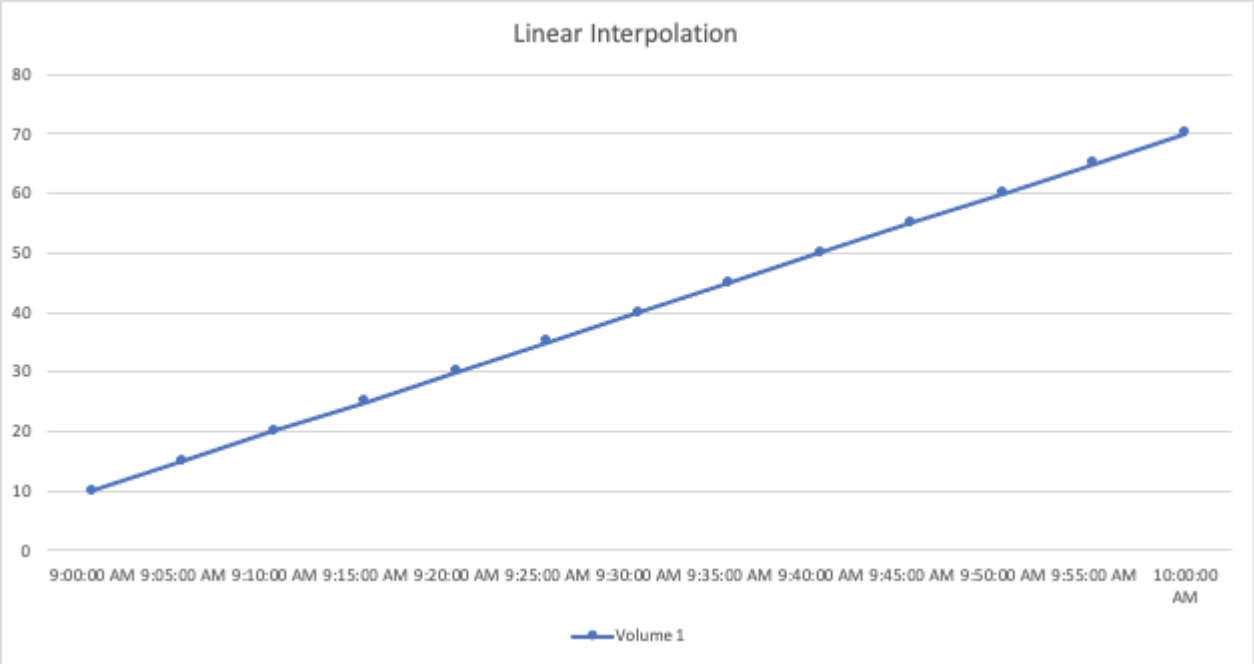
- **Keine**: Nichts tun, d.h. keine Punkte dazwischen erzeugen.



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



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



Beispiele Für Dashboards

Dashboard-Beispiel: Virtual Machine Performance

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

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

Über diese Aufgabe

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

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

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

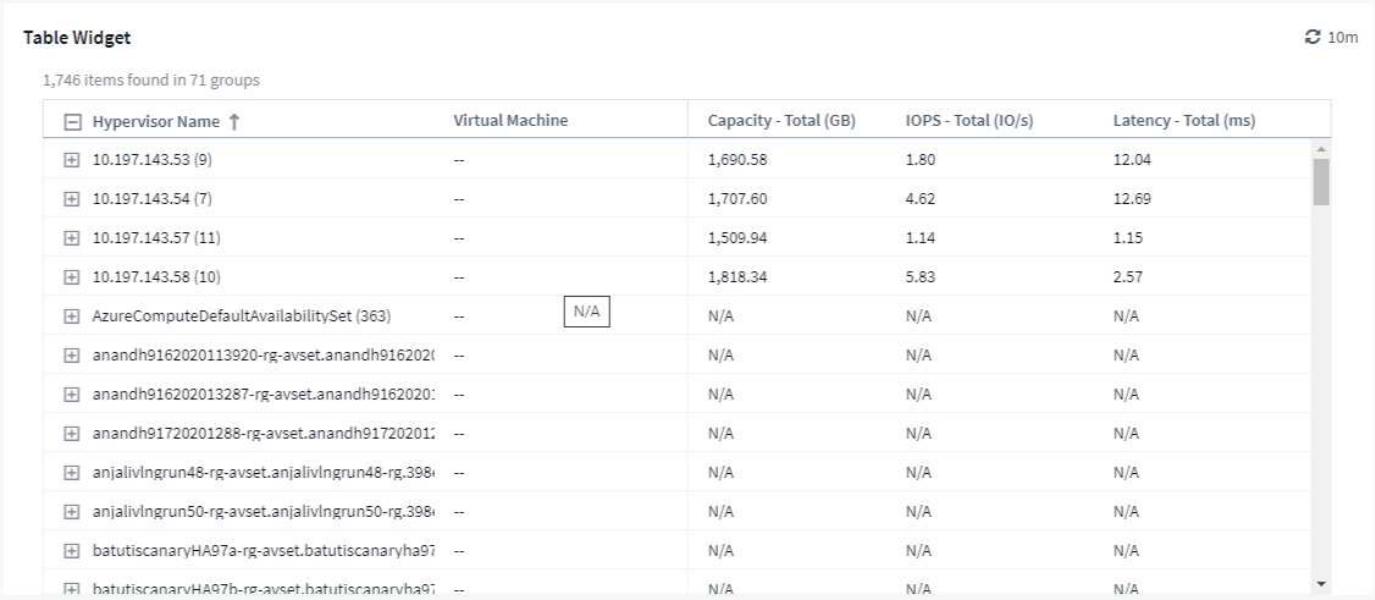
Schritte

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

   Die Seite **Neues Dashboard** wird geöffnet.

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

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



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

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

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

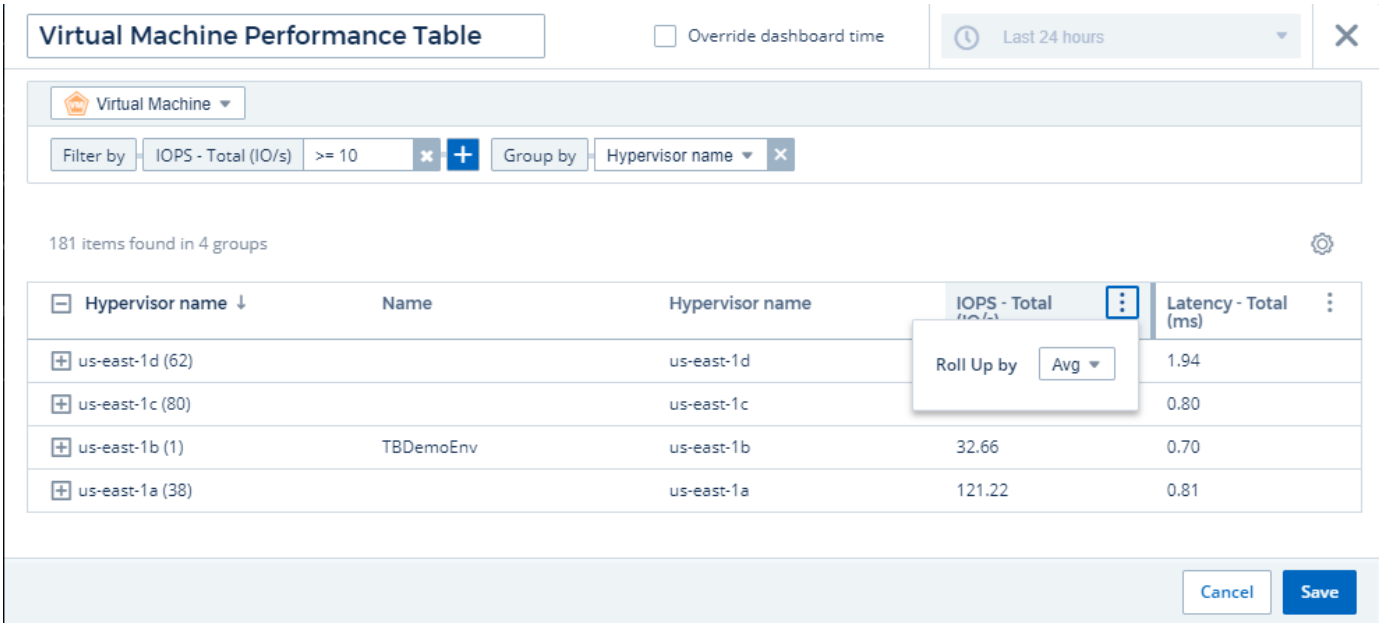
   Diese Spalten werden nun in der Tabelle angezeigt. Sie können die Tabelle nach einer dieser Spalten sortieren. Beachten Sie, dass die Spalten in der Reihenfolge angezeigt werden, in der sie dem Widget hinzugefügt wurden.

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

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

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

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



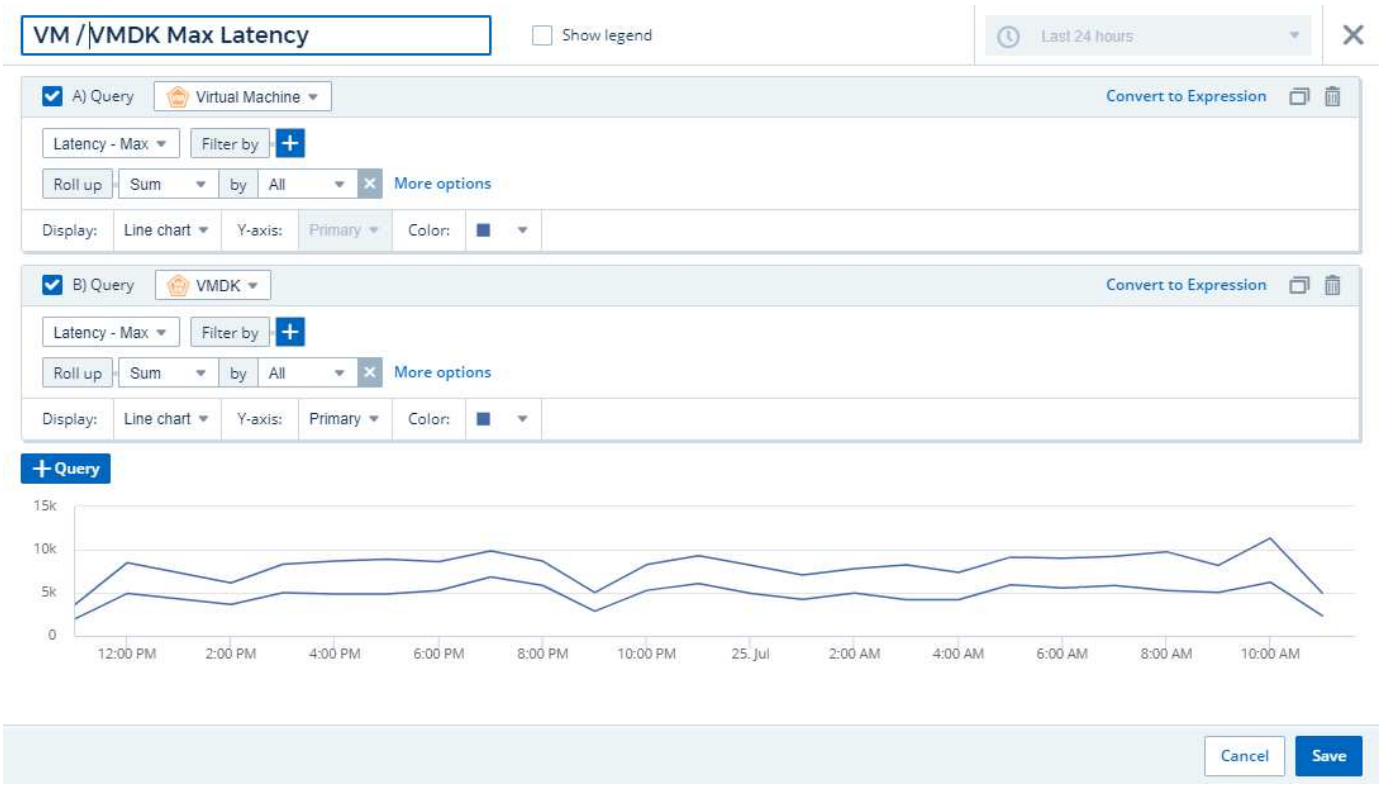
1. Wenn Sie das TabellenWidget auf Ihre Zufriedenheit angepasst haben, klicken Sie auf die Schaltfläche **[Save]**.

   Das TabellenWidget wird im Dashboard gespeichert.

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

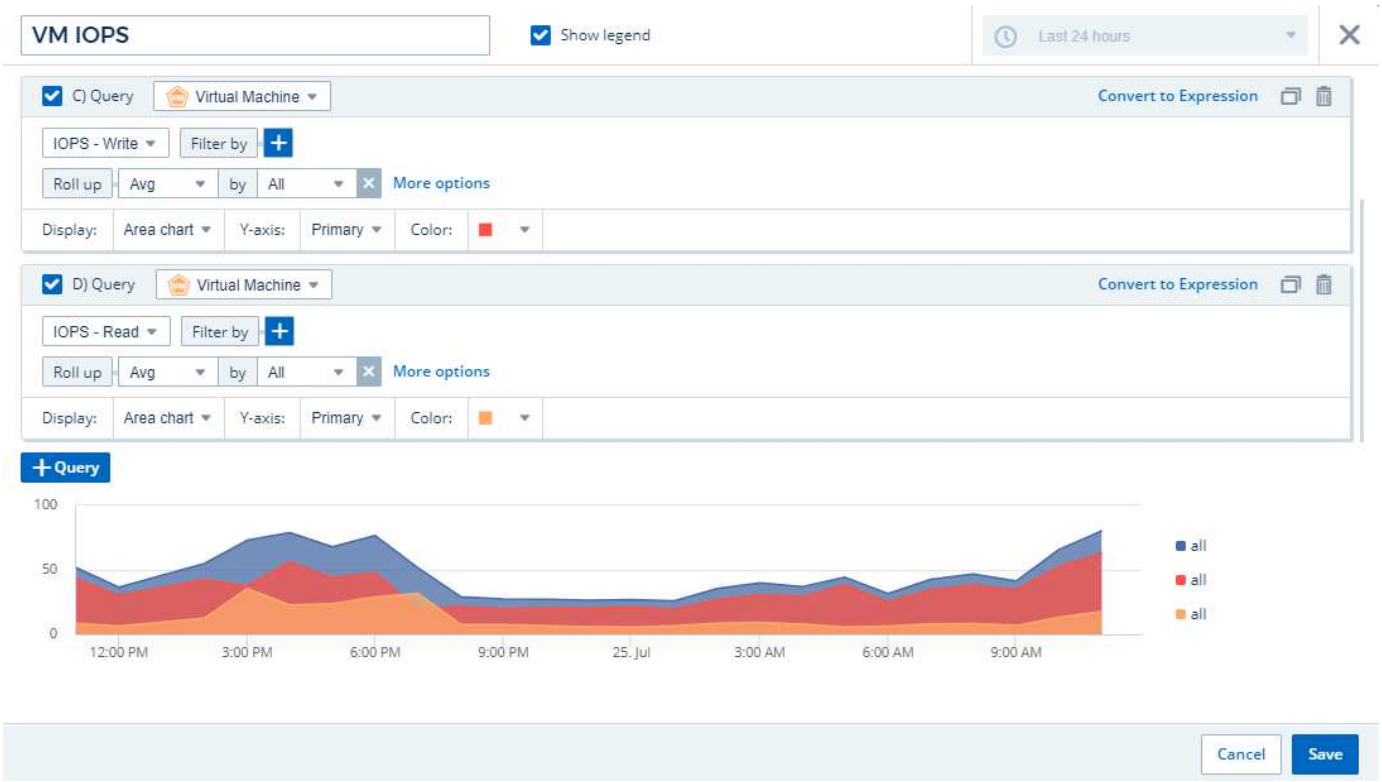
Als nächstes fügen wir einige Diagramme hinzu, um unsere VM-Performance anzuzeigen. Erstellen wir ein Liniendiagramm, in dem die VM-Latenz mit VMDK-Latenz verglichen wird.

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



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

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



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

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

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

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

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

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

Ihr letztes VM Performance Dashboard sieht so aus:

Best Practices für Dashboards und Widgets

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

Suchen der richtigen Metrik

Data Infrastructure Insights erfasst Zähler und Kennzahlen mithilfe von Namen, die sich manchmal von Datensammler zu Datensammler unterscheiden.

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

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

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

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

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

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

Ermitteln der richtigen Ressourcen

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

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

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

Dies ist keine umfassende Liste.

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

Scatter-Plot Beispiel: Ihre Achse kennen

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

Über diese Aufgabe

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

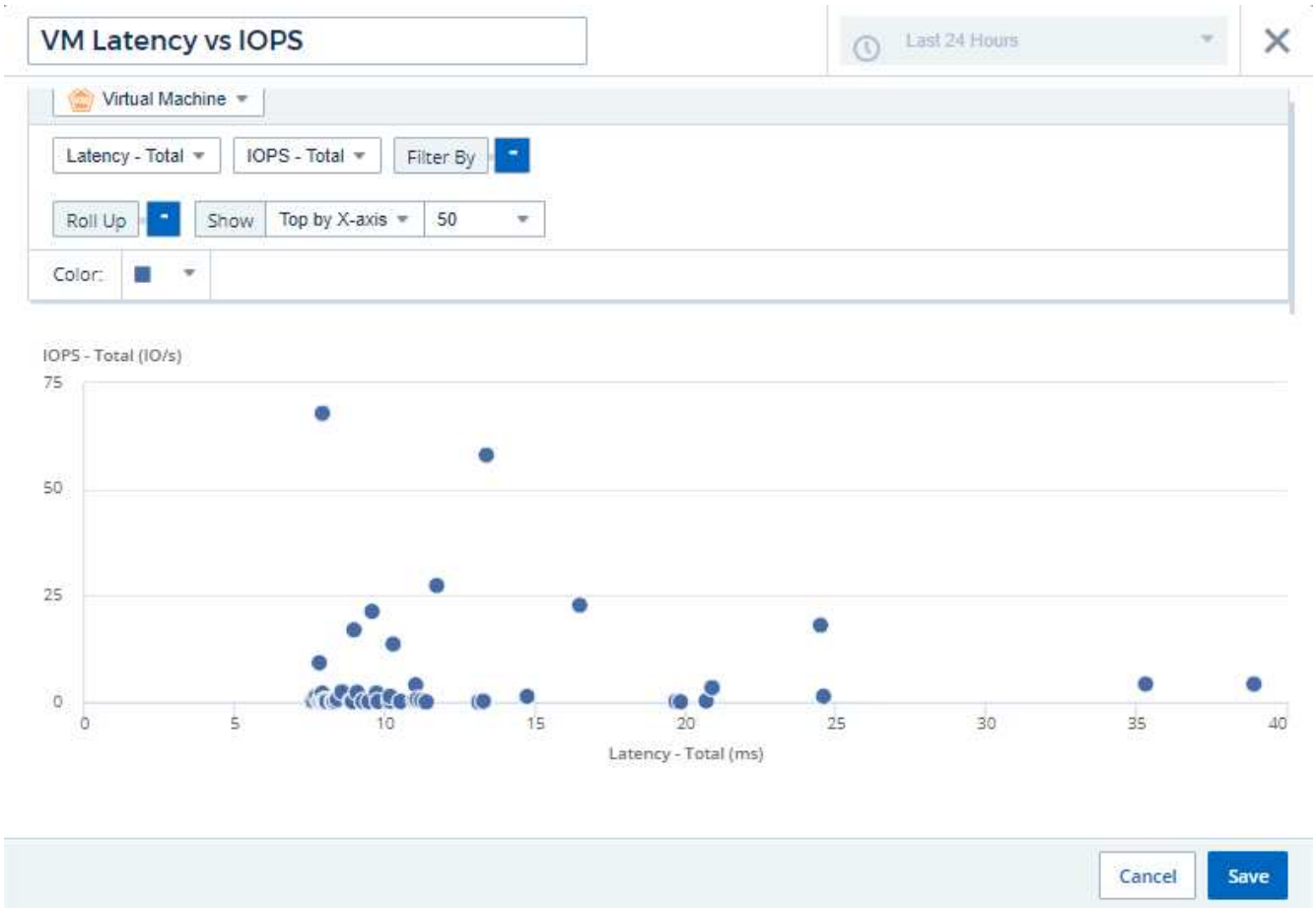
Schritte

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

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

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

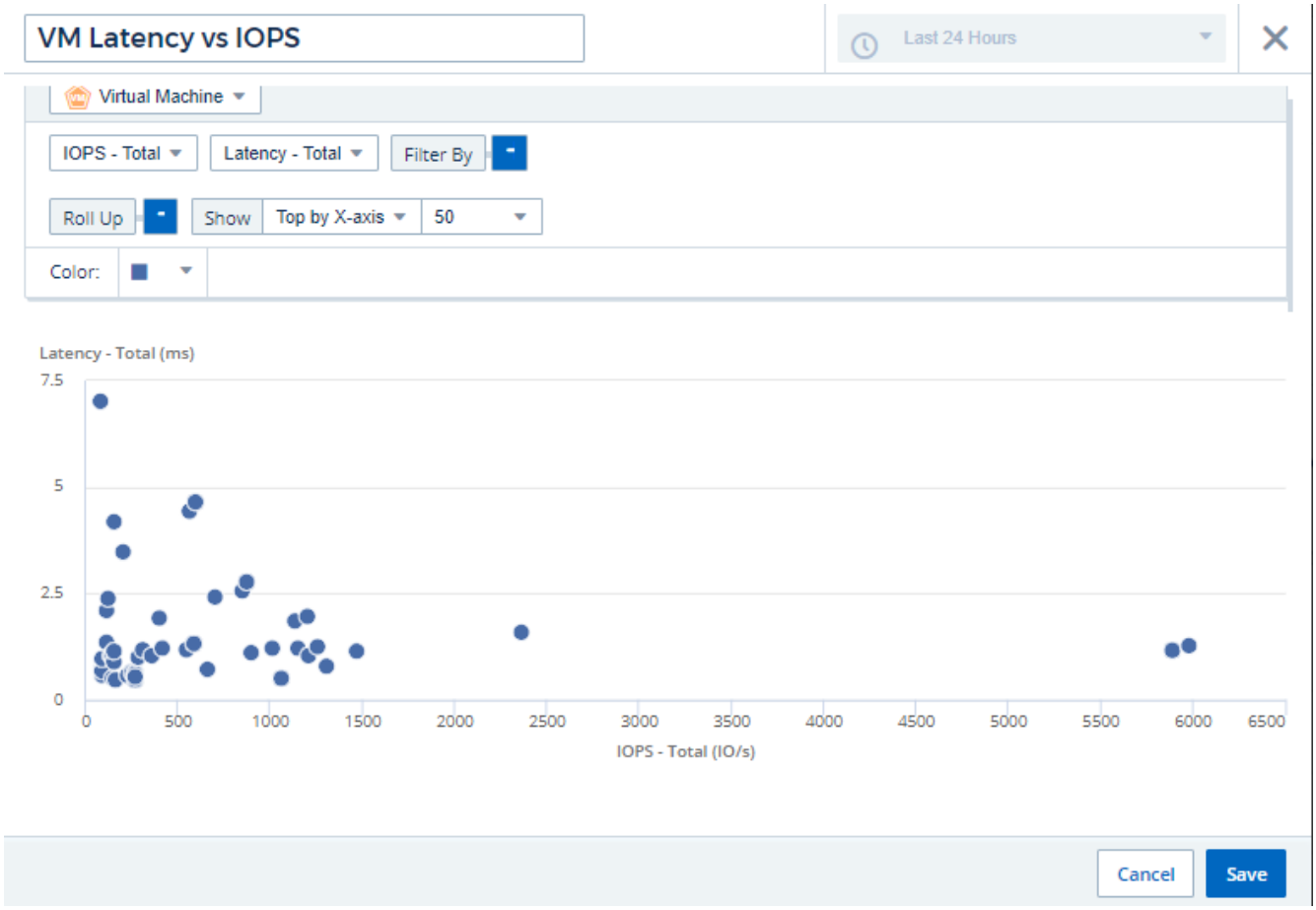
   IOPS - Total wird entlang der Y-Achse im Diagramm dargestellt. VMs mit höherer Latenz werden rechts im Diagramm angezeigt. Es werden nur die 100 VMs mit der höchsten Latenz angezeigt, da die Einstellung **Top by X-Axis** aktuell ist.



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

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

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



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

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

Arbeiten mit Abfragen

In Abfragen verwendete Ressourcen

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

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

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

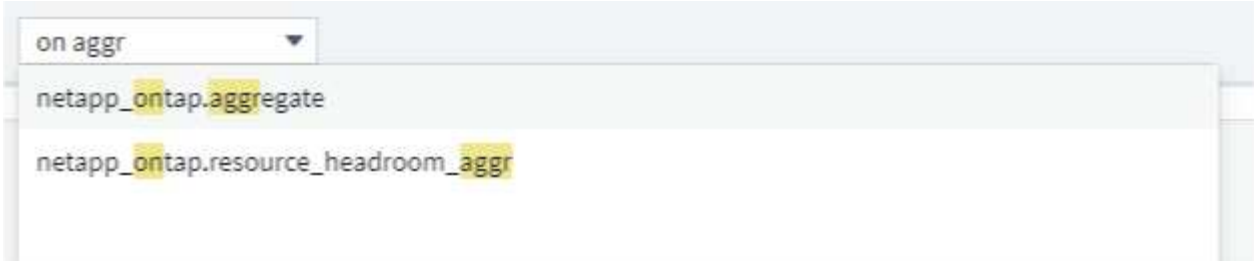
Lagerbestände

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

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

Integrationsmetriken

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



Abfragen Werden Erstellt

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

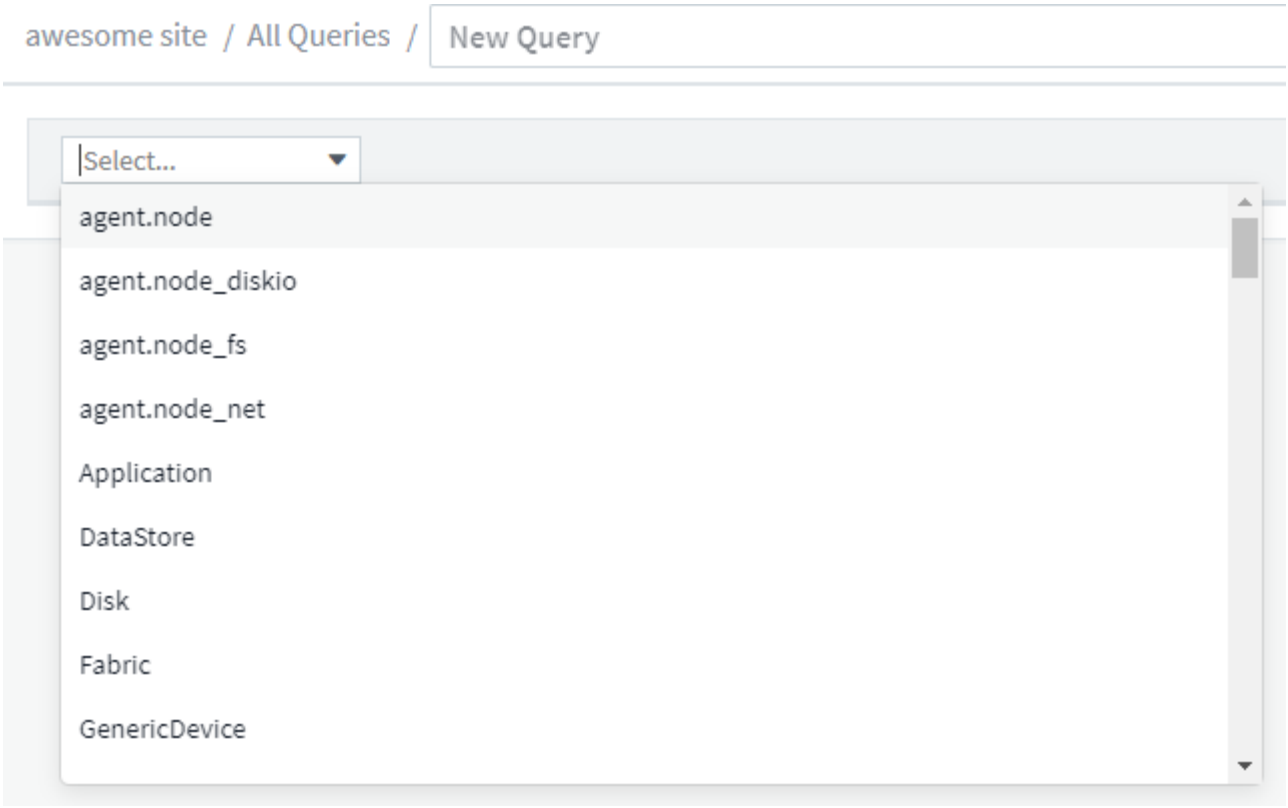
Sie können z. B. eine Abfrage für *Volumes* erstellen, einen Filter hinzufügen, um bestimmte *Storage* zu den ausgewählten Volumes zu finden, einen weiteren Filter hinzufügen, um eine bestimmte *Annotation* zu finden, z. B. „Tier 1“ auf den ausgewählten Speichern, Und schließlich noch einen Filter hinzufügen,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

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

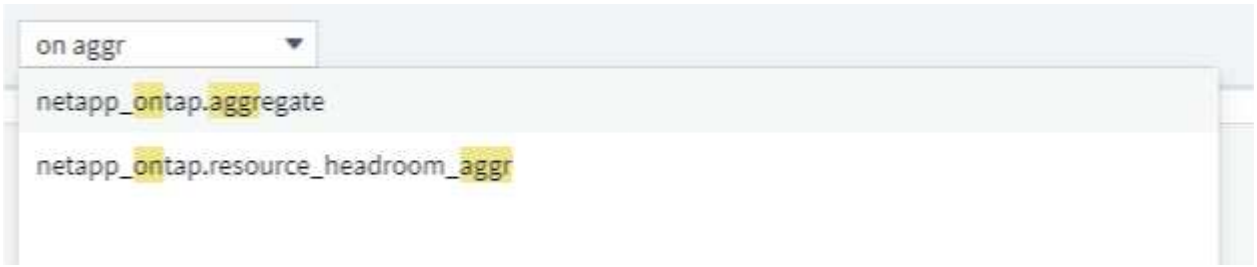
Das Erstellen einer Abfrage ist sehr einfach:

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

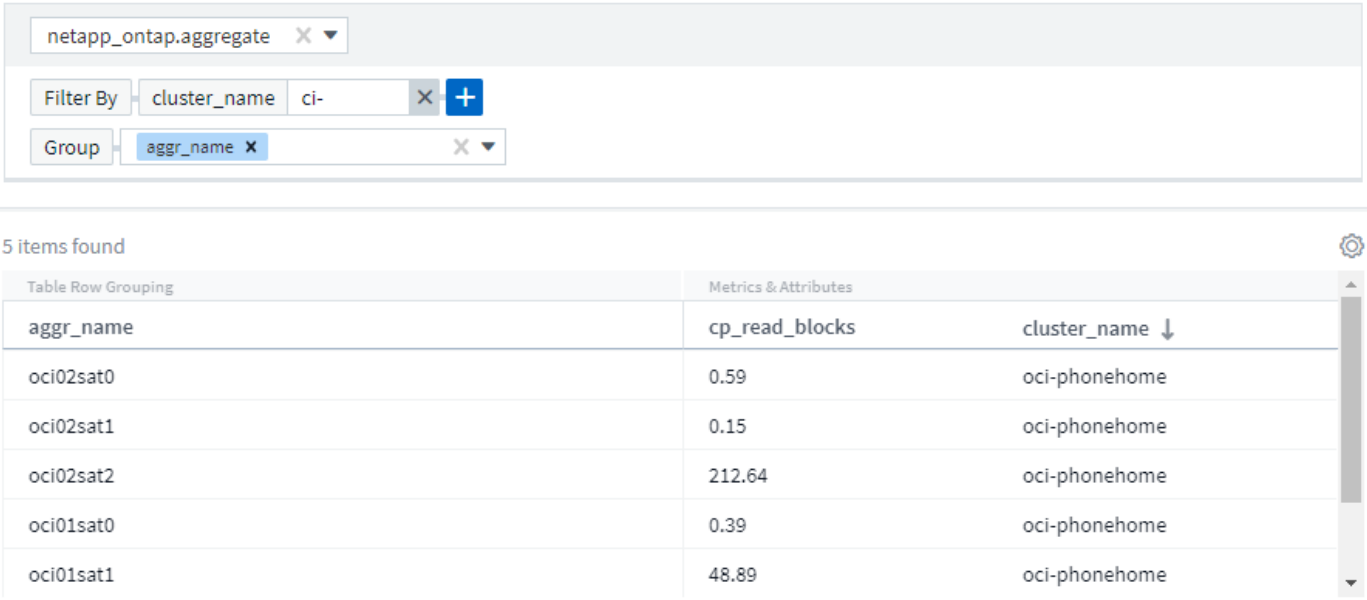
Bildlaufliste:



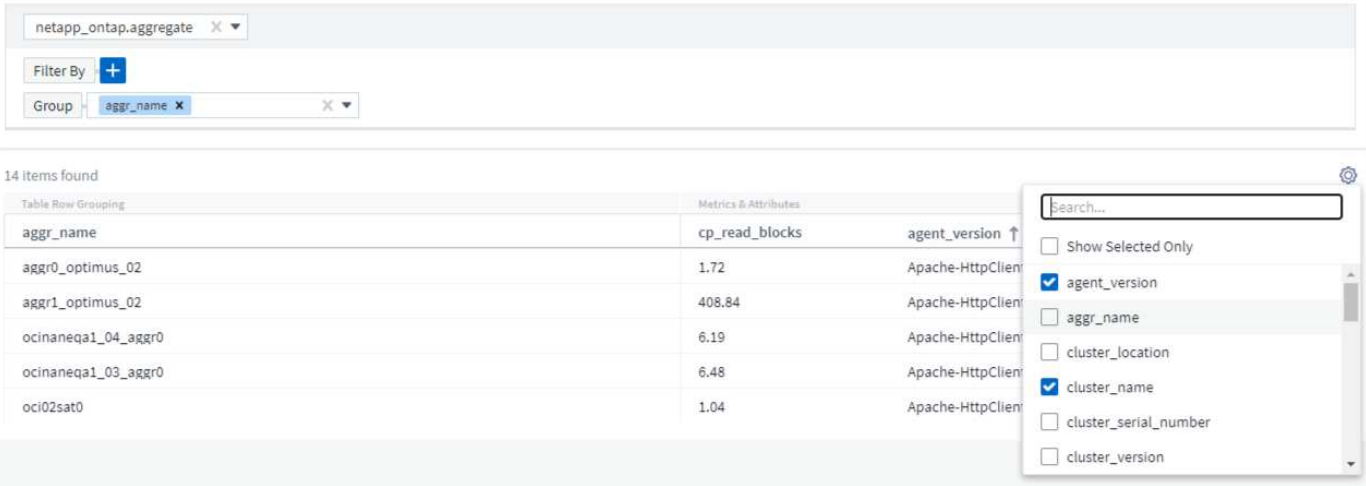
Typ-zu-Suche:



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



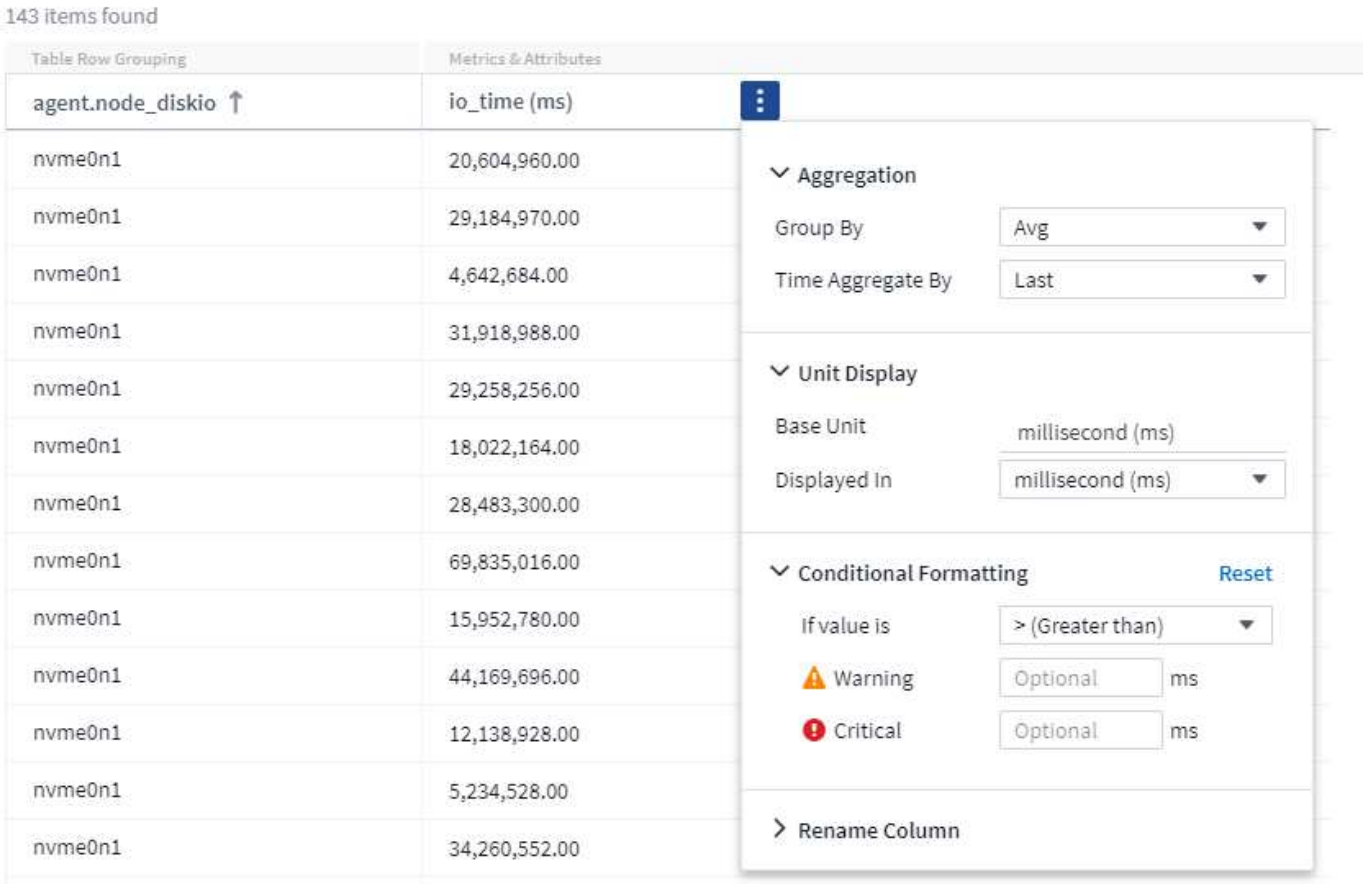
Die Liste der Abfrageergebnisse zeigt je nach dem gesuchten Objekttyp eine Reihe von Standardspalten an. Um die Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle. Die verfügbaren Spalten variieren je nach Asset/metrischem Typ.



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

Aggregation und Einheiten

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



Einheiten

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

Aggregation

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

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

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

Bedingte Formatierung

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

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

Spalte Umbenennen

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

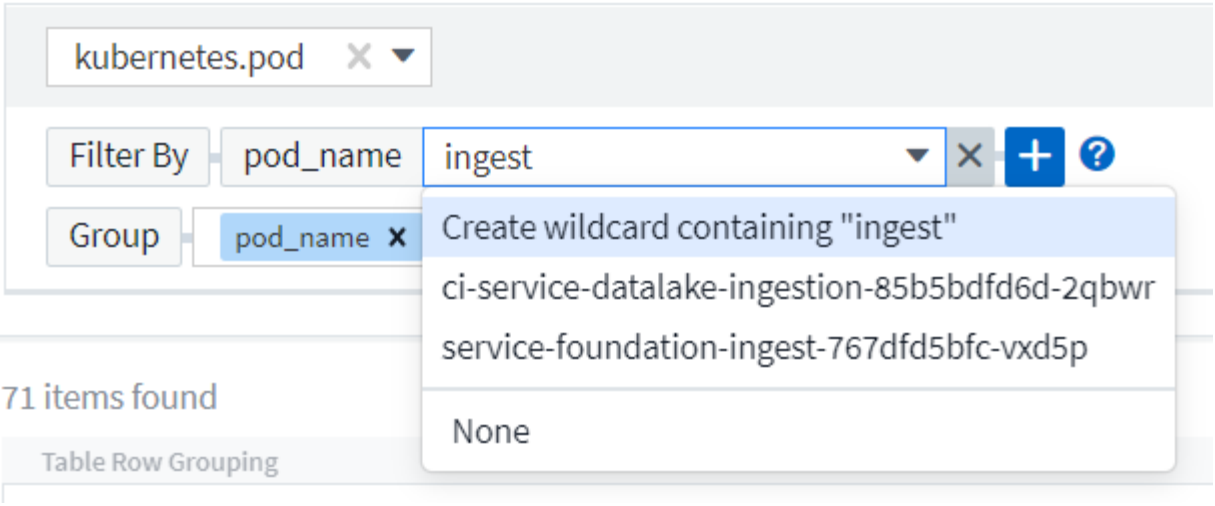
Speichern

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

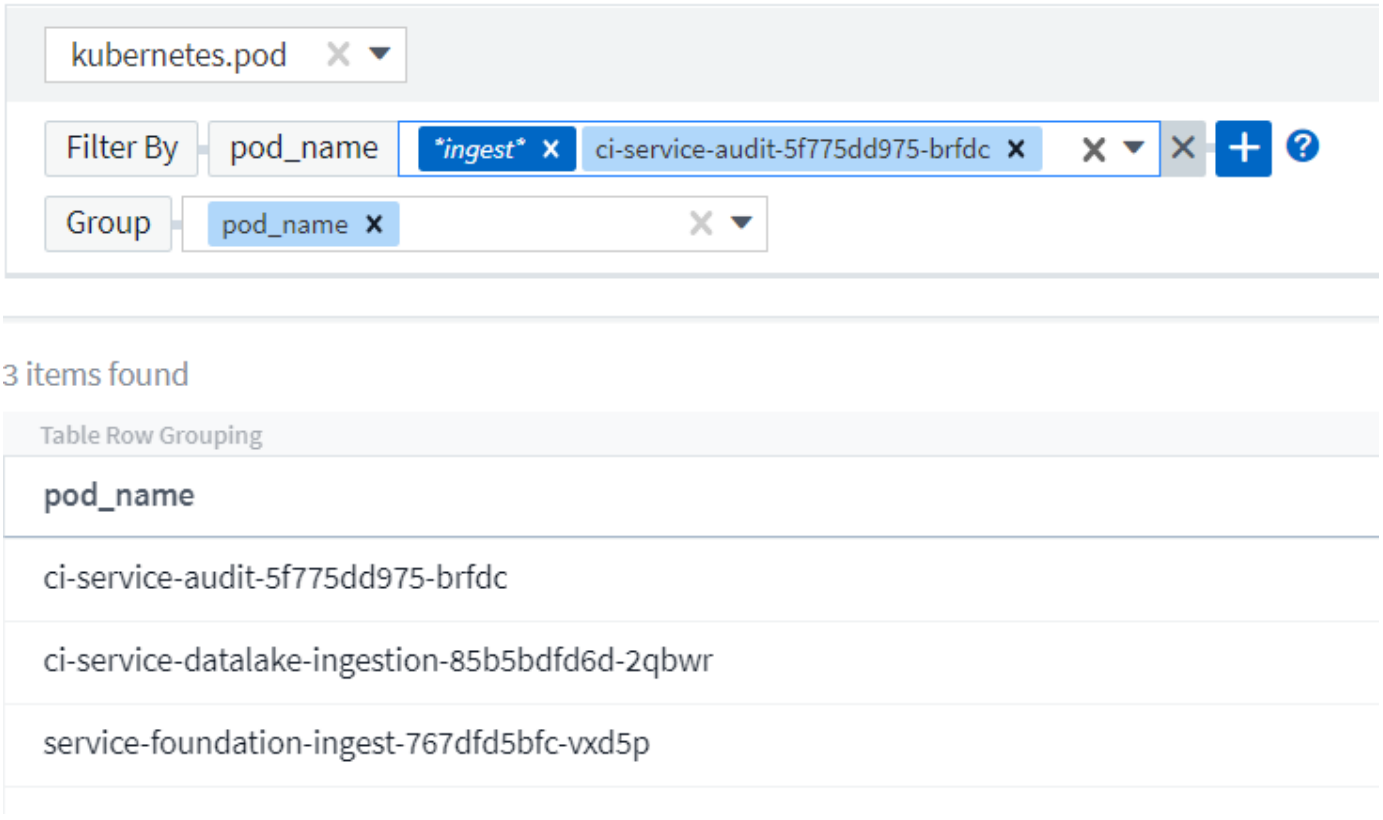
Mehr zum Filtern

Platzhalter und Ausdrücke

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



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



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

Verfeinern Von Filtern

Sie können den Filter wie folgt verfeinern:

Filtern	Das macht es	Beispiel	Ergebnis

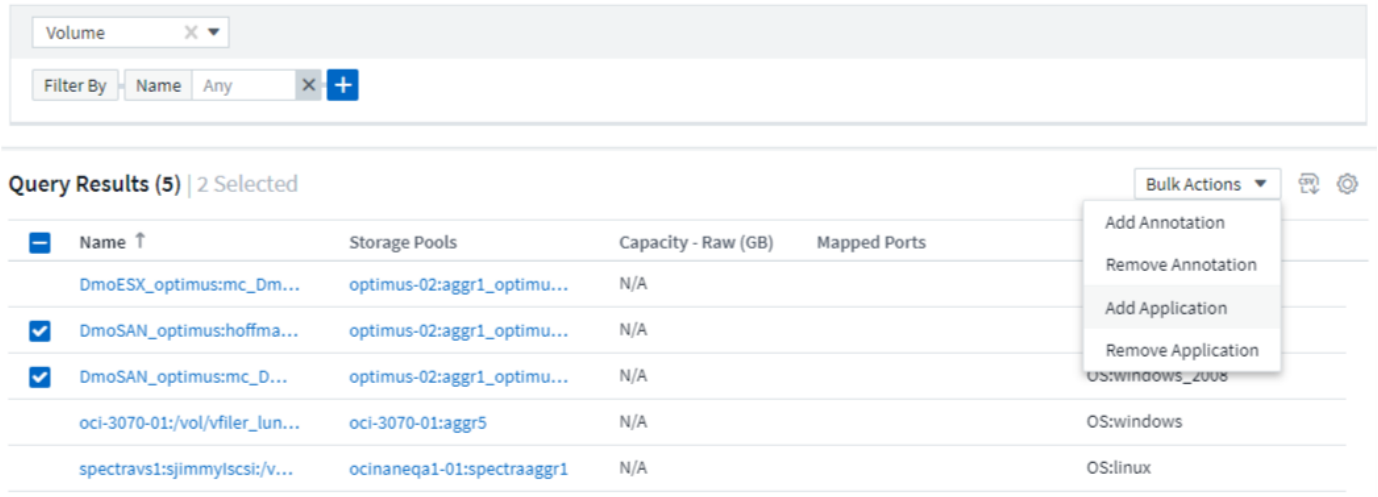
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	vol.	Gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „RHEL“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	Gibt BOS-PRD zurück***12_ -S12, BOS-PRD23_***-S12 und so weiter
ODER	Ermöglicht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

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

Was mache ich jetzt, wenn ich Abfrageergebnisse habe?

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

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



Abfrage zu Anmerkungsregeln erforderlich

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

Anzeigen von Abfragen

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

Schritte

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

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

Abfrageergebnisse werden in eine CSV-Datei exportiert

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

Schritte

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

   Die Seite Abfragen wird angezeigt.

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

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

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

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

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

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

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

   Ihre Objekte sollten in Excel im richtigen Format angezeigt werden.

Eine Abfrage ändern oder löschen

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

Ändern einer Abfrage

Schritte

1. Klicken Sie auf **Explore** und wählen Sie **All Metric Queries**.

   Die Seite Abfragen wird angezeigt.

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

Löschen einer Abfrage

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

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

Tabellenwerte werden kopiert

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

Über diese Aufgabe

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

Schritte

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

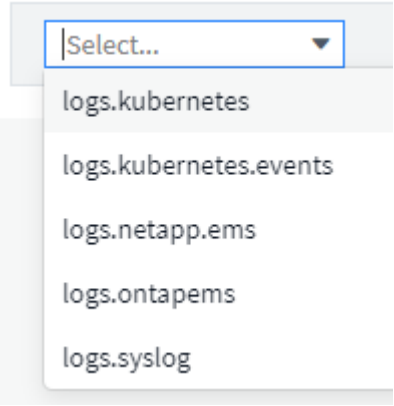
   Beachten Sie, dass nur Werte, die Verknüpfungen zu Assets sind, mit dieser Methode kopiert werden können. Nur Felder, die einzelne Werte enthalten (d. h. nicht-Listen), haben das Kopiensymbol.

Log-Explorer

Der Data Infrastructure Insights Log Explorer ist ein leistungsstarkes Tool zum Abfragen von Systemprotokollen. Zusätzlich zur Unterstützung bei Ermittlungen können Sie auch eine Protokollabfrage in einem Monitor speichern, um Warnmeldungen zu geben, wenn diese bestimmten Protokollauslöser aktiviert sind.

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

Wählen Sie ein verfügbares Protokoll aus der Liste aus.

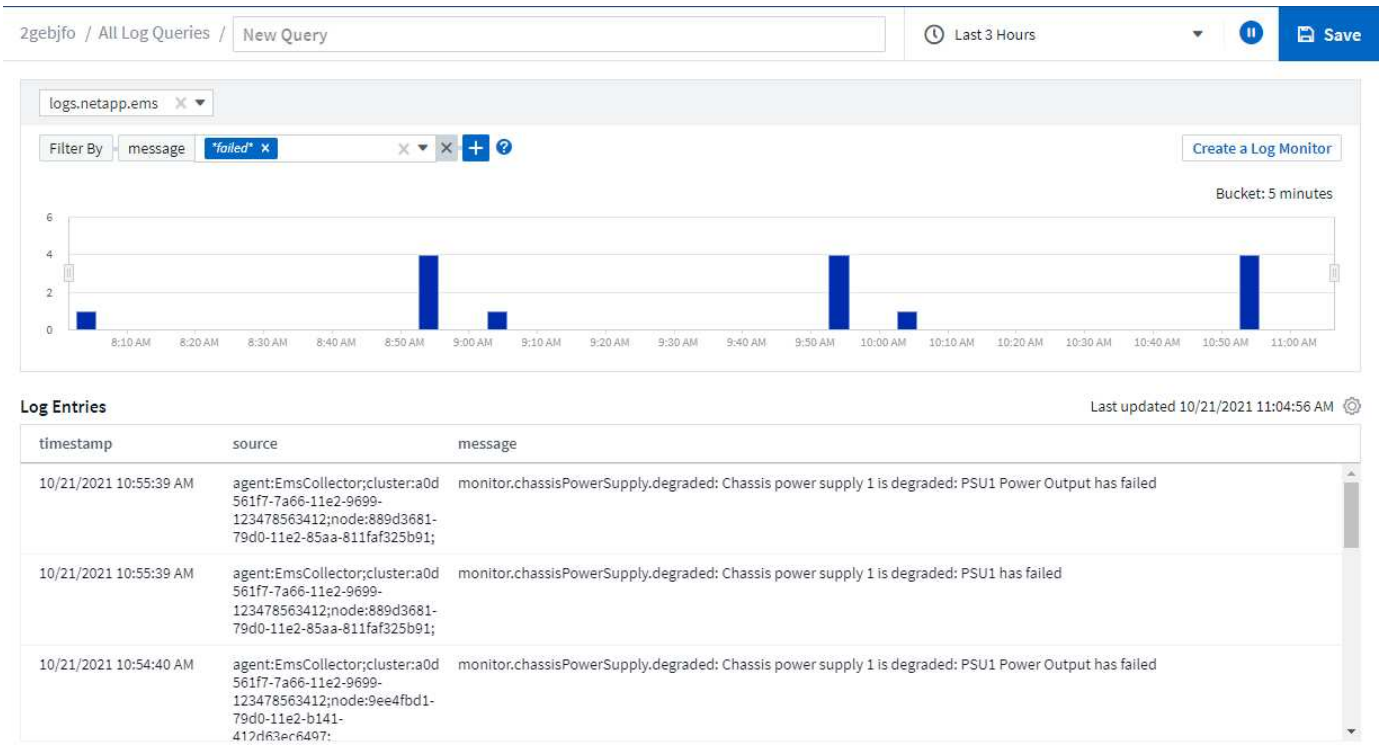


Die für das Abfragen verfügbaren Protokolltypen können je nach Umgebung variieren. Im Laufe der Zeit können weitere Protokolltypen hinzugefügt werden.

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

Sie können den gewünschten Text in das Filterfeld eingeben. Data Infrastructure Insights fordert Sie auf, bei der Eingabe eine Platzhaltersuche zu erstellen, die den String enthält.

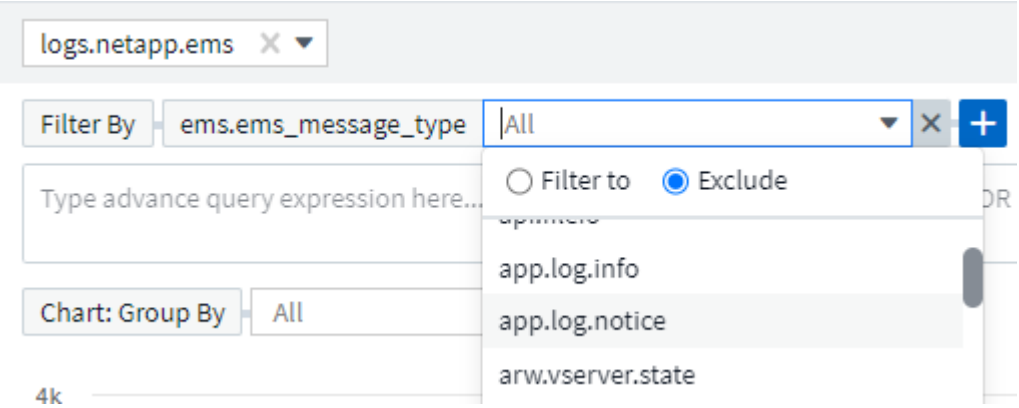
Die Ergebnisse werden in einem Diagramm angezeigt, in dem die Anzahl der Protokollinstanzen in jedem angezeigten Zeitraum angezeigt wird. Unter der Grafik sehen Sie die Protokolleinträge, die sich selbst bewegen. Das Diagramm und die Einträge werden automatisch auf der Grundlage des ausgewählten Zeitbereichs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



Filtern

Ein-/Ausschließen

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



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

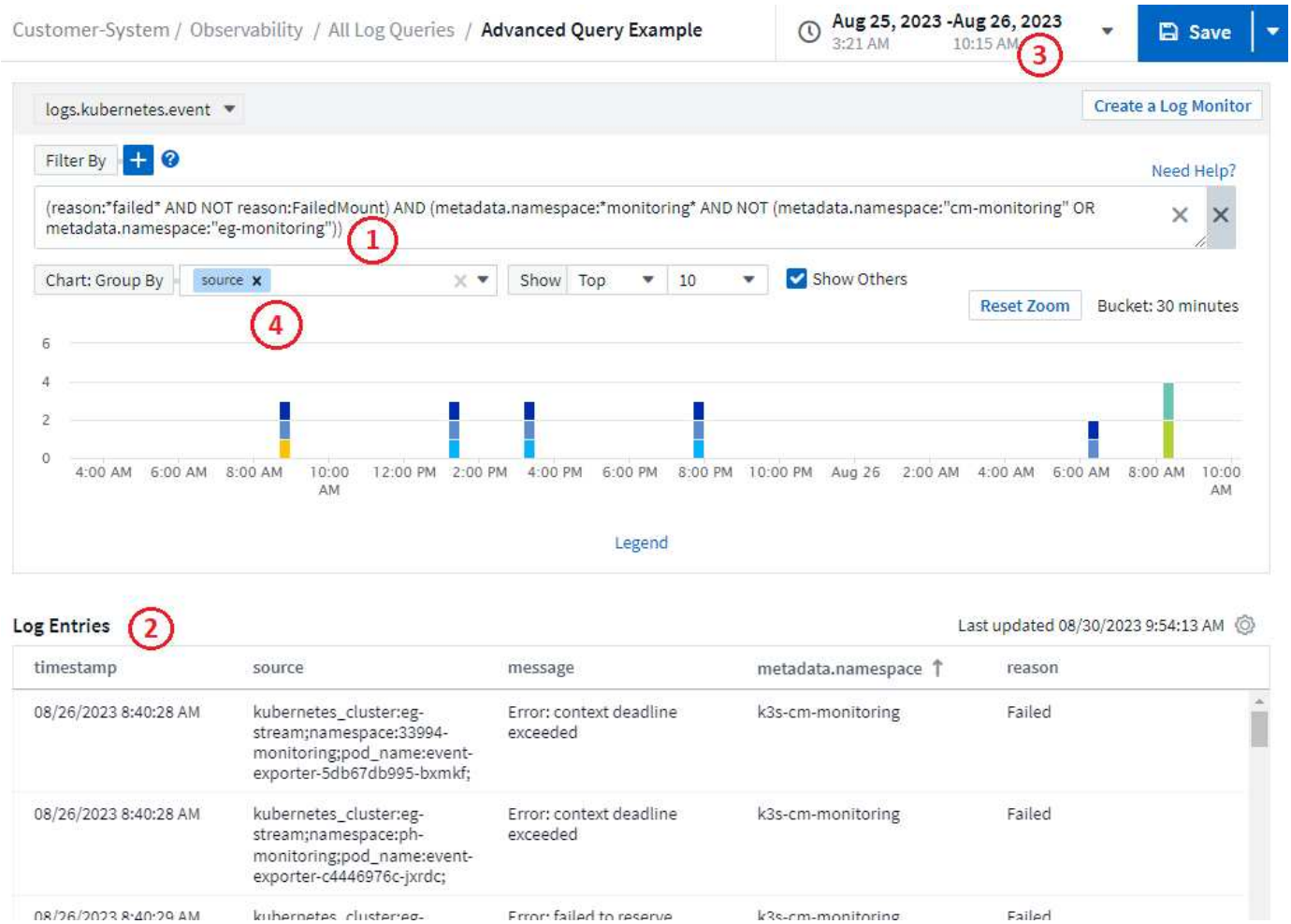
Sie können jederzeit auf *Protokollmonitor erstellen* klicken, um einen neuen Monitor basierend auf dem aktuellen Filter zu erstellen.

Erweiterte Filterung

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

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

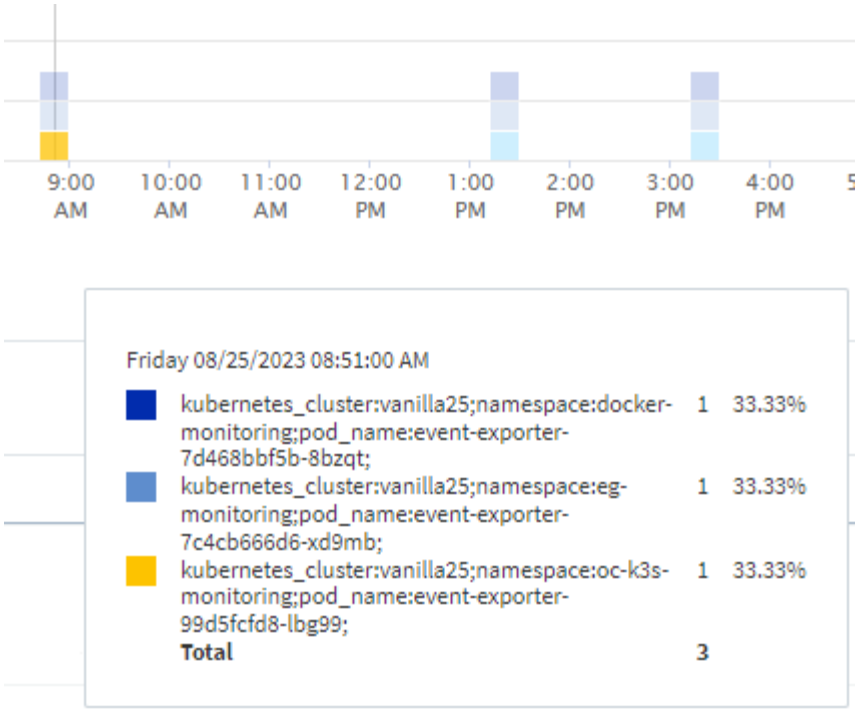
Sehen Sie sich dieses Bildschirmbild an, das gefilterte Ergebnisse für eine erweiterte Abfrage des *logs.kubernetes.Event*-Protokolls zeigt. Auf dieser Seite ist viel los, was unter dem Bild erklärt wird:



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

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

2. Die Ergebnisse des aktuellen Filters, einschließlich aller „Filtern nach“-Werte UND des erweiterten Abfragefilters, werden in der Ergebnisliste angezeigt. Die Liste kann nach allen angezeigten Spalten sortiert werden. Um weitere Spalten anzuzeigen, wählen Sie das Zahnrad-Symbol.
3. Das Diagramm wurde vergrößert, um nur Protokollergebnisse anzuzeigen, die innerhalb eines bestimmten Zeitrahmens aufgetreten sind. Der hier angezeigte Zeitbereich entspricht dem aktuellen Zoomfaktor. Wählen Sie die Schaltfläche *Zoom zurücksetzen*, um den Zoomfaktor auf den aktuellen Dateninfrastrukturzeitbereich zurückzusetzen.
4. Die Diagrammergebnisse wurden nach dem Feld *source* gruppiert. Das Diagramm zeigt die Ergebnisse in jeder Spalte, die in Farben gruppiert sind. Wenn Sie den Mauszeiger über eine Spalte im Diagramm bewegen, werden einige Details zu den spezifischen Einträgen angezeigt.



Verfeinern Von Filtern

Sie können den Filter wie folgt verfeinern:

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

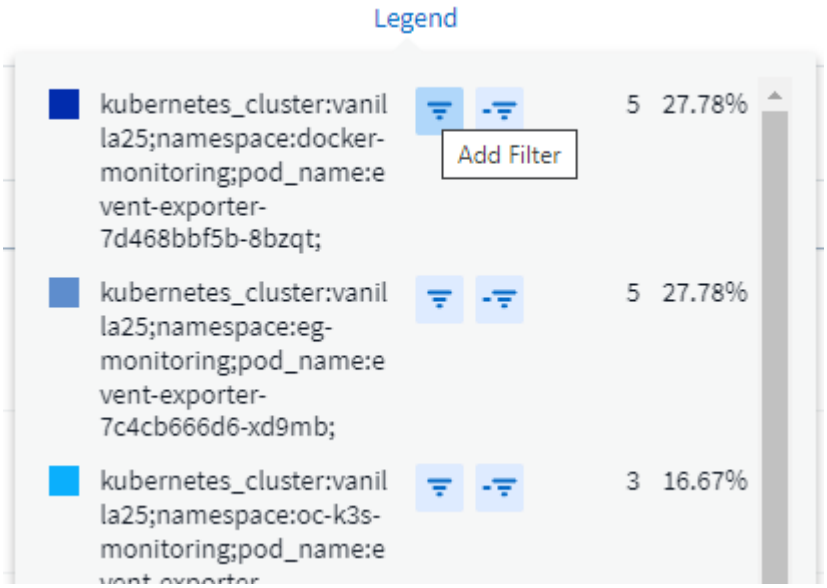
Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse,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

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

Die Diagrammlegende

Die *Legend* unterhalb des Diagramms hat auch einige Überraschungen. Für jedes in der Legende angezeigte Ergebnis (basierend auf dem aktuellen Filter) haben Sie die Möglichkeit, nur Ergebnisse für diese Zeile anzuzeigen (Filter hinzufügen) oder Ergebnisse anzuzeigen, die NICHT für diese Zeile vorhanden sind (Filter

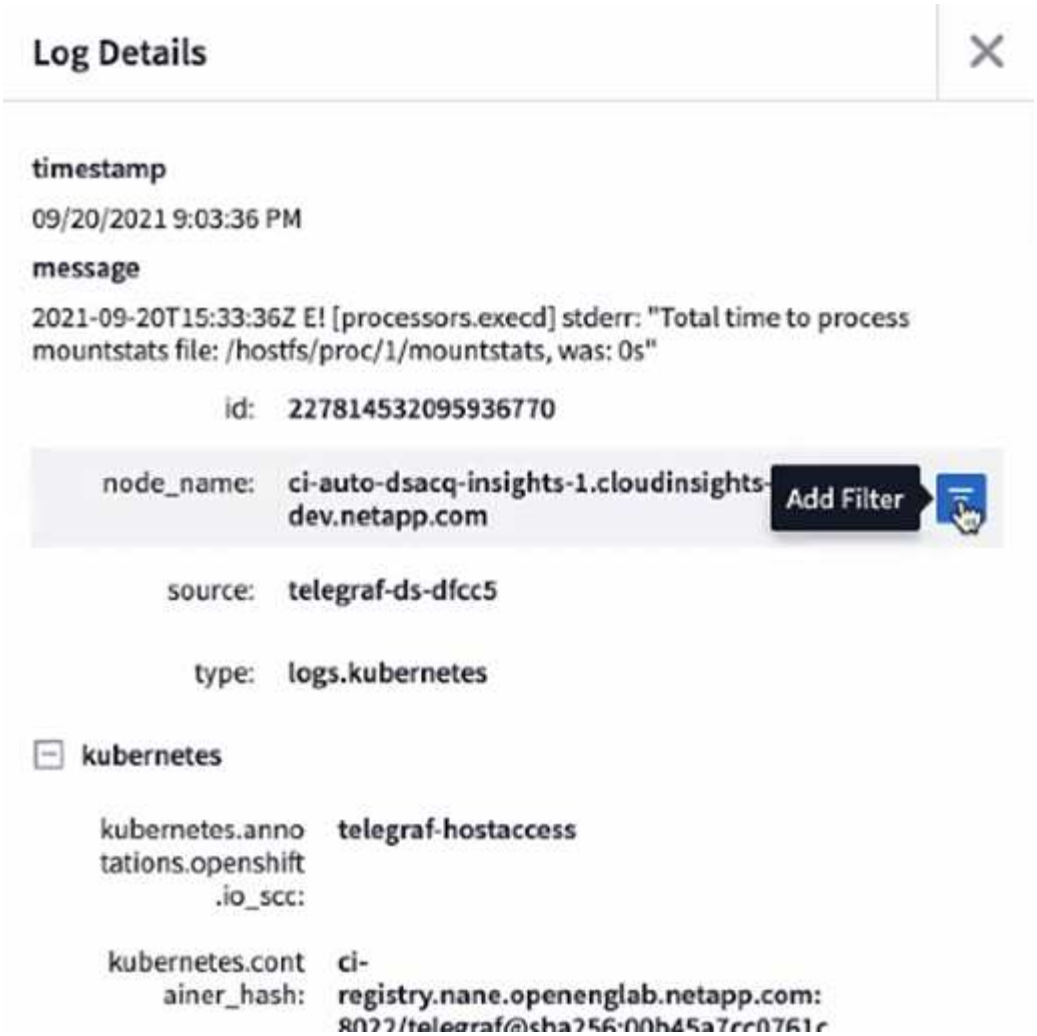
hinzufügen). Das Diagramm und die Liste Protokolleinträge werden aktualisiert, um die Ergebnisse basierend auf Ihrer Auswahl anzuzeigen. Um diese Filterung zu entfernen, öffnen Sie die Legende erneut, und wählen Sie [X], um den Legendenfilter zu löschen.



Protokolldetails

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

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



Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Protokollanfragen.

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

Einblick

Einblick

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

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

zuvor aktiv waren, aber nicht mehr auftreten.

Insight Typen

Unter Stress Abbauen

Durch Workloads mit hohen Auswirkungen kann die Performance anderer Workloads in einer gemeinsamen Ressource reduziert werden. Dadurch wird die gemeinsam genutzte Ressource unter Druck. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und Beeinträchtigungen Ihrer Umgebung untersuchen können. "Weitere Informationen"

Kubernetes Namespaces sind nicht mehr platzsparend

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

Rückgewinnung von ONTAP Cold Storage

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

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

Einblicke: Shared Ressourcen Unter Stress

Durch Workloads mit hohen Auswirkungen kann die Performance anderer Workloads in einer gemeinsamen Ressource reduziert werden. Dadurch wird die gemeinsam genutzte Ressource unter Druck. Data Infrastructure Insights bietet Tools, mit denen Sie die Ressourcensättigung und Beeinträchtigungen Ihrer Umgebung untersuchen können.

Terminologie

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

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

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

Beachten Sie, dass das Volume oder das interne Volume selbst als Workload erkannt wird, falls Data Infrastructure Insights den führenden Computing-Workload nicht erkannt hat. Dies gilt sowohl für anspruchsvolle als auch für betroffene Workloads.

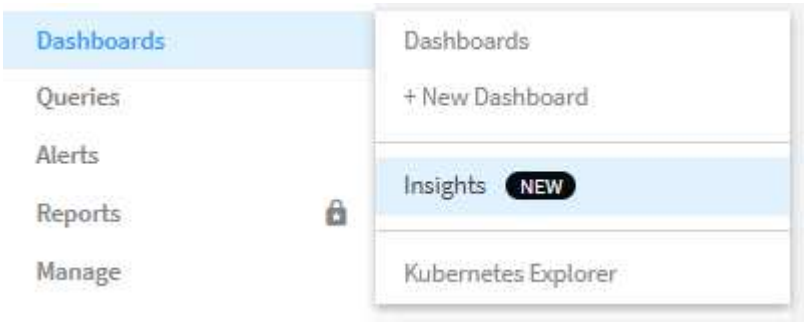
Shared Resource Sättigung ist das Verhältnis der IOPS-Auswirkung zu *Baseline*.

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

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

Anspruchsvolle Workloads

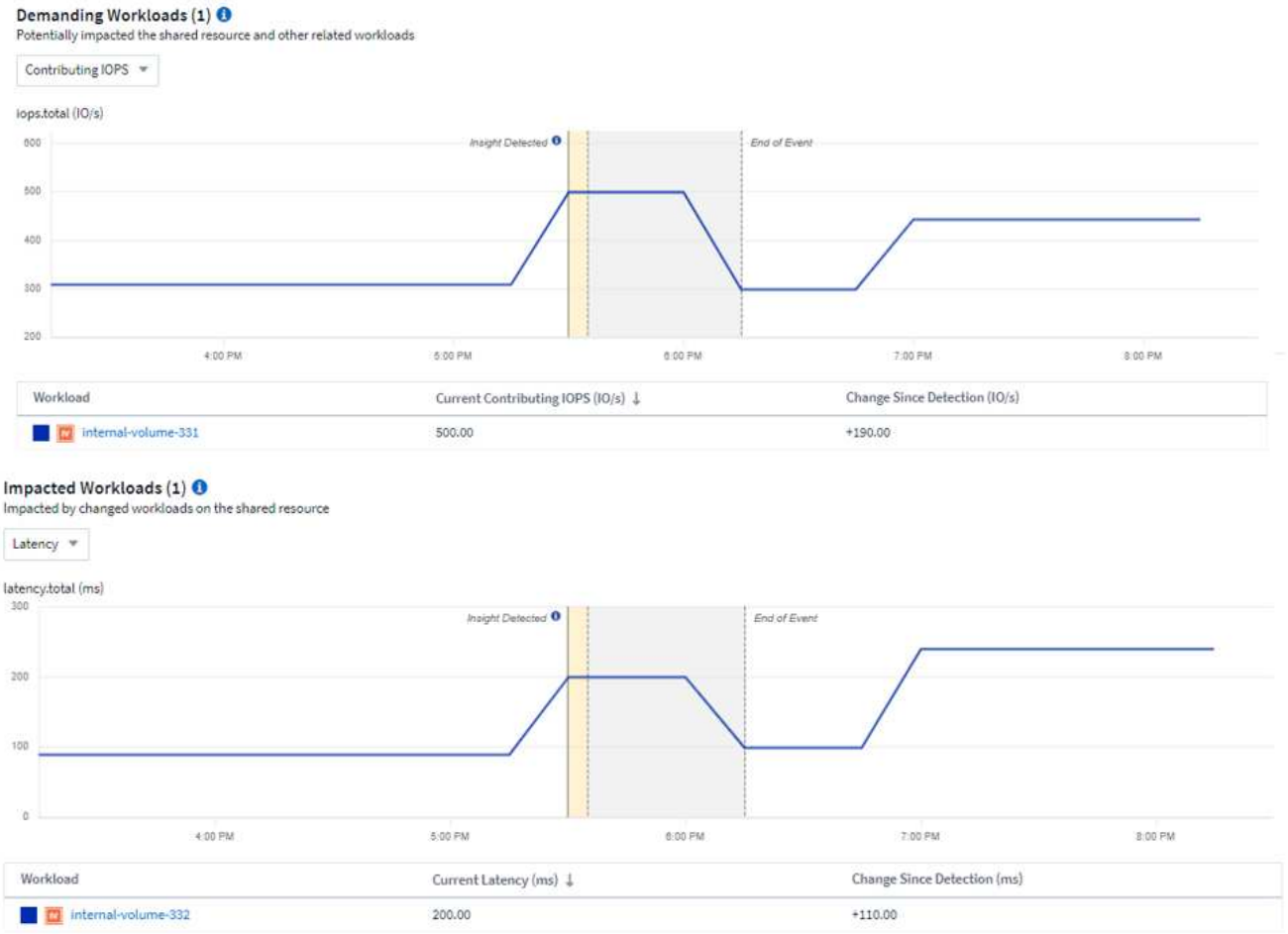
Wenn Sie sich mit anspruchsvollen und beeinträchtigten Workloads in Ihren gemeinsam genutzten Ressourcen vertraut machen möchten, klicken Sie auf **Dashboards > Insights** und wählen Sie die Option **Shared Resources under Stress** Insight aus.



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

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

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



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

Was muss ich tun, um Sättigung zu lösen?

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

- Kunden mit hohen IOPS-Werten bewegen

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

- Implementierung einer QoS-Richtlinie (Quality of Service

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

- Fügen Sie weitere Ressourcen hinzu

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

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

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

Speicherplatzbelegung in Ihrer Umgebung ist nie eine gute Situation. Mit Einblick in die Dateninfrastruktur können Sie die benötigte Zeit vorhersagen, bevor die persistenten Kubernetes-Volumes voll werden.

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

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

Kubernetes Namespaces Running Out of Space (3)

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

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

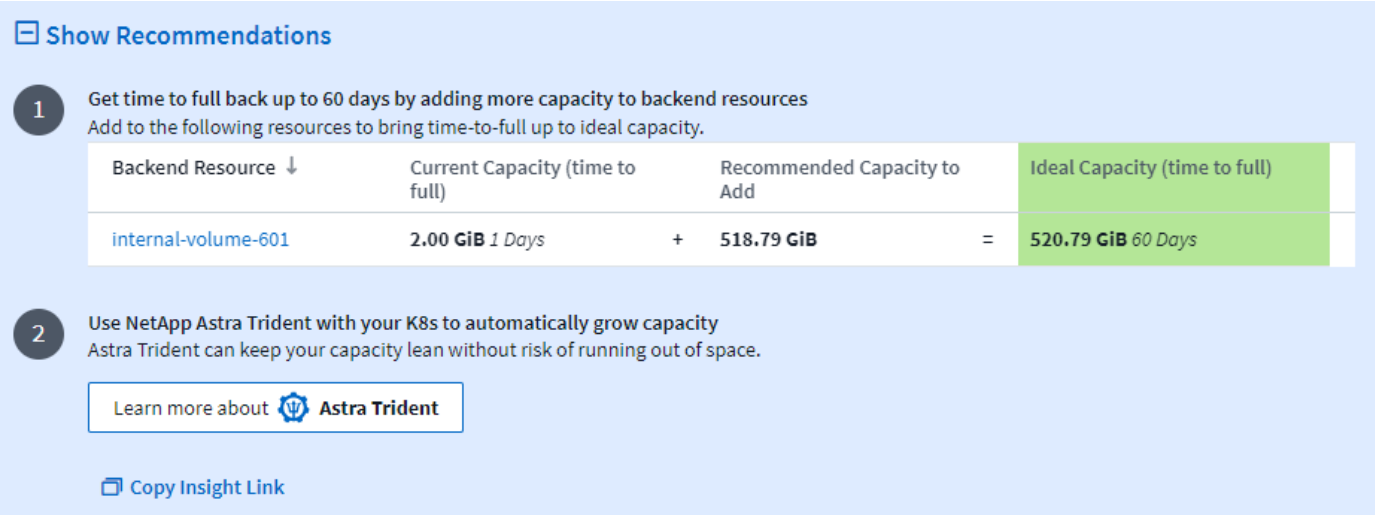
- Workload-Name
- Betroffene persistente Volumes
- Prognostizierte Zeitdauer innerhalb von Tagen
- Kapazität des persistenten Volumes
- Betroffen ist die Back-End Storage-Ressource, wobei die aktuelle Kapazität nicht mehr insgesamt belegt wird. Wenn Sie auf diesen Link klicken, wird die detaillierte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

Workloads at risk (2)

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

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

Klicken Sie auf der Insight Seite auf **+Empfehlungen anzeigen**, um mögliche Lösungen anzuzeigen. Wenn der Speicherplatz knapp wird, ist es am einfachsten, immer mehr Kapazität hinzuzufügen, und Data Infrastructure Insights bietet Ihnen die optimale Kapazität, um eine 60-Tage-Zielprognose zu verlängern. Weitere Empfehlungen sind ebenfalls aufgeführt.



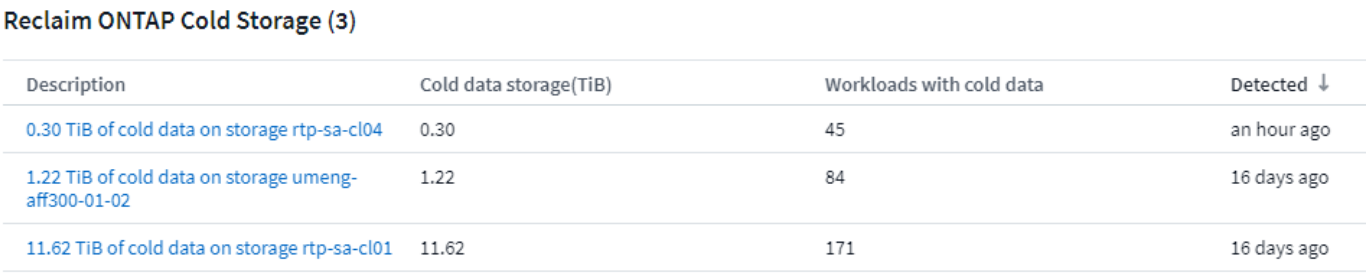
Hier können Sie auch einen bequemen Link zu dieser Insight kopieren, die Seite als Lesezeichen hinzufügen oder sie ganz einfach mit Ihrem Team teilen.

Einblick: Rückgewinnung von ONTAP Cold Storage

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

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

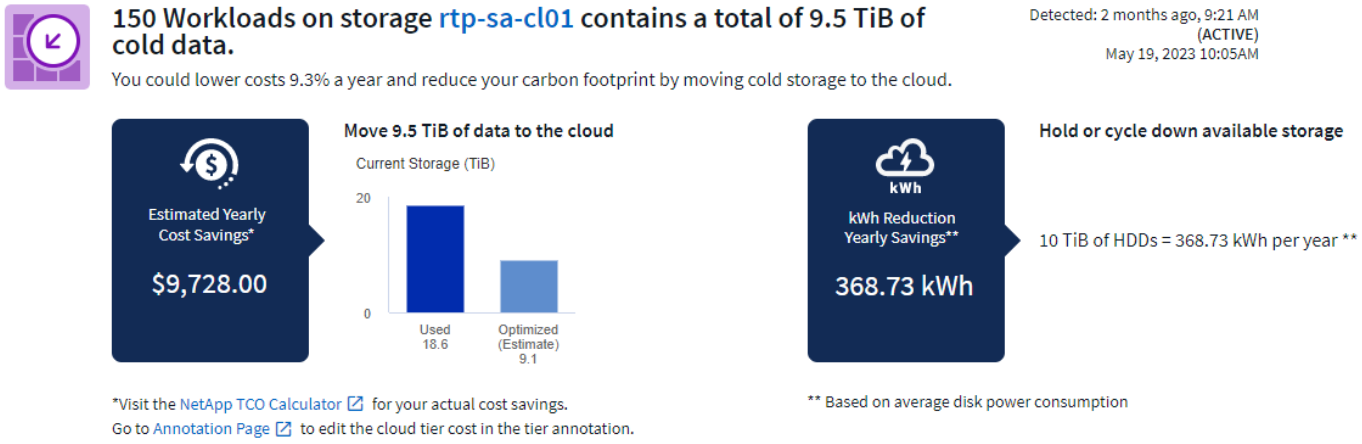
Beachten Sie, dass kalte Daten, die weniger als 30 Tage alt sind, nicht angezeigt werden.



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

Wenn Sie einen Insight aus der Liste auswählen, wird eine Seite mit weiteren Details geöffnet, darunter Empfehlungen zum Verschieben von Daten in die Cloud oder zum Herunterfahren von nicht verwendeten

Festplatten sowie geschätzte Kosten- und Energieeinsparungen, die Sie durch die Implementierung dieser Empfehlungen erzielen können. Die Seite bietet sogar einen praktischen Link zu "Der TCO-Rechner von NetApp" So können Sie mit den Zahlen experimentieren.



Empfehlungen

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

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

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

- Löschen Sie ungenutzte Workloads

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

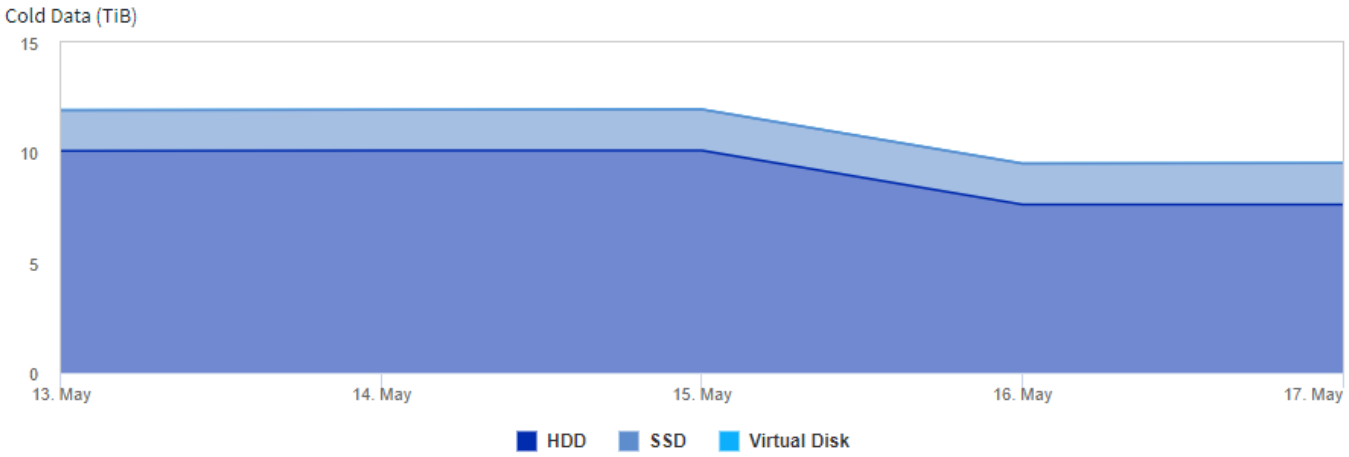
- Man betrachte die Fabric Pool Lösung von NetApp

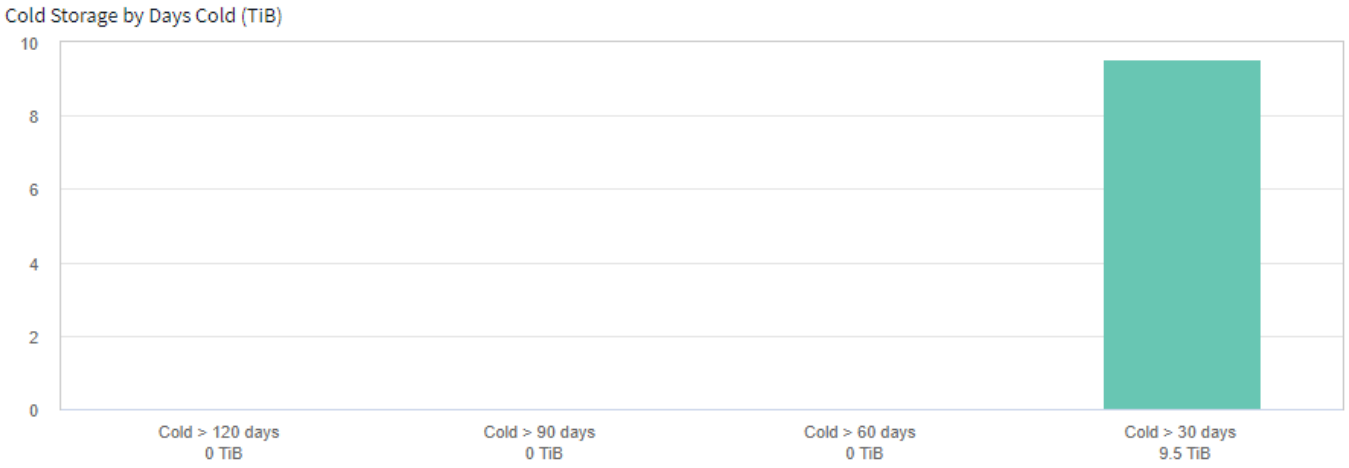
  NetApp "Fabric Pool Lösung" Verschiebt selten benötigte Daten automatisch in kostengünstigen Cloud-Storage, um so die Effizienz Ihrer Performance-Tiers zu steigern und Remote-Datensicherung zu ermöglichen.

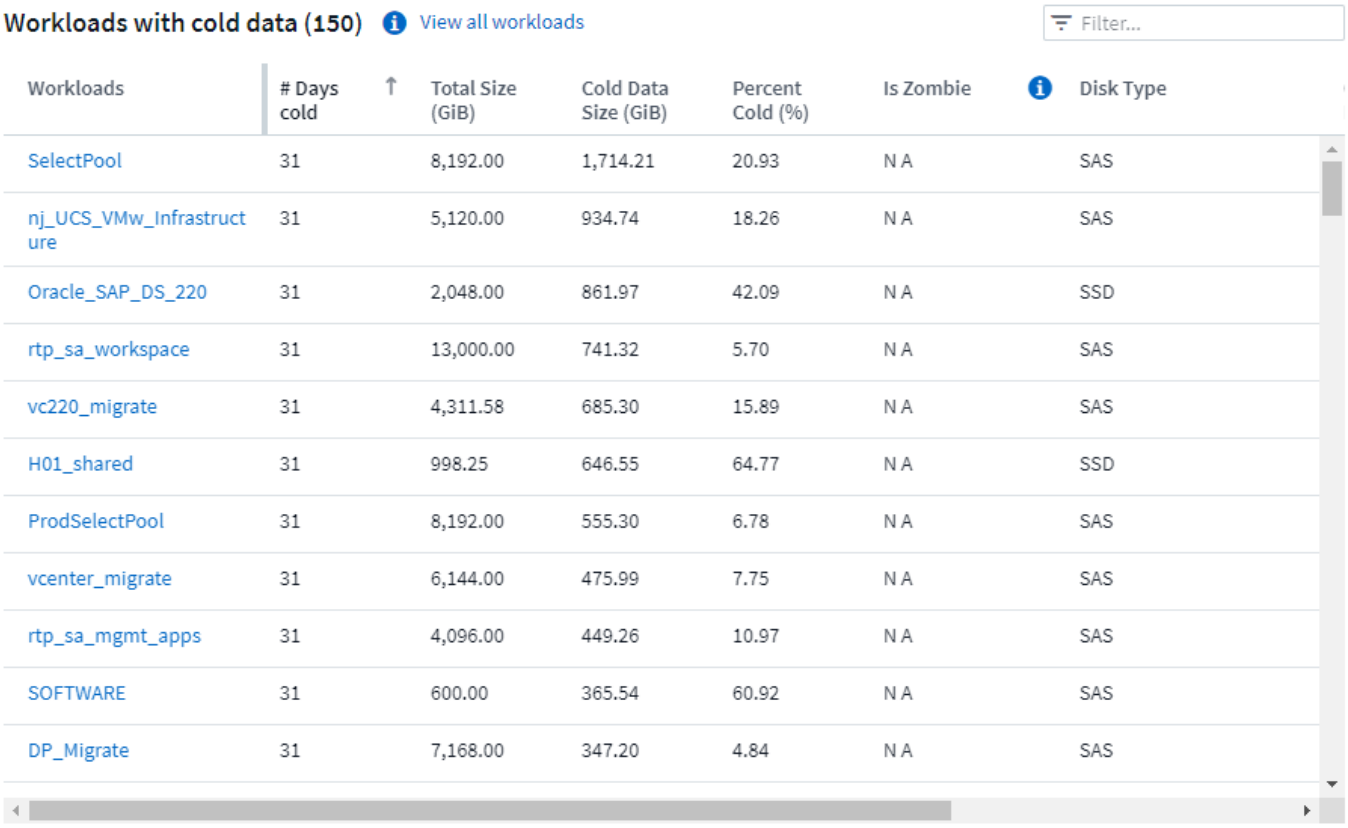
Visualisieren und erkunden

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

Cluster Cold Storage Trend Show Details







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

Monitore und Alarme

Warnfunktionen mit Monitoren

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

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

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

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

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

Best Practice Für Sicherheit

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

Metrik oder Protokollmonitor?

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

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

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

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

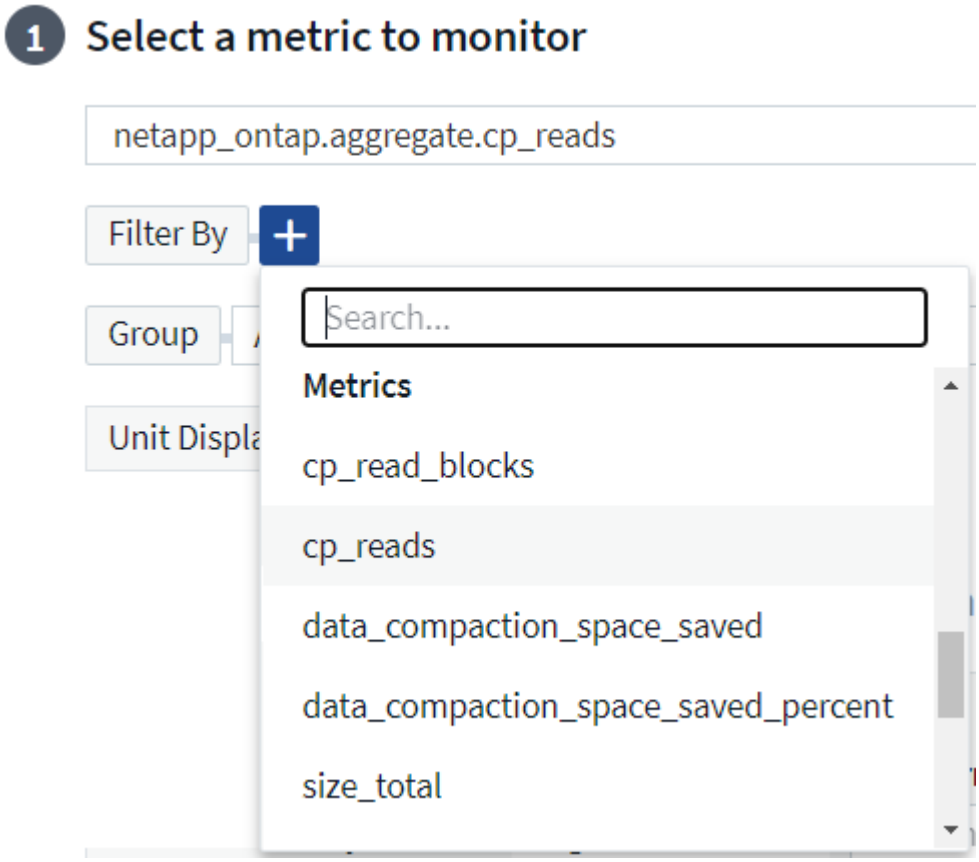
   - *Metric* überwacht Warnmeldungen zu Infrastruktur- oder Performance-bezogenen Triggern
   - *Log* überwacht die Warnung bei protokollbezogenen Aktivitäten

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

Metrischer Monitor

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

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



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

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

Definieren Sie die Bedingungen des Monitors.

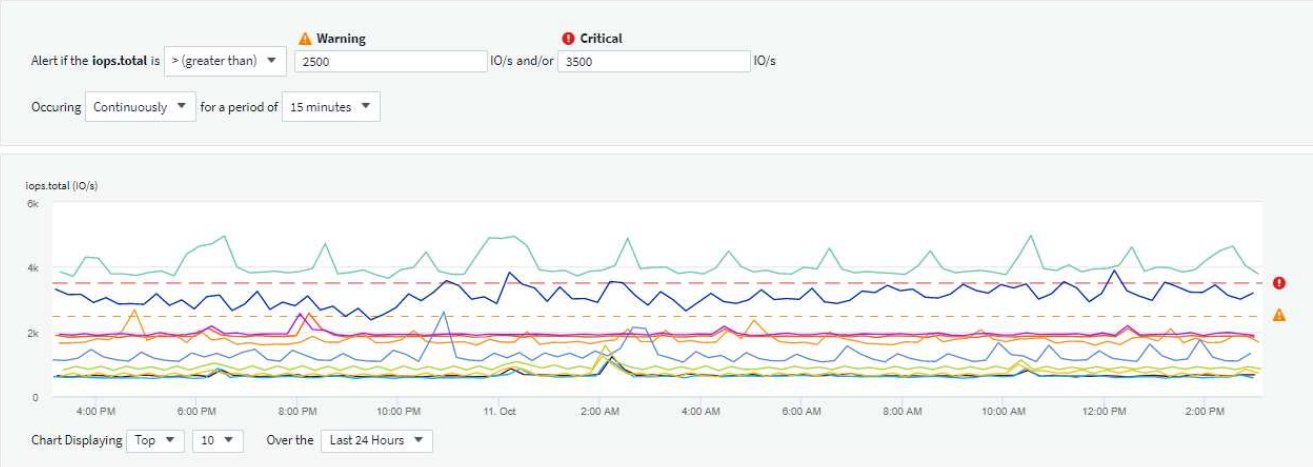
1. Nachdem Sie das zu überwachende Objekt und die Kennzahl ausgewählt haben, legen Sie die Schwellenwerte für Warnstufe und/oder kritische Stufe fest.
2. Geben Sie für die Stufe *Warnung* 200 für unser Beispiel ein. Die gestrichelte Linie, die diese Warnstufe angibt, wird im Beispieldiagramm angezeigt.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

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

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

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

dieser Werte überschreitet.



Definieren Sie das Verhalten für die Alarmauflösung

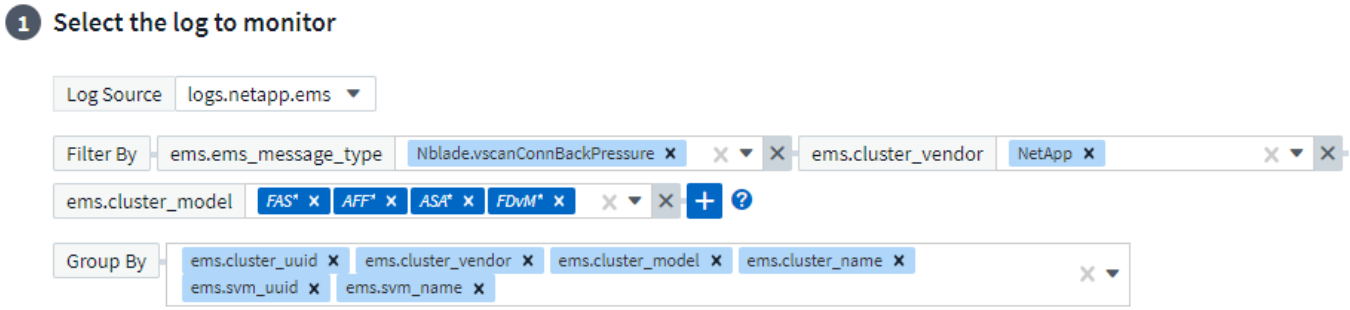
Sie können festlegen, wie eine Kennzahlüberwachung behoben werden soll. Ihnen stehen zwei Möglichkeiten zur Verfügung:

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

Protokollüberwachung

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

Der Filter Protokollmonitor darf nicht leer sein.



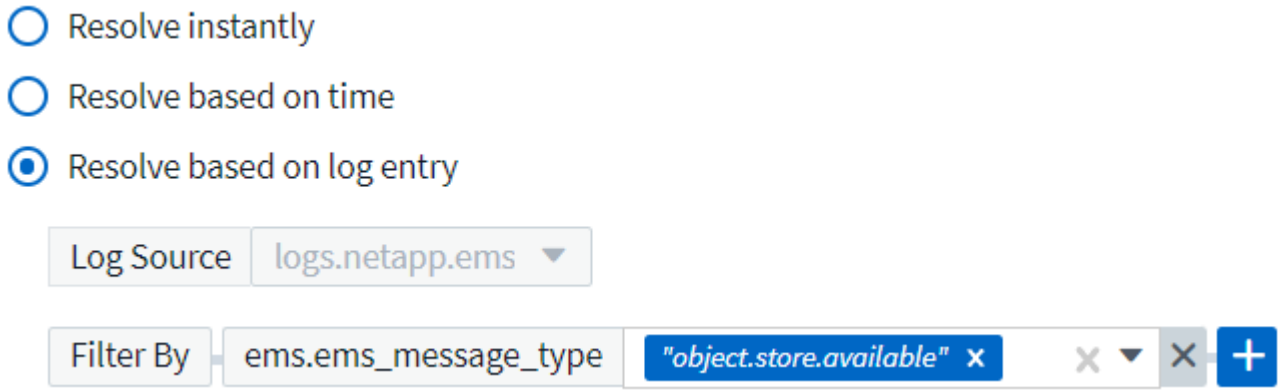
Definieren Sie das Alarmverhalten

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

Definieren Sie das Verhalten für die Alarmauflösung

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

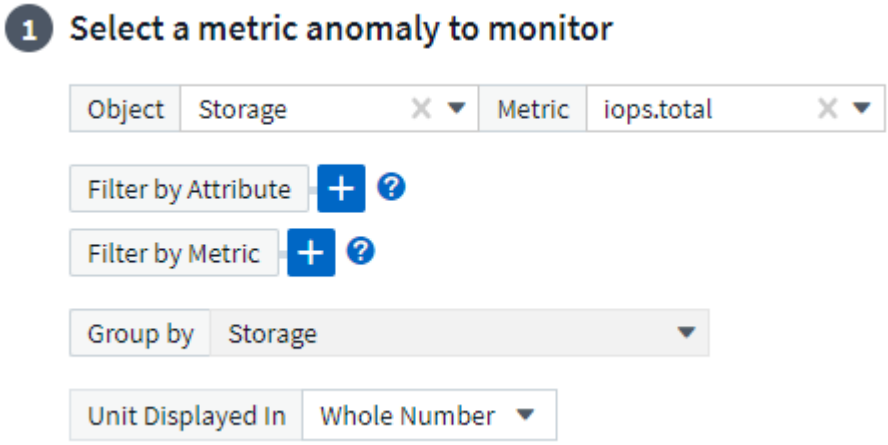
- **Sofort beheben**: Der Alarm wird sofort behoben, ohne dass weitere Maßnahmen erforderlich sind
- **Auflösung basierend auf Zeit**: Der Alarm wird nach Ablauf der angegebenen Zeit gelöst
- **Auflösung basierend auf Protokolleintrag**: Der Alarm wird aufgelöst, wenn eine nachfolgende Log-Aktivität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



Überwachung Der Anomalieerkennung

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

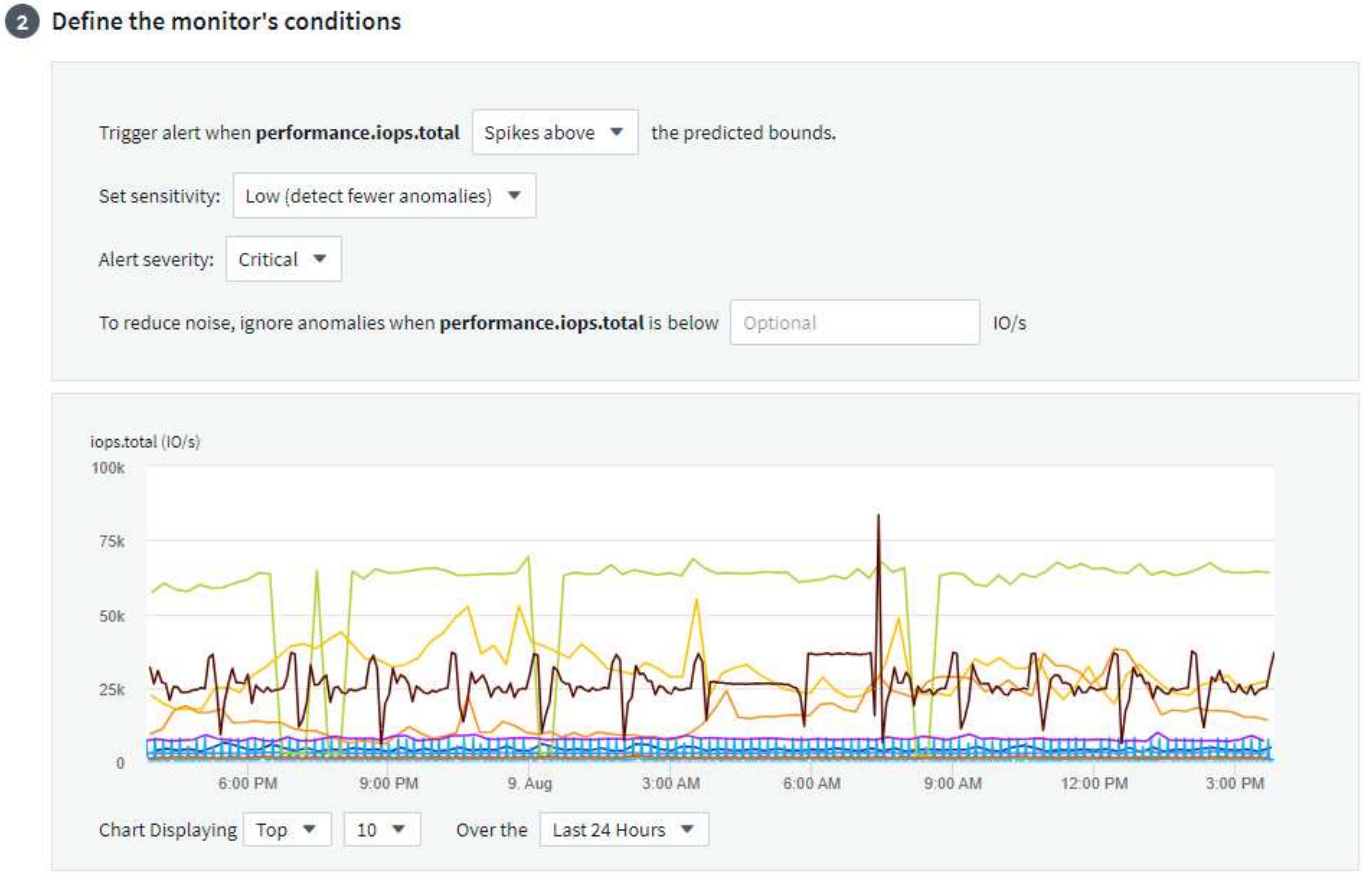
Filter können eingesetzt werden, um festzulegen, welche Objektattribute oder Metriken überwacht werden sollen.



Definieren Sie die Bedingungen des Monitors.

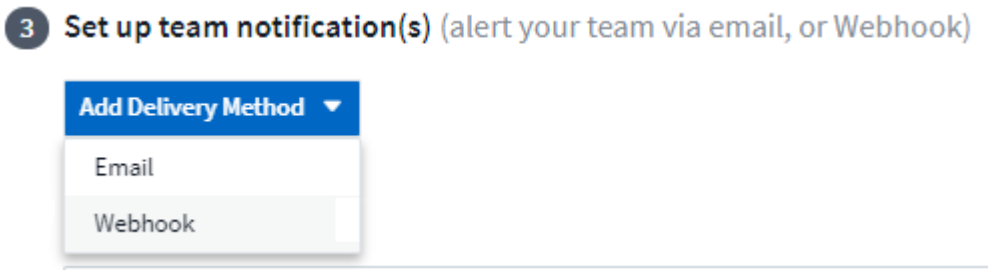
1. Nachdem Sie das zu überwachende Objekt und die zu überwachende Metrik ausgewählt haben, legen Sie die Bedingungen fest, unter denen eine Anomalie erkannt wird.
    - Wählen Sie aus, ob eine Anomalie erkannt werden soll, wenn die gewählte Metrik **über** die vorhergesagten Grenzen spikt, **unter**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

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



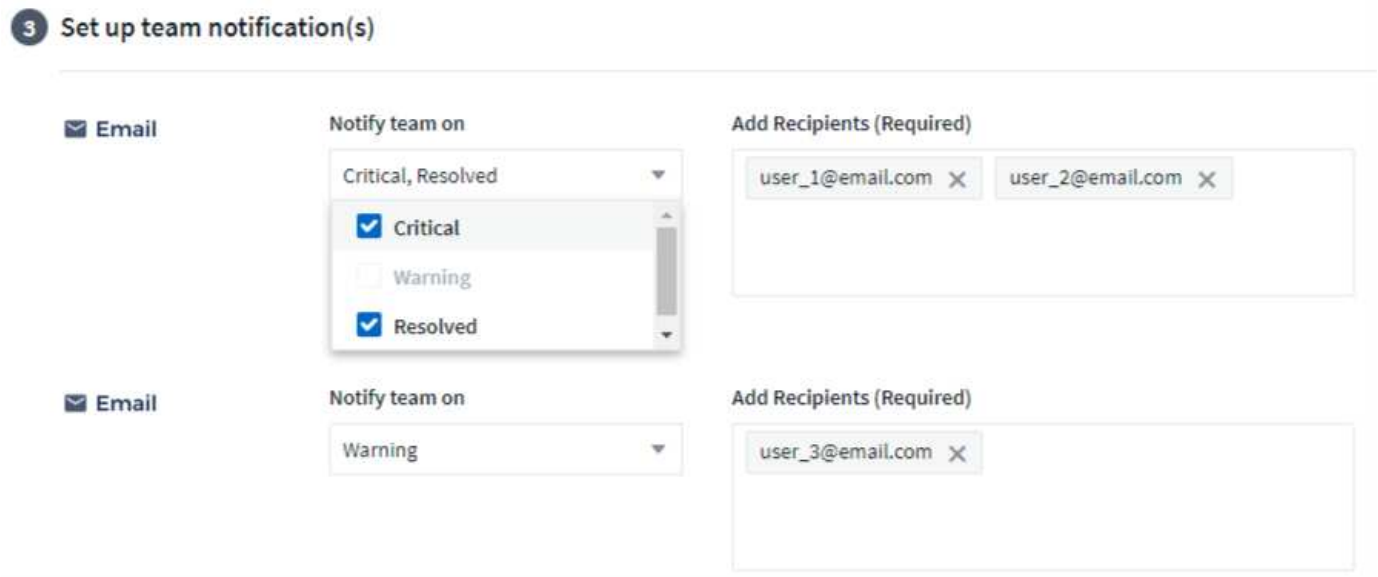
Wählen Sie Benachrichtigungstyp und Empfänger aus

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



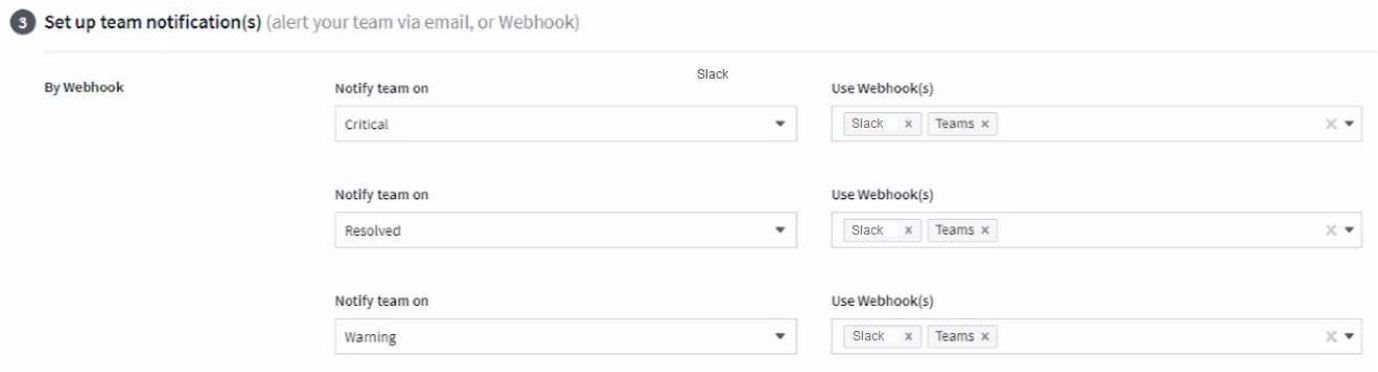
Alerting via Email:

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



Alerting via Webhook:

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

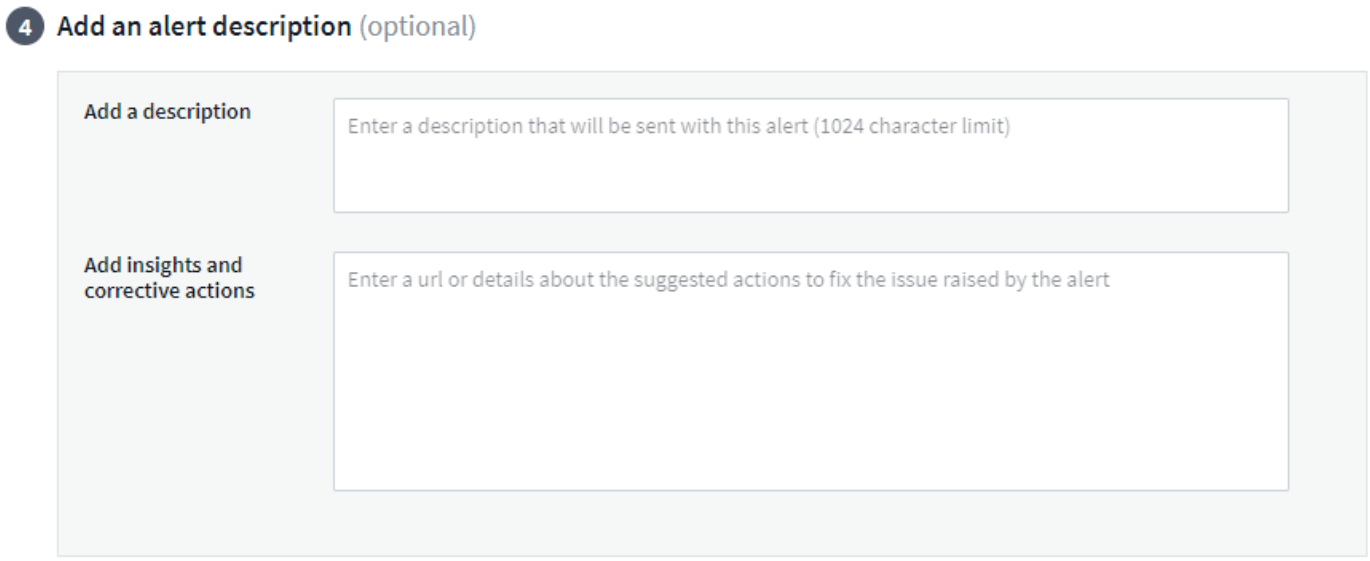


ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen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

Einstellen von Korrekturmaßnahmen oder zusätzlichen Informationen

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

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



Speichern Sie den Monitor

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

   Ihr neuer Monitor wird zur Liste der aktiven Monitore hinzugefügt.

Monitorliste

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

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

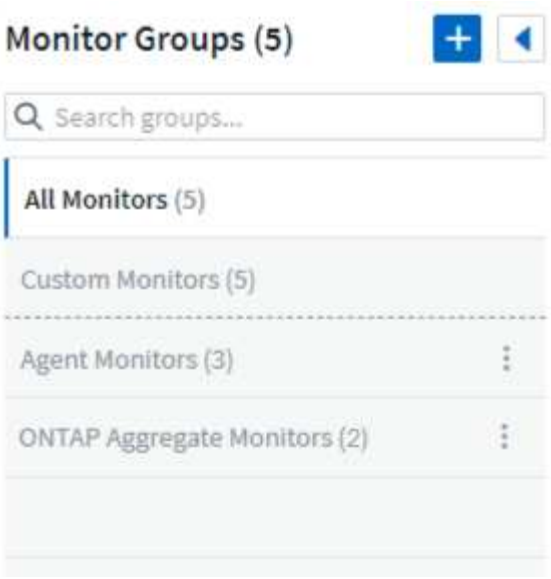
Sie können die Überwachung eines Objekttyps vorübergehend anhalten, indem Sie auf das Menü rechts neben dem Monitor klicken und **Pause** wählen. Wenn Sie bereit sind, die Überwachung fortzusetzen, klicken Sie auf **Fortsetzen**.

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

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

Gruppen Überwachen

Durch Gruppierung können Sie zugehörige Monitore anzeigen und verwalten. Sie können beispielsweise eine Monitorgruppe für den Speicher in Ihrer Umgebung einrichten oder überwachen, die für eine bestimmte Empfängerliste relevant ist.



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

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

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

Suspendierte Monitore

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

Systemdefinierte Monitore

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

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

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

Benutzerdefinierte Monitorgruppen

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

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

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

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

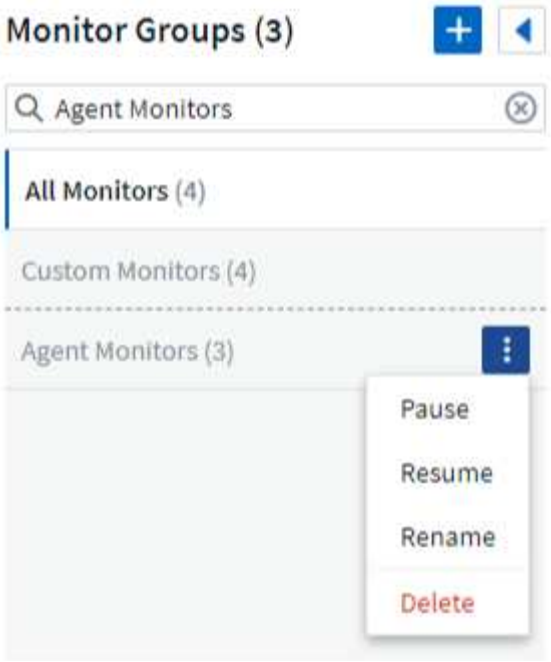
Entfernen Sie Monitore, indem Sie auf eine Gruppe klicken und im Menü *aus Gruppe* entfernen auswählen. Sie können keine Monitore aus der Gruppe „*Alle Monitore*“ oder „ Benutzerdefinierte Monitore_“ entfernen. Um einen Monitor aus diesen Gruppen zu löschen, müssen Sie den Monitor selbst löschen.

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

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

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

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



Systemdefinierte Monitore

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

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

Weitere Informationen

- "Anzeigen und Fehlstellen von Warnungen"

Anzeigen und Verwalten von Warnmeldungen von Monitoren

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

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

Anzeigen und Verwalten von Warnungen

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

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

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

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

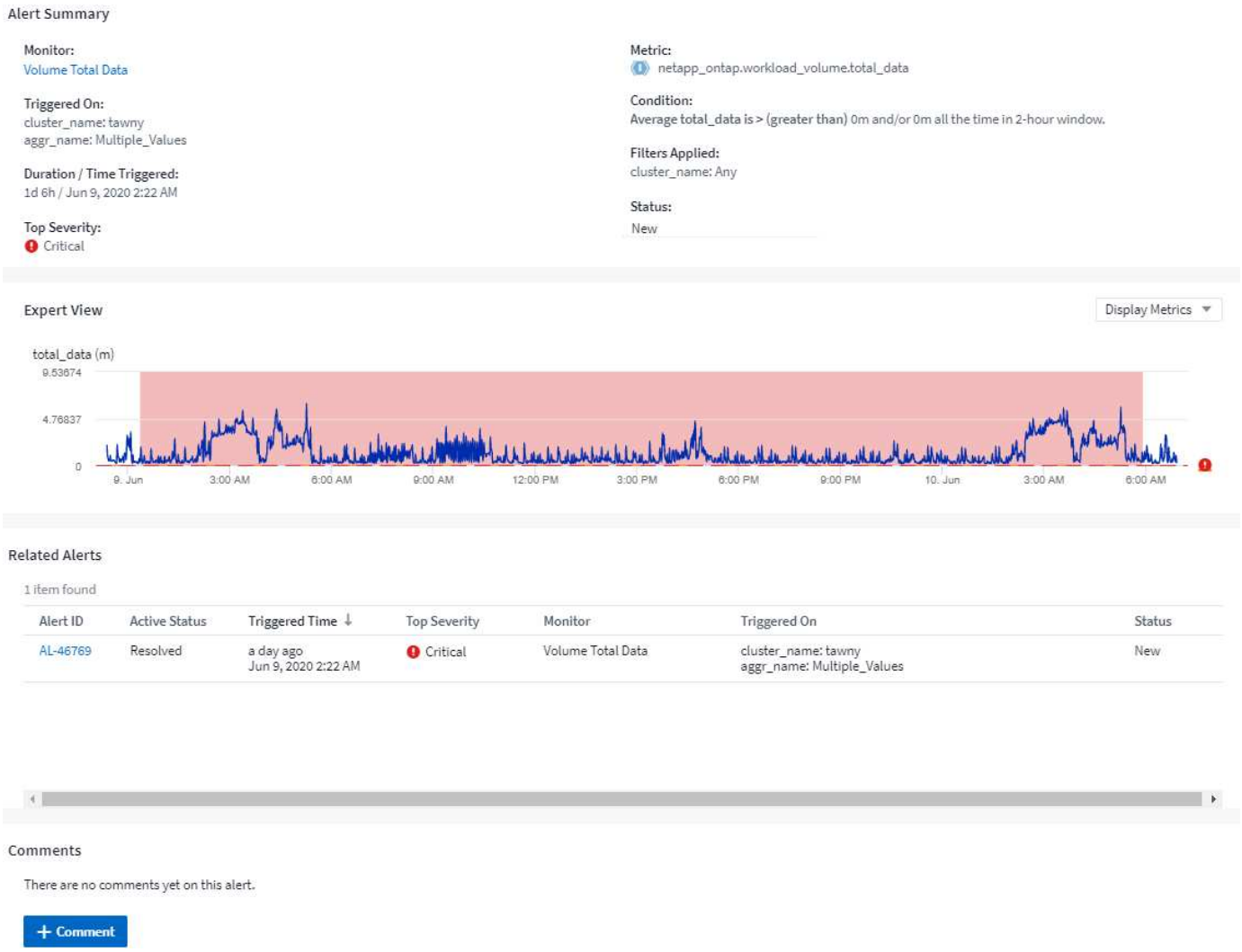
- **In Bearbeitung** um anzuzeigen, dass der Alarm untersucht wird oder anderweitig offen gehalten werden muss
- **Abweisen**, um die Warnung aus der Liste der aktiven Warnungen zu entfernen.

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

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

Seite Mit Den Alarmdetails

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



Benachrichtigt, Wenn Daten Fehlen

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

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

Wie bei langsamer Datenankunft oder keiner Datenzukunft muss der Timer-Mechanismus übernehmen, da die Dateneineinzugsrate nicht ausreicht, um Alarme in „Echtzeit“ auszulösen. So wird die Frage gewöhnlich: „Wie lange warte ich, bevor ich das Analysenfenster schließe und mir die habe?“ Wenn Sie zu lange warten, dann generieren Sie die Warnungen nicht schnell genug, um nützlich zu sein.

Wenn Sie einen Monitor mit einem 30-Minuten-Fenster haben, das bemerkt, dass eine Bedingung durch den letzten Datenpunkt vor einem langfristigen Datenverlust verletzt wird, Es wird eine Warnung generiert, da der Monitor keine weiteren Informationen erhalten hat, die zur Bestätigung der Wiederherstellung der Metrik verwendet werden müssen, oder dass die Bedingung weiterhin besteht.

„Dauerhaft Aktiv“-Warnungen

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

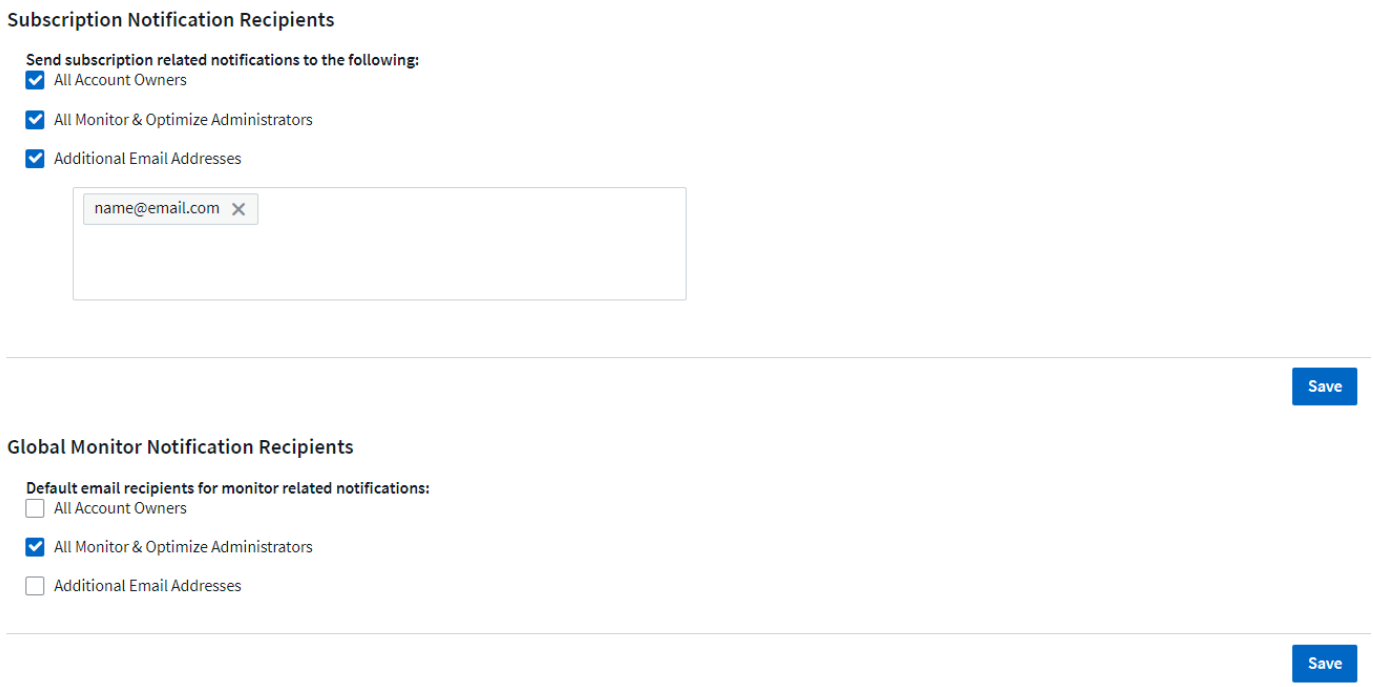
bleiben. Dies kann zu Problemen mit der Systemspannung und Stabilität im Laufe der Zeit führen.

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

E-Mail-Benachrichtigungen Werden Konfiguriert

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

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



Empfänger Für Abonnementbenachrichtigung

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

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

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

Hinweis:	**Benutzeraktion:**

Testversion oder Abonnement wurde aktualisiert	Überprüfen Sie die Abonnementdetails auf der "Abonnement" Seite
Das Abonnement läuft in 90 Tagen ab das Abonnement läuft in 30 Tagen ab	Keine Aktion erforderlich, wenn „Auto Renewal“ aktiviert ist Kontakt "NetApp Vertrieb" Um das Abonnement zu verlängern
Die Testversion endet in 2 Tagen	Verlängern Sie die Testversion vom "Abonnement" Seite. Sie können eine einmalige Testversion erneuern. Kontakt "NetApp Vertrieb" Um ein Abonnement zu erwerben
Testversion oder Abonnement abgelaufen Konto wird das Sammeln von Daten in 48 Stunden beendet Konto wird nach 48 Stunden gelöscht	Kontakt "NetApp Vertrieb" Um ein Abonnement zu erwerben

Globale Empfängerliste für Warnungen

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

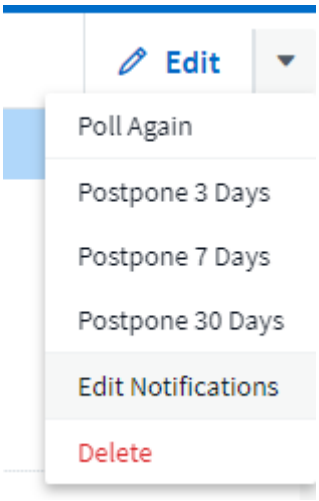
Wählen Sie zum Konfigurieren von Empfängern für globale Warnmeldungen die gewünschten Empfänger im Abschnitt **Empfänger für globale Monitorbenachrichtigungen** aus.

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

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

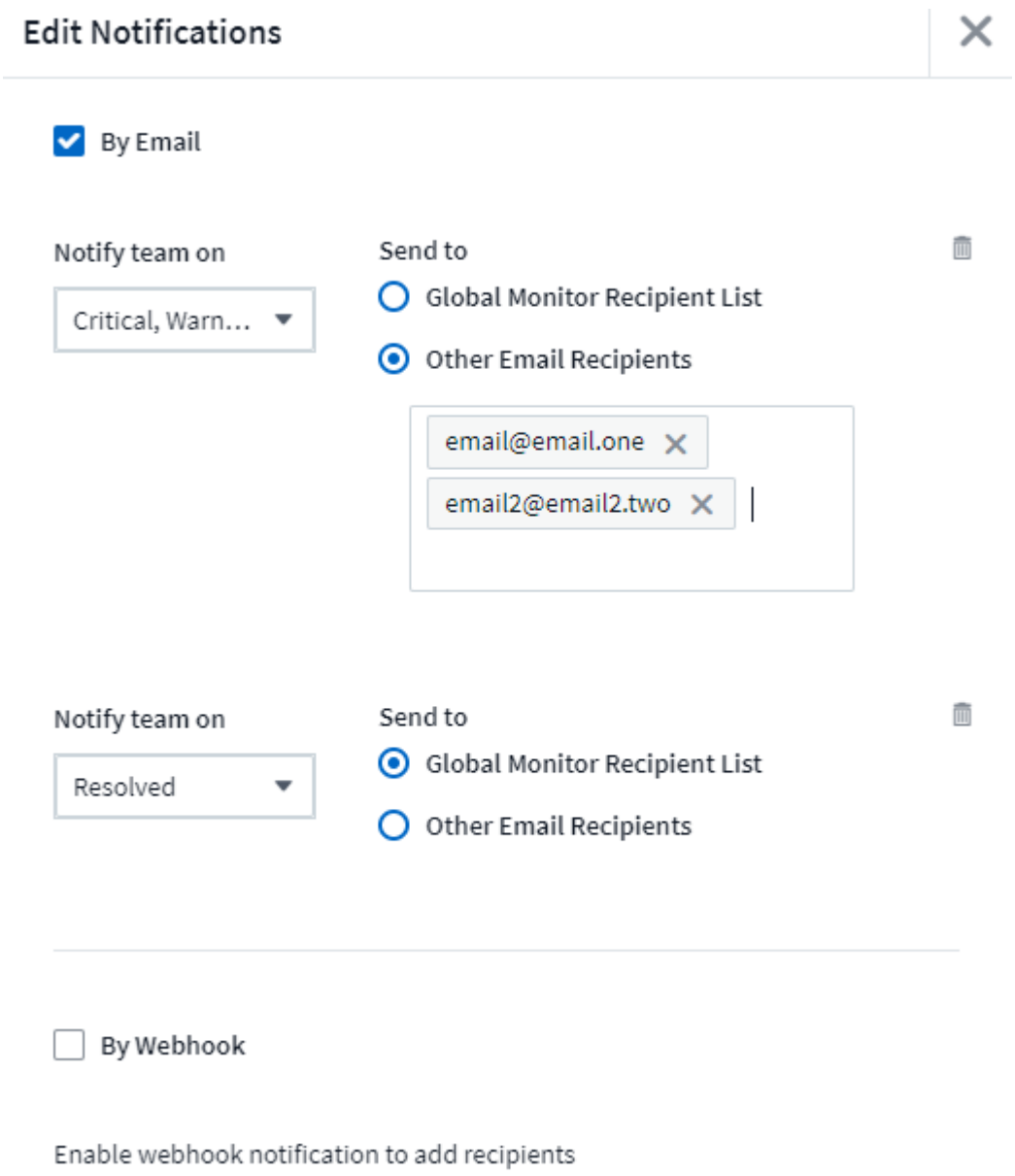
Bearbeiten von Benachrichtigungen für ONTAP

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



Von hier aus können Sie Benachrichtigungen für kritische, Warn-, Informations- und/oder gelöste

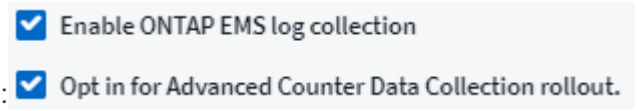
Warnmeldungen festlegen. Jedes Szenario kann die Liste der globalen Empfänger oder andere von Ihnen ausgewählte Empfänger benachrichtigen.



Systemmonitore

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

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



Monitorbeschreibungen

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

Systemdefinierte Monitorgruppen können nicht geändert oder entfernt werden.

Die folgenden systemdefinierten Monitore sind in den genannten Gruppen verfügbar.

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

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

Metrische Monitore

Monitorname	Schweregrad	Beschreibung Des Monitors	Korrekturmaßnahme

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

Lun-Latenz Hoch	KRITISCH	LUNs sind Objekte, die den I/O-Verkehr bedienen, der häufig von Performance-abhängigen Applikationen wie Datenbanken angetrieben wird. Hohe LUN-Latenzen bedeuten, dass Applikationen selbst unter Umständen darunter leiden und ihre Aufgaben nicht ausführen können.…eine Warnmeldung gibt an, dass bestimmte Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Node oder Aggregat zu verschieben.…Eine wichtige Warnmeldung gibt an, dass eine Serviceunterbrechung bevorsteht und Notfallmaßnahmen ergriffen werden sollten Sicherstellen von Servicekontinuität Die folgenden Latenzzeiten sind auf Grundlage des Medientyps zu erwarten – SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden	Falls der kritische Schwellenwert überschritten wird, sollten Sie die folgenden Maßnahmen zur Minimierung der Serviceunterbrechung berücksichtigen: Wenn der LUN oder seinem Volume eine entsprechende QoS-Richtlinie zugeordnet ist, bewerten Sie dann seine Schwellenwerte und überprüfen Sie, ob der LUN-Workload gedrosselt wird.… Falls der Warnschwellenwert nicht erreicht wird, folgende Maßnahmen ergreifen: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn der Node auch eine hohe Auslastung verzeichnet, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den Gesamtarbeitsbedarf des Node. 3. Wenn das LUN oder sein Volume eine QoS-Richtlinie damit verknüpft ist, bewerten Sie seine Schwellenwerte und validieren Sie, ob sie den LUN-Workload gedrosselt werden.

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

NVMe Namespace-Latenz hoch	KRITISCH	NVMe Namesaces sind Objekte, die den I/O-Datenverkehr verarbeiten, der von Performance-abhängigen Applikationen wie Datenbanken gesteuert wird. Hohe NVMe Namesaces Latenz bedeutet, dass Applikationen selbst möglicherweise darunter leiden und ihre Aufgaben nicht ausführen können.…eine Warnmeldung gibt an, dass bestimmte geplante Maßnahmen ergriffen werden sollten, um die LUN auf den entsprechenden Node oder Aggregat zu verschieben.…ein wichtiger Alarm zeigt, dass eine Serviceunterbrechung bevorsteht und Notfallmaßnahmen ergriffen werden sollten Für Servicekontinuität sorgen.	Falls ein kritischer Schwellenwert nicht erreicht wird, sollten sofortige Maßnahmen zur Minimierung der Service-Unterbrechung in Betracht gezogen werden: Wenn dem NVMe Namespace oder seinem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzwerte dann, falls der NVMe Namespace Workload gedrosselt wird.… Wenn der Warnschwellenwert nicht erreicht wird, folgende Maßnahmen ergreifen: 1. Wenn zudem ein Aggregat eine hohe Auslastung aufweist, verschieben Sie die LUN zu einem anderen Aggregat. 2. Wenn der Node auch eine hohe Auslastung verzeichnet, verschieben Sie das Volume auf einen anderen Node oder verringern Sie den Gesamtarbeitsbedarf des Node. 3. Wenn ihnen der NVMe Namespace oder dessen Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie dessen Grenzschwellenwerte, falls der NVMe Namespace Workload gedrosselt wird.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zurück nach oben

Protokollmonitore

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zurück nach oben

Anti-Ransomware-Protokollmonitore

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

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

Zurück nach oben

FSX für NetApp ONTAP-Monitore

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

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

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

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

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

Zurück nach oben

K8s-Monitore

Monitorname	Beschreibung	Korrekturmaßnahmen	Schweregrad/Schwellenwert

Hohe Persistent Volume Latency	Hohe persistente Volume-Latenzen bedeuten, dass die Applikationen selbst möglicherweise darunter leiden und ihre Aufgaben nicht ausführen können. Das Monitoring von Latenzen bei persistenten Volumes ist für eine applikationskonsistente Performance von entscheidender Bedeutung. Die folgenden Latenzzeiten sind auf Grundlage des Medientyps zu erwarten – SSD bis zu 1-2 Millisekunden, SAS bis zu 8-10 Millisekunden und SATA-HDD 17-20 Millisekunden.	**Sofortmaßnahmen** Wenn kritische Grenzwerte überschritten werden, sollten sofortige Maßnahmen zur Minimierung von Serviceunterbrechungen in Betracht gezogen werden: Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten Sie seine Grenzwerte, falls der Volume-Workload gedrosselt wird. **Maßnahmen, Die Bald Zu Tun Sind** Wenn der Warnungsschwellenwert überschritten wird, planen Sie die folgenden Sofortmaßnahmen: 1. Wenn der Speicherpool auch eine hohe Auslastung hat, verschieben Sie das Volume in einen anderen Speicherpool. 2. Wenn dem Volume eine QoS-Richtlinie zugewiesen ist, bewerten sie ihre Grenzwerte für den Fall, dass sie den Volume-Workload dazu bringen, gedrosselt zu werden. 3. Wenn der Controller auch eine hohe Auslastung aufweist, verschieben Sie das Volume auf einen anderen Controller oder verringern Sie die Gesamtlast des Controllers.	Warnung @ > 6,000 µs Kritisch @ > 12,000 µs

Cluster-Speichersättigung Hoch	Die zuteilbare Arbeitsspeichersättigung des Clusters ist hoch. Die Cluster-CPU-Sättigung wird als Summe der Arbeitsspeicherauslastung berechnet, geteilt durch die Summe des zuteilbaren Arbeitsspeichers aller K8s-Nodes.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von Speicher auf Nodes	Warnung @ > 80 % Kritisch @ > 90 %
POD-Anbindung fehlgeschlagen	Dieser Alarm tritt auf, wenn ein Volume-Anhang mit POD fehlgeschlagen ist.		Warnung
Hohe Wiederübertragungsrate	Hohe TCP-Übertragungsrate	Überprüfung auf Netzwerküberlastung – ermitteln von Workloads, die eine hohe Netzwerkbandbreite verbrauchen. Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks.	Warnung @ > 10 % Kritisch @ > 25 %
Kapazität Des Node-Dateisystems Hoch	Kapazität Des Node-Dateisystems Hoch	- Erhöhen Sie die Größe der Knotenplatten, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Verringern Sie die Verwendung von Anwendungsdateien.	Warnung @ > 80 % Kritisch @ > 90 %
Workload-Netzwerk-Jitter Hoch	Hoher TCP Jitter (hohe Latenz/Reaktionszeiten)	Prüfen Sie auf Netzwerküberlastung. Ermittlung von Workloads, die sehr viel Netzwerkbandbreite in Anspruch nehmen Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks	Warnung @ > 30 ms Kritisch @ > 50 ms

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

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

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

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

Knoten Nicht Bereit	Der Node war 5 Minuten lang nicht bereit	Überprüfen Sie, ob der Node über genügend CPU-, Arbeitsspeicher- und Festplattenressourcen verfügt. Prüfen Sie die Konnektivität des Node-Netzwerks. Prüfen Sie die Kubernetes-Ereignisprotokolle auf Fehlerursachen.	Kritisch @ < 1
Kapazität Des Persistenten Volumes Hoch	Die von einem persistenten Volume genutzte Back-End-Kapazität ist hoch.	- Erhöhen Sie die Volume-Größe, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Reduzierung der in Anwendungen gespeicherten Datenmenge.	Warnung @ > 80 % Kritisch @ > 90 %
Fehler beim Erstellen des Service Load Balancer	Erstellen Des Service Load Balancer Fehlgeschlagen		Kritisch
Workload-Replikatfehler	Einige Pods sind derzeit nicht für eine Bereitstellung oder ein DemonSet verfügbar.		Warnung @ > 1
ResourceQuota CPU Requests About to Exceed	CPU-Anforderungen für Namespace überschreiten ResourceQuota		Warnung @ > 80 % Kritisch @ > 90 %
Hohe Wiederübertragungsrate	Hohe TCP-Übertragungsrate	Überprüfung auf Netzwerküberlastung – ermitteln von Workloads, die eine hohe Netzwerkbandbreite verbrauchen. Überprüfen Sie die Pod-CPU-Auslastung. Prüfen Sie die Leistung des Hardwareletzwerks.	Warnung @ > 10 % Kritisch @ > 25 %

Node-Festplattendruck	Verfügbarer Speicherplatz und Inodes auf dem Root-Dateisystem des Knotens oder dem Image-Dateisystem haben einen Schwellenwert für die Entfernung erreicht.	- Erhöhen Sie die Größe der Knotenplatten, um sicherzustellen, dass genügend Platz für die Anwendungsdateien vorhanden ist. - Verringern Sie die Verwendung von Anwendungsdateien.	Kritisch @ > 0
Cluster-CPU-Sättigung hoch	Cluster-zuteilbare CPU-Sättigung ist hoch. Die Cluster-CPU-Sättigung wird als Summe der CPU-Auslastung berechnet, geteilt durch die Summe der zuteilbaren CPU aller K8s-Nodes.	Nodes hinzufügen. Beheben Sie alle nicht geplanten Knoten. Pods passender Größe zur Freigabe von CPU auf Nodes	Warnung @ > 80 % Kritisch @ > 90 %

Zurück nach oben

Protokollmonitore Ändern

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

Zurück nach oben

Datenerfassungsmonitore

Monitorname	Beschreibung	Korrekturmaßnahme

Herunterfahren Der Erfassungseinheit	Data Infrastructure Insights Acquisition Units werden regelmäßig im Rahmen von Upgrades neu gestartet, um neue Funktionen einzuführen. Dies geschieht einmal pro Monat oder weniger in einer typischen Umgebung. Eine Warnung, dass eine Erfassungseinheit heruntergefahren wurde, sollte bald darauf mit einer Auflösung folgen, die feststellt, dass die neu neu neu neu aufgestartete Erfassungseinheit eine Registrierung bei Data Infrastructure Insights abgeschlossen hat. In der Regel dauert dieser Vorgang beim Herunterfahren bis zur Registrierung 5 bis 15 Minuten.	Wenn der Alarm häufig auftritt oder länger als 15 Minuten dauert, überprüfen Sie den Betrieb des Systems, das die Erfassungseinheit, das Netzwerk und einen beliebigen Proxy hostet, der die AU mit dem Internet verbindet.
Collector Fehlgeschlagen	Bei der Abfrage eines Datensammlers ist eine unerwartete Fehlersituation aufgetreten.	Weitere Informationen zur Situation finden Sie auf der Seite Datensammler unter Data Infrastructure Insights.
Sammlerwarnung	Dieser Alarm kann in der Regel aufgrund einer fehlerhaften Konfiguration des Datensammlers oder des Zielsystems auftreten. Überprüfen Sie die Konfigurationen, um zukünftige Warnmeldungen zu vermeiden. Es kann auch durch einen Abruf von weniger als vollständigen Daten, wo der Datensammler alle Daten, die es konnte gesammelt werden. Dies kann vorkommen, wenn sich während der Datenerfassung Situationen ändern (z. B. wird während der Datenerfassung eine zu Beginn der Datenerfassung vorhandene virtuelle Maschine gelöscht und vor der Erfassung der Daten).	Überprüfen Sie die Konfiguration des Datensammlers oder Zielsystems. Beachten Sie, dass der Monitor für Collector-Warnung mehr Warnmeldungen als andere Monitortypen senden kann. Es wird daher empfohlen, keine Alarmempfänger festzulegen, es sei denn, Sie beheben die Fehlerbehebung.

Zurück nach oben

Sicherheitsmonitore

Monitorname	Schwellenwert	Beschreibung Des Monitors	Korrekturmaßnahme

AutoSupport HTTPS-Transport deaktiviert	Warnung @ < 1	AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.	Um HTTPS als Transportprotokoll für AutoSupport Meldungen festzulegen, führen Sie den folgenden ONTAP-Befehl aus:…System Node AutoSupport modify -Transport https
Cluster unsichere Chiffren für SSH	Warnung @ < 1	Gibt an, dass SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP-Befehl aus:…Security ssh remove -vserver <admin vserver> -Chiffers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Das Cluster-Anmelde-Banner Ist Deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer, die auf das ONTAP-System zugreifen, deaktiviert ist. Die Anzeige eines Anmeldebanners ist hilfreich, um die Erwartungen für den Zugriff und die Verwendung des Systems zu stellen.	Führen Sie zum Konfigurieren des Anmeldebanns für ein Cluster den folgenden ONTAP-Befehl aus:…Security Login Banner modify -vserver <admin svm> -message „Zugriff auf autorisierte Benutzer beschränkt“.
Cluster-Peer-Kommunikation Ist Nicht Verschlüsselt	Warnung @ < 1	Bei der Replizierung von Daten für Disaster Recovery, Caching oder Backup müssen die Daten während der Übertragung über das Netzwerk von einem ONTAP Cluster zum anderen gesichert werden. Die Verschlüsselung muss sowohl auf den Quell- als auch auf den Ziel-Clustern konfiguriert sein.	Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, muss das Quell- und Ziel-Cluster auf 9.6 aktualisiert werden. Verwenden Sie dann den Befehl „Cluster Peer modify“, um sowohl die Quell- als auch die Ziel-Cluster-Peering-Verschlüsselung zu ändern.…Details finden Sie im NetApp Security Hardening Guide for ONTAP 9.

Lokaler Admin-Standardbenutzer Aktiviert	Warnung @ > 0	NetApp empfiehlt, alle nicht benötigten Standard-Admin-Benutzer (integriert) mit dem Sperrbefehl zu sperren (zu deaktivieren). Es handelt sich dabei in erster Linie um Standardkonten, für die Passwörter nie aktualisiert oder geändert wurden.	Um das integrierte „admin“-Konto zu sperren, führen Sie den folgenden ONTAP-Befehl aus:…Security Login Lock -username admin
FIPS-Modus deaktiviert	Warnung @ < 1	Wenn die FIPS 140-2-Konformität aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn die FIPS 140-2-Compliance aktiviert ist.	Führen Sie zum Aktivieren der FIPS 140-2-Compliance auf einem Cluster den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security config modify -Interface SSL -is -fips-enabled true
Protokollweiterleitung Nicht Verschlüsselt	Warnung @ < 1	Das verlagern von Syslog-Informationen ist nötig, um den Umfang oder die Auswirkungen einer Sicherheitsverletzung auf ein einzelnes System oder eine einzelne Lösung zu beschränken. Daher empfiehlt NetApp, Syslog-Informationen sicher an einen sicheren Storage- oder Aufbewahrungsort zu verlagern.	Nach dem Erstellen eines Protokollweiterleitungsziel s kann sein Protokoll nicht mehr geändert werden. Wenn Sie zu einem verschlüsselten Protokoll wechseln möchten, löschen Sie das Ziel für die Protokollweiterleitung und erstellen Sie es mit dem folgenden ONTAP-Befehl:…Cluster log-fording create -Destination <Ziel-ip> -Protocol tcp-Encrypted
MD5-Kennwort gehasht	Warnung @ > 0	NetApp empfiehlt dringend, die sicherere SHA-512-Hash-Funktion für Passwörter für ONTAP-Benutzerkonten zu nutzen. Konten, die die weniger sichere MD5-Hash-Funktion verwenden, sollten auf die SHA-512-Hash-Funktion migriert werden.	NetApp empfiehlt Benutzerkonten, zur sichereren SHA-512-Lösung zu migrieren, indem Benutzer ihre Passwörter ändern.…um Konten mit Passwörtern zu sperren, die die MD5-Hash-Funktion verwenden, führen Sie den folgenden ONTAP-Befehl aus:…Security Login Lock -vserver * -username * -Hash -function md5

Es sind keine NTP-Server konfiguriert	Warnung @ < 1	Gibt an, dass auf dem Cluster keine konfigurierten NTP-Server vorhanden sind. Aus Gründen der Redundanz und des optimalen Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Um einen NTP-Server mit dem Cluster zu verknüpfen, führen Sie den folgenden ONTAP-Befehl aus: Cluster Time-Service ntp-Server create -Server <ntp-Server Host-Name oder ip-Adresse>
Die Anzahl der NTP-Server ist niedrig	Warnung @ < 3	Gibt an, dass auf dem Cluster weniger als 3 konfigurierte NTP-Server vorhanden sind. Aus Gründen der Redundanz und des optimalen Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Führen Sie den folgenden ONTAP-Befehl aus, um einen NTP-Server mit dem Cluster zu verknüpfen:…Cluster Time-Service ntp-Server create -Server <ntp-Server-Hostname oder ip-Adresse>
Remote Shell Aktiviert	Warnung @ > 0	Remote Shell ist keine sichere Methode zum Einrichten von Befehlszeilenzugriff auf die ONTAP Lösung. Die Remote-Shell sollte für einen sicheren Remote-Zugriff deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für sicheren Remote-Zugriff.…um die Remote Shell auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security Protocol modify -Application rsh-enabled false
Überwachungsprotokoll für Storage VM ist deaktiviert	Warnung @ < 1	Gibt an, dass die Überwachungsprotokollierung für SVM deaktiviert ist.	Um das Überwachungsprotokoll für einen vserver zu konfigurieren, führen Sie den folgenden ONTAP-Befehl aus:…vserver Audit enable -vserver <svm>
Storage VM unsichere Chiffren für SSH	Warnung @ < 1	Gibt an, dass SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Um die CBC-Chiffren zu entfernen, führen Sie den folgenden ONTAP-Befehl aus:…Security ssh remove -vserver <vserver> -Chiffers aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc

Anmeldebanner für Storage VM deaktiviert	Warnung @ < 1	Zeigt an, dass das Anmeldebanner für Benutzer, die auf SVMs auf dem System zugreifen, deaktiviert ist. Die Anzeige eines Anmeldebanners ist hilfreich, um die Erwartungen für den Zugriff und die Verwendung des Systems zu stellen.	Führen Sie zum Konfigurieren des Anmeldebanns für ein Cluster den folgenden ONTAP-Befehl aus:…Security Login Banner modify -vserver <svm> -message „Zugriff auf autorisierte Benutzer beschränkt“.
Telnet-Protokoll Aktiviert	Warnung @ > 0	Telnet ist keine sichere Methode zum Einrichten von Befehlszeilenzugriff auf die ONTAP-Lösung. Telnet sollte für den sicheren Remote-Zugriff deaktiviert werden.	NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff. Um Telnet auf einem Cluster zu deaktivieren, führen Sie den folgenden ONTAP-Befehl im erweiterten Berechtigungsmodus aus:…Security Protocol modify -Application telnet -enabled false

Zurück nach oben

Datensicherung Überwacht

Monitorname	Schwellenwerte	Beschreibung Des Monitors	Korrekturmaßnahme

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

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

Zurück nach oben

Cloud Volume (CVO) – Überwachung

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

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

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

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

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

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

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

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

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

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

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

Zurück nach oben

SnapMirror für Business Continuity (SMBC) Mediator Log Monitore

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

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

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

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

Zurück nach oben

Zusätzliche Monitore für Stromversorgung, Heartbeat und Sonstiges System

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

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

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

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

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

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

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

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

Zurück nach oben

Weitere Informationen

- "Anzeigen und Fehlstellen von Warnungen"

Benachrichtigung über Webhooks

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

Viele kommerzielle Anwendungen unterstützen Webhooks als Standard-Input-Schnittstelle, zum Beispiel

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

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

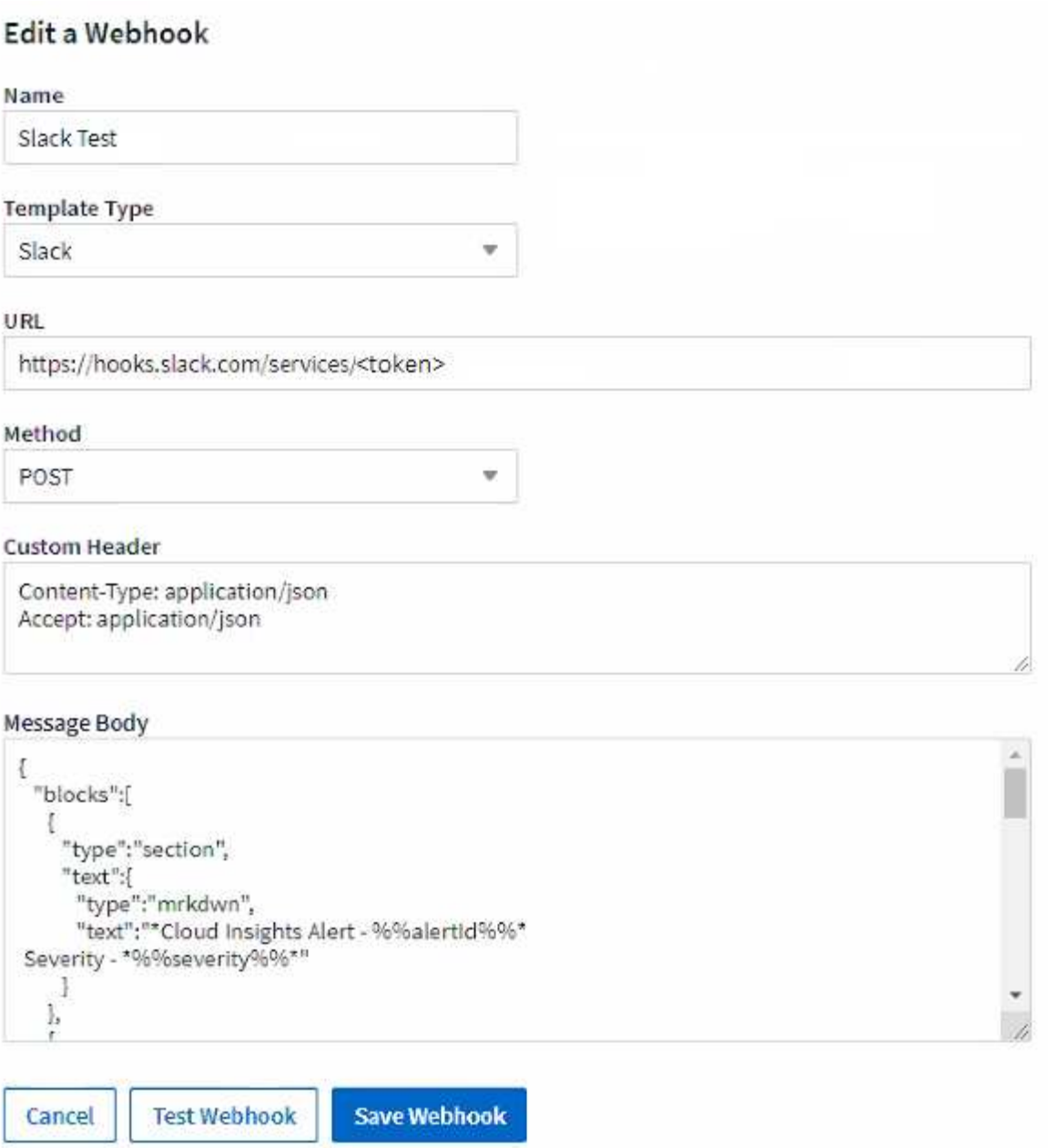
Die Instanz des Webhook-Kanals besteht aus folgenden Elementen:

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

Erstellen eines Webhook

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

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



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

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

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

Default Alert Parameters

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

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parameter: Was sind sie und wie benutze ich sie?

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

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

Benutzerdefinierte Parameter und Geheimnisse

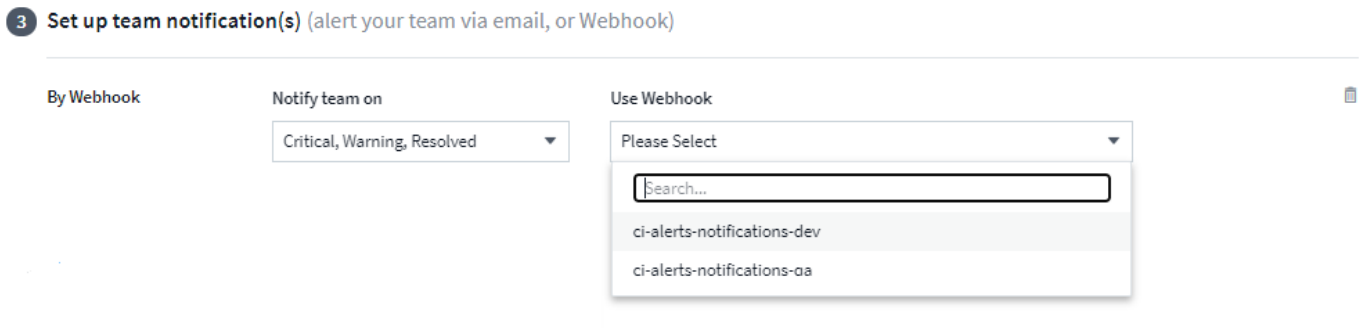
In diesem Abschnitt können Sie benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen, die Sie wünschen. Aus Sicherheitsgründen kann dieser Webhook-Kanal nur dann geändert werden, wenn ein Geheimnis definiert ist. Es ist schreibgeschützt für andere. Sie können Geheimnisse in URL/Headern als *%%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

Seite „Webhooks List“

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

Wählen Sie Webhook Notification in einem Monitor

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



Beispiele Für Webhook:

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

Arbeiten mit Anmerkungen

Anmerkungen definieren

Wenn Sie Data Infrastructure Insights an Ihre Unternehmensanforderungen anpassen, um Daten nachzuverfolgen, können Sie spezielle Notizen, sogenannte Annotationen, definieren und diese Ihren Ressourcen zuweisen.

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

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

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

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

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

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

Standard-Anmerkungstypen

Data Infrastructure Insights bietet einige standardmäßige Anmerkungstypen. Mit diesen Annotationen lassen sich Daten filtern oder gruppieren.

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

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

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

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

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

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

Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. Während Data Infrastructure Insights eine Reihe von Standardannotationen umfasst, kann es sein, dass Sie Daten auf andere Weise anzeigen möchten. Die Daten in benutzerdefinierten Annotationen ergänzen bereits erfassten Gerätedaten, wie z. B. Speicherhersteller, Anzahl Volumen und Leistungsstatistiken. Die mit Annotationen hinzugefügten Daten werden von Data Infrastructure Insights nicht erkannt.

Schritte

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

   Auf der Seite Anmerkungen wird die Liste der Anmerkungen angezeigt.

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

   Sie können in diese Felder bis zu 255 Zeichen eingeben.

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

Anmerkungstypen

Boolesch

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

Datum

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

Liste

Erstellt eine der folgenden Optionen:

- Eine feste Dropdown-Liste

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

- Eine Liste mit flexiblen Dropdown-Menüs

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

Nummer

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

Text

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

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

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

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

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

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

Nachdem Sie fertig sind

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

Mit Anmerkungen

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

Anmerkungen definieren

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. Während Data Infrastructure Insights

standardmäßig mit Annotationen ausgestattet ist, beispielsweise Lebenszyklus von Assets (Geburtstag oder Ende der Nutzungsdauer), Aufbau oder Standort des Datacenters sowie Tiering, können Daten möglicherweise auf andere Weise angezeigt werden.

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

Bevor Sie beginnen

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

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

Schritte

1. Klicken Sie im Menü Data Infrastructure Insights auf **Observability > Enrich > Annotationen**
2. Klicken Sie auf **+ Anmerkung**, um eine neue Anmerkung zu erstellen.
3. Geben Sie einen Namen, eine Beschreibung und einen Typ für die neue Anmerkung ein.

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

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

Manuelles Zuweisen von Anmerkungen zu Assets

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

Bevor Sie beginnen

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

Schritte

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

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

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

Anmerkungen mit Anmerkungsregeln zuweisen

Um Assets anhand von Kriterien, die Sie definieren, automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerkungsregeln. Data Infrastructure Insights weist Assets anhand dieser Regeln die Annotationen zu. Data Infrastructure Insights bietet außerdem zwei standardmäßige Anmerkungsregeln, die Sie an Ihre Anforderungen anpassen oder entfernen können, wenn Sie sie nicht verwenden möchten.

Anmerkungsregeln werden erstellt

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

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Über diese Aufgabe

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

Schritte

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

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

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

      Dieser Name wird auf der Seite Anmerkungsregeln angezeigt.

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

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

e. Klicken Sie Auf **Speichern**

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

Anmerkungsregeln werden erstellt

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

Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

Schritte

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

   Das Dialogfeld Regel hinzufügen wird angezeigt.

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

      Der Name wird auf der Seite Anmerkungsregeln angezeigt.

   b. Klicken Sie auf **Query**, und wählen Sie die Abfrage aus, die Data Infrastructure Insights zur Identifizierung der Assets verwendet, für die die Anmerkung gilt.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Beschriftung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

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

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

> In einer großen Data Infrastructure Insights-Umgebung können Sie bemerken, dass das Ausführen von Annotationsregeln eine Weile dauert. Dies liegt daran, dass der Indexer zuerst ausgeführt wird und vor der Ausführung der Regeln abgeschlossen werden muss. Mit dem Indexer können Data Infrastructure Insights nach neuen oder aktualisierten Objekten und Zählern in Ihren Daten suchen oder filtern. Die Regel-Engine wartet, bis der Indexer seine Aktualisierung abgeschlossen hat, bevor die Regeln angewendet werden.

Anmerkungsregeln ändern

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

Schritte

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

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

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

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

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

   Das Dialogfeld Regel bearbeiten wird angezeigt.

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

Die Reihenfolge der Regeln ändern

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

Schritte

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

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

Anmerkungsregeln werden gelöscht

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

Schritte

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

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

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

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

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

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

5. Klicken Sie auf **OK**

Anmerkungen Werden Importiert

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

Die Data Infrastructure Insights API ist in **Data Infrastructure Insights Premium Edition** verfügbar.

Importieren

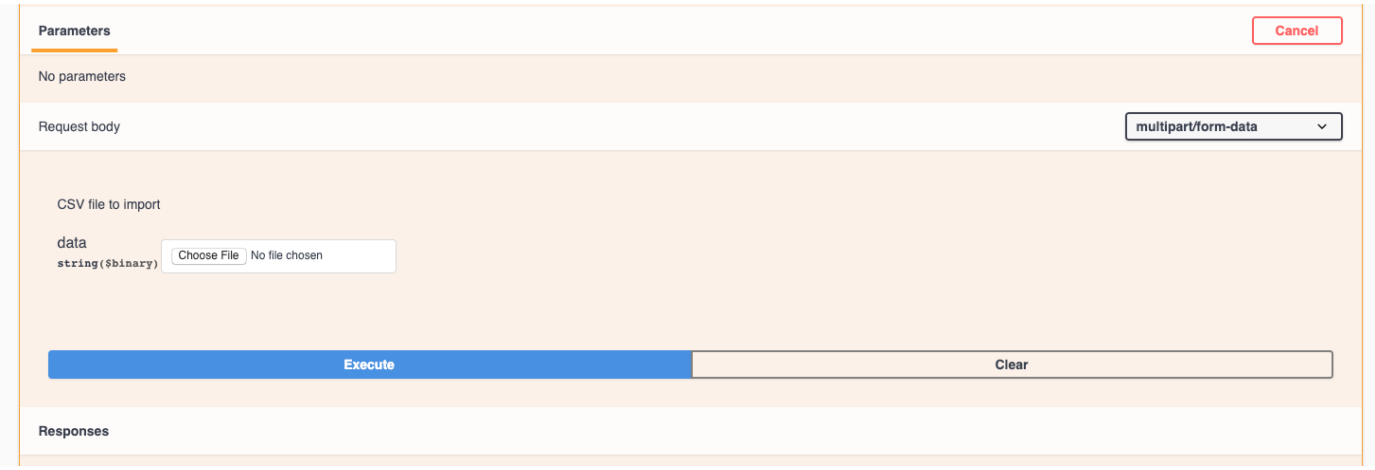
Die Links **Admin > API Access** enthalten "Dokumentation" Für die API **Assets/Import**. Diese Dokumentation enthält Informationen zum CSV-Dateiformat.

.CSV-Dateiformat

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

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

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



Importverhalten

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

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

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

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

Die folgenden Objekttypen können mit Anmerkungen versehen werden.

OBJEKTTYP	NAME ODER TASTE
Host	id-><id>, <Name> oder <IP>
VM	id-><id> oder <Name>

Storage Pool	id-><id> oder <Storage Name>-><Storage Pool Name>
InternalVolume	id-><id> oder <Storage Name>-><Name des internen Volumes>
Datenmenge	id-><id> oder <Storage Name>-><Volume Name>
Storage	id-><id>, <Name> oder <IP>
Switch	id-><id>, <Name> oder <IP>
Port	id-><id> oder <WWN>
Qtree	id-><id> oder <Storage Name>-><Name des internen Volumes>-><Qtree Name>
Share	id-><id> oder <Storage Name>-><Name des internen Volumes>-><Name der Freigabe>-><Protokoll>[-><Qtree-Name (optional im Fall von qtree Standard)>]

Arbeiten mit Anwendungen

Nachverfolgung der Asset-Nutzung nach Applikation

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

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

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

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

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

1. Erstellen Sie eine Anwendung mit dem Namen *Exchange*

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

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

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

Anwendungen Werden Erstellt

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Observability > Enrich > Applications**. Wählen Sie

   Das Dialogfeld Anwendung hinzufügen wird angezeigt.

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

Nach dem Definieren einer Anwendung kann sie Assets zugewiesen werden.

Zuweisen von Anwendungen zu Assets

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

Schritte

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

Neue Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem

anderen Asset abgeleitet wurden. Beispielsweise übernehmen Volumes Applikationen von Hosts, und wenn neuen Applikationen einem Volume zugewiesen werden, hat die neue Applikation Vorrang vor der abgeleiteten Applikation.

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

Nachdem Sie fertig sind

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

Automatische Geräteauflösung

Überblick Über Die Automatische Geräteauflösung

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

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

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

- Physische Hosts
- Storage-Arrays durchführt
- Bänder

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

Die wiederum erstellten Regeln identifizieren automatisch neue Geräte mit ähnlichen Attributen, wie sie Ihrer Umgebung hinzugefügt werden. In einigen Fällen ermöglicht die Geräteauflösung auch die manuelle Identifizierung, wobei die Regeln für die Geräteauflösung für nicht erkannte Geräte in Data Infrastructure Insights umgangen werden.

Eine unvollständige Identifizierung von Geräten kann zu folgenden Problemen führen:

- Unvollständige Pfade
- Nicht identifizierte Multipath-Verbindungen
- Applikationen können nicht gruppieren
- Ungenaue Topologieansichten

- Ungenaue Daten im Data Warehouse und Berichterstellung

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

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

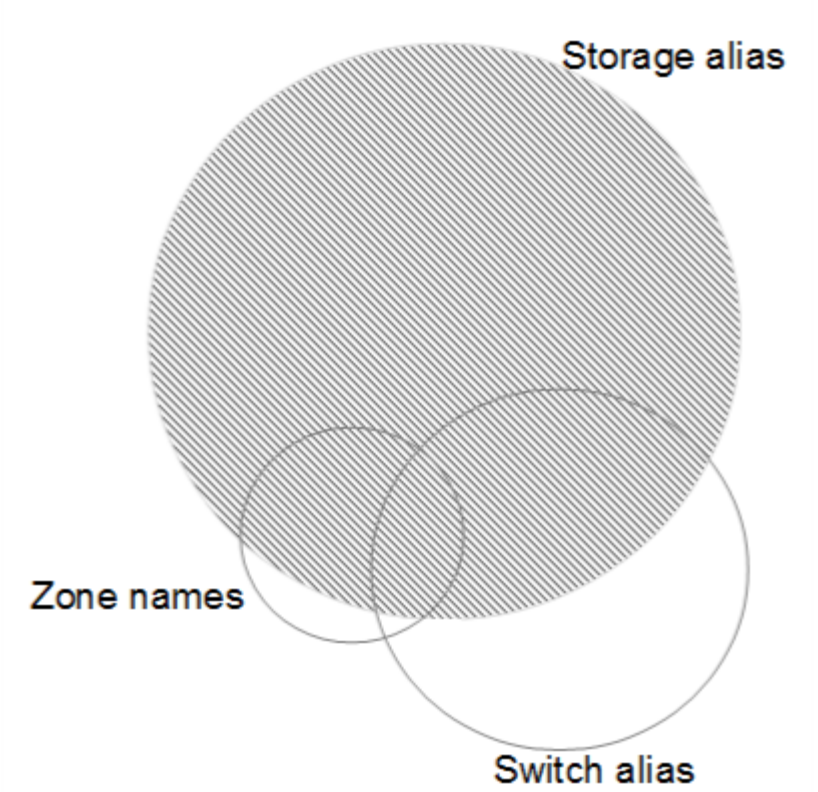
Bevor Sie Beginnen

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

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

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

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



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

Schritte zur Identifizierung von Geräten

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

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

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

Verwandte Themen:"Geräterauflösungsregeln Werden Erstellt"
"Fibre Channel-Geräteauflösung"
"IP-Geräteauflösung"

"Einstellen Der Einstellungen Für Die Geräteauflösung"

Regeln zur Geräterauflösung

Sie erstellen Regeln für die Geräteauflösung, um Hosts, Speicher und Bänder zu identifizieren, die derzeit von Data Infrastructure Insights nicht automatisch erkannt werden. Die Regeln, die Sie erstellen, identifizieren Geräte, die sich derzeit in Ihrer Umgebung befinden, und identifizieren ähnliche Geräte, die Ihrer Umgebung hinzugefügt werden.

Geräterauflösungsregeln Werden Erstellt

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

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

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

Verfahren

1. Klicken Sie Auf **Verwalten > Geräteauflösung**
2. Klicken Sie auf der Registerkarte **Regeln zur automatischen Auflösung** auf **+ Hostregel** oder **+ Bandregel**.

   Der Bildschirm **Auflösungsregel** wird angezeigt.

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

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

   Sie können *Host* oder *Band* auswählen.

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

   Je nach gewählter Quelle zeigt Data Infrastructure Insights die folgende Antwort an:

   a. **Zonen** listet die Zonen und WWN auf, die durch Data Infrastructure Insights identifiziert werden müssen.
   b. **SRM** listet die nicht identifizierten Aliase auf, die durch Data Infrastructure Insights identifiziert werden müssen

c. **Storage Alias** listet Speicheraliase und WWN auf, die durch Data Infrastructure Insights identifiziert werden müssen

d. **Switch Alias** listet die Switch-Aliase auf, die durch Data Infrastructure Insights identifiziert werden müssen

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

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

   - Für Regeln, die Trennzeichen verwenden, sind die Trennzeichen und die Mindestlänge des Hostnamens erforderlich. Die Mindestlänge des Hostnamens ist die Anzahl der Zeichen, die Data Infrastructure Insights zur Identifizierung eines Hosts verwenden sollte. Data Infrastructure Insights führt DNS-Suchvorgänge nur für Hostnamen aus, die so lange oder länger sind.

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

     - Vipsnq03_hba3_emc3_12ep0
     - Vipsnq03_hba3_emc3
     - Hba3 emc3_12ep0
     - Vipsnq03_hba3
     - Emc3_12ep0
     - Hba3_emc3
     - Vipsnq03
     - 12ep0
     - Emc3
     - Hba3
   - Regeln, die reguläre Ausdrücke verwenden, erfordern einen regulären Ausdruck, das Format und die Empfindlichkeitsauswahl für Fälle.

6. Klicken Sie auf **Run AR**, um alle Regeln auszuführen, oder klicken Sie auf den Pfeil nach unten in der Schaltfläche, um die von Ihnen erstellte Regel (und alle anderen Regeln, die seit der letzten vollständigen Ausführung von AR erstellt wurden) auszuführen.

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

Starten einer automatischen Aktualisierung der Geräteauflösung

Ein Update zur Geräteauflösung setzt manuelle Änderungen fest, die seit der letzten vollständigen

automatischen Gerätelaufauflösung hinzugefügt wurden. Das Ausführen eines Updates kann verwendet werden, um nur die neuen manuellen Einträge für die Konfiguration der Geräteauflösung zu übergeben und auszuführen. Es wird keine vollständige Gerätelaufauflösung durchgeführt.

Verfahren

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

Regelgestützte manuelle Identifizierung

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

Bevor Sie beginnen

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

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

Verfahren

1. Melden Sie sich bei der Web-UI 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 Identify-Bildschirm an, der eine Liste aller Regeln enthält, die Geräte erfolgreich identifiziert haben.

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

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

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

Data Infrastructure Insights führt den Prozess der Hostauflösung in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit den Methoden oben.

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

Verwandte Themen:"Fibre Channel-Geräteauflösung"
"IP-Geräteauflösung"

"Einstellen Der Einstellungen Für Die Geräteauflösung"

Fibre Channel-Geräteauflösung

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

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

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

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

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

Manuelles Hinzufügen eines Fibre-Channel-Geräts

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

Bevor Sie beginnen

Zum erfolgreichen Hinzufügen einer Geräteidentifikation zum System müssen Sie die WWN- oder IP-Adresse und den Gerätenamen kennen.

Über diese Aufgabe

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

Verfahren

1. Melden Sie sich bei der Web-UI von Data Infrastructure Insights an
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte * Fibre Channel Identify*.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Dialogfeld **Gerät hinzufügen** wird angezeigt

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

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

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

Sie können die Identifizierung von Fibre-Channel-Geräten manuell in die Geräteauflösung von Data Infrastructure Insights importieren, indem Sie eine Liste von Geräten in einer CSV-Datei verwenden.

1. Bevor Sie beginnen

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

WWN	IP	Name	Typ

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

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

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

Um Fibre Channel zu importieren, identifizieren Sie Informationen:

1. Melden Sie sich bei der Web-UI von Data Infrastructure Insights an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte * Fibre Channel Identify* aus.
4. Klicken Sie auf die Schaltfläche * Identifizieren > aus Datei identifizieren*.
5. Navigieren Sie zu dem Ordner, der Ihre .CSV-Dateien zum Importieren enthält, und wählen Sie die gewünschte Datei aus.

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

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

Sie können vorhandene Fibre-Channel-Gerätekennungen aus der Funktion Data Infrastructure Insights Geräteauflösung in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können. Dort werden dann Geräte identifiziert, die denen ähneln, die ursprünglich mit der exportierten Identifizierung übereinstimmen.

Über diese Aufgabe

Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die einfach in der .CSV-Datei

bearbeitet und dann wieder in das System importiert werden können.

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

WWN	IP	Name	Typ

Verfahren

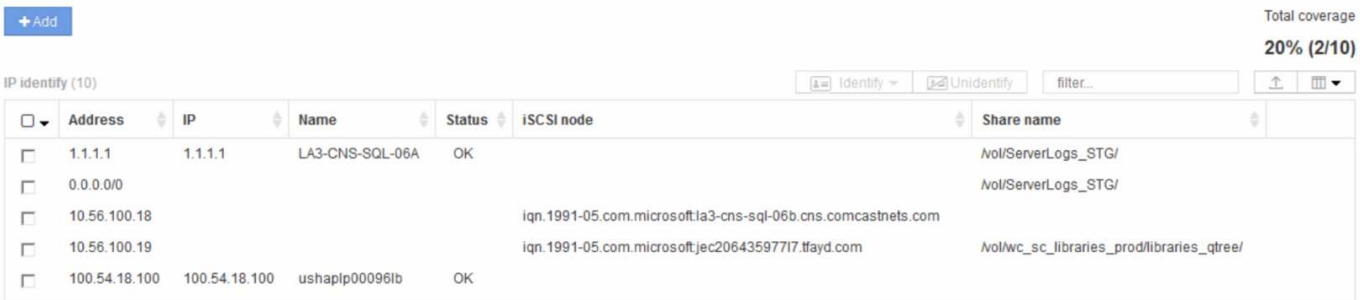
1. Melden Sie sich bei der Web-UI von Data Infrastructure Insights an.
2. Klicken Sie Auf **Verwalten > Geräteauflösung**
3. Wählen Sie die Registerkarte * Fibre Channel Identify* aus.
4. Wählen Sie das Fibre-Channel-Gerät oder die Geräte aus, deren Kennung Sie exportieren möchten.
5. Klicken Sie auf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

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

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

IP-Geräteauflösung

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



Manuelles Hinzufügen von IP-Geräten

Sie können Data Infrastructure Insights manuell ein IP-Gerät hinzufügen, indem Sie die manuelle Add-Funktion verwenden, die im Bildschirm IP Identify verfügbar ist.

Verfahren

1. Melden Sie sich bei der Web-UI von Data Infrastructure Insights an.
2. Klicken Sie auf **Verwalten > Geräteauflösung**
3. Klicken Sie auf die Registerkarte * IP-Adresse identifizieren*.

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Dialogfeld Gerät hinzufügen wird angezeigt

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

Ergebnis

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

Importieren der IP-Geräteidentifizierung aus einer .CSV-Datei

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

1. Bevor Sie beginnen

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

Adresse	IP	Name

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

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

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

Exportieren der IP-Gerätekennung in eine CSV-Datei

Sie können vorhandene IP-Gerätekennungen aus der Funktion Data Infrastructure Insights Geräteauflösung in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Data Infrastructure Insights importieren können. Dort werden dann Geräte identifiziert, die denen ähneln, die ursprünglich mit der exportierten Identifizierung übereinstimmen.

Über diese Aufgabe

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

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

Adresse	IP	Name

Verfahren

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

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

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

Einstellungen auf der Registerkarte Einstellungen

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

Zeitplan für die automatische Auflösung

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

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

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

DNS-Verarbeitungsoptionen

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

- Wenn die Verarbeitung der DNS-Suchtresultat aktiviert ist, können Sie eine Liste von DNS-Namen hinzufügen, die an aufgelöste Geräte angehängt werden sollen.
- Sie können die Option Automatische Auflösung von IPs auswählen: Ermöglicht die automatische Hostauflösung für iSCSI-Initiatoren und Hosts, die über DNS-Lookup auf NFS-Freigaben zugreifen. Wenn dies nicht angegeben wird, wird nur FC-basierte Auflösung ausgeführt.

- Sie können Unterstriche in Hostnamen zulassen und anstelle des Standard-Port-Alias in Results einen Alias „Connected to“ verwenden.

Einschließlich oder mit Ausnahme bestimmter Storage- und Tape-Anbieter

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

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

Siehe auch: "Beispiele Für Reguläre Ausdrücke"

Beispiele für reguläre Ausdrücke

Wenn Sie den Ansatz für reguläre Ausdrücke als Namensstrategie für die Quelle 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 von regulären Ausdrücken

Wenn Sie reguläre Ausdrücke für die automatische Auflösung von Data Infrastructure Insights erstellen, können Sie das Ausgabeformat konfigurieren, indem Sie Werte in ein Feld namens *FORMAT* eingeben.

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

Möglicherweise haben Sie beispielsweise die folgenden Zonennamen für diese Zonenbenennung:

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

Möglicherweise soll die Ausgabe im folgenden Format vorliegen:

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

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

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

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

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

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

Beispiele

Beispiel 1 mit Zonennamen

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

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

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

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

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

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

Beispiel 2

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

ZONE: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

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

Beispiel 3

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

ZONE: A_VSAN3_SR48KENT_A_CX2578_SPA0

Hostname: SR48KENT

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

Beispiel 4 zeigt ein komplizierteren Benennungsmuster

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

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

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

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

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

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

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

Beispiel 5 zeigt Zonennamen ohne Muster an

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

- MyComputerName_HBA1_Symm1_FA1
- MyComputerName123_HBA1_Symm1_FA1

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

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

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

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

Beispiel 6 zeigt Computernamen mit einem Muster an

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

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

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

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

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.
- Die ? Charakter macht den Match nicht-gierig. Dies zwingt es, beim ersten Unterstrich nicht beim letzten zu stimmen.
- Das Unterstrich-Zeichen entspricht dem ersten Unterstrich im Zonennamen.
- Somit entspricht die erste Kombination .*?_ den Zeichen Storage1_ im Beispiel des ersten Zonennamens.
- Die zweite Kombination .*?_ verhält sich wie die erste, stimmt aber im Beispiel für den Namen der ersten Zone mit Switch1_ überein.
- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Die Klammern [A-ZA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig vom Fall) oder jede Ziffer übereinstimmen wird.

- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die Klammern im regulären Ausdruck [ABT] entsprechen einem einzelnen Zeichen im Zonennamen, das A, B oder T. sein muss
- Der _ (Unterstrich) nach den Klammern zeigt an, dass der [ABT]-Zeichenabgleiche einen Unterstrich nachgehen muss.
- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.

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

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

Beispiel 7

Zone: myComputerName123_HBA1_Symm1_FA1

Hostname: myComputerName123

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

Beispiel 8

Dieses Beispiel findet alles vor dem ersten _.

Zone: MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname: MyComputerName

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

Beispiel 9

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

Zone: Z_MyComputerName_StorageName

Hostname: MyComputerName

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

Beispiel 10

Dieses Beispiel extrahiert „MyComputerName123“ aus den Zonenbeispielen.

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Hostname: MyComputerName123

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

Beispiel 11

Zone: Storage1_Switch1_MyComputerName123A_A1_FC1

Hostname: MyComputerName123A

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

Beispiel 12

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

Zone: mhs_apps44_d_A_10a0_0429

Hostname: mhs-apps44-d

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

Beispiel 13

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

Speicheralias: \Hosts\E2DOC01C1\E2DOC01N1

Hostname: E2DOC01N1

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

Beispiel 14

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

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

HOSTNAME: PD-RV-W-AD-2

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

Beispiel 15

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

ZONE: SRV_USBVM11_F1

HOSTNAME: US-BV-M11

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

Format: US-BV-\1

Informationen Zur Asset-Seite

Übersicht Über Die Asset-Seite

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

Arten von Asset-Seiten

Data Infrastructure Insights bietet Asset-Seiten für die folgenden Ressourcen:

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

Ändern des Zeitbereichs der angezeigten Daten

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

Sie können das Zeitsegment der angezeigten Daten ändern, indem Sie eine Option verwenden, die sich auf jeder Asset-Seite befindet, unabhängig vom Asset-Typ. Um den Zeitbereich zu ändern, klicken Sie in der oberen Leiste auf den angezeigten Zeitbereich, und wählen Sie zwischen den folgenden Zeitsegmenten aus:

- Letzte 15 Minuten
- Letzte 30 Minuten
- Letzte 60 Minuten
- Die Letzten 2 Stunden
- Die letzten 3 Stunden (dies ist die Standardeinstellung)
- Letzte 6 Stunden

- Letzte 12 Stunden
- Letzte 24 Stunden
- Letzte 2 Tage
- Letzte 3 Tage
- Letzte 7 Tage
- Letzte 30 Tage
- Benutzerdefinierter Zeitbereich

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

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

Benutzerdefinierte Widgets Hinzufügen

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

Filtern nach Objekten im Kontext

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

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

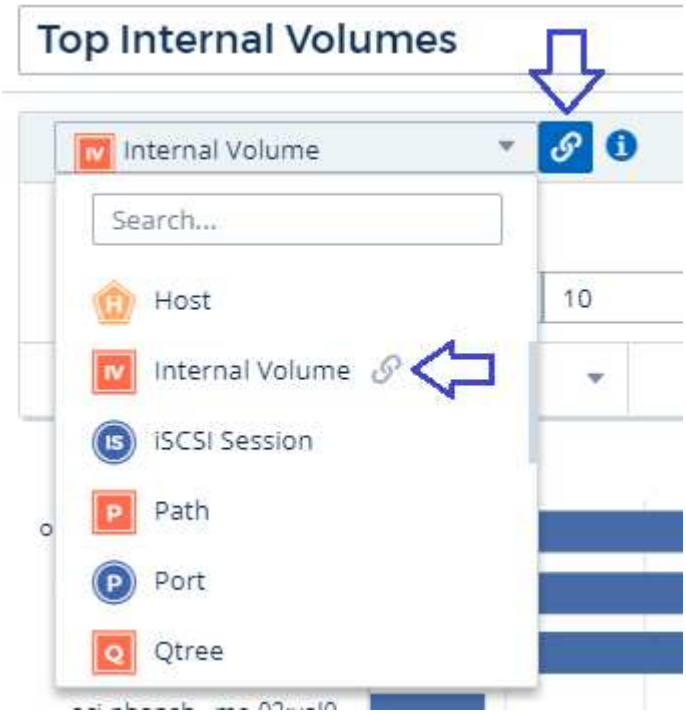
Beispielsweise können Sie auf einer Storage Asset-Seite ein Balkendiagramm-Widget hinzufügen, um die wichtigsten IOPS nur für interne Volumes auf diesem Storage anzuzeigen. Standardmäßig werden beim Hinzufügen eines Widgets *alle* interne Volumes in Ihrer Umgebung angezeigt.

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

Schritte

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

Symbol „Verknüpfung“ ist standardmäßig aktiviert.



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

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

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

Um die Verknüpfung der Objektdaten 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 in Ihrer Umgebung an.

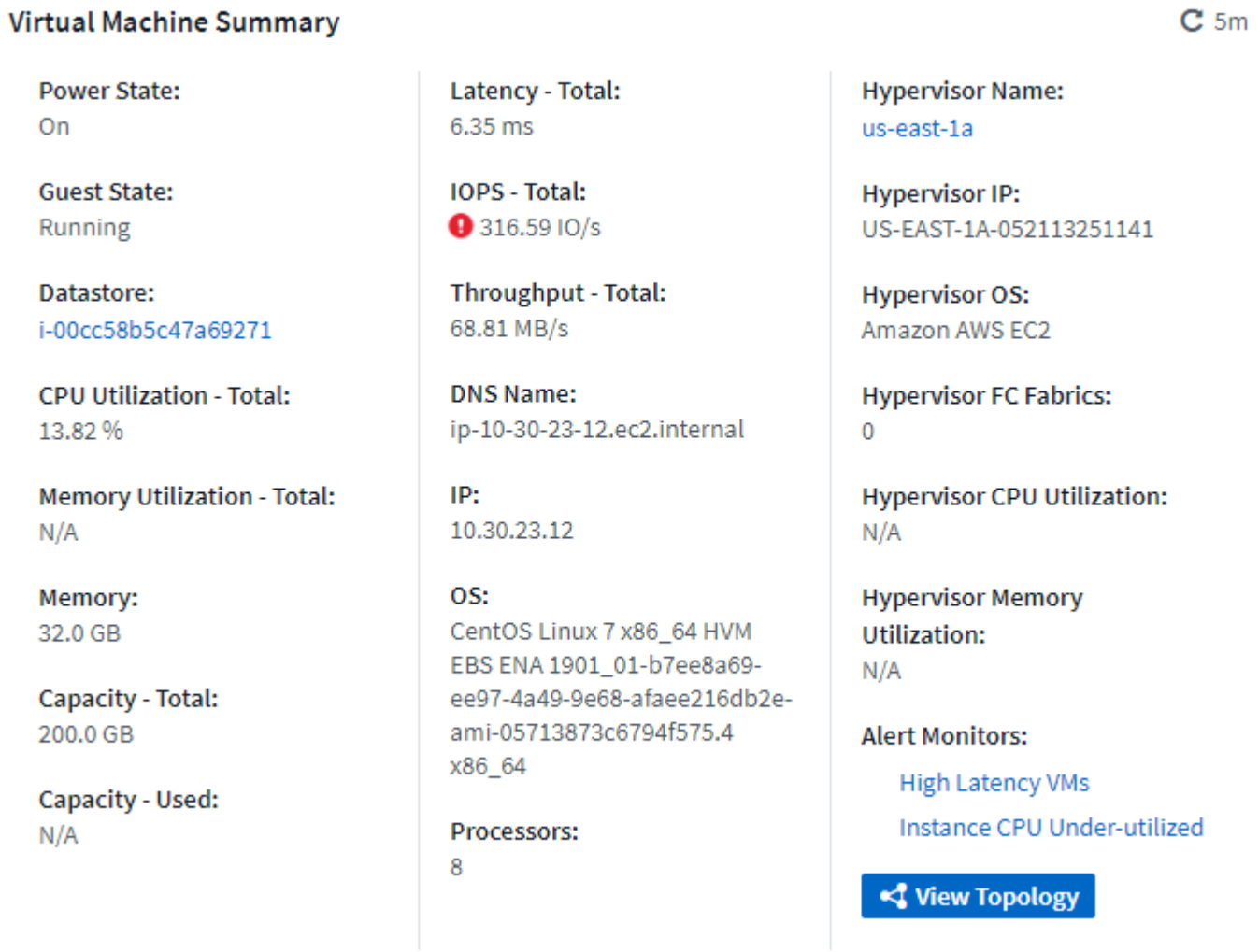
Sie können auch verwenden **"Sondervariablen in Widgets"** Um Asset-bezogene Informationen auf Landing Pages anzuzeigen.

Abschnitt „Ressourcen-Seite-Übersicht“

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

Die Informationen in der Zusammenfassung sowie in beliebigen Tabellen oder benutzerdefinierten Widgets auf

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



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

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

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

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

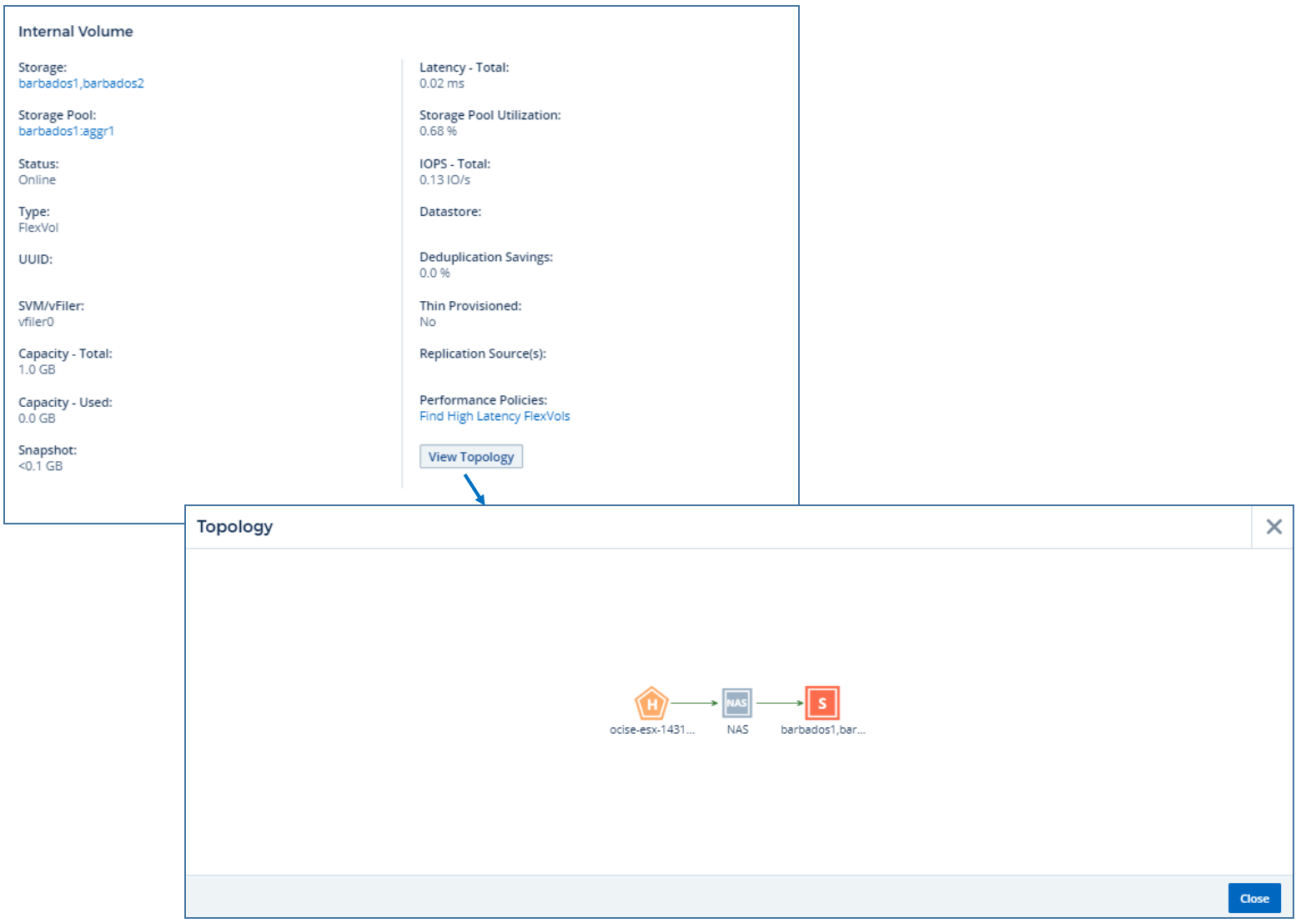
Falls zutreffend, können Sie auf einen Warnlink klicken, um die mit dem Gerät verknüpfte Warnung und den Monitor anzuzeigen.

Topologie

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

Die Topologie ist für die folgenden Asset-Typen verfügbar:

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

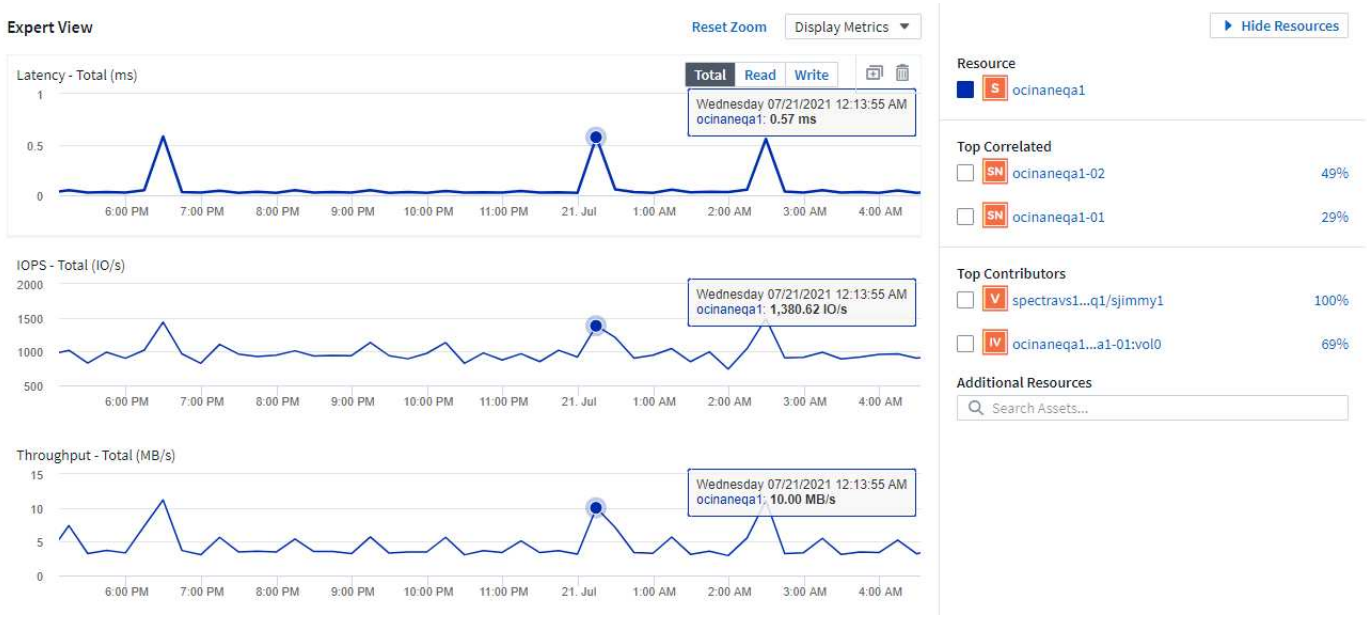


Expertensicht

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

Verwenden des Abschnitts „Expertenansicht“

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



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

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

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

- Oben korreliert

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

- Top-Mitwirkende

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

- Workload-Konflikte

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

Warnmeldungen in der Ansicht „Experten“

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

Metrische Definitionen der Expertenansicht

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

Metrisch	Beschreibung
BB Credit Null Rx, Tx	Die Anzahl der Empfangs-/Übertragungs-Buffer-zu-Buffer-Gutschriften wurde während des Probenzeitraums auf Null übertragen. Diese Metrik gibt an, wie oft der angeschlossene Port die Übertragung beenden musste, da dieser Port nicht mehr als Credits zur Verfügung stand.
BB Kredit Null Dauer Tx	Zeit in Millisekunden, während der der transmit BB-Guthaben während des Abtastintervalls null war.
Cache-Trefferverhältnis (gesamt, Lesen, Schreiben) %	Prozentsatz von Anforderungen, die zu Cache-Treffern führen. Je höher die Anzahl der Treffer im Vergleich zum Volume ist, desto besser ist die Performance. Diese Spalte ist leer für Speicher-Arrays, die keine Cache-Trefferinformationen erfassen.
Cache-Auslastung (gesamt) %	Gesamtprozentsatz der Cacheanforderungen, die zu Cache-Treffern führen
Discards der Klasse 3	Anzahl der Rückwürfe für die Datenübertragung in der Fibre Channel-Klasse 3

CPU-Auslastung (gesamt) %	Menge der aktiv genutzten CPU-Ressourcen als Prozentsatz der insgesamt verfügbaren (über alle virtuellen CPUs)
CRC-Fehler	Anzahl der Frames mit ungültigen zyklischen Redundanzprüfungen (CRCs), die vom Port während des Probenahmezeitraums erkannt wurden
Frame-Rate	Bildrate in Bildern pro Sekunde übertragen (FPS)
Bildgröße durchschnittlich (Rx, Tx)	Verhältnis von Datenverkehr zu Bildgröße. Mit dieser Metrik können Sie feststellen, ob es Overhead Frames in der Fabric gibt.
Rahmengröße zu lang	Anzahl der zu langen Fibre Channel-Datenübertragungsrahmen
Rahmengröße zu kurz	Anzahl der zu kurzen Fibre Channel-Datenübertragungsrahmen
I/O-Dichte (gesamt, Lesen, Schreiben)	Anzahl der IOPS geteilt durch genutzte Kapazität (wie bei der letzten Inventarabfrage der Datenquelle erworben) für das Element Volume, Internal Volume oder Storage. Diese wird anhand der Anzahl der I/O-Vorgänge pro Sekunde pro TB gemessen.
IOPS (gesamt, Lesen, Schreiben)	Anzahl der Lese-/Schreib-I/O-Serviceanfragen, die den I/O-Kanal oder einen Teil dieses Kanals pro Zeiteinheit durchlaufen (gemessen in I/O pro Sekunde)
IP-Durchsatz (gesamt, Lesen, Schreiben)	Gesamt: Aggregierte Rate, bei der IP-Daten in Megabyte pro Sekunde übertragen und empfangen wurden.
Lesen: IP-Durchsatz (Empfangen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde empfangen wurden.
Schreiben: IP-Durchsatz (übertragen):	Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde übertragen wurden.
Latenz (Gesamt, Lesen, Schreiben)	Latenz (R&W): Geschwindigkeit, mit der Daten in einem festgelegten Zeitraum gelesen oder auf die Virtual Machines geschrieben werden Der Wert wird in Megabyte pro Sekunde gemessen.
Latenz	Durchschnittliche Antwortzeit von den Virtual Machines in einem Datenspeicher.
Höchste Latenz:	Die höchste Reaktionszeit von den Virtual Machines in einem Datenspeicher.
Verbindungsfehler	Anzahl der Verbindungsfehler, die der Port während des Probenahmezeitraums entdeckt hat.
Link Reset Rx, Tx	Anzahl der Rücksetzungen von Empfangs- oder Übertragungsverbindung während des Probenzeitraums. Diese Metrik gibt die Anzahl der vom angeschlossenen Port an diesen Port ausgegebenen Link-Resets an.

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

Ausstehende Schreibvorgänge (Gesamt)	Anzahl der ausstehenden Schreib-I/O-Serviceanfragen.

Verwenden des Abschnitts „Expertenansicht“

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

Schritte

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

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

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

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

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

3. Sie können den Cursor über das Diagramm positionieren und die für das Diagramm angezeigten metrischen Daten ändern, indem Sie je nach Anlage auf eine der folgenden Optionen klicken:
   - Lesen, Schreiben oder Gesamt
   - TX, Rx oder Total

     Die Gesamtsumme ist die Standardvorgabe.

   Sie können den Cursor über die Datenpunkte im Diagramm ziehen, um zu sehen, wie sich der Wert der Metrik im ausgewählten Zeitraum ändert.

4. Im Abschnitt Ressourcen können Sie den Leistungsdiagrammen alle zugehörigen Assets hinzufügen:
   - Sie können eine zugehörige Ressource in den Abschnitten **Top Correlated**, **Top Contributors**, **Greedy** und **degraded** auswählen, um Daten aus dieser Ressource in das Leistungsdiagramm für jede ausgewählte Metrik hinzuzufügen.

     Nachdem Sie das Element ausgewählt haben, wird neben dem Element ein Farbblock angezeigt, der die Farbe seiner Datenpunkte im Diagramm kennzeichnet.

5. Klicken Sie auf **Ressourcen ausblenden**, um das Fenster zusätzliche Ressourcen auszublenden. Klicken Sie auf **Ressourcen**, um das Fenster anzuzeigen.
    - Für alle angezeigten Assets können Sie auf den Namen des Assets klicken, um die Seite des Assets anzuzeigen. Sie können auch auf den Prozentsatz klicken, der das Asset korreliert oder zum Basisspital beiträgt, um weitere Informationen über die Beziehung des Assets zum BasisinAsset anzuzeigen.

      Wenn Sie beispielsweise auf den verknüpften Prozentsatz neben einem Top-korrelierten Asset klicken, wird eine Informationsmeldung angezeigt, die den Typ der Korrelation zwischen der Anlage und der Basisinressource vergleicht.

    - Wenn der Abschnitt „Top Correlated“ keine Anlage enthält, die in einem Leistungsdiagramm zum Vergleich angezeigt werden soll, können Sie im Abschnitt „zusätzliche Ressourcen“ das Feld „Assets suchen“ verwenden, um andere Assets zu finden.

Nachdem Sie ein Asset ausgewählt haben, wird es im Abschnitt zusätzliche Ressourcen angezeigt. Wenn Sie keine Informationen mehr über das Asset anzeigen möchten, klicken Sie auf das Papierkorb-Symbol, um es zu löschen.

Abschnitt „Benutzerdaten“

Der Abschnitt „Benutzerdaten“ einer Asset-Seite wird angezeigt und ermöglicht das Ändern benutzerdefinierter Daten wie Anwendungen und Anmerkungen.

Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anwendungen

Sie können Applikationen, die in Ihrer Umgebung ausgeführt werden, bestimmten Assets (Host, Virtual Machines, Volumes, interne Volumes, qtrees, Und Hypervisoren). Im Abschnitt „Benutzerdaten“ können Sie die Anwendungen hinzufügen, ändern oder entfernen, die einem Asset zugewiesen sind. Für alle diese Asset-Typen außer für Volumes können Sie mehr als eine Anwendung zuweisen.

Schritte

1. Suchen Sie eine Asset-Seite, indem Sie einen der folgenden Schritte ausführen:
    a. Abfrage nach einer Liste von Assets, und wählen Sie dann eine aus der Liste aus.
    b. Suchen Sie in einem Dashboard nach einem Asset-Namen, und klicken Sie darauf.
    c. Führen Sie eine Suche durch, und wählen Sie aus den Ergebnissen eine Anlage aus.

       Die Seite Anlage wird angezeigt. Im Abschnitt „Benutzerdaten“ auf der Seite werden aktuell zugewiesene Anwendungen oder Anmerkungen angezeigt.

Um die zugewiesene Anwendung zu ändern oder eine Anwendung oder weitere Anwendungen zuzuweisen, klicken Sie auf die Liste **Anwendung** und wählen Sie die Anwendung(en) aus, die Sie dem Asset zuweisen möchten. Sie können eingeben, um nach einer Anwendung zu suchen, oder eine aus der Liste auswählen.

Um eine Anwendung zu entfernen, legen Sie die Anwendungsliste herunter und deaktivieren Sie die Prüfung der Anwendung.

Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anmerkungen

Wenn Sie Data Infrastructure Insights an Ihre Unternehmensanforderungen anpassen, um Daten nachzuverfolgen, können Sie spezielle Notizen als Anmerkungen definieren und sie Ihren Ressourcen zuweisen. Im Abschnitt „Benutzerdaten“ einer Asset-Seite werden Anmerkungen angezeigt, die einem Asset

zugeordnet sind, und Sie können auch die Anmerkungen ändern, die diesem Asset zugewiesen sind.

Schritte

1. Um dem Asset eine Anmerkung hinzuzufügen, klicken Sie im Bereich Benutzerdaten auf der Asset-Seite auf **+Annotation**.
2. Wählen Sie eine Anmerkung aus der Liste aus.
3. Klicken Sie auf „Wert“ und führen Sie eine der folgenden Aktionen aus, je nachdem, welche Anmerkungstypen Sie ausgewählt haben:
   a. Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   b. Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
4. Klicken Sie auf Speichern .

Die Anmerkung wird dem Asset zugewiesen. Sie können Assets später mithilfe einer Abfrage nach Anmerkungen filtern.

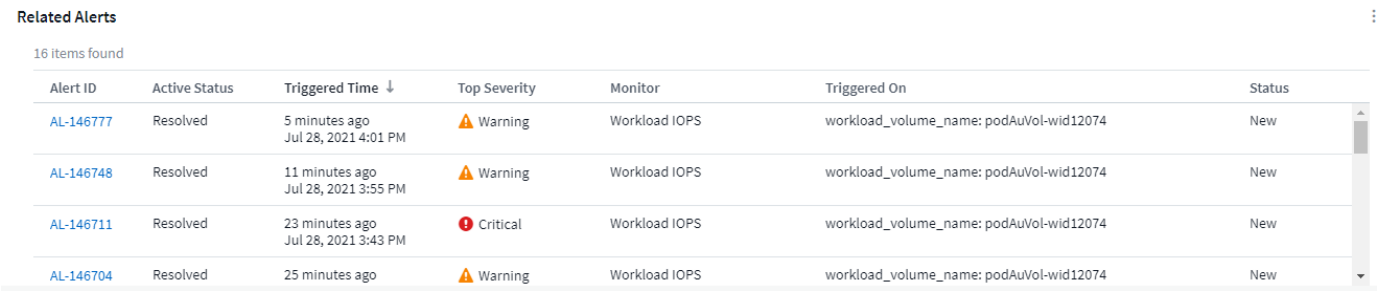
Wenn Sie den Wert der Anmerkung nach der Zuweisung ändern möchten, lassen Sie die Anmerkungsliste herunter und geben einen anderen Wert ein.

Wenn die Anmerkung vom Listentyp ist, für den die Option *neue Werte hinzufügen auf der Fly* ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Wertes einen neuen Wert hinzufügen.

Abschnitt „Hinweise auf der Seite „Ressourcen“

Sie können den Abschnitt „Verwandte Warnungen“ einer Asset-Seite verwenden, um alle Warnmeldungen anzuzeigen, die in Ihrer Umgebung als Ergebnis eines Monitors auftreten, der einem Asset zugewiesen ist. Monitore generieren Warnungen auf der Grundlage von festgelegten Bedingungen. So können Sie Implikationen identifizieren und die Auswirkungen und Ursache des Problems auf eine schnelle und effektive Korrektur analysieren.

Das folgende Beispiel zeigt einen typischen Abschnitt „Verwandte Warnungen“, der auf einer Asset-Seite angezeigt wird:



Im Abschnitt „Verwandte Warnungen“ können Sie die Warnmeldungen anzeigen und verwalten, die in Ihrem Netzwerk aufgrund von Überwachungsbedingungen auftreten, die einem Asset zugewiesen sind.

Schritte

- Suchen Sie eine Asset-Seite, indem Sie einen der folgenden Schritte ausführen:
  - Geben Sie den Namen des Assets im Suchbereich ein, und wählen Sie das Element aus der Liste aus.

- Klicken Sie in einem Dashboard-Widget auf den Namen eines Assets.
- Fragen Sie nach einem Satz von Assets ab, und wählen Sie in der Ergebnisliste ein aus.

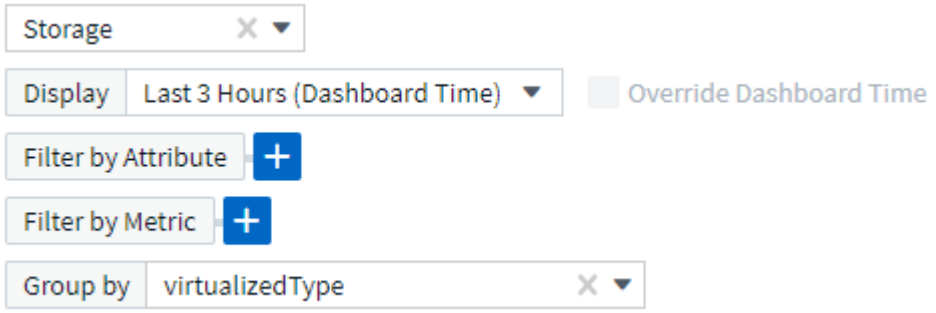
Die Seite Anlage wird angezeigt. Im Abschnitt „Verwandte Warnungen“ werden die Zeit angezeigt, zu der die Warnmeldung ausgelöst wurde, sowie der aktuelle Status der Warnmeldung und der Monitor, der sie ausgelöst hat. Sie können auf die Alarm-ID klicken, um die Landing Page für die Warnmeldung zur weiteren Untersuchung zu öffnen.

Storage-Virtualisierung

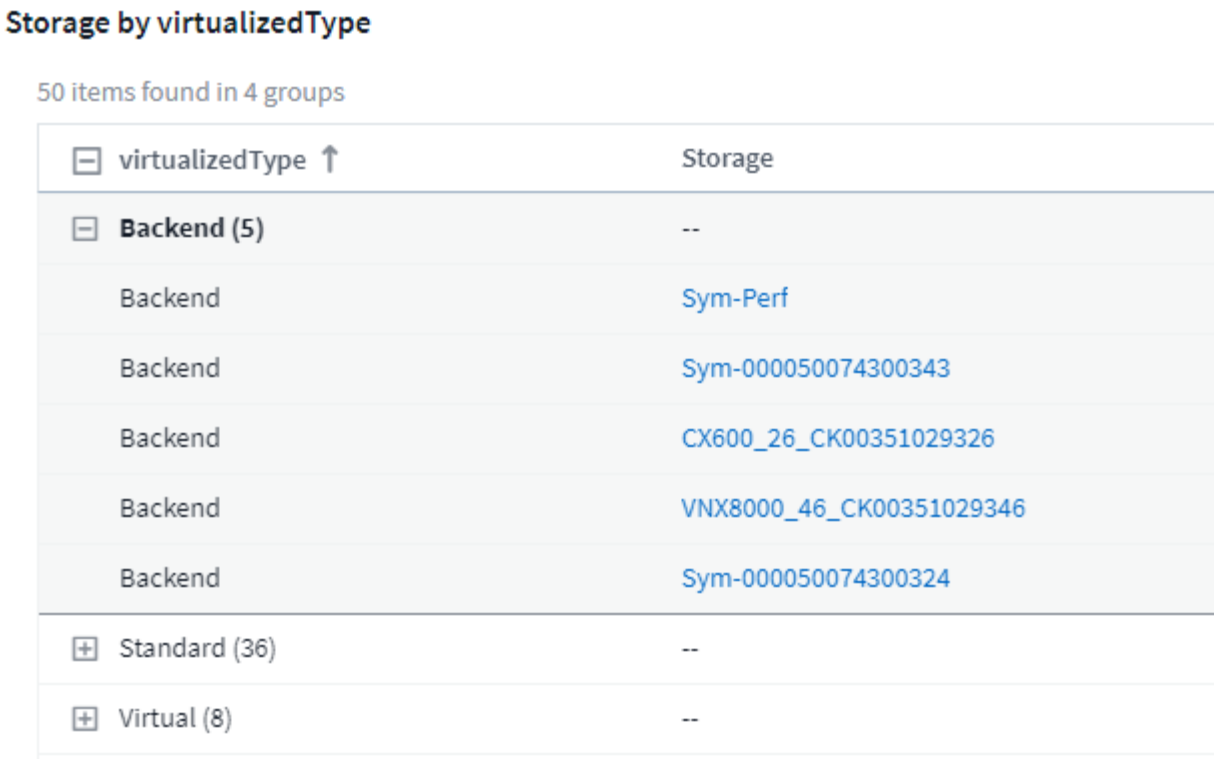
Anhand von Dateninfrastrukturdaten können Storage-Arrays mit lokalem Storage oder der Virtualisierung anderer Storage-Arrays unterschieden werden. So können Sie Kosten nachvollziehen und die Performance vom Front-End bis zum Back-End Ihrer Infrastruktur differenzieren.

Widget „Virtualisierung in einer Tabelle“

Eine der einfachsten Möglichkeiten zur Betrachtung Ihrer Storage-Virtualisierung ist die Erstellung eines Dashboard-Tabellen-Widgets mit virtualisierter Art. Wenn Sie die Abfrage für das Widget erstellen, fügen Sie einfach „virtualizedType“ zu Ihrer Gruppierung oder Ihrem Filter hinzu.

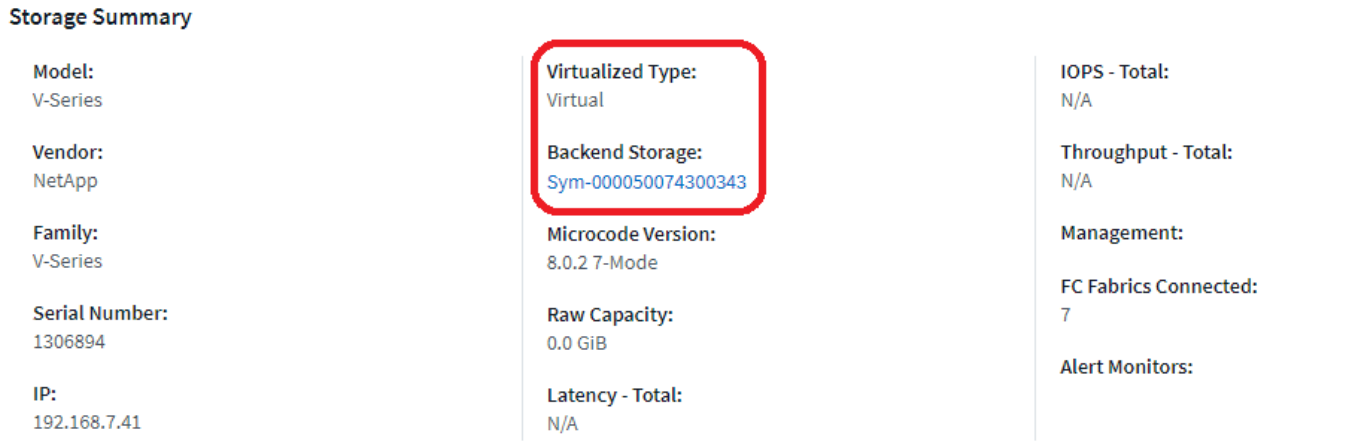


Das resultierende Tabellen-Widget zeigt Ihnen die *Standard*, *Backend* und *Virtual* Speicher in Ihrer Umgebung.



Landing Pages zeigen virtualisierte Informationen an

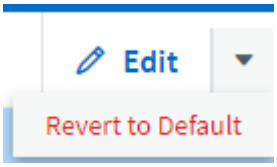
Auf einer Storage-, Volume-, internen Volume- oder Disk-Landing Page können Sie die relevanten Virtualisierungsinformationen sehen. Wenn Sie beispielsweise auf der unten stehenden Storage-Landing Page sehen, sehen Sie, dass es sich um einen virtuellen Storage handelt und welches Back-End-Storage-System angewendet wird. Alle relevanten Tabellen auf Landing-Pages enthalten je nach Bedarf auch Virtualisierungsinformationen.



Vorhandene Landing Pages und Dashboards

Beachten Sie, dass wenn Sie derzeit benutzerdefinierte Landing Pages oder Dashboards in Ihrer Umgebung haben, diese nicht automatisch alle Virtualisierungsinformationen standardmäßig anzeigen. Sie können jedoch jedes benutzerdefinierte Dashboard oder jede Landing Page *revert to Default* (Sie müssen Ihre Anpassungen neu implementieren) oder die relevanten Widgets so ändern, dass sie die gewünschten Virtualisierungsattribute oder Metriken enthalten.

Auf Standard zurücksetzen ist in der oberen rechten Ecke eines benutzerdefinierten Dashboard- oder Landing Page-Bildschirms verfügbar.



Tipps und Tricks für die Suche nach Ressourcen und Warnungen

Es können mehrere Suchmethoden verwendet werden, um in Ihrer überwachten Umgebung nach Daten oder Objekten zu suchen.

- **Platzhaltersuche**

  Sie können Platzhaltersuche für mehrere Zeichen mit dem * Zeichen durchführen. Zum Beispiel würde *Application*n__Application* zurückgeben.

- **Phrasen verwendet bei der Suche**

  Ein Begriff ist eine Gruppe von Wörtern, die von doppelten Anführungszeichen umgeben sind, z. B. „VNX LUN 5“. Sie können doppelte Anführungszeichen verwenden, um nach Dokumenten zu suchen, die Leerzeichen in ihren Namen oder Attributen enthalten.

- **Boolesche Operatoren**

  Mit Booleschen Operatoren ODER, UND, und, und NICHT können Sie mehrere Begriffe kombinieren, um eine komplexere Abfrage zu bilden.

  ODER

  Der OR-Operator ist der Standard-Konjunktion-Operator.

  Wenn zwischen zwei Begriffen kein Boolescher Operator vorhanden ist, wird der OPERATOR ODER verwendet.

  Der OR-Operator verknüpft zwei Begriffe und findet ein passendes Dokument, wenn einer der Termini in einem Dokument vorhanden ist.

  Beispielsweise sucht *Storage ODER netapp* nach Dokumenten, die entweder *Storage* oder *netapp* enthalten.

  Hohe Bewertungen werden an Dokumente vergeben, die den meisten Bedingungen entsprechen.

  UND

  Sie können den OPERATOR UND verwenden, um Dokumente zu suchen, in denen beide Suchbegriffe in einem einzigen Dokument vorhanden sind. Beispielsweise sucht *Storage UND netapp* nach Dokumenten, die *Storage* und *netapp* enthalten.

  Sie können anstelle des Wortes UND das Symbol **&** verwenden.

  NICHT

Wenn Sie den NICHT-Operator verwenden, werden alle Dokumente, die den Begriff nachher NICHT enthalten, von den Suchergebnissen ausgeschlossen. Beispiel: *Storage NOT netapp* sucht nach Dokumenten, die nur *Storage* und nicht *netapp* enthalten.

Anstelle des Wortes NOT können Sie das Symbol **!** verwenden.

Die Groß-/Kleinschreibung der Suche wird nicht berücksichtigt.

Suche mit indizierten Begriffen

Suchvorgänge, die mehr der indizierten Begriffe entsprechen, führen zu höheren Punktzahlen.

Der Suchstring wird in separate Suchbegriffe nach Leerzeichen aufgeteilt. Die Suchzeichenfolge „Storage aurora netapp“ ist beispielsweise in drei Schlagwörter unterteilt: „Storage“, „aurora“ und „netapp“. Die Suche wird unter Verwendung aller drei Begriffe durchgeführt. Die Dokumente, die den meisten dieser Begriffe entsprechen, haben die höchste Punktzahl. Je mehr Informationen Sie zur Verfügung stellen, desto besser sind die Suchergebnisse. Sie können zum Beispiel nach einem Storage mit dessen Namen und Modell suchen.

Die Benutzeroberfläche zeigt die Suchergebnisse für verschiedene Kategorien mit den drei besten Ergebnissen pro Kategorie an. Wenn Sie ein Objekt nicht gefunden haben, das Sie erwartet haben, können Sie weitere Termini in die Suchzeichenfolge eingeben, um die Suchergebnisse zu verbessern.

Die folgende Tabelle enthält eine Liste indizierter Begriffe, die der Suchzeichenfolge hinzugefügt werden können.

Kategorie	Indizierte Begriffe
Storage	Name des Anbieters „Storage“
Storage Pool	„storagepool“: Name der Storage-IP-Adressen der Storage-Seriennummer des Storage-Anbieters Namen von Storage-Modellen aller damit verbundenen internen Volumes-Namen aller zugehörigen Festplatten
Internes Volumen	Name des Storage IP-Adressen der Storage-Seriennummer des Storage-Anbieters Name des Storage-Modells: Namen des Storage-Pools aller damit verbundenen Shares Namen aller zugehörigen Applikationen
Datenmenge	„Volume“: Name aller internen Volumes Name des Storage-Pools Name der Storage-IP-Adressen der Storage-Seriennummer des Storage-Anbietermodells
Storage-Node	Name des Storage-IP-Adressen der Storage-Serialnummer des Storage-Anbieters, Name des Storage-Modells
Host	Name „Host“ IP-Adressen Namen aller zugehörigen Anwendungen
Datenspeicher	„Datastore“: Name der virtuellen Center-IP-Namen aller Volumes Namen aller internen Volumes

Kategorie	Indizierte Begriffe
Virtual Machines	„virtualmachine“ Name DNS Name IP-Adressen Name der Host-IP-Adressen der Hostnamen aller Datenspeicher Namen aller zugehörigen Anwendungen
Switches (normal und Kapitalwert)	„Switch“-IP-Adresse wwn-Name Seriennummer Modell Domain-ID-Name des Fabric-wwn der Fabric
Applikation	„Applikation“: Name des Mandantenbereichsprojekts der Geschäftseinheit
Tape	„Tape“-IP-Adresse Name Seriennummer Anbieter
Port	„Port“ wwn-Name
Fabric	„Fabric“ wwn-Name
Storage Virtual Machine (SVM)	Name UUID von „storagevirtualMachine“

Berichterstellung

Data Infrastructure Insights Reporting – Übersicht

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 Berichterstellung zu Data Infrastructure Insights bietet Ihnen folgende Aufgaben:

- Führen Sie einen vordefinierten Bericht aus
- Erstellen Sie einen benutzerdefinierten Bericht
- Passen Sie das Format und die Bereitstellungsmethode eines Berichts an
- Planen Sie die automatische Ausführung von Berichten
- E-Mail-Berichte
- Verwenden Sie Farben, um Schwellenwerte für Daten darzustellen

Data Infrastructure Insights Reporting kann individuelle Berichte für Bereiche wie Kostenverrechnung, Verbrauchsanalyse und Prognosen erstellen und hilft bei der Beantwortung von Fragen wie folgenden:

- Welche Bestände habe ich?
- Wo ist mein Inventar?
- Wer nutzt unsere Ressourcen?
- Wie sieht die Rückberechnung von zugewiesenem Storage für einen Geschäftsbereich aus?
- Wie lange dauert es, bis ich zusätzliche Storage-Kapazität anschaffen muss?
- Werden die Geschäftseinheiten auf die entsprechenden Storage Tiers abgestimmt?
- Inwiefern ändert sich die Storage-Zuweisung über einen Monat, ein Quartal oder ein Jahr?

Zugriff Auf Data Infrastructure Insights Reporting

Sie können auf Data Infrastructure Insights Reporting zugreifen, indem Sie im Menü auf den Link **Reports** klicken.

Sie werden zur Berichtsschnittstelle geleitet. Data Infrastructure Insights verwendet IBM Cognos Analytics für seine Reporting Engine.

Was ist ETL?

Bei der Arbeit mit Reporting hören Sie die Begriffe „Data Warehouse“ und „ETL“. ETL steht für „Extract, Transform, Load“. Der ETL-Prozess ruft die in Data Infrastructure Insights gesammelten Daten ab und wandelt die Daten in ein Format für die Verwendung in Reporting um. „Data Warehouse“ bezieht sich auf die gesammelten Daten, die für die Berichterstattung zur Verfügung stehen.

Der ETL-Prozess umfasst folgende Einzelprozesse:

- **Extract**: Daten aus Data Infrastructure Insights.
- **Transform**: Wendet Regeln oder Funktionen der Geschäftslogik auf die Daten an, während diese aus Data Infrastructure Insights extrahiert werden.
- **Load**: Speichert die umgewandelten Daten in das Data Warehouse zur Verwendung in Reporting.

Dateninfrastruktur Insights Reporting Benutzerrollen

Wenn Sie über Data Infrastructure Insights Premium Edition mit Reporting verfügen, verfügt jeder Data Infrastructure Insights-Benutzer in Ihrer Umgebung über eine Single Sign-On (SSO)-Anmeldung bei der Reporting-Anwendung (z. B. 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:

Einblicke Aus Die Dateninfrastruktur	Berichtsrolle	Reporting-Berechtigungen
Gast	Verbraucher	Es können Berichte angezeigt, geplant und erstellt sowie persönliche Einstellungen wie z. B. für Sprachen und Zeitzonen festgelegt werden. Verbraucher können keine Berichte erstellen oder administrative Aufgaben ausführen.
Benutzer	Autor	Kann alle Funktionen des Verbrauchers ausführen sowie Berichte und Dashboards erstellen und verwalten.

Verwalter	Verwalter	Kann alle Author-Funktionen sowie alle administrativen Aufgaben wie die Konfiguration von Berichten und das Herunterfahren und Neustarten von Reporting-Aufgaben ausführen.

Die folgende Tabelle zeigt die Funktionen, die den einzelnen Berichtsrollen zur Verfügung stehen.

Merkmal	Verbraucher	Autor	Verwalter
Anzeigen von Berichten auf der Registerkarte „Teaminhalt“	Ja.	Ja.	Ja.
Berichte erstellen	Ja.	Ja.	Ja.
Planen von Berichten	Ja.	Ja.	Ja.
Externe Dateien hochladen	Nein	Ja.	Ja.
Erstellen Von Jobs	Nein	Ja.	Ja.
Erstellen von Geschichten	Nein	Ja.	Ja.
Erstellen von Berichten	Nein	Ja.	Ja.
Erstellen von Paketen und Datenmodulen	Nein	Ja.	Ja.
Ausführung administrativer Aufgaben	Nein	Nein	Ja.
HTML-Element hinzufügen/bearbeiten	Nein	Nein	Ja.
Bericht mit HTML-Element ausführen	Ja.	Ja.	Ja.
Benutzerdefinierte SQL hinzufügen/bearbeiten	Nein	Nein	Ja.
Berichte mit benutzerdefiniertem SQL ausführen	Ja.	Ja.	Ja.

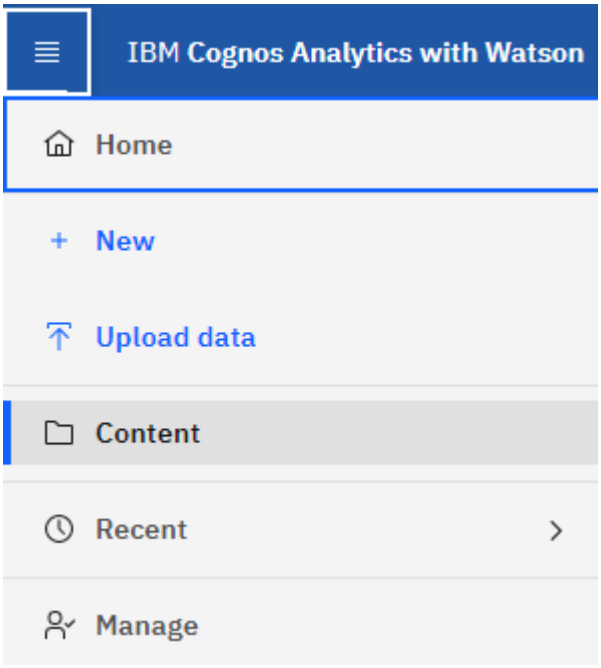
Festlegen der E-Mail-Einstellungen für Berichte (Cognos)

Wenn Sie Ihre Benutzer-E-Mail-Einstellungen in Data Infrastructure Insights Reporting (d. h. der Cognos-Anwendung) ändern, sind diese Einstellungen *only für die aktuelle Sitzung* aktiv. Wenn Sie sich bei Cognos und wieder zurück in anmelden, werden Ihre E-Mail-Einstellungen zurückgesetzt.

Welche Schritte sollte ich Unternehmen, um meine vorhandene Umgebung auf die Aktivierung von SSO vorzubereiten?

Um sicherzustellen, dass Ihre Berichte erhalten bleiben, migrieren Sie alle Berichte von *My Content* zu *Team Content*. Gehen Sie dabei wie folgt vor. Vor der Aktivierung von SSO in Ihrer Umgebung sind folgende Schritte erforderlich:

1. Navigieren Sie zu **Menü > Inhalt**



1. Erstellen Sie einen neuen Ordner in ***Team Content***
   a. Wenn mehrere Benutzer erstellt wurden, erstellen Sie für jeden Benutzer einen separaten Ordner, um zu vermeiden, dass Berichte mit doppelten Namen überschrieben werden
2. Navigieren Sie zu *My Content*
3. Wählen Sie alle Berichte aus, die Sie beibehalten möchten.
4. Wählen Sie oben rechts im Menü die Option „Kopieren oder Verschieben“ aus.
5. Navigieren Sie zum neu erstellten Ordner in *Team Content*
6. Fügen Sie die Berichte mithilfe der Schaltflächen „Kopieren nach“ oder „Verschieben nach“ in den neu erstellten Ordner ein
7. Sobald SSO für Cognos aktiviert ist, melden Sie sich mit der E-Mail-Adresse, die zum Erstellen Ihres Kontos verwendet wird, bei Data Infrastructure Insights an.
8. Navigieren Sie in Cognos zum Ordner „*Team Content*“, und kopieren oder verschieben Sie die zuvor gespeicherten Berichte zurück zu „*My Content*“.

Vordefinierte Berichte Leicht Gemacht

Die Data Infrastructure Insights Reporting umfasst vordefinierte Berichte zu verschiedenen gängigen Reporting-Anforderungen und bietet wichtige Einblicke, die notwendig sind, um fundierte Entscheidungen zur Storage-Infrastruktur zu treffen.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

Sie können vordefinierte Berichte über das Data Infrastructure Insights Reporting Portal erstellen, diese per E-Mail an andere Benutzer senden und sogar ändern. Mithilfe mehrerer Berichte können Sie nach Gerät, Geschäftseinheit oder Tier filtern. Die Berichterstellungs-Tools verwenden IBM Cognos als Grundlage und bieten Ihnen viele Möglichkeiten zur Datenpräsentation.

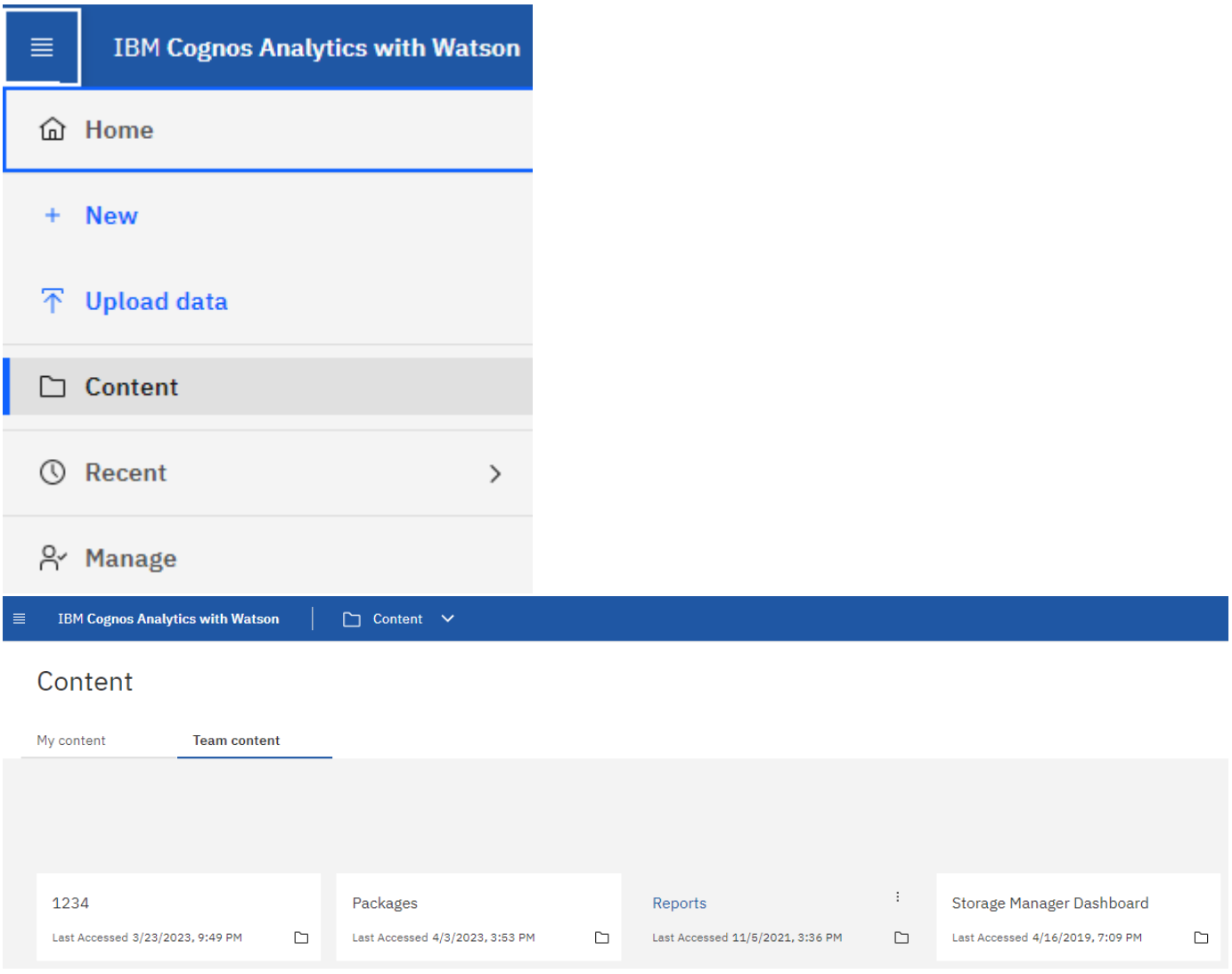
In den vordefinierten Berichten werden Ihr Inventar, Storage-Kapazität, Kostenzuordnung, Performance, Storage-Effizienz Und Cloud-kosten Daten. Sie können diese vordefinierten Berichte ändern und Ihre Änderungen speichern.

Sie können Berichte in verschiedenen Formaten generieren, darunter HTML, PDF, CSV, XML, Und Excel.

Navigieren zu vordefinierten Berichten

Wenn Sie das Reporting Portal öffnen, können Sie anhand des Ordners *Team Content* den Informationstyp auswählen, den Sie in den Berichten zu Data Infrastructure Insights benötigen.

1. Wählen Sie im linken Navigationsbereich **Inhalt > Teaminhalt**.
2. Wählen Sie **Reports**, um auf die vordefinierten Berichte zuzugreifen.



Verwenden von vordefinierten Berichten zur Beantwortung häufiger Fragen

Die folgenden vordefinierten Berichte stehen unter **Teaminhalt > Berichte** zur Verfügung.

Kapazität und Performance des Applikations-Service-Level

Der Bericht Application Service Level Capacity and Performance liefert einen allgemeinen Überblick über die Applikationen. Diese Informationen können für die Kapazitätsplanung oder für einen Migrationsplan verwendet

werden.

Kostenverrechnung

Der Bericht Chargeback liefert Informationen zur Rückberechnung von Storage-Kapazitäten nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein.

Um zu verhindern, dass die Doppelzählung keine ESX Server beinhaltet, überwachen Sie nur die VMs.

Datenquellen

Der Bericht „Datenquellen“ zeigt alle Datenquellen an, die auf Ihrem Standort installiert sind, den Status der Datenquelle (Erfolg/Fehler) und Statusmeldungen. Der Bericht enthält Informationen darüber, wo mit der Fehlerbehebung von Datenquellen begonnen werden soll. Fehlerhafte Datenquellen wirken sich auf die Genauigkeit der Berichterstellung und die allgemeine Benutzerfreundlichkeit des Produkts aus.

ESX im Vergleich zur VM-Performance

Der Bericht ESX vs VM Performance zeigt einen Vergleich der ESX Server und VMs und zeigt die durchschnittliche und Spitzen-IOPS, den Durchsatz und die Latenz sowie die Auslastungen für ESX-Server und VMs an. Um eine Doppelzählung zu verhindern, schließen Sie die ESX Server aus; schließen Sie nur die VMs ein. Eine aktualisierte Version dieses Berichts finden Sie im NetApp Storage Automation Store.

Fabric – Zusammenfassung

Der Bericht Fabric Summary identifiziert Switches und Switch-Informationen, einschließlich der Anzahl von Ports, Firmware-Versionen und Lizenzstatus. Der Bericht enthält keine NPV Switch-Ports.

Host HBAs

Der Bericht Host HBAs bietet einen Überblick über die Hosts in der Umgebung und bietet die Hersteller-, Modell- und Firmware-Version von HBAs sowie die Firmware-Ebene der Switches, mit denen sie verbunden sind. Dieser Bericht kann zur Analyse der Firmware-Kompatibilität bei der Planung eines Firmware-Upgrades für einen Switch oder einen HBA verwendet werden.

Kapazität und Performance des Host Service Level

Der Bericht über Kapazität und Performance auf Host Service Level bietet einen Überblick über die Storage-Auslastung je Host für rein Block-beschränkte Applikationen.

Host-Zusammenfassung

Der Host Summary Report bietet einen Überblick über die Speichernutzung für jeden ausgewählten Host mit Informationen für Fibre Channel- und iSCSI-Hosts. Der Bericht ermöglicht den Vergleich von Ports und Pfaden, der Fibre Channel- und ISCSI-Kapazität und der Anzahl der Verstöße.

Lizenzdetails

Im Bericht Lizenzdetails wird die berechtigte Menge an Ressourcen angezeigt, die Sie für alle Standorte mit aktiven Lizenzen lizenziert haben. Der Bericht zeigt außerdem eine Zusammenfassung der tatsächlichen Menge an allen Standorten mit aktiven Lizenzen. Die Zusammenfassung kann Überschneidungen von Storage Arrays umfassen, die von mehreren Servern gemanagt werden.

Zugeordneten, aber nicht maskierten Volumes

Der Bericht zugeordnete, jedoch nicht maskierte Volumes enthält die Volumes, deren Logical Unit Number (LUN) von einem bestimmten Host zur Verwendung zugeordnet wurde, jedoch nicht für diesen Host maskiert ist. In einigen Fällen können diese LUNs deaktiviert werden, die nicht maskiert wurden. Auf nicht maskierte Volumes kann jeder Host zugegriffen werden, wodurch sie anfällig für Datenkorruption sind.

NetApp Kapazität und Performance

Der Bericht NetApp Capacity and Performance liefert globale Daten für zugewiesene, genutzte und zugeteilte Kapazitäten im Rahmen von Trend- und Performance-Daten zur NetApp Kapazität.

Scorecard

Der Scorecard-Bericht enthält eine Zusammenfassung und einen allgemeinen Status aller von Data Infrastructure Insights erfassten Assets. Der Status wird mit grünen, gelben und roten Markierungen angezeigt:

- Grün zeigt den normalen Zustand an
- Gelb zeigt ein potenzielles Problem in der Umgebung an
- Rot weist auf ein Problem hin, das Aufmerksamkeit erfordert

Alle Felder im Bericht werden im Data Dictionary beschrieben, das mit dem Bericht bereitgestellt wird.

Zusammenfassung

Der Bericht „Storage Summary“ bietet eine vollständige Übersicht über genutzte und nicht genutzte Kapazitätsdaten für Brutto-, zugewiesene Storage-Pools und Volumes. Dieser Bericht bietet einen Überblick über den gesamten erkannten Storage.

VM-Kapazität und Performance

Beschreibt die VM-Umgebung (Virtual Machine) und ihre Kapazitätsauslastung. VM-Tools müssen aktiviert sein, um einige Daten anzuzeigen, z. B. wenn die VMs heruntergefahren wurden.

VM-Pfade

Der Bericht zu VM-Pfaden enthält Daten zur Storage-Kapazität und Performancemetriken, wobei Virtual Machines auf welchem Host ausgeführt werden, welche Hosts auf welche gemeinsam genutzten Volumes zugreifen, was der aktive Zugriffspfad ist und welche Kapazitätszuweisung und -Nutzung umfasst.

HDS-Kapazität durch Thin Pool

Der HDS Bericht zur Kapazität nach Thin Pool zeigt die Menge der nutzbaren Kapazität in einem Storage-Pool, der per Thin Provisioning bereitgestellt ist.

NetApp Kapazität nach Aggregat

Der Bericht NetApp-Kapazität nach Aggregaten zeigt die Gesamtmenge, die Gesamtzahl der genutzten, verfügbaren und den engagierten Speicherplatz von Aggregaten.

Symmetrix-Kapazität durch Thick Array

Der Bericht Symmetrix Capacity by Thick Array zeigt die Rohkapazität, nutzbare Kapazität, freie Kapazität, zugeordnet, maskiert, Und der gesamten freien Kapazität.

Symmetrix-Kapazität durch Thin Pool

Der Bericht Symmetrix Capacity by Thin Pool zeigt die Rohkapazität, nutzbare Kapazität, genutzte Kapazität, freie Kapazität, verwendeter Prozentsatz, Abonnierte Kapazitäten und Abonnementtarif.

XIV Kapazität nach Array

Der Bericht XIV Capacity by Array zeigt genutzte und ungenutzte Kapazität des Arrays an.

XIV Kapazität pro Pool

Der Bericht zur Nutzung der XIV-Kapazität anhand von Pools zeigt genutzte und nicht genutzte Kapazität für Storage Pools an.

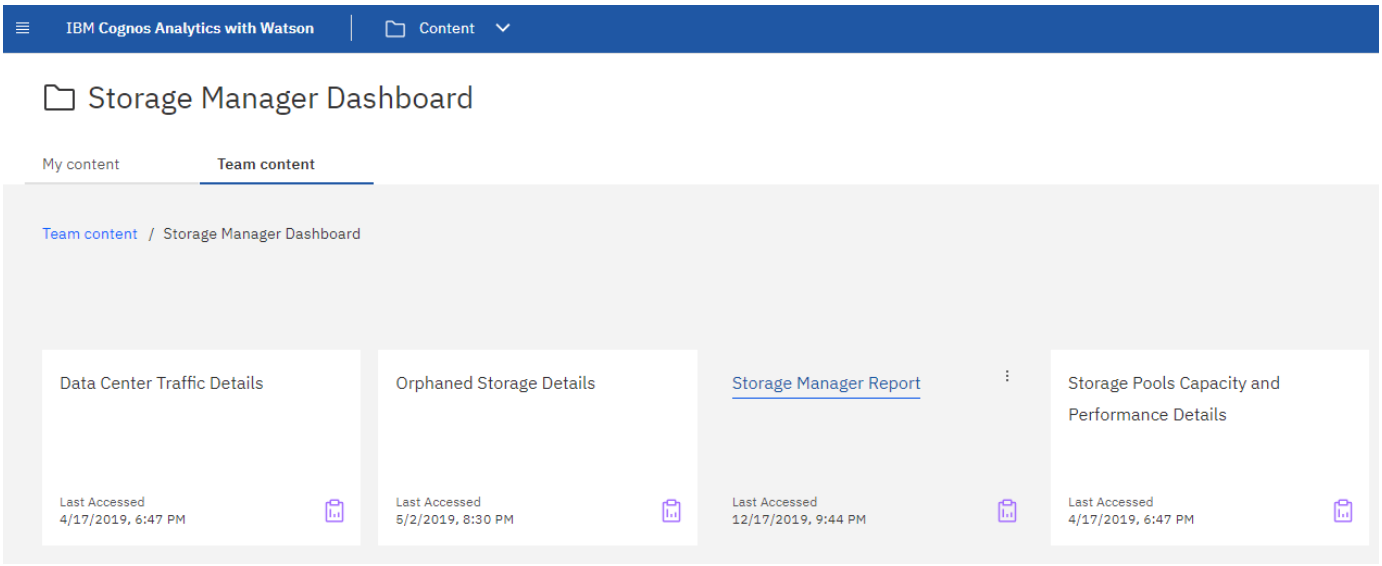
Storage Manager Dashboard

Das Storage Manager Dashboard bietet Ihnen eine zentrale Visualisierung, mit der Sie die Ressourcennutzung im Laufe der Zeit mit dem akzeptablen Bereich und den vorherigen Aktivitätstagen vergleichen und kontrastieren können. Wenn nur die wichtigsten Performance-Metriken für Ihre Storage-Services angezeigt werden, können Sie Entscheidungen zur Wartung Ihres Datacenters treffen.

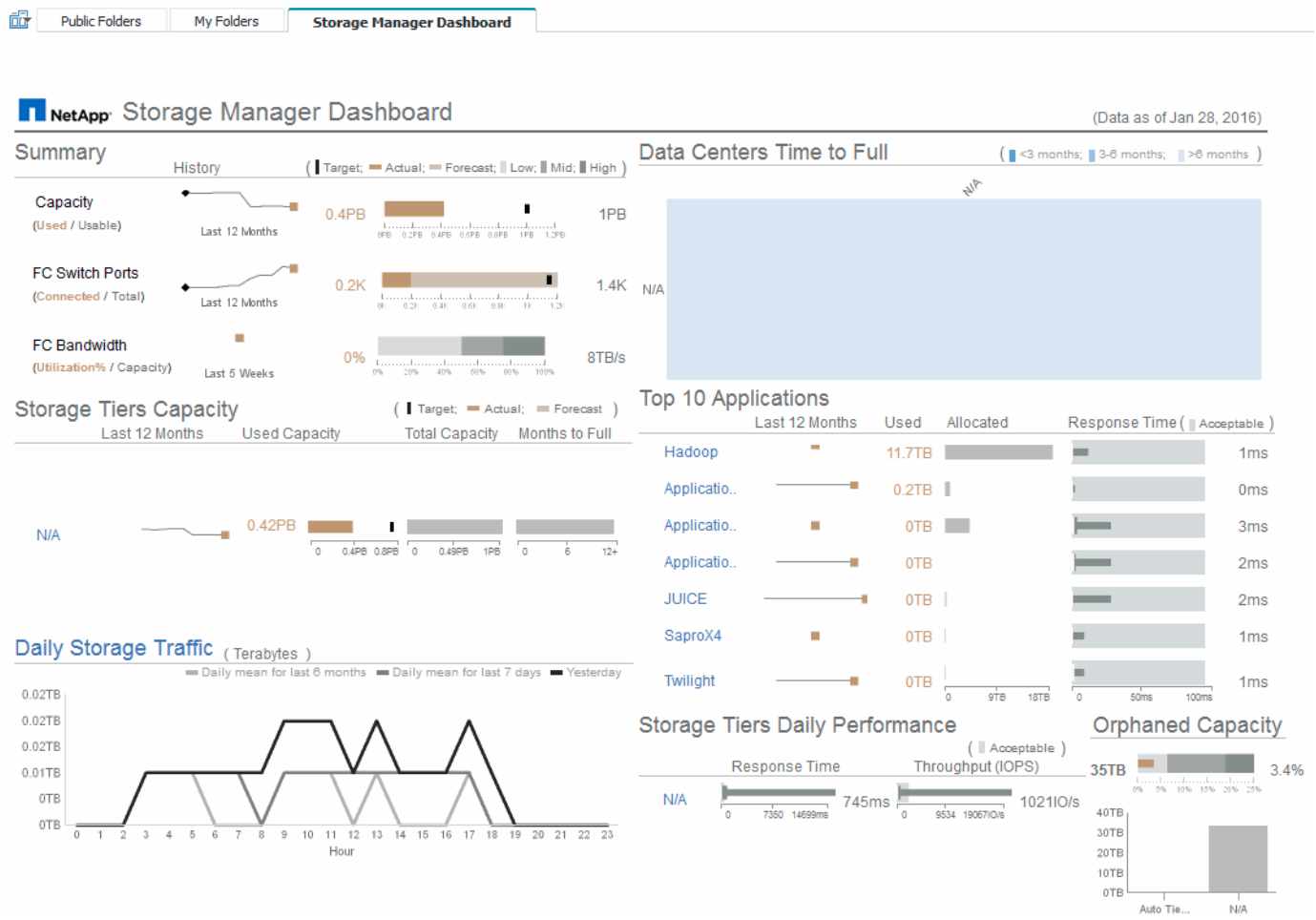
Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

Zusammenfassung

Wenn Sie **Storage Manager Dashboard** aus Team Content auswählen, erhalten Sie mehrere Berichte, die Informationen über Ihren Datenverkehr und Ihren Speicher enthalten.



Der **Storage Manager Report** besteht aus sieben Komponenten, die Kontextinformationen zu vielen Aspekten Ihrer Speicherumgebung enthalten. Sie können die Aspekte Ihrer Storage-Services detailliert analysieren und einen Abschnitt, der für Sie am wichtigsten ist, analysieren.



Diese Komponente zeigt die genutzte im Vergleich zur nutzbaren Storage-Kapazität, die Switch-Ports insgesamt gegenüber der Anzahl der verbundenen Switch-Ports sowie die Gesamtauslastung des verbundenen Switch-Ports gegenüber der Bandbreite und die jeweiligen Trends im Laufe der Zeit an. Sie können die tatsächliche Auslastung im Vergleich zum niedrigen, mittleren und hohen Bereich anzeigen, sodass Sie die Nutzung anhand eines Ziels vergleichen und einen Kontrast zwischen Projektionen und den gewünschten ist-Werten festlegen können. Für Kapazität und Switch Ports können Sie dieses Ziel konfigurieren. Die Prognose basiert auf einer Extrapolation der aktuellen Wachstumsrate und des festgelegten Datums. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, das Ziel überschreitet, wird neben der Kapazität eine Warnmeldung (roter Kreis) angezeigt.

Kapazität Des Storage-Tiers

Diese Komponente zeigt die genutzte Tier-Kapazität im Vergleich zur dem Tier zugewiesenen Kapazität. Dadurch wird angegeben, wie die genutzte Kapazität über einen Zeitraum von 12 Monaten erhöht oder verringert wird und wie viele Monate für die volle Kapazität übrig sind. Die Kapazitätsauslastung wird mit Werten für die tatsächliche Nutzung, die Nutzungsprognose und ein Ziel für die Kapazität angezeigt, die Sie konfigurieren können. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, die Zielkapazität überschreitet, wird neben einer Tier eine Warnmeldung (roter Kreis) angezeigt.

Sie können auf eine beliebige Ebene klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen, in dem freie Kapazitäten und nicht genutzte Kapazitäten, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier angezeigt werden. Sie können auch auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Täglicher Storage-Traffic

Diese Komponente zeigt die Performance der Umgebung, falls ein großes Wachstum, Änderungen oder potenzielle Probleme im Vergleich zu den vorangegangenen sechs Monaten auftreten. Es zeigt auch den durchschnittlichen Verkehr gegenüber dem Verkehr für die letzten sieben Tage, und für den Vortag. Sie können Anomalien in der Performance der Infrastruktur visualisieren, da sie Informationen liefert, die sowohl zyklische (vorherige sieben Tage) als auch saisonale Schwankungen (vorherige sechs Monate) hervorheben.

Sie können auf den Titel (täglicher Speicherverkehr) klicken, um den Bericht Speicherdatenverkehr anzuzeigen, der die Heatmap des stündlichen Speicherverkehrs für den Vortag für jedes Speichersystem anzeigt. Klicken Sie auf einen beliebigen Speichernamen in diesem Bericht, um die Seite „Anlage“ anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

Datacenter voll Zeit

Diese Komponente zeigt alle Datacenter im Vergleich zu allen Tiers und wie viel Kapazität für jeden Storage Tier verbleibt, basierend auf prognostizierten Wachstumsraten. Die Füllstandkapazität wird blau angezeigt. Je dunkler die Farbe ist, desto geringer ist die Zeit, die die Tier an der Position verlassen hat, bevor sie voll ist.

Sie können auf einen Abschnitt einer Ebene klicken, um den Bericht „Storage Pools Days to Full Details“ anzuzeigen. Dieser zeigt die Gesamtkapazität, die freie Kapazität und die Anzahl der Tage an, die für alle Pools in der ausgewählten Tier und im Datacenter voll werden sollen. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

Top 10 Applikationen

Diese Komponente zeigt die 10 wichtigsten Applikationen auf Grundlage der genutzten Kapazität an. Unabhängig davon, wie der Tier die Daten organisiert, werden in diesem Bereich die aktuelle Kapazität und der Anteil der Infrastruktur angezeigt. Sie können die Benutzerfreundlichkeit der letzten sieben Tage visualisieren, um zu sehen, ob der Verbraucher akzeptable (oder, was noch wichtiger ist, nicht akzeptable) Reaktionszeiten hat.

In diesem Bereich werden auch Trendanalysen angezeigt, die angeben, ob die Applikationen ihre Service Level Objectives (SLOs) hinsichtlich der Performance erfüllen. Sie können die Mindestreaktionszeit der letzten Woche, das erste Quartil, das dritte Quartil und die maximale Reaktionszeit anzeigen, wobei ein Median im Vergleich zu einer akzeptablen SLO angezeigt wird, die Sie konfigurieren können. Wenn die mittlere Antwortzeit für eine Applikation außerhalb des zulässigen SLO-Bereichs liegt, wird neben der Applikation ein Alarm (ein roter Kreis) angezeigt. Sie können auf eine Anwendung klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Storage Tiers Tägliche Performance

Diese Komponente zeigt eine Zusammenfassung der Performance der Tier für Reaktionszeit und IOPS für die letzten sieben Tage. Die Performance wird mit einer SLO verglichen, die Sie konfigurieren können. Dadurch sehen Sie, ob es Möglichkeiten gibt, die Storage Tiers zu konsolidieren, die von diesen Tiers bereitgestellten Workloads neu auszurichten oder Probleme mit bestimmten Tiers zu identifizieren. Wenn sich die mittlere Antwortzeit oder der mittlere IOPS außerhalb des akzeptablen SLO-Bereichs befindet, wird eine Warnmeldung (ein roter Kreis) neben einer Tier angezeigt.

Sie können auf einen Tier-Namen klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen. Er enthält Angaben zu freier und genutzter Kapazität, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

„Verlorene“ Kapazität

Diese Komponente zeigt die gesamte verwaiste Kapazität und verwaiste Kapazität je Tier. Sie wird verglichen mit einem akzeptablen Bereich für die gesamte nutzbare Kapazität und zeigt die tatsächliche verwaiste Kapazität an. Verwaiste Kapazität wird durch die Konfiguration und die Performance definiert. Der nach der Konfiguration verwaiste Storage beschreibt die Situation, in der einem Host Speicher zugewiesen ist. Die Konfiguration wurde jedoch nicht ordnungsgemäß ausgeführt, und der Host kann nicht auf den Speicher zugreifen. Diese Performance ist dann verwaist, wenn der Storage korrekt konfiguriert ist, damit ein Host auf sie zugreifen kann. Es gab jedoch keinen Lagerverkehr.

Der horizontale gestapelte Balken zeigt die zulässigen Bereiche an. Je dunkler das Grau ist, desto unannehmbarer ist die Situation. Die tatsächliche Situation wird mit dem schmalen Bronzebalken angezeigt, der die tatsächliche verwaiste Kapazität anzeigt.

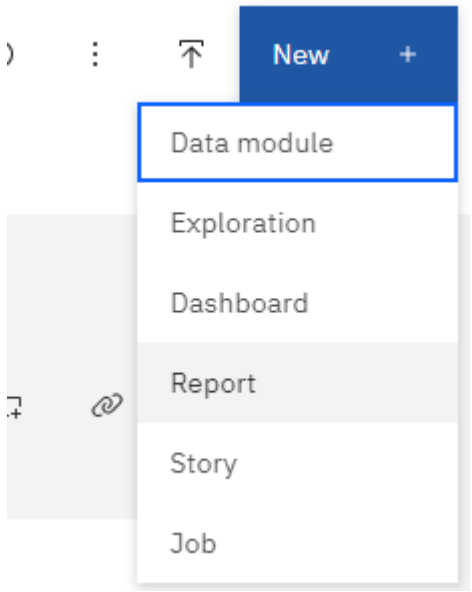
Sie können auf eine Tier klicken, um den Bericht „Verlorene Storage-Details“ anzuzeigen. In diesem Bericht werden alle Volumes angezeigt, die nach Konfiguration und Performance der ausgewählten Tier als „verwaist“ identifiziert wurden. Klicken Sie in diesem Bericht auf eine beliebige Ablage, einen Speicherpool oder ein beliebiges Volume, um die Seite „Asset“ anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

Erstellen eines Berichts (Beispiel)

Erstellen Sie anhand der Schritte in diesem Beispiel einen einfachen Bericht zur physischen Kapazität von Storage- und Speicherpools in verschiedenen Datacentern.

Schritte

1. Navigieren Sie zu **Menü > Inhalt > Teaminhalt > Berichte**
2. Wählen Sie oben rechts im Bildschirm **[Neu +]** aus
3. Wählen Sie **Bericht**



4. Wählen Sie auf der Registerkarte **Templates** die Option *leer*

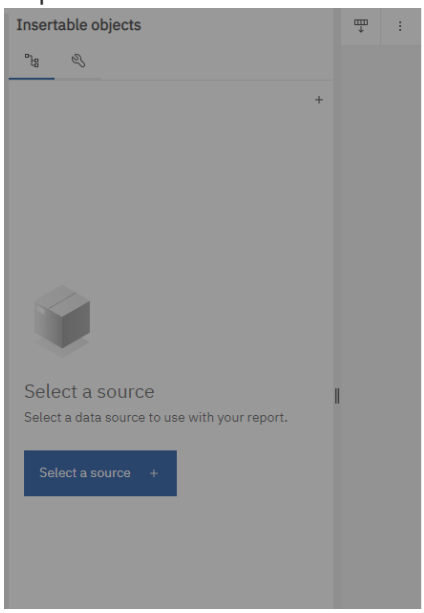
   Die Registerkarte „Quelle und Daten“ wird angezeigt

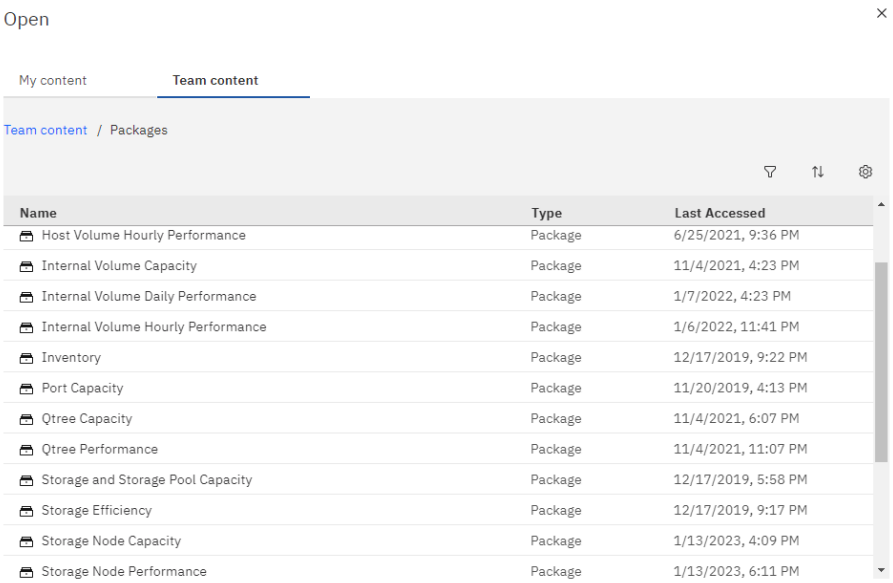
5. Öffnen **Quelle auswählen +**

6. Öffnen Sie unter **Team content Packages**

   Eine Liste der verfügbaren Pakete wird angezeigt.

7. Wählen Sie *Speicher- und Speicherpool-Kapazität*





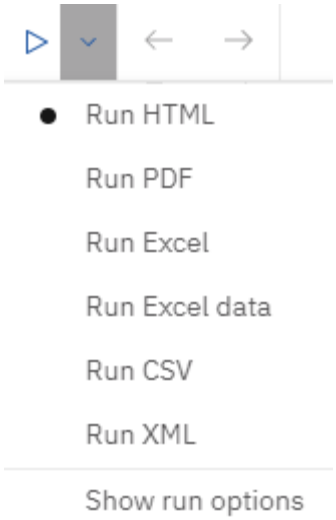
8. Wählen Sie * Öffnen*

   Die verfügbaren Stile für Ihren Bericht werden angezeigt.

9. Wählen Sie **Liste**

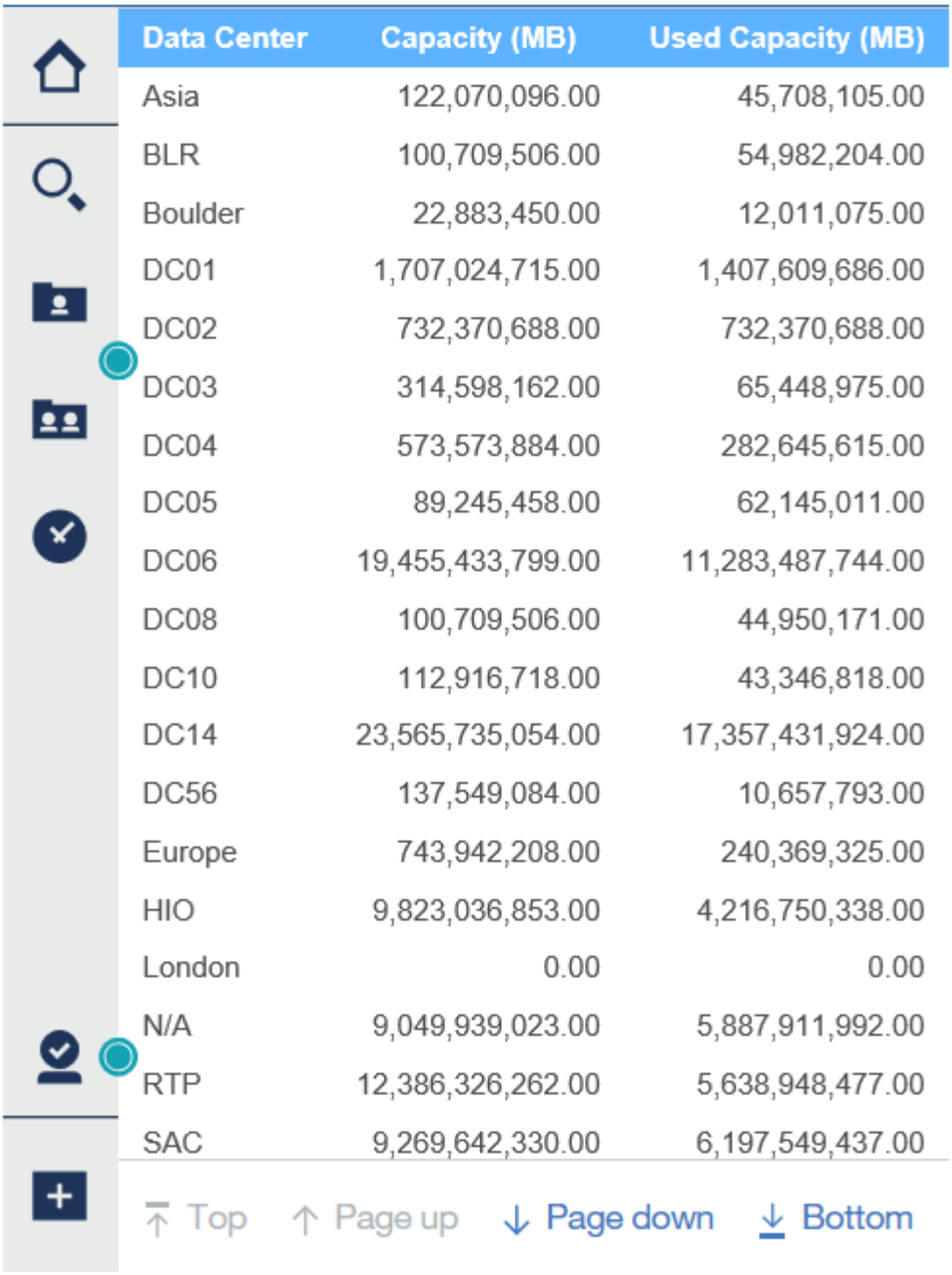
   Fügen Sie entsprechende Namen für Liste und Abfrage hinzu

10. Wählen Sie **OK**
11. Erweiterung_Physische Kapazität_
12. Erweitern Sie das System auf die unterste Ebene *Data Center*
13. Ziehen Sie *Data Center* zum Reporting-Gaumen.
14. Erweitern Sie *Capacity (MB)*
15. Ziehen Sie *Kapazität (MB)* zum Berichtspaue.
16. Ziehen Sie *genutzte Kapazität (MB)* zum Berichtsausgang.
17. Führen Sie den Bericht durch, indem Sie einen Ausgabetyp aus dem Menü **Ausführen** auswählen.



Ergebnis

Ein Bericht wie der folgende wird erstellt:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Verwalten Von Berichten

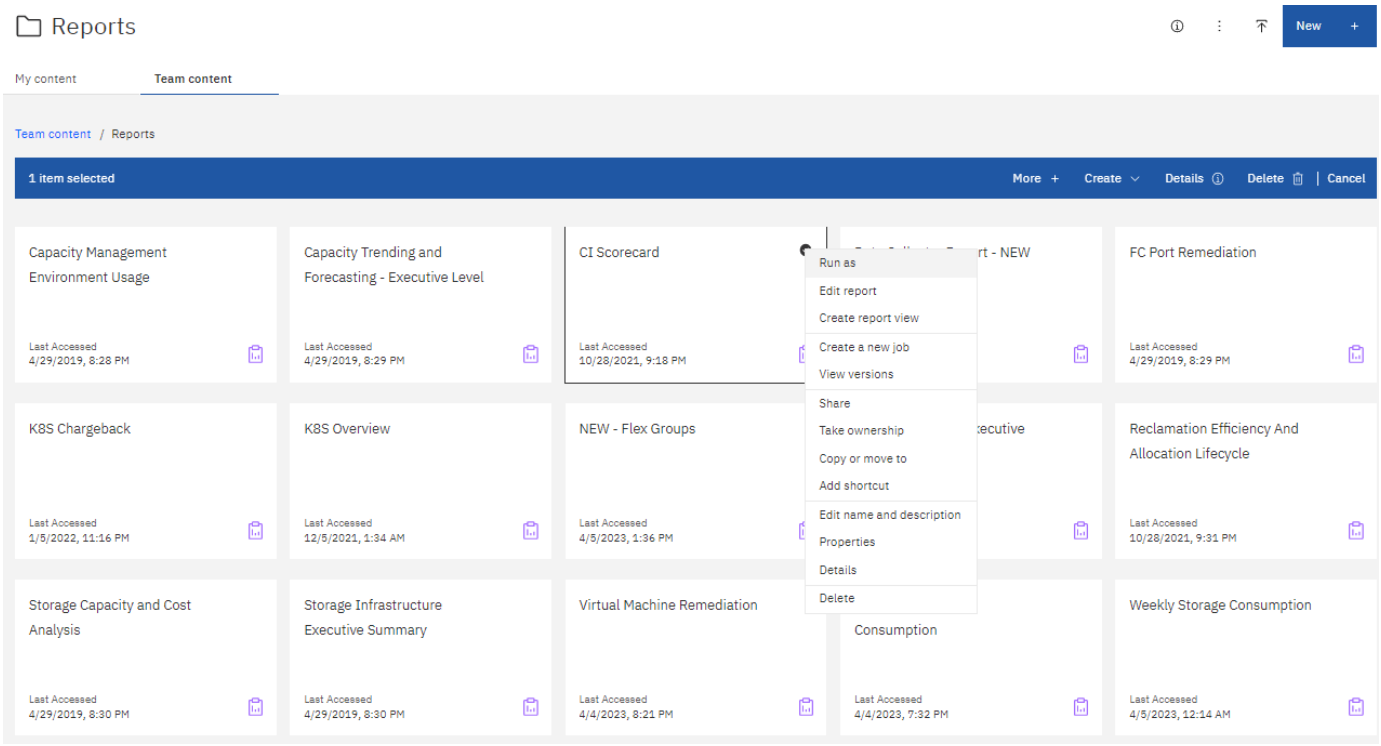
Sie können das Ausgabeformat und die Ausgabe eines Berichts anpassen, Berichteigenschaften oder Zeitpläne festlegen und E-Mail-Berichte erstellen.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

Anpassen des Ausgabeformats und der Bereitstellung eines Berichts

Sie können das Format und die Bereitstellungsmethode von Berichten anpassen.

1. Gehen Sie im Data Infrastructure Insights Reporting Portal zu **Menü > Inhalt > My Content/Team Content**. Bewegen Sie die Maus über den Bericht, den Sie anpassen möchten, und öffnen Sie das Menü „drei Punkte“.

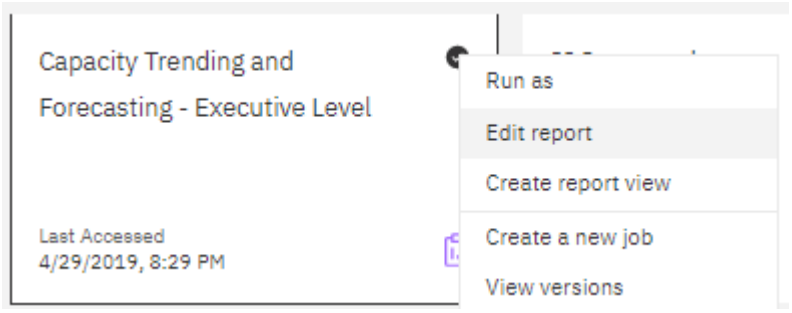


1. Klicken Sie Auf **Eigenschaften > Zeitplan**
2. Sie können folgende Optionen festlegen:
   - **Zeitplan**, wenn Sie Berichte ausführen möchten.
   - Wählen Sie **Optionen** für Berichtformat und -Zustellung (Speichern, Drucken, E-Mail) und Sprachen für den Bericht.
3. Klicken Sie auf **Speichern**, um den Bericht anhand der von Ihnen getroffenen Auswahl zu erstellen.

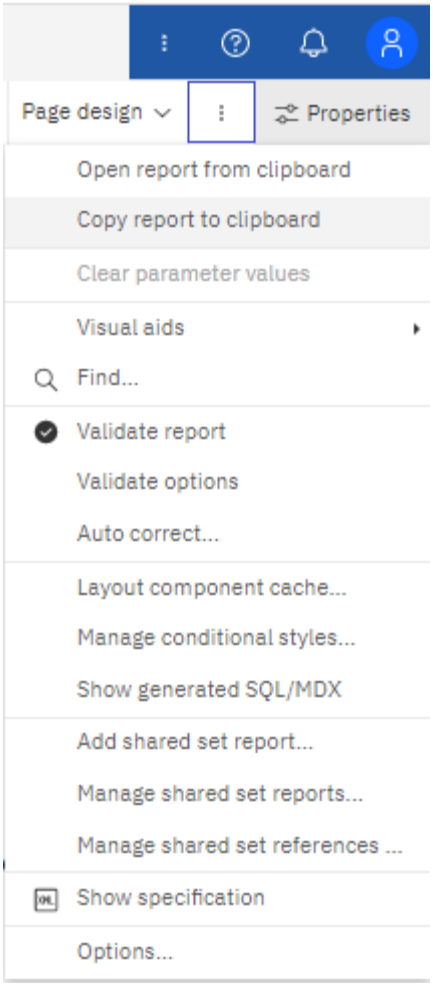
Kopieren eines Berichts in die Zwischenablage

Verwenden Sie diesen Vorgang, um einen Bericht in die Zwischenablage zu kopieren.

1. Wählen Sie einen zu kopierenden Bericht aus (**Menü > Inhalt > Mein Inhalt oder Teaminhalt**)
2. Wählen Sie im Dropdown-Menü des Berichts die Option *Report bearbeiten*



3. Öffnen Sie oben rechts auf dem Bildschirm das Menü „drei Punkte“ neben „Eigenschaften“.
4. Wählen Sie **Bericht in Zwischenablage kopieren**.

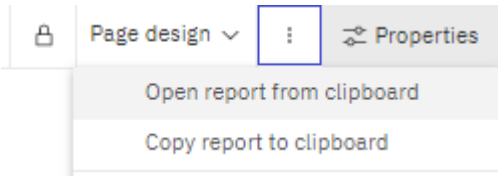


Öffnen von Berichten aus der Zwischenablage

Sie können eine Berichtsspezifikation öffnen, die zuvor in die Zwischenablage kopiert wurde.

Über diese Aufgabe Erstellen Sie zunächst einen neuen Bericht oder öffnen Sie einen vorhandenen Bericht, den Sie durch den kopierten Bericht ersetzen möchten. Die folgenden Schritte gelten für einen neuen Bericht.

1. Wählen Sie **Menü > +Neu > Bericht** und erstellen Sie einen leeren Bericht.
2. Öffnen Sie oben rechts auf dem Bildschirm das Menü „drei Punkte“ neben „Eigenschaften“.
3. Wählen Sie **Bericht aus Zwischenablage öffnen**.



1. Fügen Sie den kopierten Code in das Fenster ein und wählen Sie **OK**.
2. Wählen Sie das Diskettensymbol, um den Bericht zu speichern.
3. Wählen Sie, wo der Bericht gespeichert werden soll (*My Content*, *Team Content*, oder erstellen Sie einen neuen Ordner).
4. Geben Sie dem neuen Bericht einen aussagekräftigen Namen und wählen Sie **Speichern**.

Bearbeiten eines vorhandenen Berichts

Beachten Sie, dass die Bearbeitung von Dateien am Standardspeicherort das Risiko birgt, dass diese Berichte bei der nächsten Aktualisierung des Berichtkatalogs überschrieben werden. Es wird empfohlen, den bearbeiteten Bericht unter einem neuen Namen zu speichern oder an einem nicht standardmäßigen Speicherort zu speichern.

Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Problemen mit der Berichterstattung.

Problem:	Teste das:
Bei der Planung eines Berichts, der per E-Mail versendet werden soll, wird der Name des angemeldeten Benutzers im Feld „an“ der E-Mail vorausgefüllt. Der Name ist jedoch in der Form von "Vorname Nachname" (Vorname, Leerzeichen, Nachname). Da es sich hierbei nicht um eine gültige E-Mail-Adresse handelt, wird die E-Mail nicht gesendet, wenn der geplante Bericht ausgeführt wird.	Löschen Sie bei der Planung des zu sendenden Berichts per E-Mail den vorausgefüllten Namen und geben Sie eine gültige, korrekt formatierte E-Mail-Adresse in das Feld „To“ ein.

Erstellen Von Benutzerdefinierten Berichten

Sie können die Tools zur Erstellung benutzerdefinierter Berichte verwenden. Nachdem Sie Berichte erstellt haben, können Sie sie speichern und regelmäßig ausführen. Die Ergebnisse der Berichte können automatisch per E-Mail an sich selbst und andere gesendet werden.

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

Die Beispiele in diesem Abschnitt zeigen den folgenden Prozess, der für jedes Datenmodell der Data Infrastructure Insights Reporting-Funktion verwendet werden kann:

- Ermitteln einer Frage, die mit einem Bericht beantwortet werden soll
- Ermitteln der für die Ergebnisse erforderlichen Daten
- Auswählen von Datenelementen für den Bericht

Bevor Sie Ihren benutzerdefinierten Bericht erstellen, müssen Sie einige erforderliche Aufgaben ausführen. Wenn Sie diese nicht ausfüllen, können die Berichte ungenau oder unvollständig sein.

Wenn Sie beispielsweise den Gerätekennungsprozess nicht abschließen, sind die Kapazitätsberichte nicht korrekt. Oder, wenn Sie die Einrichtung von Annotationen (wie z. B. Tiers, Geschäftsbereiche und Datacenter) nicht abschließen, werden in Ihren individuellen Berichten möglicherweise keine Daten aus der gesamten Domäne genau gemeldet oder „N/A“ für einige Datenpunkte angezeigt.

Bevor Sie Ihre Berichte entwerfen, führen Sie die folgenden Aufgaben aus:

- Alle konfigurieren "Datensammler" Richtig.
- Geben Sie Annotationen (z. B. Tiers, Datacenter und Geschäftsbereiche) auf Geräten und Ressourcen in Ihrer Umgebung ein. Vor der Berichterstellung ist es von Vorteil, dass die Annotationen stabil sind, da in Data Infrastructure Insights Reporting Verlaufsdaten erfasst werden.

Berichtserstellung

Der Prozess der Erstellung benutzerdefinierter (auch als „Ad-hoc“ bezeichnet) Berichte umfasst mehrere Aufgaben:

- Planen Sie die Ergebnisse Ihres Berichts.
- Daten identifizieren, um Ergebnisse zu unterstützen
- Wählen Sie das Datenmodell aus (z. B. Chargeback-Datenmodell, Bestandsdatenmodell usw.), das die Daten enthält.
- Datenelemente für den Bericht auswählen.
- Optional können Sie Berichtsergebnisse formatieren, sortieren und filtern.

Planen der Ergebnisse Ihres benutzerdefinierten Berichts

Bevor Sie die Tools zur Erstellung von Berichten öffnen, sollten Sie die gewünschten Ergebnisse aus dem Bericht planen. Mit den Tools zur Erstellung von Berichten können Sie problemlos Berichte erstellen und benötigen möglicherweise keine umfangreiche Planung. Es ist jedoch sinnvoll, den Berichtsinfragesteller zu den Berichtanforderungen zu verstehen.

- Geben Sie die genaue Frage an, die Sie beantworten möchten. Beispiel:
  - Wie viel Kapazität habe ich noch übrig?
  - Wie hoch sind die Kosten für die Rückberechnung pro Geschäftsbereich?
  - Wie groß ist die Kapazität je Tier, um sicherzustellen, dass die Geschäftsbereiche auf die richtige Storage-Tier ausgerichtet sind?
  - Wie kann ich einen Strom- und Kühlungsbedarf vorhersagen? (Fügen Sie benutzerdefinierte Metadaten durch Hinzufügen von Annotationen zu Ressourcen hinzu.)
- Ermitteln Sie die Datenelemente, die Sie zur Unterstützung der Antwort benötigen.
- Identifizieren Sie die Beziehungen zwischen Daten, die in der Antwort angezeigt werden sollen. Nehmen Sie keine unlogischen Beziehungen in Ihre Frage auf, zum Beispiel: „Ich möchte die Ports sehen, die sich auf die Kapazität beziehen.“
- Ermitteln der für Daten erforderlichen Berechnungen
- Bestimmen Sie, welche Filtertypen erforderlich sind, um die Ergebnisse zu begrenzen.
- Bestimmen, ob aktuelle oder historische Daten verwendet werden müssen.
- Legen Sie fest, ob Sie Zugriffsberechtigungen für Berichte festlegen müssen, um die Daten auf bestimmte Zielgruppen zu beschränken.
- Ermitteln Sie, wie der Bericht verteilt werden soll. Sollte er beispielsweise per E-Mail an einen festgelegten Zeitplan gesendet oder im Bereich „Team Content Folder“ enthalten sein?
- Bestimmen Sie, wer den Bericht verwalten soll. Dies kann sich auf die Komplexität des Designs auswirken.
- Erstellen Sie ein Modell des Berichts.

Tipps für das Design von Berichten

Bei der Erstellung von Berichten sind einige Tipps hilfreich.

- Legen Sie fest, ob Sie aktuelle oder historische Daten verwenden müssen.

  In den meisten Berichten müssen Sie nur zu den neuesten Daten berichten, die unter Data Infrastructure

Insights verfügbar sind.

- Data Infrastructure Insights Reporting liefert Verlaufsdaten zu Kapazität und Performance, jedoch nicht zu Bestand.
- Jeder sieht alle Daten, aber möglicherweise müssen Sie die Daten auf bestimmte Zielgruppen beschränken.

  Um die Informationen für verschiedene Benutzer zu segmentieren, können Sie Berichte erstellen und Zugriffsberechtigungen für sie festlegen.

Reporting-Datenmodelle

Data Infrastructure Insights umfasst mehrere Datenmodelle, aus denen Sie entweder vordefinierte Berichte auswählen oder Ihren eigenen individuellen Bericht erstellen können.

Jedes Datenmodell enthält einen einfachen Data Marts und einen erweiterten Data Marts:

- Der einfache Data Mart bietet schnellen Zugriff auf die am häufigsten verwendeten Datenelemente und enthält nur den letzten Snapshot der Data Warehouse-Daten, enthält keine Verlaufsdaten.
- Der erweiterte Data Marts stellt alle Werte und Details zur Verfügung, die über den einfachen Data Marts verfügbar sind, und bietet Zugriff auf historische Datenwerte.

Kapazitätsdatenmodelle

Mit können Sie Fragen zur Storage-Kapazität, Auslastung des Filesystems, zur internen Volume-Kapazität, Port-Kapazität, qtree-Kapazität, beantworten. Und Kapazität von Virtual Machines (VMs). Das Kapazitätsdatenmodell ist ein Container für mehrere Kapazitätsmodelle. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen beantworten:

Modell für Storage- und Storage-Pool-Kapazitätsdaten

Ermöglicht das Antworten auf Fragen zur Ressourcenplanung von Storage-Kapazitäten, einschließlich Storage- und Storage-Pools, und umfasst sowohl physische als auch virtuelle Storage-Pool-Daten. Dieses einfache Datenmodell unterstützt Sie bei der Beantwortung von Fragen hinsichtlich Kapazität im Boden und der Kapazitätsauslastung von Storage-Pools nach Tier und Datacenter im Laufe der Zeit. Neue Kapazitätsberichte sind die Basis für ein Datenmodell, da es sich um ein einfacheres, zielgerichtetes Datenmodell handelt. Sie können Fragen wie die folgenden beantworten, indem Sie dieses Datenmodell verwenden:

- Welches ist der voraussichtliche Termin für die Erreichung der Kapazitätsgrenze von 80 % meines physischen Storage?
- Wie hoch ist die physische Storage-Kapazität auf einem Array für eine bestimmte Tier?
- Wie groß ist meine Speicherkapazität nach Hersteller und Familie sowie nach Rechenzentrum?
- Welchen Trend geht zur Storage-Auslastung bei einem Array für alle Tiers?
- Welches sind meine 10 wichtigsten Storage-Systeme bei höchster Auslastung?
- Wie sieht der Trend zur Storage-Auslastung der Storage Pools aus?
- Wie viel Kapazität ist bereits zugewiesen?
- Welche Kapazität ist für die Zuweisung verfügbar?

Datenmodell für die Dateisystemauslastung

Dieses Datenmodell bietet eine Übersicht über die Kapazitätsauslastung durch Hosts auf Filesystem-Ebene. Administratoren können zugewiesene und genutzte Kapazität pro Filesystem ermitteln, den Typ des Filesystems festlegen und Trendstatistiken nach Filesystem-Typ ermitteln. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

- Wie groß ist das Filesystem?
- Wo sind die Daten aufbewahrt und wie wird auf sie zugegriffen, z. B. lokal oder SAN?
- Was sind historische Trends für die Kapazität des Filesystems? Und was können wir dann, basierend auf diesen, für zukünftige Anforderungen erwarten?

Internes Datenmodell für die Volume-Kapazität

Hier können Sie Fragen zur verwendeten Kapazität des internen Volume, zu der zugewiesenen Kapazität und zur Kapazitätsauslastung beantworten:

- Welche internen Volumes haben eine Auslastung über einem vordefinierten Schwellenwert?
- Welche internen Volumes besteht in der Gefahr, dass die Kapazität aufgrund von Trends nicht mehr verfügbar ist? 8 welche Kapazität wird genutzt im Vergleich zur zugewiesenen Kapazität bei unseren internen Volumes?

Datenmodell für Port-Kapazität

Mit dieser Option können Sie Fragen zu Switch-Port-Konnektivität, Portstatus und Portgeschwindigkeit im Laufe der Zeit beantworten. Sie können folgende Fragen beantworten, um Ihnen beim Kauf neuer Switches zu helfen: Wie kann ich eine Prognose zum Portverbrauch erstellen, die die Verfügbarkeit von Ressourcen (Ports) prognostiziert (je nach Rechenzentrum, Switch-Anbieter und Port-Geschwindigkeit)?

- Welche Ports werden wahrscheinlich zu Kapazitätsknapp, wenn es um Datengeschwindigkeit, Datacenter, Anbieter und Anzahl der Host- und Storage-Ports geht?
- Welche Trends haben die Switch-Port-Kapazität im Laufe der Zeit?
- Welche Port-Geschwindigkeiten werden verwendet?
- Welche Art von Port-Kapazität ist erforderlich und welches Unternehmen wird gerade dabei sein, einen bestimmten Port-Typ oder einen bestimmten Anbieter zu nutzen?
- Wie lange kann diese Kapazität optimal erworben und verfügbar gemacht werden?

Datenmodell für qtree Kapazität

Ermöglicht die Trend-Nutzung von qtree (mit Daten wie genutzter bzw. zugewiesener Kapazität) im Laufe der Zeit. Sie können die Informationen nach verschiedenen Dimensionen anzeigen, beispielsweise nach Geschäftseinheit, Applikation, Ebene und Service Level. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

- Wie hoch ist die genutzte Kapazität von qtrees im Vergleich zu den Limits, die pro Applikation oder Geschäftseinheit gesetzt werden?
- Welche Trends haben wir bei unserer genutzten und freien Kapazität, sodass wir Kapazitäten planen können?
- Welche Geschäftseinheiten nutzen die größte Kapazität?
- Welche Applikationen belegen die größte Kapazität?

Datenmodell für VM-Kapazität

Ermöglicht Ihnen, Berichte über Ihre virtuelle Umgebung und deren Kapazitätsauslastung zu erstellen. Mit diesem Datenmodell können Sie Änderungen des Kapazitätsverbrauchs über die Zeit für VMs und Datenspeicher berichten. Das Datenmodell bietet außerdem Thin Provisioning und Chargeback-Daten für Virtual Machines.

- Wie kann ich das Kapazitätszuordnungsberechnung basierend auf der Kapazität bestimmen, die für VMs und Datenspeicher bereitgestellt wird?
- Welche Kapazitäten werden nicht von VMs genutzt, und welcher Anteil ungenutzte Kapazitäten ist frei, verwaist oder anderer?
- Welche Anschaffungen müssen wir anhand von Verbrauchstrends erwerben?
- Wie hoch sind meine Storage-Effizienzeinsparungen durch Storage Thin Provisioning und Deduplizierungstechnologien?

Die Kapazitäten im VM-Kapazitätsdatenmodell werden von virtuellen Festplatten (VMDKs) genutzt. Das bedeutet, dass die bereitgestellte Größe einer VM mit dem VM-Kapazitätsdatenmodell die Größe der virtuellen Festplatten entspricht. Dies unterscheidet sich von der bereitgestellten Kapazität in der Ansicht „Data Infrastructure Insights“ für Virtual Machines, in der die bereitgestellte Größe der VM angezeigt wird.

Datenmodell für Volume-Kapazität

Ermöglicht die Analyse sämtlicher Volumes in Ihrer Umgebung und die Organisation von Daten nach Anbieter, Modell, Tier, Service Level und Datacenter.

Sie können die Kapazität für verwaiste Volumes, ungenutzte Volumes und Datensicherungs-Volumes (zur Replizierung genutzt) anzeigen. Außerdem können Sie unterschiedliche Volume-Technologien (iSCSI oder FC) sehen und virtuelle Volumes mit nicht-virtuellen Volumes vergleichen, um Probleme bei der Array-Virtualisierung zu beheben.

Sie können Fragen wie die folgenden mit diesem Datenmodell beantworten:

- Welche Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
- Welchen Trend geht in meinem Datacenter hinsichtlich verwaister Volume-Kapazität?
- Wie viel meiner Datacenter-Kapazität ist virtualisiert oder Thin Provisioning?
- Wie viel meiner Datacenter-Kapazität muss für die Replizierung reserviert werden?

Modell für die Kostenzuordnung

Ermöglicht das Antworten auf Fragen zur genutzten Kapazität und zugewiesenen Kapazität in Storage-Ressourcen (Volumes, interne Volumes und qtrees). Dieses Datenmodell liefert Informationen zur Kostenverrechnung und Transparenz der Storage-Kapazität nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein. Berichtsdaten können nach Service Level und Storage Tier kategorisiert werden.

Sie können dieses Datenmodell verwenden, um Berichte zur Rückberechnung zu erstellen, indem Sie die Menge an Kapazität ermitteln, die von einer Geschäftseinheit verwendet wird. Dieses Datenmodell ermöglicht Ihnen die Erstellung einheitlicher Berichte für verschiedene Protokolle (einschließlich NAS, SAN, FC und iSCSI).

- Bei Storage ohne interne Volumes werden Berichte zur Kostenverrechnung nach Volumes angezeigt.
- Zur Speicherung mit internen Volumes:

- Wenn den Volumes Geschäftseinheiten zugewiesen sind, werden Chargeback-Berichte nach Volumes angezeigt.
- Wenn Geschäftseinheiten nicht Volumes zugewiesen, aber qtrees zugewiesen sind, werden Chargeback-Berichte durch qtrees angezeigt.
- Wenn Geschäftseinheiten nicht Volumes zugewiesen und nicht qtrees zugewiesen sind, wird das interne Volume durch Chargeback-Berichte angezeigt.
- Die Entscheidung, ob die Kostenzuordnung nach Volume, qtree oder internem Volume angezeigt werden soll, wird für jedes interne Volume getroffen. Somit ist es möglich, dass verschiedene interne Volumes im selben Storage Pool die Chargeback auf verschiedenen Ebenen zur Verfügung stehen.

Kapazitätfakten werden nach einem Standard-Zeitintervall gelöscht. Weitere Informationen finden Sie unter Data Warehouse-Prozesse.

Berichte, die das Chargeback-Datenmodell verwenden, können unter Umständen unterschiedliche Werte als Berichte mit dem Speicherkapazitätsdatenmodell anzeigen.

- Bei Storage Arrays, die keine NetApp Storage-Systeme sind, bleiben die Daten beider Datenmodelle gleich.
- Bei Storage-Systemen von NetApp und Celerra verwendet das Chargeback-Datenmodell eine einzelne Schicht (von Volumes, internen Volumes oder qtrees), um die Gebühren zu senken. Das Storage-Kapazitätsdatenmodell nutzt dagegen mehrere Schichten (von Volumes und internen Volumes), um ihre Gebühren zu sichern.

Bestandsdatenmodell

Mit Hilfe von Antworten auf Fragen zu Bestandsressourcen, einschließlich Hosts, Speichersystemen, Switches, Festplatten, Tapes Qtrees, Quotas, Virtual Machines und Server sowie generische Geräte. Das Bestandsdatenmodell enthält mehrere Unterverzeichnis, mit denen Sie Informationen zu Replikationen, FC-Pfaden, iSCSI-Pfaden, NFS-Pfaden und Verstößen anzeigen können. Das Bestandsdatenmodell enthält keine historischen Daten. Fragen, die Sie mit diesen Daten beantworten können

- Welche Assets habe ich und wo sind sie?
- Wer nutzt die Ressourcen?
- Welche Gerätetypen habe ich und welche Komponenten sind diese Geräte?
- Wie viele Hosts je Betriebssystem habe ich und wie viele Ports sind auf diesen Hosts vorhanden?
- Welche Storage-Arrays pro Anbieter gibt es in den einzelnen Datacentern?
- Über wie viele Switches je Anbieter verfügt ich in jedem Datacenter?
- Wie viele Ports sind nicht lizenziert?
- Welche Anbieter-Tapes verwenden wir und wie viele Ports sind auf jedem Tape vorhanden? Re alle generischen Geräte, die identifiziert wurden, bevor wir mit der Arbeit an Berichten beginnen?
- Welche Pfade sind zwischen den Hosts und Storage Volumes oder Tapes?
- Welche Pfade gibt es zwischen generischen Geräten und Speicher-Volumes oder Bändern?
- Wie viele Verstöße gegen die einzelnen Typen gibt es pro Datacenter?
- Was sind die Quell- und Ziel-Volumes für jedes replizierte Volume?
- Erhalte ich Firmware-Inkompatibilitäten oder falsche Portgeschwindigkeiten zwischen Fibre Channel Host HBAs und Switches?

Performance-Datenmodell

Antworten auf Fragen zur Performance von Volumes, Applikations-Volumes, internen Volumes, Switches, Applikationen VMs, VMDKs, ESX und VM, Hosts und Applikations-Nodes. Viele dieser Berichte *hourly* Daten, *Daily* Daten oder beides. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen zum Performance-Management beantworten:

- Auf welche Volumes oder internen Volumes wurde in einem bestimmten Zeitraum nicht zugegriffen?
- Können wir mögliche Fehlkonfigurationen beim Storage für eine (nicht verwendete) Applikation ermitteln?
- Wie sieht das Zugriffsverhalten einer Applikation insgesamt aus?
- Werden für eine bestimmte Applikation entsprechend Tiered Volumes zugewiesen?
- Könnten wir für eine Applikation, die derzeit läuft, einen günstigeren Storage nutzen, ohne die Applikations-Performance zu beeinträchtigen?
- Welche Applikationen bieten mehr Zugriffe auf den derzeit konfigurierten Storage?

Wenn Sie die Switch-Leistungstabellen verwenden, können Sie folgende Informationen abrufen:

- Ist mein Host-Verkehr durch verbundene Ports ausgeglichen?
- Welche Switches oder Ports weisen eine hohe Anzahl an Fehlern auf?
- Welche Switches werden am häufigsten an der Port-Performance verwendet?
- Welche nicht ausgelasteten Switches basieren auf der Port-Performance?
- Welcher Durchsatz beim Trending des Hosts basiert auf der Port-Performance?
- Wie hoch ist die Performance-Auslastung der letzten X Tage für einen angegebenen Host, ein Storage-System, ein Tape oder Switch?
- Welche Geräte erzeugen Datenverkehr auf einem bestimmten Switch (z. B. welche Geräte sind für den Einsatz eines stark genutzten Switches verantwortlich)?
- Wie hoch ist der Durchsatz für einen bestimmten Geschäftsbereich in unserer Umgebung?

Wenn Sie die Tabellen zur Festplatten-Performance verwenden, erhalten Sie folgende Informationen:

- Wie ist der Durchsatz für einen angegebenen Storage-Pool auf Basis von Festplatten-Performance-Daten?
- Was ist der am höchsten genutzte Storage-Pool?
- Wie hoch ist die durchschnittliche Festplattenauslastung für einen bestimmten Storage?
- Was ist der Trend zur Nutzung eines Storage-Systems oder eines Storage-Pools basierend auf den Festplatten-Performance-Daten?
- Wie sieht der Trend zur Festplattennutzung für einen bestimmten Storage Pool aus?

Wenn Sie VM- und VMDK-Performance-Tabellen verwenden, erhalten Sie folgende Informationen:

- Arbeitet meine virtuelle Umgebung mit optimaler Performance?
- Welche VMDKs stellen die höchsten Workloads dar?
- Wie kann ich die von VMDs gemeldete Performance bei verschiedenen Datastores nutzen, um Entscheidungen zum Re-Tiering zu treffen.

Das Performance-Datenmodell enthält Informationen, mit denen Sie die Angemessenheit von Tiers, Storage-Fehlkonfigurationen für Applikationen und die letzten Zugriffszeiten von Volumes und internen Volumes ermitteln können. Dieses Datenmodell bietet Daten wie Reaktionszeiten, IOPS, Durchsatz, Anzahl der

ausstehenden Schreibvorgänge und den Status des Datenzugriffs.

Storage-Effizienz-Datenmodell

Nachverfolgung des Storage-Effizienz-Ergebnisses und des Potenzials im Laufe der Zeit Dieses Datenmodell speichert Messungen nicht nur der bereitgestellten Kapazität, sondern auch der genutzten oder verbrauchten Menge (der physischen Messung). Wenn beispielsweise Thin Provisioning aktiviert ist, zeigt Data Infrastructure Insights an, wie viel Kapazität vom Gerät belegt wird. Mithilfe dieses Modells lässt sich außerdem die Effizienz bei aktivierter Deduplizierung bestimmen. Sie können verschiedene Fragen mithilfe des Storage-Effizienz-Data Marts beantworten:

- Wie hoch sind unsere Storage-Effizienzeinsparungen als Ergebnis der Implementierung von Thin Provisioning und Deduplizierungstechnologien?
- Wie hoch sind die Storage-Einsparungen in den gesamten Datacentern?
- Wann müssen wir, basierend auf Trends bei früheren Kapazitäten, zusätzlichen Storage erwerben?
- Was würde der Kapazitätsgewinn bedeuten, wenn wir Technologien wie Thin Provisioning und Deduplizierung aktivieren würden?
- Sind Sie hinsichtlich der Storage-Kapazität aktuell in Gefahr?

Daten-Modell-Fakt- und Bemaßungstabellen

Jedes Datenmodell enthält Fakt- und Bemaßungstabellen.

- Fact-Tabellen: Enthalten Daten, die gemessen werden, z. B. Menge, Rohkapazität und nutzbare Kapazität. Fremdschlüssel in Bemaßungstabellen enthalten.
- Bemaßungstabellen: Enthalten beschreibende Informationen zu Fakten, beispielsweise Datacenter und Geschäftseinheiten. Eine Dimension ist eine Struktur, die häufig aus Hierarchien besteht, die Daten kategorisiert. Maßattribute helfen, die Maßwerte zu beschreiben.

Mithilfe verschiedener oder mehrerer Bemaßungsattribute (siehe Spalten in den Berichten) erstellen Sie Berichte, die für jede im Datenmodell beschriebene Dimension auf Daten zugreifen.

Farben, die in Datenmodellelementen verwendet werden

Farben auf Datenmodellelementen haben unterschiedliche Indikationen.

- Gelbe Werte: Stellen Messungen dar.
- Nicht-gelbe Werte: Repräsentieren Attribute. Diese Werte aggregieren nicht.

Verwenden mehrerer Datenmodelle in einem Bericht

Normalerweise verwenden Sie ein Datenmodell pro Bericht. Sie können jedoch einen Bericht schreiben, in dem Daten aus mehreren Datenmodellen kombiniert werden.

Um einen Bericht zu schreiben, der Daten aus mehreren Datenmodellen zusammenfasst, wählen Sie eines der Datenmodelle aus, die als Basis verwendet werden sollen, und schreiben Sie dann SQL-Abfragen, um auf die Daten der zusätzlichen Datentabellen zuzugreifen. Sie können die SQL-Join-Funktion verwenden, um die Daten aus den verschiedenen Abfragen in einer einzigen Abfrage zu kombinieren, mit der Sie den Bericht schreiben können.

Beispielsweise möchten Sie die aktuelle Kapazität für jedes Storage Array bereitstellen und benutzerdefinierte Anmerkungen zu den Arrays erfassen. Sie können den Bericht mithilfe des Datenmodells für die Storage-Kapazität erstellen. Sie können die Elemente aus den Tabellen „Aktuelle Kapazität und Dimension“ verwenden

und eine separate SQL-Abfrage hinzufügen, um auf die Annotationsinformationen im Bestandsdatenmodell zuzugreifen. Abschließend können Sie die Daten kombinieren, indem Sie die Bestandsspeicherdaten mit der Tabelle Speicherdimension verknüpfen, indem Sie den Speichernamen und die Kriterien für den Beitritt verwenden.

Greifen Sie über die API auf die Berichtsdatenbank zu

Dank der leistungsstarken API von Data Infrastructure Insights können Benutzer die Data Infrastructure Insights Reporting-Datenbank direkt abfragen, ohne die Cognos Reporting-Umgebung zu durchlaufen.

Diese Dokumentation bezieht sich auf die Data Infrastructure Insights Reporting-Funktion, die in der Data Infrastructure Insights Premium Edition verfügbar ist.

Odata

Die Data Infrastructure Insights Reporting API folgt dem "OData v4"Standard (Open Data Protocol) für die Abfrage der Berichtsdatenbank. Weitere Informationen oder weitere Informationen finden Sie "Dieses Lernprogramm"unter OData.

Alle Anfragen beginnen mit der url *https://<Data-Infrastruktureinblicke-URL>/Rest/v1/dwh-Management/odata*

APIKey wird generiert

Lesen Sie mehr über "Einblick in die Dateninfrastruktur – APIs".

Gehen Sie zum Generieren eines API-Schlüssels wie folgt vor:

- Melden Sie sich bei Ihrer Data Infrastructure Insights-Umgebung an, und wählen Sie **Admin > API Access**.
- Klicken Sie auf „+ API Access Token“.
- Geben Sie einen Namen und eine Beschreibung ein.
- Wählen Sie für Typ *Data Warehouse*.
- Legen Sie Berechtigungen als Lese-/Schreibzugriff fest.
- Legen Sie ein Ablaufdatum für „Wünsche“ fest.
- Klicken Sie auf „Speichern“, dann kopieren Sie den Schlüssel und speichern Sie ihn* irgendwo sicher. Sie können später nicht auf den vollständigen Schlüssel zugreifen.

APIkeys sind gut für *Sync* oder *Async*.

Direkte Abfrage von Tabellen

Mit dem vorhandenen API-Schlüssel sind nun direkte Abfragen der Reporting-Datenbank möglich. Lange URLs können zu Anzeigezwecken auf https://…/odata/ vereinfacht werden, anstatt die vollständige https://<Data-Infrastruktur-Insights-URL>/Rest/v1/dwh-Management/odata/

Versuchen Sie einfache Abfragen wie

- Einblicke in die https://<Data-Infrastruktur – URL>/Rest/v1/dwh-Management/odata/dwh_Custom
- https://<Data-Infrastruktureinblicke URL>/Rest/v1/dwh-Management/odata/dwh_Inventory

- Einblicke in die https://<Data-Infrastruktur – URL>/Rest/v1/dwh-Management/odata/dwh_Inventory/Storage
- https://<Data-Infrastruktureinblicke URL>/Rest/v1/dwh-Management/odata/dwh_Inventory/Disk
- https://…/odata/dwh_custom/custom_queries

Beispiele FÜR REST-API

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-Infrastruktureinblicke URL>/Rest/v1/dwh-Management/odata/<schema_name>/<query>*

Beispiel:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Ergebnis:
```


```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```

Hilfreiche Tipps

Beachten Sie bei der Arbeit mit Reporting API-Abfragen Folgendes:

- Die Zuladung der Abfrage muss ein gültiger JSON-String sein
- Die Zuladung der Abfrage muss in einer einzigen Zeile enthalten sein
- Doppelte Anführungszeichen müssen entfloh werden, d. h. \“
- Registerkarten werden als \t unterstützt
- Kommentare vermeiden
- Tabellennamen mit niedrigerer Groß-/Kleinschreibung werden unterstützt

Zusätzlich:

- 2 Kopfzeilen sind erforderlich:
  - Name „X-CloudInsights-ApiKey“
  - Attributwert „<apikey>“

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 Anforderung und die Antwort wird sofort zurückgegeben. Manchmal kann die Ausführung einer Abfrage jedoch lange dauern, was zu einer Zeitüberschreitung der Anfrage führen kann. Um dies zu umgehen, können Sie eine Anfrage *asynchron* ausführen. Im asynchronen Modus gibt die Anforderung eine URL zurück, über die die Ausführung überwacht werden kann. Die URL gibt das Ergebnis zurück, wenn sie fertig ist.

Um eine Abfrage im asynchronen Modus auszuführen, fügen Sie den Header hinzu **`Prefer: respond-async`** Auf die Anfrage. Nach erfolgreicher Ausführung enthält die Antwort die folgenden Kopfzeilen:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

Wenn Sie die URL für den Speicherort abfragen, werden die gleichen Header zurückgegeben, wenn die Antwort noch nicht bereit ist, oder wenn die Antwort bereit ist, wird sie mit dem Status 200 zurückgegeben. Der Antwortinhalt ist vom Typ Text und enthält den http-Status der ursprünglichen Abfrage sowie einige Metadaten, gefolgt von den Ergebnissen der ursprünglichen Abfrage.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Um eine Liste aller asynchronen Abfragen zu sehen und welche davon bereit sind, verwenden Sie den folgenden Befehl:

```
 GET https://<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
       }
   ]
}
```

Aufbewahrung historischer Daten für die Berichterstellung

Data Infrastructure Insights speichert historische Daten für die Verwendung in Reporting auf der Grundlage der Datentabellen und der Granularität der Daten, wie in der folgenden Tabelle dargestellt.

Datentabellen	Gemessenes Objekt	Granularität	Aufbewahrungszeitraum
Performance Marts	Volumes und interne Volumes	Stündlich	14 Tage
Performance Marts	Volumes und interne Volumes	Täglich	13 Monaten
Performance Marts	Applikation	Stündlich	13 Monaten
Performance Marts	Host	Stündlich	13 Monaten
Performance Marts	Switch-Leistung für Port	Stündlich	35 Tage
Performance Marts	Performance-Switch für Host, Storage und Tape	Stündlich	13 Monaten
Performance Marts	Storage-Node	Stündlich	14 Tage
Performance Marts	Storage-Node	Täglich	13 Monaten
Performance Marts	VM-Performance	Stündlich	14 Tage
Performance Marts	VM-Performance	Täglich	13 Monaten
Performance Marts	Hypervisor-Performance	Stündlich	35 Tage

Performance Marts	Hypervisor-Performance	Täglich	13 Monaten
Performance Marts	VMDK-Performance	Stündlich	35 Tage
Performance Marts	VMDK-Performance	Täglich	13 Monaten
Performance Marts	Disk Performance	Stündlich	14 Tage
Performance Marts	Disk Performance	Täglich	13 Monaten
Capacity Marts	Alle (außer einzelne Volumes)	Täglich	13 Monaten
Capacity Marts	Alle (außer einzelne Volumes)	Monatlicher Vertreter	14 Monaten und darüber hinaus
Inventarmarke	Einzelne Volumes	Aktueller Stand	1 Tag (oder bis zum nächsten ETL)

Data Infrastructure Insights Reporting Schema Diagramms

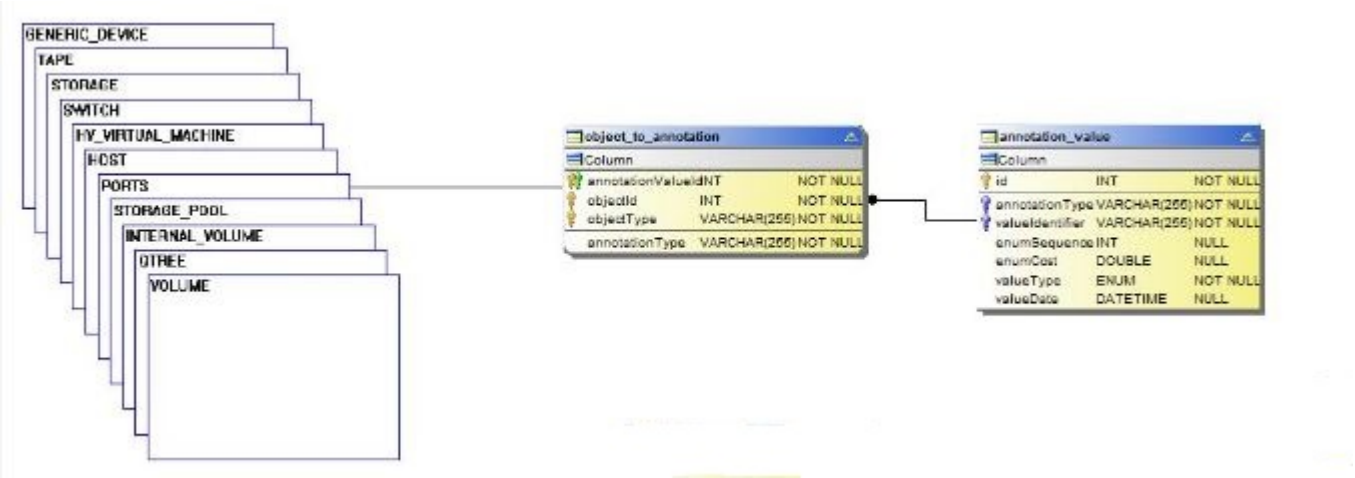
Dieses Dokument enthält die Schemadiagramme für die Berichtsdatenbank. Sie können auch eine Datei mit der herunterladen "Schematabellen".

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

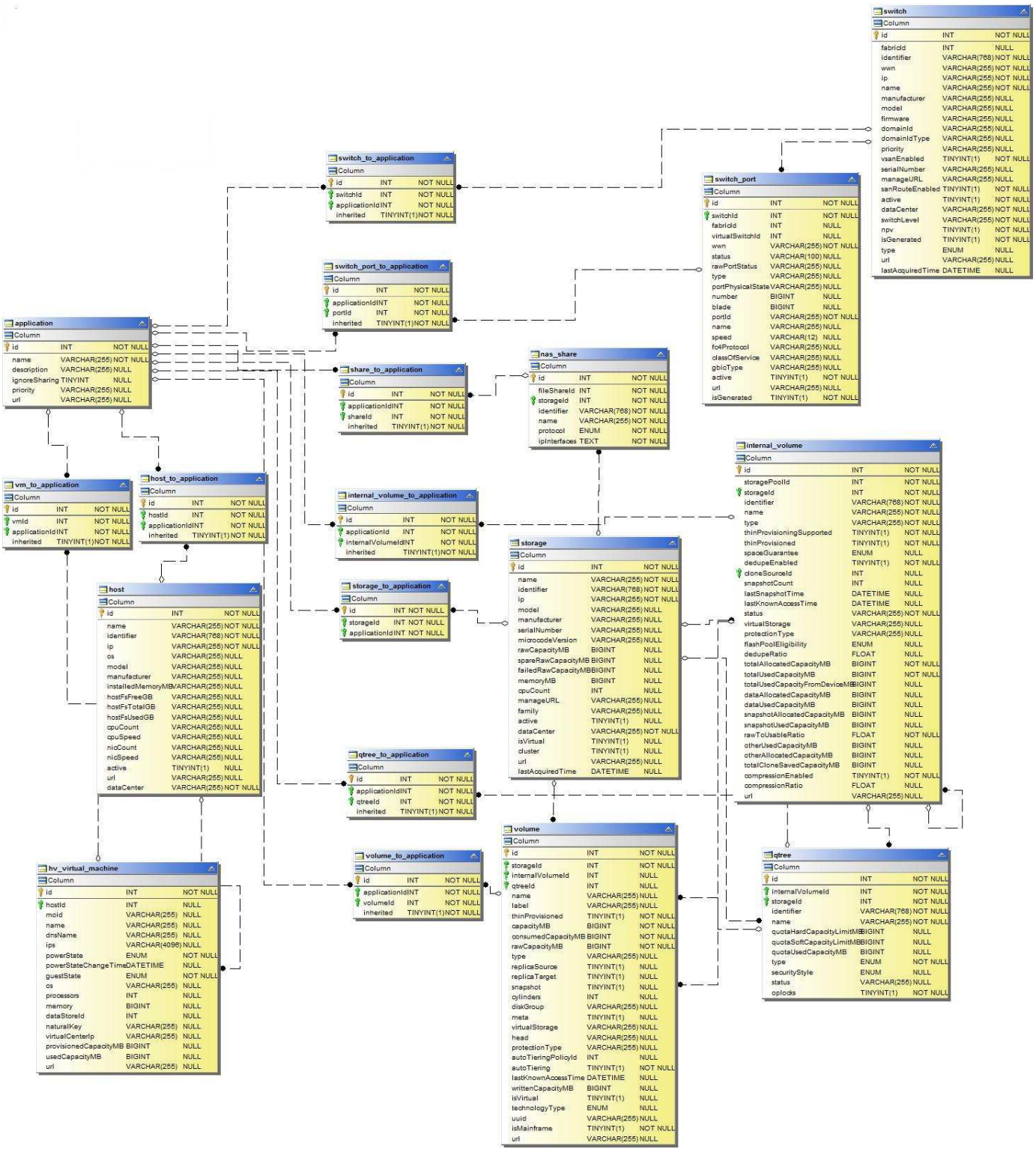
Inventory Datamart

Die folgenden Bilder beschreiben das Inventurdatamart.

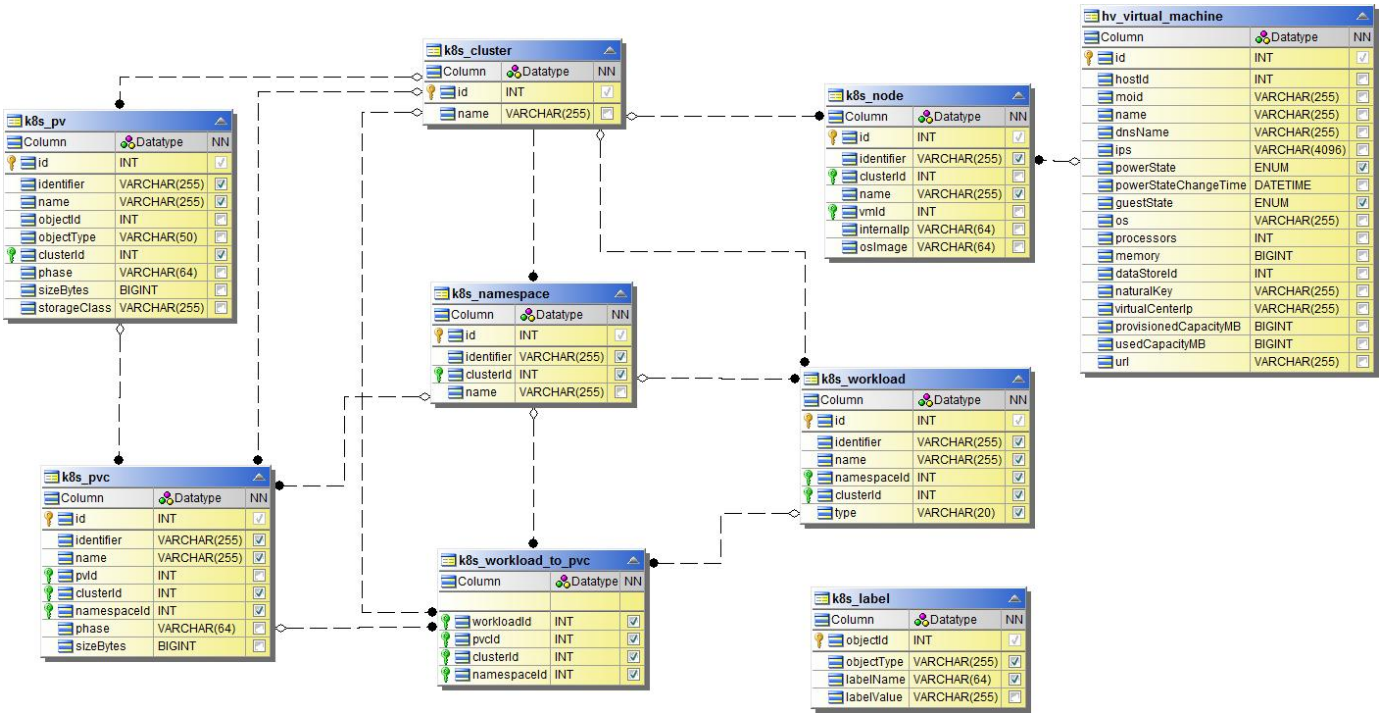
Anmerkungen



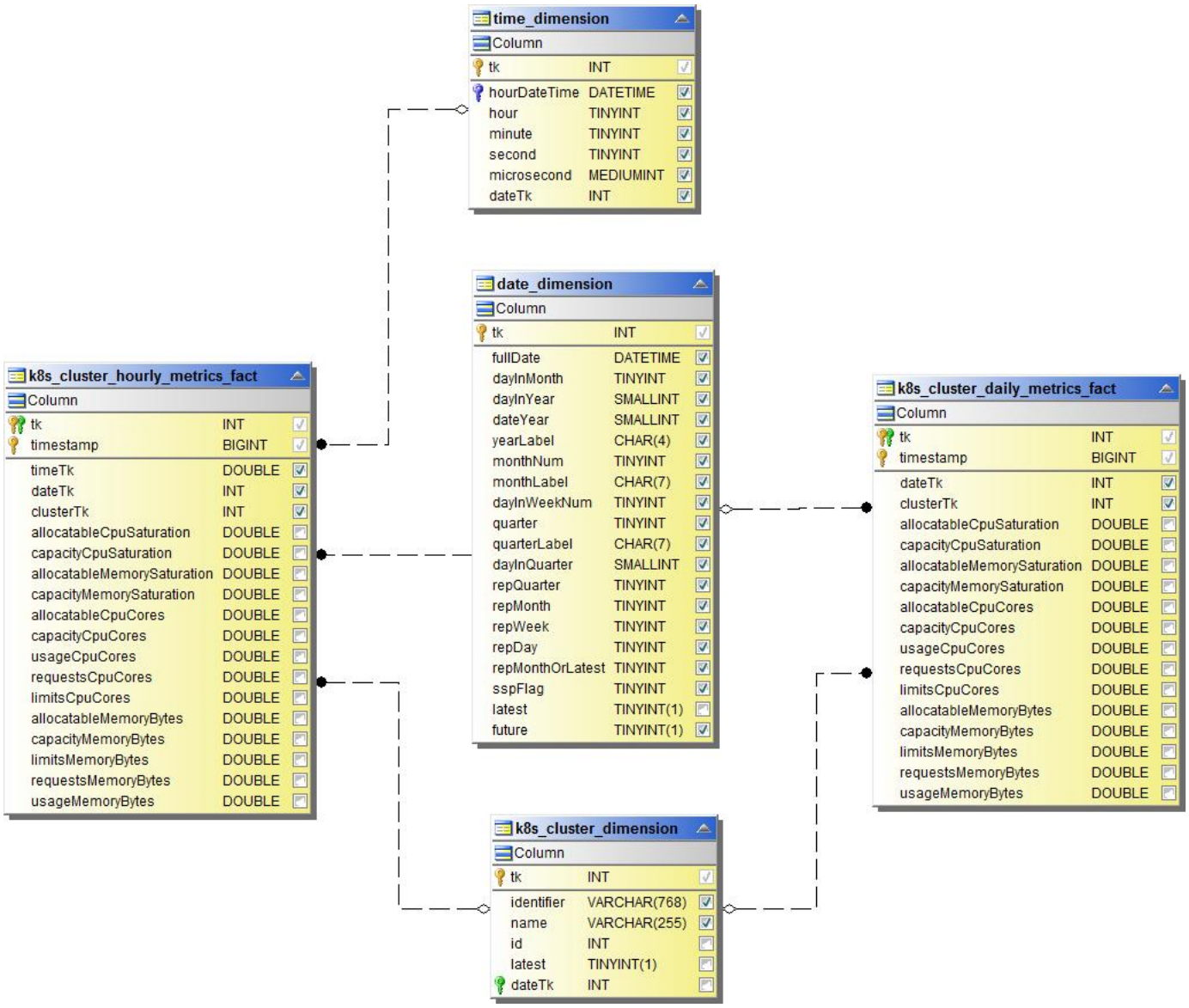
Applikationen Unterstützt



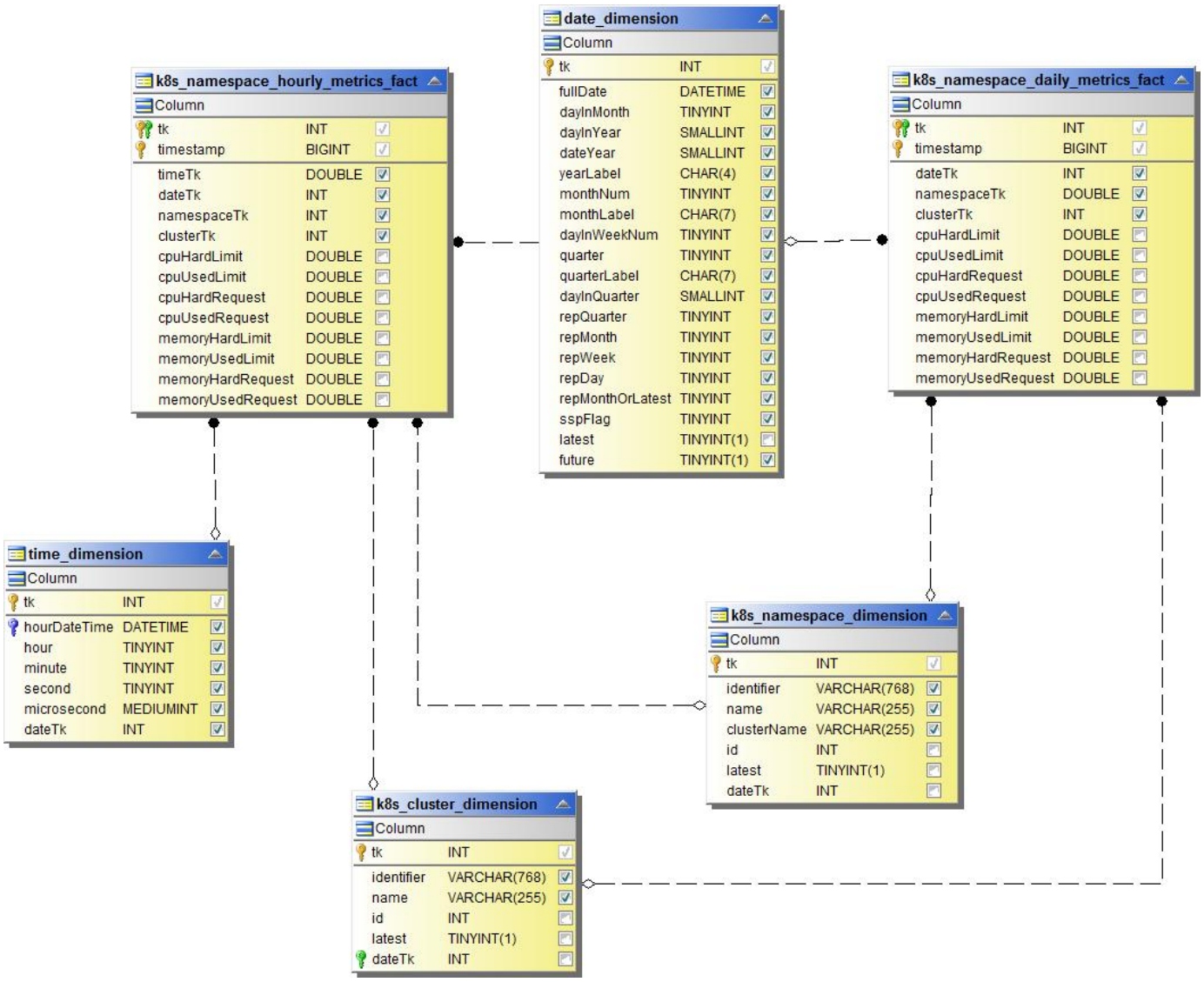
Kubernetes-Kennzahlen



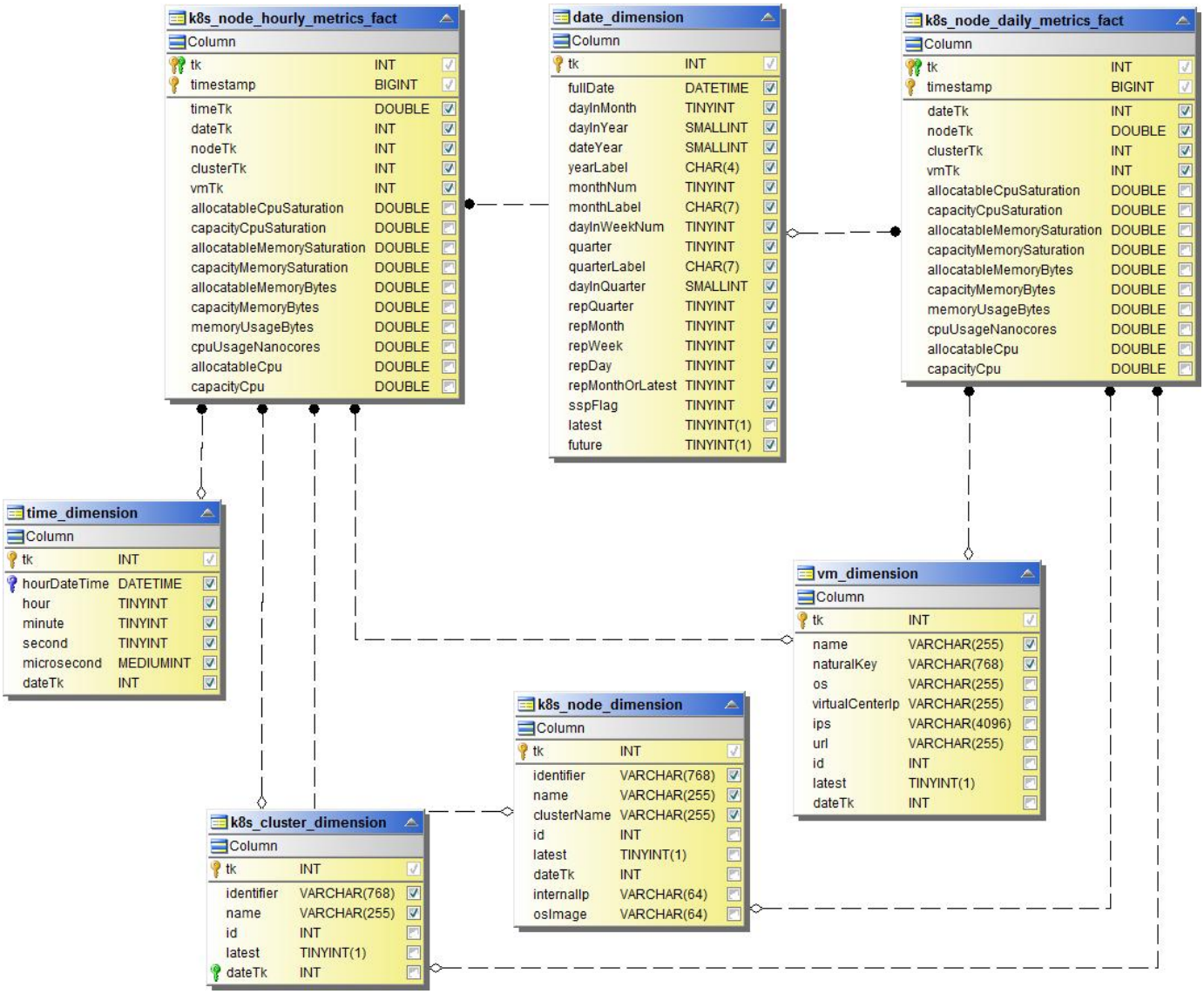
Kennzahlen Für Kubernetes Cluster



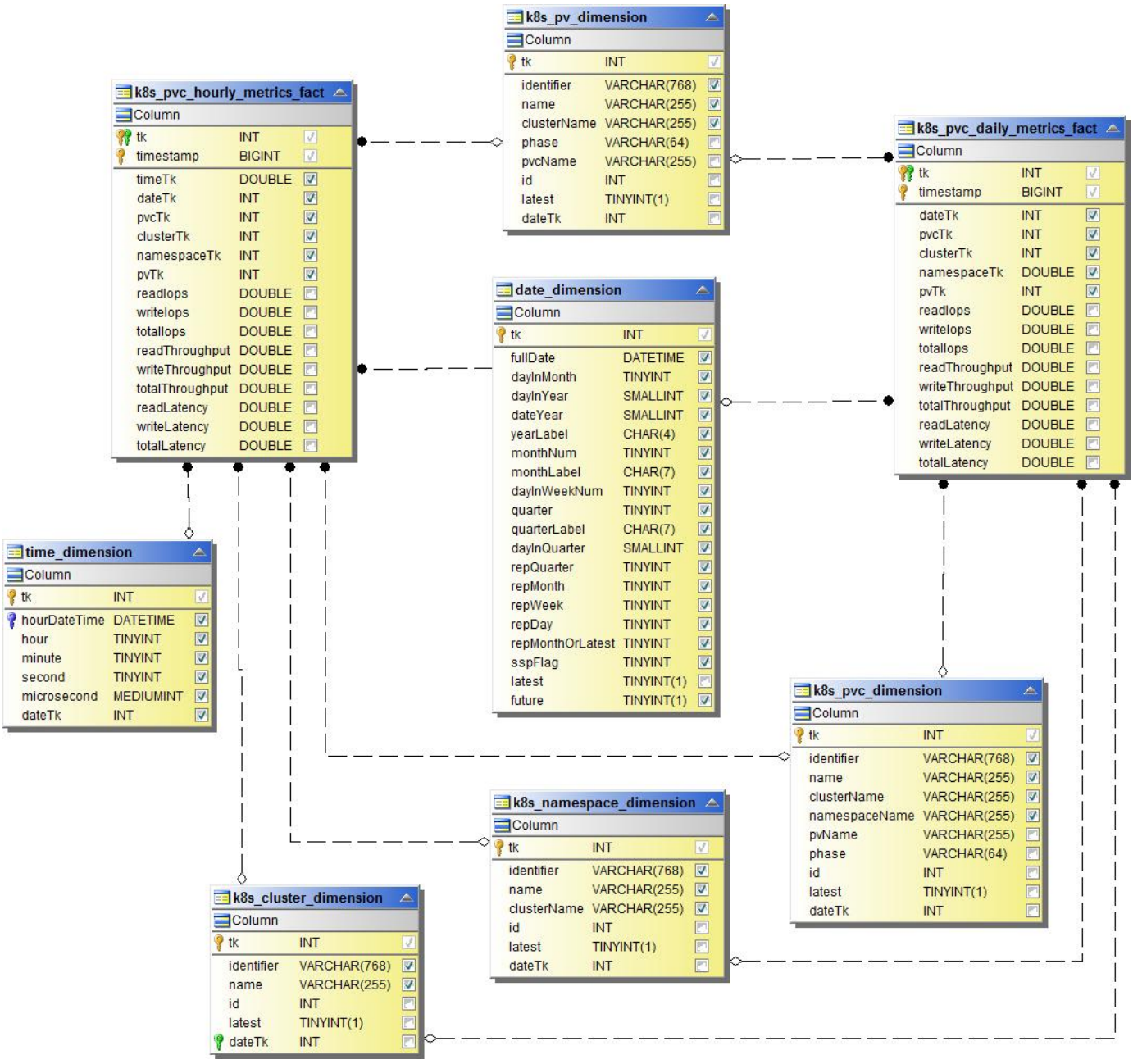
Kenngrößen Für Kubernetes-Namespace



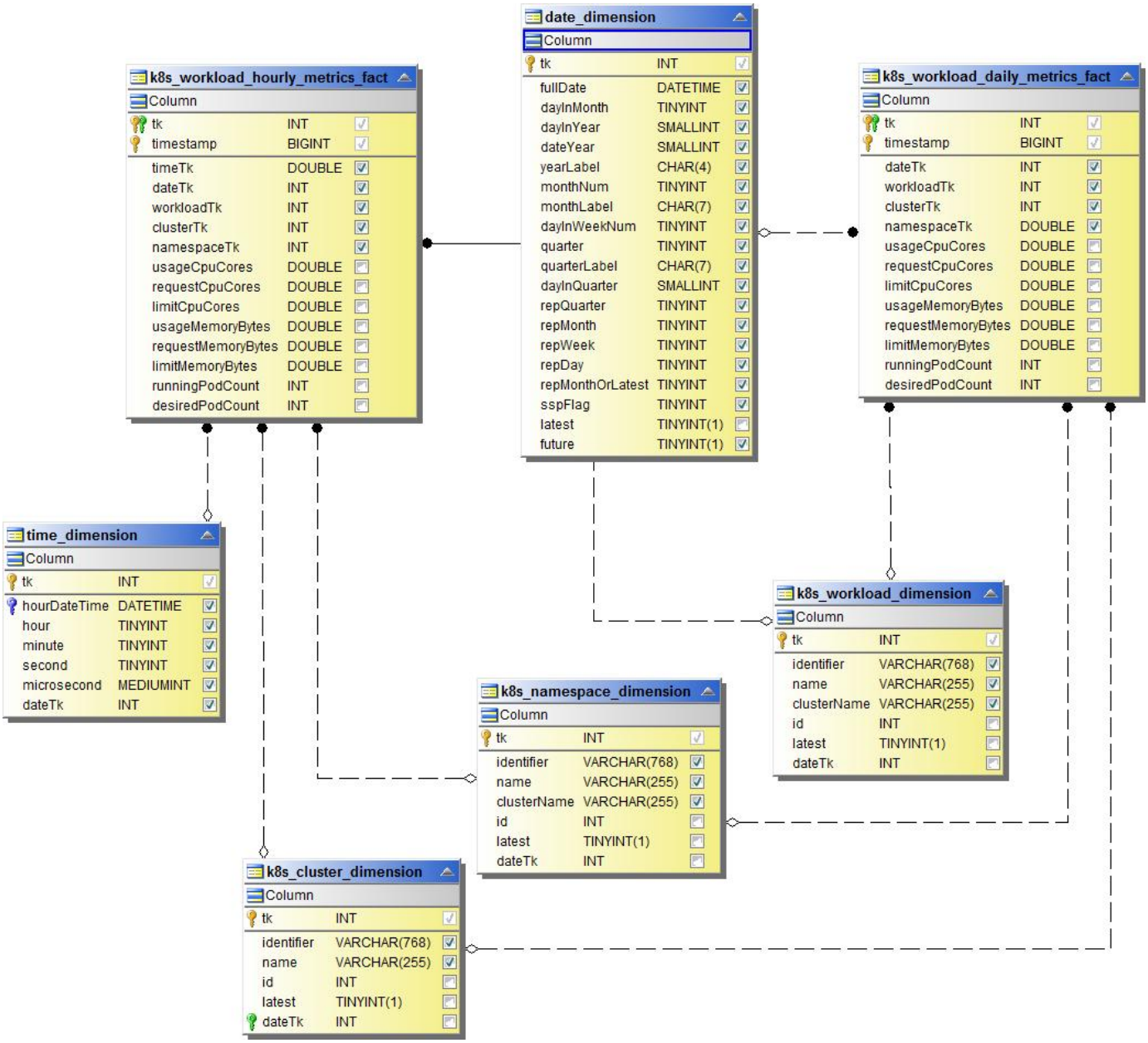
Kenngrößen Für Kubernetes-Nodes



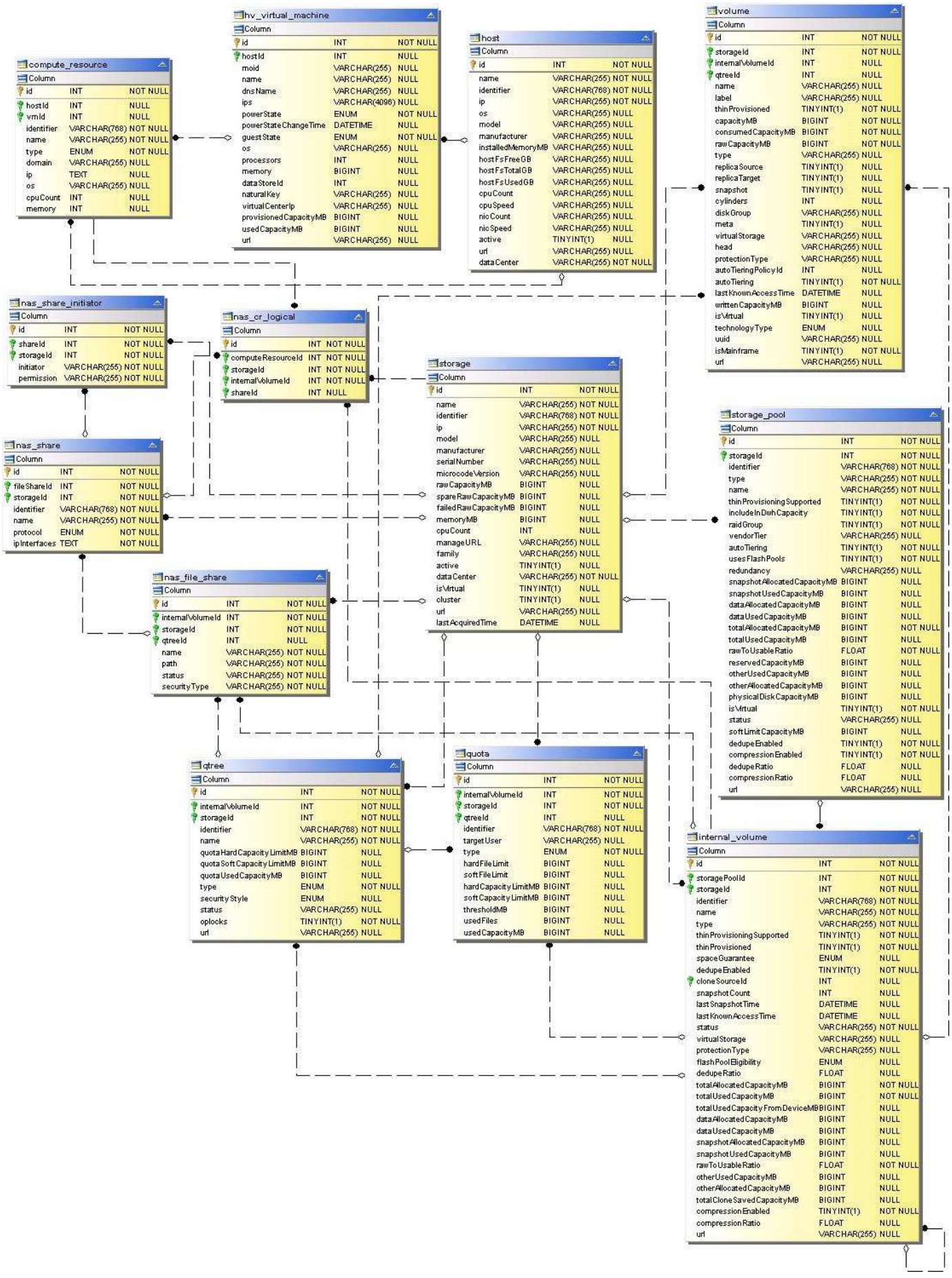
Kennzahl der Kubernetes PVC



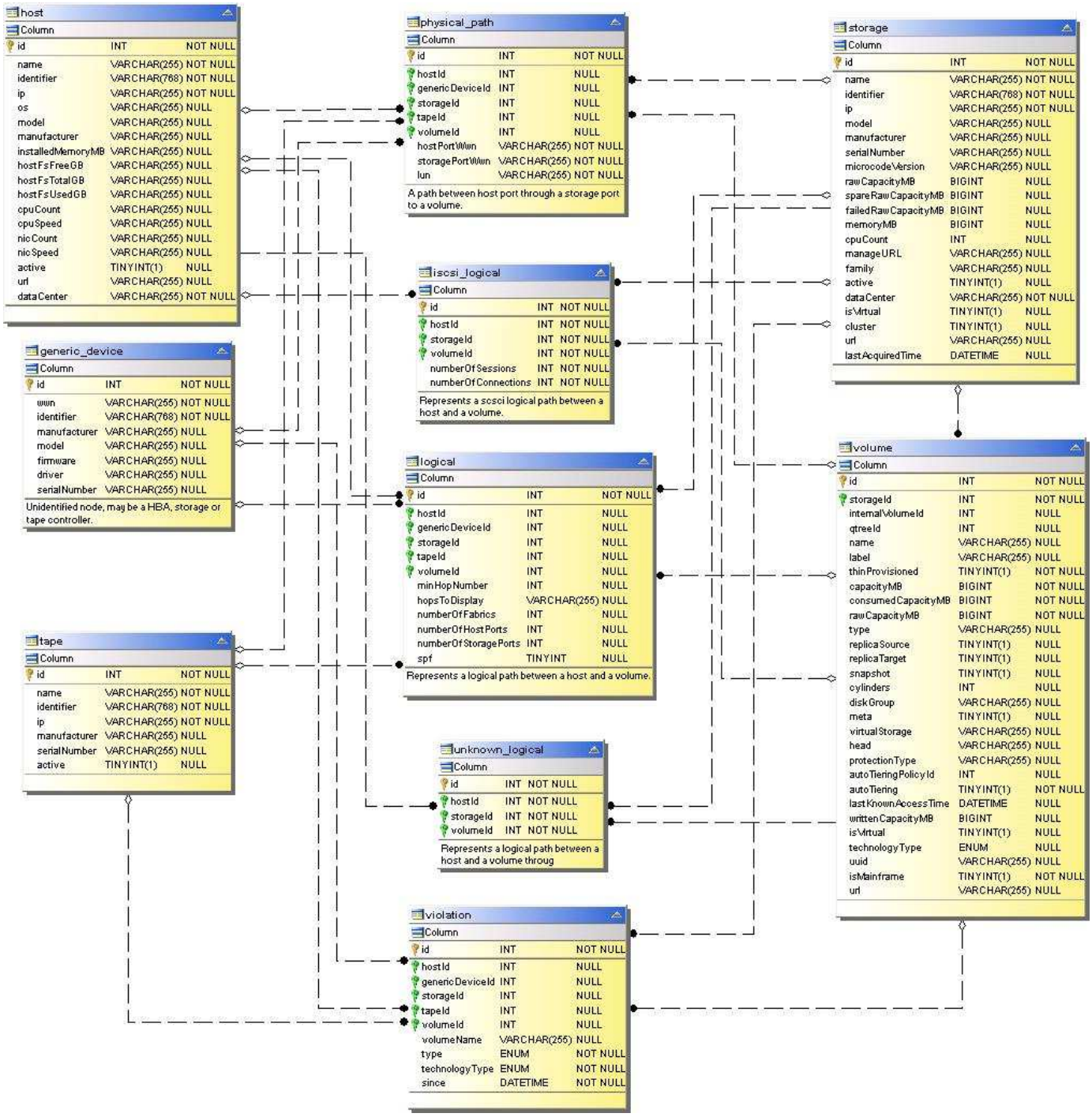
Kenngrößen Für Kubernetes-Workloads


k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

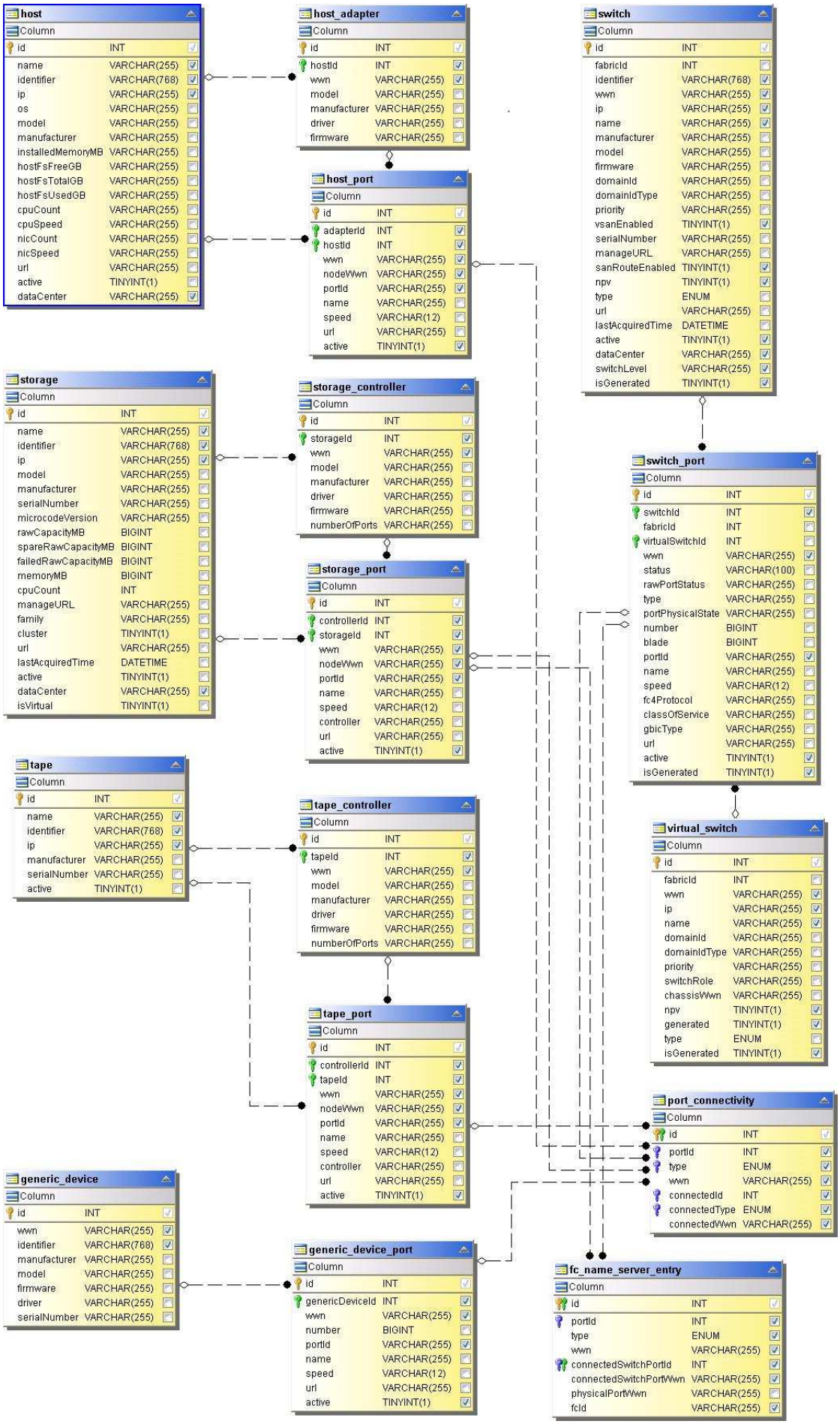
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDuhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL

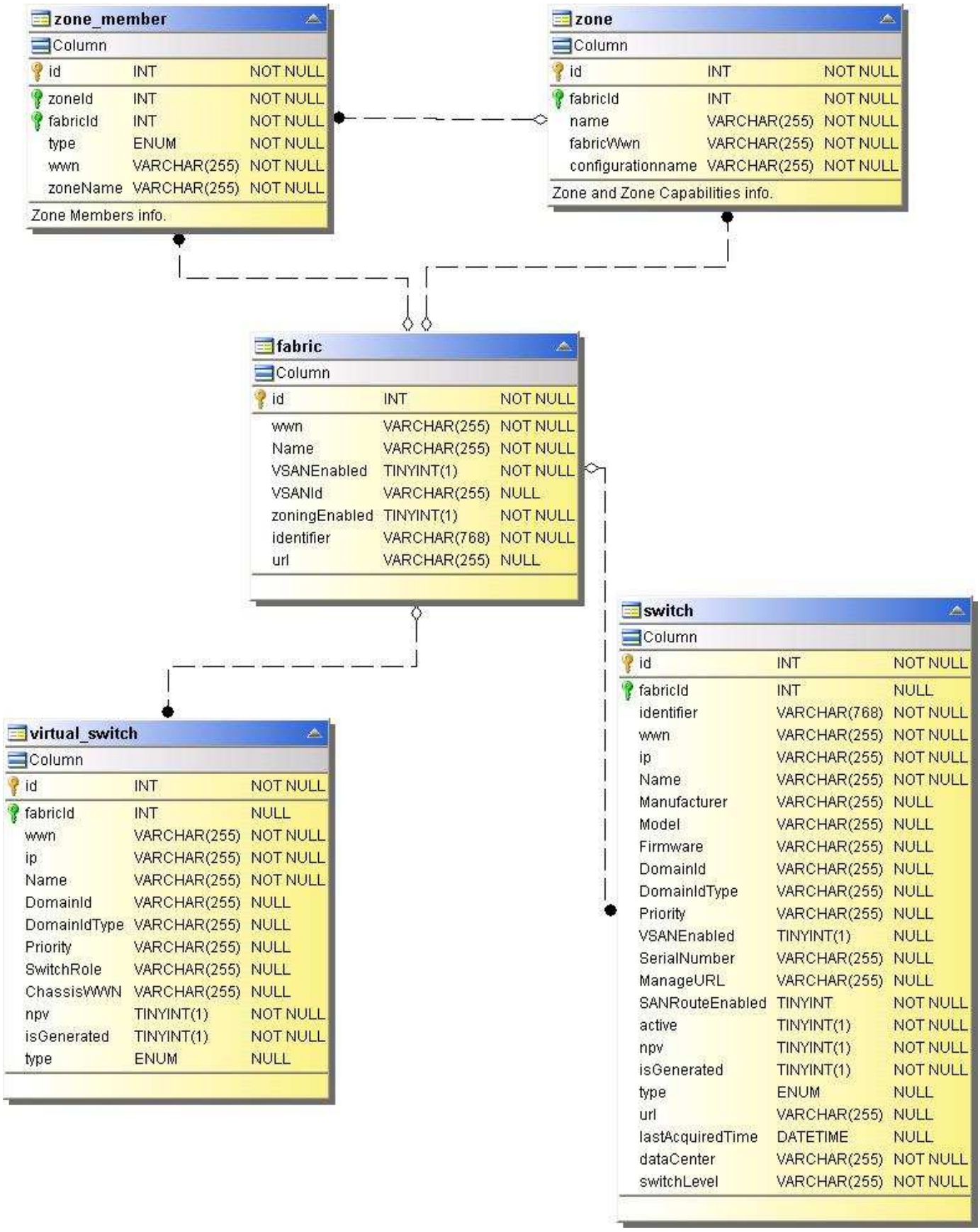
Pfade und Verstöße



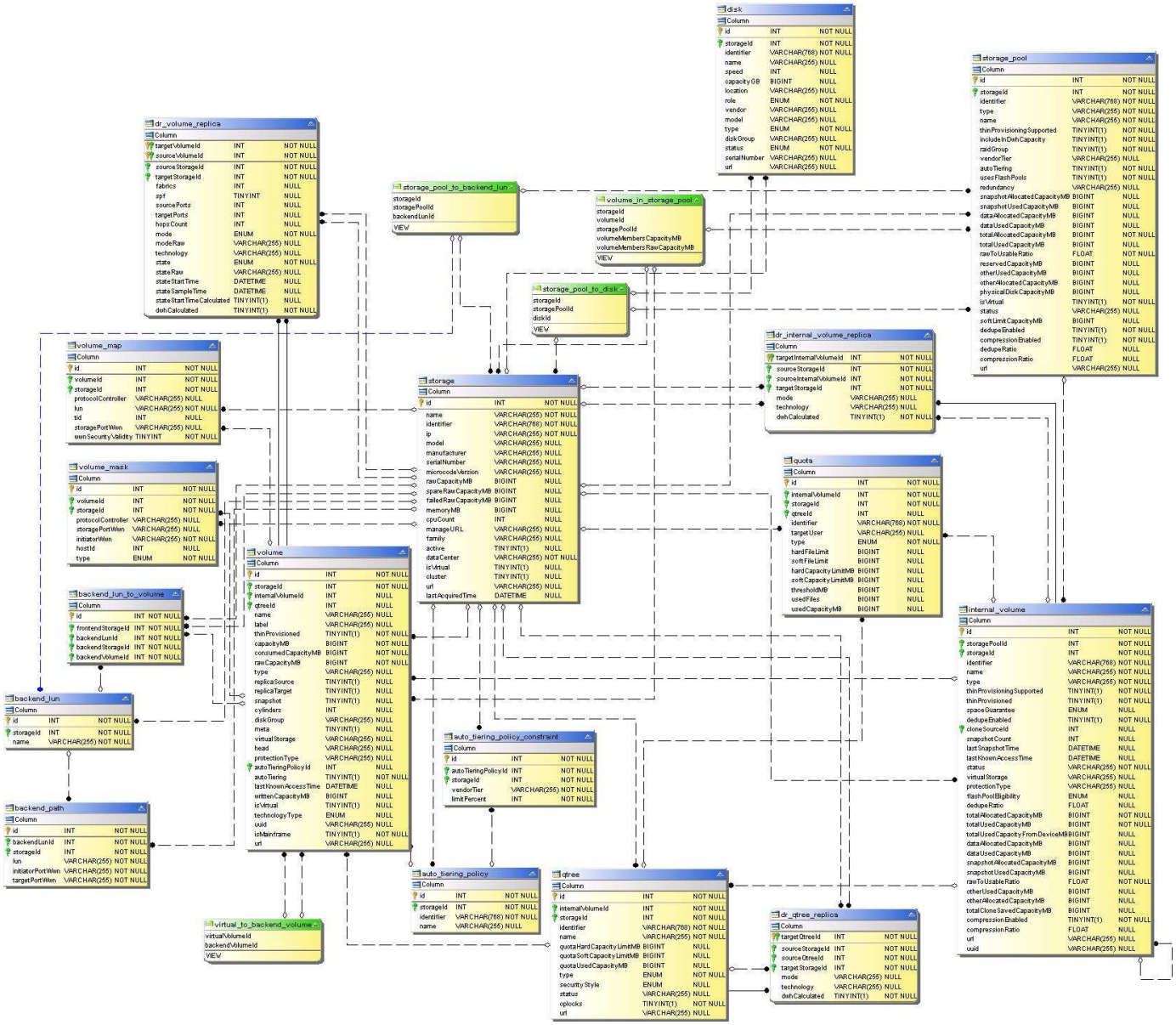
Port-Konnektivität


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

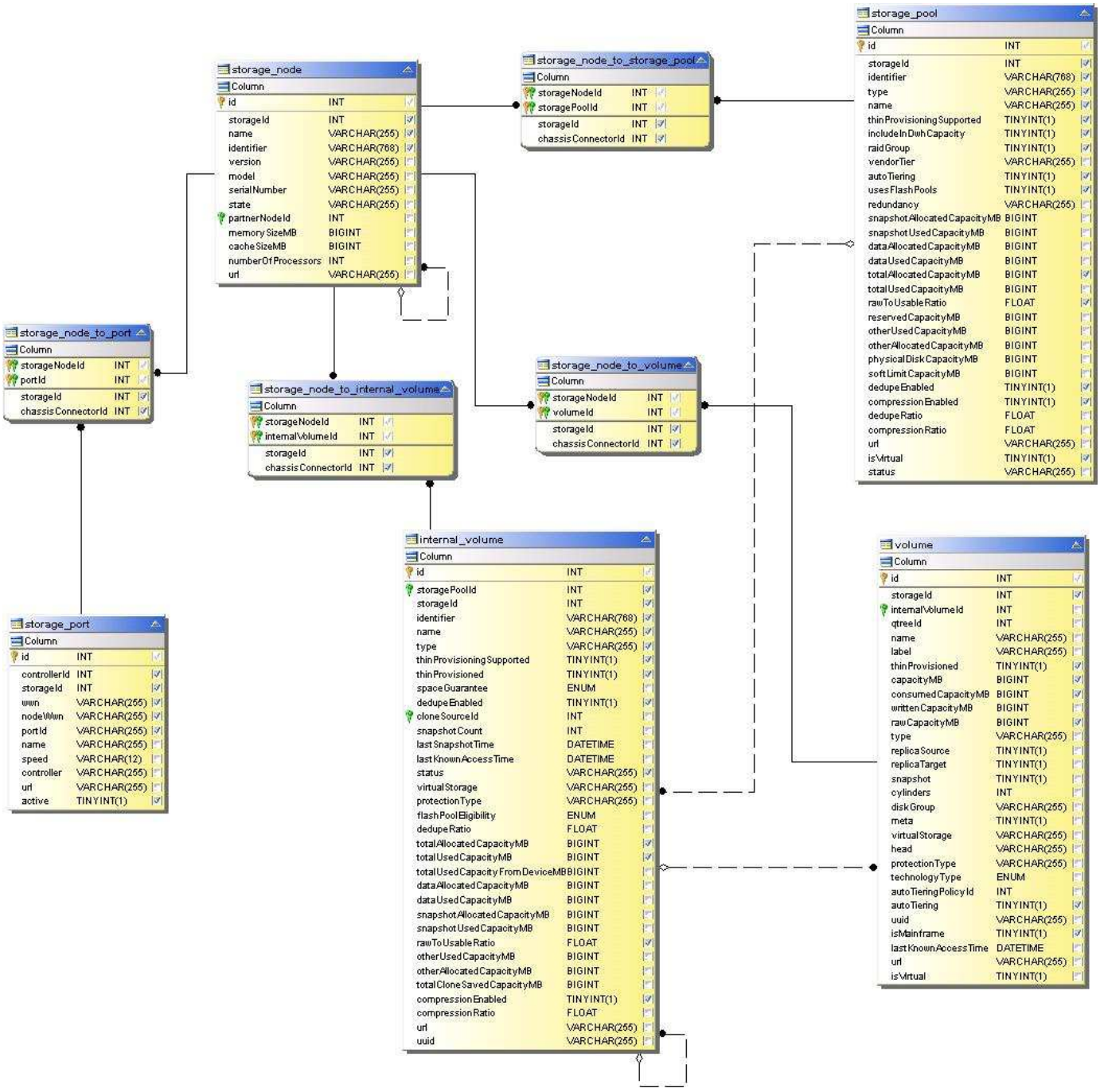
SAN-Fabric


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL

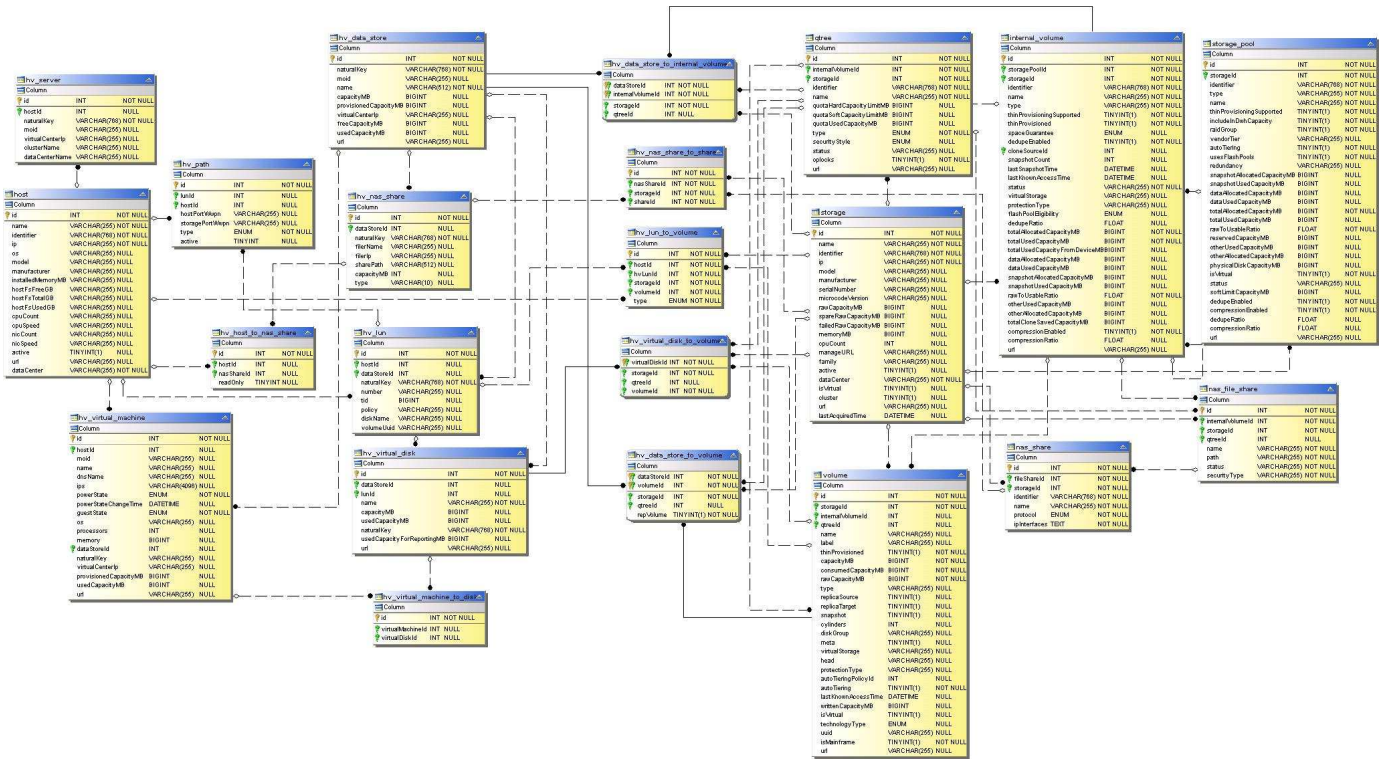
Storage



Storage-Node


storage_node
Column
id INT
storageId INT
name VARCHAR(255)
identifier VARCHAR(768)
version VARCHAR(255)
model VARCHAR(255)
serialNumber VARCHAR(255)
state VARCHAR(255)
partnerNodeId INT
memorySizeMB BIGINT
cacheSizeMB BIGINT
numberOfProcessors INT
url VARCHAR(255)
storage_node_to_storage_pool
Column
storageNodeId INT
storagePoolId INT
storageId INT
chassisConnectorId INT
storage_pool
Column
id INT
storageId INT
identifier VARCHAR(768)
type VARCHAR(255)
name VARCHAR(255)
thinProvisioningSupported TINYINT(1)
includeInDwhCapacity TINYINT(1)
raidGroup TINYINT(1)
vendorTier VARCHAR(255)
autoTiering TINYINT(1)
usesFlashPools TINYINT(1)
redundancy VARCHAR(255)
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
reservedCapacityMB BIGINT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
physicalDiskCapacityMB BIGINT
softLimitCapacityMB BIGINT
dedupeEnabled TINYINT(1)
compressionEnabled TINYINT(1)
dedupeRatio FLOAT
compressionRatio FLOAT
url VARCHAR(255)
isVirtual TINYINT(1)
status VARCHAR(255)
storage_node_to_port
Column
storageNodeId INT
portId INT
storageId INT
chassisConnectorId INT
storage_node_to_internal_volume
Column
storageNodeId INT
internalVolumeId INT
storageId INT
chassisConnectorId INT
storage_node_to_volume
Column
storageNodeId INT
volumeId INT
storageId INT
chassisConnectorId INT
internal_volume
Column
id INT
storagePoolId INT
storageId INT
identifier VARCHAR(768)
name VARCHAR(255)
type VARCHAR(255)
thinProvisioningSupported TINYINT(1)
thinProvisioned TINYINT(1)
spaceGuarantee ENUM
dedupeEnabled TINYINT(1)
cloneSourceId INT
snapshotCount INT
lastSnapshotTime DATETIME
lastKnownAccessTime DATETIME
status VARCHAR(255)
virtualStorage VARCHAR(255)
protectionType VARCHAR(255)
flashPoolEligibility ENUM
dedupeRatio FLOAT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
totalUsedCapacityFromDeviceMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
totalCloneSavedCapacityMB BIGINT
compressionEnabled TINYINT(1)
compressionRatio FLOAT
url VARCHAR(255)
uuid VARCHAR(255)
volume
Column
id INT
storageId INT
internalVolumeId INT
qtreeId INT
name VARCHAR(255)
label VARCHAR(255)
thinProvisioned TINYINT(1)
capacityMB BIGINT
consumedCapacityMB BIGINT
writtenCapacityMB BIGINT
rawCapacityMB BIGINT
type VARCHAR(255)
replicaSource TINYINT(1)
replicaTarget TINYINT(1)
snapshot TINYINT(1)
cylinders INT
diskGroup VARCHAR(255)
meta TINYINT(1)
virtualStorage VARCHAR(255)
head VARCHAR(255)
protectionType VARCHAR(255)
technologyType ENUM
autoTieringPolicyId INT
autoTiering TINYINT(1)
uuid VARCHAR(255)
isMainframe TINYINT(1)
lastKnownAccessTime DATETIME
url VARCHAR(255)
isVirtual TINYINT(1)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)

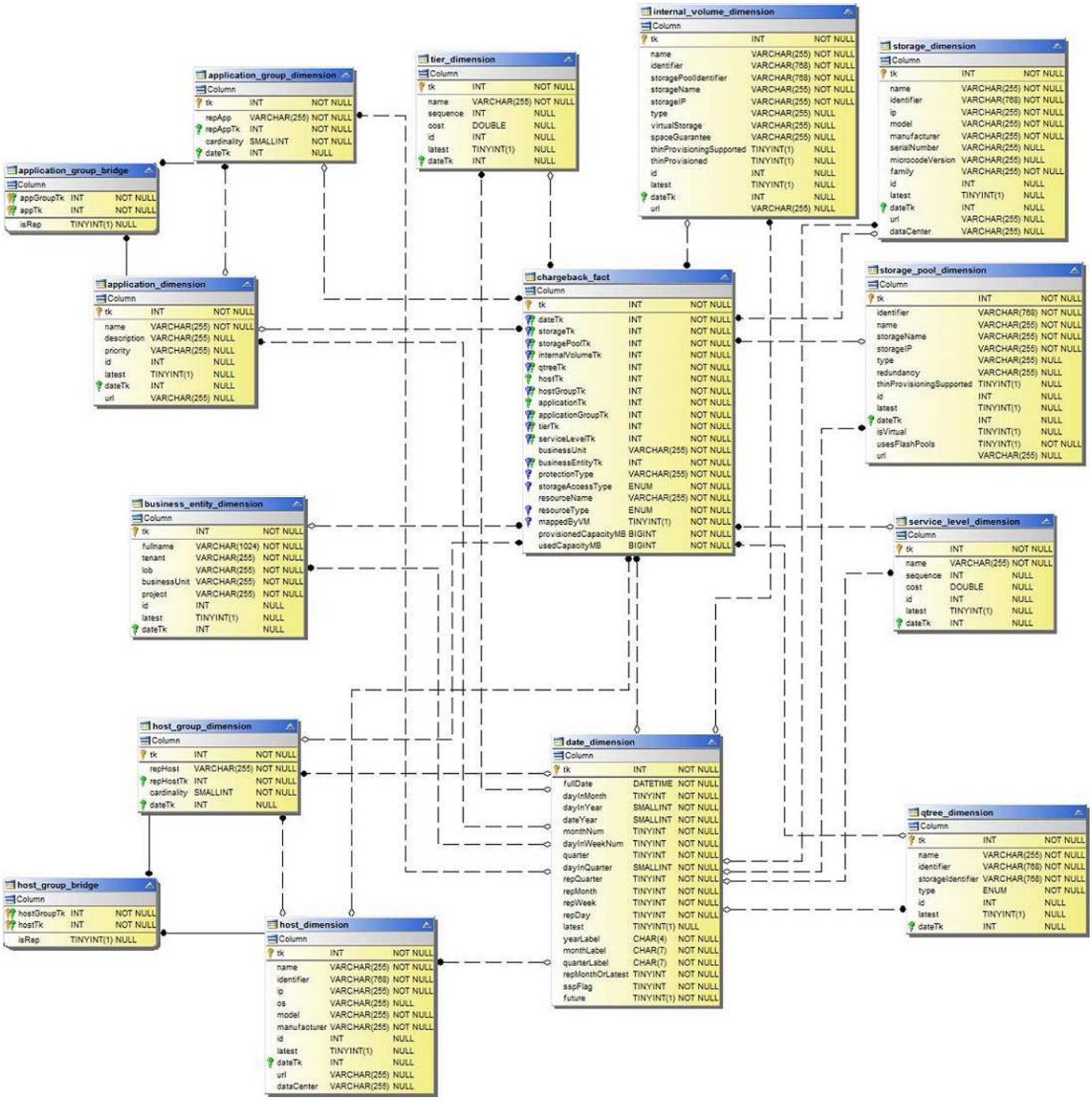
VM



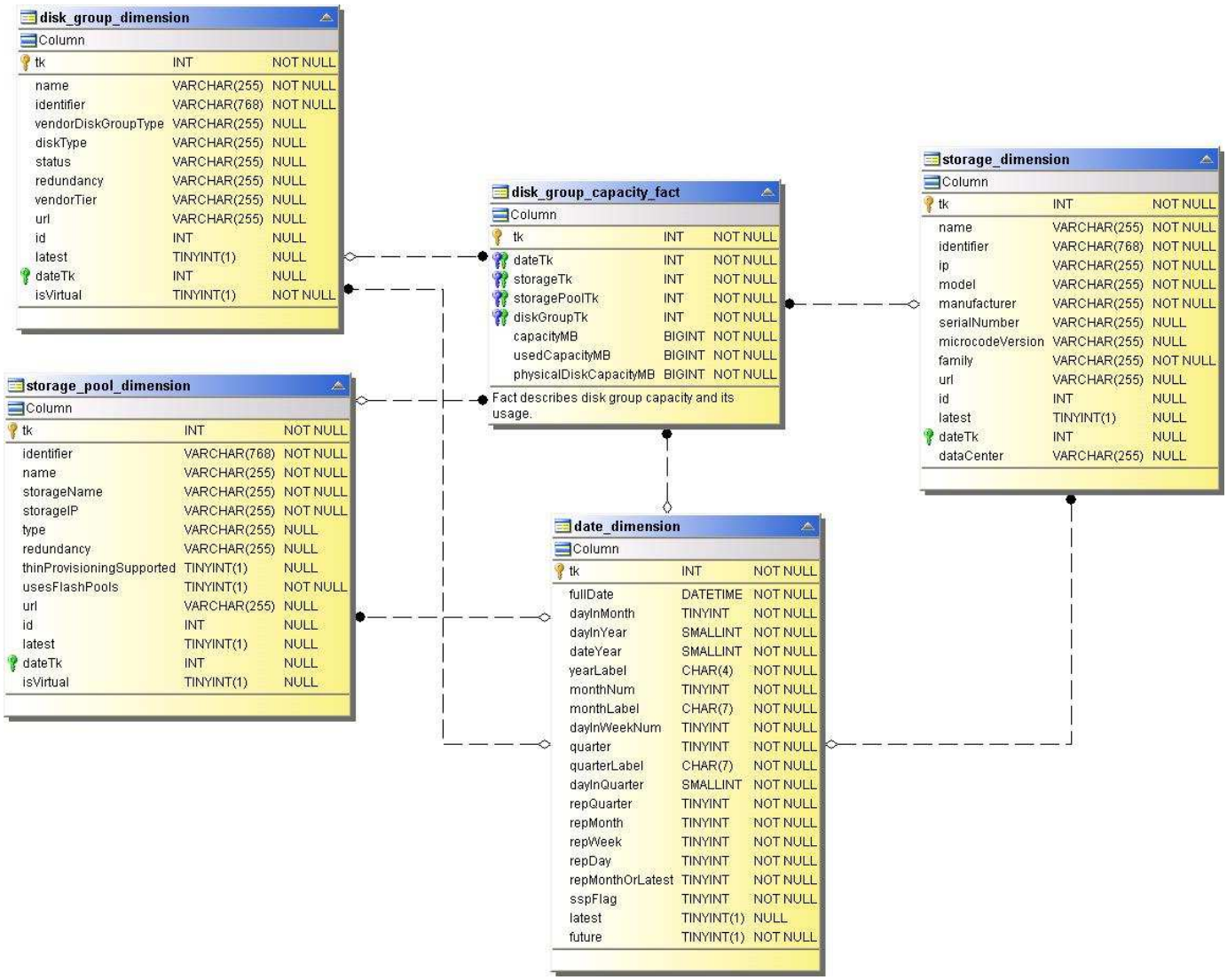
Kapazitätsdatamart

Die folgenden Bilder beschreiben die Datenkapazität.

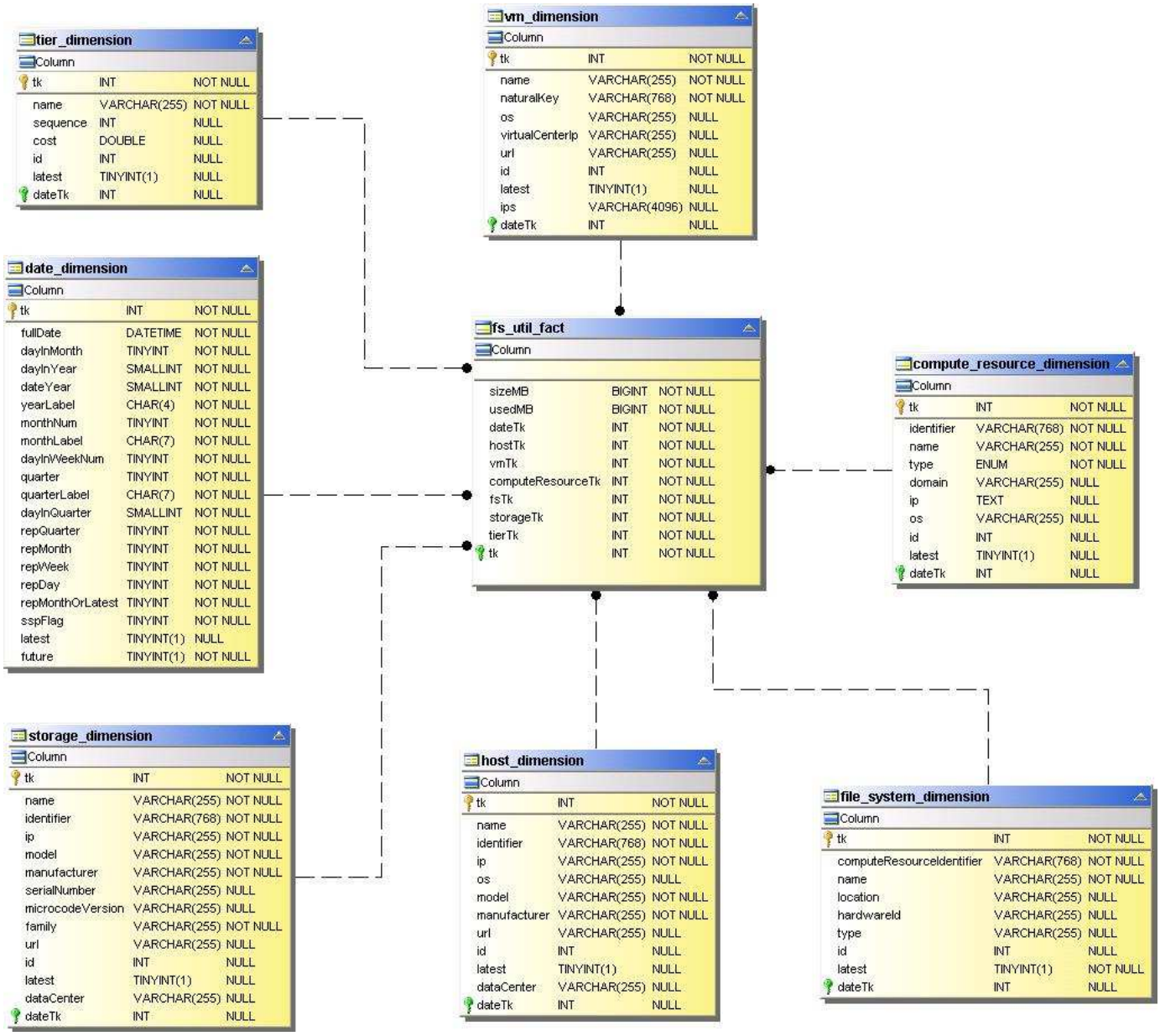
Kostenverrechnung



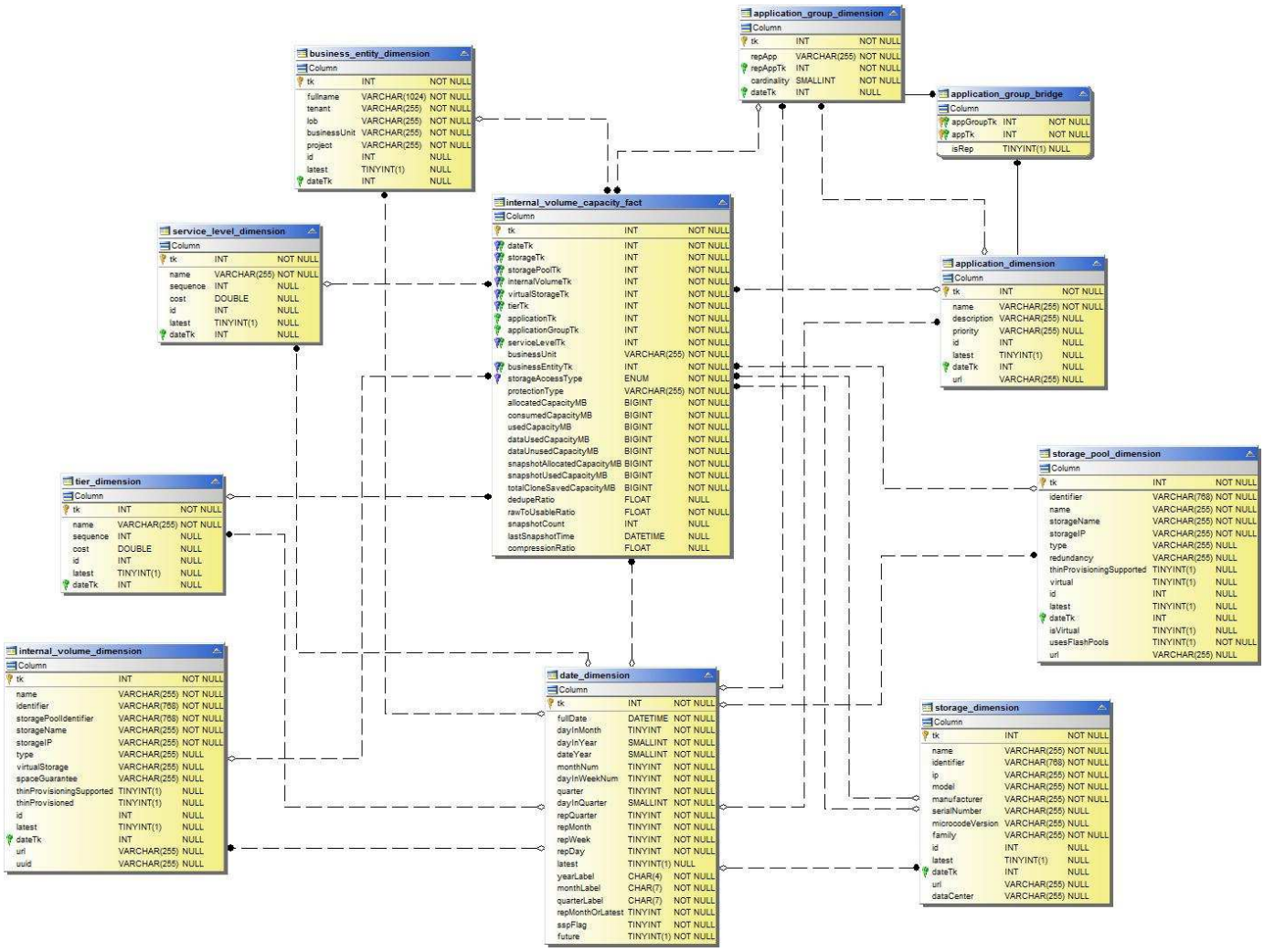
Kapazität Der Festplattengruppe



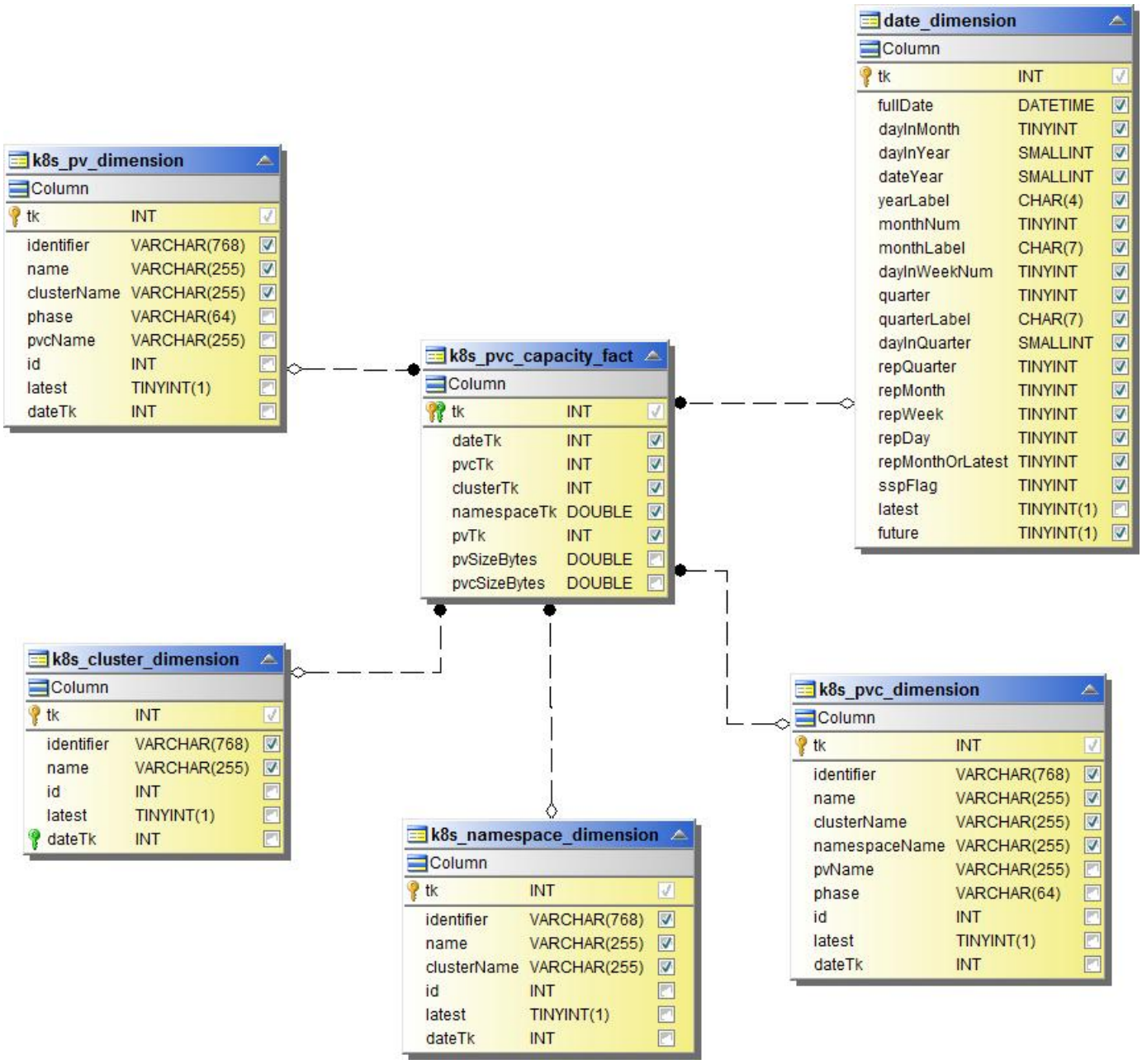
Auslastung Des Filesystems



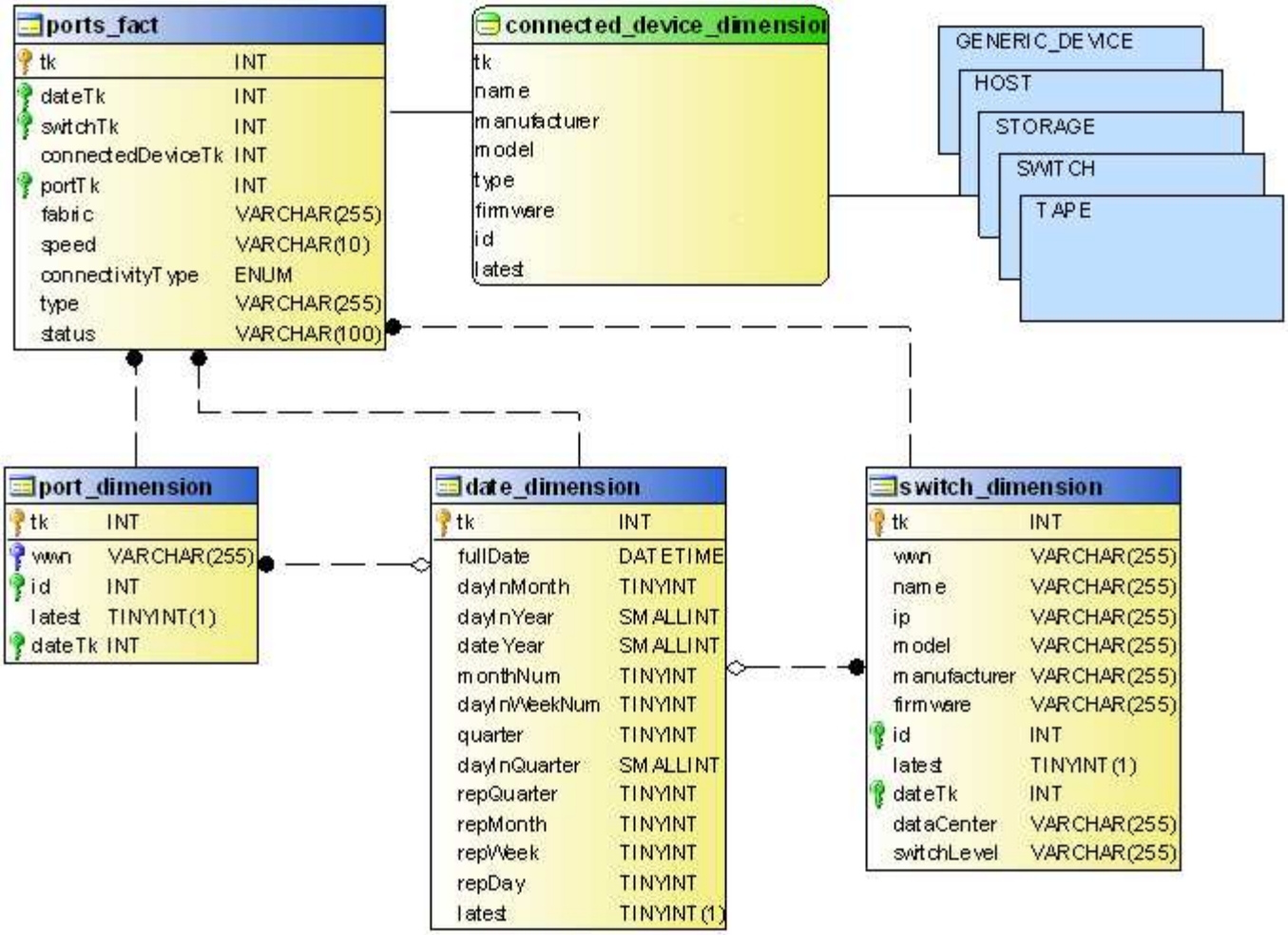
Kapazität Des Internen Volumes



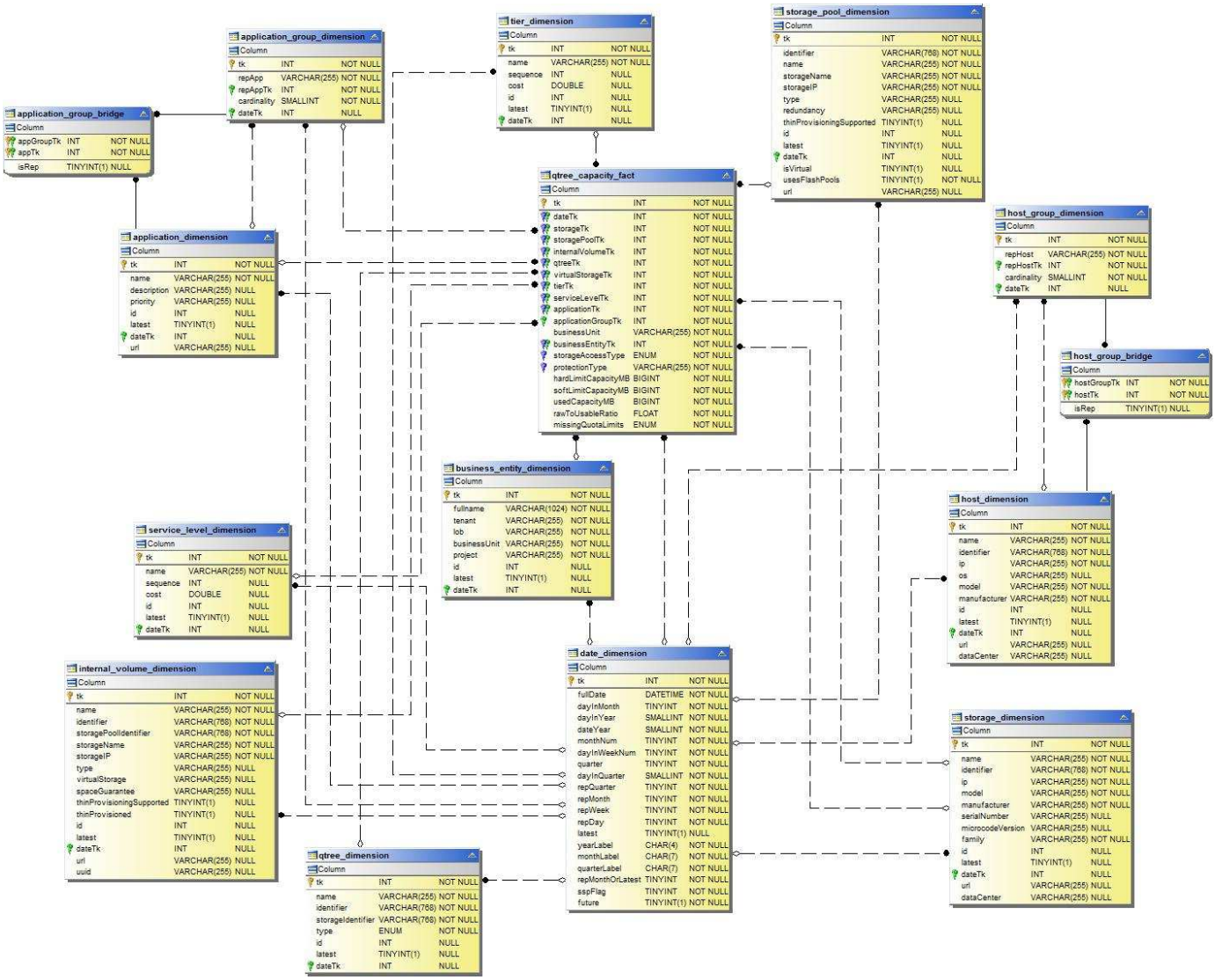
Kubernetes PV-Kapazität



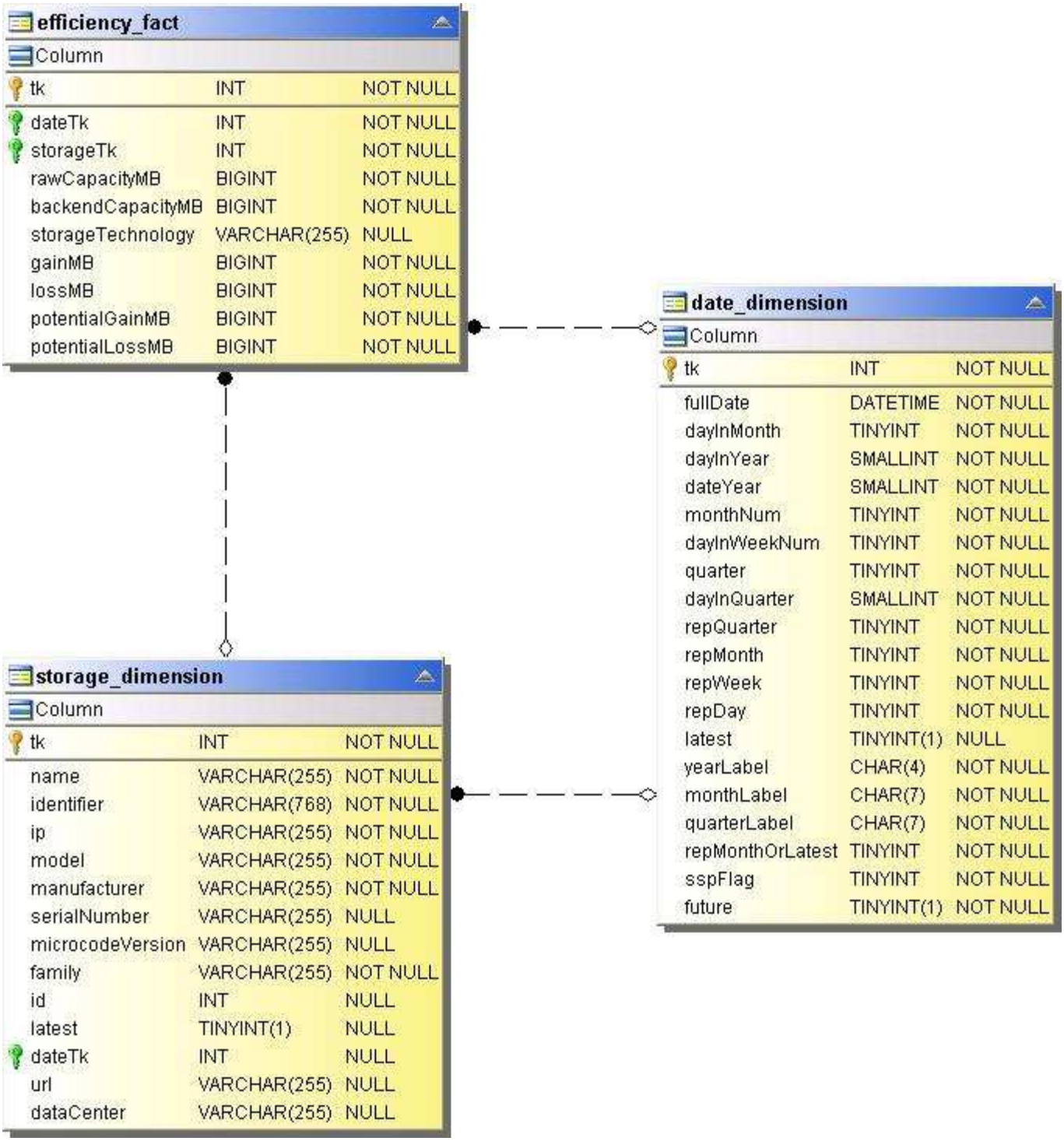
Port-Kapazität



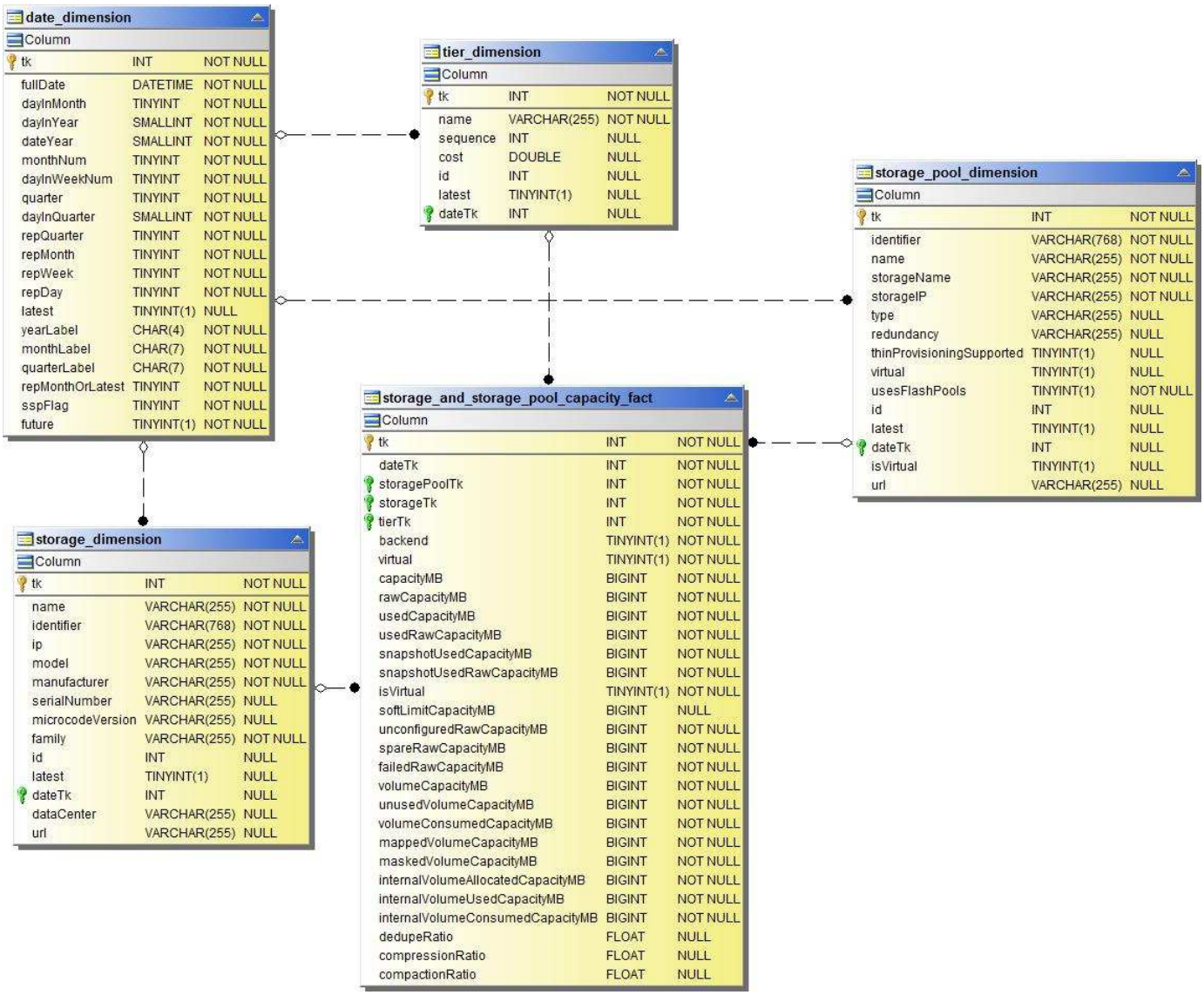
Qtree-Kapazität



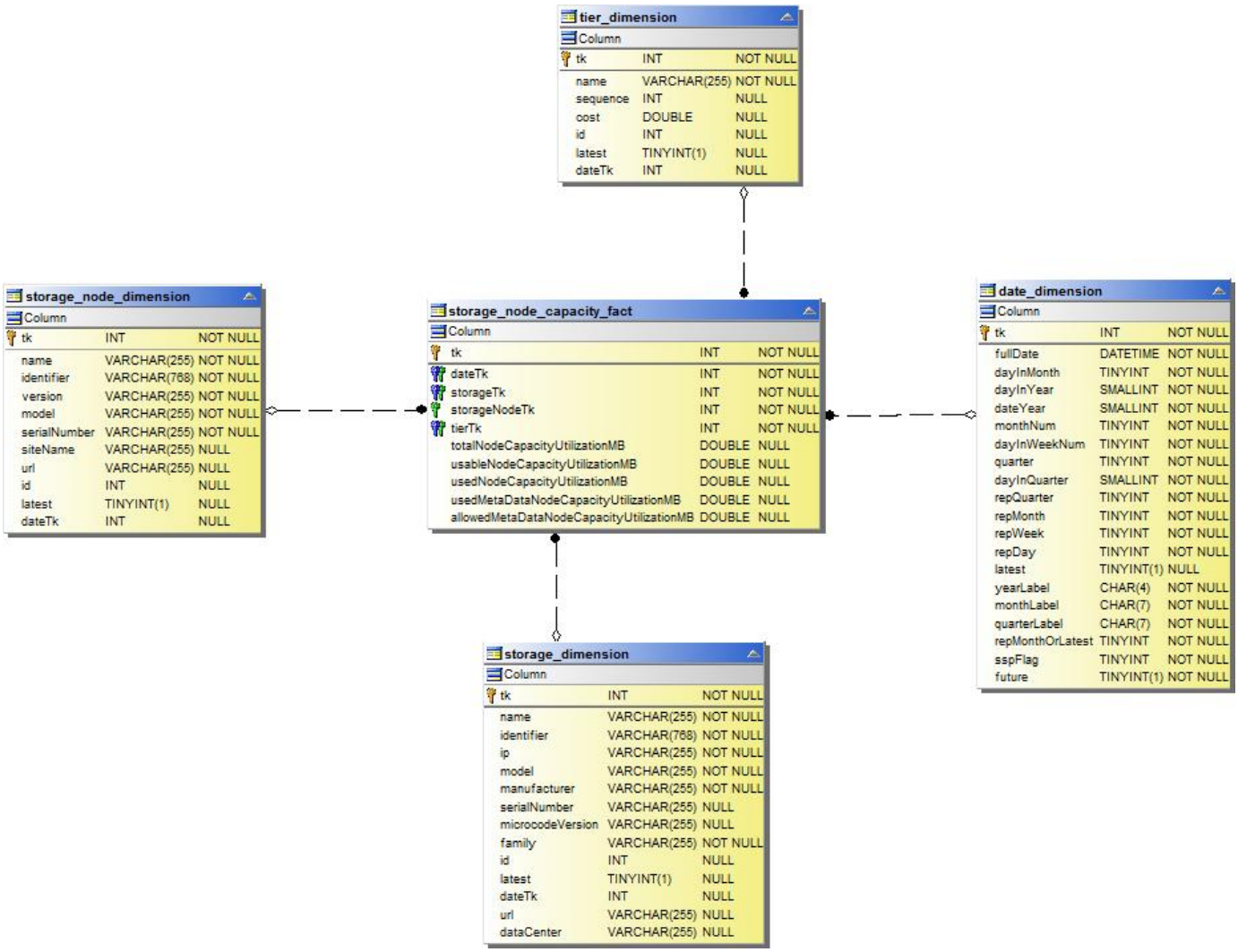
Storage-Kapazitätseffizienz



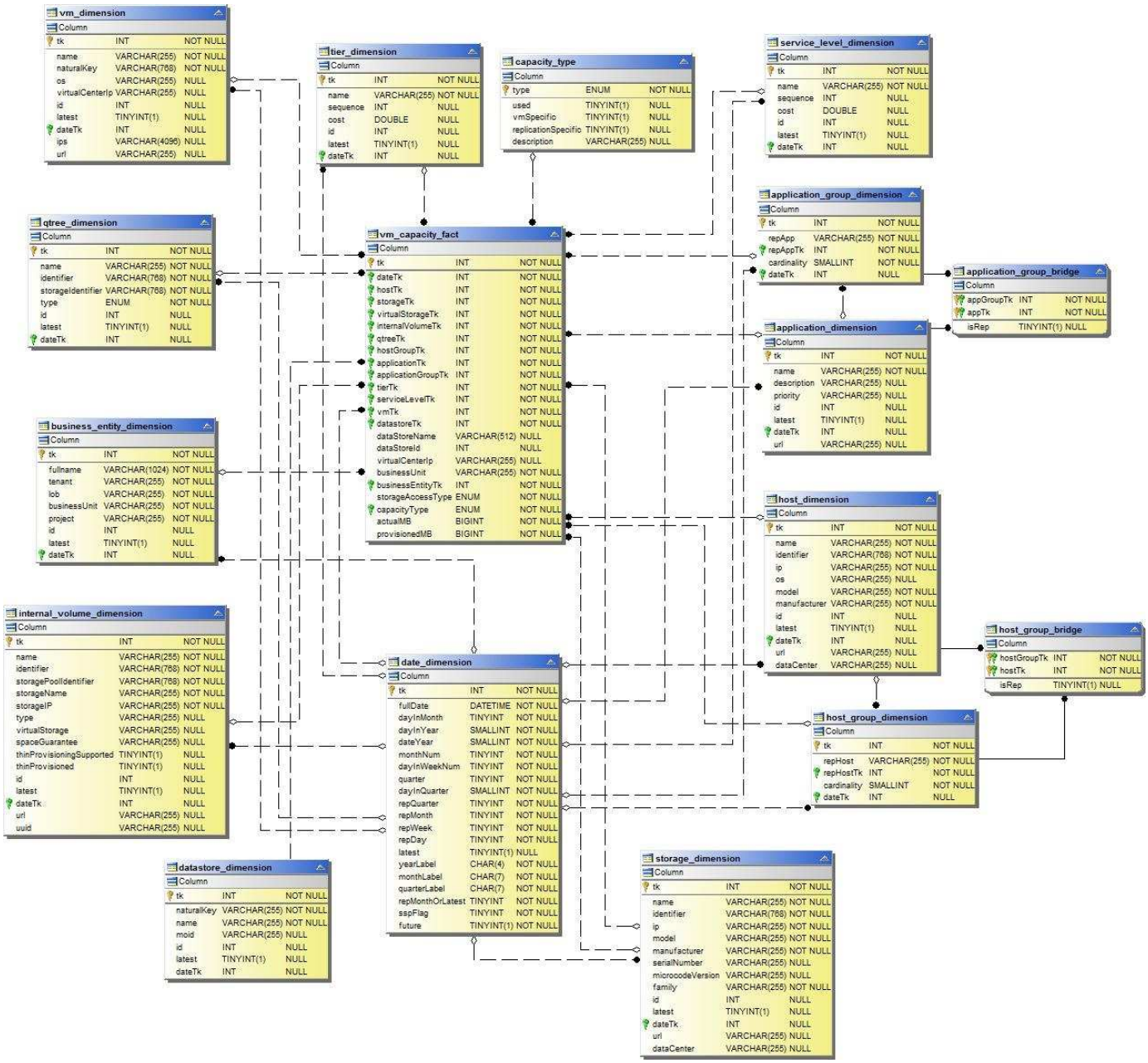
Kapazität im Storage- und Speicherpool



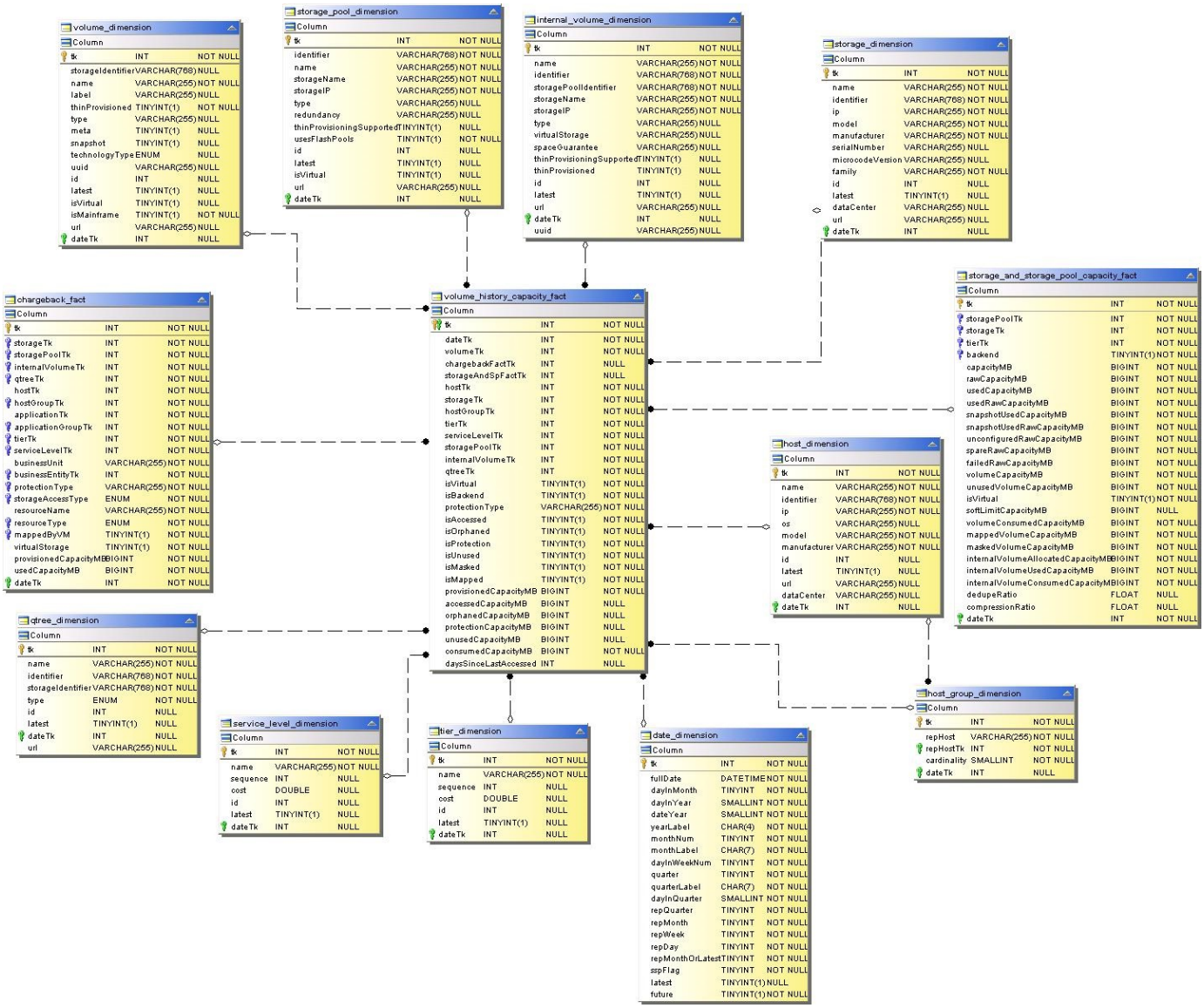
Kapazität Des Storage-Nodes



VM-Kapazität



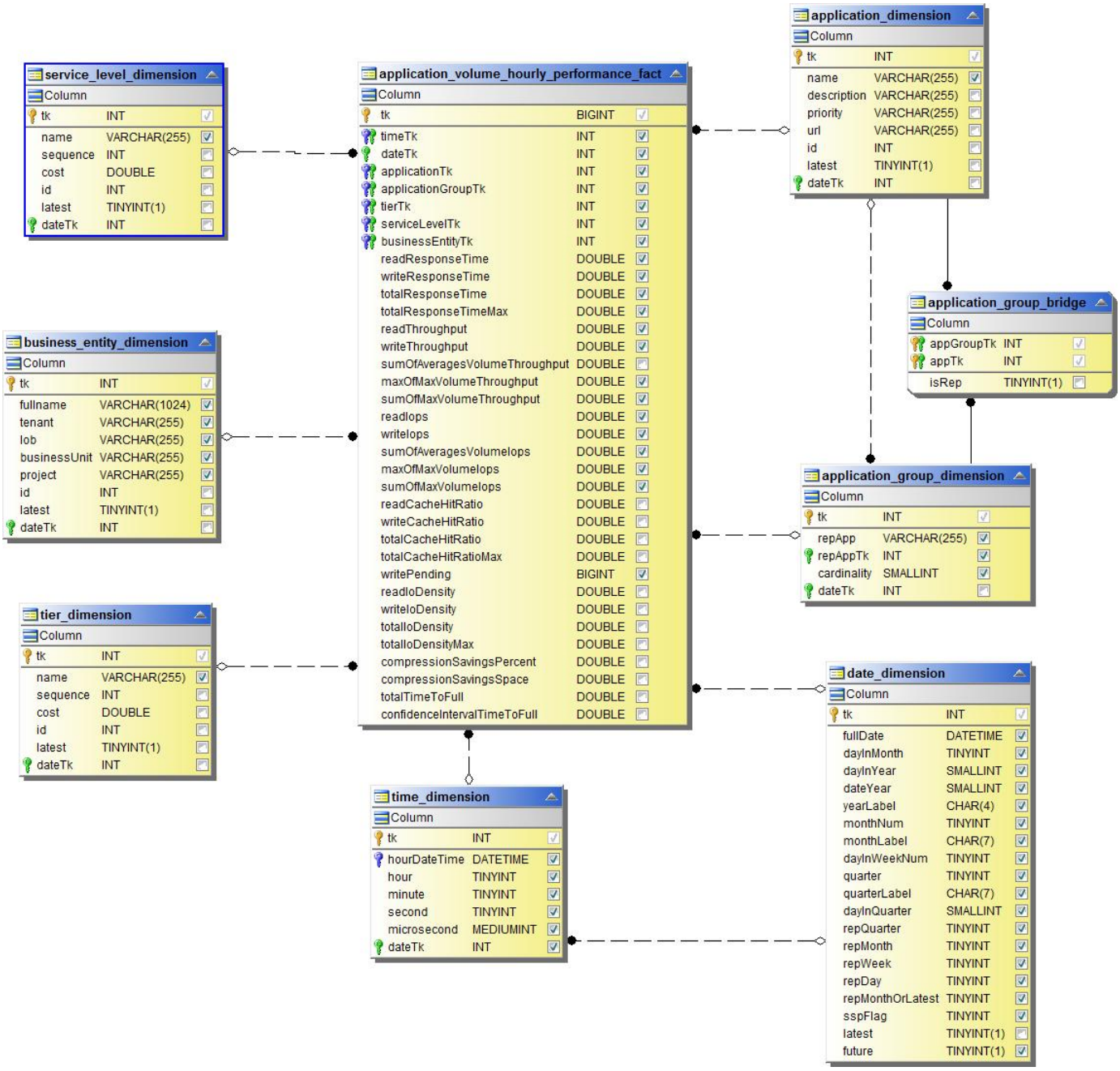
Volume-Kapazität



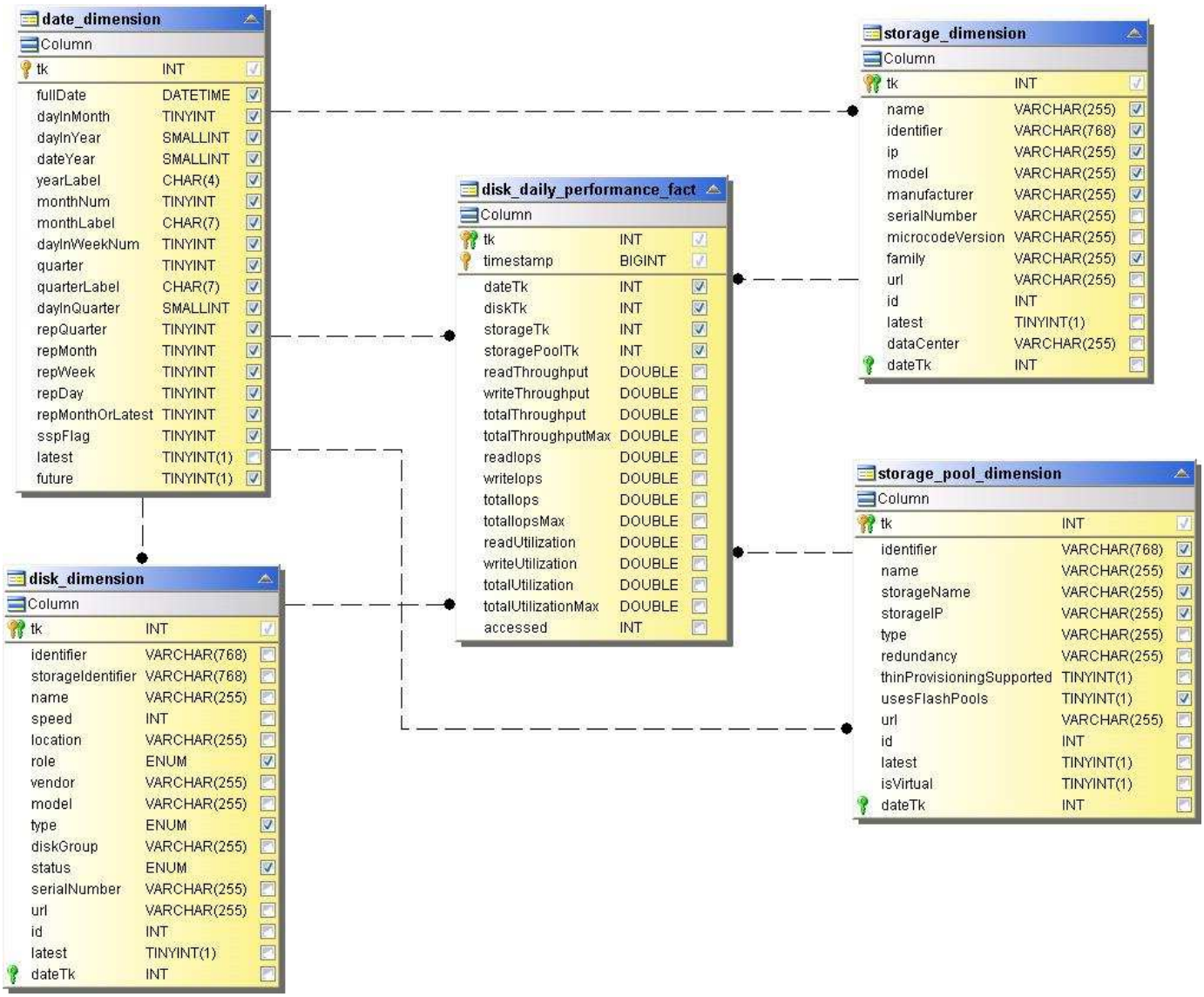
Performance Datamart

Die folgenden Bilder beschreiben das Performance-Datum.

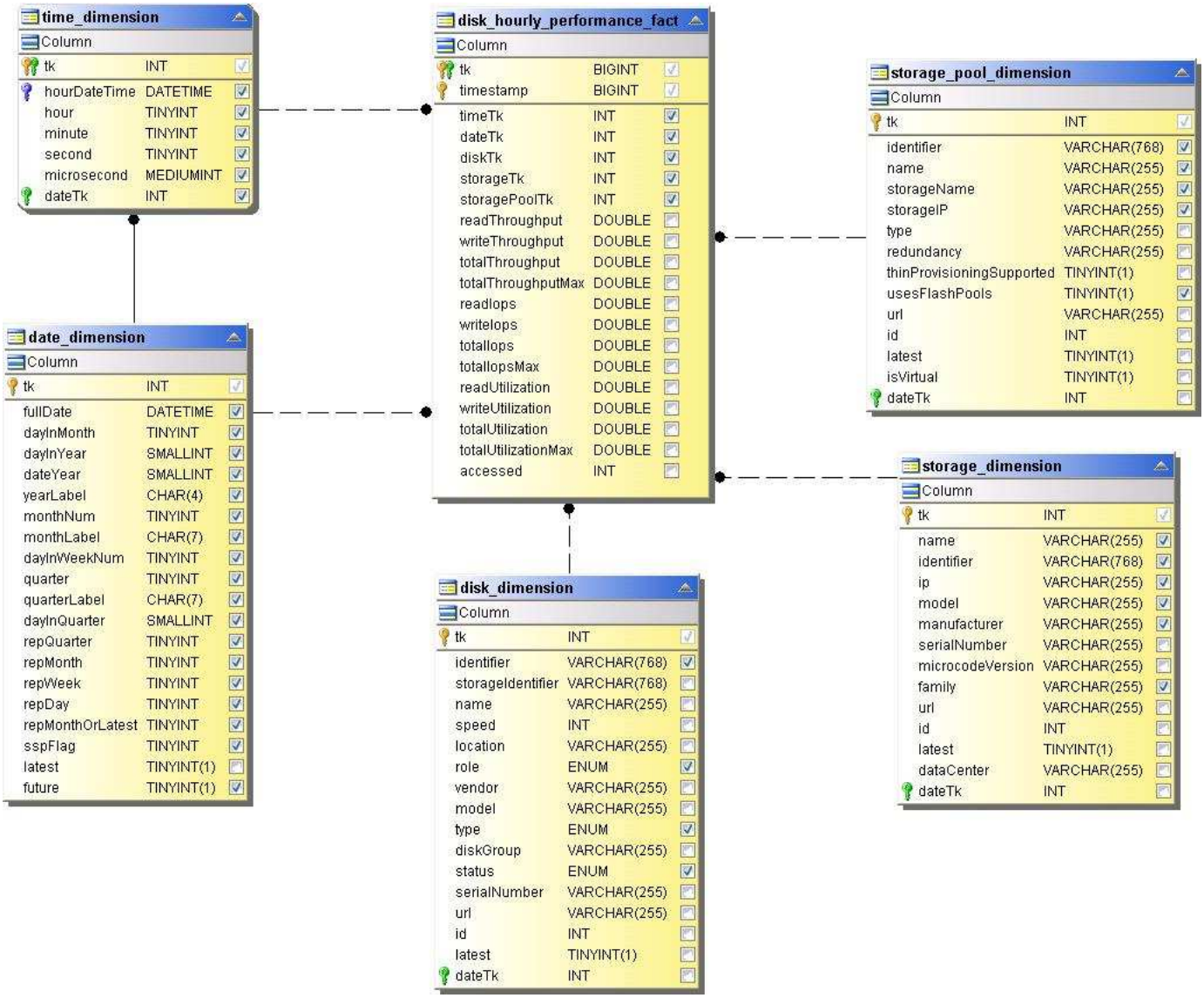
Stündliche Performance Des Applikations-Volumes



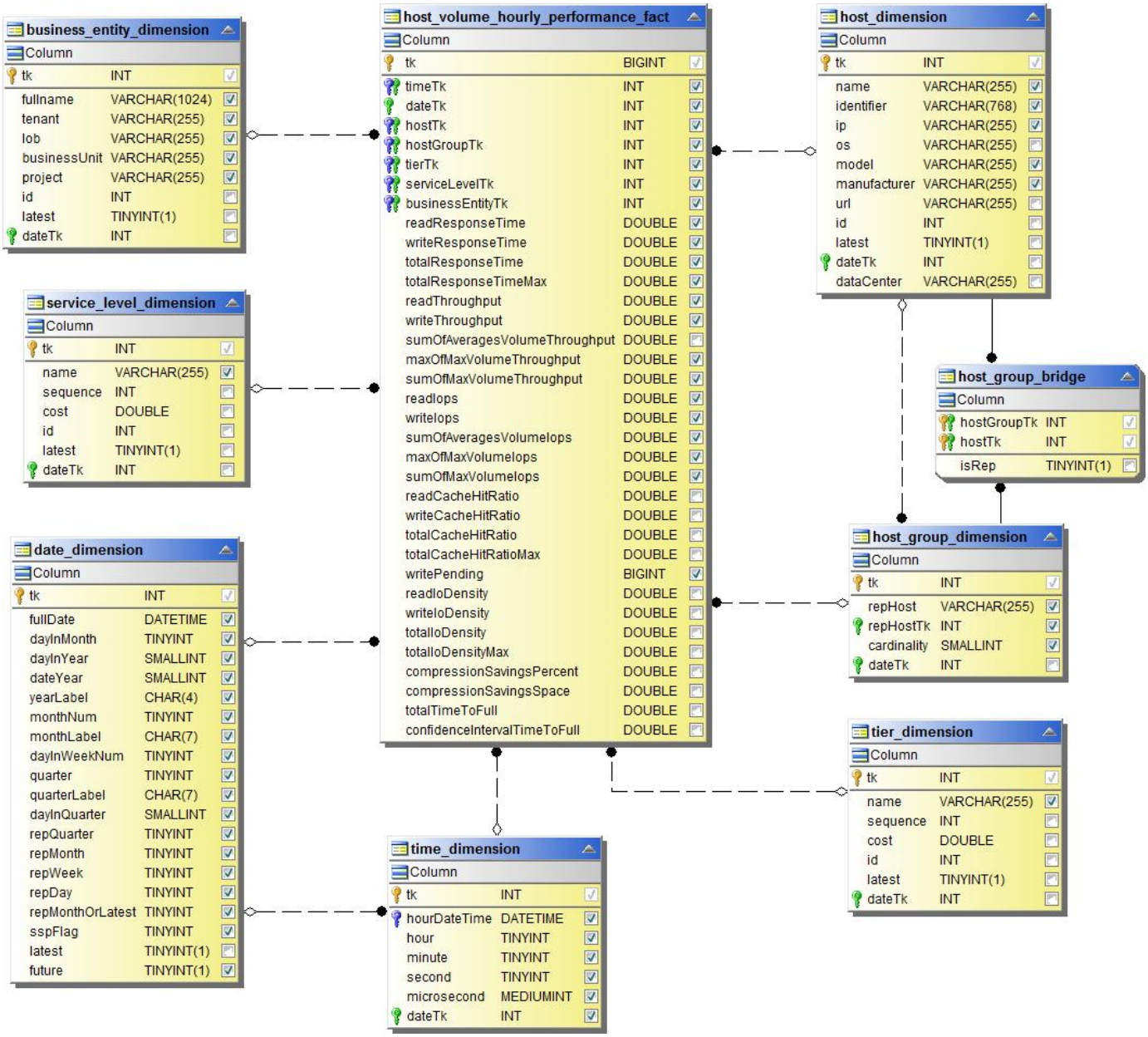
Tägliche Festplatten-Performance



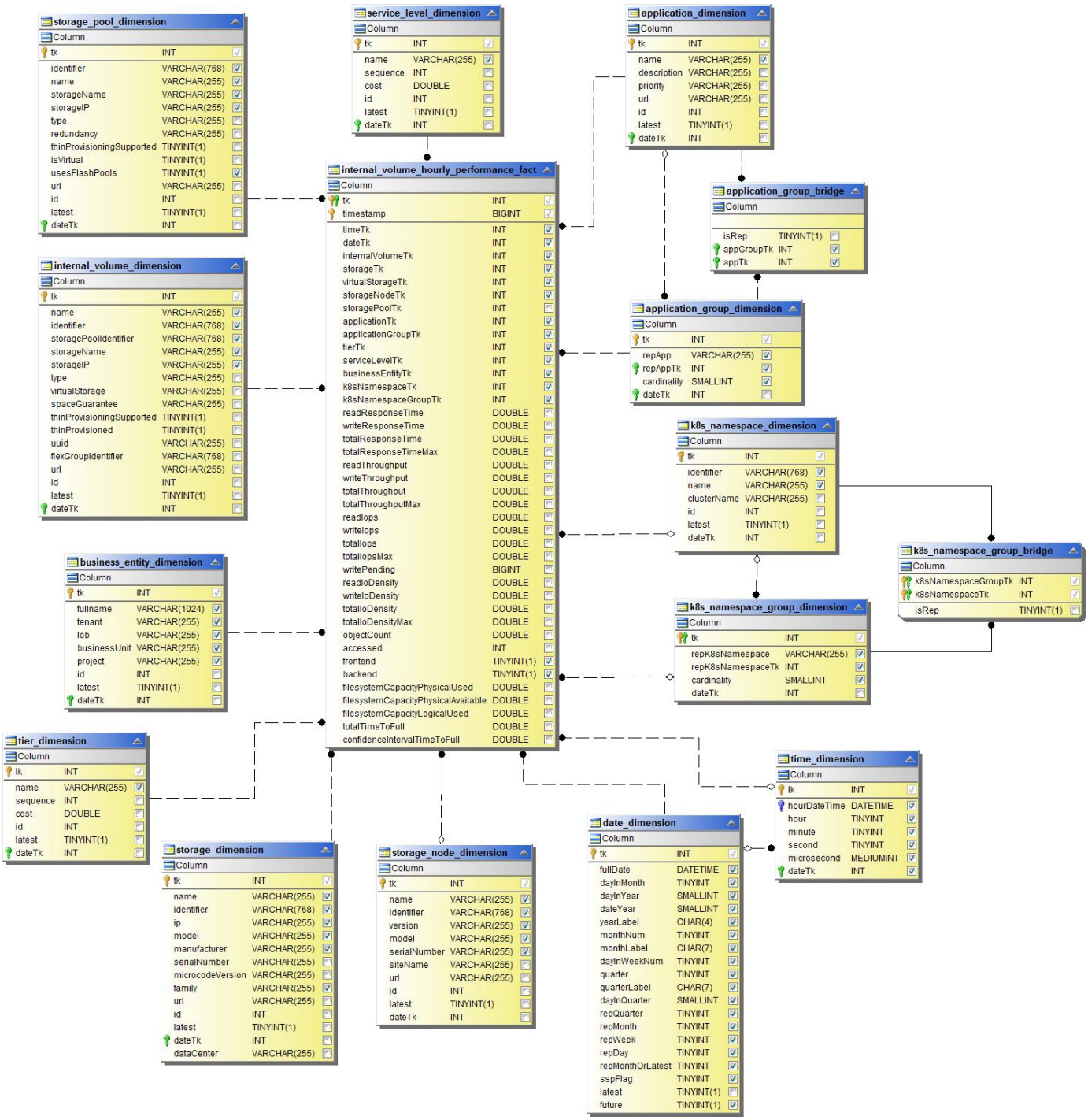
Stündliche Festplatten-Performance



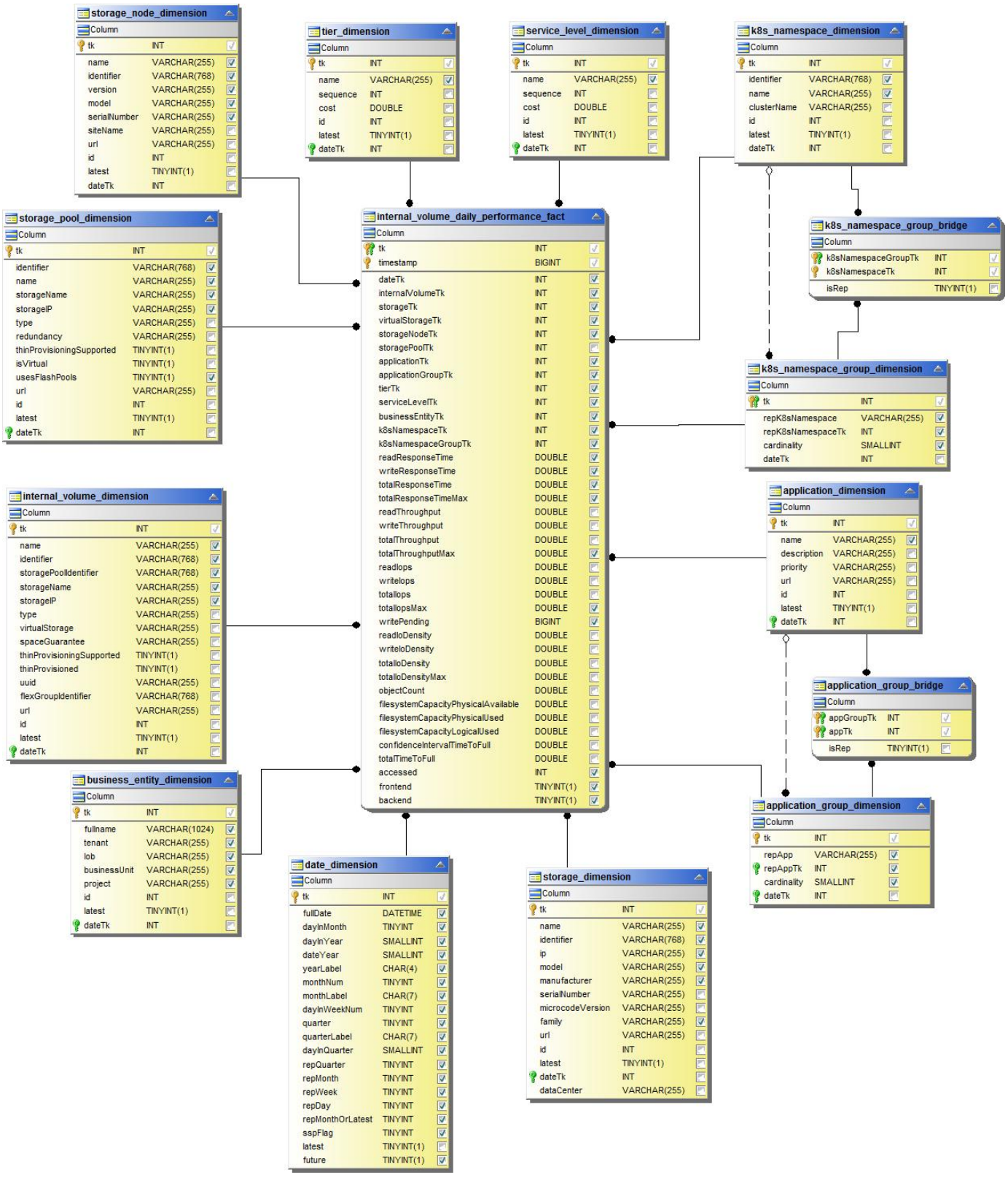
Stündliche Host-Performance



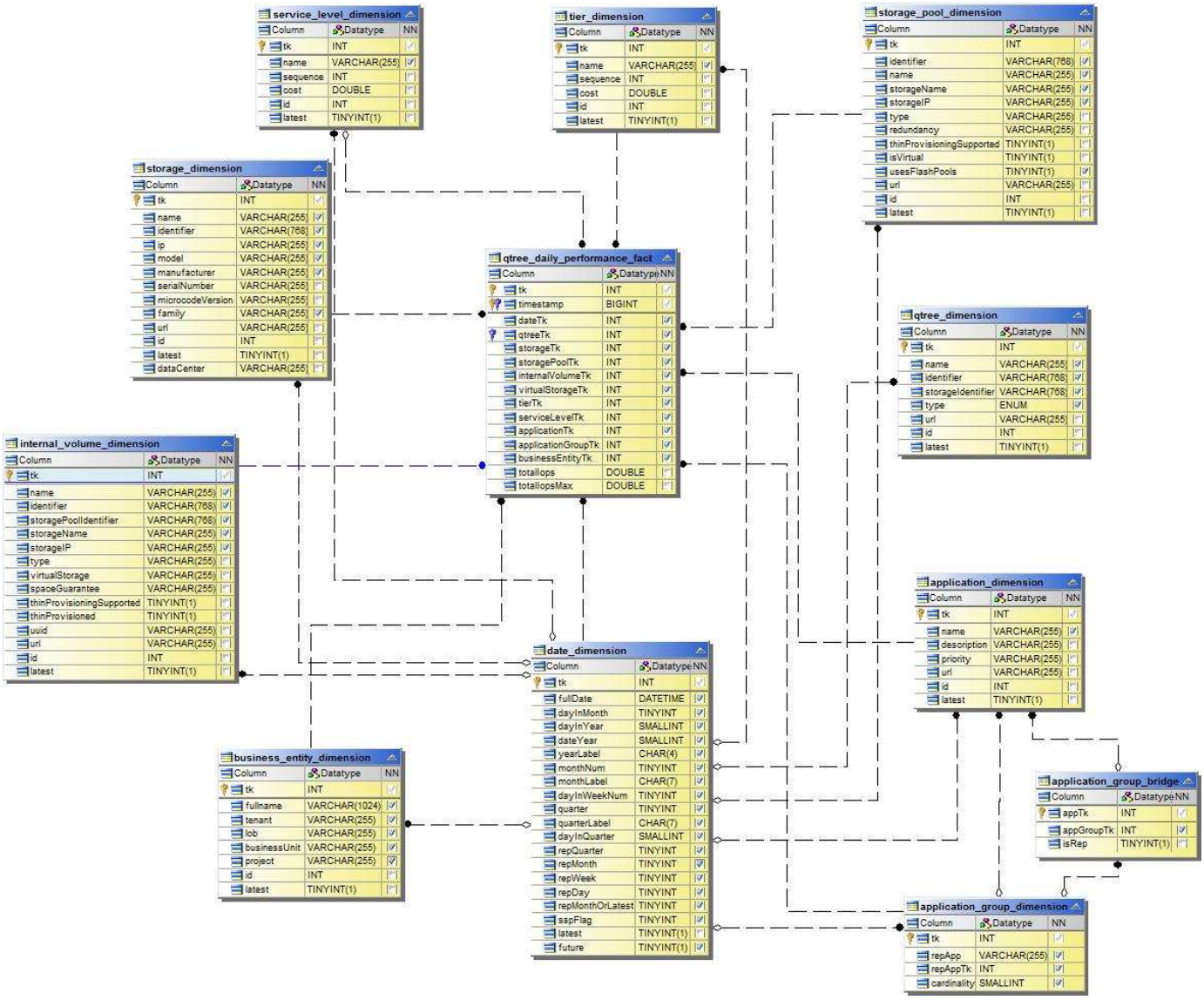
Stündliche Performance Des Internen Volumes



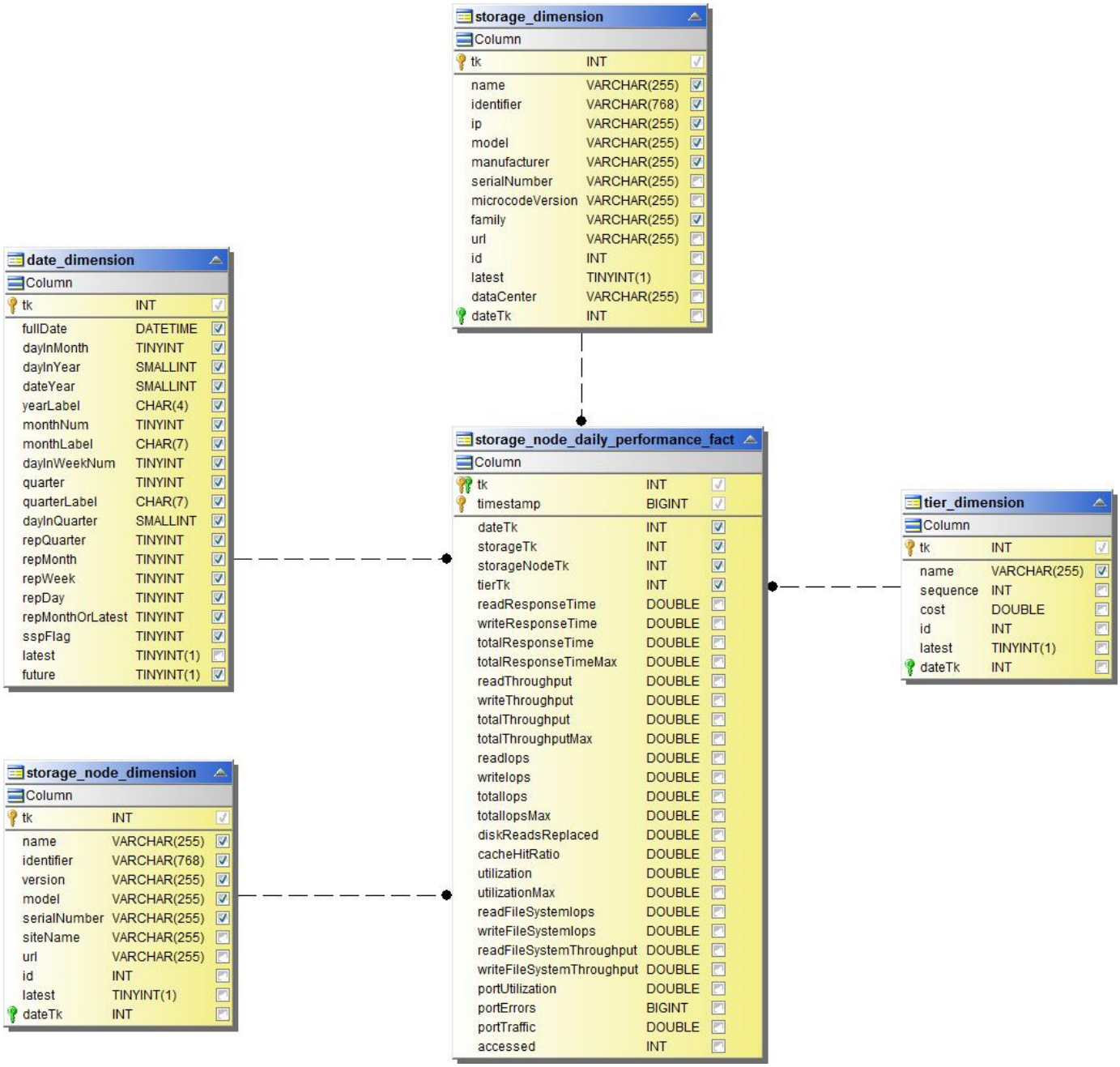
Tägliche Performance Des Internen Volumes



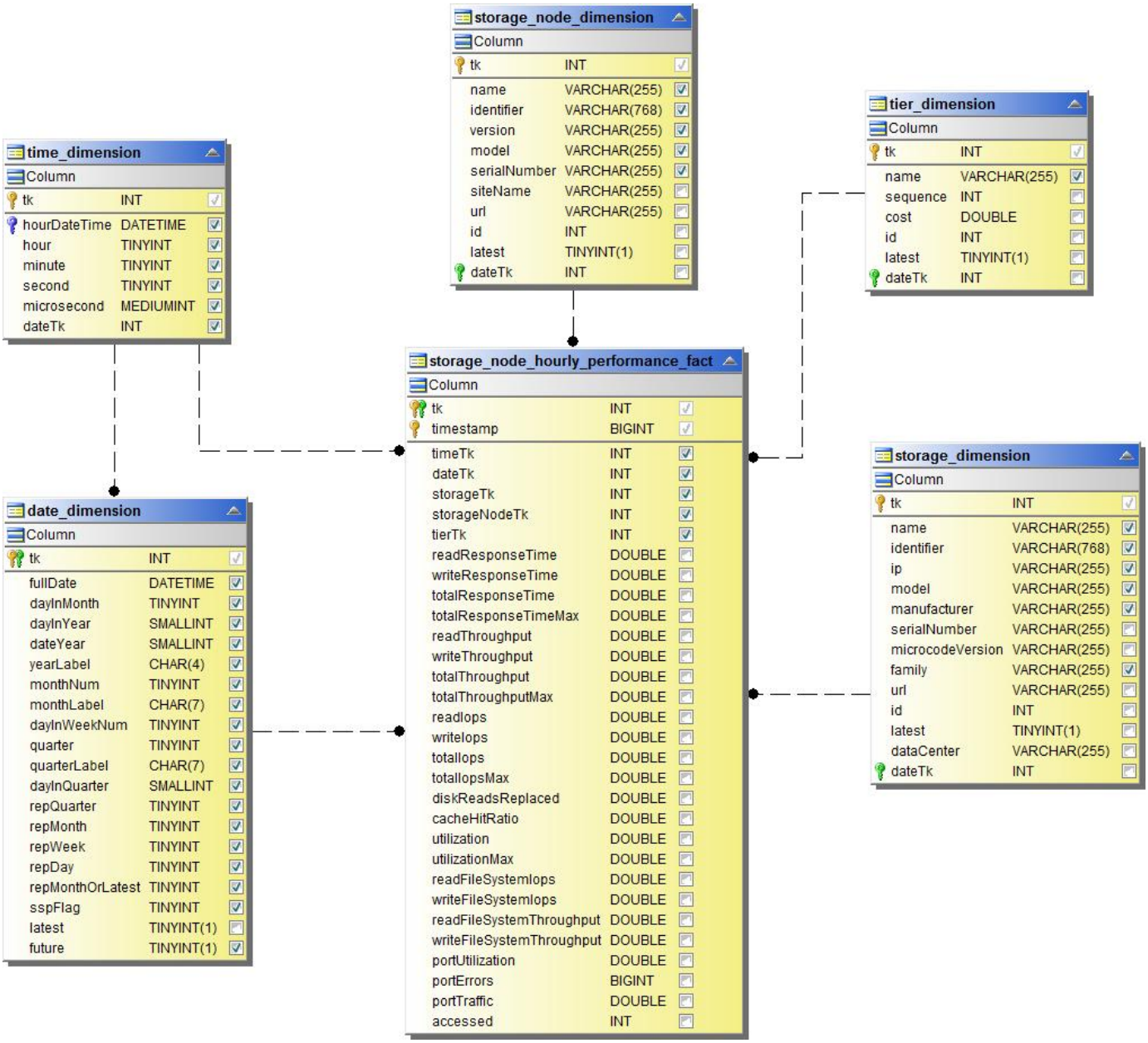
Tägliche Qtree Performance



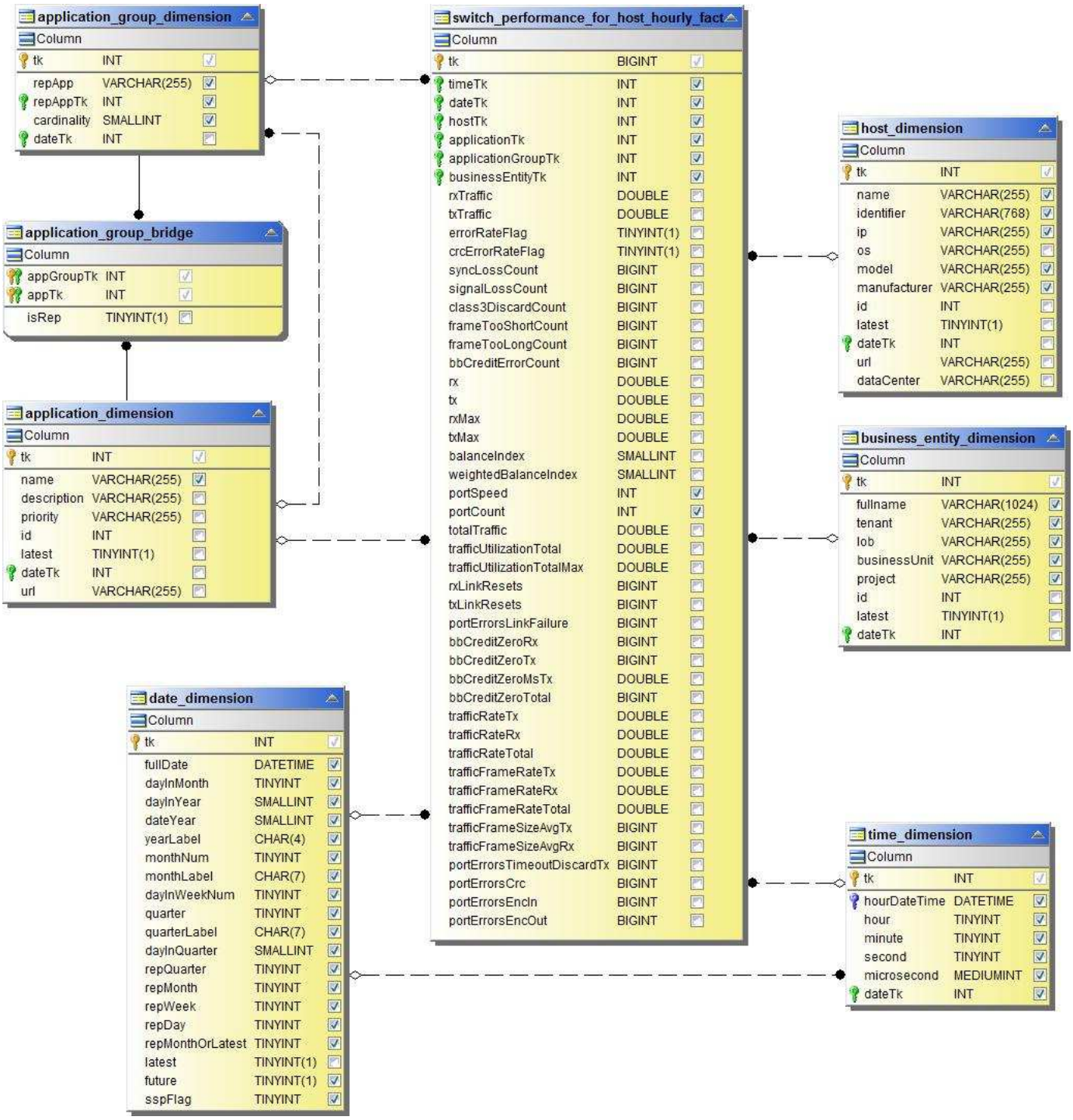
Tägliche Storage-Node-Performance



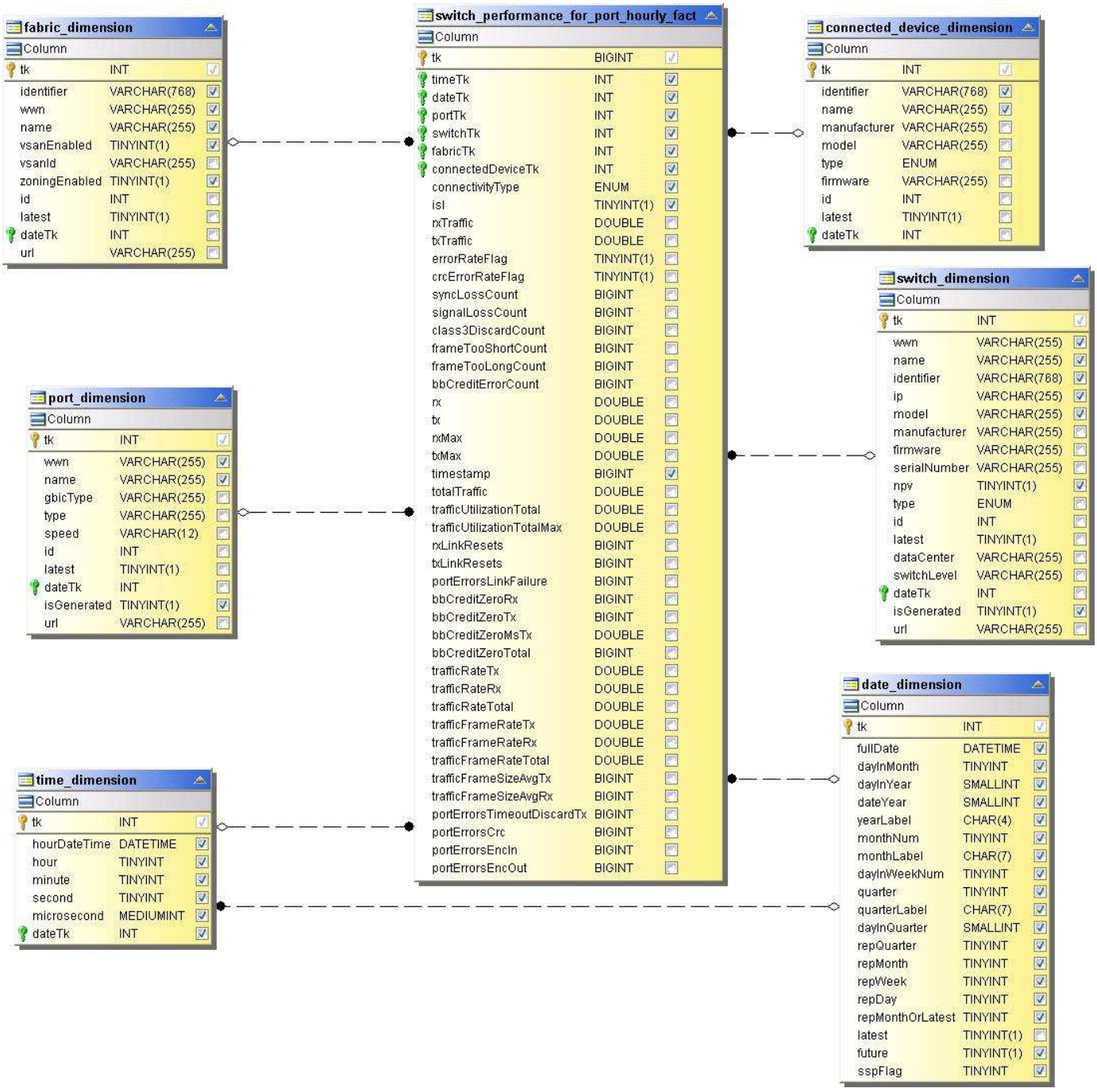
Stündliche Storage-Node-Performance



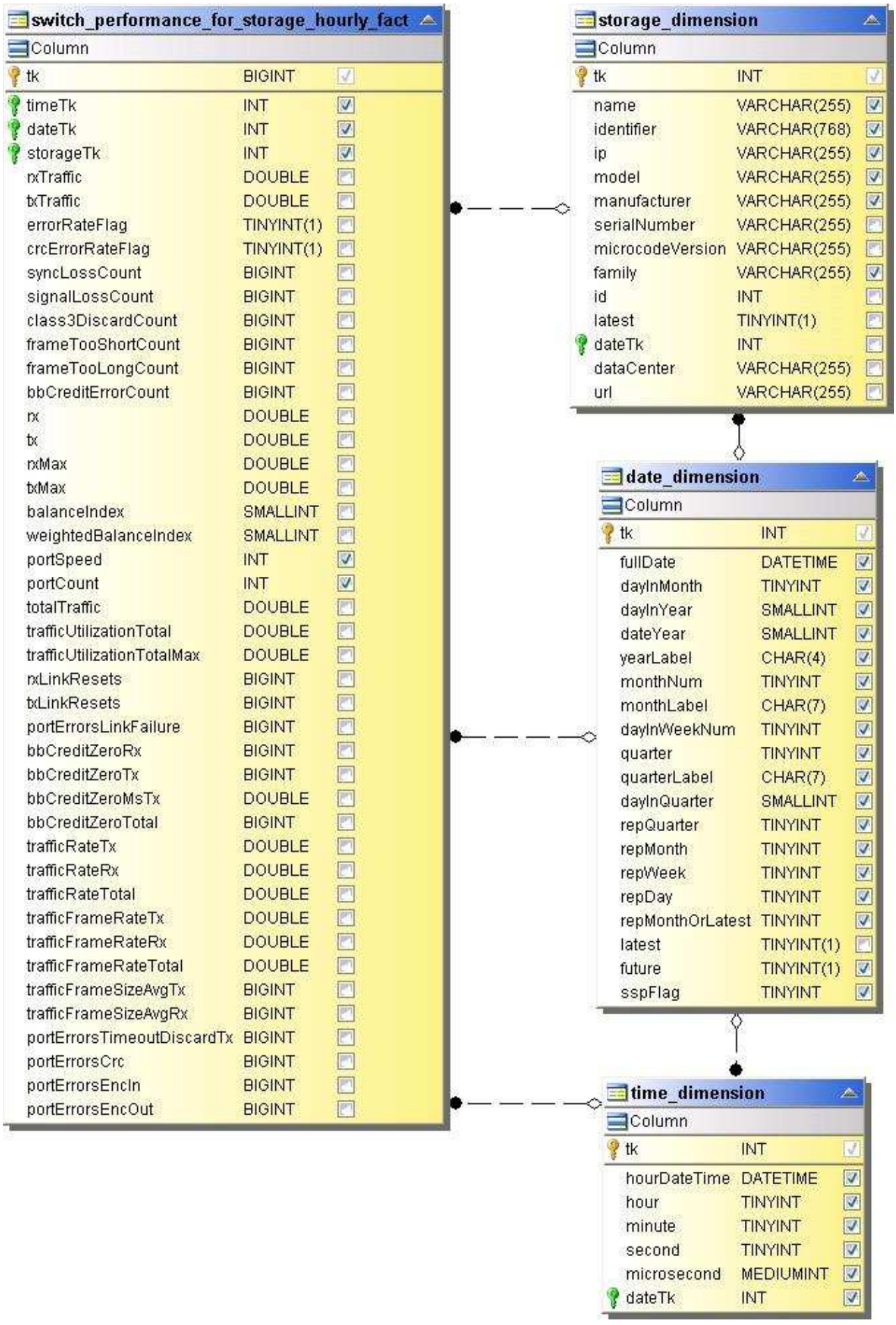
Wechseln Sie die stündliche Performance für den Host



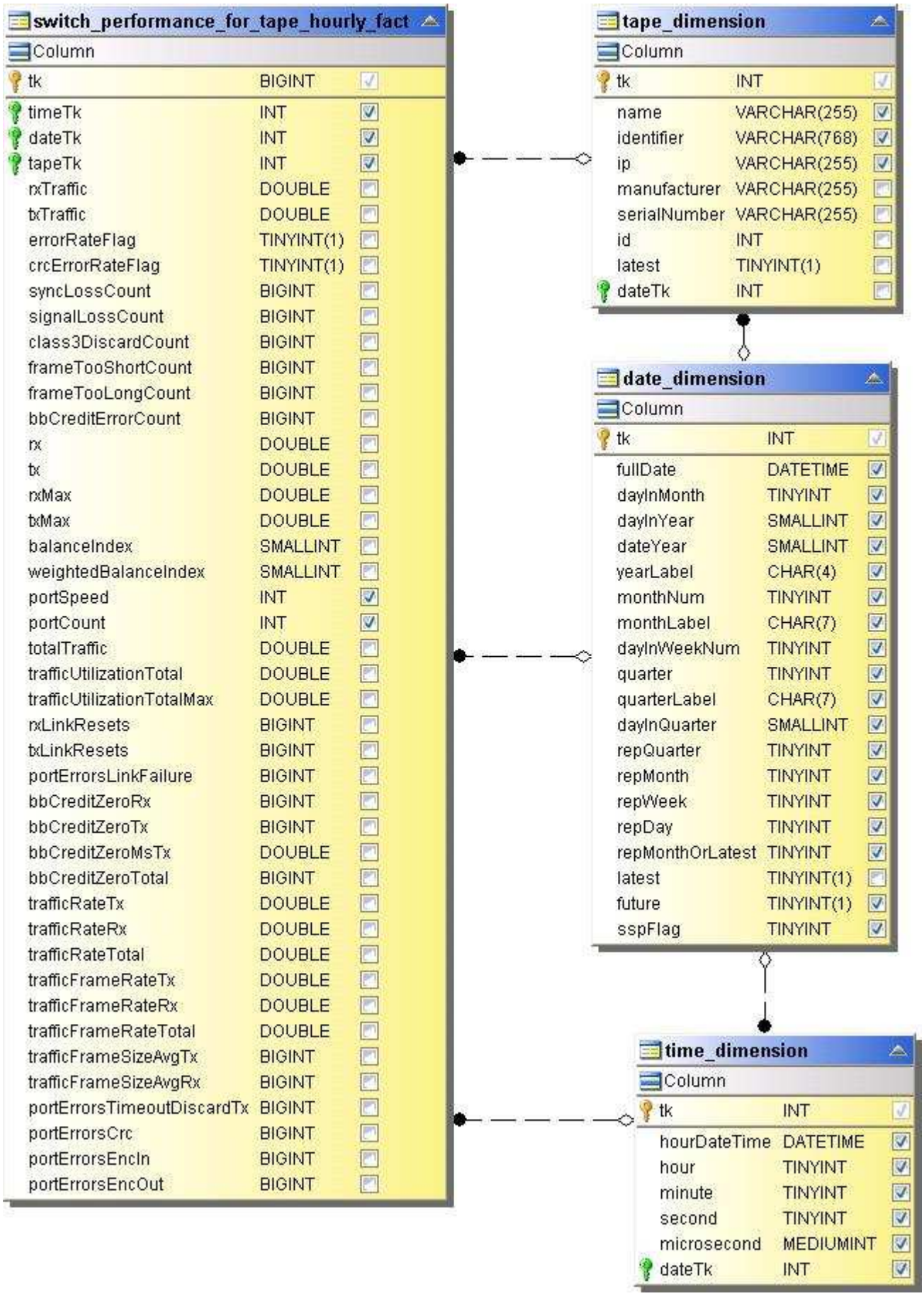
Wechseln Sie die stündliche Leistung für den Port



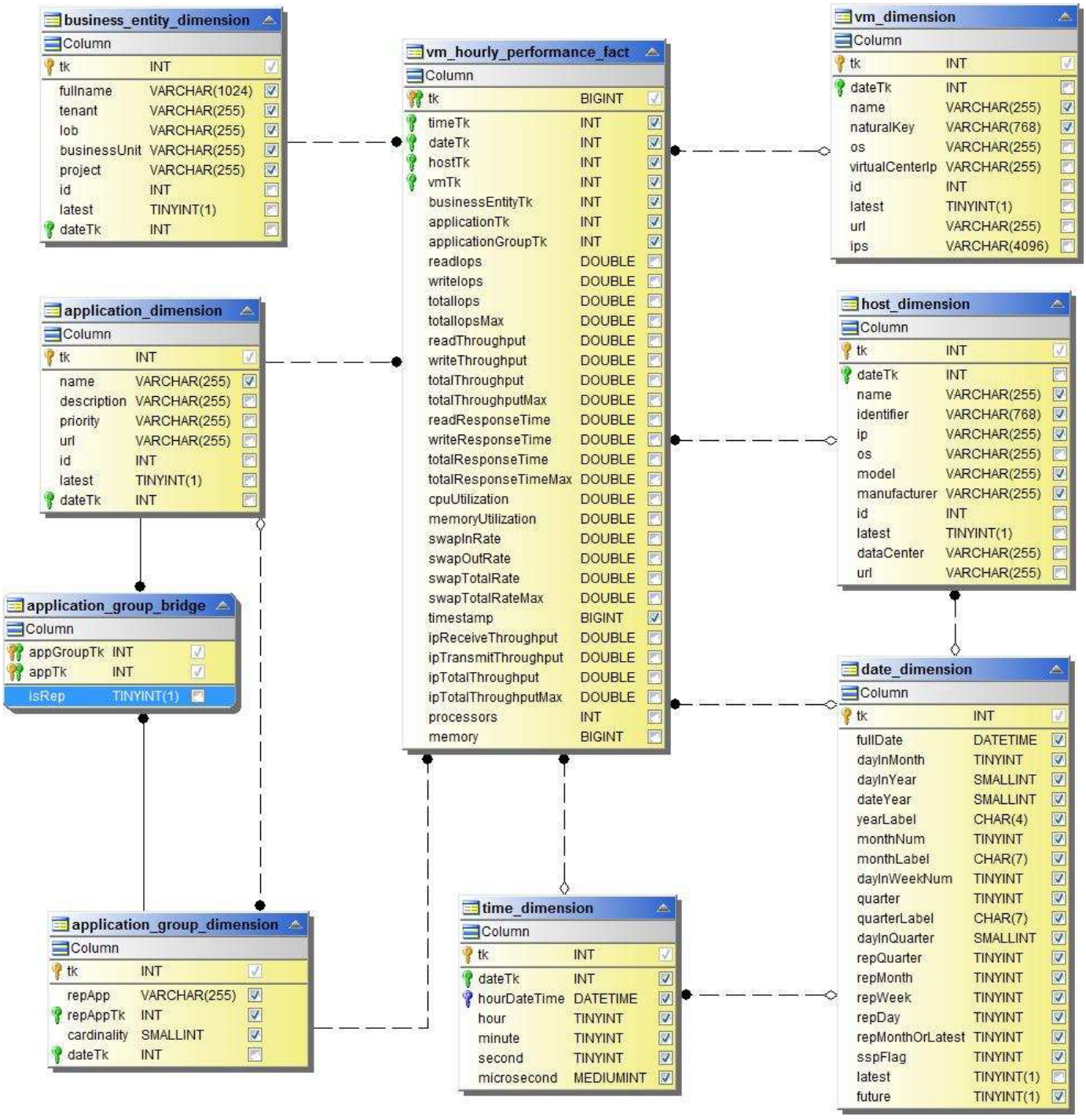
Stündliche Wechsel der Performance für Storage erforderlich


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

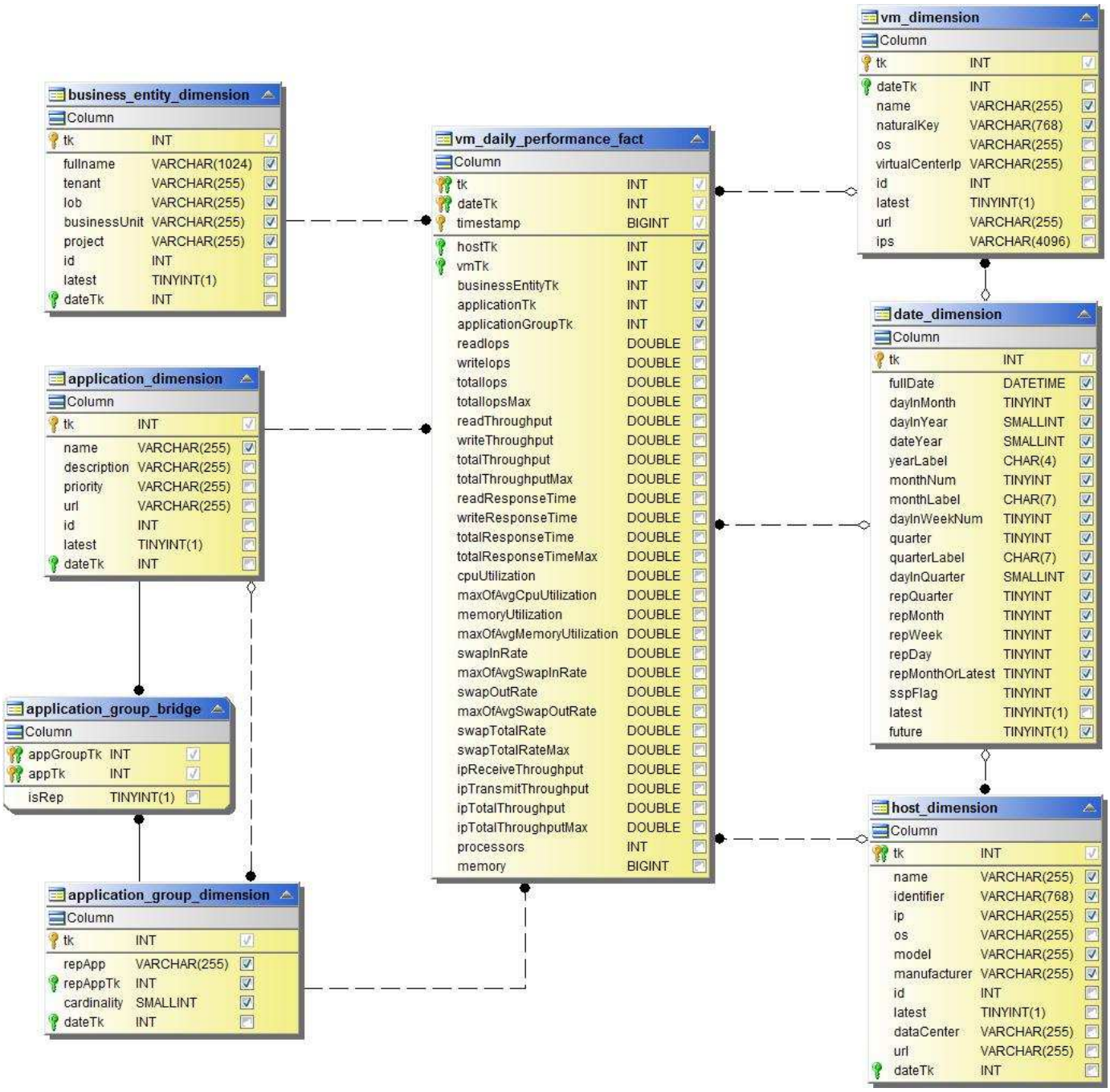
Stündliche Wechsel der Performance für Tape möglich



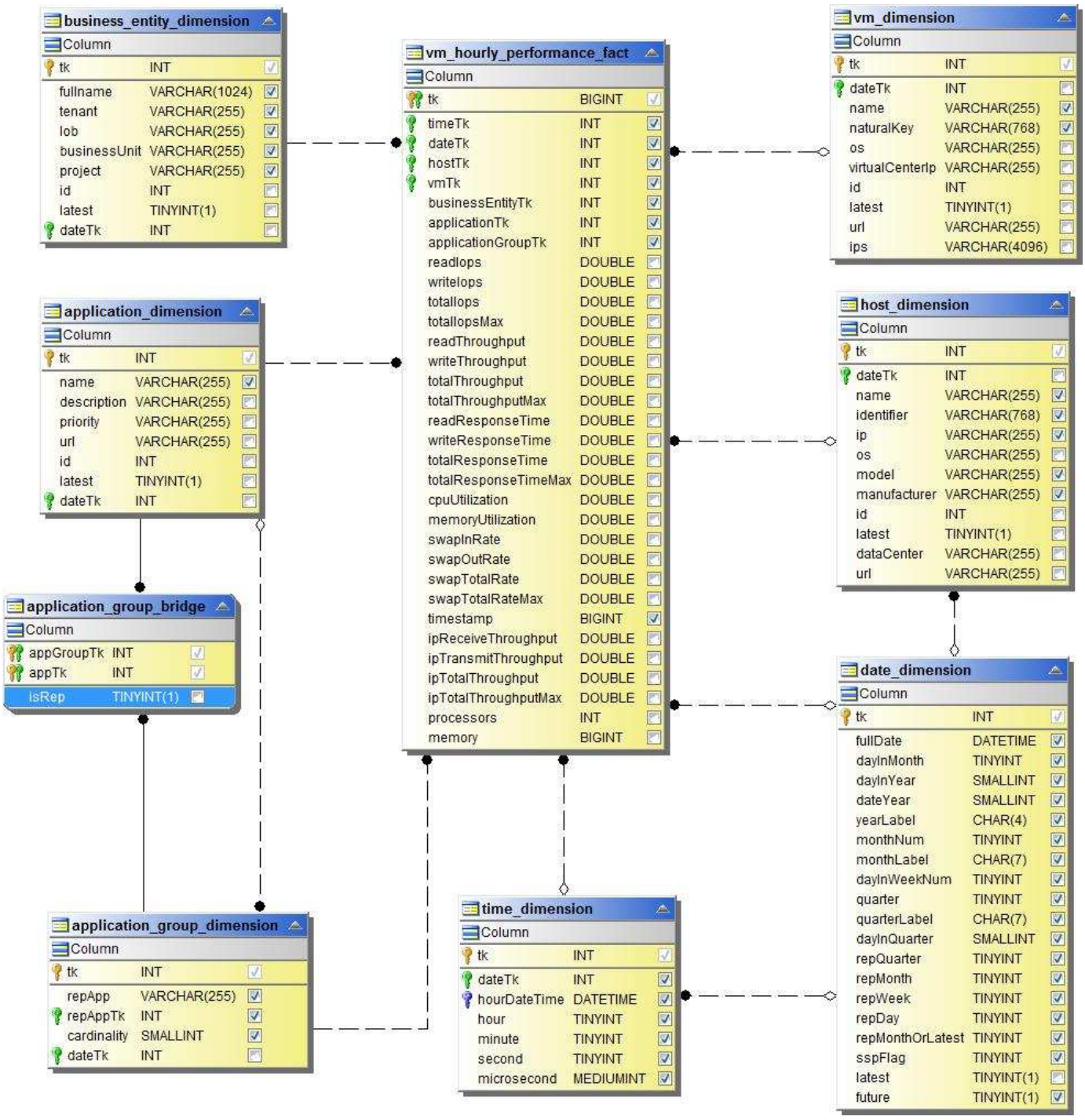
VM Performance



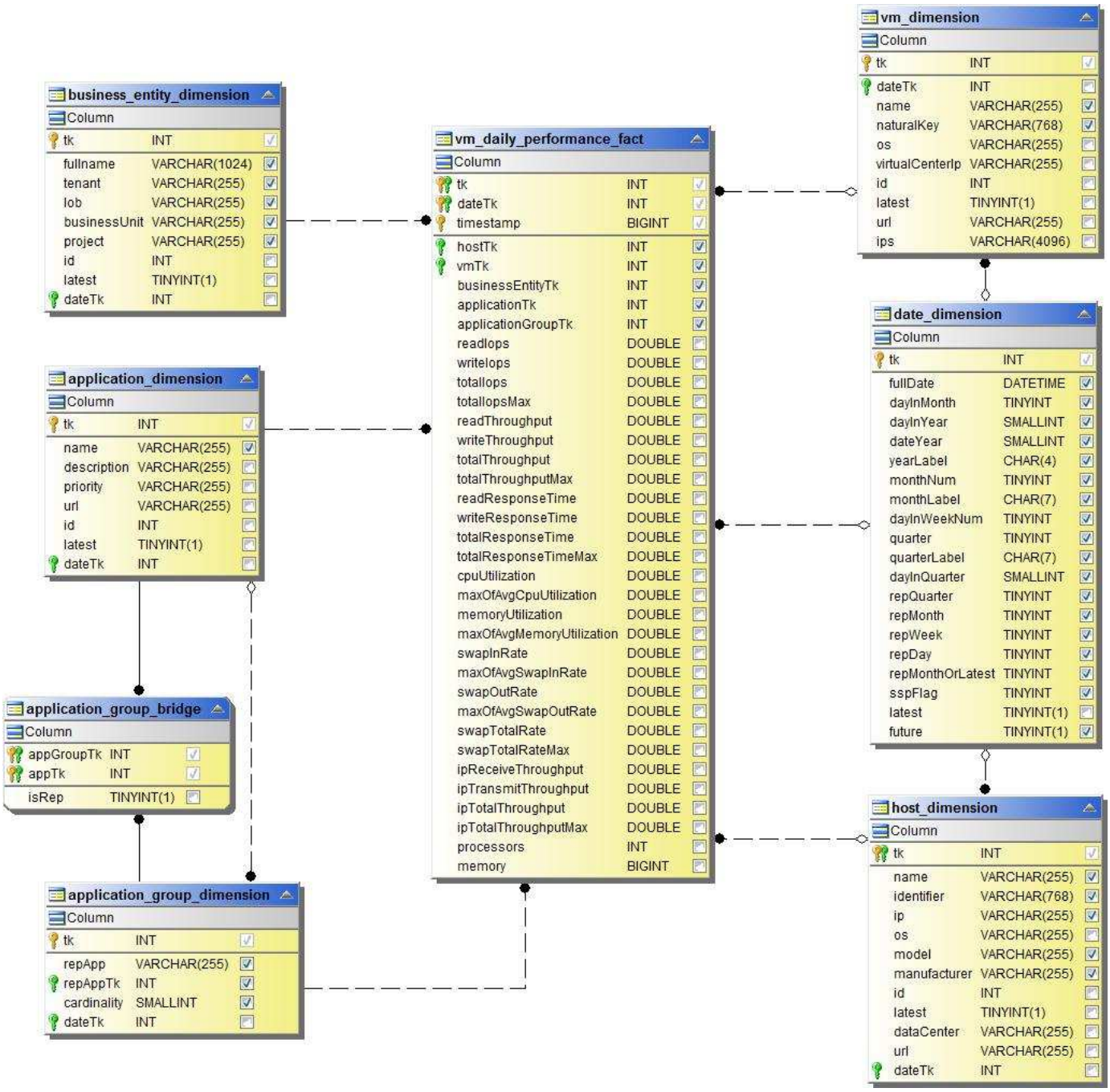
VM tägliche Performance für Host



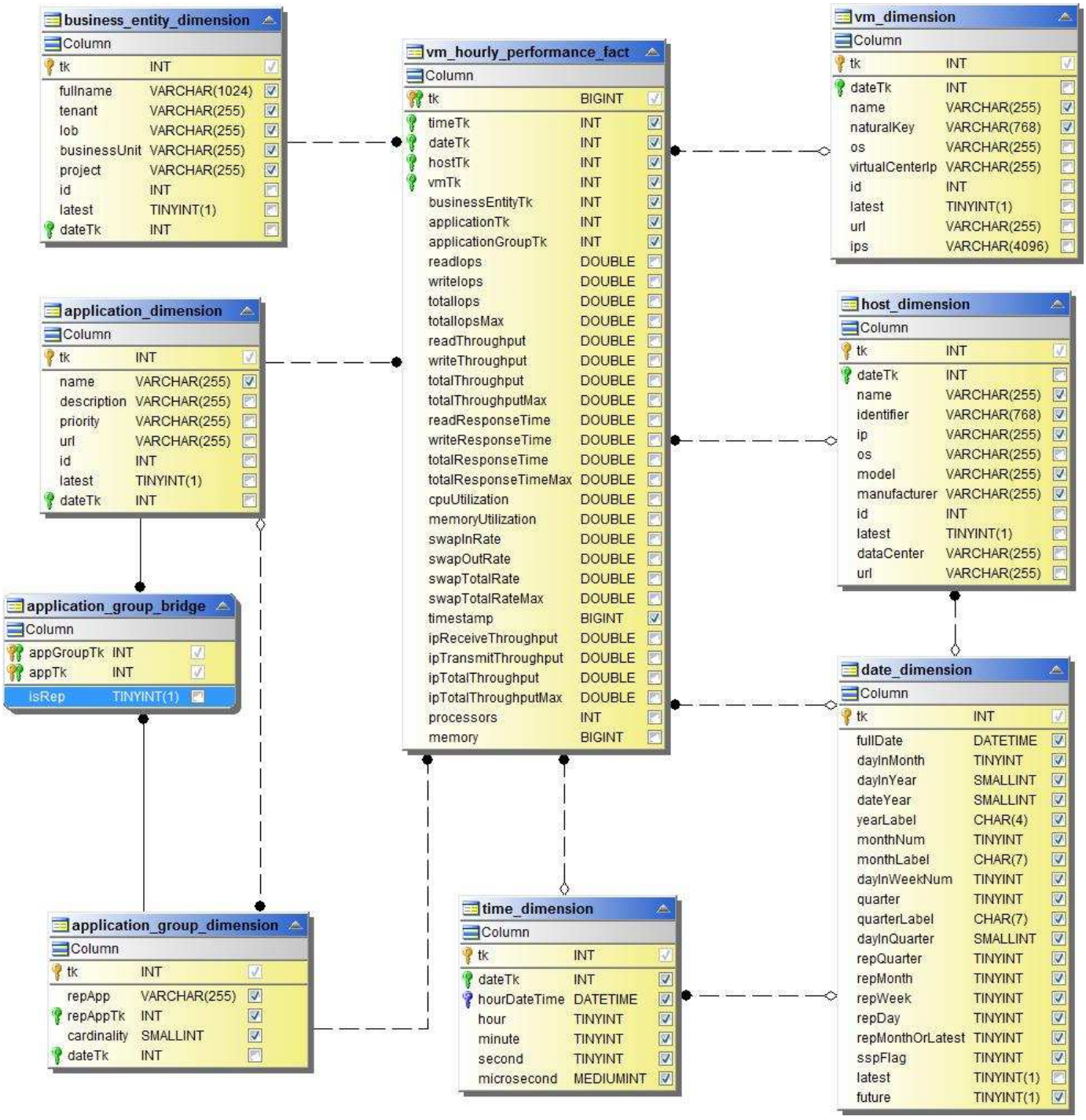
VM stündliche Performance für Host



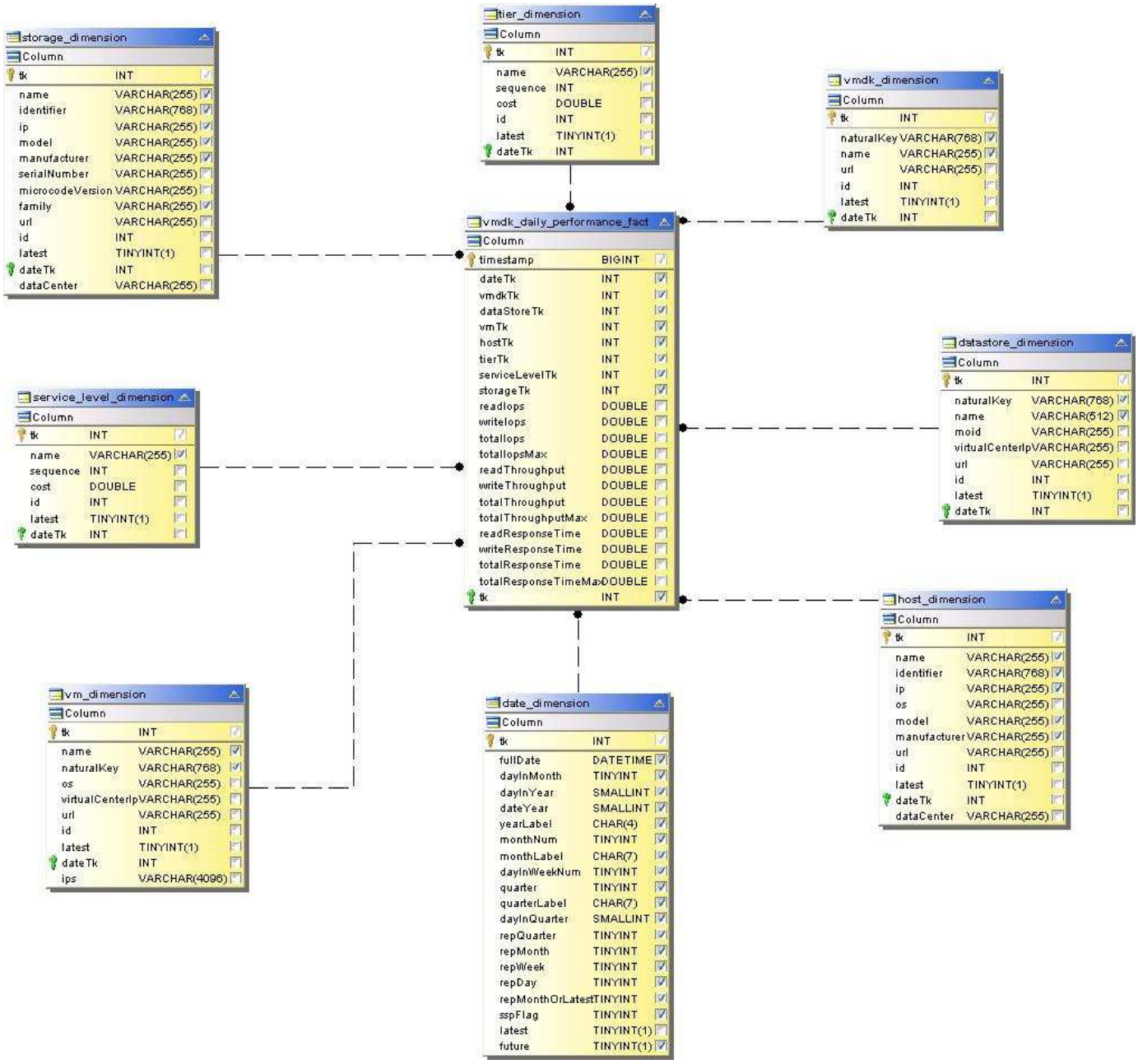
VM tägliche Performance für Host



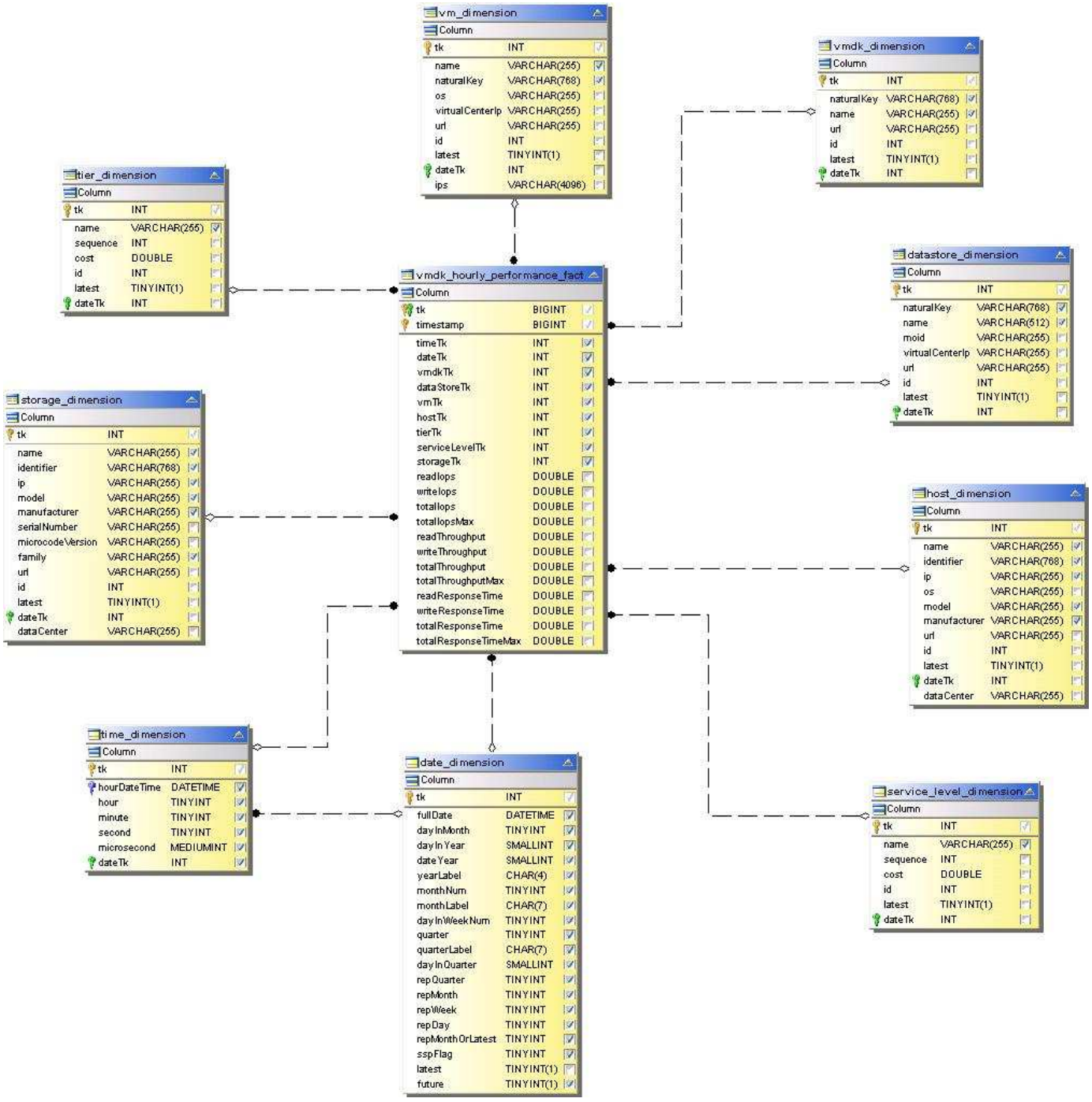
VM stündliche Performance für Host



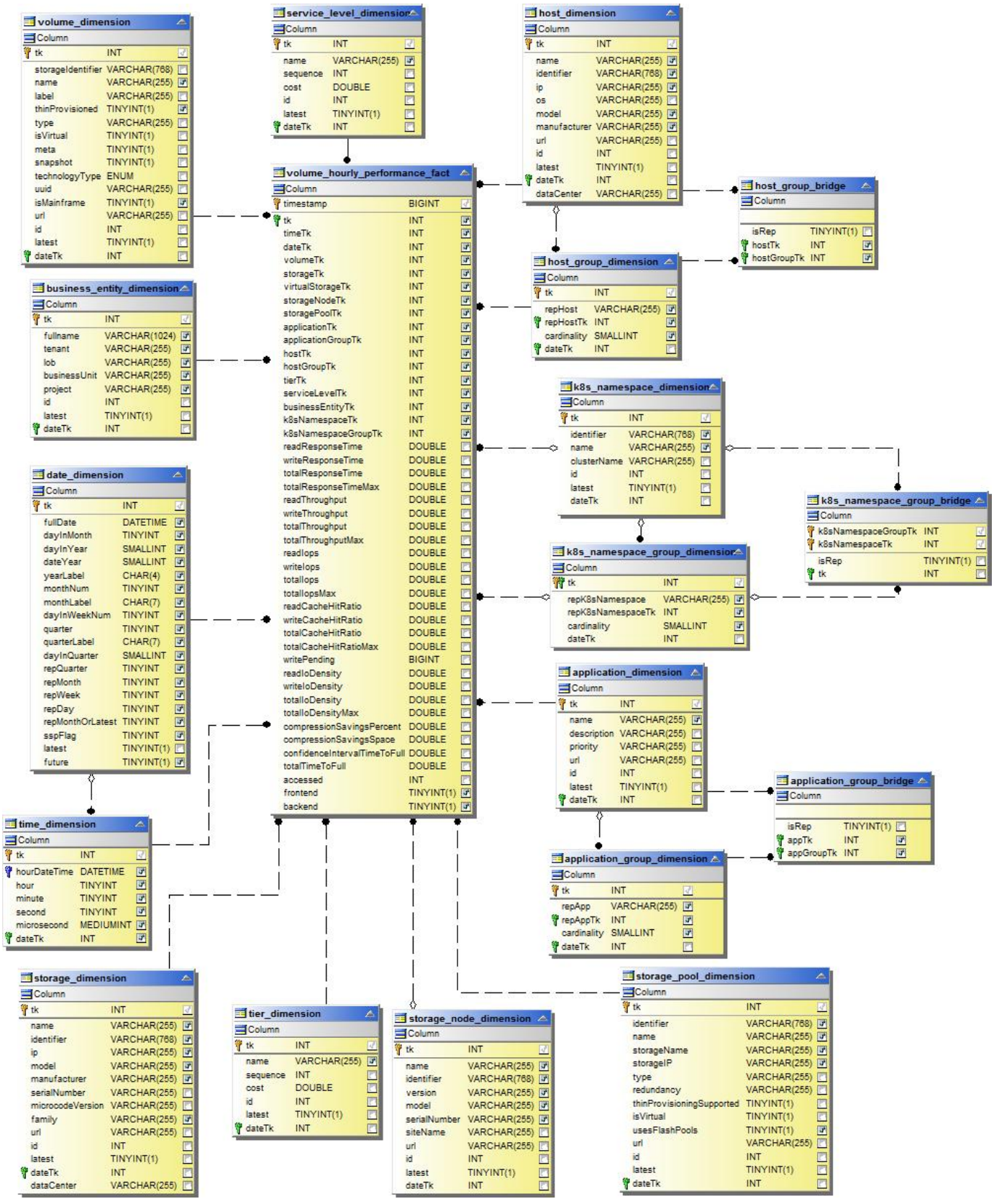
VMDK tägliche Performance



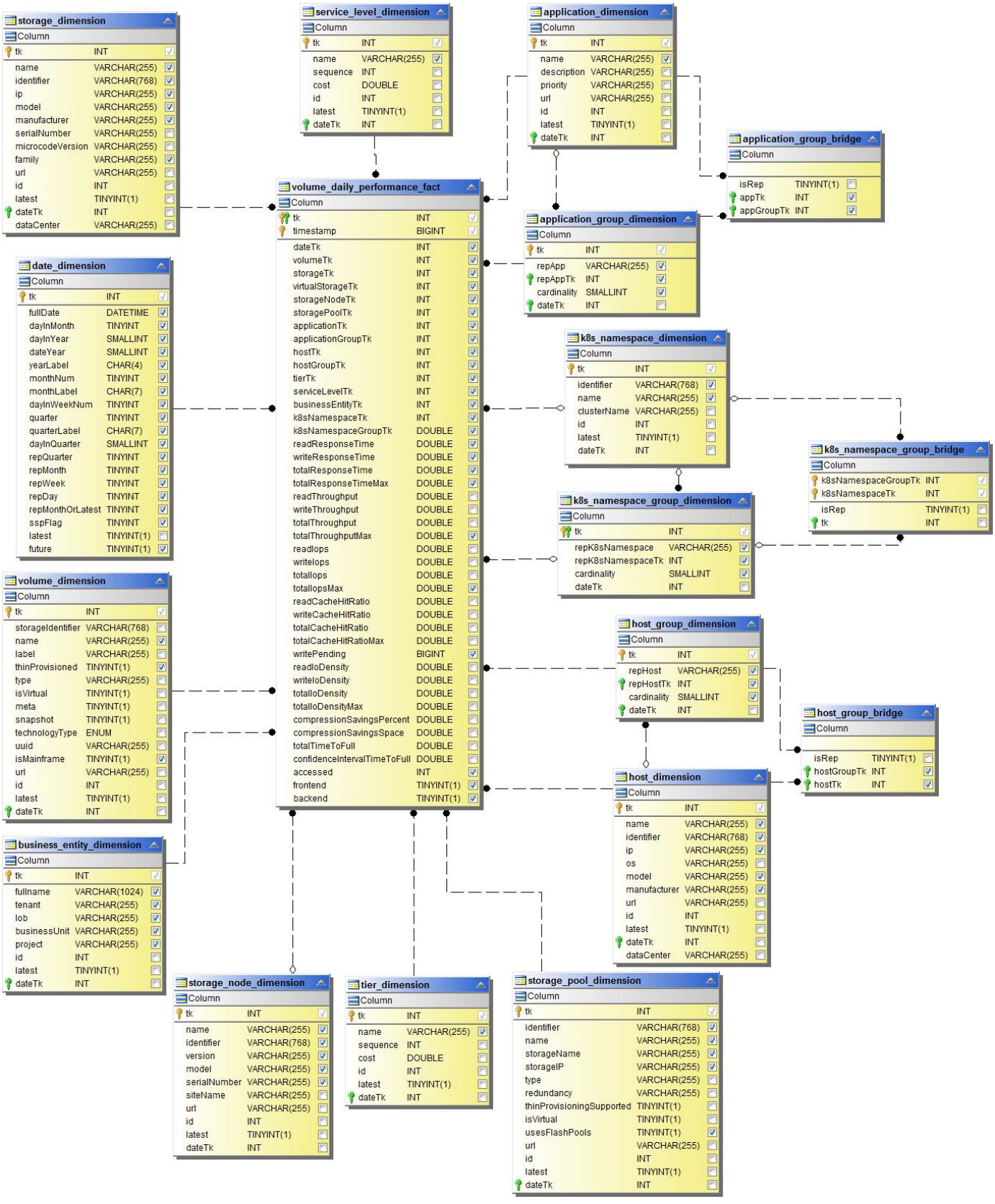
Stündliche VMDK-Performance



Stündliche Volume-Performance



Tägliche Volume Performance



Data Infrastructure Insights Schemas für die Berichterstellung

Diese Schematabellen und Diagramme werden hier als Referenz für Data Infrastructure Insights Reporting bereitgestellt.

"Schema-Tabellen" Im PDF-Format. Klicken Sie auf den Link zum Öffnen, oder klicken Sie mit der rechten Maustaste, und wählen Sie zum Herunterladen *Speichern unter…*.

"Schema Diagramme"

Die Berichtsfunktion ist in Data Infrastructure Insights verfügbar"Premium Edition".

Kubernetes

Kubernetes-Cluster – Übersicht

Der Data Infrastructure Insights Kubernetes Explorer ist ein leistungsstarkes Tool zum Anzeigen des Gesamtzustands und der Auslastung Ihrer Kubernetes-Cluster. Hier können Sie ganz einfach detaillierte Untersuchungsbereiche aufschlüsseln.

Durch Klicken auf **Dashboards > Kubernetes Explorer** wird die Listenseite für Kubernetes-Cluster geöffnet. Diese Übersichtsseite enthält Tabellen der Kubernetes Cluster in Ihrer Umgebung.

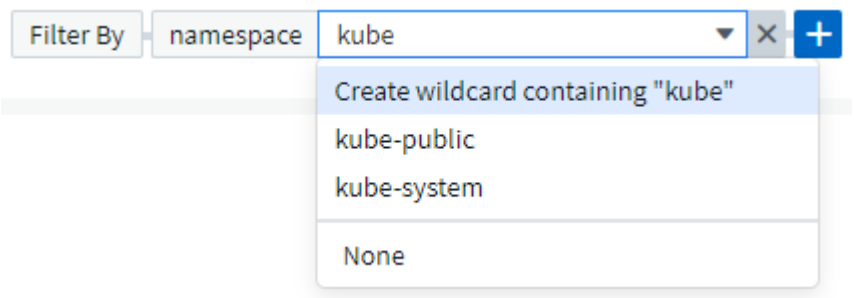
Cluster-Liste

In der Cluster-Liste werden für jedes Cluster in Ihrer Umgebung die folgenden Informationen angezeigt:

- Cluster **Name**. Wenn Sie auf einen Cluster-Namen klicken, wird das geöffnet **"Detailseite"** Für diesen Cluster zu erstellen.
- **Sättigung** Prozentsätze. „Gesamteinlagerung“ entspricht dem höchsten Wert für CPU, Speicher oder Speichersättigung.
- Anzahl **Nodes** im Cluster. Wenn Sie auf diese Nummer klicken, wird die Seite Knotenliste geöffnet.
- Anzahl **Pods** im Cluster. Wenn Sie auf diese Nummer klicken, wird die Pod-Listenseite geöffnet.
- Anzahl **Namesaces** im Cluster. Wenn Sie auf diese Nummer klicken, wird die Namespace-Listenseite geöffnet.
- Anzahl **Workloads** im Cluster. Wenn Sie auf diese Nummer klicken, wird die Listenseite Workload geöffnet.

Verfeinern des Filters

Wenn Sie filtern, werden Sie beim Eingeben mit der Option angezeigt, basierend auf dem aktuellen Text einen **Platzhalterfilter** zu erstellen. Wenn Sie diese Option auswählen, werden alle Ergebnisse angezeigt, die dem Platzhalterausdruck entsprechen. Sie können auch **Expressions** mit NOT oder UND erstellen, oder Sie können die Option "Keine" auswählen, um nach Null-Werten im Feld zu filtern.



Filter basierend auf Platzhalter oder Ausdrücken (z. B. NOT, AND, „None“ etc.) wird im Filterfeld dunkelblau angezeigt. Elemente, die Sie direkt aus der Liste auswählen, werden hellblau angezeigt.

Kubernetes-Filter sind kontextbezogen, d. h., wenn Sie sich beispielsweise auf einer bestimmten Knotenseite befinden, listet der Pod_Name-Filter nur die Pods auf, die mit diesem Node zusammenhängen. Wenn Sie darüber hinaus einen Filter für einen bestimmten Namespace anwenden, werden im Pod_Name-Filter nur Pods auf diesem Node *und* in diesem Namespace aufgelistet.

Beachten Sie, dass die Platzhalter- und Ausdrucksfilterung mit Text oder Listen funktioniert, jedoch nicht mit numerischen Werten, Daten oder Booleanen.

Bevor Sie den NetApp Kubernetes Monitoring Operator installieren oder aktualisieren

Lesen Sie diese Informationen, bevor Sie das installieren oder aktualisieren "Kubernetes Monitoring Operator".

Komponente	Anforderungen
Kubernetes-Version	Kubernetes v1.20 und höher
Kubernetes Distributionen	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes-Service (AKS) Google Kubernetes Engine (GKE) Red hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Linux BS	Data Infrastructure Insights unterstützt keine Nodes, die mit einer Arm64-Architektur ausgeführt werden. Netzwerküberwachung: Muss Linux Kernel Version 4.18.0 oder höher ausführen. Photon OS wird nicht unterstützt.
Etiketten	Data Infrastructure Insights unterstützt das Monitoring von Kubernetes-Nodes, auf denen Linux ausgeführt wird, indem eine Kubernetes-Node-Auswahl angegeben wird, die auf diesen Plattformen nach den folgenden Kubernetes-Labels sucht: Kubernetes v1.20 und höher: Kubernetes.io/os = linux Rancher + Cattle.io als Orchestrierungs-/Kubernetes-Plattform: Cattle.io/os = linux
Befehle	Die Befehle Curl und kubectl müssen verfügbar sein.; für optimale Ergebnisse fügen Sie diese Befehle dem PFAD hinzu.

Komponente	Anforderungen
Konnektivität	Kubectl cli ist für die Kommunikation mit dem Ziel-K8s-Cluster konfiguriert und verfügt über eine Internetverbindung zur Data Infrastructure Insights Umgebung. Wenn Sie während der Installation hinter einem Proxy stehen, befolgen Sie die Anweisungen im "Proxy-Unterstützung Wird Konfiguriert"Abschnitt der Installation des Bedieners. Für genaue Audit- und Datenberichte synchronisieren Sie die Zeit auf dem Agent-Computer mit Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP).
Andere	Wenn Sie OpenShift 4.6 oder höher verwenden, müssen Sie die folgenden Schritte ausführen "OpenShift-Anweisungen" Zusätzlich zur Sicherstellung, dass diese Voraussetzungen erfüllt sind.
API-Token	Wenn Sie den Operator neu bereitstellen (d. h. aktualisieren oder ersetzen), müssen Sie kein neues API-Token erstellen; Sie können das vorherige Token erneut verwenden.

Wichtige Dinge, die Sie beachten sollten, bevor Sie beginnen

Wenn Sie mit einem laufen Proxy, Haben Sie eine Benutzerdefiniertes Repository, Oder verwenden OpenShift, Lesen Sie die folgenden Abschnitte sorgfältig.

Lesen Sie auch darüber Berechtigungen.

Proxy-Unterstützung Wird Konfiguriert

An zwei Stellen können Sie in Ihrer Umgebung einen Proxy verwenden, um den NetApp Kubernetes Monitoring Operator zu installieren. Es kann sich um dieselben oder separate Proxy-Systeme handelt:

- Proxy wird während der Ausführung des Installationscode-Snippets (mit „Curl“) benötigt, um das System zu verbinden, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights-Umgebung
- Der vom Kubernetes Ziel-Cluster benötigte Proxy für die Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur ist erforderlich

Wenn Sie einen Proxy für eine oder beide dieser Optionen verwenden, müssen Sie zuerst sicherstellen, dass Ihr Proxy für eine gute Kommunikation mit Ihrer Data Infrastructure Insights-Umgebung konfiguriert ist, um den NetApp Kubernetes Operating Monitor zu installieren. Beispielsweise müssen Sie auf den Servern/VMs, von denen Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen und Binärdateien von Data Infrastructure Insights herunterladen können.

Legen Sie für den Proxy, der zur Installation des NetApp Kubernetes Operating Monitor verwendet wurde, vor der Installation des Operators die Umgebungsvariablen *http_Proxy/https_Proxy* fest. In einigen Proxy-Umgebungen müssen Sie möglicherweise auch die Variable *no_Proxy Environment* festlegen.

Um die Variable(en) festzulegen, führen Sie auf Ihrem System **vor** der Installation des NetApp Kubernetes Monitoring Operators folgende Schritte aus:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:
   a. Wenn der Proxy, der eingerichtet wird, keine Authentifizierung (Benutzername/Passwort) aufweist, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der Proxy, der eingerichtet wird, über Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie folgenden Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Wenn der Proxy, der für das Kubernetes-Cluster zur Kommunikation mit der Insights Umgebung für die Dateninfrastruktur verwendet wird, verwendet wird, installieren Sie den NetApp Kubernetes Monitoring Operator, nachdem Sie alle diese Anweisungen gelesen haben.

Konfigurieren Sie den Proxy-Abschnitt von AgentConfiguration in Operator-config.yaml, bevor Sie den NetApp Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker Repositorys

Standardmäßig zieht der NetApp-Kubernetes-Überwachungsoperator Container-Images aus dem Repository „Einblicke in die Dateninfrastruktur“. Wenn Sie ein Kubernetes-Cluster als Ziel für das Monitoring verwenden

und der Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder der Container-Registrierung zieht, müssen Sie den Zugriff auf die Container konfigurieren, die vom NetApp Kubernetes Monitoring Operator benötigt werden.

Führen Sie das „Image Pull Snippet“ aus der NetApp Monitoring Operator Installationskachel aus. Dieser Befehl meldet sich beim Repository Data Infrastructure Insights an, zieht alle Image-Abhängigkeiten für den Operator ab und meldet sich vom Repository Data Infrastructure Insights ab. Wenn Sie dazu aufgefordert werden, geben Sie das angegebene temporäre Repository-Passwort ein. Mit diesem Befehl werden alle vom Bediener verwendeten Bilder heruntergeladen, einschließlich optionaler Funktionen. Nachfolgend sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Core Operator-Funktionalität und Kubernetes Monitoring

- netapp Monitoring
- kube-rbac-Proxy
- status-Kennzahlen von kube
- telegraf
- Distroless-root-user

Ereignisprotokoll

- Fluent-Bit
- kubernetes Event Exporter

Netzwerkleistung und -Zuordnung

- ci-Netz-Beobachter

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in das private/lokale/unternehmenseigene Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Images in Ihrem Repository mit denen im Data Infrastructure Insights Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Monitoring-Operators in Operator-Deployment.yaml, und ändern Sie alle Bildverweise, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in Operator-config.yaml, um die neue Position des Docker-Repo zu berücksichtigen. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher ausführen, müssen Sie die AgentConfiguration in *Operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift kann zusätzliche Sicherheitsstufen implementieren, die den Zugriff auf einige Kubernetes-Komponenten blockieren könnten.

Berechtigungen

Wenn das zu überwachende Cluster benutzerdefinierte Ressourcen enthält, für die keine ClusterRole vorhanden ist "AnzuzeiEinblick in Aggregate"Sie müssen dem Bediener manuell Zugriff auf diese Ressourcen gewähren, um sie mit Ereignisprotokollen zu überwachen.

1. Bearbeiten Sie *Operator-additional-permissions.yaml* vor der Installation oder nach der Installation bearbeiten Sie die Ressource *ClusterRole/<namespace>-additional-permissions*
2. Erstellen Sie eine neue Regel für die gewünschten apiGroups und Ressourcen mit den Verben ["get", "watch", "list"]. Siehe https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Übernehmen Sie die Änderungen auf das Cluster

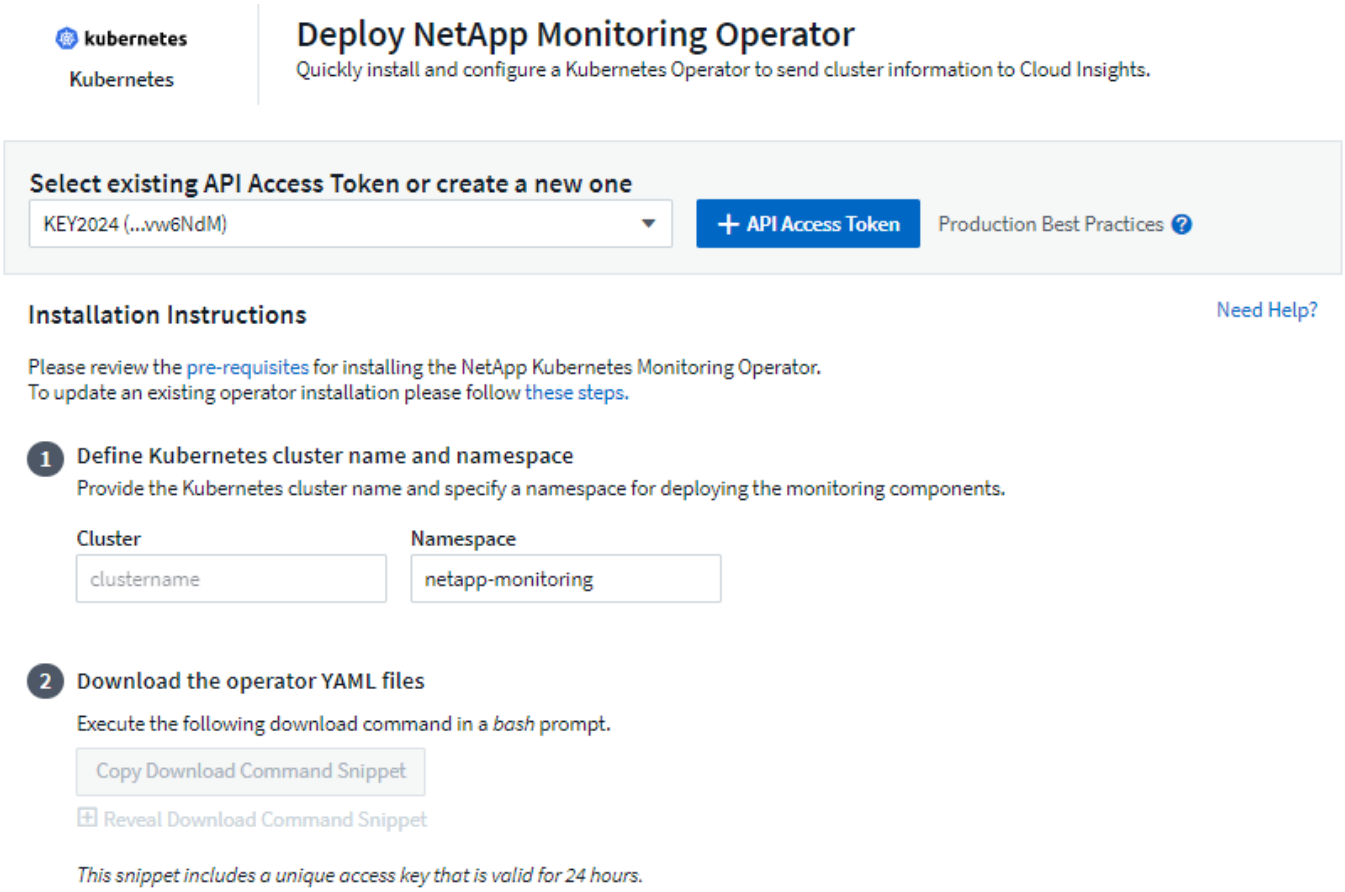
Installation und Konfiguration des Kubernetes Monitoring Operator

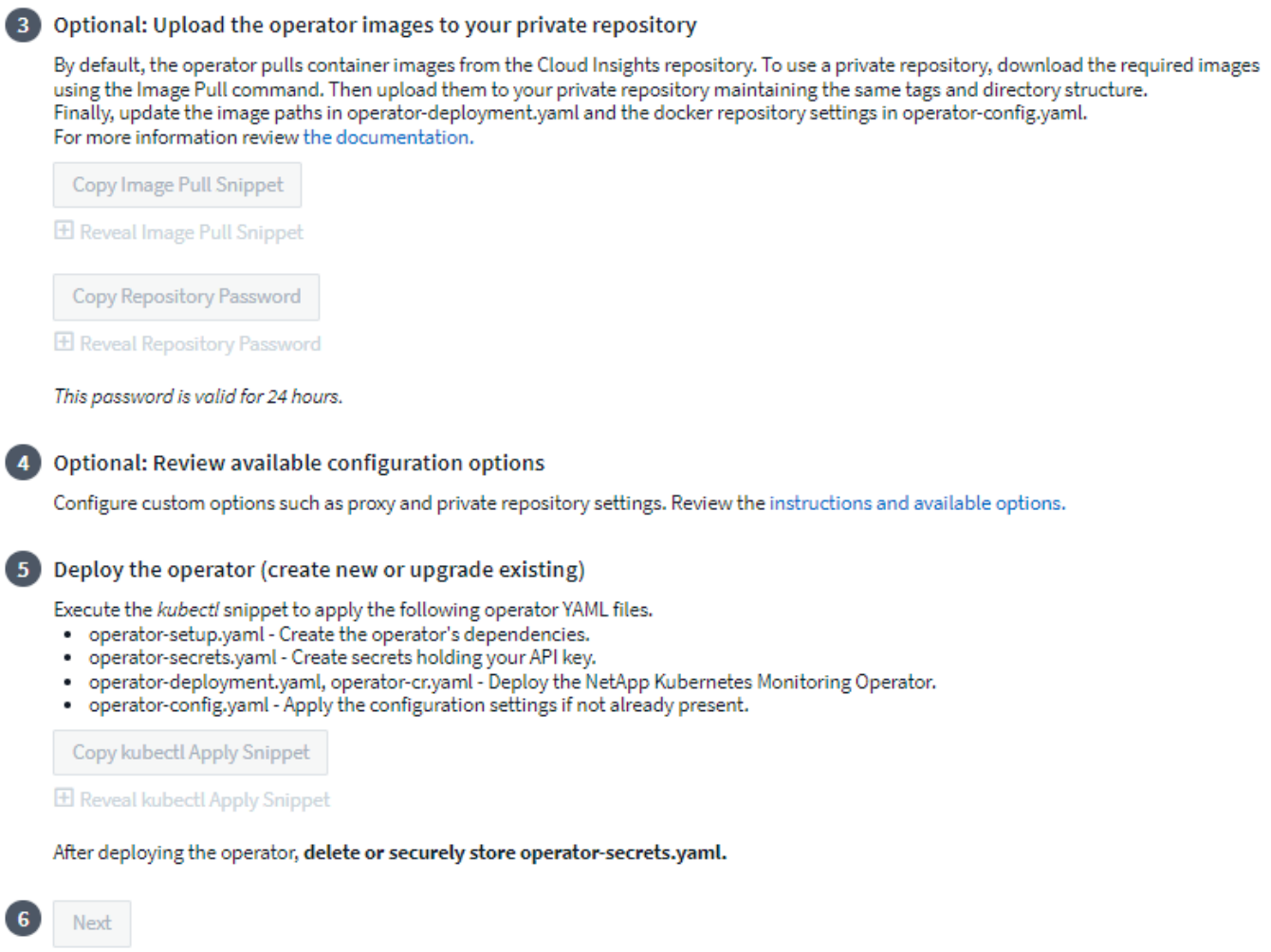
Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung an. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Bevor Sie den Kubernetes Monitoring Operator installieren

Siehe "Voraussetzungen" Dokumentation vor der Installation oder dem Upgrade des Kubernetes Monitoring Operator.

Installieren des Kubernetes Monitoring Operator





Schritte zum Installieren des Kubernetes Monitoring Operator Agent auf Kubernetes:

1. Geben Sie einen eindeutigen Cluster-Namen und einen eindeutigen Namespace ein. Wenn Sie es sind Aktualisierung Verwenden Sie aus einem früheren Kubernetes-Operator den gleichen Cluster-Namen und Namespace.
2. Sobald diese eingegeben wurden, können Sie den Download-Befehl-Snippet in die Zwischenablage kopieren.
3. Fügen Sie das Snippet in ein *bash* Fenster ein und führen Sie es aus. Die Installationsdateien des Bedieners werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und für 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie das optionale Bild-Pull-Snippet, fügen Sie es in eine *bash*-Shell ein und führen Sie es aus. Nachdem die Bilder gezogen wurden, kopieren Sie sie in Ihr privates Repository. Stellen Sie sicher, dass Sie dieselben Tags und Ordnerstrukturen beibehalten. Aktualisieren Sie die Pfade in *Operator-Deployment.yaml* sowie die Einstellungen des Docker-Repository in *Operator-config.yaml*.
5. Prüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen, z. B. Proxy- oder private Repository-Einstellungen. Sie können mehr über lesen "Konfigurationsoptionen".
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie den kubectl Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation wird automatisch ausgeführt. Klicken Sie anschließend auf die Schaltfläche „*Next*“.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche „*Next*“. Achten Sie darauf, auch die Datei *Operator-Secrets.yaml* zu löschen oder sicher zu speichern.

Wenn Sie einen Proxy verwenden, lesen Sie mehr über Proxy wird konfiguriert.

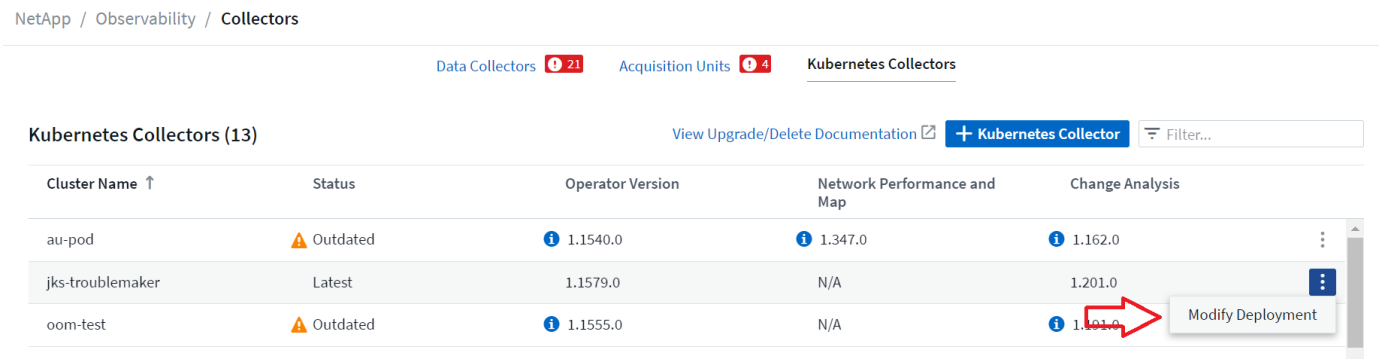
Wenn Sie über ein benutzerdefiniertes Repository verfügen, lesen Sie mehr über Ein benutzerdefiniertes/privates Docker-Repository verwenden.

Kubernetes-Monitoring-Komponenten

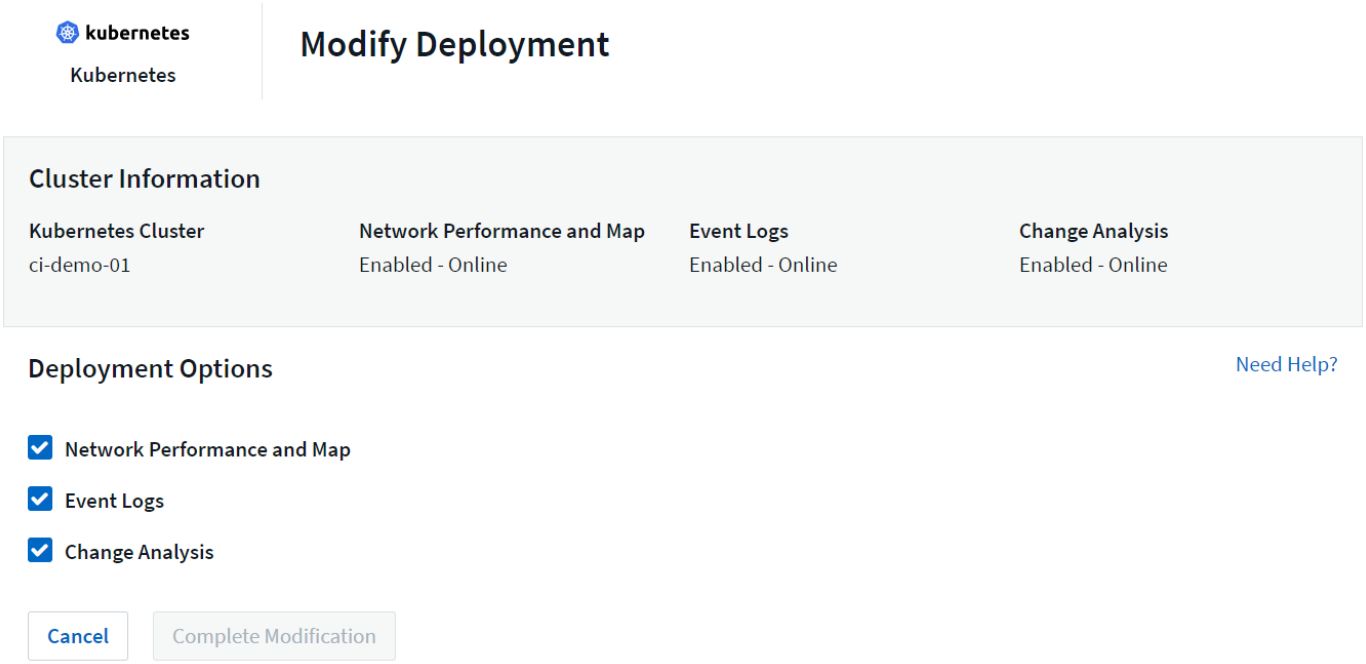
Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Monitoring-Komponenten:

- Cluster-Kennzahlen
- Netzwerkleistung und -Zuordnung (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben aufgeführten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie sich entscheiden, keine Komponente für einen bestimmten Collector zu benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Collector-Menü „drei Punkte“ rechts auf dem Bildschirm *Modify Deployment* auswählen.



Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht es Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.



Aktualisierung

Upgrade auf den neuesten Kubernetes Monitoring Operator

Ermitteln Sie, ob eine AgentConfiguration bei dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardwert *netapp-Monitoring* ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
Wenn eine AgentConfiguration vorhanden ist:
```

- Installieren Der letzte Operator über den vorhandenen Operator.
  - Stellen Sie sicher, dass Sie es sind Die neuesten Container-Bilder werden angezeigt Wenn Sie ein benutzerdefiniertes Repository verwenden.

Wenn AgentConfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Cluster-Namen (wenn Ihr Namespace nicht das standardmäßige NetApp-Monitoring ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Erstellen Sie eine Sicherung des bestehenden Operators (wenn Ihr
Namespace nicht der Standard-netapp-Überwachung ist, ersetzen Sie den
entsprechenden Namespace):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>> Der
vorhandene Operator.
* <<installing-the-kubernetes-monitoring-operator,Installieren>> Der
neueste Operator.
```

- Verwenden Sie denselben Cluster-Namen.
- Nachdem Sie die neuesten Operator YAML-Dateien heruntergeladen haben, können Sie alle in Agent_Backup.yaml gefundenen Anpassungen vor der Bereitstellung an den heruntergeladenen Operator-config.yaml übertragen.
- Stellen Sie sicher, dass Sie es sind Die neuesten Container-Bilder werden angezeigt Wenn Sie ein benutzerdefiniertes Repository verwenden.

Anhalten und Starten des Kubernetes Monitoring Operator

So beenden Sie den Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

Um den Kubernetes Monitoring Operator zu entfernen

Beachten Sie, dass der Standard-Namespace für den Kubernetes Monitoring Operator „netapp-Monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Überwachungsoperators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Wenn der Überwachungsoperator in seinem eigenen dedizierten Namespace bereitgestellt wurde, löschen Sie den Namespace:

```
 kubectl delete ns <NAMESPACE>
Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt, verwenden
Sie die folgenden Anweisungen, um ältere Versionen des
Überwachungsoperators zu deinstallieren.
```

Führen Sie jeden der folgenden Befehle in der Reihenfolge aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle Nachrichten ‘object not found’ zurückgeben. Diese Meldungen können sicher ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Sicherheitskontextbeschränkung erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert seine eigenen kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.

Informationen über Kube-State-Metrics finden Sie unter "Auf dieser Seite".

Konfigurieren/Anpassen des Bedieners

Diese Abschnitte enthalten Informationen zur Anpassung Ihrer Bedienerkonfiguration, zur Arbeit mit Proxy, zur Verwendung eines benutzerdefinierten oder privaten Docker-Repositorys oder zur Arbeit mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource bearbeiten, bevor Sie den Operator bereitstellen, indem Sie die Datei *Operator-config.yaml* bearbeiten. Diese Datei enthält kommentierte Beispiele für Einstellungen. Siehe Liste von "Verfügbare Einstellungen" Für die neueste Version des Bedieners.

Sie können diese Ressource auch bearbeiten, nachdem der Operator bereitgestellt wurde, indem Sie den

folgenden Befehl verwenden:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Um festzustellen, ob die bereitgestellte Version des Operators
AgentConfiguration unterstützt, führen Sie den folgenden Befehl aus:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Wenn die Meldung „Fehler vom Server (notfound)“ angezeigt wird, muss Ihr
Bediener aktualisiert werden, bevor Sie die AgentConfiguration verwenden
können.
```

Proxy-Unterstützung Wird Konfiguriert

Es gibt zwei Stellen, an denen Sie einen Proxy in Ihrer Umgebung verwenden können, um den Kubernetes Monitoring Operator zu installieren. Es kann sich um dieselben oder separate Proxy-Systeme handelt:

- Proxy wird während der Ausführung des Installationscode-Snippets (mit „Curl“) benötigt, um das System zu verbinden, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights-Umgebung
- Der vom Kubernetes Ziel-Cluster benötigte Proxy für die Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur ist erforderlich

Wenn Sie einen Proxy für eine oder beide dieser Optionen verwenden, müssen Sie zur Installation des Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights-Umgebung möglich ist. Wenn Sie über einen Proxy verfügen und von dem Server/der VM, von dem aus Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, legen Sie vor der Installation des Operators die Umgebungsvariablen *http_Proxy/https_Proxy* fest. In einigen Proxy-Umgebungen müssen Sie möglicherweise auch die Variable *no_Proxy Environment* festlegen.

Um die Variablen festzulegen, führen Sie die folgenden Schritte auf Ihrem System aus * bevor* den Kubernetes Monitoring Operator installiert:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:
   a. Wenn der Proxy, der eingerichtet wird, keine Authentifizierung (Benutzername/Passwort) aufweist, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der Proxy, der eingerichtet wird, über Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie folgenden Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Wenn der Proxy, der für das Kubernetes-Cluster zur Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur verwendet wird, verwendet wird, installieren Sie den Kubernetes Monitoring Operator, nachdem Sie alle diese Anweisungen gelesen haben.

Konfigurieren Sie den Proxy-Abschnitt von AgentConfiguration in Operator-config.yaml, bevor Sie den Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker Repositorys

Standardmäßig zieht der Kubernetes Monitoring Operator Container-Images aus dem Repository Data Infrastructure Insights. Wenn Sie ein Kubernetes-Cluster als Ziel für das Monitoring verwenden und der Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder der Container-Registrierung zieht, müssen Sie den Zugriff auf die Container konfigurieren, die vom Kubernetes Monitoring Operator benötigt werden.

Führen Sie das „Image Pull Snippet“ aus der NetApp Monitoring Operator Installationskachel aus. Dieser Befehl meldet sich beim Repository Data Infrastructure Insights an, zieht alle Image-Abhängigkeiten für den Operator ab und meldet sich vom Repository Data Infrastructure Insights ab. Wenn Sie dazu aufgefordert werden, geben Sie das angegebene temporäre Repository-Passwort ein. Mit diesem Befehl werden alle vom Bediener verwendeten Bilder heruntergeladen, einschließlich optionaler Funktionen. Nachfolgend sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Core Operator-Funktionalität und Kubernetes Monitoring

- netapp Monitoring
- ci-kube-rbac-Proxy
- ci-ksm

- ci-telegraf
- Distroless-root-user

Ereignisprotokoll

- ci-Fluent-Bit
- ci-kubernetes-Event-Exporteur

Netzwerkleistung und -Zuordnung

- ci-Netz-Beobachter

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in das private/lokale/unternehmenseigene Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Images in Ihrem Repository mit denen im Data Infrastructure Insights Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Monitoring-Operators in Operator-Deployment.yaml, und ändern Sie alle Bildverweise, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in Operator-config.yaml, um die neue Position des Docker-Repo zu berücksichtigen. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher ausführen, müssen Sie die AgentConfiguration in *Operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift kann zusätzliche Sicherheitsstufen implementieren, die den Zugriff auf einige Kubernetes-Komponenten blockieren könnten.

Ein Hinweis über Geheimnisse

Um die Berechtigung für den Kubernetes Monitoring Operator zum Anzeigen der geheimen Daten im gesamten Cluster zu entfernen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *Operator-Setup.yaml*:

```
 ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Wenn es sich um ein Upgrade handelt, löschen Sie auch die Ressourcen aus Ihrem Cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Wenn die Änderungsanalyse aktiviert ist, ändern Sie die Optionen *AgentConfiguration* oder *Operator-config.yaml*, um den Änderungsmanagementabschnitt zu entkommentieren und *kindsToIgnoreFromWatch: '"Secrets"* im Bereich Change-Management aufzunehmen. Notieren Sie sich das Vorhandensein und die Position von einfachen und doppelten Anführungszeichen in dieser Zeile.

```
# change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Überprüfen Von Kubernetes Prüfsummen

Das Installationsprogramm von Data Infrastructure Insights Agent führt Integritätsprüfungen durch, einige Benutzer möchten jedoch möglicherweise ihre eigenen Überprüfungen durchführen, bevor heruntergeladene Artefakte installiert oder angewendet werden. Um einen nur-Download-Vorgang durchzuführen (im Gegensatz zum Standard-Download-and-install), können diese Benutzer den Agent-Installation Befehl erhalten von der UI und entfernen Sie die nachhängbare "Installation" Option.

Führen Sie hierzu folgende Schritte aus:

1. Kopieren Sie das Agent Installer-Snippet wie angewiesen.
2. Anstatt das Snippet in ein Befehlsfenster einzufügen, fügen Sie es in einen Texteditor ein.
3. Entfernen Sie den nachfolgenden „--install“ aus dem Befehl.
4. Kopieren Sie den gesamten Befehl aus dem Texteditor.
5. Fügen Sie es nun in Ihr Befehlsfenster ein (in einem Arbeitsverzeichnis) und führen Sie es aus.
    - Download und Installation (Standard):

```
 installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download --install
** Nur Download:
```

```
installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download
```

Mit dem Befehl „nur herunterladen“ werden alle erforderlichen Artefakte aus Data Infrastructure Insights in das Arbeitsverzeichnis heruntergeladen. Die Artefakte umfassen, dürfen aber nicht beschränkt sein auf:

- Ein Installationsskript
- Einer Umgebungsdatei
- YAML-Dateien
- Eine signierte Prüfsumme-Datei (sha256.signed)
- Eine PEM-Datei (netapp_cert.pem) zur Signaturverifizierung

Das Installationsskript, die Umgebungsdatei und die YAML-Dateien können mittels Sichtprüfung verifiziert werden.

Die PEM-Datei kann durch Bestätigung des Fingerabdrucks wie folgt verifiziert werden:

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
Genauer gesagt,
```

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
Die signierte Prüfsummendatei kann mit der PEM-Datei verifiziert werden:
```

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die
Agenteninstallation durch Ausführen von gestartet werden:
```

```
sudo -E -H ./<installation_script_name> --install
```

Toleranzen und Verfleckungen

Die DemonSets *netapp-CI-telegraf-ds*, *netapp-CI-Fluent-Bit-ds* und *netapp-CI-net-Observer-l4-ds* müssen für jeden Node im Cluster einen Pod planen, damit Daten auf allen Nodes korrekt erfasst werden. Der Operator wurde so konfiguriert, dass er einige bekannte **Fehler** toleriert. Wenn Sie auf Ihren Nodes benutzerdefinierte Taints konfiguriert haben und damit verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie für diese Taints eine **Toleration** erstellen "In der *AgentConfiguration*". Wenn Sie auf alle Nodes im Cluster benutzerdefinierte Taints angewendet haben, müssen Sie der Operator-Bereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Weitere Informationen zu Kubernetes "Tönungen und Tolerationen".

Kehren Sie zum zurück "**NetApp Kubernetes Monitoring Operator Installation** Seite"

Fehlerbehebung

Bei Problemen beim Einrichten des Kubernetes Monitoring Operator sollten Sie Folgendes versuchen:

Problem:	**Versuchen Sie dies:**
Ich sehe keinen Hyperlink/Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End Storage-Gerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Storage-Servers konfiguriert.	Befolgen Sie die Schritte, um den bestehenden Telegraf-Agent zu deinstallieren, und installieren Sie dann den neuesten Telegraf-Agent erneut. Sie müssen Telegraf Version 2.0 oder höher verwenden. Der Kubernetes-Cluster-Storage muss aktiv durch Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie dies:
Ich sehe Nachrichten in den Protokollen, die folgendermaßen aussehen: E0901 15:21:39.962145 1 Reflector.go:178] k8s.io/kube-State-metrics/internal/Store/Builder.go:352: Konnte *v1.MutatingWebhookKonfiguration: Der Server konnte die angeforderte Ressource nicht finden E0901 15:21:43.168161 1 Reflector.go:178] k8s.io/kube-State-metrics/internal/Store/Builder.go:352: Fehler beim Auflisten von *v1.Lease: Der Server konnte die angeforderte Ressource nicht finden (get Leases.Coordination.k8s.io) Usw.	Diese Nachrichten können auftreten, wenn Sie kube-State-Metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. So erhalten Sie die Kubernetes-Version: *Kubectl Version* So erhalten Sie die kube-State-metrics-Version: *Kubectl get deploy/kube-State-metrics -o jsonpath='{..image}'* Um zu verhindern, dass diese Meldungen stattfinden, können Benutzer ihre Bereitstellung von kube-State-Metrics ändern, um die folgenden Leasings zu deaktivieren: *Mutatingwebhookkonfigurationen* *Validatingwebhookkonfigurationen* *Volumeattachments-Ressourcen* Genauer gesagt können sie das folgende CLI-Argument verwenden: Ressourcen=zertifiziertigningrequests,configmaps,cronjobs,demonsets, Bereitstellungen,Endpunkte,horizontalpodautoscalers,ingresses,Jobs,limitranges, Namespaces,Netzwerkrichtlinien,Nodes,persistent Volumeclaims,persistent Volumes, poddisruptionbudgets,Pods,Replikasets,Replikationcontroller,resourcequotas, Secrets,Services,Statefulsets,Storageclasses Die Standardressourcenliste lautet: „Zertificatezigningrequest,configmaps,cronjobs,demonsets,Bereitstellungen, Endpunkte,horizontalpodautoscalers,ingresses,Jobs,Leases,limitranges, mutatingwebhookkonfigurationen,Namespaces,Netzwerkrichtlinien,Nodes,persistent Volumeclaims,persistent,Volumes,poddisruptionbudgets,Pods,Replikasets,resourcequotas,Secrets,Services,statectorSets,statectoresets Validatingwebhookkonfigurationen, Volumeanhänge“

Problem:	Versuchen Sie dies:
Ich sehe Fehlermeldungen von Telegraf wie die folgenden, aber Telegraf startet und läuft: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Startete den Plugin-gesteuerten Server-Agent für die Berichterstattung von Kennzahlen in InfluxDB. Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„konnte kein Cache-Verzeichnis erstellen. /Etc/telegraf/.Cache/snowflake, err: Mkdir /etc/telegraf/.ca Che: Erlaubnis verweigert. Ignored\n“ func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:120“ Okt. 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„Öffnen fehlgeschlagen. Ignoriert. Open /etc/telegraf/.Cache/snowflake/ocsp_response_Cache .json: Nicht so Datei oder Verzeichnis\n“ func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:120“ Okt. 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z i! Telegraf 1.19.3 Starten	Dies ist ein bekanntes Problem. Siehe "Dieser GitHub-Artikel" Entnehmen. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.
Auf Kubernetes berichten meine Telegraf POD(s) die folgende Fehlermeldung: "Fehler bei der Verarbeitung von mountstats-Info: Mountstats-Datei konnte nicht geöffnet werden: /Hostfs/proc/1/mountstats, Fehler: Open /hostfs/proc/1/mountstats: Berechtigung verweigert"	Wenn SELinux aktiviert und durchgesetzt wird, wird wahrscheinlich verhindert, dass die Telegraf PODs auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen. Um diese Einschränkung zu überwinden, bearbeiten Sie die Agentkonfiguration und aktivieren Sie die runPrivileged-Einstellung. Weitere Informationen finden Sie im "OpenShift-Anweisungen".
Auf Kubernetes meldet mein Telegraf ReplicaSet POD den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Konnte keypair /etc/kubernetes/pki/etcd/Server.crt:/etc/kubernetes/pki /etcd/Server.key nicht laden: Öffnen /etc/kubernetes/pki/etcd/Server.crt: Datei oder Verzeichnis nicht vorhanden	Der Pod Telegraf ReplicaSet soll auf einem Knoten ausgeführt werden, der als Master oder für etc bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master/etcd-Knoten eine Tönungswalle haben. Fügen Sie in diesem Fall die erforderlichen Verträgungen in das Telegraf ReplicaSet, telegraf-rs ein. Bearbeiten Sie beispielsweise das ReplicaSet… Kubectl bearbeiten rs telegraf-rs …Und fügen Sie die entsprechenden Toleranzen in die Spezifikation ein. Starten Sie anschließend den Pod ReplicaSet neu.

Problem:	Versuchen Sie dies:
Ich habe eine PSP/PSA Umgebung. Hat dies Auswirkungen auf meinen Überwachungsperator?	Wenn Ihr Kubernetes-Cluster mit Pod-Sicherheitsrichtlinie (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie ein Upgrade auf den aktuellen Kubernetes Monitoring Operator durchführen. Führen Sie die folgenden Schritte aus, um auf den aktuellen Bediener mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren Der vorherige Überwachungsoperator: Kubectl delete Agent-Monitoring-netapp -n netapp-Monitoring Kubectl löschen ns netapp-Monitoring Kubectl löschen crd agents.monitoring.netapp.com Kubectl delete clusterrole Agent-Manager-role Agent-Proxy-role Agent-metrics-reader Kubectl delete clusterrolebinding Agent-Manager-rolebinding Agent-Proxy-rolebinding Agent-Cluster-admin-rolebinding 2. Installieren Die neueste Version des Überwachungsbedieners.
Ich habe Probleme beim Versuch, den Operator bereitzustellen, und ich habe PSP/PSA in Gebrauch.	1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: Kubectl -n <name-space>-Bearbeitungsagent 2. Markieren Sie "Sicherheit-Politik-aktiviert" als "falsch". Dadurch werden Pod-Sicherheitsrichtlinien und Pod-Sicherheitszulassung deaktiviert und der Bediener kann die Bereitstellung durchführen. Bestätigen Sie die Bestätigung mit folgenden Befehlen: Kubectl get psp (sollte zeigen, dass die Pod-Sicherheitsrichtlinie entfernt wurde) Kubectl get all -n <namespace> (sollte zeigen, dass nichts gefunden wird)
„ImagePullBackoff“-Fehler erkannt	Diese Fehler können auftreten, wenn Sie über ein benutzerdefiniertes oder privates Docker-Repository verfügen und den Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass er es richtig erkennt. Weitere Informationen Info zur Konfiguration für benutzerdefinierte/private Repo.

Problem:	Versuchen Sie dies:
Ich habe ein Problem mit der Installation meines Monitoring-Bedieners, und die aktuelle Dokumentation hilft mir nicht, es zu lösen.	Erfassen oder notieren Sie die Ausgabe der folgenden Befehle, und wenden Sie sich an den technischen Support. ``` kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true ```
NET-Observer (Workload Map)-Pods im Operator Namespace befinden sich in CrashLoopBackOff	Diese Pods entsprechen dem Workload Map-Datensammler für Network Observability. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die minimale Kernel-Version zu bestätigen. Beispiel: ---- {„CI-Tenant-id“:„your-Tenant-id“,„Collector-Cluster“:„your-k8s-Cluster-Name“,„environment“:„prod“,„Level“:„error“,„msg“:„failed in validation. Grund: Kernelversion 3.10.0 ist kleiner als die minimale Kernelversion von 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • Net-Observer PODs benötigen die Linux Kernel Version mindestens 4.18.0. Überprüfen Sie die Kernel-Version mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 sind
Pods werden im Operator Namespace ausgeführt (Standard: netapp-Monitoring), es werden jedoch keine Daten in der UI für die Workload-Zuordnung oder Kubernetes-Metriken in Abfragen angezeigt	Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Rechner mit Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.

Problem:	Versuchen Sie dies:
Einige der Net-Observer-Pods im Namespace Operator befinden sich im Status „Ausstehend“	NET-Observer ist ein DemonSet und führt in jedem Knoten des K8s-Clusters einen Pod aus. • Beachten Sie den Pod, der sich im Status „Ausstehend“ befindet, und prüfen Sie, ob ein Ressourcenproblem für CPU oder Speicher vorliegt. Stellen Sie sicher, dass der erforderliche Arbeitsspeicher und die erforderliche CPU im Knoten verfügbar sind.
Ich sehe Folgendes in meinen Protokollen sofort nach der Installation des Kubernetes Monitoring Operator: [inputs.prometheus] Fehler im Plugin: Fehler beim Erstellen einer HTTP-Anforderung an http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.Cluster.local: Kein solcher Host	Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert ist und der Pod „*telegraf-rs*“ vor dem Einschalten des Pod „*ksm*“ steht. Diese Meldungen sollten beendet werden, sobald alle Pods ausgeführt werden.
Ich sehe keine Kennzahlen für die Kubernetes-Kronjobs, die in meinem Cluster vorhanden sind, erfasst.	Überprüfen Ihrer Kubernetes Version (d. h. `kubectl version`). Wenn es v1.20.x oder niedriger ist, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator implementierte Version von kube-State-Metrics unterstützt nur v1.cronjob. Bei Kubernetes 1.20.x und niedriger befindet sich die Ressource cronjob unter v1beta.cronjob. Daher können kube-State-Metriken die Ressource cronjob nicht finden.
Nach der Installation des Bedieners geben die telegraf-ds-Pods CrashLoopBackOff ein und die POD-Protokolle zeigen „su: Authentication failure“ an.	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und setzen Sie *dockerMetricCollectionEnabled* auf false. Weitere Informationen finden Sie im "Konfigurationsoptionen". HINWEIS: Wenn Sie Data Infrastructure Insights Federal Edition verwenden, können Benutzer mit Einschränkungen hinsichtlich der Verwendung von *su* keine Docker-Metriken sammeln, da der Zugriff auf den Dockersockel entweder den telegraf-Container als root ausführen muss oder *su* verwenden muss, um den telegraf-Benutzer zur Docker-Gruppe hinzuzufügen. Docker metric Collection und die Verwendung von *su* sind standardmäßig aktiviert; um beides zu deaktivieren, entfernen Sie den Eintrag *telegraf.Docker* in der *AgentConfiguration*-Datei: … Spec: … telegraf: … - Name: docker Run-Mode: - DemonSet Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCK_PLACEHOLDER Wert: unix:///run/Docker.Sock … …

Problem:	Versuchen Sie dies:
Ich sehe wiederholte Fehlermeldungen wie die folgenden in meinen Telegraf-Protokollen: E! [Agent] Fehler beim Schreiben in Outputs.http: Post "https://<tenant_url>/Rest/v1/Lake/ingest/influxdb": Kontext-Deadline überschritten (Client. Zeitüberschreitung beim Warten auf Header überschritten)	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und erhöhen Sie *outputTimeout* auf 10s. Weitere Informationen finden Sie im Abschnitt des Bedieners "Konfigurationsoptionen".
Ich vermisse *involvedobject* Daten für einige Event Logs.	Stellen Sie sicher, dass Sie die Schritte im befolgt haben "Berechtigungen" Abschnitt oben.
Wieso werden zwei Monitoring Operator Pods ausgeführt, einer mit dem Namen netapp-CI-Monitoring-Operator-<pod> und der andere mit dem Namen Monitoring-Operator-<pod>?	Seit dem 12. Oktober 2023 hat Data Infrastructure Insights den Betreiber refaktorisiert, um unseren Benutzern besser dienen zu können. Damit diese Änderungen vollständig umgesetzt werden, müssen Sie Entfernen Sie den alten Bedienerund Installieren Sie den neuen.
Meine kubernetes-Ereignisse haben unerwartet aufgehört, Daten bei Infrastruktur-Insights zu melden.	Rufen Sie den Namen des POD für den Event-Exporter ab: `` `kubectl -n netapp-monitoring get pods ``
grep event-exporter	awk '{print $1}'
sed 's/event-exporter./event-exporter/` Es sollte entweder „netapp-CI-Event-Exporteur“ oder „Event-Exporteur“ sein. Bearbeiten Sie anschließend den Monitoring-Agent `kubectl -n netapp-monitoring edit agent`, Und legen Sie den Wert für LOG_FILE so fest, dass der entsprechende POD-Name für den Event-Exporter im vorherigen Schritt angezeigt wird. Genauer gesagt sollte LOG_FILE auf "/var/log/Containers/netapp-CI-Event-exporteur.log" oder "/var/log/Containers/Event-exporteur*.log" gesetzt werden …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativ kann man auch Deinstallieren Und Neu installieren Der Agent.	Ich sehe POD(s), die vom Kubernetes-Monitoring-Operator bereitgestellt werden, aufgrund unzureichender Ressourcen.

Problem:	Versuchen Sie dies:
Weitere Informationen finden Sie im Kubernetes Monitoring Operator "Konfigurationsoptionen" Um die CPU- und/oder Speichergrenzen je nach Bedarf zu erhöhen.	Durch ein fehlendes Image oder eine ungültige Konfiguration wurden die netapp-CI-kube-State-metrics Pods nicht gestartet oder nicht einsatzbereit gemacht. Jetzt bleibt StatefulSet stecken und Konfigurationsänderungen werden nicht auf die Pods mit den netapp-CI-kube-State-Metriken angewendet.
Das StatefulSet befindet sich in A "Defekt" Bundesland. Nachdem Sie Konfigurationsprobleme behoben haben, springen die netapp-CI-kube-State-metrics-Pods an.	Pods mit netapp-CI-kube-Status-Metriken können nicht gestartet werden, nachdem ein Kubernetes Operator Upgrade ausgeführt wurde. Es wird ErrImagePull geworfen (es konnte nicht das Image entfernt werden).
Versuchen Sie, die Pods manuell zurückzusetzen.	„Event disorded as being alder then maxEventAgeSeconds“ Meldungen werden für meinen Kubernetes Cluster unter Log Analysis beobachtet.
Ändern Sie den Operator *agentkonfiguration*, und erhöhen Sie die Erweiterung *Event-exporteur-maxEventAgeSeconds* (d. h. auf 60s), *Event-exporteur-kubeQPS* (d. h. auf 100) und *Event-exporteur-kubeBurst* (d. h. auf 500). Weitere Informationen zu diesen Konfigurationsoptionen finden Sie im "Konfigurationsoptionen" Seite.	Telegraf warnt vor unzureichenden, abschließbaren Speichern oder stürzt ab.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurationsoptionen Für Kubernetes Monitoring Operator

Der "Kubernetes Monitoring Operator" Die Konfiguration kann angepasst werden.

In der folgenden Tabelle sind die möglichen Optionen für die *AgentConfiguration*-Datei aufgeführt:

Komponente	Option	Beschreibung
Agent		Konfigurationsoptionen, die allen Komponenten gemeinsam sind, die der Bediener installieren kann. Diese können als "globale" Optionen betrachtet werden.
	DockerRepo	Ein ockerRepo-Überschreiben, um Bilder von privaten Docker-Repos des Kunden im Vergleich zu Data Infrastructure Insights Docker Repo zu beziehen. Der Standardwert ist Data Infrastructure Insights Docker Repo
	DockerImagePullSecret	Optional: Ein Geheimnis für den Kunden private repo

Komponente	Option	Beschreibung
	ClusterName	Freitextfeld, das einen Cluster über alle Kundencluster eindeutig identifiziert. Diese sollte bei einem Mandanten von Dateninfrastruktur Insights eindeutig sein. Der Standardwert ist das, was der Kunde in die Benutzeroberfläche für das Feld „Cluster Name“ eingibt
	Proxy Format: Proxy: Server: Anschluss: Benutzername: Kennwort: Noproxy: IsTelegrafProxyEnabled: IsAuProxyEnabled: IsFluentbitProxyEnabled: IsCollectorProxyEnabled:	Optional zum Festlegen des Proxys. Dies ist in der Regel der Unternehmensvertreter des Kunden.
telegraf		Konfigurationsoptionen, mit denen die telegraf-Installation des Bedieners angepasst werden kann
	Erfassungsintervall	Messgrößen-Erfassungsintervall, in Sekunden (max. = 60 s)
	DsCpuLimit	CPU-Limit für telegraf ds
	DsMemLimit	Speicherlimit für telegraf ds
	DsCpuRequest	CPU-Anforderung für telegraf ds
	DsMemRequest	Speicheranforderung für telegraf ds
	RsCpuLimit	CPU-Limit für telegraf rs
	RsMemLimit	Speichergrenze für telegraf rs
	RsCpuRequest	CPU-Anforderung für telegraf rs
	RsMemRequest	Speicheranforderung für telegraf rs
	RunPrivileged	Führen Sie den telegraf Container im privilegierten Modus aus. Setzen Sie diese Einstellung auf TRUE, wenn SELinux auf Ihren K8s-Knoten aktiviert ist
	Stapelgröße	Siehe "Telegraf-Konfigurationsdokumentation"
	BufferLimit	Siehe "Telegraf-Konfigurationsdokumentation"
	Rundintervall	Siehe "Telegraf-Konfigurationsdokumentation"
	SammlungJitter	Siehe "Telegraf-Konfigurationsdokumentation"
	Präzision	Siehe "Telegraf-Konfigurationsdokumentation"

Komponente	Option	Beschreibung
	Flushintervall	Siehe "Telegraf-Konfigurationsdokumentation"
	FlushJitter	Siehe "Telegraf-Konfigurationsdokumentation"
	AusgabeTimeout	Siehe "Telegraf-Konfigurationsdokumentation"
	DsToleranzen	telegraf-ds zusätzliche Toleranzen.
	RsToleranzen	telegraf-rs zusätzliche Toleranzen.
	SkipProcessorsAfterAggregatoren	Siehe "Telegraf-Konfigurationsdokumentation"
	Ungeschützt	Siehe das "Bekanntes Problem mit Telegraf". Durch die Einstellung „*Unprotected*“ wird der Kubernetes Monitoring Operator angewiesen, Telegraf mit dem auszuführen `--unprotected` Flagge.
status-Kennzahlen von kube		Konfigurationsoptionen, mit denen die installation von kube-Statusmetriken des Operators angepasst werden kann
	CpuLimit	CPU-Limit für die bereitstellung von kube-State-Metriken
	MemLimit	MEM-Limit für die implementierung von kube-State-Metriken
	CpuRequest	CPU-Anforderung für die Bereitstellung von kube-Statusmetriken
	MemRequest	MEM-Anforderung für die Bereitstellung von kube-Statuskennzahlen
	Ressourcen	Eine kommagetrennte Liste der zu erfassenden Ressourcen. Beispiel: Cronjobs,demonsets,Bereitstellungen,ingress,Jobs,Namespaces,Nodes,persistent Volumeclaims, persistent Volumes,Pods,Replikasets,resourcequotas,Services,statefulsets
	Toleranzen	zusätzliche Toleranzen für kube-State-Metriken.
	Etiketten	Eine kommagetrennte Liste von Ressourcen, die kube-State-metrics erfassen sollte Beispiel: Cronjobs=[*],demonsets=[*],Deployments=[*],ingresses=[*],Jobs=[*],Namespaces=[*],Nodes=[*], Persistent volumeclaims=[*],persistent Volumes=[*],Pods=[*],replikasets=[*],resourcequotas=[*],Services=[*],statefulsets=[*]
Protokolle		Konfigurationsoptionen, mit denen die Protokollsammlung und die Installation des Bedieners angepasst werden können

Komponente	Option	Beschreibung
	Wieder FromHead	Wahr/falsch, sollte fließendes Bit das Protokoll vom Kopf lesen
	Zeitüberschreitung	Timeout in Sekunden
	DnsMode	TCP/UDP, Modus für DNS
	Fluent-Bit-Tolerationen	Fluent-Bit-ds zusätzliche Toleranzen.
	Ereignis-Exporteur-Tolerationen	Ereignis-Exporteur zusätzliche Toleranzen.
	Event-Exporteur-maxEventAgeSeconds	Ereignis-Exporteur max. Ereignisalter. Siehe https://github.com/jkroepke/resmoio-kubernetes-event-exporter
	RunPrivileged	Setzen Sie runPrivileged auf true, wenn Fluent Bit nicht startet und versucht, seine Datenbank zu öffnen/zu erstellen.
Workload-Zuordnung		Konfigurationsoptionen, mit denen die Erfassung der Workload-Zuordnung und die Installation des Operators angepasst werden können
	CpuLimit	CPU-Limit für Netto-Observer ds
	MemLimit	MEM-Grenze für Netto-Beobachter ds
	CpuRequest	CPU-Anforderung für Netto-Observer-ds
	MemRequest	MEM-Anforderung für Netto-Beobachter ds
	MetricAggregationInterval	Intervall für die metrische Aggregation in Sekunden
	BpfPollInterval	BPF-Abfrageintervall in Sekunden
	EnableDNSLookup	True/false, DNS-Suche aktivieren
	l4-Tolerationen	NET-Observer-l4-ds zusätzliche Toleranzen.
	RunPrivileged	True/false - Setzen Sie runPrivileged auf true, wenn SELinux auf Ihren Kubernetes-Knoten aktiviert ist.
Änderungsmanagement		Konfigurationsoptionen für das Kubernetes Change Management und die Analyse
	CpuLimit	CPU-Limit für Change-Observer-watch-rs
	MemLimit	MEM Limit für Change-Observer-Watch-rs
	CpuRequest	CPU-Anforderung für Change-Observer-watch-rs
	MemRequest	MEM-Anforderung für Change-Observer-Watch-rs
	AusfallerklärungIntervalMins	Intervall in Minuten, nach dem eine nicht erfolgreiche Bereitstellung eines Workloads als fehlgeschlagen markiert wird
	EinsatzAggrIntervalSekunden	Häufigkeit, mit der Ereignisse zur laufenden Workload-Bereitstellung gesendet werden

Komponente	Option	Beschreibung
	Nicht-WorkloadAggrIntervalSekunden	Häufigkeit der Kombination und des Sendeens von nicht-Workload-Implementierungen
	TermsToAkt	Ein Satz von regulären Ausdrücken, die in Env-Namen und Datenkarten verwendet werden, deren Wert bearbeitet wird Beispielbegriffe:„pwd“, „Passwort“, „Token“, „apikey“, „API-key“, „jwt“
	Zusätzlich KindsToWatch	Eine kommagetrennte Liste mit weiteren Arten, die von den vom Sammler überwachten Standardtypen überwacht werden sollen
	KindsToIgnoreFromWatch	Eine kommagetrennte Liste von Arten, die ignoriert werden sollen, wenn sie von den vom Sammler überwachten Standardtypen überwacht werden
	LogRecordAggrIntervalSekunden	Häufigkeit, mit der Protokolldatensätze vom Collector an CI gesendet werden
	Überwachen von Toleranzen	Change-Observer-watch-ds zusätzliche Toleranzen. Nur abgekürztes Einzelzeilenformat. Beispiel: '{key: Taint1, Operator: Existiert, Effekt: NoSchedule},{key: Taint2, Operator: Existiert, Effekt: NoExecute}'

Beispieldatei für AgentConfiguration

Unten finden Sie eine *AgentConfiguration*-Beispieldatei.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
reference
  # #   To update them, uncomment the line, change the value, and apply
the updated AgentConfiguration.
  agent:
    # # [Required Field] A uniquely identifiable user-friendly
clustername.
    # # clusterName must be unique across all clusters in your Data
Infrastructure Insights environment.
```

```
    clusterName: "my_cluster"

    # # Proxy settings. The proxy that the operator should use to send
metrics to Data Infrastructure Insights.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    # # [Required Field] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
name.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    # # [Required Field] The name of the imagePullSecret for dockerRepo.
    # # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
    dockerImagePullSecret: 'netapp-ci-docker'

    # # Allow the operator to automatically rotate its ApiKey before
expiration.
    # tokenRotationEnabled: 'true'
    # # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
    # tokenRotationThresholdDays: '30'

  telegraf:
    # # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
    # # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#a
gent

    # # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
    # collectionInterval: '60s'
```

```
    # # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
    # batchSize: '10000'
    # # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
    # bufferLimit: '150000'
    # # Collect metrics on multiples of interval (round_interval).
    # roundInterval: 'true'
    # # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
    # collectionJitter: '0s'
    # # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
    # precision: '0s'
    # # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
    # flushInterval: '60s'
    # # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
    # flushJitter: '0s'
    # # Timeout for writing to outputs (timeout).
    # outputTimeout: '5s'

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    # # telegraf-rs CPU/Mem limits and requests.
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    # # Skip second run of processors after aggregators
    # skipProcessorsAfterAggregators: 'true'

    # # telegraf additional tolerations. Use the following abbreviated
single line format only.
    # # Inspect telegraf-rs/-ds to view tolerations which are always
```

```
present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # dsTolerations: ''
    # rsTolerations: ''


    # If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node.  If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages.  While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
    # unprotected: 'false'

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # runPrivileged: 'false'

    # # Collect container Block IO metrics.
    # dsBlockIOEnabled: 'true'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: 'true'

    # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher).  Set this to true if you want collect these
metrics.
    # managedK8sSystemMetricCollectionEnabled: 'false'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: 'false'

    # # Declare Rancher cluster as managed.  Set this to true if your
Rancher cluster is managed as opposed to on-premise.
    # isManagedRancher: 'false'

    # # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

  # kube-state-metrics:
    # # kube-state-metrics CPU/Mem limits and requests.
```

```
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Comma-separated list of resources to enable.
    # # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

    # # Comma-separated list of metrics to enable.
    # # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
```

```
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests'

    # # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
    # # See metric-labels-allowlist in https://github.com/kubernetes/kube-
state-metrics/blob/main/docs/cli-arguments.md
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'

    # # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
```

```
    # # No tolerations are applied by default
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # tolerations: ''

    # # kube-state-metrics shards.  Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
    # shards: '2'

  # # Settings for the Events Log feature.
  # logs:
    # # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
    # runPrivileged: 'false'

    # # If Fluent Bit should read new files from the head, not tail.
    # # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
    # readFromHead: "true"

    # # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
    # dnsMode: "UDP"

    # # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
    # fluentBitDNSResolver: "LEGACY"

    # # Logs additional tolerations. Use the following abbreviated single
line format only.
    # # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # fluent-bit-tolerations: ''
    # event-exporter-tolerations: ''

    # # event-exporter CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    # # event-exporter max event age.
    # # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
```

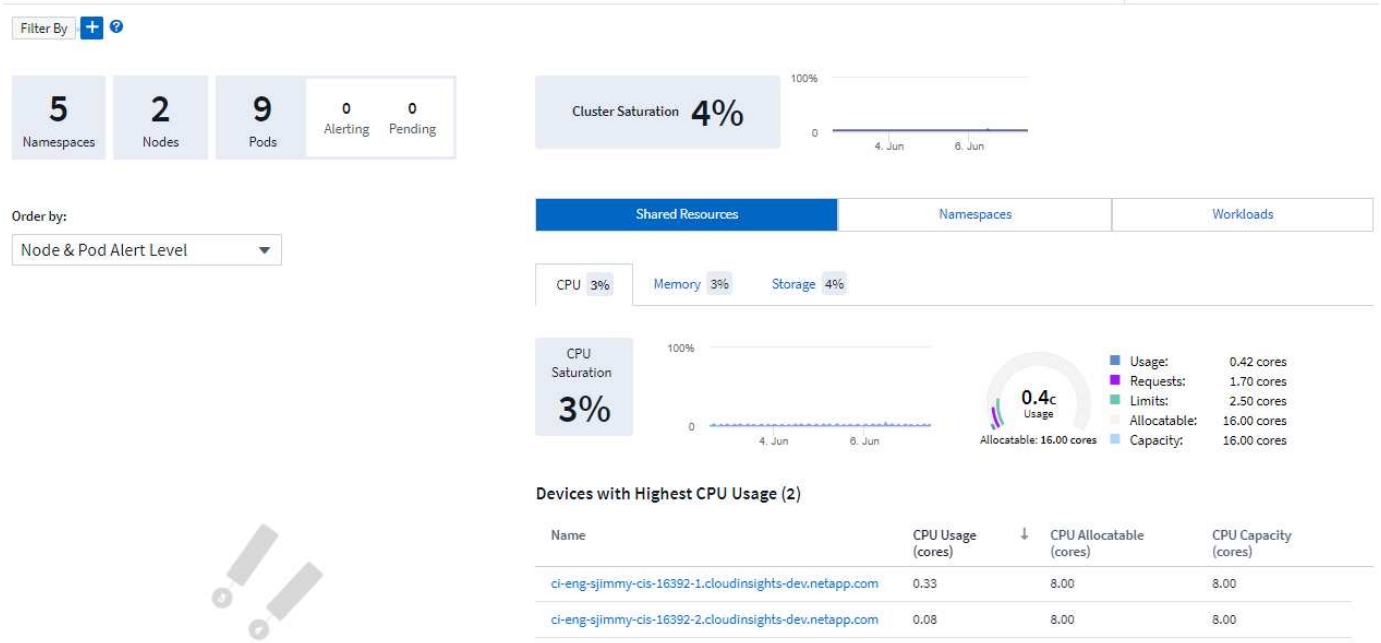
```
    # event-exporter-maxEventAgeSeconds: '10'

    # # event-exporter client-side throttling
    # # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
    # # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    # # fluent-bit CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'

  # # Settings for the Network Performance and Map feature.
  # workload-map:
    # # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Metric aggregation interval in seconds. Min=30, Max=120
    # metricAggregationInterval: '60'

    # # Interval for bpf polling. Min=3, Max=15
    # bpfPollInterval: '8'

    # # Enable performing reverse DNS lookups on observed IPs.
    # enableDNSLookup: 'true'

    # # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
    # # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # l4-tolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
```

```
nodes.
    # # Note: In OpenShift environments, this is set to true
automatically.
    # runPrivileged: 'false'

  # change-management:
    # # change-observer-watch-rs CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    # # Interval in minutes after which a non-successful deployment of a
workload will be marked as failed
    # failureDeclarationIntervalMins: '30'

    # # Frequency at which workload deployment in-progress events are sent
    # deployAggrIntervalSeconds: '300'

    # # Frequency at which non-workload deployments are combined and sent
    # nonWorkloadAggrIntervalSeconds: '15'

    # # A set of regular expressions used in env names and data maps whose
value will be redacted
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    # # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"authorization.k8s.io.subjectaccessreviews"'
    # additionalKindsToWatch: ''

    # # A comma separated list of additional field paths whose diff is
ignored as part of change analytics. This list in addition to the default
set of field paths ignored by the collector.
    # # Example: '"metadata.specTime", "data.status"'
    # additionalFieldsDiffToIgnore: ''

    # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
```

```
    # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    # kindsToIgnoreFromWatch: ''

    # # Frequency with which log records are sent to CI from the collector
    # logRecordAggrIntervalSeconds: '20'

    # # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect change-observer-watch-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # watch-tolerations: ''
```

Detailseite Zu Kubernetes Cluster

Auf der Kubernetes-Cluster-Detailseite wird eine detaillierte Übersicht über das Kubernetes-Cluster angezeigt.



Namespace, Node und Pod-Anzahl

Die Zählungen oben auf der Seite zeigen Ihnen die Gesamtzahl der Namespaces, Nodes und Pods im Cluster sowie die Anzahl der Pops, die derzeit Warnungen und ausstehend sind.

Shared Ressourcen und Sättigung

Oben rechts auf der Detailseite ist Ihre Cluster-Sättigung als aktueller Prozentsatz sowie ein Diagramm, das den letzten Trend im Laufe der Zeit zeigt. Cluster-Sättigung ist der höchste CPU-, Arbeitsspeicher- oder

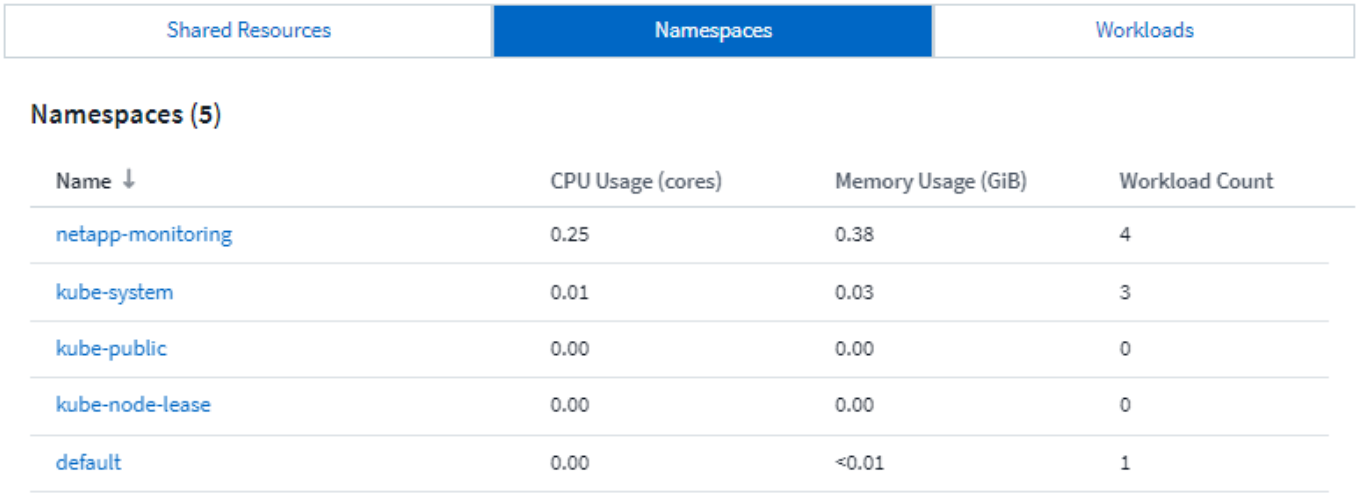
Storage-Sättigung bei jedem Zeitpunkt.

Im Folgenden wird die Seite standardmäßig **Nutzung von freigegebenen Ressourcen** mit Registerkarten für CPU, Speicher und Speicher angezeigt. Auf jeder Registerkarte werden der Sättigungspunkt und der Trend über die Zeit mit zusätzlichen Nutzungsdetails angezeigt. Für den Storage ist der angezeigte Wert der größere Backend- und Filesystem-Sättigung, die unabhängig voneinander berechnet wird.

Die Geräte mit der höchsten Nutzung werden in einer Tabelle unten angezeigt. Klicken Sie auf einen beliebigen Link, um diese Geräte zu durchsuchen.

Namespaces

Auf der Registerkarte Namespaces wird eine Liste aller Namespaces in der Kubernetes-Umgebung angezeigt. Die CPU- und Arbeitsspeicherauslastung sowie die Anzahl der Workloads in jedem Namespace werden angezeigt. Klicken Sie auf die Namenslinks, um die einzelnen Namespaces zu erkunden.



Workloads

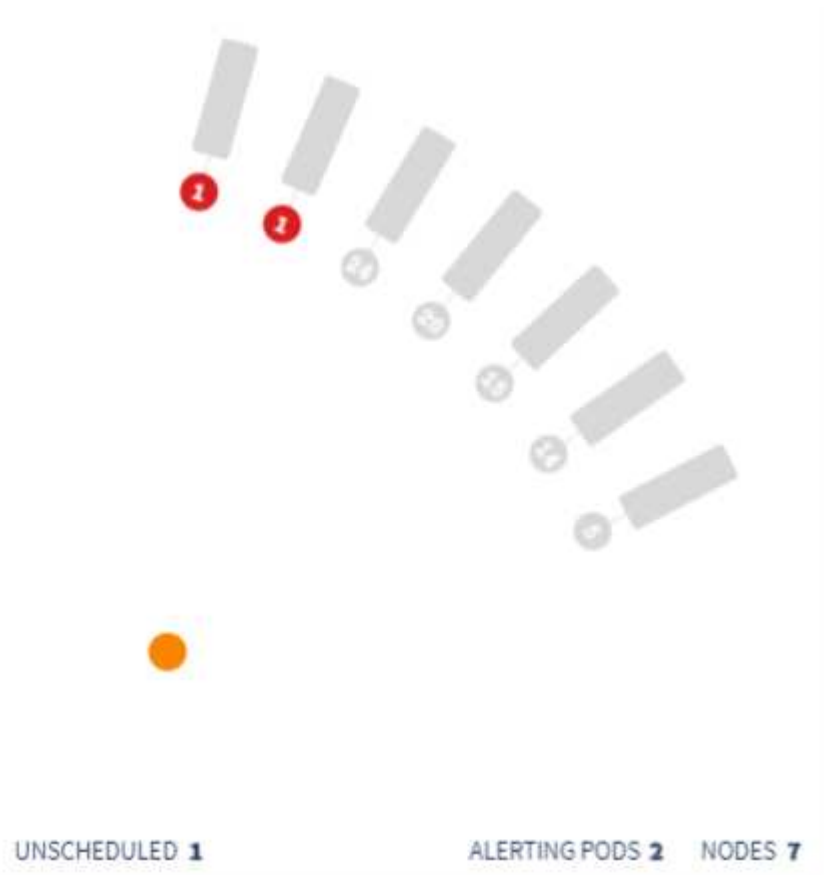
Auf der Registerkarte Workloads wird zudem eine Liste der Workloads in den einzelnen Namespace angezeigt. Auch hier wird die CPU- und Arbeitsspeicherauslastung angezeigt. Wenn Sie auf den Namespace-Links klicken, ist jeder Link bohrt.

Shared Resources | Namespaces | Workloads

Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

Das Cluster „Wheel“

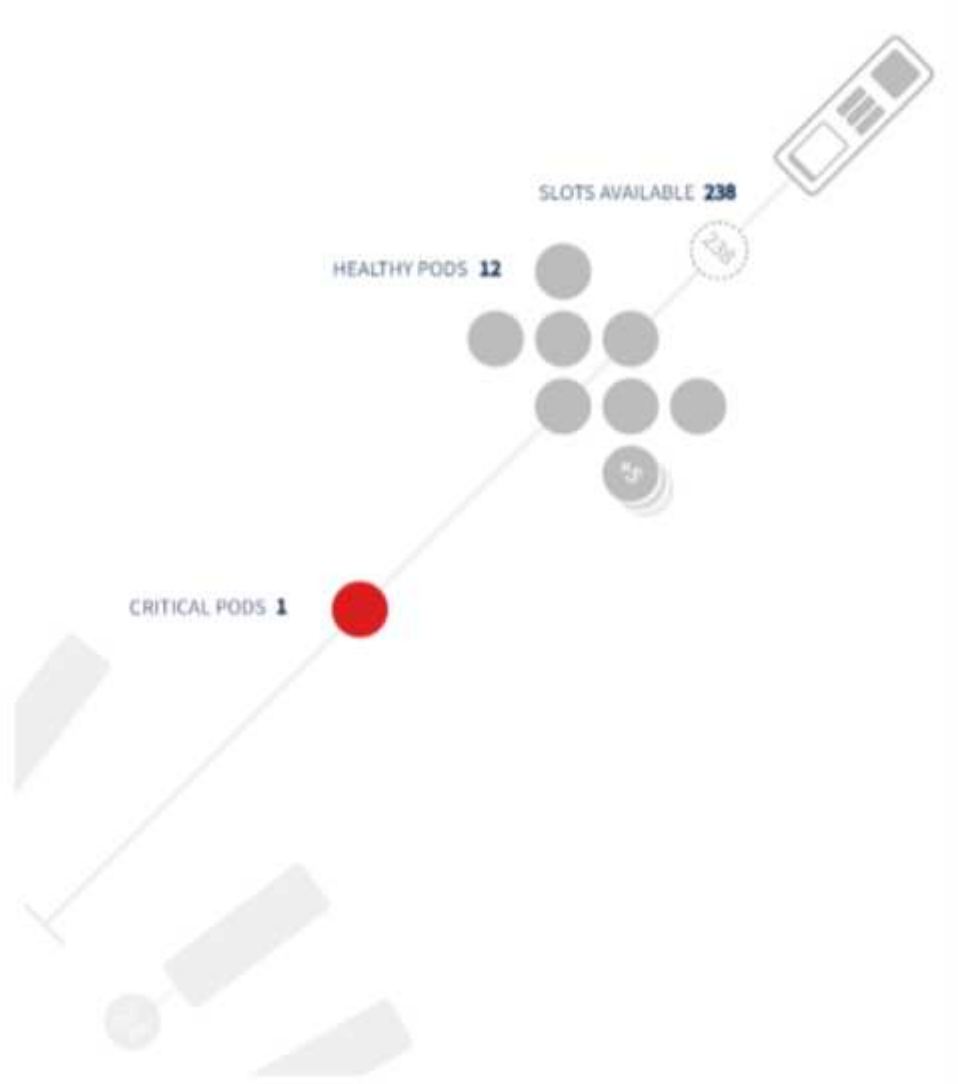


Im Abschnitt „Cluster „Wheel“ finden Sie auf einen Blick den Zustand der Nodes und des POD. Weitere Informationen hierzu finden Sie unter. Wenn Ihr Cluster mehr Nodes enthält, als in diesem Bereich der Seite angezeigt werden kann, können Sie das Rad mit den verfügbaren Schaltflächen drehen.

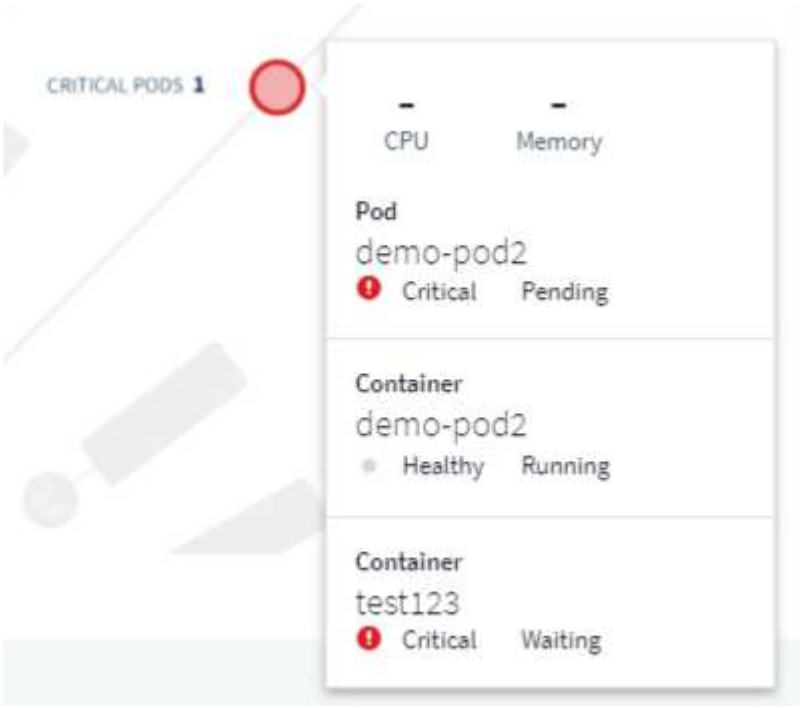
AlarmPods oder Nodes werden rot angezeigt. Die Bereiche „Warnung“ werden orange angezeigt. PODs, die nicht geplant sind (d.h. unangebracht), werden in der unteren Ecke des Cluster „Wheel“ angezeigt.

Wenn Sie sich über einen Pod (Kreis) oder Knoten (Balken) bewegen, wird die Ansicht des Knotens erweitert.

Wenn Sie in der Ansicht auf den Pod oder Node klicken, wird die Ansicht „erweiterter Node“ vergrößert.



Von hier aus können Sie mit dem Mauszeiger auf ein Element zeigen, um Details zu diesem Element anzuzeigen. Beispiel: Wenn Sie den Mauszeiger über den kritischen POD in diesem Beispiel halten, werden Details zu diesem POD angezeigt.



Sie können Filesystem-, Speicher- und CPU-Informationen anzeigen, indem Sie den Mauszeiger über die Knoten-Elemente bewegen.

Ein Hinweis zu den Messgeräten

Die Speicher- und CPU-Anzeigen zeigen drei Farben, da sie *used* in Bezug auf *zuteilbare Kapazität* und *Gesamtkapazität* zeigen.

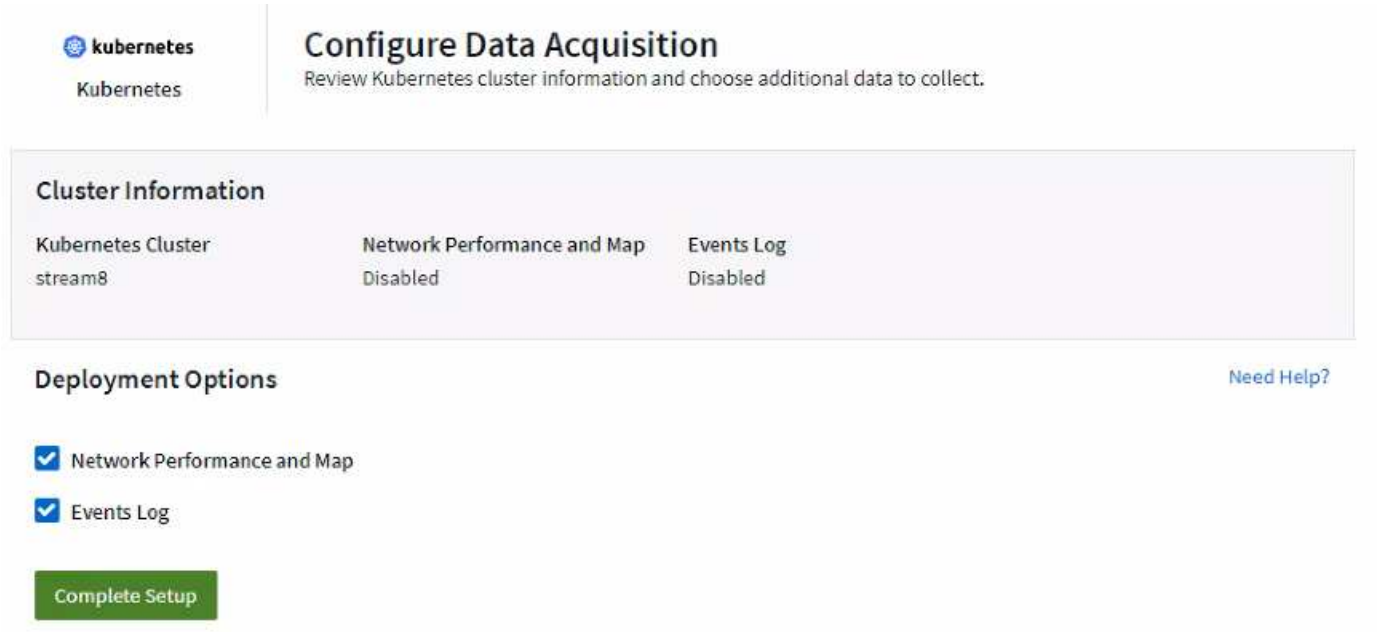
Performance-Monitoring und -Zuordnung des Kubernetes-Netzwerks

Die Kubernetes Network Performance Monitoring and Map Funktion vereinfacht die Fehlerbehebung durch die Zuordnung von Abhängigkeiten zwischen Services (auch Workloads genannt). Sie bietet Echtzeiteinblick in Latenzen und Anomalien bei der Netzwerk-Performance. So können Performance-Probleme erkannt werden, bevor sie sich auf die Benutzer auswirken.
Diese Funktion hilft Unternehmen, durch Analyse und Prüfung des Kubernetes-Traffic-Flows die Gesamtkosten zu senken.

Die wichtigsten Funktionen • die Workload-Map präsentiert Kubernetes-Workload-Abhängigkeiten und -Abläufe und hebt Netzwerk- und Performance-Probleme hervor. • Monitoring des Netzwerkverkehrs zwischen Kubernetes-Pods, Workloads und Nodes; Ermittlung der Quelle von Traffic- und Latenzproblemen • Senkung der Gesamtkosten durch Analyse des Ingress-, Egress-, Regions- und zonenübergreifenden Netzwerk-Traffics.

Voraussetzungen

Bevor Sie die Kubernetes-Netzwerk-Performance-Überwachung und -Zuordnung verwenden können, müssen Sie den konfiguriert haben "NetApp Kubernetes Monitoring Operator" Um diese Option zu aktivieren. Aktivieren Sie während der Bereitstellung des Operators das Kontrollkästchen „Netzwerkleistung und Zuordnung“, um es zu aktivieren. Sie können diese Option auch aktivieren, indem Sie zu einer Kubernetes-Landing Page navigieren und „Implementierung ändern“ auswählen.



Monitore

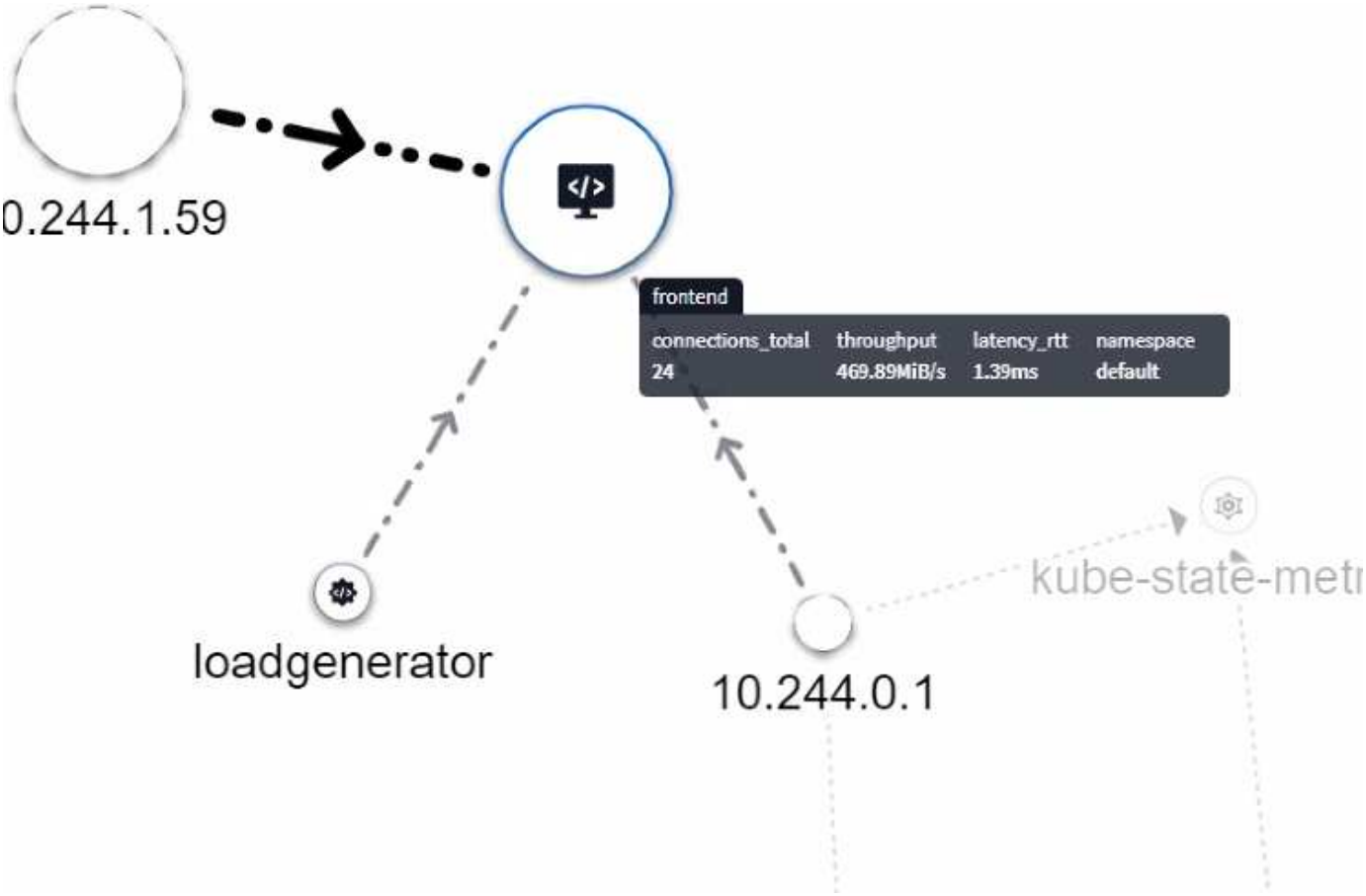
Die Workload Map verwendet"Monitore", um Informationen abzuleiten. Data Infrastructure Insights bietet eine Reihe von Kubernetes-Standardmonitoren (beachten Sie, dass diese standardmäßig „*Paused*“ sein können. Sie können die gewünschten Monitore *Resume* (d. h. aktivieren) oder benutzerdefinierte Monitore für kubernetes-Objekte erstellen, die auch von der Workload Map verwendet werden.

Sie können für jeden der unten aufgeführten Objekttypen metrische Warnmeldungen zu Data Infrastructure Insights erstellen. Stellen Sie sicher, dass die Daten nach dem Standardobjekttyp gruppiert sind.

- kubernetes.Workload
- kubernetes.demonset
- kubernetes.deployment
- kubernetes.cronjob
- kubernetes.Job
- kubernetes.Replicaset
- kubernetes.statefulset
- kubernetes.POD
- kubernetes.network_traffic_l4

Die Karte

Die Karte zeigt Services/Workloads und deren Beziehungen zueinander an. Pfeile zeigen die Verkehrsrichtung. Wenn Sie den Mauszeiger über einen Workload halten, werden zusammenfassende Informationen zu diesem Workload angezeigt, wie im folgenden Beispiel zu sehen ist:



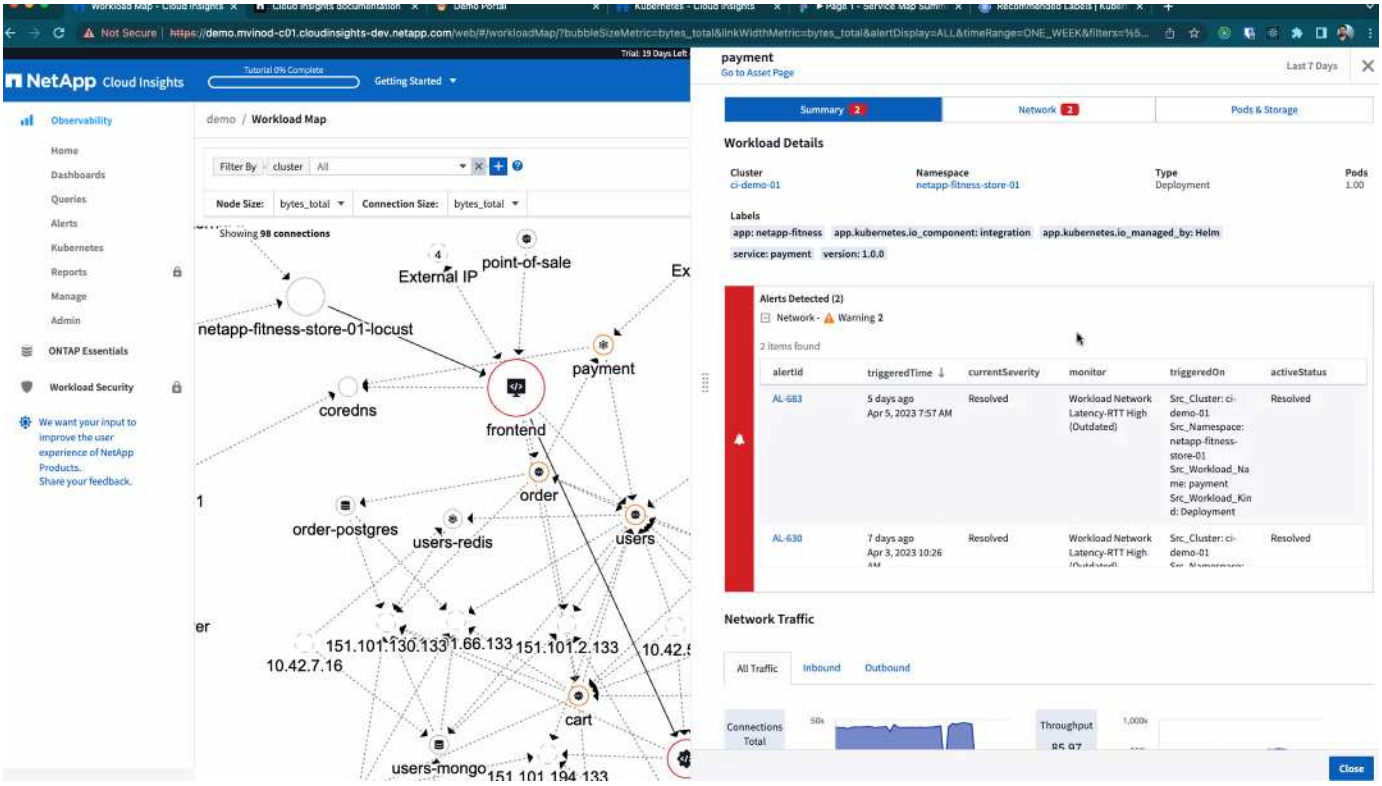
Symbole innerhalb der Kreise stellen verschiedene Diensttypen dar. Beachten Sie, dass Symbole nur sichtbar sind, wenn die zugrunde liegenden Objekte vorhanden sind Etiketten.

Die Größe jedes Kreises gibt die Knotengröße an. Beachten Sie, dass diese Größen relativ sind. Ihr Browser-Zoom-Level oder die Bildschirmgröße kann sich auf die tatsächlichen Kreisgrößen auswirken. Auf die gleiche Weise gibt Ihnen der Linienstil einen schnellen Überblick über die Verbindungsgröße; fett leuchtete Linien sind stark frequentlicht, während die gestrichelten Linien weniger Verkehr aufweisen.

Zahlen innerhalb der Kreise sind die Anzahl der externen Verbindungen, die derzeit vom Dienst verarbeitet werden.

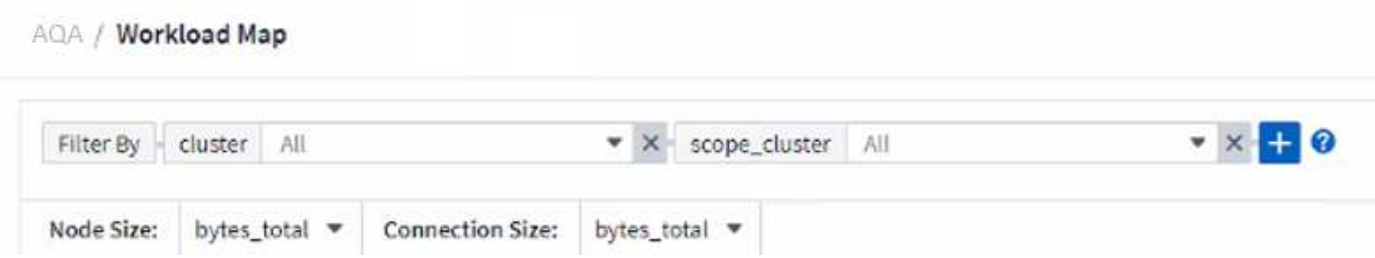
Workload-Details und -Alarme

Farbige Kreise weisen auf eine Warnung auf Warn- oder kritische Ebene für die Arbeitslast hin. Bewegen Sie den Mauszeiger über den Kreis, um eine Zusammenfassung des Problems zu erhalten, oder klicken Sie auf den Kreis, um ein Slideout-Fenster mit mehr Details zu öffnen.

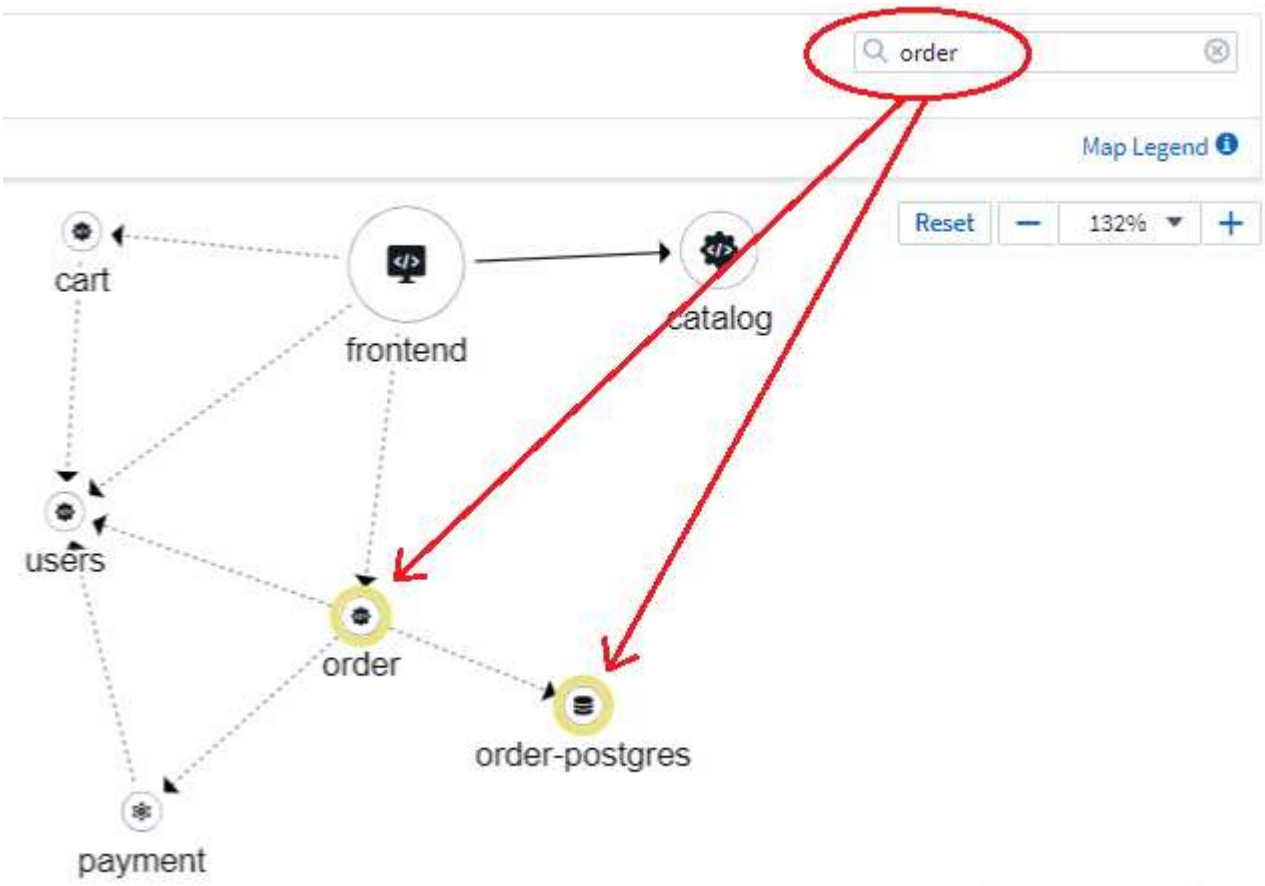


Suchen und Filtern

Wie andere Funktionen von Data Infrastructure Insights können Sie auch hier ganz einfach Filter festlegen, die sich ganz auf die gewünschten Objekte oder Workload-Attribute konzentrieren.



Ebenso wird durch Eingabe einer Zeichenfolge im Feld *Find* die übereinstimmenden Workloads hervorgehoben.



Workload-Etiketten

Workload-Bezeichnungen sind erforderlich, wenn die Zuordnung die angezeigten Workload-Typen (d. h. die Kreissymbole) identifizieren soll. Die Bezeichnungen werden wie folgt abgeleitet:

- Name des Dienstes/der Anwendung, der allgemein ausgeführt wird
- Wenn es sich bei der Quelle um einen Pod handelt:
  - Die Bezeichnung leitet sich vom Workload-Etikett des Pods ab
  - Erwartetes Label für den Workload: App.kubernetes.io/component
  - Bezeichnung Name Referenz: https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Empfohlene Etiketten:
    - Frontend

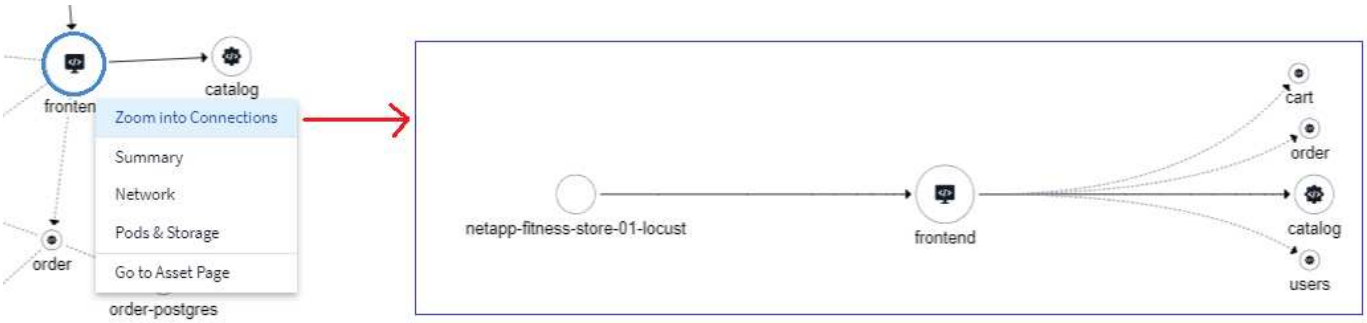
- Back-End
- Datenbank
- Cache
- Warteschlange
- kafka

- Wenn sich die Quelle außerhalb des kubernetes-Clusters befindet:
  - Data Infrastructure Insights versucht, den DNS-aufgelösten Namen zu analysieren, um den Diensttyp zu extrahieren.

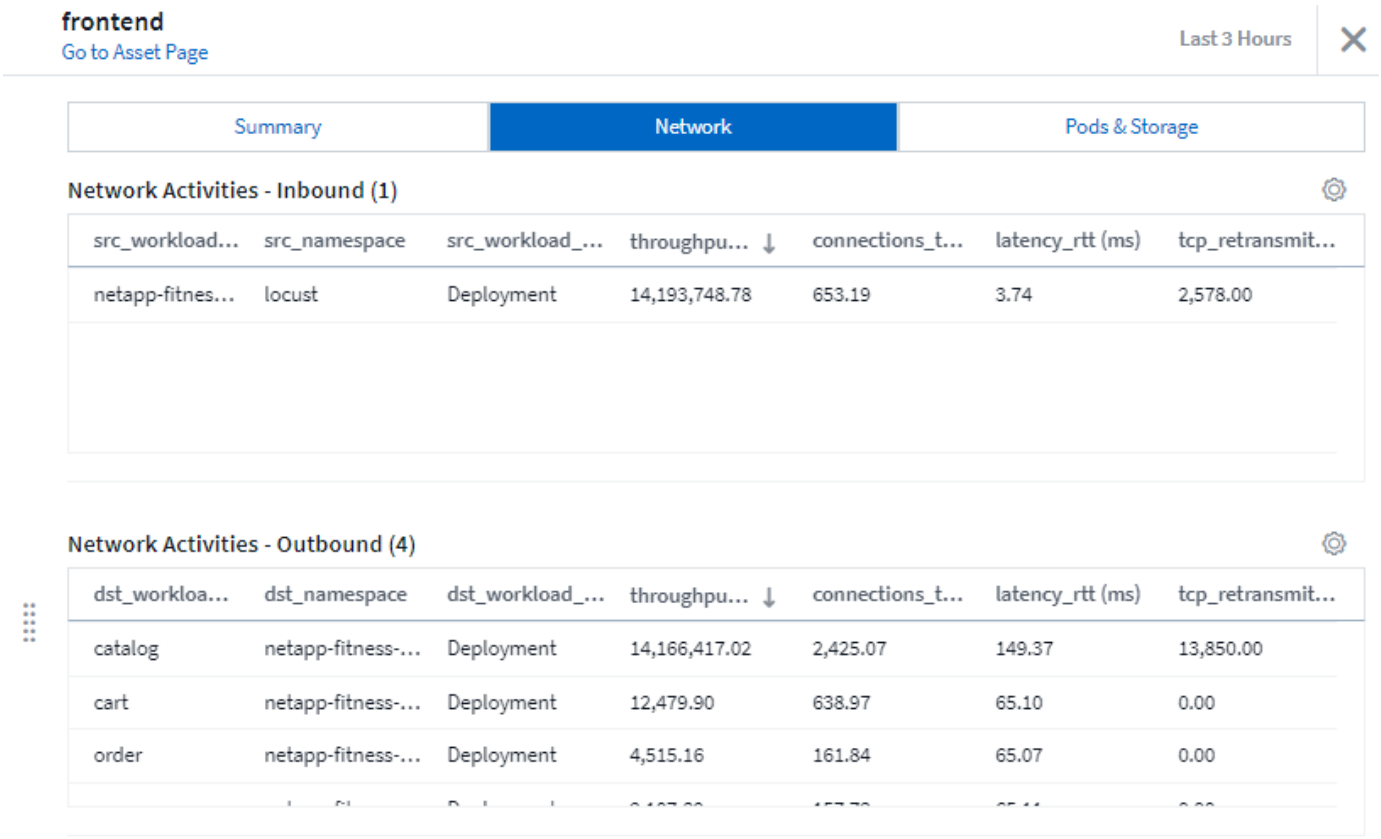
    Beispiel: Mit einem DNS-aufgelösten Namen von *s3.eu-north-1.amazonaws.com* wird der aufgelöste Name analysiert, um *s3* als Diensttyp zu erhalten.

So Geht Es Richtig

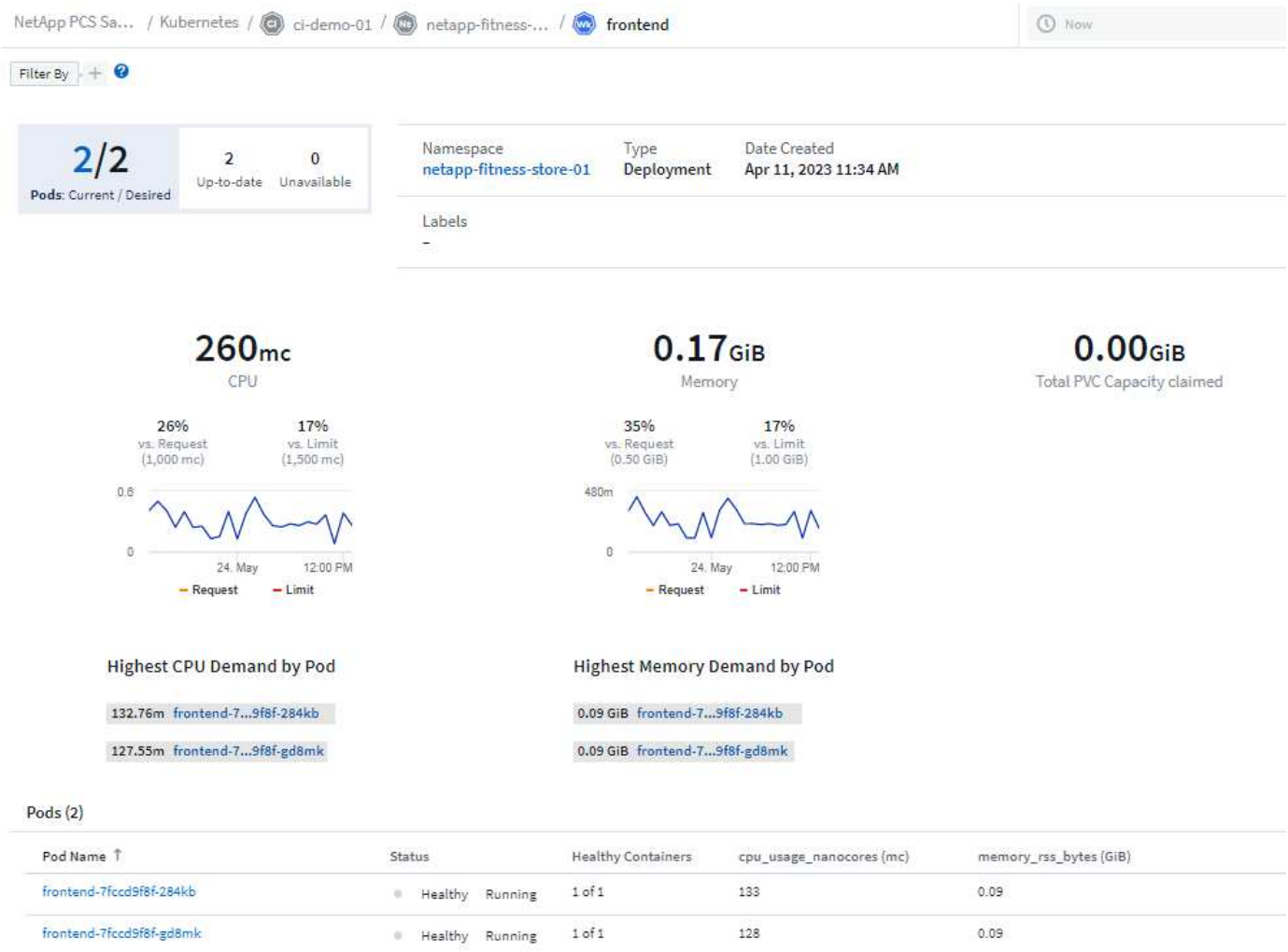
Mit einem Rechtsklick auf einen Workload erhalten Sie zusätzliche Optionen, um weitere Informationen zu erhalten. Von hier aus können Sie beispielsweise die Ansicht vergrößern, um die Verbindungen für diesen Workload anzuzeigen.



Alternativ können Sie das Detailslideout-Panel öffnen, um die Registerkarte *Summary*, *Network* oder *Pod & Storage* direkt anzuzeigen.



Durch Auswahl von *Gehe zu Anlagenseite* wird die detaillierte Zielseite für die Anlage für den Workload geöffnet.



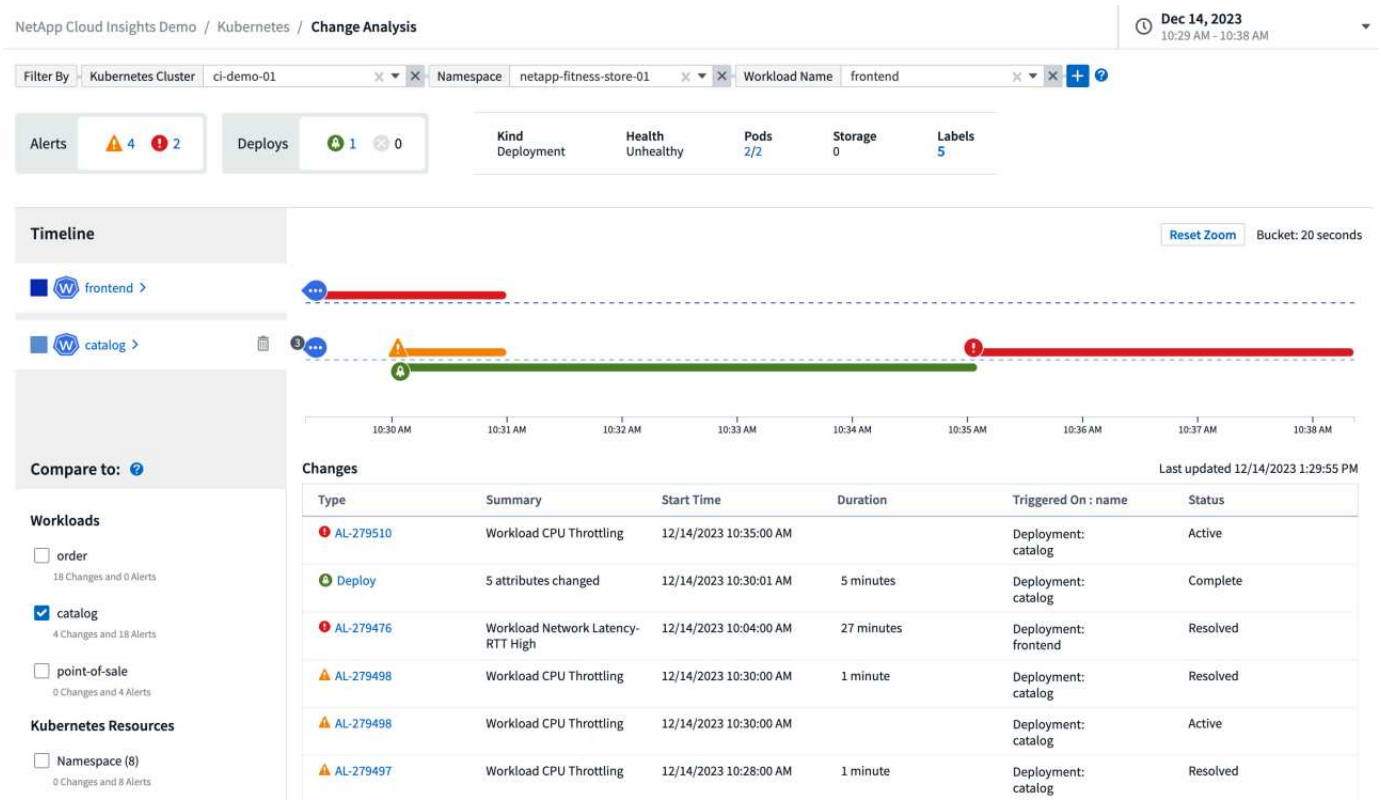
Kubernetes Change Analytics

Kubernetes Change Analytics bietet Ihnen einen All-in-One-Überblick über die letzten Änderungen an Ihrer K8s-Umgebung. Warnmeldungen und Bereitstellungsstatus stehen Ihnen jederzeit zur Verfügung. Mit Change Analytics lassen sich jede Implementierungs- und Konfigurationsänderung nachverfolgen und mit dem Zustand und der Performance von Kubernetes-Services, Infrastruktur und Clustern korrelieren.

Wie hilft die Änderungsanalyse?

- In mandantenfähigen Kubernetes-Umgebungen können Ausfälle aufgrund falsch konfigurierter Änderungen auftreten. Change Analytics unterstützt dies durch die Bereitstellung eines zentralen Fensters zur Ansicht und Korrelation des Systemzustands von Workloads und Konfigurationsänderungen. Dies kann bei der Fehlerbehebung in dynamischen Kubernetes-Umgebungen helfen.

Um Kubernetes Change Analytics anzuzeigen, navigieren Sie zu **Kubernetes > Change Analysis**.



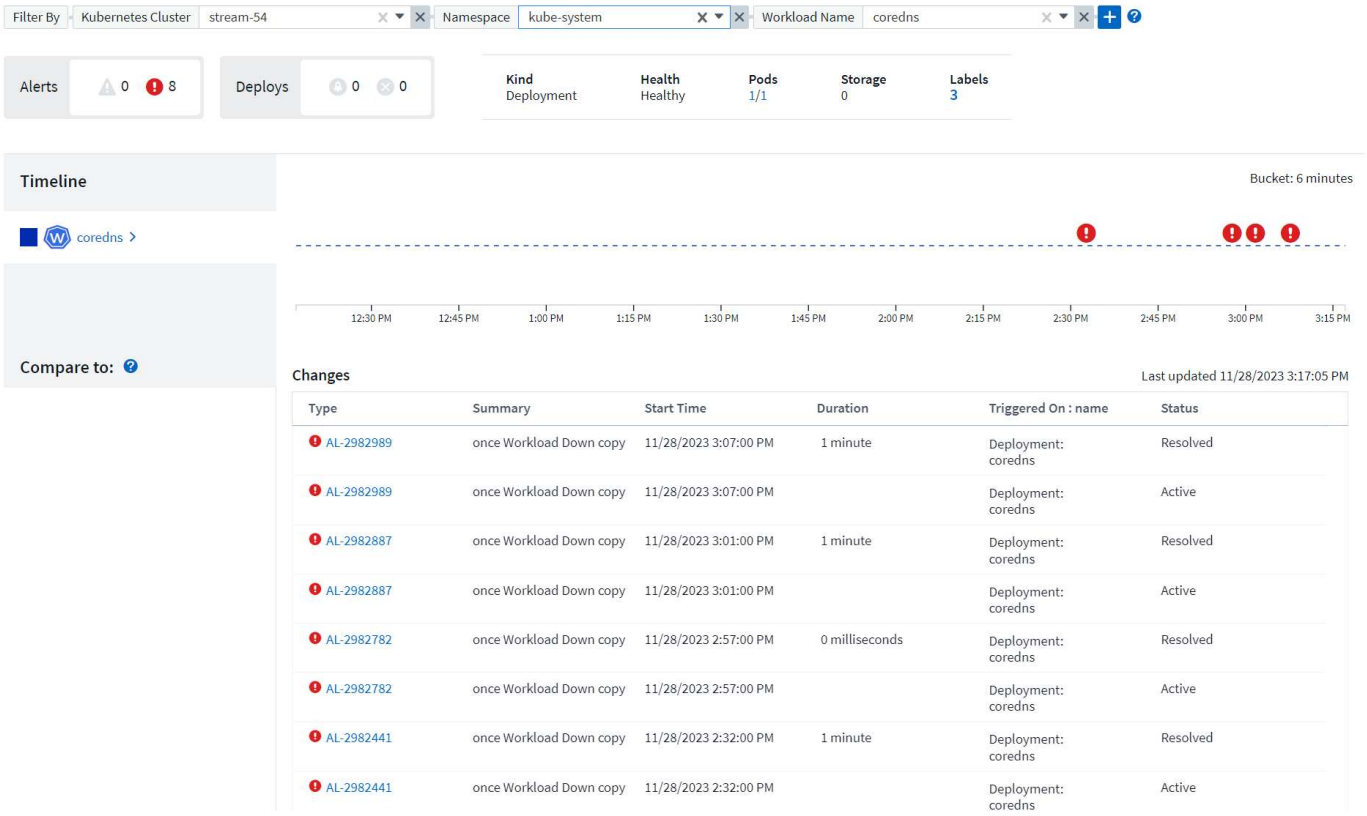
.

Die Seite wird automatisch aktualisiert, basierend auf dem aktuell ausgewählten Zeitbereich von Data Infrastructure Insights. Kleinere Zeitbereiche bedeuten eine häufigere Bildschirmerneuerung.

Filtern

Wie bei allen Funktionen von Data Infrastructure Insights ist auch das Filtern der Änderungsliste intuitiv: Ganz oben auf der Seite können Sie Werte für Ihren Kubernetes-Cluster, Namespace oder Workload eingeben oder auswählen oder mit der Schaltfläche {+] eigene Filter hinzufügen.

Wenn Sie nach unten zu einem bestimmten Cluster, Namespace und Workload filtern (zusammen mit allen anderen Filtern, die Sie festlegen), wird Ihnen ein Zeitplan für die Implementierungen und Warnungen für diesen Workload in diesem Namespace auf dem Cluster angezeigt. Vergrößern Sie die Ansicht weiter, indem Sie auf das Diagramm klicken und es ziehen, um einen bestimmten Zeitraum zu fokussieren.

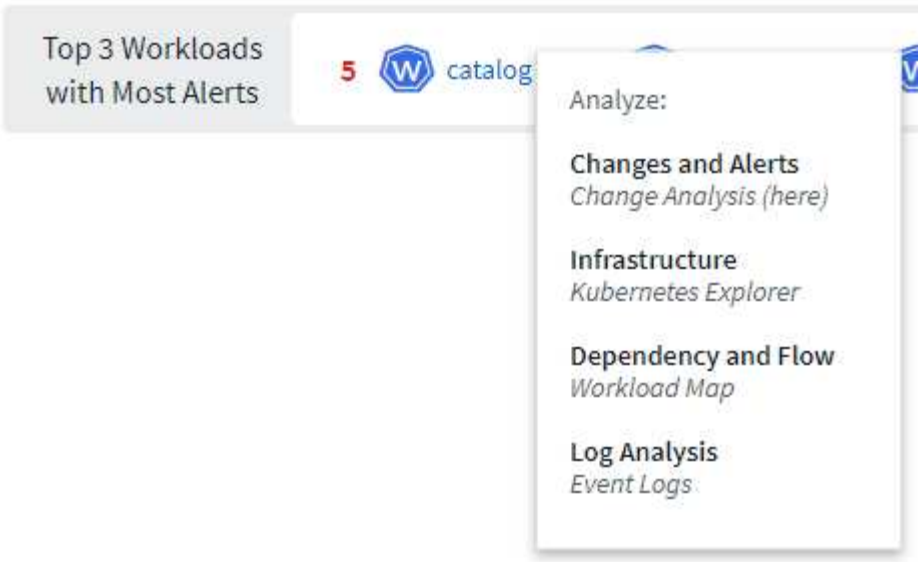


Schnellstatus

Unterhalb des Filterbereichs befinden sich eine Reihe von High-Level-Indikatoren. Auf der linken Seite ist die Anzahl der Warnungen (Warnung und kritisch). Diese Nummer enthält sowohl *Active* als auch *Resolved* Warnungen. Um nur *Active*-Warnungen anzuzeigen, setzen Sie einen Filter für „Status“ und wählen Sie „aktiv“.

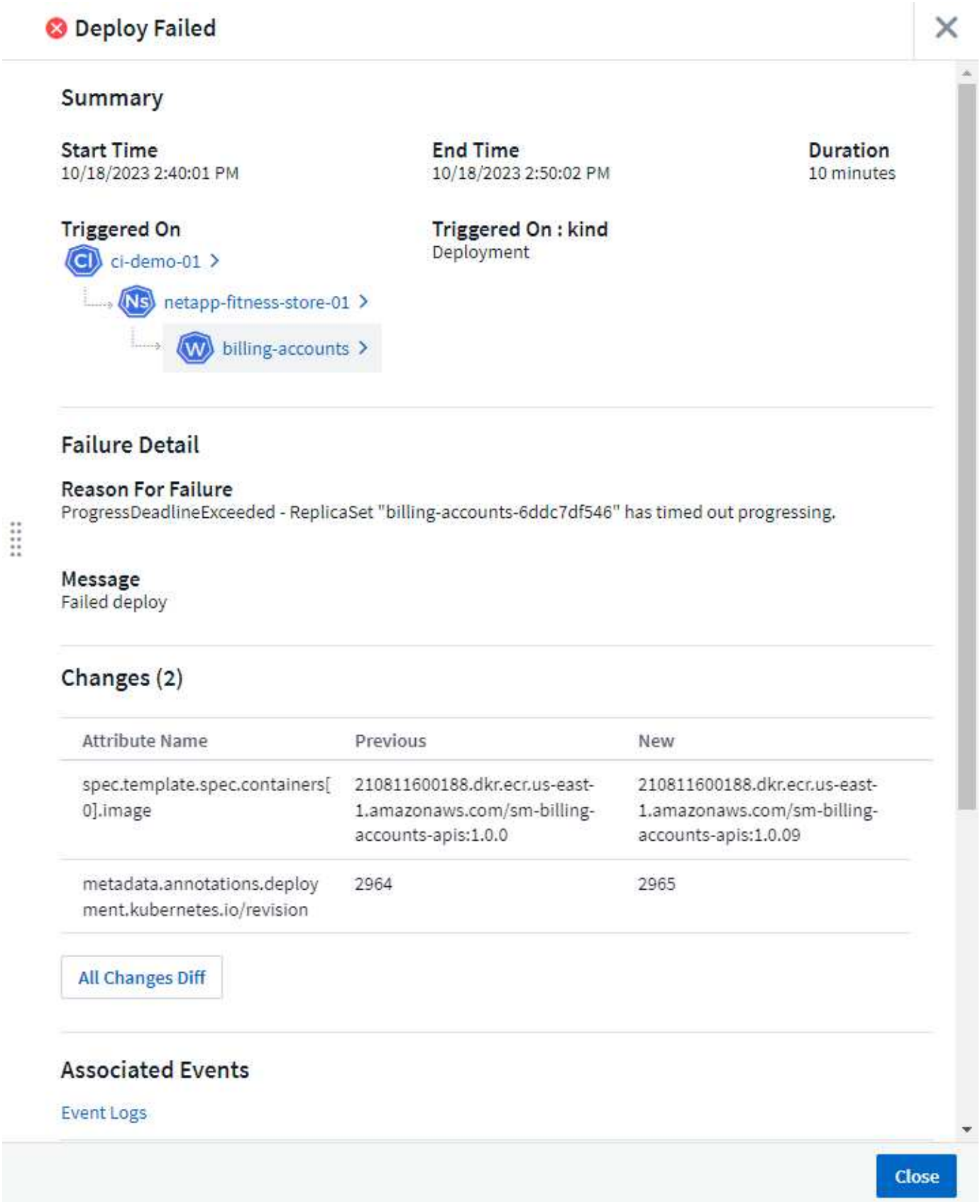
Hier wird auch der Bereitstellungsstatus angezeigt. Auch hier wird standardmäßig die Anzahl der Bereitstellungen *started*, *complete* und *failed* angezeigt. Um nur *failed*-Bereitstellungen anzuzeigen, setzen Sie einen Filter für „Status“ und wählen Sie „failed“ aus.

Als Nächstes kommen die 3 wichtigsten Workloads mit den meisten Warnmeldungen zum Einsatz. Die Zahl in rot neben jedem Workload gibt die Anzahl der Warnmeldungen in Bezug auf diesen Workload an. Klicken Sie auf den Workload-Link, um ihn in Ihre Infrastruktur (Kubernetes Explorer), Abhängigkeiten (Workload Map) oder Protokollanalyse (Event Logs) zu untersuchen.



Detailfenster

Durch Auswahl einer Änderung in der Liste wird ein Fenster geöffnet, in dem die Änderung näher beschrieben wird. Wenn Sie beispielsweise eine fehlgeschlagene Bereitstellung auswählen, wird eine Zusammenfassung der Bereitstellung mit Start- und Endzeiten, Dauer und dem Auslösungsort der Bereitstellung sowie Links zur Untersuchung dieser Ressourcen angezeigt. Außerdem werden der Grund für den Fehler, alle zugehörigen Änderungen und alle zugehörigen Ereignisse angezeigt.



Durch die Auswahl einer Warnmeldung erhalten Sie ebenfalls Details zur Warnmeldung, einschließlich des Monitors, der die Warnmeldung ausgelöst hat, sowie ein Diagramm mit einer visuellen Zeitleiste für die Warnmeldung.

ONTAP Essentials

ONTAP Essentials enthält eine Sammlung von Dashboards und Workflows, die einen detaillierten Überblick über Ihre ONTAP-Bestände und Workloads geben. Bei der Arbeit in den ONTAP-Grundlagen werden die folgenden Begriffe verwendet:

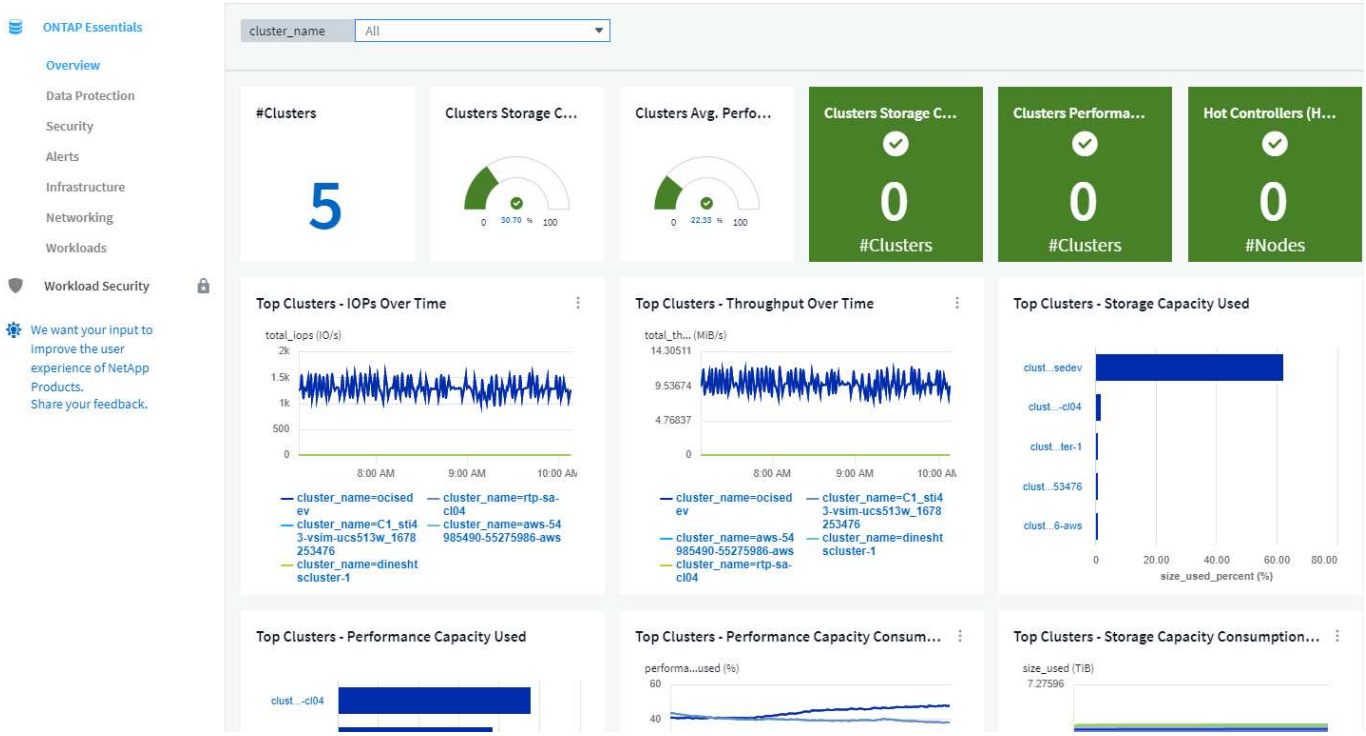
- Infrastruktur/Inventar: Objekte, die Benutzerdaten Storage-/Netzwerkservices bereitstellen
- Workloads: Objekte, die Benutzern eine Schnittstelle zum Lesen/Schreiben von Daten bieten
- Datensicherung: Objekte, die mit NetApp Datensicherungs-Technologien gesichert werden können

Weitere Begriffe und Definitionen zu ONTAP finden Sie im "ONTAP Data Collector" Dokumentation.

ONTAP Essentials erfordert mindestens einen funktionierenden ONTAP Data Collector mit Daten, die innerhalb der letzten sieben Tage erfasst werden.

Überblick

Wählen Sie zum Erkunden der Informationen **ONTAP Essentials** aus dem Hauptmenü Dateninfrastrukturdaten.



Das Dashboard **Übersicht** zeigt nützliche Informationen wie die Anzahl der Cluster in Ihrer Umgebung mit ihrer Gesamtkapazität und ihren Prozentwerten an Performance an. Außerdem werden Prognosedaten zur Anzahl der erwarteten Tage angezeigt, bis ihnen die Storage-Kapazität oder Performance-Kapazität nicht mehr genügend Speicherplatz zur Verfügung steht. Außerdem, wenn Controller in Ihrer Infrastruktur mit einer CPU von mehr als 65 % laufen - wodurch Ihr Cluster möglicherweise im Falle eines Failovers gefährdet wird - zeigt ONTAP Essentials diese als „Hot“ Controller an.

Informative Diagramme geben Ihnen einen Überblick über die Performance über einen längeren Zeitraum und über Ausfälle der Kapazitätsauslastung. Jede dieser Diagramme oder Datenpunkte kann als Ausgangspunkt

für Untersuchungen oder Untersuchungen verwendet werden.

Hinweis: Eine „Tage bis zur vollen“ Zahl von „0“ (Null) gibt an, dass die Tage für die volle Anzahl von mehr als 90 Tagen geschätzt werden. Mit anderen Worten: Ihre Systeme sind nicht in der Gefahr, dass der Speicherplatz zu jeder Zeit knapp wird.

Datensicherung

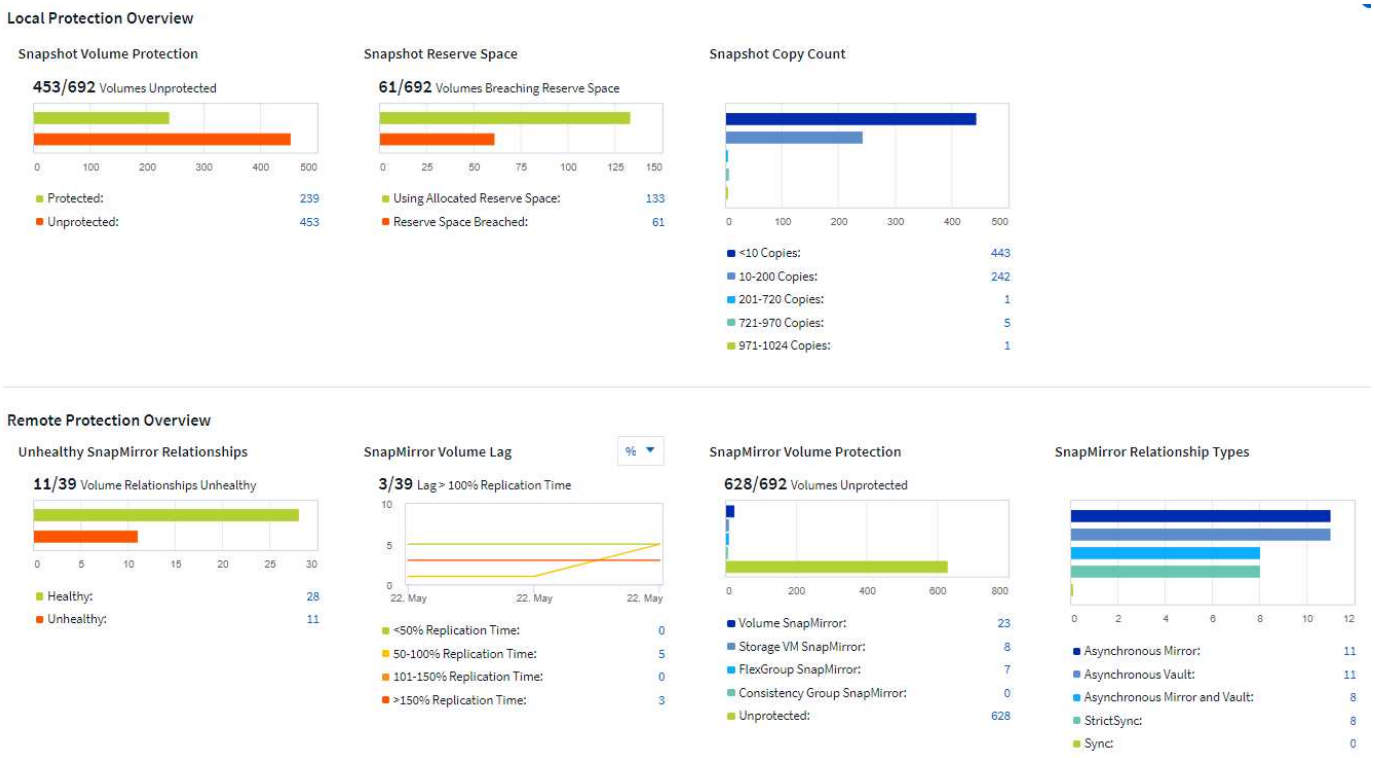
Auf der Seite **Data Protection** wird der Status von Volumes angezeigt, die durch **Snapshot-Kopien** oder **SnapMirror-Richtlinien** geschützt sind.

Im Abschnitt *Local Protection Overview* bieten die Diagramme die folgenden Informationen für Volumes, die durch Snapshot-Kopien geschützt sind:

- Die Anzahl der durch Snapshot Kopien geschützten Volumes bzw. Volumes, die nicht geschützt sind.
- Die Anzahl der Volumes, die den reservierten Speicherplatz für die Snapshot-Kopien verwenden oder überschreiten.
- Die Anzahl der Volumes in einem bestimmten Bereich der Anzahl der Snapshot Kopien (d. h. weniger als 10 Kopien, 10 bis 200 usw.).

Im Abschnitt *Remote Protection Overview* bieten die Diagramme Informationen zu Volumes, die durch SnapMirror Richtlinien geschützt sind:

- Anzahl fehlerhafter und fehlerhafter SnapMirror Beziehungen
- Die Anzahl der SnapMirror Beziehungen, die eine Verzögerung beim Recovery Point Objective (RPO) verzeichnen, basierend auf dem lag Status.
- Die Anzahl der durch SnapMirror Volume-Sicherungstypen geschützten Beziehungen, z. B. Volume SnapMirror, SVMDR-Beziehungen, FlexGroup SnapMirror Beziehungen, SnapMirror Business Continuity (SMBC)-Beziehungen und ungesicherte Volumes.
- Die Anzahl der durch die SnapMirror-Beziehungstypen geschützten Beziehungen, z. B. Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync und Sync.



Das *Clusters*-Raster unten auf der Seite enthält Details zu folgenden Themen:

- Volumes, die nicht durch Snapshots geschützt sind.
- Volumes, die den Speicherplatz der Snapshot-Reserve nicht erreichen.
- Volumes, die nicht durch snapmirror Richtlinien geschützt sind, und snapmirror Beziehungen weisen Verzögerungen auf.
- Ungesunde SnapMirror Beziehungen.

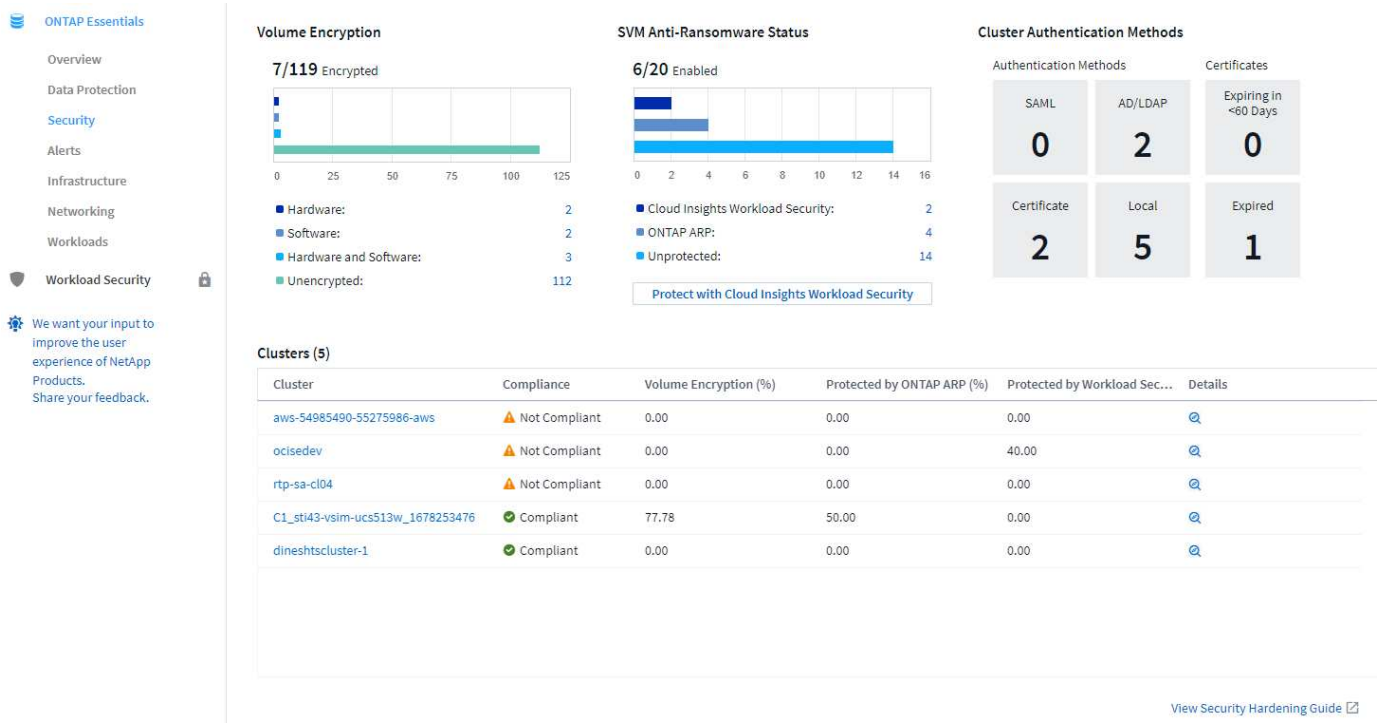
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Sicherheit

Das Security Dashboard bietet Ihnen einen sofortigen Überblick über Ihre aktuelle Sicherheitssituation und zeigt Diagramme zur Verschlüsselung von Hardware- und Software-Volumes, zum Ransomware-Schutz und zu Clusterauthentifizierungsmethoden an. Die Sicherheitskriterien werden anhand der in definierten Empfehlungen bewertet **"NetApp Security Hardening Guide for ONTAP 9"**.

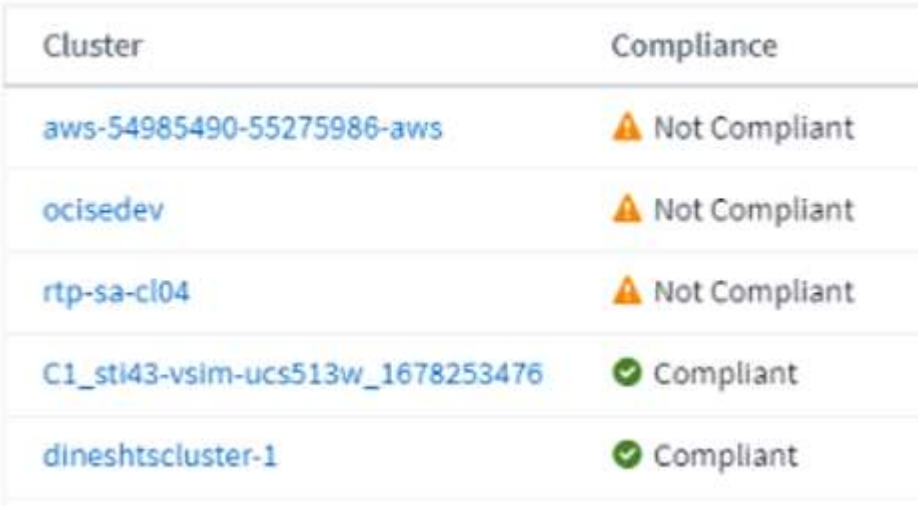
Wählen Sie eine beliebige Verschlüsselung oder Anti-Ransomware-Zählung aus, um in Ihre Umgebung einzutauchen.



Das ONTAP Essentials SicherheitsDashboard überwacht die Umgebung, um den Cluster-Compliance-Status zu ermitteln. Siehe "Cluster-Compliance-Kategorien" Um mehr zu erfahren. ONTAP Essentials verwendet die folgenden Monitore zur Bestimmung der Compliance:

Monitorname	Attributname (angezeigt in Cluster-Details)	Attributkonformer Wert
FIPS-Modus deaktiviert	FIPS-Modus	Aktiviert
Cluster unsichere Chiffren für SSH	Sichere SSH-Einstellungen	Ja.
Telnet-Protokoll Aktiviert	Telnet	Deaktiviert
Remote Shell Aktiviert	Remote Shell	Deaktiviert
Lokaler Admin-Standardbenutzer Aktiviert	Standard-Admin-Benutzer	Deaktiviert
MD5-Kennwort gehasht	MD5 wird verwendet	Nein
Cluster-Peer-Kommunikation Ist Nicht Verschlüsselt	Cluster-Peering	Verschlüsselt/Kein Peer
AutoSupport HTTPS-Transport deaktiviert	AutoSupport über HTTPS	Ja.
Es sind keine NTP-Server konfiguriert	Network Time Protocol	Konfiguriert
NTP-Serveranzahl ist niedrig	Network Time Protocol	Konfiguriert
Das Cluster-Anmelde-Banner Ist Deaktiviert	Anmelde-Banner	Aktiviert
Protokollweiterleitung Nicht Verschlüsselt	Protokollweiterleitung Verschlüsselt	Ja.

Wenn ein Monitor oben deaktiviert ist, wird der Wert für das entsprechende Sicherheitsattribut in den Cluster-Details als ‘nicht aktiviert’ angezeigt.

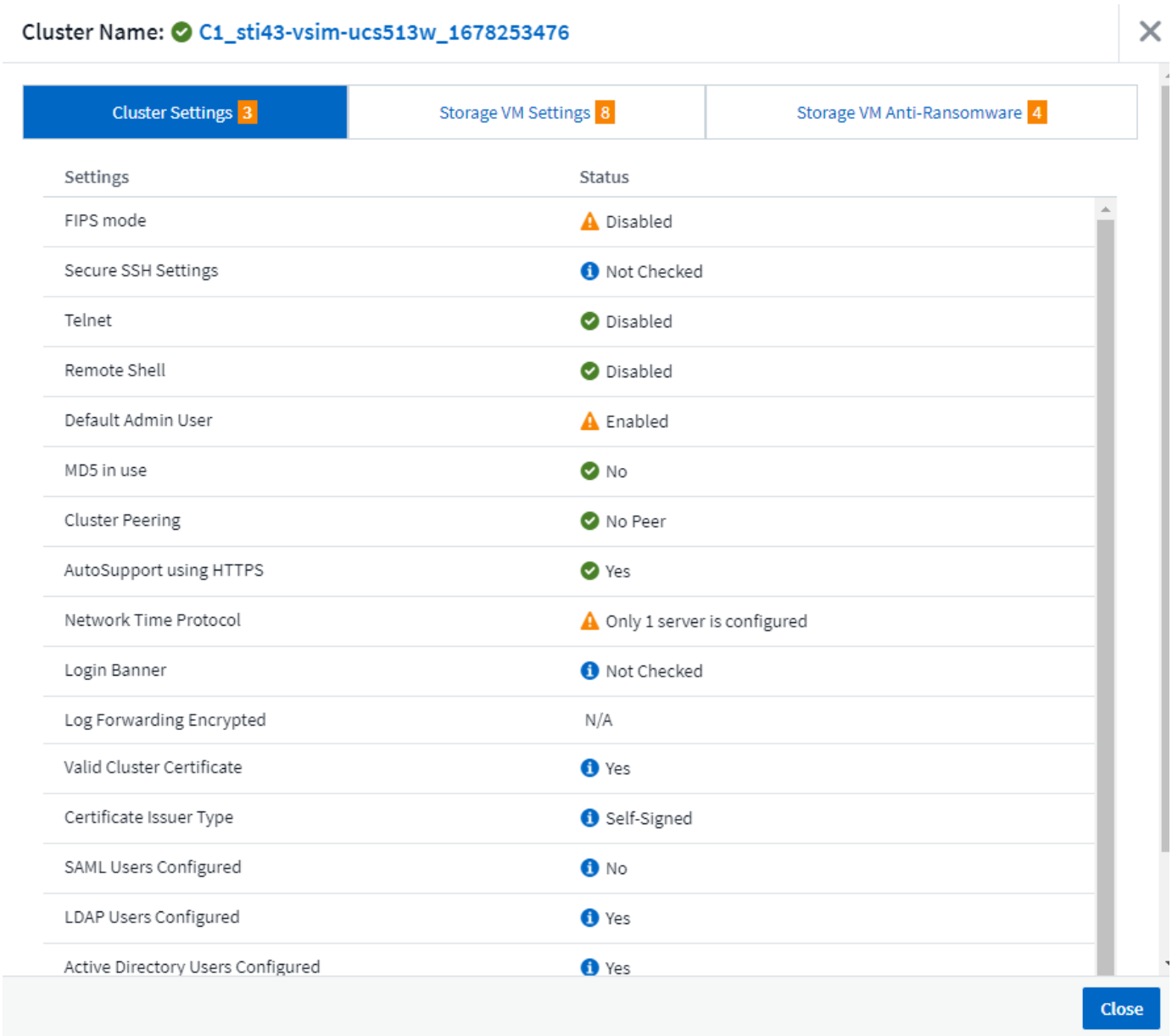


Bei SVMs werden die folgenden Monitore im Security Dashboard angezeigt:

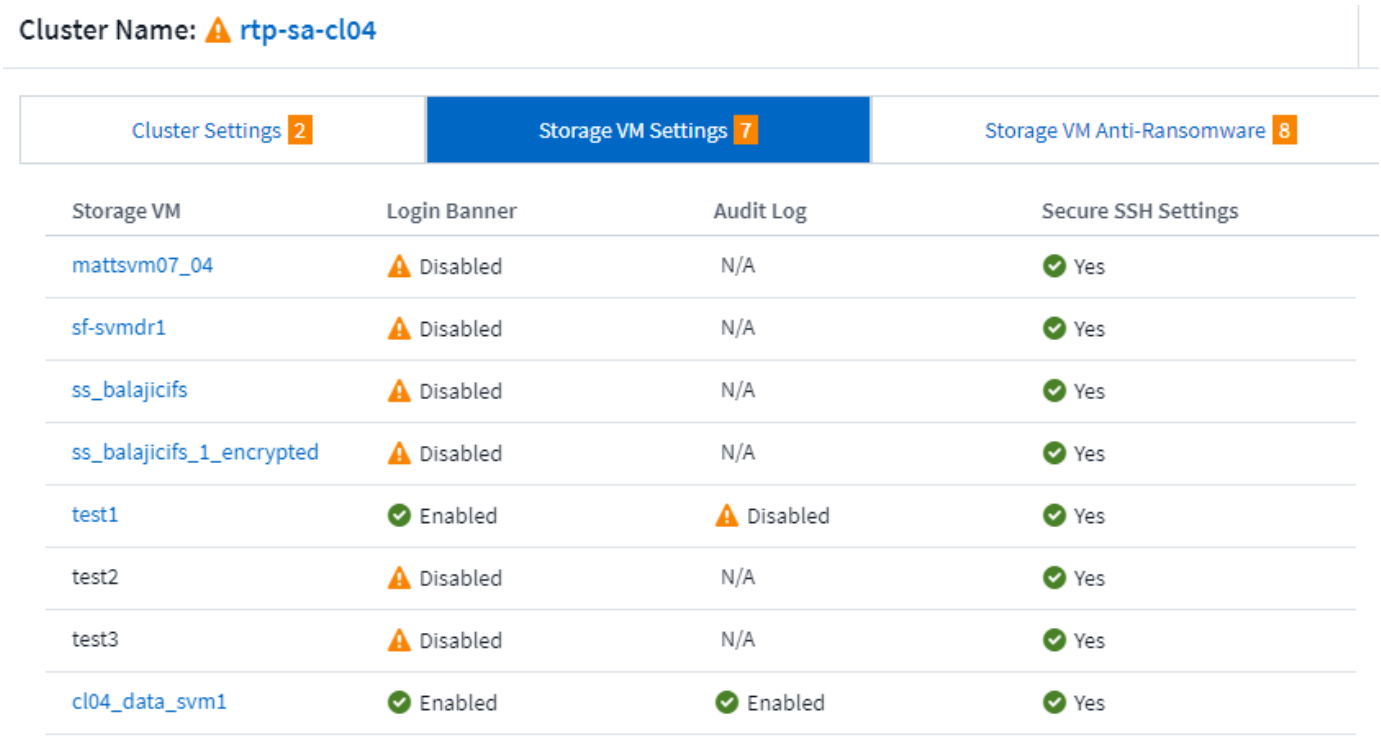
Monitorname	**Attributname (angezeigt unter Storage VM Settings)**	**Attributkonformer Wert**
Storage VM unsichere Chiffren für SSH	Sichere SSH-Einstellungen	Ja.
Anmeldebanner für Storage VM deaktiviert	Anmelde-Banner	Aktiviert
Überwachungsprotokoll für Storage VM ist deaktiviert	Überwachungsprotokoll	Aktiviert

Wählen Sie in der Cluster-Liste *View Details* für jedes Cluster aus, um ein „Slideout“-Fenster zu öffnen, in dem die aktuellen Einstellungen für *Cluster, Storage VM,* oder *Anti-Ransomware* angezeigt werden.

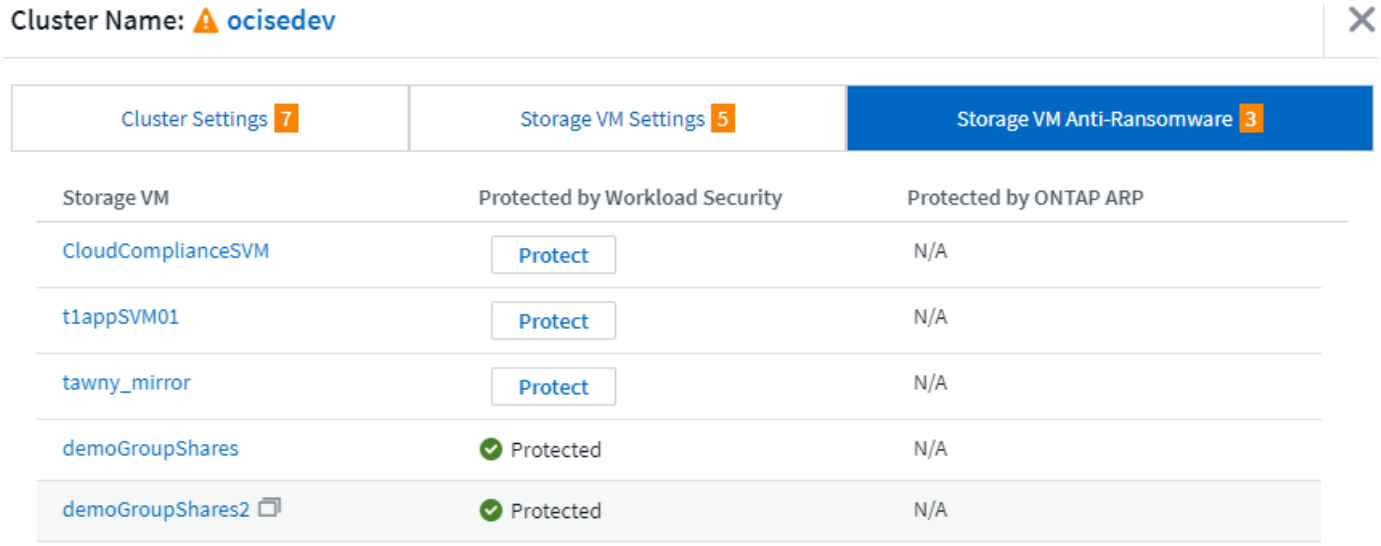
Cluster-Details umfassen den Verbindungsstatus, Zertifikatsinformationen und vieles mehr:



Details zur Storage VM zeigen Audit- und SSH-Informationen an:

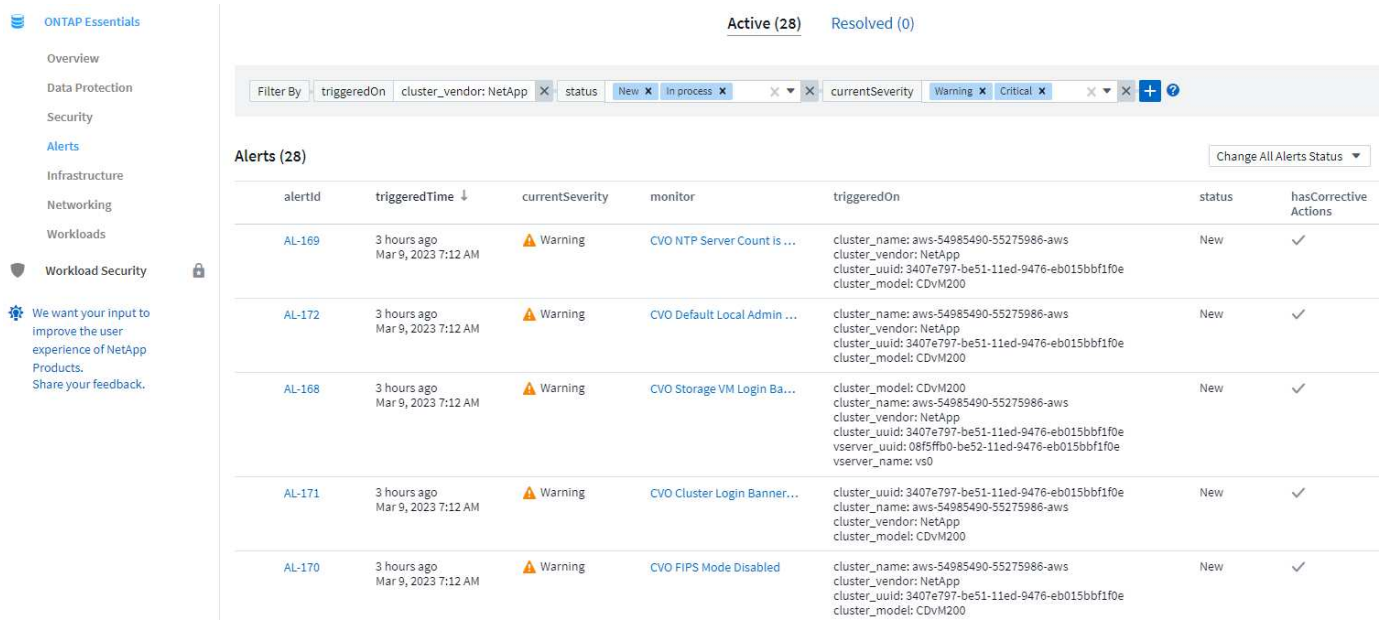


Details zur Ransomware-Bekämpfung zeigen, ob eine Storage-VM durch den Schutz vor Ransomware von ONTAP oder Einblicke in die Dateninfrastruktur geschützt ist Workload Security. Beachten Sie, dass in der Spalte „ONTAP ARP“ der aktuelle Status des integrierten Schutzes vor Ransomware von ONTAP angezeigt wird, der auf dem ONTAP System konfiguriert ist. Data Infrastructure Insights Workload Security kann durch Auswahl von „Protect“ in dieser Spalte aktiviert werden.



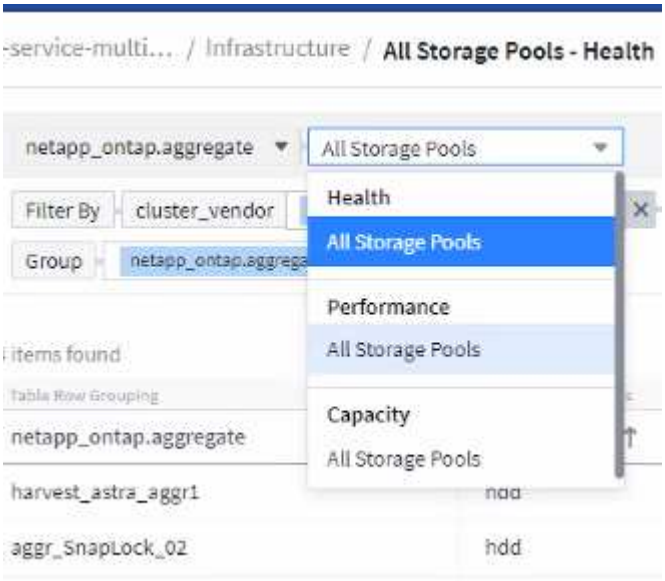
Meldungen

Hier können Sie die Active Alerts in Ihrer Umgebung anzeigen und potenzielle Probleme schnell auf den Blick nehmen. Wählen Sie die Registerkarte *aufgelöst* aus, um die Warnmeldungen anzuzeigen, die behoben wurden.

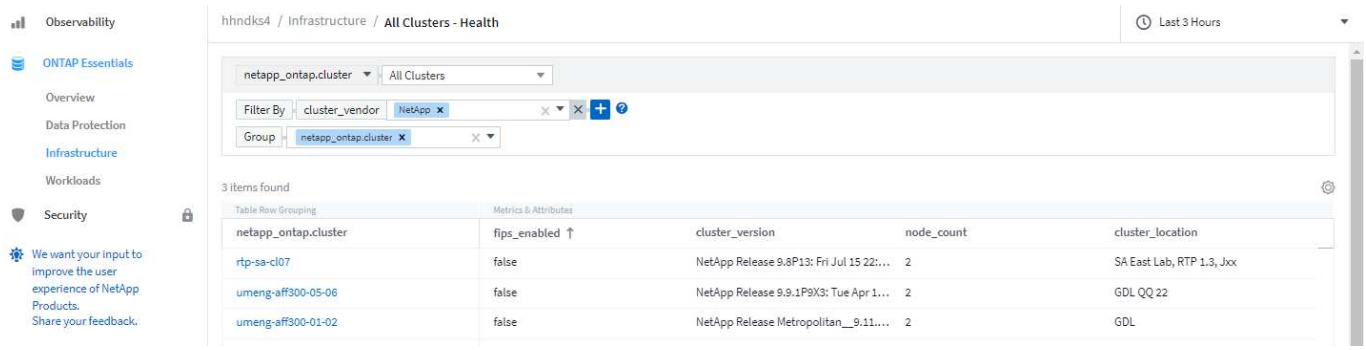


Infrastruktur

Die Seite ONTAP Essentials **Infrastruktur** bietet Ihnen einen Überblick über den Zustand und die Leistung des Clusters. Dabei werden vorkonfigurierte Abfragen für alle grundlegenden ONTAP-Objekte verwendet. Wählen Sie den Objekttyp aus, den Sie erkunden möchten (Cluster, Storage Pool usw.), und legen Sie fest, ob Informationen zu Systemzustand und Performance angezeigt werden sollen. Stellen Sie Filter ein, um sich tiefer in einzelne Systeme einzutauchen.

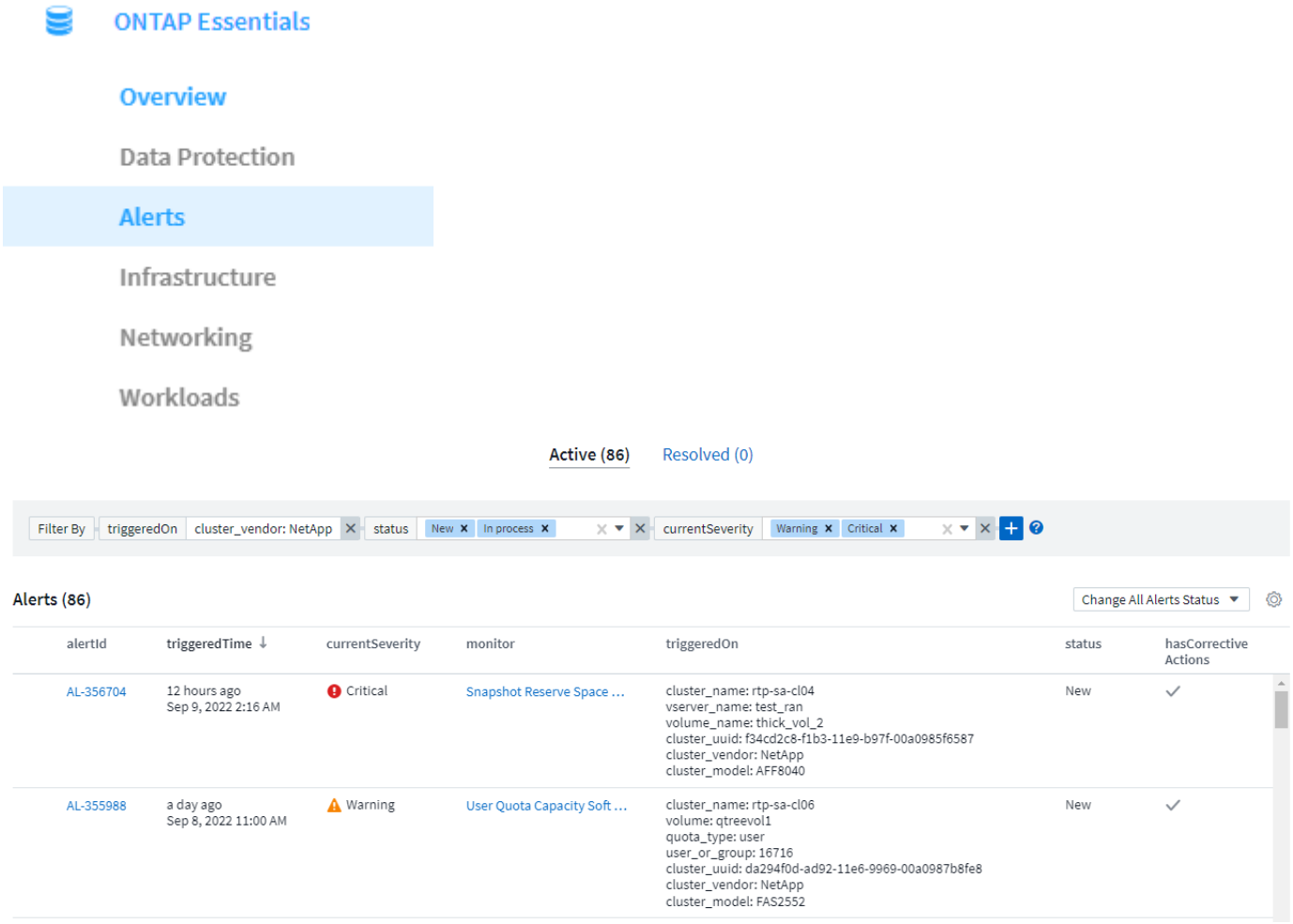


Infrastrukturseite mit Cluster-Zustand:



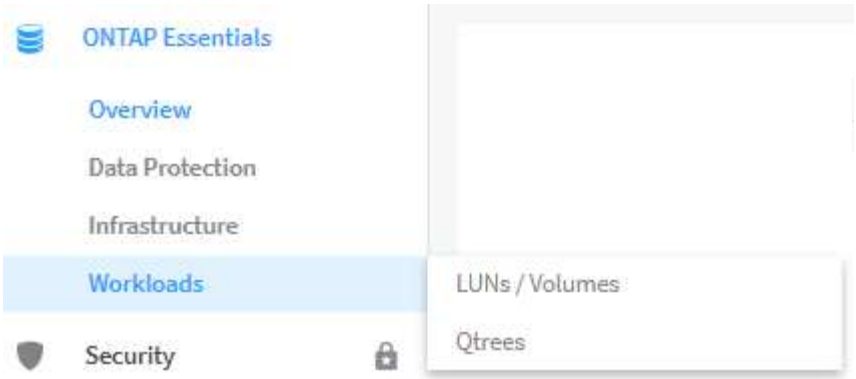
Netzwerkbetrieb

Das ONTAP Essentials Networking verschafft Ihnen Ansichten Ihrer FC-, NVME FC-, Ethernet- und iSCSI-Infrastruktur. Auf diesen Seiten können Sie Dinge wie Ports in Ihren Clustern und deren Knoten erkunden.



Workloads

Workloads auf LUNs/Volumes, NFS- oder SMB-Freigaben oder qtrees in Ihrer Umgebung anzeigen und erkunden.



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

Verwaltung und andere Aufgaben

Data Infrastructure Insights API

Die Insights API der Dateninfrastruktur ermöglicht es NetApp Kunden und unabhängigen Softwareanbietern (ISVs), Dateninfrastrukturanalysen mit anderen Applikationen wie beispielsweise CMDBs oder anderen Ticketsystemen zu integrieren.

Beachten Sie, dass die Data Infrastructure Insights APIs auf Basis Ihrer aktuellen Edition verfügbar sind:

API-Typ	Basic	Standard	Premium
Erfassungseinheit	✔	✔	✔
Datenerfassung	✔	✔	✔
Meldungen		✔	✔
Ressourcen		✔	✔
Datenaufnahme		✔	✔
Aufnahme Protokollieren		✔	✔

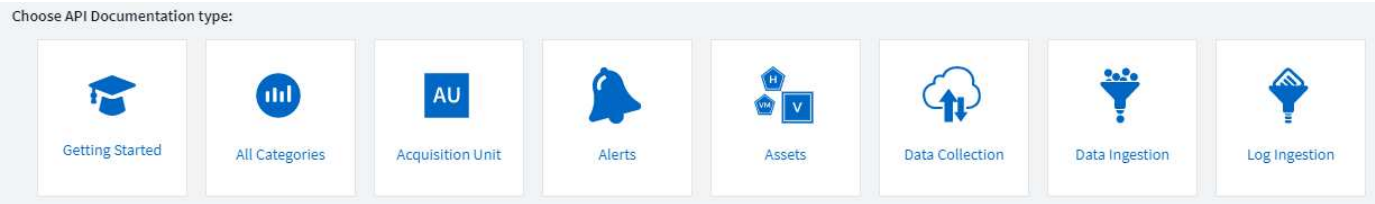
Außerdem "Funktionsgruppe Rolle"bestimmt Ihre Data Infrastructure Insights, auf welche APIs Sie zugreifen können. Benutzer- und Gastrollen haben weniger Berechtigungen als Administratorrolle. Wenn Sie z. B. in Überwachen und Optimieren eine Administratorrolle haben, die Rolle Benutzer jedoch in Reporting verwendet wird, können Sie alle API-Typen außer Data Warehouse verwalten.

Anforderungen für den API-Zugriff

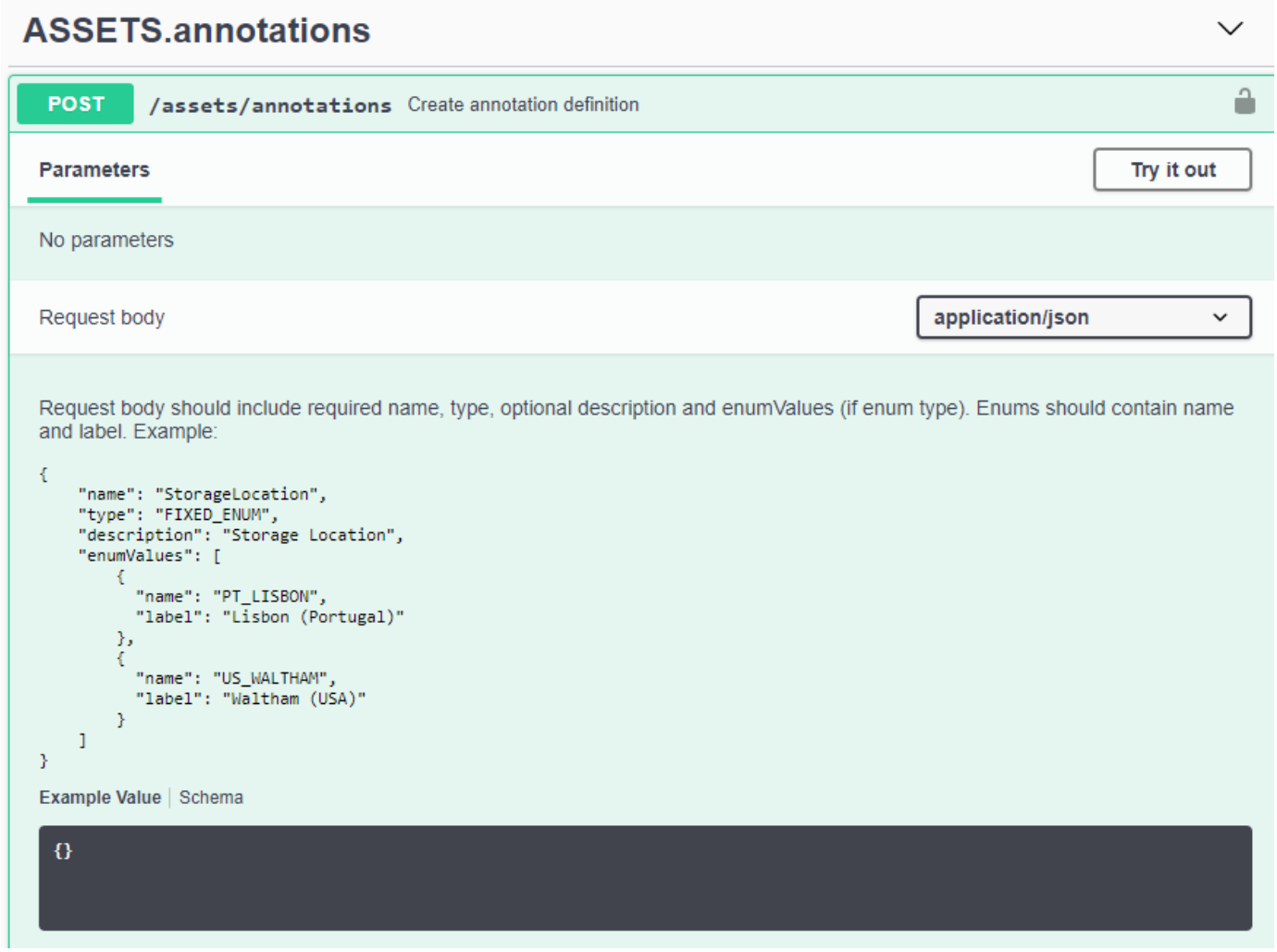
- Ein API-Zugriffstoken-Modell wird verwendet, um den Zugriff zu gewähren.
- Das API-Token-Management wird von Benutzern von Data Infrastructure Insights mit der Administratorrolle ausgeführt.

API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Data Infrastructure Insights anmelden und zu **Admin > API Access** navigieren. Klicken Sie auf den Link **API Documentation**.



Die API-Dokumentation ist Swagger-basiert, die eine kurze Beschreibung und Verwendungsinformationen für die API, und ermöglicht es Ihnen, es in Ihrer Umgebung zu testen. Abhängig von Ihrer Benutzerrolle und/oder Data Infrastructure Insights Edition können die für Sie verfügbaren API-Typen variieren.



API-Zugriffs-Tokens

Bevor Sie die Data Infrastructure Insights API verwenden können, müssen Sie mindestens ein **API Access Token** erstellen. Access Tokens werden für angegebene API-Typen verwendet und können Lese- und/oder Schreibberechtigungen gewähren. Sie können auch die Ablauffrist für jedes Access Token festlegen. Alle APIs unter den angegebenen Typen sind für das Access-Token gültig. Jedes Token ist ungültig für einen Benutzernamen oder ein Kennwort.

So erstellen Sie ein Access Token:

- Klicken Sie auf **Admin > API Access**
- Klicken Sie auf **+API Access Token**
  - Geben Sie Den Namen Des Tokens Ein
  - Wählen Sie API-Typen aus
  - Geben Sie die Berechtigungen an, die für diesen API-Zugriff gewährt wurden
  - Legen Sie Den Ablauf Des Tokens Fest

Ihr Token kann nur während des Erstellungsvorgangs in die Zwischenablage kopiert und gespeichert werden. Token können nicht abgerufen werden, nachdem sie erstellt wurden. Daher wird dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche **Copy API Access Token** zu klicken, bevor Sie den Bildschirm zur Tokenerstellung schließen können.

Sie können Token deaktivieren, aktivieren und widerrufen. Deaktivierte Token können aktiviert werden.

Tokens gewähren aus Kundensicht allgemeinen Zugang zu APIs; Management des Zugriffs auf APIs im Umfang ihres eigenen Mandanten. Kundenadministratoren können diese Token ohne direkte Beteiligung des Back-End-Personals von Data Infrastructure Insights gewähren und widerrufen.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Access Token dann als Berechtigung, wenn es die Ziel-API anruft. Das übergebene Token informiert die API, dass der Inhaber des Tokens berechtigt ist, auf die API zuzugreifen und bestimmte Aktionen durchzuführen, die vom Umfang festgelegt wurden, der während der Autorisierung gewährt wurde.

Der HTTP-Header, in dem das Access Token übergeben wird, ist **X-CloudInsights-ApiKey:**.

Verwenden Sie zum Abrufen von Lagerbeständen beispielsweise Folgendes:

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Wobei _<API_Access_Token>_ das Token ist, das Sie bei der Erstellung des
API-Zugriffs gespeichert haben.
```

Beispiele für die API, die Sie verwenden möchten, finden Sie auf den Seiten der Schwagger.

API-Typ

Die Data Infrastructure Insights API ist kategorienbasiert und enthält derzeit die folgenden Typen:

- DER ASSET-Typ enthält Asset-, Abfrage- und Such-APIs.
  - Assets: Listen Sie Objekte der obersten Ebene auf und rufen Sie ein bestimmtes Objekt oder eine Objekthierarchie ab.
  - Abfrage: Abrufen und Verwalten von Dateninfrastruktur Insights Abfragen.
  - Import: Importieren Sie Anmerkungen oder Anwendungen und weisen Sie sie Objekten zu
  - Suche: Suchen Sie ein bestimmtes Objekt, ohne die eindeutige ID oder den vollständigen Namen des Objekts zu kennen.
- DER DATENERFASSUNGSTYP dient zum Abrufen und Verwalten von Datensammlern.
- Mit DEM AUFNAHMERUNGSTYP können Aufnahmedaten und benutzerdefinierte Metriken abgerufen und gemanagt werden, beispielsweise von Telegraf-Agenten
- MITHILFE DER PROTOKOLLAUFNAHME werden Protokolldaten abgerufen und gemanagt

Weitere Typen und/oder APIs können im Laufe der Zeit verfügbar sein. Die neuesten API-Informationen finden Sie im "API-Swagger-Dokumentation".

Beachten Sie, dass die API-Typen, auf die ein Benutzer Zugriff "Benutzerrolle"hat, auch von den in den

einzelnen Funktionen von Data Infrastructure Insights (Monitoring, Workload Security, Reporting) vorhanden sind.

Inventurtraversal

In diesem Abschnitt wird beschrieben, wie eine Hierarchie von Data Infrastructure Insights Objekten durchlaufen wird.

Objekte Der Obersten Ebene

Einzelne Objekte werden in Anfragen durch eine eindeutige URL (in JSON als „selbst“ bezeichnet) identifiziert und erfordern Kenntnisse über Objekttyp und interne ID Für einige der Objekte der obersten Ebene (Hosts, Storage usw.) bietet DIE REST API Zugriff auf die vollständige Sammlung.

Das allgemeine Format einer API-URL lautet:

```
 https://<tenant>/rest/v1/<type>/<object>
Um beispielsweise alle Speicher von einem Mandanten mit dem Namen
_mysite.c01.cloudinsights.netapp.com_ abzurufen, lautet die Anfrage-URL:
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Kinder und verwandte Objekte

Objekte auf oberster Ebene, wie z. B. Speicherung, können für andere Kinder und verwandte Objekte verwendet werden. Zum Beispiel, um alle Datenträger für einen bestimmten Speicher abzurufen, verketten Sie die Speicher-URL „selbst“ mit „/Disks“, zum Beispiel:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Erweitert

Viele API-Befehle unterstützen den Parameter **Expand**, der zusätzliche Details zum Objekt oder URLs für verwandte Objekte enthält.

Der gemeinsame Expand-Parameter ist *Expands*. Die Antwort enthält eine Liste aller verfügbaren spezifischen Expands für das Objekt.

Beispiel: Wenn Sie Folgendes anfordern:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
Die API gibt alle verfügbaren Expands für das Objekt wie folgt zurück:
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resources"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

Jede Erweiterung enthält Daten, eine URL oder beides. Der Parameter Expand unterstützt mehrere und verschachtelte Attribute, z. B.:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Mit Expand lassen sich zahlreiche verwandte Daten in einer einzigen Lösung
integrieren. NetApp rät Ihnen, nicht zu viele Informationen gleichzeitig
anzufordern. Dies kann zu einer Verschlechterung der Performance führen.
```

Um dies zu entmutigen, können Anfragen nach Beständen der obersten Ebene nicht erweitert werden. Beispielsweise können Sie keine Expand-Daten für alle Speicherobjekte gleichzeitig anfordern. Die Clients müssen die Liste der Objekte abrufen und dann spezifische Objekte auswählen, die erweitert werden sollen.

Performance-Daten

Performancedaten werden über viele Geräte als separate Proben erfasst. Data Infrastructure Insights sammelt stündlich (standardmäßig) Performance-Proben und fasst sie zusammen.

Die API ermöglicht den Zugriff auf sowohl die Proben als auch auf die zusammengefassten Daten. Bei einem Objekt mit Performance-Daten ist eine Performance-Zusammenfassung als *Expand=Performance* verfügbar. Die Zeitreihen für den Leistungsverlauf sind über die verschachtelte_Expand=Performance.history_ verfügbar.

Beispiele für Performance-Datenobjekte:

- Storage Performance
- StoragePoolPerformance
- PortPerformance
- DiskPerformance

Eine Leistungsmetric hat eine Beschreibung und einen Typ und enthält eine Sammlung von Leistungsübersichten. Beispiel: Latenz, Datenverkehr und Rate.

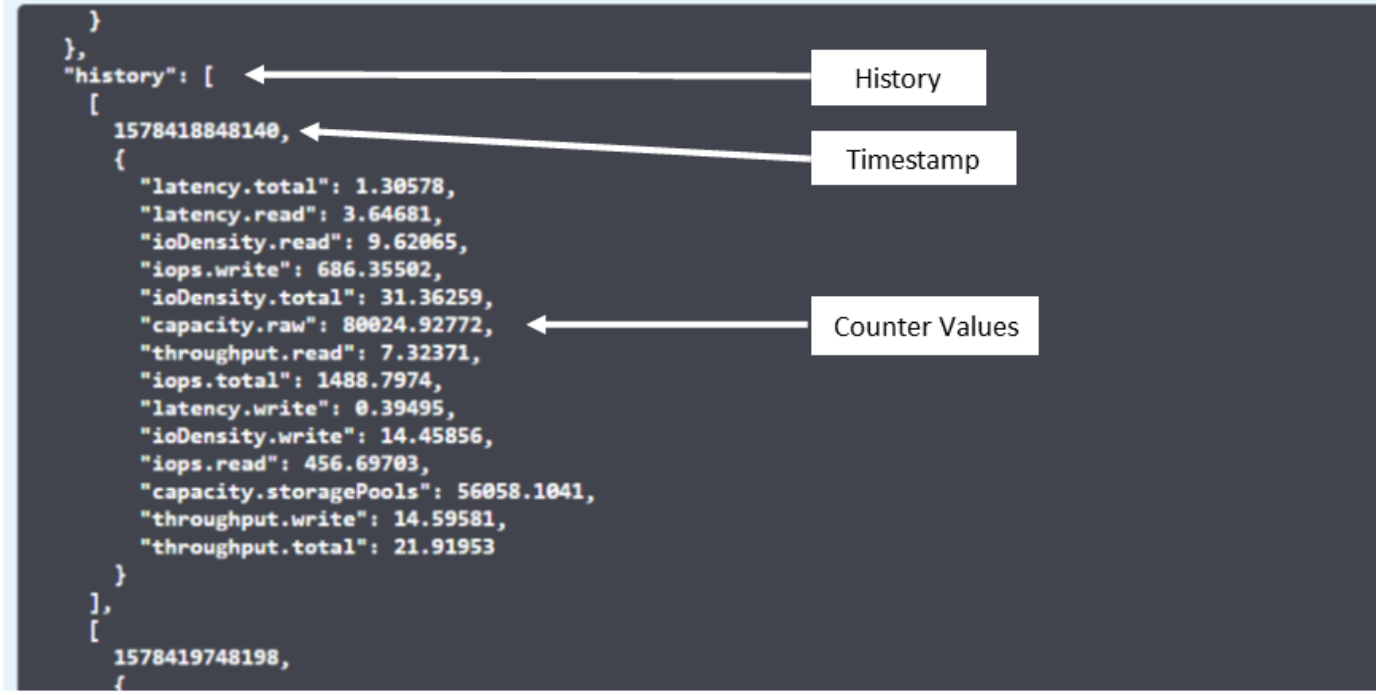
Eine Leistungsübersicht enthält eine Beschreibung, Einheit, Beispielstartzeit, Probenendzeit und eine Sammlung von zusammengefassten Werten (Strom, min, max, avg usw.), die aus einem einzelnen Leistungszähler über einen Zeitbereich (1 Stunde, 24 Stunden, 3 Tage usw.) berechnet werden.

https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body

Response body



Das resultierende Wörterbuch für Leistungsdaten enthält die folgenden Schlüssel:

- „Selbst“ ist die eindeutige URL des Objekts

- „History“ ist die Liste der Paare von Zeitstempel und Karte von Zählerwerten
- Jeder andere Wörterbuchschlüssel („diskThrughput“ usw.) ist der Name einer Leistungsmetrik.

Jeder Performance-Datenobjekttyp verfügt über einen eigenen Satz von Performance-Kennzahlen. Das Performance-Objekt der virtuellen Maschine unterstützt beispielsweise „diskThrughput“ als Leistungskennzahl. Jede unterstützte Leistungsmetrik ist eine bestimmte „performanceCategory“, die im metrischen Wörterbuch dargestellt wird. Data Infrastructure Insights unterstützt mehrere später in diesem Dokument aufgeführte Performance-Kenngrößen. Jedes Wörterbuch der Leistungsmetrik hat auch das Feld „Beschreibung“, das eine vom Menschen lesbare Beschreibung dieser Leistungsmetrik und eine Reihe von Zähleinträgen mit Leistungszusammenfassung ist.

Der Zähler der Leistungsübersicht ist die Zusammenfassung der Leistungsindikatoren. Er zeigt typische aggregierte Werte wie Min., Max. Und Avg für einen Zähler sowie den neuesten beobachteten Wert, den Zeitbereich für zusammengefasste Daten, den Einheitstyp für Zähler und die Schwellenwerte für Daten. Nur Schwellenwerte sind optional; die restlichen Attribute müssen angegeben werden.

Leistungsübersichten stehen für diese Zählertypen zur Verfügung:

- Lesen – Zusammenfassung für Lesevorgänge
- Write – Zusammenfassung für Schreibvorgänge
- Gesamt: Zusammenfassung für alle Operationen. Es kann höher sein als die einfache Summe von Lesen und Schreiben; es kann auch andere Operationen.
- Total Max – Zusammenfassung für alle Operationen. Dies ist der maximale Gesamtwert im angegebenen Zeitbereich.

Kennzahlen Für Die Objekt-Performance

Die API kann detaillierte Metriken für Objekte in Ihrer Umgebung zurückgeben, z. B.:

- Storage-Performance-Kennzahlen wie IOPS (Anzahl der ein-/Ausgabe-Anfragen pro Sekunde), Latenz oder Durchsatz.
- Kennzahlen zur Switch-Performance, z. B. Datenverkehrsnutzung, BB Credit Zero Daten oder Port-Fehler.

Siehe "API-Swagger-Dokumentation" Weitere Informationen zu Metriken für die einzelnen Objekttypen.

Performance-Verlaufsdaten

Verlaufsdaten werden in Leistungsdaten als Liste der Zeitstempel- und Zählermaps-Paare präsentiert.

Verlaufszähler werden basierend auf dem Objektnamen der Performance-Metrik benannt. Das Performance-Objekt der virtuellen Maschine unterstützt beispielsweise „diskThrughput“, so dass die Geschichtskarte Schlüssel mit den Namen „diskThrughput.read“, „diskThrughput.write“ und „diskThrughput.total“ enthält.

Zeitstempel befindet sich im UNIX-Zeitformat.

Dies ist ein Beispiel für einen Performance-Daten-JSON für eine Festplatte:

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


Objekte mit Kapazitätsattributen

Objekte mit Kapazitätsattributen verwenden grundlegende Datentypen und das kapazitätItem zur Darstellung.

KapazitätArtikel

KapazitätItem ist eine einzige logische Einheit der Kapazität. Er hat „Wert“ und „highThreshold“ in Einheiten, die durch sein übergeordnetes Objekt definiert sind. Zudem unterstützt es eine optionale Übersichtskarte, in der die Konstruktion des Kapazitätswerts erläutert wird. So wäre beispielsweise die Gesamtkapazität eines 100 TB StoragePool ein KapazitätItem mit einem Wert von 100. Die Aufschlüsselung kann 60 TB für „Daten“ und 40 TB für „Snapshots“ zugewiesen zeigen.

Hinweis

„HighThreshold“ stellt systemdefinierte Schwellenwerte für die entsprechenden Metriken dar, mit denen ein Kunde Alarme oder visuelle Hinweise auf Werte generieren kann, die außerhalb des zulässigen konfigurierten Messebereiches liegen.

Die folgende Anzeige zeigt die Kapazität von StoragePools mit mehreren Kapazitätszählern:

Suchen von Objekten mit Suchen

Die Such-API ist ein einfacher Einstiegspunkt zum System. Der einzige Eingabeparameter für die API ist eine freie Zeichenfolge, und der resultierende JSON enthält eine kategorisierte Liste der Ergebnisse. Typen sind verschiedene Asset-Typen aus dem Inventar, z. B. Speicher, Hosts, Datenspeicher usw. Jeder Typ würde eine Liste von Objekten des Typs enthalten, die den Suchkriterien entsprechen.

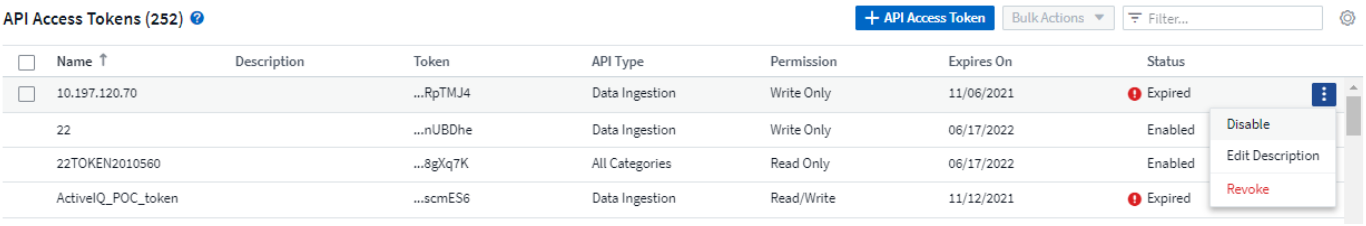
Data Infrastructure Insights ist eine erweiterbare (weit offene) Lösung, die die Integration in Orchestrierungs-, Business Management-, Change Control- und Ticketsysteme von Drittanbietern sowie benutzerdefinierte CMDB-Integrationen ermöglicht.

Die RESTful API von Cloud Insight ist ein primärer Integrationspunkt für eine einfache und effektive Datenverschiebung und ermöglicht Anwendern nahtlosen Zugriff auf ihre Daten.

Deaktivieren oder Deaktivieren eines API-Tokens

Um ein API-Token vorübergehend zu deaktivieren, klicken Sie auf der API-Token-Listenseite auf das Menü „drei Punkte“ für die API und wählen Sie *Disable*. Sie können das Token jederzeit über dasselbe Menü wieder aktivieren und *Enable* auswählen.

Um ein API-Token dauerhaft zu entfernen, wählen Sie im Menü die Option „Widerruf“. Sie können ein entzogen Token nicht erneut aktivieren; Sie müssen ein neues Token erstellen.



Token für abgelaufenen API-Zugriff werden gedreht

Die Token für den API-Zugriff haben ein Ablaufdatum. Wenn ein API-Zugriffstoken abläuft, müssen Benutzer ein neues Token generieren (vom Typ *Datenaufnahme* mit Lese-/Schreibberechtigungen) und Telegraf neu konfigurieren, um das neu generierte Token anstelle des abgelaufenen Tokens zu verwenden. In den folgenden Schritten wird die Vorgehensweise beschrieben.

Kubernetes

Beachten Sie, dass diese Befehle den Standard-Namespace „netapp-Monitoring“ verwenden. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Hinweis: Wenn Sie die neueste Installation von NetApp Kubernetes Monitoring Operator und ein erneuerbares API-Zugriffstoken verwenden, werden auslaufende Tokens automatisch durch neue/aktualisierte API-Zugriffs-Tokens ersetzt. Die unten aufgeführten manuellen Schritte müssen nicht ausgeführt werden.

- Bearbeiten Sie den NetApp Kubernetes Monitoring Operator.

```
 kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* Ändern Sie den Wert _spec.output-sink.API-key_ und ersetzen Sie das
alte API-Token durch das neue API-Token.
```

```
spec:
…
  output-sink:
  - api-key:<NEW_API_TOKEN>
```

RHEL/CentOS und Debian/Ubuntu

- Bearbeiten Sie die Telegraf-Konfigurationsdateien und ersetzen Sie alle Instanzen des alten API-Tokens durch das neue API-Token.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Telegraf Neu Starten.
```

```
sudo systemctl restart telegraf
```

Windows

- Ersetzen Sie für jede Telegraf-Konfigurationsdatei in *C:\Programme\telegraf\telegraf.d* alle Instanzen des alten API-Tokens durch das neue API-Token.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Telegraf Neu Starten.

```
Stop-Service telegraf
Start-Service telegraf
```

Monitoring Ihrer Umgebung

Prüfung

Um sowohl erwartete (für die Nachverfolgung) als auch unerwartete (für die Fehlerbehebung) Änderungen zu erkennen, können Sie einen Audit-Trail der Systemereignisse und Benutzeraktivitäten von Data Infrastructure Insights anzeigen.

Anzeigen Von Geprüften Ereignissen

Um die Seite „Audit“ anzuzeigen, klicken Sie im Menü auf **Admin > Audit**. Die Seite „Audit“ wird angezeigt und enthält die folgenden Details für jeden Audit-Eintrag:

- **Zeit** - Datum und Uhrzeit der Veranstaltung oder Aktivität
- **Benutzer** - der Benutzer, der die Aktivität initiiert hat
- **Rolle** - die Rolle des Benutzers in Data Infrastructure Insights (Gast, Benutzer, Administrator)
- **IP** - die IP-Adresse, die dem Ereignis zugeordnet ist
- **Aktion** - Art der Aktivität, z. B. Login, Erstellen, Aktualisieren
- **Kategorie** - die Kategorie der Aktivität
- **Details** - Details zur Aktivität

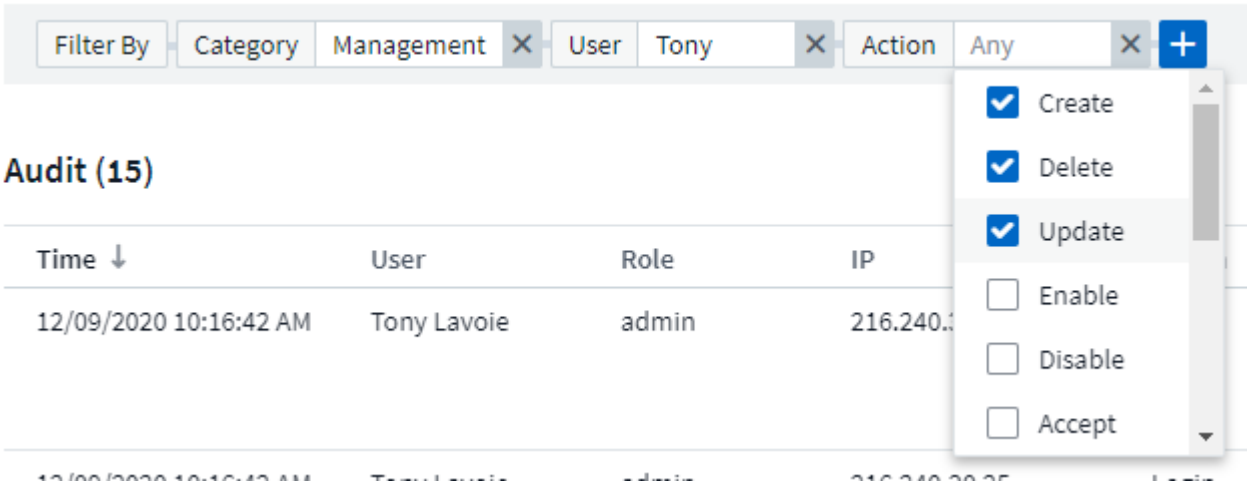
Anzeigen von Audit-Einträgen

Es gibt verschiedene Möglichkeiten, Audit-Einträge anzuzeigen:

- Sie können Audit-Einträge anzeigen, indem Sie einen bestimmten Zeitraum (1 Stunde, 24 Stunden, 3 Tage usw.) auswählen.
- Sie können die Sortierreihenfolge der Einträge entweder auf aufsteigend (nach-oben-Pfeil) oder absteigend (nach-unten-Pfeil) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken.

  Standardmäßig werden in der Tabelle die Einträge in absteigender Reihenfolge angezeigt.

- Mit den Filterfeldern können Sie nur die Einträge anzeigen, die in der Tabelle angezeigt werden sollen. Klicken Sie auf die Schaltfläche [+], um weitere Filter hinzuzufügen.



Mehr zum Filtern

Sie können einen der folgenden Optionen verwenden, um Ihren Filter zu verfeinern:

Filtern	Das macht es	Beispiel	Ergebnis
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	vol.	Gibt alle Ressourcen zurück, die mit „vol“ beginnen und mit „RHEL“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	BOS-PRD??-S12	Gibt BOS-PRD zurück***12_ -S12, BOS-PRD23_***-S12 und so weiter
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	FAS2240, CX600 ODER FAS3270	Gibt eine beliebige von FAS2440, CX600 oder FAS3270 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT EMC*	Liefert alles zurück, was nicht mit „EMC“ beginnt
Keine	Sucht in einem beliebigen Feld nach leer/Null/Keine	*Keine*	Gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist
Nicht *	Wie bei *None* oben, aber Sie können dieses Formular auch verwenden, um in *Text-only*-Feldern nach Null-Werten zu suchen	Nicht *	Gibt Ergebnisse zurück, bei denen das Zielfeld nicht leer ist.
„“	Sucht nach einer genauen Übereinstimmung	„NetApp*“	Liefert Ergebnisse mit der exakten Zeichenfolge *NetApp**

Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „*“ filtern, erhalten Sie Ergebnisse, die ein wortwörtlicher Stern sind; das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in doppelten Anführungszeichen eingeschlossen sind.

Geprüfte Ereignisse und Maßnahmen

Die von Data Infrastructure Insights geprüften Ereignisse und Aktionen lassen sich in die folgenden allgemeinen Bereiche einteilen:

- **Benutzerkonto**: Anmelden, Abmelden, Rollenänderung, etc

  Beispiel: *User **Tony Lavoie** angemeldet von **10.1.120.15**, User Agent **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, wie Gecko) Chrome/85.0.4183.121 Safari/537.36**, Login-Methode(en) **BlueXP Portal Login***

- **Erfassungseinheit**: Erstellen, löschen usw.

  Beispiel: *Acquisition Unit **AU-Boston-1** entfernt*.

- **Data Collector**: Hinzufügen, entfernen, ändern, verschieben/fortsetzen, Erfassungseinheit ändern, Start/Stopp usw.

  Beispiel: *Datasource **FlexPod Lab** entfernt, Anbieter **NetApp**, Modell **ONTAP Datenmanagement-Software**, ip **192.168.106.5***.

- **Anwendung**: Hinzufügen, Objekt zuweisen, entfernen, etc

  Beispiel: *Internes Volumen **ocisedev:t1appSVM01:t1appFlexVol01** zur Anwendung hinzugefügt **Test App***.

- **Anmerkung**: Hinzufügen, zuweisen, entfernen, Anmerkungsregeln Aktionen, Anmerkungswert ändert sich, Usw.

  Beispiel: *Anmerkungswert **Boston** wurde dem Anmerkungstyp **SalesOffice*** hinzugefügt.

- **Abfrage**: Hinzufügen, entfernen, etc

  Beispiel: *Query **TL Sales Query** wird hinzugefügt*.

- **Monitor**: Hinzufügen, entfernen, etc

  Beispiel: Monitor *Aggr Size - CI Alerts Notifications Dev* aktualisiert

- **Benachrichtigung**: E-Mail ändern, etc

  Beispiel: Empfänger *ci-Alerts-notifications-dl* erstellt

Audit-Ereignisse Werden Exportiert

Sie können die Ergebnisse Ihrer Audit-Anzeige in eine .CSV-Datei exportieren, mit der Sie die Daten analysieren oder in eine andere Anwendung importieren können.

Schritte

1. Legen Sie auf der Seite „Audit“ den gewünschten Zeitbereich und alle gewünschten Filter fest. Data Infrastructure Insights exportiert nur die Überwachungseinträge, die mit dem von Ihnen festgelegten Filter und Zeitbereich übereinstimmen.
2. Klicken Sie auf die Schaltfläche *Export* Rechts oben am Tisch.

Die angezeigten Audit-Ereignisse werden in eine .CSV-Datei mit maximal 10,000 Zeilen exportiert.

Aufbewahrung von Audit-Daten

Der Zeitraum, den Data Infrastructure Insights Audit-Daten aufbewahrt, basiert auf Ihrer Edition:

- Basic Edition: Audit-Daten werden 30 Tage lang aufbewahrt
- Standard- und Premium-Editionen: Audit-Daten werden für 1 Jahr plus 1 Tag aufbewahrt

Überwachungseinträge, die älter als die Aufbewahrungszeit sind, werden automatisch gelöscht. Es ist keine Benutzerinteraktion erforderlich.

Fehlerbehebung

Hier finden Sie Vorschläge zur Fehlerbehebung bei Audit-Problemen.

Problem:	Teste das:
Ich sehe die Meldungen von Audit, die mir sagen, dass ein Monitor exportiert wurde.	Der Export einer benutzerdefinierten Monitorkonfiguration wird von NetApp Technikern üblicherweise bei der Entwicklung und dem Testen neuer Funktionen verwendet. Wenn Sie diese Meldung nicht erwarten, sollten Sie die in der geprüften Aktion genannten Maßnahmen des Benutzers oder den Support des Kontakts untersuchen.

Active IQ

NetApp "Active IQ" Bietet NetApp Kunden eine Reihe von Visualisierungen, Analysen und anderen Support-Services für ihre Hardware- und Softwaresysteme. Die von Active IQ gemeldeten Daten können die Fehlerbehebung bei Systemproblemen verbessern und auch Einblicke in Optimierungs- und vorausschauende Analysen für Ihre Geräte bieten.

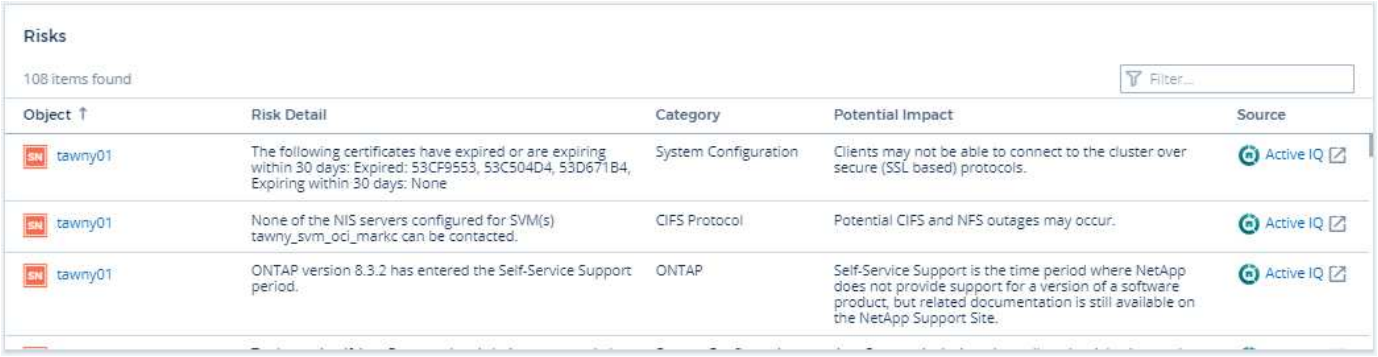
ActiveIQ ist in Data Infrastructure Insights Federal Edition nicht verfügbar.

Data Infrastructure Insights erfasst **Risiken** für jedes NetApp Clustered Data ONTAP Storage-System, das von Active IQ überwacht und gemeldet wird. Die für die Speichersysteme gemeldeten Risiken werden von Data Infrastructure Insights im Rahmen der Datenerfassung von diesen Geräten automatisch erfasst. Sie müssen den entsprechenden Datensammler zu Data Infrastructure Insights hinzufügen, um Active IQ-Risikoinformationen zu erfassen.

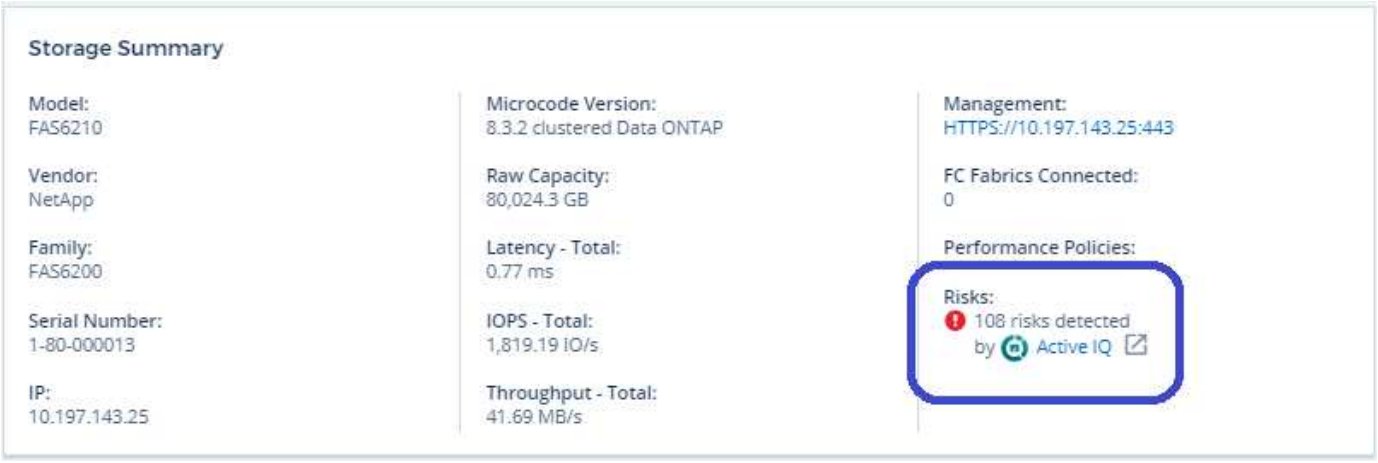
Die Einblicke in die Dateninfrastruktur zeigen keine Risikodaten für ONTAP Systeme an, die nicht von Active IQ überwacht und gemeldet werden.

Die gemeldeten Risiken werden in Data Infrastructure Insights auf den Landing Pages *Storage* und *Storage*

Node in der Tabelle „Risiken“ angezeigt. Die Tabelle enthält Risikodetails, Risikokategorie und potenzielle Auswirkungen des Risikos und einen Link zur Active IQ-Seite, die alle Risiken für den Storage-Node (Anmeldung für einen NetApp Support Account erforderlich) enthält.



Eine Anzahl der gemeldeten Risiken wird auch im Widget „Zusammenfassung“ der Landing Page angezeigt. Der Link führt zur entsprechenden Active IQ-Seite. Auf einer Landing Page „*Storage*“ stellt die Anzahl die Risiken aller zugrunde liegenden Storage Nodes dar.



Active IQ-Seite wird geöffnet

Wenn Sie auf den Link zu einer Active IQ-Seite klicken und Sie derzeit nicht bei Ihrem Active IQ-Konto angemeldet sind, müssen Sie die folgenden Schritte durchführen, um die Active IQ-Seite für den Storage-Node anzuzeigen.

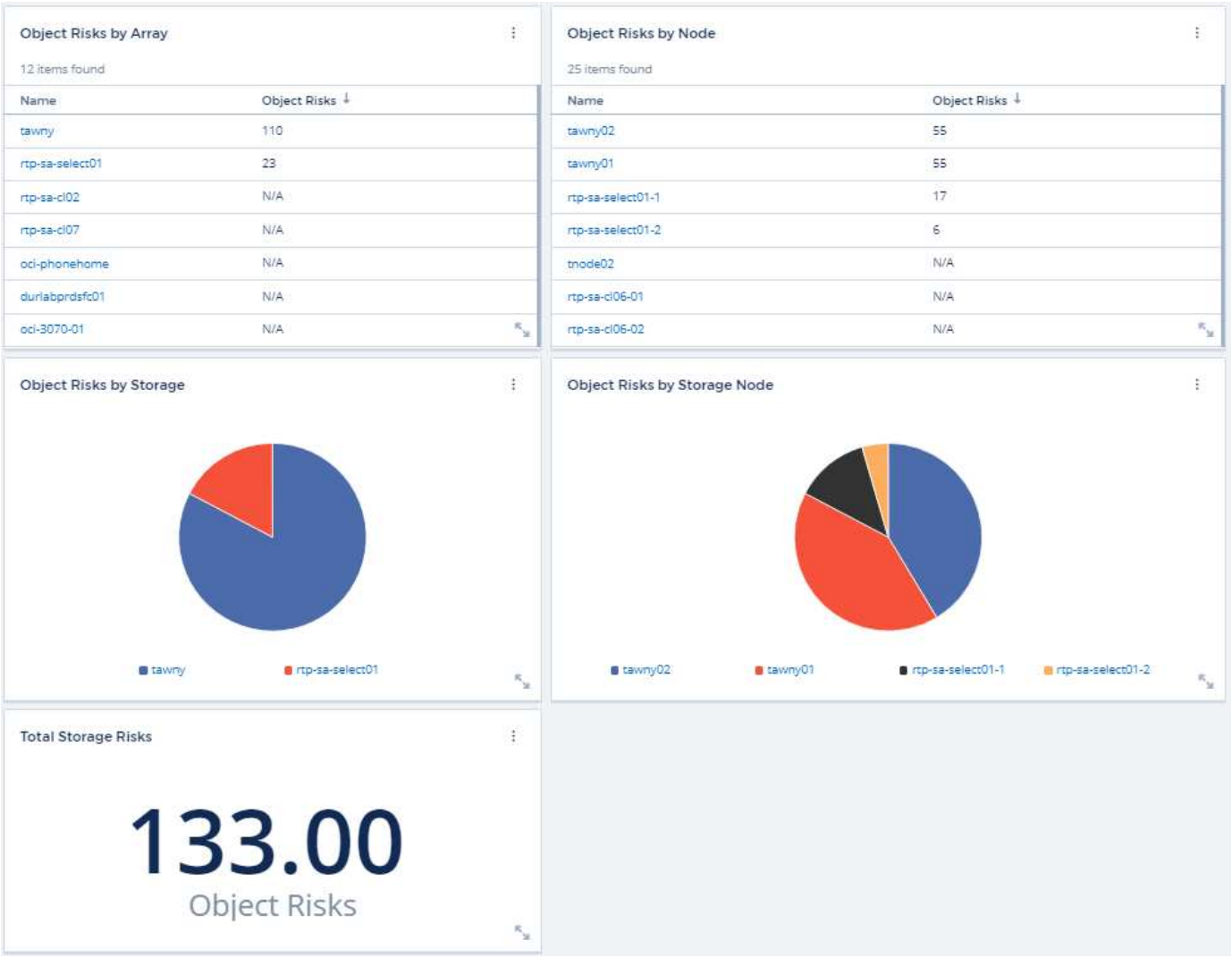
1. Klicken Sie im Widget „Data Infrastructure Insights Summary“ oder in der Risiketabelle auf den Link „Active IQ“.
2. Melden Sie sich bei Ihrem NetApp Support Konto an. Sie werden direkt zur Seite Storage-Node in Active IQ weitergeleitet.

Abfrage nach Risiken

In Data Infrastructure Insights können Sie die Spalte **Monitoring.count** einer Speicher- oder Speicher-Node-Abfrage hinzufügen. Wenn das zurückgegebene Ergebnis aus Active IQ-überwachten Storage-Systemen besteht, wird in der Spalte Monitoring.count die Anzahl der Risiken für das Storage-System oder den Node angezeigt.

Dashboards

Sie können Widgets erstellen (z. B. Kreisdiagramm, Tabelle-Widget, Balken, Spalte, Streudiagramm, Und Widgets mit einem Mehrwert) zur Visualisierung der Objektrisiken für Storage- und Storage-Nodes für von Active IQ überwachte NetApp Clustered Data ONTAP Systeme „Objektrisiken“ können in diesen Widgets als Spalte oder Metrik ausgewählt werden, wobei Storage oder Storage Node das Objekt des Fokus ist.



Workload-Sicherheit

Allgemeines Zur Storage Workload Security

Einblicke in die Dateninfrastruktur Storage Workload Security (ehemals Cloud Secure) schützt Ihre Daten durch verwertbare Informationen zu Bedrohungen von innen. Es ermöglicht eine zentrale Übersicht und Kontrolle über den Zugriff auf alle Unternehmensdaten in Hybrid-Cloud-Umgebungen, damit Sicherheits- und Compliance-Ziele erfüllt werden.

Workload Security ist in Data Infrastructure Insights Federal Edition nicht verfügbar.

Übersicht

Verschaffen Sie sich einen zentralen Überblick und kontrollieren Sie den Benutzerzugriff auf wichtige Unternehmensdaten, die lokal oder in der Cloud gespeichert sind.

Ersetzen Sie Tools und manuelle Prozesse, die nicht zeitgerecht und präzise Einblicke in Datenzugriff und -Kontrolle bieten. Workload Security wird auf einzigartige Weise in der Cloud und in lokalen Storage-Systemen ausgeführt, sodass Sie über schädliches Benutzerverhalten in Echtzeit benachrichtigt werden können.

Darstellt

Dank erweitertem Machine Learning und Anomalieerkennung werden Unternehmensdaten vor Missbrauch durch böswillige oder kompromittierte Benutzer geschützt.

Benachrichtigt Sie über erweitertes Machine Learning und Anomalieerkennung des Benutzerverhaltens bei ungewöhnlichen Datenzugriff.

Compliance

Durch Auditing von Benutzerzugriffen auf lokal oder in der Cloud gespeicherte wichtige Unternehmensdaten wird die unternehmensinterne Compliance gewahrt.

Erste Schritte

Erste Schritte mit Workload Security

Es müssen Konfigurationsaufgaben abgeschlossen werden, bevor Sie mit Workload Security beginnen können, um die Benutzeraktivitäten zu überwachen.

Das Workload Security-System verwendet einen Agenten, um Zugriffsdaten von Speichersystemen und Benutzerinformationen von Directory Services-Servern zu erfassen.

Sie müssen Folgendes konfigurieren, bevor Sie mit dem Erfassen von Daten beginnen können:

Aufgabe	Verwandte Informationen

Konfigurieren eines Agenten	"Anforderungen An Den Agenten" "Agent Hinzufügen" "**Video**: Agentenbereitstellung"
Konfigurieren Sie einen User Directory Connector	"Fügen Sie Den User Directory Connector Hinzu" "**Video**: Active Directory-Verbindung"
Konfigurieren Sie Datensammler	Klicken Sie Auf **Workload-Sicherheit > Collectors** Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt Data Collector Vendor Reference in der Dokumentation. "**Video**: ONTAP SVM Verbindung"
Erstellen Von Benutzerkonten	"Benutzerkonten Verwalten"
Fehlerbehebung	"**Video**: Fehlerbehebung"

Auch die Workload-Sicherheit lässt sich in andere Tools integrieren. Beispiel: "Siehe diesen Leitfaden" Bei der Integration mit Splunk:

Anforderungen An Security Agent Für Workloads

Unbedingt "Installieren Sie einen Agenten" Um Informationen von Ihren Datensammlern zu erhalten. Bevor Sie den Agent installieren, sollten Sie sicherstellen, dass Ihre Umgebung den Anforderungen an Betriebssystem, CPU, Arbeitsspeicher und Speicherplatz entspricht.

Komponente	Linux-Anforderungen Erfüllt
Betriebssystem	Computer mit einer lizenzierten Version von einer der folgenden Versionen: * CentOS 8 Stream (64-Bit), SELinux * openSUSE Leap 15.3 bis 15.5 (64-Bit) * Oracle Linux 8.6 bis 8.8, 9.1 bis 9.2 (64-Bit) * Red hat Enterprise Linux 8.6 bis 8.8, 9.1 bis 9.2 (64-Bit), SELinux * Rocky 9.2 (64 Bit), SELinux * SUSE Linux Enterprise Server 15 SP3 bis 15 SP3 (64 Bit) * Ubuntu 20.04 LTS und 22.04 LTS (64 Bit) auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen.
Befehle	Für die Installation ist „entpacken“ erforderlich. Darüber hinaus ist für die Installation, das Ausführen von Skripten und die Deinstallation der Befehl 'udo su –' erforderlich.
CPU	4 CPU-Kerne
Speicher	16 GB RAM

Komponente	Linux-Anforderungen Erfüllt
Verfügbarer Festplattenspeicher	Der Festplattenspeicher sollte folgendermaßen zugewiesen werden: /Opt/netapp 36 GB (mindestens 35 GB freier Speicherplatz nach der Dateisystemerstellung) Hinweis: Es wird empfohlen, etwas zusätzlichen Speicherplatz zuzuweisen, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass mindestens 35 GB freier Speicherplatz im Dateisystem vorhanden ist. Wenn /opt ein eingebrachter Ordner aus einem NAS-Speicher ist, stellen Sie sicher, dass lokale Benutzer Zugriff auf diesen Ordner haben. Agent oder Data Collector können nicht installiert werden, wenn lokale Benutzer nicht über die Berechtigung zu diesem Ordner verfügen. Siehe "Fehlerbehebung" Weitere Informationen finden Sie in diesem Abschnitt.
Netzwerk	100 Mbit/s bis 1 Gbit/s Ethernet-Verbindung, statische IP-Adresse, IP-Konnektivität zu allen Geräten und ein erforderlicher Port zur Workload Security-Instanz (80 oder 443).

Hinweis: Der Workload Security Agent kann auf demselben Rechner installiert werden wie eine Data Infrastructure Insights Erfassungseinheit und/oder ein Agent. Es ist jedoch eine Best Practice, diese in separaten Maschinen zu installieren. Wenn diese auf demselben Rechner installiert sind, weisen Sie den Festplattenspeicherplatz wie unten gezeigt zu:

Verfügbarer Festplattenspeicher	50-55 GB für Linux sollte auf diese Weise Speicherplatz zugewiesen werden: /Opt/netapp 25-30 GB /var/log/netapp 25 GB

Zusätzliche Empfehlungen

- Es wird dringend empfohlen, die Zeit auf dem ONTAP-System und dem Agent-Rechner mit **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Zugriffsregeln Für Das Cloud-Netzwerk

Für * US-basierte * -Sicherheitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01.cloudinsights.netapp.com <site_Name>.c01.cloudinsights.netapp.com <site_Name>.c02.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Für **Europa-basierte** Arbeitslastsicherheitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01-eu-1.cloudinsights.netapp.com <site_Name>.c01-eu-1.cloudinsights.netapp.com <site_Name>.c02-eu-1.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Für * APAC-basierte * -Arbeitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01-ap-1.cloudinsights.netapp.com <site_Name>.c01-ap-1.cloudinsights.netapp.com <site_Name>.c02-ap-1.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Netzwerkregeln

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPS/Start-tls)	Workload Security Agent	LDAP-Server-URL	Mit LDAP verbinden
TCP	443	Workload Security Agent	Cluster- oder SVM-Management-IP-Adresse (abhängig von der SVM-Collector-Konfiguration)	API-Kommunikation mit ONTAP
TCP	35000 - 55000	SVM-Daten-LIF-IP-Adressen	Workload Security Agent	Kommunikation von ONTAP zum Workload Security Agent für FPolicy-Ereignisse. Diese Ports müssen gegenüber dem Workload Security Agent geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich jeglicher Firewall auf dem Workload Security Agent selbst (falls vorhanden). BEACHTEN SIE, dass Sie nicht **all** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von ~100 Ports zu beginnen, und bei Bedarf zu erhöhen.
TCP	7	Workload Security Agent	SVM-Daten-LIF-IP-Adressen	Echo vom Agent zu SVM-Daten-LIFs
SSH	22	Workload Security Agent	Cluster-Management	Erforderlich für das Blockieren von CIFS/SMB-Benutzern.

Systemgröße

Siehe "Ereignisprüfung" Dokumentation für Informationen zur Größenanpassung

Installation Von Workload Security Agent

Workload Security (ehemals Cloud Secure) erfasst Daten zu Benutzeraktivitäten mithilfe eines oder mehrerer Agenten. Mitarbeiter stellen Verbindungen zu Geräten in Ihrer Umgebung her und erfassen Daten, die zur Analyse an die SaaS-Ebene für die Workload-Sicherheit gesendet werden. Siehe "Anforderungen An Den Agenten" So konfigurieren Sie eine Agent-VM:

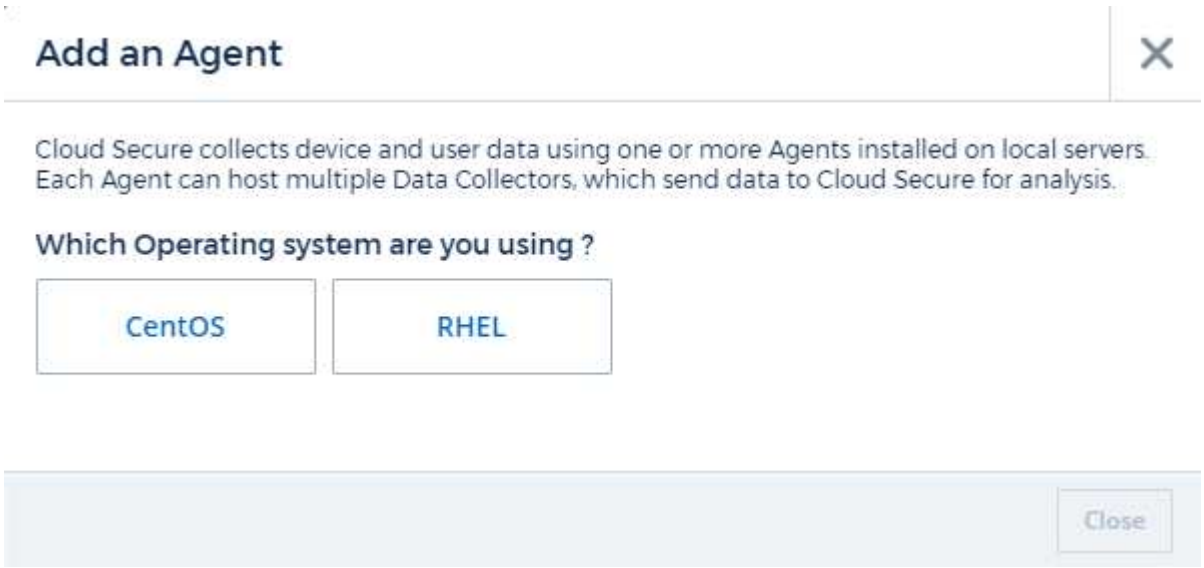
Bevor Sie Beginnen

- Die sudo-Berechtigung ist für die Installation, das Ausführen von Skripten und die Deinstallation erforderlich.
- Während der Installation des Agenten werden ein lokaler Benutzer *cssys* und eine lokale Gruppe *cssys* auf dem Computer erstellt. Wenn die Berechtigungseinstellungen die Erstellung eines lokalen Benutzers nicht zulassen und stattdessen Active Directory benötigen, muss im Active Directory-Server ein Benutzer mit dem Benutzernamen *csys* erstellt werden.
- Erfahren Sie mehr über Data Infrastructure Insights Security "Hier".

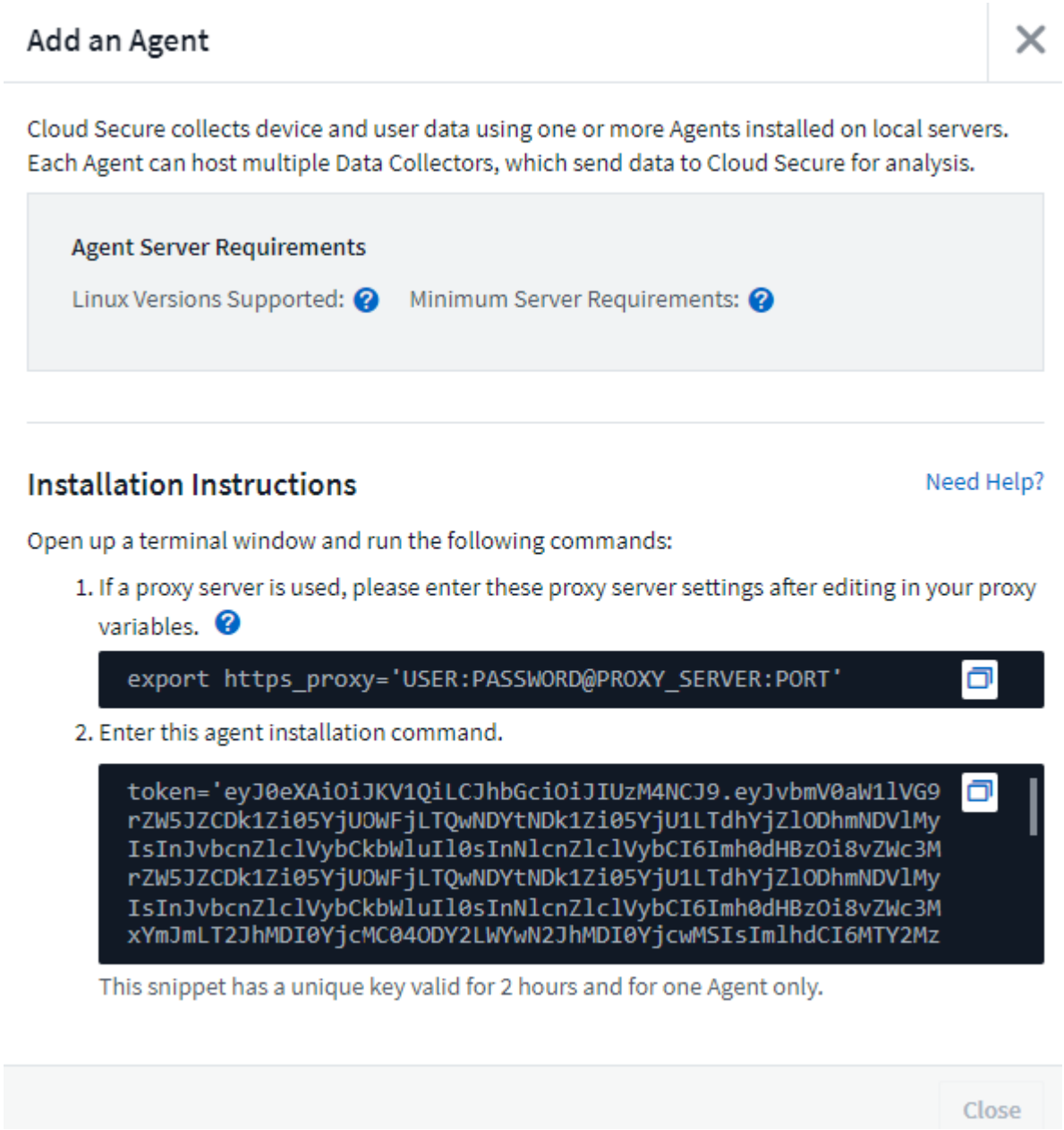
Schritte zum Installieren von Agent

1. Melden Sie sich als Administrator oder Account-Inhaber an Ihrer Workload Security-Umgebung an.
2. Wählen Sie **Collectors > Agenten > +Agent**

   Das System zeigt die Seite Agent hinzufügen an:



3. Vergewissern Sie sich, dass der Agent-Server die Mindestsystemanforderungen erfüllt.
4. Um zu überprüfen, ob auf dem Agent-Server eine unterstützte Version von Linux ausgeführt wird, klicken Sie auf *Version supported (i)*.
5. Wenn Ihr Netzwerk Proxy-Server verwendet, legen Sie die Proxy-Server-Details fest. Befolgen Sie dazu die Anweisungen im Proxy-Abschnitt.



6. Klicken Sie auf das Symbol in Zwischenablage kopieren, um den Installationsbefehl zu kopieren.
7. Führen Sie den Installationsbefehl in einem Terminalfenster aus.
8. Das System zeigt die folgende Meldung an, wenn die Installation erfolgreich abgeschlossen wurde:

Nach Dem Beenden

1. Sie müssen ein konfigurieren "Benutzerverzeichnissammler".
2. Sie müssen einen oder mehrere Data Collectors konfigurieren.

Netzwerkkonfiguration

Führen Sie auf dem lokalen System die folgenden Befehle aus, um Ports zu öffnen, die von Workload Security verwendet werden. Wenn ein Sicherheitsbedenken bezüglich des Portbereichs bestehen, können Sie einen kleineren Portbereich verwenden, z. B. *35000:35100*. Jede SVM verwendet zwei Ports.

Schritte

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Befolgen Sie die nächsten Schritte nach Ihrer Plattform:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Probenausgabe:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` (Für CentOS 8)

Probenausgabe:

```
35000-55000/tcp
```

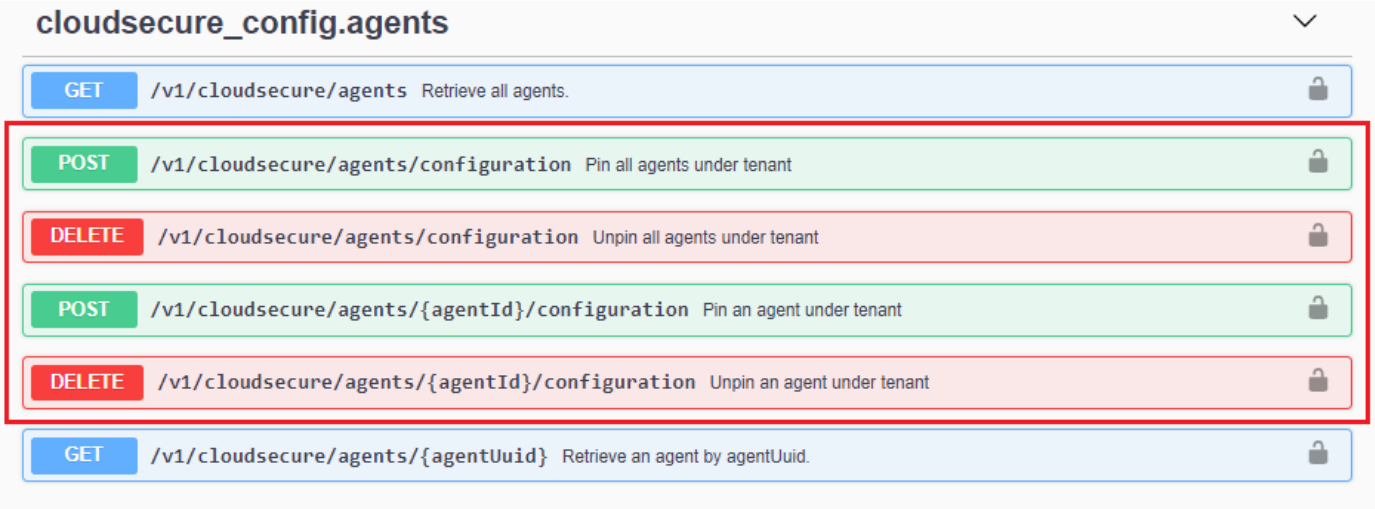
„Pinning“ an einen Agenten in der aktuellen Version

Standardmäßig aktualisiert Data Infrastructure Insights Workload Security die Agenten automatisch. Einige Kunden möchten die automatische Aktualisierung anhalten, sodass ein Agent die aktuelle Version verwendet, bis eine der folgenden Aktionen durchgeführt wird:

- Der Kunde nimmt die automatischen Agentenaktualisierungen wieder auf.
- 30 Tage sind vergangen. Beachten Sie, dass die 30 Tage am Tag der letzten Agentenaktualisierung beginnen, nicht an dem Tag, an dem der Agent angehalten wurde.

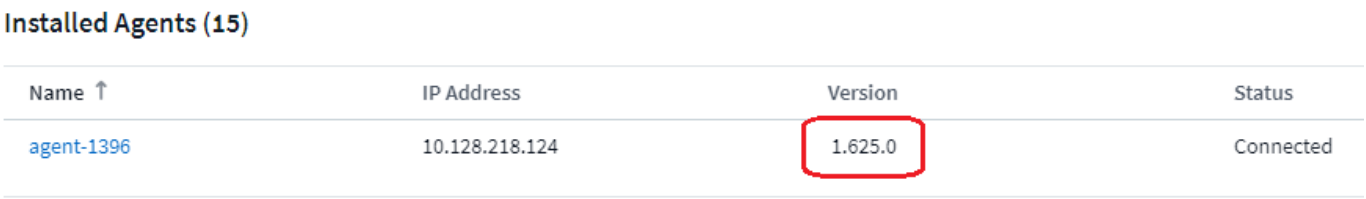
In jedem dieser Fälle wird der Agent bei der nächsten Aktualisierung der Workload-Sicherheit aktualisiert.

Um automatische Agentenaktualisierungen anzuhalten oder fortzusetzen, verwenden Sie die APIs *cloudSecure_config.Agents*:



Beachten Sie, dass es bis zu fünf Minuten dauern kann, bis die Aktion Pause oder Wiederaufnahme wirksam wird.

Sie können Ihre aktuellen Agentenversionen auf der Seite **Workload Security > Collectors** auf der Registerkarte **Agents** anzeigen.



Fehlerbehebung Bei Agentenfehlern

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

Problem:	Auflösung:
Bei der Installation des Agenten wird der Ordner /opt/netapp/cloudSecure/Agent/logs/agent.log nicht erstellt, und die Datei install.log enthält keine relevanten Informationen.	Dieser Fehler tritt beim Bootstrapping des Agenten auf. Der Fehler wird nicht in Protokolldateien protokolliert, da er vor der Initialisierung des Loggers auftritt. Der Fehler wird an die Standardausgabe umgeleitet und ist mit dem `journalctl -u cloudsecure-agent.service` Befehl im Service-Protokoll sichtbar. Dieser Befehl kann zur weiteren Problembehandlung verwendet werden. est
Agent-Installation schlägt fehl mit ‘Diese linux-Distribution wird nicht unterstützt. Beenden der Installation“.	Dieser Fehler wird angezeigt, wenn Sie versuchen, den Agent auf einem nicht unterstützten System zu installieren. Siehe "Anforderungen An Den Agenten".
Agent-Installation fehlgeschlagen mit dem Fehler "-bash: Unzip: Command not found"	Installieren Sie unzip und führen Sie dann den Installationsbefehl erneut aus. Wenn Yum auf dem Computer installiert ist, versuchen Sie „yum install unzip“, um unzip Software zu installieren. Danach kopieren Sie den Befehl von der Agent Installations-UI erneut, und fügen ihn in die CLI ein, um die Installation erneut auszuführen.

Problem:	Auflösung:

Agent wurde installiert und wurde ausgeführt. Der Agent ist jedoch plötzlich angehalten.	SSH an den Agent-Rechner. Überprüfen Sie den Status des Agent-Dienstes über `sudo systemctl status cloudsecure-agent.service`. 1. Überprüfen Sie, ob die Protokolle eine Meldung „Workload Security Daemon Service konnte nicht gestartet werden“ anzeigen. 2. Prüfen, ob csys-Benutzer in der Agent-Maschine vorhanden ist oder nicht. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus, und überprüfen Sie, ob der Benutzer und die Gruppe der csys vorhanden sind.
	`sudo id cssys`
	`sudo groups cssys`3. Wenn keine vorhanden ist, kann eine zentrale Überwachungsrichtlinie den csys-Benutzer gelöscht haben. 4. Erstellen Sie csys Benutzer und Gruppe manuell durch die Ausführung der folgenden Befehle.
	`sudo useradd cssys`
	`sudo groupadd cssys`5. Starten Sie danach den Agent-Service neu, indem Sie den folgenden Befehl ausführen:
	`sudo systemctl restart cloudsecure-agent.service`6. Wenn es noch nicht ausgeführt wird, überprüfen Sie bitte die anderen Fehlerbehebungsoptionen.

Es können nicht mehr als 50 Datensammler zu einem Agenten hinzugefügt werden.	Es können nur 50 Datensammler zu einem Agenten hinzugefügt werden. Dabei kann es sich um eine Kombination aller Collector-Typen, z. B. Active Directory, SVM und anderer Collectors handelt.
UI zeigt an, dass der Agent im Status „NOT_CONNECTED“ steht.	Schritte zum Neustart des Agenten. 1. SSH an den Agent-Rechner. 2. Starten Sie danach den Agent-Service neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service`3. Prüfen Sie den Status des Agent-Service über `sudo systemctl status cloudsecure-agent.service`. 4. Agent sollte in DEN ANGESCHLOSSENEN Zustand gehen.
Agent VM befindet sich hinter Zscaler Proxy und die Agent-Installation ist gescheitert. Wegen der SSL-Inspektion von Zscaler Proxy werden die Workload Security-Zertifikate präsentiert, da sie von Zscaler CA signiert ist, so dass der Agent die Kommunikation nicht anvertraut.	Deaktivieren Sie die SSL-Inspektion im Zscaler Proxy für die *.cloudinsights.netapp.com url. Wenn Zscaler die SSL-Prüfung übernimmt und die Zertifikate ersetzt, funktioniert Workload Security nicht.

Problem:	Auflösung:
Bei der Installation des Agenten bleibt die Installation nach dem Entpacken hängen.	Der Befehl „chmod 755 -RF“ schlägt fehl. Der Befehl schlägt fehl, wenn der Agent-Installationsbefehl von einem nicht-Root-Sudo-Benutzer ausgeführt wird, der Dateien im Arbeitsverzeichnis hat, die zu einem anderen Benutzer gehören, und die Berechtigungen dieser Dateien können nicht geändert werden. Wegen des fehlerhaften chmod-Befehls wird die restliche Installation nicht ausgeführt. 1. Erstellen Sie ein neues Verzeichnis namens „cloudSecure“. 2. Gehen Sie zu diesem Verzeichnis. 3. Kopieren Sie und fügen Sie die vollständige “Token=…… … ./cloudSecure-Agent-install.sh“-Installationsbefehl und drücken Sie die Eingabetaste. 4. Die Installation sollte fortgesetzt werden können.
Falls der Agent sich immer noch nicht mit Saas verbinden kann, öffnen Sie bitte einen Fall mit dem NetApp Support. Geben Sie die Seriennummer von Data Infrastructure Insights an, um einen Fall zu öffnen und Protokolle wie angegeben an den Fall anzuhängen.	Protokolle an den Fall anhängen: 1. Führen Sie das folgende Skript mit Root-Berechtigung aus und teilen Sie die Ausgabedatei (cloudSecure-Agent-symptoms.zip). a. /Opt/netapp/cloudSecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und teilen Sie die Ausgabe. a. id csys B. Gruppen cssys c. CAT /etc/os-Freigabe
Das Skript cloudsecure-agent-symptom-collector.sh schlägt mit folgendem Fehler fehl. [Root@Machine tmp]# /opt/netapp/cloudSecure/Agent/bin/cloudsecure-agent-symptom-collector.sh Service-Protokoll erfassen Erfassung von Anwendungsprotokollen Erfassung von Agent-Konfigurationen Aufnahme des Service-Status-Snapshots unter Verwendung von Agent-Verzeichnisstruktur-Snapshot …… . …… . /Opt/netapp/cloudSecure/Agent/bin/cloudSecure-Agent-Symptom-Collector.sh: Zeile 52: ZIP: Befehl nicht gefunden FEHLER: /Tmp/cloudsecure-agent-symptoms.zip konnte nicht erstellt werden	Zip-Werkzeug ist nicht installiert. Installieren Sie das Zip-Tool, indem Sie den Befehl „yum install zip“ ausführen. Führen Sie dann die cloudsecure-agent-symptom-collector.sh erneut aus.
Agent-Installation schlägt bei useradd fehl: Verzeichnis /Home/cssys kann nicht erstellt werden	Dieser Fehler kann auftreten, wenn das Login-Verzeichnis des Benutzers unter /Home nicht erstellt werden kann, da keine Berechtigungen vorhanden sind. Die Problemumgehung wäre, csys Benutzer zu erstellen und sein Login-Verzeichnis manuell mit dem folgenden Befehl hinzuzufügen: *Sudo useradd user_Name -m -d HOME_dir* -m :Erstellen Sie das Home-Verzeichnis des Benutzers, wenn es nicht existiert. -D : der neue Benutzer wird mit HOME_dir als Wert für das Login-Verzeichnis des Benutzers erstellt. Zum Beispiel, *sudo useradd cssys -m -d /cssys*, fügt einen Benutzer_cssys_ hinzu und erstellt sein Login-Verzeichnis unter root.

Problem:	Auflösung:
Agent wird nach der Installation nicht ausgeführt. *Systemctl Status cloudsecure-agent.service* zeigt Folgendes an: [Root@Demo ~]# systemctl Status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service loaded: Loaded (/usr/lib/systemd/System/cloudsecure-agent.service; enabled; Vendor Preset: Deabled: Disabled) Active: Actiting (Auto-restart) (Ergebnis: Exit-Code) since Di 2021-08-03 21:12 126:26 PDT; 2s ago Process: 25889 Start=/bin/bash /opt/Secure-Agent/cloudcode 25889 (Code=verlassen, Status=126), Aug 03 21:12:26 Demo-System[1]: cloudsecure-agent.service: Hauptprozess beendet, Code=verlassen, Status=126/n/a Aug 03 21:12:26 Demo-System[1]: Einheit cloudsecure-agent.service hat den Status fehlgeschlagen. Aug 03 21:12:26 Demo-System[1]: cloudsecure-agent.service fehlgeschlagen.	Dies kann fehlschlagen, da *csys*-Benutzer möglicherweise nicht über die Berechtigung zur Installation verfügt. Wenn /opt/netapp ein NFS-Mount ist und wenn der Benutzer *cssys* keinen Zugriff auf diesen Ordner hat, schlägt die Installation fehl. *Csys* ist ein lokaler Benutzer, der vom Workload Security Installer erstellt wurde und möglicherweise nicht über die Berechtigung zum Zugriff auf die gemountete Freigabe verfügt. Sie können dies überprüfen, indem Sie versuchen, über *cssys* user auf /opt/netapp/cloudSecure/Agent/bin/cloudSecure-Agent zuzugreifen. Wenn die „Berechtigung verweigert“ zurückgegeben wird, ist keine Installationsberechtigung vorhanden. Installieren Sie anstelle eines bereitgestellten Ordners in einem lokalen Verzeichnis auf dem Computer.
Der Agent wurde zunächst über einen Proxy-Server verbunden und während der Installation des Agenten wurde der Proxy festgelegt. Jetzt hat sich der Proxy-Server geändert. Wie kann die Proxy-Konfiguration des Agenten geändert werden?	Sie können die Datei agent.properties bearbeiten, um die Proxydetails hinzuzufügen. Führen Sie folgende Schritte aus: 1. Wechseln Sie in den Ordner mit der Eigenschaftendatei: cd /opt/netapp/cloudSecure/conf 2. Öffnen Sie die Datei *agent.properties* mit Ihrem bevorzugten Texteditor zum Bearbeiten. 3. Fügen Sie folgende Zeilen hinzu oder ändern Sie sie: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Speichern Sie die Datei. 5. Starten Sie den Agent: Sudo systemctl restart cloudsecure-agent.service

Löschen eines Workload Security Agent

Wenn Sie einen Workload Security Agent löschen, müssen alle dem Agent zugeordneten Datensammler zuerst gelöscht werden.

Löschen eines Agenten

Durch das Löschen eines Agenten werden alle dem Agenten zugeordneten Datensammler gelöscht. Wenn Sie die Datensammler mit einem anderen Agenten konfigurieren möchten, sollten Sie vor dem Löschen des Agenten ein Backup der Data Collector-Konfigurationen erstellen.

Bevor Sie beginnen

1. Stellen Sie sicher, dass alle mit dem Agenten verknüpften Datensammler aus dem Workload Security-Portal gelöscht werden.

   Hinweis: Ignorieren Sie diesen Schritt, wenn sich alle zugehörigen Kollektoren im STATUS „GESTOPPT“ befinden.

Schritte zum Löschen eines Agenten:

1. SSH in der Agent VM und führen Sie den folgenden Befehl aus. Wenn Sie dazu aufgefordert werden, geben Sie „y“ ein, um fortzufahren.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Klicken Sie Auf **Workload-Sicherheit > Collectors > Agents**

   Das System zeigt die Liste der konfigurierten Agenten an.

3. Klicken Sie auf das Optionsmenü für den Agenten, den Sie löschen möchten.
4. Klicken Sie Auf **Löschen**.

   Das System zeigt die Seite **Agent löschen** an.

5. Klicken Sie auf **Löschen**, um den Löschvorgang zu bestätigen.

Konfigurieren eines Active Directory (AD)-Benutzerverzeichnissammler

Workload Security kann so konfiguriert werden, dass Benutzerattribute von Active Directory-Servern erfasst werden.

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Account Owner sein, um diese Aufgabe ausführen zu können.
- Sie müssen über die IP-Adresse des Servers verfügen, der den Active Directory-Server hostet.
- Ein Agent muss konfiguriert werden, bevor Sie einen Benutzerverzeichnisanschluss konfigurieren.

Schritte zum Konfigurieren eines Benutzerverzeichnissammler

1. Klicken Sie im Menü Workload-Sicherheit auf:
   Collectors > User Directory Collectors > + User Directory Collector und wählen Sie **Active Directory**

   Das System zeigt den Bildschirm Benutzerverzeichnis hinzufügen an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

Name	Beschreibung
Name	Eindeutiger Name für das Benutzerverzeichnis. Beispiel: *GlobalADCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domain-Name	IP-Adresse oder Fully-Qualified Domain Name (FQDN) des Servers, der das Active Directory hostet

Waldname	Gesamtebene der Verzeichnisstruktur. Forest Name ermöglicht beide Formate: *X. y.y.z* ⇒ direkter Domainname, wie Sie ihn auf Ihrer SVM haben. [Beispiel: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ relative Distinguished Names [Beispiel: DC=hq,DC= commeryname,DC=com] oder Sie können wie folgt angeben: *OU=Engineering,DC=hq,DC= commeryname,DC=com* [nach spezifischer OU-Technik filtern] *CN=username,OU=Engineering,DC=comcompyname , DC=netapp, DC=com* [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu erhalten] _CN=Acrobat Nutzer,CN=Benutzer,DC=hq,DC=commeryname,DC= alle Benutzer innerhalb von Boston, die innerhalb der Organisation unterstützt werden.
DN binden	Benutzer erlaubt, das Verzeichnis zu durchsuchen. Beispiel: *username@companyname.com* oder *username@domainname.com* Darüber hinaus ist eine schreibgeschützte Domänenberechtigung erforderlich. Der Benutzer muss Mitglied der Sicherheitsgruppe *Read-Only Domain Controller* sein.
Kennwort BINDEN	Kennwort des Verzeichnisservers (d. h. Kennwort für in Bind DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-Start-tls
Ports	Wählen Sie Port

Geben Sie die folgenden Directory Server-erforderlichen Attribute ein, wenn die Standardattributnamen in Active Directory geändert wurden. Meistens werden diese Attributnamen in Active Directory geändert, in diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Merkmale	Attributname im Verzeichnisserver
Anzeigename	Name
SID	Objektsid
Benutzername	SAMAccountName

Klicken Sie auf Optionale Attribute einschließen, um eines der folgenden Attribute hinzuzufügen:

Merkmale	Attributname im Verzeichnisserver
E-Mail-Adresse	E-Mail
Telefonnummer	Telefonnummerierung
Rolle	Titel
Land	Co
Bundesland	Bundesland

Abteilung	Abteilung
Foto	Daumennagelfoto
ManagerDN	manager an
Gruppen	Mitgliedschafts

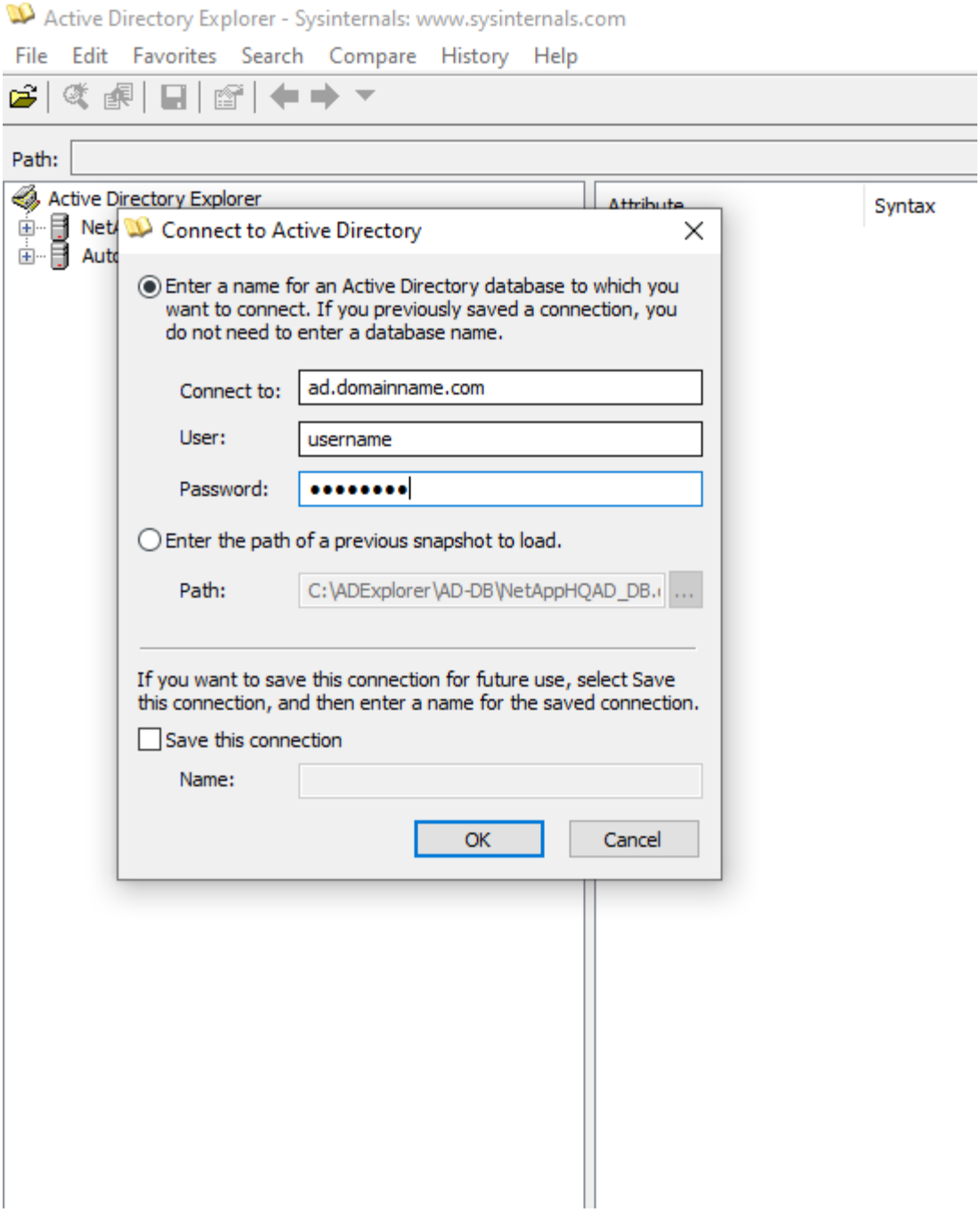
Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die Berechtigung für LDAP-Benutzer für die Workload-Sicherheit zu validieren:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Verwenden Sie AD Explorer, um in einer AD-Datenbank zu navigieren, Objekteigenschaften und -Attribute anzuzeigen, Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen, ausgefeilte Suchen auszuführen, die Sie speichern und erneut ausführen können.
  - Installieren "AD-Explorer" Auf jedem Windows-Rechner, der eine Verbindung zum AD-Server herstellen kann.
  - Stellen Sie eine Verbindung zum AD-Server mit dem Benutzernamen/Passwort des AD-Verzeichnisservers her.



Fehlerbehebung Bei Konfigurationsfehlern Des Benutzerverzeichnisses

In der folgenden Tabelle werden bekannte Probleme und Auflösungen beschrieben, die während der Kollektor-Konfiguration auftreten können:

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt, „ungültige Anmeldeinformationen für LDAP-Server bereitgestellt“.	Benutzername oder Passwort falsch angegeben. Bearbeiten und geben Sie den korrekten Benutzernamen und das richtige Passwort an.

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt: „Das Objekt, das DN=DC=hq,DC=Domainname,DC=com als Waldname angegeben hat, konnte nicht abgerufen werden.“	Falscher Waldname angegeben. Bearbeiten und geben Sie den richtigen Namen für die Gesamtstruktur an.
Die optionalen Attribute des Domänenbenutzers werden auf der Seite „Workload Security User Profile“ nicht angezeigt.	Dies ist wahrscheinlich auf eine Diskrepanz zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie die korrekten optionalen Attributnamen an.
Datensammler im Fehlerzustand mit „LDAP-Benutzer konnten nicht abgerufen werden. Grund für Fehler: Verbindung auf dem Server nicht möglich, Verbindung ist Null“	Starten Sie den Kollektor neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’.	Stellen Sie sicher, dass Sie für die erforderlichen Felder gültige Werte angegeben haben (Server, Forest-Name, BIND-DN, BIND-Password). Vergewissern Sie sich, dass die Eingabe von BIND-DN immer als ‘Administrator@<Domain_Forest_Name>’ oder als Benutzerkonto mit Administratorrechten für die Domäne angegeben wird.
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum ‘reVERSUCH’ Status. Zeigt den Fehler „kann den Status des Collectors nicht definieren,Grund TCP Befehl [Connect(localhost:35012,None,List(),some(,seconds),true)] fehlgeschlagen, weil java.net.ConnectionException:Connection abgelehnt wurde.“	Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN.
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt: „LDAP-Verbindung konnte nicht hergestellt werden“.	Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN.
Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt, “die Einstellungen konnten nicht geladen werden. Grund: Datasource Configuration hat einen Fehler. Spezifischer Grund: /Connector/conf/Application.conf: 70: ldap.ldap-Port hat type STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den AD-Server zu verwenden.
Ich begann mit den obligatorischen Attributen, und es funktionierte. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies ist wahrscheinlich auf eine Diskrepanz zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie den korrekten obligatorischen oder optionalen Attributnamen an.

Problem:	Auflösung:
Wann erfolgt nach dem Neustart des Collectors die AD-Synchronisierung?	DIE ANZEIGENSYNCHRONISATION erfolgt sofort nach dem Neustart des Collectors. Es dauert etwa 15 Minuten, bis Benutzerdaten von etwa 300.000 Benutzern abgerufen wurden. Und wird automatisch alle 12 Stunden aktualisiert.
Benutzerdaten werden von AD zu CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang aufbewahrt, wenn keine Aktualisierung erfolgt. Wenn der Mandant gelöscht wird, werden die Daten gelöscht.
Der Benutzerverzeichnisanschluss hat den Status ‘Fehler’. „Der Stecker befindet sich im Fehlerzustand. Dienstname: UsersLdap. Grund für Fehler: Abrufen von LDAP-Benutzern fehlgeschlagen. Grund für Fehlschlag: 80090308: LdapErr: DSID-0C090453, Kommentar: ACkeptSecurityContext error, Data 52e, v3839“	Falscher Waldname angegeben. Siehe oben, wie Sie den richtigen Namen für die Gesamtstruktur angeben.
Die Telefonnummer wird nicht auf der Benutzerprofilseite ausgefüllt.	Dies ist wahrscheinlich auf ein Problem bei der Attributzuordnung mit dem Active Directory zurückzuführen. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Informationen des Benutzers aus Active Directory abrufen wird. 2. Hinweis unter optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut ‘Telefonnummernnummer’ zugeordnet ist. 4. Verwenden Sie jetzt das Active Directory Explorer-Tool wie oben beschrieben, um das Active Directory zu durchsuchen und den korrekten Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass in Active Directory ein Attribut namens ‘Telefonnummernnummer’, das in der Tat die Telefonnummer des Benutzers hat, vorhanden ist. 5. Sagen wir ‘Active Directory, dass es in „Phonenumber“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich ‘Telefonnummerierung’ durch ‘Phonenumber’. 7. Speichern Sie den Active Directory-Collector, wird der Sammler neu starten und erhalten die Telefonnummer des Benutzers und die gleiche in der Benutzerprofil Seite.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Serververschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurde, wird es dort für 13 Monate sein. Wenn der AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Um erneut abzurufen, muss der Benutzer-Verzeichnis-Collector mit AD verbunden sein.

Problem:	Auflösung:
Daten aus Active Directory sind in CloudInsights Security vorhanden. Alle Benutzerinformationen von CloudInsights löschen möchten.	Active Directory-Benutzerinformationen können nicht NUR von CloudInsights Security gelöscht werden. Um den Benutzer zu löschen, muss der gesamte Mandant gelöscht werden.

Konfigurieren eines LDAP Directory Server Collectors

Sie konfigurieren die Workload Security so, dass Benutzerattribute von LDAP Directory-Servern erfasst werden.

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Account Owner sein, um diese Aufgabe ausführen zu können.
- Sie müssen über die IP-Adresse des Servers verfügen, der den LDAP-Directory-Server hostet.
- Ein Agent muss konfiguriert werden, bevor Sie einen LDAP-Directory-Konnektor konfigurieren.

Schritte zum Konfigurieren eines Benutzerverzeichnissammler

1. Klicken Sie im Menü Workload-Sicherheit auf:
   Collectors > User Directory Collectors > + User Directory Collector und wählen Sie **LDAP Directory Server**

   Das System zeigt den Bildschirm Benutzerverzeichnis hinzufügen an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

Name	Beschreibung
Name	Eindeutiger Name für das Benutzerverzeichnis. Beispiel: *GlobalLDAPCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domain-Name	IP-Adresse oder vollqualifizierter Domain-Name (FQDN) des Servers, der den LDAP-Verzeichnisserver hostet

Suchbasis	Search Base des LDAP-Servers Search Base ermöglicht die beiden folgenden Formate: *X. y.y.z* ⇒ Direkter Domänenname, wie Sie ihn auf Ihrer SVM haben. [Beispiel: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ relative Distinguished Names [Beispiel: DC=hq,DC= commeryname,DC=com] oder Sie können wie folgt angeben: *OU=Engineering,DC=hq,DC= commeryname,DC=com* [nach spezifischer OU-Technik filtern] *CN=username,OU=Engineering,DC=comcompyname , DC=netapp, DC=com* [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu bekommen] _CN=Acrobat Nutzer,CN=Benutzer,DC=hq,DC=commeryname,DC= alle Benutzer innerhalb der Organisation zu bekommen, die innerhalb von Boston, C=S=e,
DN binden	Benutzer erlaubt, das Verzeichnis zu durchsuchen. Beispiel: uid=ldapuser,cn=users,cn=Accounts,dc=Domain,dc=companyname,dc=com uid=john,cn=Users,cn=Accounts,dc=dorp,dc=company,dc=com für einen Benutzer john@dorp.company.com. dorp.company.com
--Konten	--user
--john	--anna
Kennwort BINDEN	Kennwort des Verzeichnisservers (d. h. Kennwort für in Bind DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-Start-tls
Ports	Wählen Sie Port

Geben Sie die folgenden Directory Server-erforderlichen Attribute ein, wenn die Standardattributnamen im LDAP Directory-Server geändert wurden. Meistens werden diese Attributnamen in LDAP Directory Server geändert, in diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Merkmale	Attributname im Verzeichnisserver
Anzeigename	Name
UNIXID	Nummer der Uidnummer
Benutzername	uid

Klicken Sie auf Optionale Attribute einschließen, um eines der folgenden Attribute hinzuzufügen:

Merkmale	Attributname im Verzeichnisserver
E-Mail-Adresse	E-Mail
Telefonnummer	Telefonnummerierung
Rolle	Titel

Land	Co
Bundesland	Bundesland
Abteilung	Abteilnummer
Foto	Foto
ManagerDN	manager an
Gruppen	Mitgliedschafts

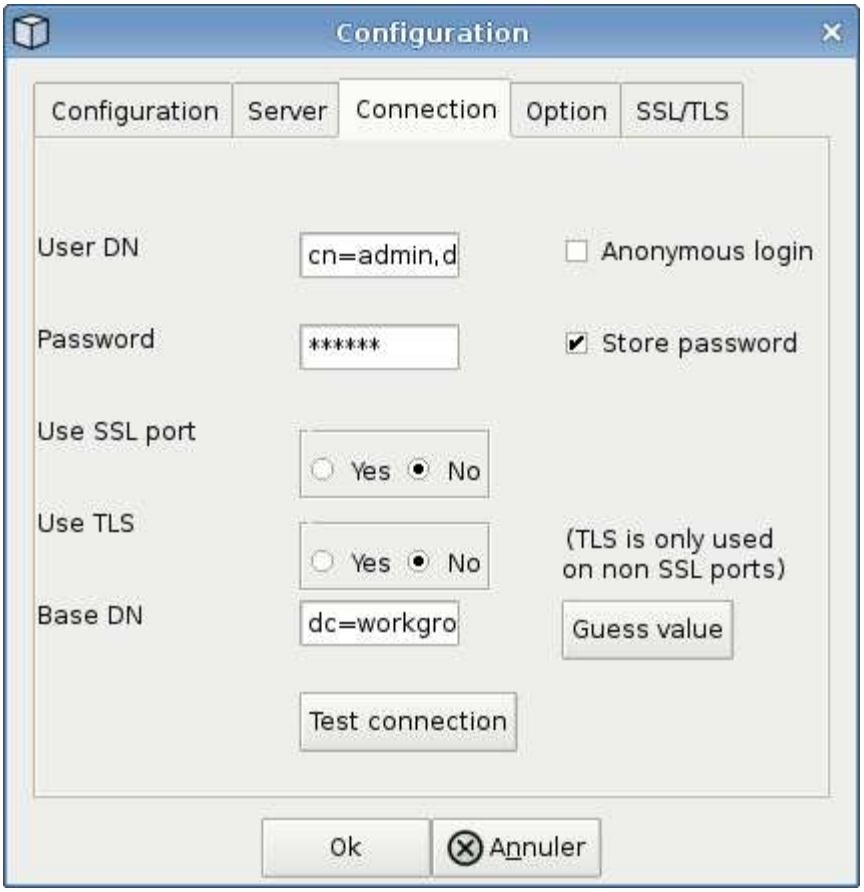
Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die Berechtigung für LDAP-Benutzer für die Workload-Sicherheit zu validieren:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Verwenden Sie den LDAP Explorer, um in einer LDAP-Datenbank zu
navigieren, Objekteigenschaften und -Attribute anzuzeigen,
Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen und
komplexe Suchen auszuführen, die Sie speichern und erneut ausführen
können.
```

  - Installieren Sie den LDAP Explorer Oder Java LDAP Explorer Auf jedem Windows-Rechner, der eine Verbindung zum LDAP-Server herstellen kann.
  - Stellen Sie eine Verbindung mit dem LDAP-Server unter Verwendung des Benutzernamens/Kennworts des LDAP-Verzeichnisservers her.



Fehlerbehebung bei LDAP Directory Collector-Konfigurationsfehlern

In der folgenden Tabelle werden bekannte Probleme und Auflösungen beschrieben, die während der Kollektor-Konfiguration auftreten können:

Problem:	Auflösung:
Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status 'Fehler'. Fehler sagt, „ungültige Anmeldeinformationen für LDAP-Server bereitgestellt".	Falscher Bind-DN oder Bind-Kennwort oder die Suchbasis angegeben. Bearbeiten Sie die richtigen Informationen, und geben Sie sie an.
Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status 'Fehler'. Fehler sagt: „Das Objekt, das DN=DC=hq,DC=Domainname,DC=com als Waldname angegeben hat, konnte nicht abgerufen werden."	Falsche Suchbasis angegeben. Bearbeiten und geben Sie den richtigen Namen für die Gesamtstruktur an.
Die optionalen Attribute des Domänenbenutzers werden auf der Seite „Workload Security User Profile" nicht angezeigt.	Dies ist wahrscheinlich auf eine Diskrepanz zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bei Feldern wird die Groß-/Kleinschreibung beachtet. Bearbeiten und geben Sie die korrekten optionalen Attributnamen an.

Problem:	Auflösung:
Datensammler im Fehlerzustand mit „LDAP-Benutzer konnten nicht abgerufen werden. Grund für Fehler: Verbindung auf dem Server nicht möglich, Verbindung ist Null“	Starten Sie den Kollektor neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’.	Stellen Sie sicher, dass Sie für die erforderlichen Felder gültige Werte angegeben haben (Server, Forest-Name, BIND-DN, BIND-Password). Stellen Sie sicher, dass die Eingabe von Bind-DN immer als uid=ldapuser,cn=users,cn=Accounts,dc=Domain,dc=commeryname,dc=com angegeben ist.
Das Hinzufügen eines LDAP-Directory-Connectors führt zum ‘reVERSUCH’-Status. Zeigt Fehler „Fehler bei der Ermittlung des Zustands des Kollektors und damit erneuter Versuch“ an.	Stellen Sie sicher, dass die Server-IP und die Search Base korrekt sind ///
Beim Hinzufügen des LDAP-Verzeichnisses wird der folgende Fehler angezeigt: „Fehler bei der Ermittlung des Zustands des Collectors innerhalb von 2 Wiederholungen, versuchen Sie erneut, den Collector neu zu starten (Fehlercode: AGENT008)“	Stellen Sie sicher, dass die Server-IP-Adresse und die Suchbasis korrekt sind
Das Hinzufügen eines LDAP-Directory-Connectors führt zum ‘reVERSUCH’-Status. Zeigt den Fehler „kann den Status des Collectors nicht definieren,Grund TCP Befehl [Connect(localhost:35012,None,List(),some(,seconds),true)] fehlgeschlagen, weil java.net.ConnectionException:Connection abgelehnt wurde.“	Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. ////
Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt: „LDAP-Verbindung konnte nicht hergestellt werden“.	Für den LDAP-Server wurde eine falsche IP oder ein falscher FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. Oder falscher Wert für den angegebenen Port. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den LDAP-Server zu verwenden.
Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt, “die Einstellungen konnten nicht geladen werden. Grund: Datasource Configuration hat einen Fehler. Spezifischer Grund: /Connector/conf/Application.conf: 70: ldap.ldap-Port hat type STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den AD-Server zu verwenden.
Ich begann mit den obligatorischen Attributen, und es funktionierte. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies ist wahrscheinlich auf eine Diskrepanz zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie den korrekten obligatorischen oder optionalen Attributnamen an.

Problem:	Auflösung:
Wann erfolgt die LDAP-Synchronisierung nach dem Neustart des Collectors?	Die LDAP-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Es dauert etwa 15 Minuten, bis Benutzerdaten von etwa 300.000 Benutzern abgerufen wurden. Und wird automatisch alle 12 Stunden aktualisiert.
Benutzerdaten werden von LDAP zu CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang aufbewahrt, wenn keine Aktualisierung erfolgt. Wenn der Mandant gelöscht wird, werden die Daten gelöscht.
Der LDAP-Directory-Konnektor führt zum 'Fehler'-Status. „Der Stecker befindet sich im Fehlerzustand. Dienstname: UsersLdap. Grund für Fehler: Abrufen von LDAP-Benutzern fehlgeschlagen. Grund für Fehlschlag: 80090308: LdapErr: DSID-0C090453, Kommentar: ACkeptSecurityContext error, Data 52e, v3839“	Falscher Waldname angegeben. Siehe oben, wie Sie den richtigen Namen für die Gesamtstruktur angeben.
Die Telefonnummer wird nicht auf der Benutzerprofilseite ausgefüllt.	Dies ist wahrscheinlich auf ein Problem bei der Attributzuordnung mit dem Active Directory zurückzuführen. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Informationen des Benutzers aus Active Directory abrufen wird. 2. Hinweis unter optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut 'Telefonnummernnummer' zugeordnet ist. 4. Verwenden Sie jetzt das Active Directory Explorer-Tool wie oben beschrieben, um den LDAP Directory-Server zu durchsuchen und den korrekten Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass im LDAP-Verzeichnis ein Attribut namens 'Telefonnummernnummer' vorhanden ist, das tatsächlich die Telefonnummer des Benutzers hat. 5. Sagen wir 'LDAP-Verzeichnis, dass es in „Phonenumber“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich 'Telefonnummerierung' durch 'Phonenumber'. 7. Speichern Sie den Active Directory-Collector, wird der Sammler neu starten und erhalten die Telefonnummer des Benutzers und die gleiche in der Benutzerprofil Seite.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Serververschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurde, wird es dort für 13 Monate sein. Wenn der AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Um wieder abrufen zu können, muss der Benutzer-Verzeichnis-Collector mit AD verbunden sein.

Konfiguration des ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen.

Bevor Sie beginnen

- Dieser Datensammler wird unterstützt durch:
  - Data ONTAP 9.2 und höher. Verwenden Sie für die beste Performance eine Data ONTAP-Version über 9.13.1.
  - SMB-Protokollversion 3.1 und früher.
  - NFS-Versionen bis einschließlich NFS 4.1 mit ONTAP 9.15.1 oder höher
  - FlexGroup wird von ONTAP 9.4 und höheren Versionen unterstützt
  - ONTAP Select wird unterstützt
- Es werden nur SVMs vom Datentyp unterstützt. SVMs mit Infinite Volumes werden nicht unterstützt.
- SVM hat mehrere Untertypen. Davon werden nur *default*, *Sync_source* und *Sync_Destination* unterstützt.
- Ein Agent "Muss konfiguriert sein" Bevor Sie Datensammler konfigurieren können.
- Stellen Sie sicher, dass Sie über einen richtig konfigurierten User Directory Connector verfügen, sonst werden bei Ereignissen kodierte Benutzernamen und nicht der tatsächliche Name des Benutzers (wie in Active Directory gespeichert) auf der Seite „Activity Forensics“ angezeigt.
- • ONTAP persistenter Speicher wird von 9.14.1 unterstützt.
- Um eine optimale Performance zu erzielen, sollten Sie den FPolicy-Server so konfigurieren, dass er sich im gleichen Subnetz wie das Storage-System befindet.
- Sie müssen eine SVM mit einer der folgenden beiden Methoden hinzufügen:
  - Mit Cluster-IP, SVM-Name und Cluster-Management-Benutzername und -Passwort. ***Dies ist die empfohlene Methode.***
    - Der SVM-Name muss exakt wie in ONTAP angegeben sein und bei Groß-/Kleinschreibung beachtet werden.
  - Mit SVM Vserver Management IP, Benutzername und Passwort
  - Wenn Sie den vollständigen Administrator-Benutzernamen und -Kennwort für Cluster-/SVM-Management nicht verwenden können oder nicht bereit sind, können Sie einen benutzerdefinierten Benutzer mit geringeren Berechtigungen erstellen, wie im erwähnt „Ein Hinweis über Berechtigungen“ Abschnitt unten. Dieser benutzerdefinierte Benutzer kann für einen SVM- oder Cluster-Zugriff erstellt werden.
    - o Sie können auch einen AD-Benutzer mit einer Rolle verwenden, die mindestens die Berechtigungen von csrolle hat, wie im Abschnitt „Hinweis auf Berechtigungen“ unten erwähnt. Weitere Informationen finden Sie im "ONTAP-Dokumentation".
- Stellen Sie sicher, dass die korrekten Applikationen für die SVM festgelegt sind, indem Sie den folgenden Befehl ausführen:

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

Beispielausgabe:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name            Application Method        Role Name        Locked Method
--------------- ----------- ------------- ---------------- ------ --------------
vsadmin         http        password      vsadmin          no     none
vsadmin         ontapi      password      vsadmin          no     none
vsadmin         ssh         password      vsadmin          no     none
3 entries were displayed.
```

- Stellen Sie sicher, dass für die SVM ein konfigurierter CIFS-Server ist: Clustershell:> `vserver cifs show`

  Das System gibt den Namen des Vservers, den CIFS-Servernamen und weitere Felder zurück.

- Legen Sie ein Passwort für den SVM vsadmin Benutzer fest. Wenn Sie benutzerdefinierten Benutzer oder Cluster-Admin-Benutzer verwenden, überspringen Sie diesen Schritt. Clustershell:> `security login password -username vsadmin -vserver svmname`
- Der SVM vsadmin-Benutzer für externen Zugriff entsperren. Wenn Sie benutzerdefinierten Benutzer oder Cluster-Admin-Benutzer verwenden, überspringen Sie diesen Schritt. Clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Stellen Sie sicher, dass die Firewall-Policy der Daten-LIF auf 'mgmt' (nicht 'data') eingestellt ist. Überspringen Sie diesen Schritt, wenn Sie die SVM mit einem dedizierten Management- lif hinzufügen. Clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Wenn eine Firewall aktiviert ist, muss eine Ausnahme definiert sein, die TCP-Datenverkehr für den Port unter Verwendung des Data ONTAP Data Collectors zulässt.

  Siehe "Anforderungen an den Agenten" Für Konfigurationsinformationen. Dies gilt für lokale Agenten und Agenten, die in der Cloud installiert sind.

- Wenn ein Agent in einer AWS EC2 Instanz zum Monitoring einer Cloud ONTAP SVM installiert wird, müssen sich der Agent und der Storage in derselben VPC befinden. Wenn sie in separaten VPCs sind, muss es eine gültige Route zwischen den VPC geben.

Voraussetzungen für die Sperrung des Benutzerzugriffs

Beachten Sie für Folgendes "Sperrung Des Benutzerzugriffs":

Für diese Funktion sind Anmeldedaten auf Cluster-Ebene erforderlich.

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *cscuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, führen Sie die folgenden Schritte aus, um Workload Security-Berechtigungen zum Blockieren des Benutzers zu erteilen.

Führen Sie für CSuser mit Cluster-Anmeldedaten die folgenden Schritte in der ONTAP-Befehlszeile aus:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Ein Hinweis zu Berechtigungen

Berechtigungen beim Hinzufügen über Cluster Management IP:

Wenn Sie den Cluster Management Administrator-Benutzer nicht verwenden können, um Workload Security den Zugriff auf den ONTAP SVM-Datensammler zu erlauben, können Sie einen neuen Benutzer namens „cscuser“ mit den Rollen erstellen, wie in den Befehlen unten gezeigt. Verwenden Sie den Benutzernamen „CSuser“ und das Passwort für „cscuser“, wenn Sie den Workload Security Data Collector für die Verwendung der Cluster Management IP konfigurieren.

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clustermanagements-Administrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
```

Berechtigungen beim Hinzufügen über Vserver Management IP:

Wenn Sie den Cluster Management Administrator-Benutzer nicht verwenden können, um Workload Security den Zugriff auf den ONTAP SVM-Datensammler zu erlauben, können Sie einen neuen Benutzer namens „cscuser“ mit den Rollen erstellen, wie in den Befehlen unten gezeigt. Verwenden Sie den Benutzernamen „CSuser“ und das Passwort für „cscuser“, wenn Sie den Workload Security Data Collector für die Verwendung von Vserver Management IP konfigurieren.

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clustermanagements-Administrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus. Die folgenden Befehle sollten einfacher in einen Text Editor kopiert und vor der Ausführung der folgenden Befehle auf ONTAP den <vservername> mit Ihrem Vserver-Namen ersetzt werden:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
```

Berechtigungen für autonomen ONTAP-Ransomware-Schutz und ONTAP-Zugriff verweigert

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, befolgen Sie die folgenden Schritte, um Workload Security-Berechtigungen zum Sammeln von ARP-bezogenen Informationen aus ONTAP zu erteilen.

Weitere Informationen finden Sie unter "Integration mit ONTAP-Zugriff verweigert"

Und "Integration in ONTAP Autonomous Ransomware Protection"

Konfigurieren Sie den Datensammler

Schritte zur Konfiguration

1. Melden Sie sich als Administrator oder Account Owner bei Ihrer Data Infrastructure Insights-Umgebung an.
2. Klicken Sie Auf **Workload Security > Collectors > +Data Collectors**

   Das System zeigt die verfügbaren Datensammler an.

3. Bewegen Sie den Mauszeiger über die Kachel **NetApp SVM und klicken Sie auf *+Monitor**.

   Das System zeigt die Konfigurationsseite der ONTAP SVM an. Geben Sie die erforderlichen Daten für die einzelnen Felder ein.

Feld	Beschreibung
Name	Eindeutiger Name für den Data Collector
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus.
Verbindung über Management-IP herstellen für:	Wählen Sie eine Cluster-IP oder eine SVM-Management-IP aus
Management-IP-Adresse für Cluster/SVM	Je nach Ihrer obigen Auswahl die IP-Adresse für das Cluster oder die SVM.
SVM-Name	Name der SVM (dieses Feld ist erforderlich, wenn eine Verbindung über Cluster-IP hergestellt wird)
Benutzername	Benutzername für den Zugriff auf die SVM/Cluster beim Hinzufügen über Cluster IP die Optionen sind: 1. Cluster-Admin 2. 'Cuser' 3. AD-User mit ähnlicher Rolle wie CSuser. Beim Hinzufügen über SVM IP haben Sie folgende Optionen: 4. Vsadmin 5. 'Cuser' 6. AD-Benutzername mit ähnlicher Rolle wie CSuser.
Passwort	Kennwort für den oben genannten Benutzernamen
Freigaben/Volumes Filtern	Wählen Sie aus, ob Freigaben/Volumes aus der Ereignissammlung einbezogen oder ausgeschlossen werden sollen
Geben Sie vollständige Freigabennamen ein, die ausgeschlossen/include werden sollen	Kommagetrennte Liste von Freigaben, die ausgeschlossen oder (je nach Bedarf) aus der Ereignissammlung aufgenommen werden sollen
Geben Sie vollständige Volume-Namen ein, die ausgeschlossen/include werden sollen	Kommagetrennte Liste von Volumes zum Ausschließen oder Einschließen (je nach Bedarf) aus der Ereignissammlung

Überwachen Sie Den Ordnerzugriff	Wenn diese Option aktiviert ist, werden Ereignisse für die Überwachung des Ordnerzugriffs aktiviert. Beachten Sie, dass Ordner erstellen/umbenennen und löschen auch ohne diese Option überwacht werden. Wenn Sie diese Option aktivieren, erhöht sich die Anzahl der überwachten Ereignisse.
Festlegen der Puffergröße für ONTAP-Senden	Legt die Größe des ONTAP FPolicy-Sendepuffers fest. Wenn eine ONTAP-Version vor 9.8p7 verwendet wird und Performance-Problem auftritt, kann die Puffergröße des ONTAP send geändert werden, um die ONTAP-Leistung zu verbessern. Wenden Sie sich an den NetApp Support, wenn diese Option nicht angezeigt wird und Sie sie erkunden möchten.

Nachdem Sie fertig sind

- Auf der Seite installierte Datensammler können Sie den Datensammler über das Optionsmenü rechts neben jedem Collector bearbeiten. Sie können den Datensammler neu starten oder die Konfigurationsattribute des Datensammlers bearbeiten.

Empfohlene Konfiguration für Metro Cluster

Die folgenden Empfehlungen für MetroCluster:

1. Verbinden Sie zwei Data Collectors – eine mit der Quell-SVM und eine andere mit der Ziel-SVM.
2. Die Datensammler sollten durch *Cluster IP* verbunden werden.
3. Zu jedem Zeitpunkt sollte ein Datensammler in Betrieb sein, ein anderer wird im Fehler sein.

   Der aktuelle ‘running’ SVM-Datensammler wird als *running* angezeigt. Der Datensammler der aktuellen ‘stovered’ SVM wird als *Error* angezeigt.

4. Bei jeder Umschaltung ändert sich der Zustand des Datensammlers von ‘running’ zu ‘error’ und umgekehrt.
5. Es dauert bis zu zwei Minuten, bis der Datensammler den Fehlerstatus in den Ausführungszustand wechselt.

Service-Richtlinie

Bei Verwendung der Service-Policy aus ONTAP Version 9.9.1, um eine Verbindung zum Datenquellensammler herzustellen, ist der Dienst *Data-fpolicy-Client* zusammen mit dem Datendienst *Data-nfs* und/oder *Data-cifs* erforderlich.

Beispiel:

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

In Versionen von ONTAP vor 9.9 muss *Data-fpolicy-Client* nicht gesetzt werden.

Data Collector Wiedergeben/Anhalten

2 neue Operationen werden jetzt auf dem Kebab-Menü des Sammlers angezeigt (PAUSE und WIEDERAUFNAHME).

Wenn sich der Data Collector im Status *Running* befindet, können Sie die Erfassung anhalten. Öffnen Sie das Menü „drei Punkte“ für den Collector und wählen Sie PAUSE. Während der Collector angehalten wird, werden keine Daten von ONTAP erfasst und keine Daten vom Collector an ONTAP gesendet. Dies bedeutet, dass keine FPolicy-Ereignisse vom ONTAP zum Datensammler und von dort zu Dateninfrastruktureinblicken übertragen werden.

Wenn neue Volumes usw. auf ONTAP erstellt werden, während der Collector angehalten ist, erfasst Workload Security die Daten nicht, und diese Volumes usw. werden nicht in Dashboards oder Tabellen angezeigt.

Beachten Sie Folgendes:

- Das Löschen von Snapshots geschieht nicht gemäß den Einstellungen, die auf einem angehaltenen Collector konfiguriert wurden.
- EMS-Ereignisse (wie ONTAP ARP) werden nicht auf einem angehaltenen Collector verarbeitet. Das heißt, wenn ONTAP einen Ransomware-Angriff identifiziert, kann Data Infrastructure Insights Workload Security dieses Ereignis nicht erfassen.
- Für einen angehaltenen Collector werden KEINE Integritätsbenachrichtigungen-E-Mails gesendet.
- Manuelle oder automatische Aktionen (wie Snapshot oder Benutzerblockierung) werden auf einem angehaltenen Collector nicht unterstützt.
- Bei Agent- oder Collector-Upgrades, Neustart/Neustart der Agent-VM oder Neustart des Agent-Dienstes bleibt ein angehaltener Collector im Status „*Paused*“.
- Wenn sich der Datensammler im Status *Error* befindet, kann der Collector nicht in den Status *Paused* geändert werden. Die Schaltfläche Pause wird nur aktiviert, wenn der Status des Collectors *Running* lautet.
- Wenn die Verbindung zum Agenten unterbrochen wird, kann der Collector nicht in den Status *Paused* geändert werden. Der Collector geht in den Status *stopped* und die Schaltfläche Pause wird deaktiviert.

Persistenter Speicher

Persistenter Speicher wird von ONTAP 9.14.1 und höher unterstützt. Beachten Sie, dass die Anweisungen für Volume-Namen von ONTAP 9.14 bis 9.15 variieren.

Persistenter Speicher kann durch Aktivieren des Kontrollkästchens auf der Seite Collector Edit/Add aktiviert werden. Nach dem Aktivieren des Kontrollkästchens wird ein Textfeld für die Annahme des Volume-Namens angezeigt. Der Volume-Name ist ein obligatorisches Feld für die Aktivierung von Persistent Store.

- Für ONTAP 9.14.1 müssen Sie das Volume erstellen, bevor Sie die Funktion aktivieren, und den gleichen Namen im Feld „*Volume Name*“ eingeben. Die empfohlene Volume-Größe beträgt 16 GB.
- Für ONTAP 9.15.1 wird das Volume automatisch mit 16 GB Größe vom Collector erstellt. Dabei wird der Name verwendet, der im Feld *Volume Name* angegeben ist.

Für Persistent Store sind bestimmte Berechtigungen erforderlich (einige oder alle dieser Berechtigungen sind möglicherweise bereits vorhanden):

Clustermodus:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

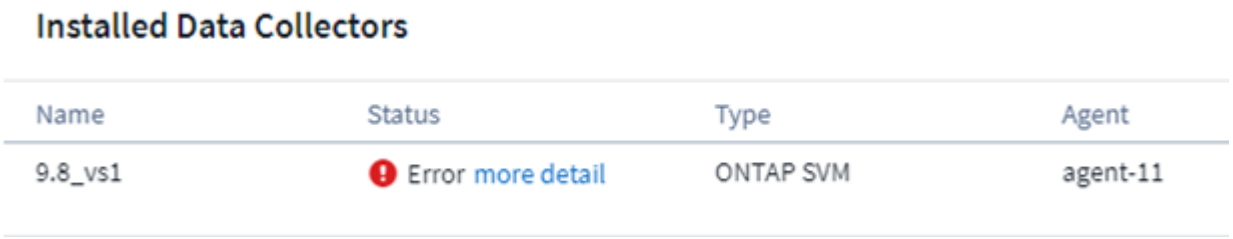
VServer-Modus:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

Fehlerbehebung

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

Im Fehlerfall klicken Sie in der Spalte *Status* auf *more Detail*, um Details zum Fehler zu erhalten.



Problem:	Auflösung:
Data Collector wird einige Zeit ausgeführt und stoppt nach einer zufälligen Zeit, schlägt fehl mit: "Fehlermeldung: Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Externer fpolicy-Server überlastet.“	Die Ereignisrate von ONTAP war weit höher als die, die das Feld Agent verarbeiten kann. Damit wurde die Verbindung beendet. Überprüfen Sie den Peak Traffic in CloudSecure, wenn die Verbindung unterbrochen wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensics > Alle Aktivitäten** überprüfen. Wenn der maximale aggregierte Datenverkehr höher ist als der, was die Agent Box verarbeiten kann, lesen Sie die Seite Event Rate Checker zur Dimensionierung der Collector-Bereitstellung in einer Agent-Box. Wenn der Agent vor dem 4. März 2021 in der Agent-Box installiert wurde, führen Sie die folgenden Befehle in der Agent-Box aus: Echo 'net.Core.rmem_max=8388608' >> /etc/sysctl.conf Echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p Neustart des Sammlers von der UI nach der Größenänderung.

Problem:	Auflösung:
Collector meldet Fehlermeldung: „Keine lokale IP-Adresse auf dem Anschluss gefunden, die die Datenschnittstellen der SVM erreichen kann“.	Dies ist sehr wahrscheinlich auf der Seite des ONTAP-Netzwerks zurückzuführen. Bitte befolgen Sie diese Schritte: 1. Stellen Sie sicher, dass es keine Firewalls auf den SVM-Daten-LIF oder das Management-LIF gibt, die die Verbindung von der SVM blockieren. 2. Beim Hinzufügen einer SVM über eine Cluster-Management-IP, stellen Sie bitte sicher, dass die Daten- und Management- lif der SVM von der Agent-VM pingfähig sind. Bei Problemen prüfen Sie Gateway, Netzmaske und Routen für den Lif. Sie können auch versuchen, sich mithilfe von ssh unter Verwendung der Cluster-Management-IP beim Cluster anzumelden und die Agent-IP zu pingen. Stellen Sie sicher, dass die Agent-IP pingfähig ist: *Network ping -vserver <vserver name> -Destination <Agent IP> -lif <Lif Name> -show-Detail* Wenn nicht pingfähig, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, so dass der Agent-Rechner pingfähig ist. 3. Wenn Sie eine Verbindung über Cluster-IP versucht haben und es nicht funktioniert, versuchen Sie, direkt über SVM-IP zu verbinden. Die Schritte zur Verbindung über SVM IP finden Sie oben. 4. Beim Hinzufügen des Collectors über SVM IP und vsadmin Zugangsdaten prüfen, ob die SVM Lif die Data PLUS Mgmt-Rolle aktiviert hat. In diesem Fall funktioniert der Ping an die SVM Lif, allerdings funktioniert SSH an die SVM Lif nicht. Wenn ja, erstellen Sie ein SVM Management-only-Lif und versuchen Sie, eine Verbindung über diese SVM-Management-only-Lizenz herzustellen. 5. Wenn es immer noch nicht funktioniert, erstellen Sie eine neue SVM-Lif und versuchen Sie eine Verbindung über diese Lif. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist. 6. Erweitertes Debugging: A) Starten Sie eine Paketverfolgung in ONTAP. b) Versuchen Sie, einen Datensammler von der CloudSecure UI aus mit der SVM zu verbinden. c) Warten Sie, bis der Fehler angezeigt wird. Stoppen Sie die Paketverfolgung in ONTAP. d) Öffnen Sie die Paketverfolgung von ONTAP. Sie ist an diesem Standort verfügbar

Problem:	Auflösung:
Nachricht: „Es konnte der ONTAP-Typ für [Hostname: <IP-Adresse> nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)“	1. Überprüfen Sie, ob die richtige SVM-IP-Management-Adresse oder Cluster-Management-IP angegeben wurde. 2. SSH zu der SVM oder dem Cluster, mit dem Sie beabsichtigen zu verbinden. Sobald Sie eine Verbindung hergestellt haben, stellen Sie sicher, dass der SVM oder der Cluster-Name korrekt ist.

Problem:	Auflösung:
Fehlermeldung: „Konnektor befindet sich im Fehlerzustand. Service.name: Audit. Grund für Fehlschlag: Externer fpolicy-Server beendet.“	1. Es ist sehr wahrscheinlich, dass eine Firewall die notwendigen Ports in der Agent-Maschine blockiert. Überprüfen Sie, ob der Port-Bereich 35000-55000/tcp geöffnet ist, damit der Agent-Rechner eine Verbindung von der SVM herstellen kann. Stellen Sie außerdem sicher, dass keine Firewalls von der ONTAP-Seite aus aktiviert sind, die die Kommunikation mit dem Agenten-Rechner blockieren. 2. Geben Sie den folgenden Befehl in das Feld Agent ein und stellen Sie sicher, dass der Port-Bereich geöffnet ist. *Sudo iptables-save 3500** Beispielausgabe sollte aussehen wie: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEU -j ACCEPT* 3. Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein und überprüfen Sie, ob für die Kommunikation mit ONTAP keine Firewall eingerichtet ist. *Systemdienste Firewall show Systemdienste Firewall-Policy show_"Überprüfen Sie die Firewall-Befehle" Auf der ONTAP-Seite. 4. SSH an die SVM/Cluster, die Sie überwachen möchten. Ping the Agent Box from the SVM Data lif (with CIFS, NFS Protocols Support) und Sicherstellen, dass Ping funktioniert: _Network ping -vserver <vserver Name> -Destination <Agent IP> -lif <Lif Name> -show-Detail* Wenn nicht pingfähig, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, damit der Agent-Rechner pingfähig ist. 5.Wenn eine einzelne SVM über 2 Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die UI. Starten Sie dann den anderen Datensammler über die UI neu. Dann wird der Data Collector den Status „RUNNING“ anzeigen und beginnt, Ereignisse von der SVM zu empfangen. Im Prinzip sollte in einem Mandanten nur eine SVM über 1 Datensammler hinzugefügt werden. 1 SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden. 6. In Fällen, in denen in zwei verschiedenen Workload-Sicherheitsumgebungen (Mandanten) dieselbe SVM hinzugefügt wurde, wird der letzte Aspekt immer erfolgreich sein. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und startet die erste. So wird der Sammler in der ersten aufhören, Ereignisse zu empfangen, und sein "Audit"-Service wird in Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzigen Umgebung. 7. Dieser Fehler kann auch auftreten, wenn Dienstrichtlinien nicht richtig konfiguriert sind. Mit ONTAP 9.8 oder höher ist zur Verbindung mit dem Data Source Collector der datenrichtlinienclient-Dienst zusammen mit dem Datenservice Data-nfs und/oder Data-cifs erforderlich. Darüber hinaus muss der datenrichtlinienclient-Service den Daten-Lif(s) für die überwachte SVM zugeordnet werden.

Problem:	Auflösung:
Auf der Aktivitätsseite werden keine Ereignisse angezeigt.	1. Prüfen, ob ONTAP Collector im „LAUFENDEN“ Zustand ist. Wenn ja, stellen Sie sicher, dass einige cifs-Ereignisse auf den cifs-Client-VMs durch das Öffnen einiger Dateien generiert werden. 2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bei der SVM an und geben Sie den folgenden Befehl ein. *<SVM>Ereignisprotokoll show -source fpolicy* Stellen Sie sicher, dass fpolicy keine Fehler enthält. 3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bei der SVM an. Geben Sie den folgenden Befehl ein: *<SVM>fpolicy show* Überprüfen Sie, ob die fpolicy mit dem Präfix „cloudSecure_“ festgelegt wurde und der Status „ein“ lautet. Ist er nicht eingestellt, kann der Agent die Befehle in der SVM höchstwahrscheinlich nicht ausführen. Stellen Sie sicher, dass alle Voraussetzungen, die am Anfang der Seite beschrieben sind, eingehalten wurden.
SVM Data Collector befindet sich im Fehlerzustand und Fehlermeldung „Agent konnte keine Verbindung zum Collector herstellen“	1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellenkollektoren herstellen. 2. Überprüfen Sie, wie viele Datenquellensammler mit dem Agenten verbunden sind. 3. Überprüfen Sie auch die Datenflussrate auf der Seite „Alle Aktivitäten“ in der UI. 4. Wenn die Anzahl der Vorgänge pro Sekunde signifikant hoch ist, installieren Sie einen anderen Agenten und verschieben einige der Datenquellensammler auf den neuen Agenten.
SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Node konnte keine Verbindung zum FPolicy-Server „12.195.15.146“ herstellen (Grund: „Select Timed Out“)“	Firewall ist in SVM/Cluster aktiviert. fpolicy Engine kann also keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP, die verwendet werden können, um weitere Informationen zu erhalten sind: Event Log show -source fpolicy, die das Fehlerereignisprotokoll show -source fpolicy -fields Event,Action,Beschreibung zeigt, die weitere Details."Überprüfen Sie die Firewall-Befehle" Auf der ONTAP-Seite.
Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname:Audit. Grund für Fehler: Keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beides, Status: Up) auf der SVM gefunden.“	Stellen Sie sicher, dass es eine Betriebsschnittstelle gibt (Rolle als Daten und Datenprotokoll als CIFS/NFS.

Problem:	Auflösung:
Der Datensammler wechselt in den Fehlerzustand und geht nach einiger Zeit in DEN LAUFENDEN Zustand, dann wieder zurück zu Fehler. Dieser Zyklus wiederholt sich.	Dies geschieht typischerweise im folgenden Szenario: 1. Es werden mehrere Datensammler hinzugefügt. 2. Die Datensammler, die diese Art von Verhalten zeigen, haben 1 SVM zu diesen Datensammlern hinzugefügt. Das bedeutet, dass 2 oder mehr Datensammler mit 1 SVM verbunden sind. 3. Sicherstellen, dass 1 Datensammler eine Verbindung mit nur 1 SVM herstellt. 4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind.
Der Anschluss befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Konnte nicht konfiguriert werden (Richtlinie auf SVM svmname. Grund: Ungültiger Wert angegeben für Element 'shares-to-include' in 'fpolicy.Policy.Scope-modify: "Federal'	Die Freigabennamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die DSC-Konfiguration der ONTAP SVM, um die Freigabennamen zu korrigieren. *Aktien einschließen und ausschließen* ist nicht für eine lange Liste von Share-Namen gedacht. Verwenden Sie stattdessen Filtern nach Volume, wenn eine große Anzahl an Shares enthalten oder ausschließen muss.
Im Cluster gibt es bereits frichtlinien, die nicht verwendet werden. Was sollte vor der Installation von Workload Security getan werden?	Es wird empfohlen, alle vorhandenen nicht verwendeten fpolicy-Einstellungen zu löschen, selbst wenn sie sich im getrennten Zustand befinden. Workload Security erstellt fpolicy mit dem Präfix „cloudSecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden. CLI-Befehl zum Anzeigen der fpolicy-Liste: *fpolicy show* Steps zum Löschen von fpolicy-Konfigurationen: *fpolicy disable -vserver <svmname> -Policy-Name <Policy_Name>* fpolicy-Name_vserver_Name_vmserver_delete -vmserver_name_vmserver_list_vmserver_delete_vengine_Name_vmserver_vengine_Name_vmserver_vmserver_list_vmserver_<_vmgine_Name_vmserver_<_vmgine_list_Name_vmserver_<_vmserver_nement-Name_<_vmserver_vmserver_Name_vmserver_<_vmserver_list_vmserver_Name_<<<_next-
Nach Aktivierung der Workload-Sicherheit beeinträchtigt die ONTAP-Performance: Sporadisch steigt die Latenz an und IOPS werden sporadisch niedrig.	Bei der Verwendung von ONTAP mit Workload-Sicherheit können in ONTAP manchmal Latenzprobleme auftreten. Dafür gibt es eine Reihe von möglichen Gründen, wie im Folgenden beschrieben: "1372994", "1415152", "1438207", "1479704", "1354659". Alle diese Probleme wurden in ONTAP 9.13.1 und höher behoben. Es wird dringend empfohlen, eine dieser neueren Versionen zu verwenden.

Problem:	Auflösung:
Datensammler ist fehlerhaft, zeigt diese Fehlermeldung an. „Fehler: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Richtlinie konnte nicht für SVM svm_Test konfiguriert werden. Grund: Fehlender Wert für zapi Feld: Ereignisse. „	Beginnen Sie mit einer neuen SVM, wobei nur ein NFS-Service konfiguriert ist. Hinzufügen eines ONTAP SVM-Datensammlers zur Workload-Sicherheit CIFS ist als zulässiges Protokoll für die SVM konfiguriert und fügt den ONTAP SVM Data Collector zur Workload-Sicherheit hinzu. Warten Sie, bis der Datensammler in Workload Security einen Fehler anzeigt. Da der CIFS-Server NICHT auf der SVM konfiguriert ist, wird dieser Fehler, wie in der linken Seite dargestellt, durch Workload Security angezeigt. Bearbeiten Sie den ONTAP SVM Data Collector und deaktivieren Sie die Prüfung CIFS als zulässiges Protokoll. Speichern Sie den Datensammler. Er wird erst ausgeführt, wenn das NFS-Protokoll aktiviert ist.
Der Data Collector zeigt die Fehlermeldung „Fehler: Fehler: Fehler: Fehler, den Zustand des Collectors innerhalb von 2 Wiederholungen zu ermitteln. Versuchen Sie erneut, den Collector neu zu starten (Fehlercode: AGENT008)“.	1. Scrollen Sie auf der Seite Data Collectors rechts vom Datensammler, der den Fehler gibt, und klicken Sie auf das Menü mit 3 Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Save* drücken. Der Data Collector wird neu gestartet, und der Fehler sollte behoben werden. 2. Der Agent-Rechner kann nicht genügend CPU- oder RAM-Reserve, deshalb sind die DSCs gescheitert. Überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf dem Computer hinzugefügt werden. Wenn es mehr als 20 ist, erhöhen Sie die CPU- und RAM-Kapazität des Agent-Rechners. Sobald die CPU und der RAM erhöht sind, werden die DSCs in die Initialisierung und dann automatisch in den laufenden Zustand versetzt. Schauen Sie sich den Leitfaden zur Größenanpassung an "Auf dieser Seite".
Der Data Collector wird beim Auswählen des SVM-Modus fehlgesetzt.	Wenn beim Herstellen einer Verbindung im SVM-Modus die Cluster-Management-IP verwendet wird, um eine Verbindung anstelle der SVM-Management-IP herzustellen, wird die Verbindung getrennt. Stellen Sie sicher, dass die richtige SVM-IP verwendet wird.

Wenn Sie immer noch Probleme haben, wenden Sie sich an die auf der Seite * Hilfe > Support* genannten Support-Links.

Konfiguration des Cloud Volumes ONTAP und Amazon FSX für NetApp ONTAP Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von

Geräten zu erfassen.

Cloud Volumes ONTAP Storage-Konfiguration

In der OnCommand Cloud Volumes ONTAP-Dokumentation können Sie eine AWS-Instanz mit einem Node/HA für das Hosting des Workload Security Agent konfigurieren:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Führen Sie nach Abschluss der Konfiguration die Schritte aus, um die SVM einzurichten:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Unterstützte Plattformen

- Cloud Volumes ONTAP, unterstützt bei allen verfügbaren Cloud-Service-Providern. Zum Beispiel Amazon, Azure, Google Cloud.
- ONTAP Amazon FSX

Agent-Gerätekonfiguration

Die Agent-Maschine muss in den jeweiligen Subnetzen der Cloud-Service-Provider konfiguriert sein. Weitere Informationen zum Netzwerkzugriff finden Sie unter [Agent-Anforderungen].

Unten sind die Schritte für die Installation von Agenten in AWS aufgeführt. Die entsprechenden Schritte, die für den Cloud-Service-Provider gelten, können für die Installation in Azure oder Google Cloud befolgt werden.

Konfigurieren Sie in AWS die Maschine, die als Workload Security Agent verwendet werden soll, mit den folgenden Schritten:

Konfigurieren Sie die Maschine, die als Workload Security Agent verwendet werden soll, wie folgt:

Schritte

1. Melden Sie sich bei der AWS Konsole an, und navigieren Sie zur Seite EC2-instances, und wählen Sie *Launch Instance* aus.
2. Wählen Sie eine RHEL- oder CentOS AMI-Lösung mit der entsprechenden Version aus, wie auf dieser Seite erwähnt:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Wählen Sie die VPC und das Subnetz aus, in der die Cloud-ONTAP-Instanz residiert.
4. Wählen Sie *t2.xlarge* (4 vcpus und 16 GB RAM) als zugewiesene Ressourcen aus.
    a. Erstellen Sie die EC2-Instanz.
5. Installieren Sie die erforderlichen Linux-Pakete mithilfe des YUM-Paketmanagers:
    a. Installieren Sie die nativen Linux-Pakete *wget* und *unzip*.

Installieren Sie den Workload Security Agent

1. Melden Sie sich als Administrator oder Account Owner bei Ihrer Data Infrastructure Insights-Umgebung an.
2. Navigieren Sie zu Workload Security **Collectors** und klicken Sie auf die Registerkarte **Agents**.
3. Klicken Sie auf **+Agent** und geben Sie RHEL als Zielplattform an.
4. Kopieren Sie den Befehl Agenteninstallation.
5. Fügen Sie den Befehl „Agent Installation“ in die RHEL EC2-Instanz ein, bei der Sie angemeldet sind. Dadurch wird der Workload Security Agent installiert, der alle zur Verfügung stellt "Agent-

Voraussetzungen" Werden erfüllt.

Ausführliche Schritte finden Sie über den folgenden Link: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Fehlerbehebung

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

Problem	Auflösung
„Workload-Sicherheit: Fehler beim ermitteln des ONTAP-Typs für Amazon FxSN Datensammler“ Fehler wird vom Data Collector angezeigt. Der Kunde kann den neuen Amazon FSxN Data Collector nicht zur Workload Security hinzufügen. Die Verbindung zum FSxN-Cluster an Port 443 vom Agenten ist zeitabhängig. Für die Kommunikation sind Firewall- und AWS Sicherheitsgruppen die erforderlichen Regeln aktiviert. Ein Agent wurde bereits bereitgestellt und befindet sich auch im selben AWS Konto. Dieser Agent wird verwendet, um die verbleibenden NetApp-Geräte zu verbinden und zu überwachen (und alle funktionieren).	Lösen Sie dieses Problem, indem Sie fsxadmin LIF-Netzwerksegment zur Sicherheitsregel des Agenten hinzufügen. Erlaubt alle Ports, wenn Sie sich nicht sicher über die Ports sind.

Benutzerverwaltung

Benutzerkonten für die Workload-Sicherheit werden über Cloud Insights gemanagt.

Cloud Insights bietet vier Benutzerkontoebenen: Kontoinhaber, Administrator, Benutzer und Gast. Jedem Konto werden bestimmte Berechtigungsebenen zugewiesen. Ein Benutzerkonto mit Administratorrechten kann Benutzer erstellen oder ändern und jedem Benutzer eine der folgenden Workload-Sicherheitsrollen zuweisen:

Rolle	Zugriff Auf Die Workload-Sicherheit
Verwalter	Alle Workload-Sicherheitsfunktionen, einschließlich derer für Warnmeldungen, Forensik, Datensammler, automatisierte Antwortrichtlinien und APIs für Workload-Sicherheit, sind möglich. Ein Administrator kann auch andere Benutzer einladen, kann aber nur Workload-Sicherheitsrollen zuweisen.
Benutzer	Kann Warnungen anzeigen und verwalten und Forensik anzeigen. Benutzer können den Alarmstatus ändern, eine Notiz hinzufügen, Snapshots manuell erstellen und den Benutzerzugriff einschränken.
Gast	Kann Warnungen und Forensik anzeigen. Gastrolle kann den Alarmstatus nicht ändern, Notizen hinzufügen, Snapshots manuell erstellen oder den Benutzerzugriff einschränken.

Schritte

1. Melden Sie sich bei Workload Security an

2. Klicken Sie im Menü auf **Admin > Benutzerverwaltung**

   Sie werden zur Seite User Management von Cloud Insights weitergeleitet.

3. Wählen Sie die gewünschte Rolle für jeden Benutzer aus.

Wählen Sie beim Hinzufügen eines neuen Benutzers einfach die gewünschte Rolle aus (normalerweise Benutzer oder Gast).

Weitere Informationen zu Benutzerkonten und Rollen finden Sie im Cloud Insights "Benutzerrolle" Dokumentation.

SVM Event Rate Checker (Agent Sizing Guide)

Das Event Rate Checker wird verwendet, um die kombinierte Ereignisrate von NFS/SMB in der SVM zu prüfen, bevor Sie einen ONTAP SVM Data Collector installieren, um zu ermitteln, wie viele SVMs ein Agent Machine überwachen können. Verwenden Sie den Event Rate Checker als Leitfaden zur Größenbestimmung, um Ihre Sicherheitsumgebung zu planen.

Ein Agent kann bis zu 50 Datensammler unterstützen.

Voraussetzungen:

- Cluster-IP
- Benutzername und Passwort für den Cluster-Admin

> Wenn dieses Skript ausgeführt wird, sollte kein ONTAP SVM Data Collector für die SVM ausgeführt werden, für die die Ereignisrate ermittelt wird.

Schritte

1. Installieren Sie den Agent, indem Sie die Anweisungen in CloudSecure befolgen.
2. Führen Sie nach der Installation des Agent das Skript *Server_Data_Rate_Checker.sh* als Sudo-Benutzer aus:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Dieses Skript erfordert die Installation von _sshapass_ auf dem linux-
Rechner. Es gibt zwei Möglichkeiten, es zu installieren:
```

   a. Führen Sie den folgenden Befehl aus:

```
 linux_prompt> yum install sshpass
.. Wenn das nicht funktioniert, laden Sie _sshapass_ aus dem Internet
auf den linux-Rechner herunter, und führen Sie den folgenden Befehl
aus:
```

```
linux_prompt> rpm -i sshpass
```

3. Geben Sie die richtigen Werte ein, wenn Sie dazu aufgefordert werden. Ein Beispiel hierfür finden Sie unten.
4. Das Skript dauert etwa 5 Minuten.
5. Nach Abschluss des Durchlaufs wird die Ereignisrate vom SVM gedruckt. Sie können die Ereignisrate pro SVM in der Konsolenausgabe überprüfen:

```
“Svm svm_rate is generating 100 events/sec”.
```

Jeder ONTAP SVM Data Collector kann einer einzelnen SVM zugeordnet werden. Dies bedeutet, dass jeder Data Collector die Anzahl der von einer einzelnen SVM generierten Ereignisse erhalten kann.

Beachten Sie Folgendes:

A) Verwenden Sie diese Tabelle als allgemeinen Leitfaden zur Größenbemessung. Sie können die Anzahl der Kerne und/oder des Speichers erhöhen, um die Anzahl der unterstützten Datensammler zu erhöhen, bis zu maximal 50 Datensammler:

Agent-Gerätekonfiguration	Anzahl der SVM Data Collectors	Max. Ereignisrate, die der Agent-Rechner verarbeiten kann
4 Cores, 16 GB	10 Datensammler	20.000 Ereignisse/Sek.
4 Kerne, 32 GB	20 Datensammler	20.000 Ereignisse/Sek.

B) um Ihre gesamten Ereignisse zu berechnen, fügen Sie die für alle SVMs erzeugten Ereignisse für diesen Agenten hinzu.

C) Wenn das Skript nicht während der Stoßzeiten ausgeführt wird oder der Spitzenverkehr schwer vorherzusagen ist, dann einen Ereignissatz-Puffer von 30 % behalten.

B + C sollte kleiner Als A sein, andernfalls kann der Agent-Rechner nicht überwacht werden.

Mit anderen Worten, die Anzahl der Datensammler, die einem einzelnen Agenten-Rechner hinzugefügt werden können, sollte der folgenden Formel entsprechen:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Siehe
xref:{relative_path}concept_cs_agent_requirements.html["Anforderungen An
Den Agenten"] Seite für zusätzliche Voraussetzungen und Anforderungen.
```

Beispiel

Lassen Sie uns sagen, wir haben drei SVMS mit Ereignissätzen von 100, 200 und 300 Ereignissen pro Sekunde.

Wir verwenden die Formel:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

Die Konsolenausgabe ist auf dem Agent-Rechner im Dateinamen _*fpolicy_stat*<SVM Name>.log_ im vorliegenden Arbeitsverzeichnis verfügbar.

Das Skript kann in den folgenden Fällen fehlerhafte Ergebnisse liefern:

- Falsche Anmeldedaten, IP oder SVM-Name werden angegeben.
- Eine bereits vorhandene fpolicy mit demselben Namen, der gleichen Sequenznummer usw. gibt einen Fehler.
- Das Skript wird während des Laufs abrupt unterbrochen.

Ein Beispiel für einen Skriptdurchlauf ist unten dargestellt:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
------------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

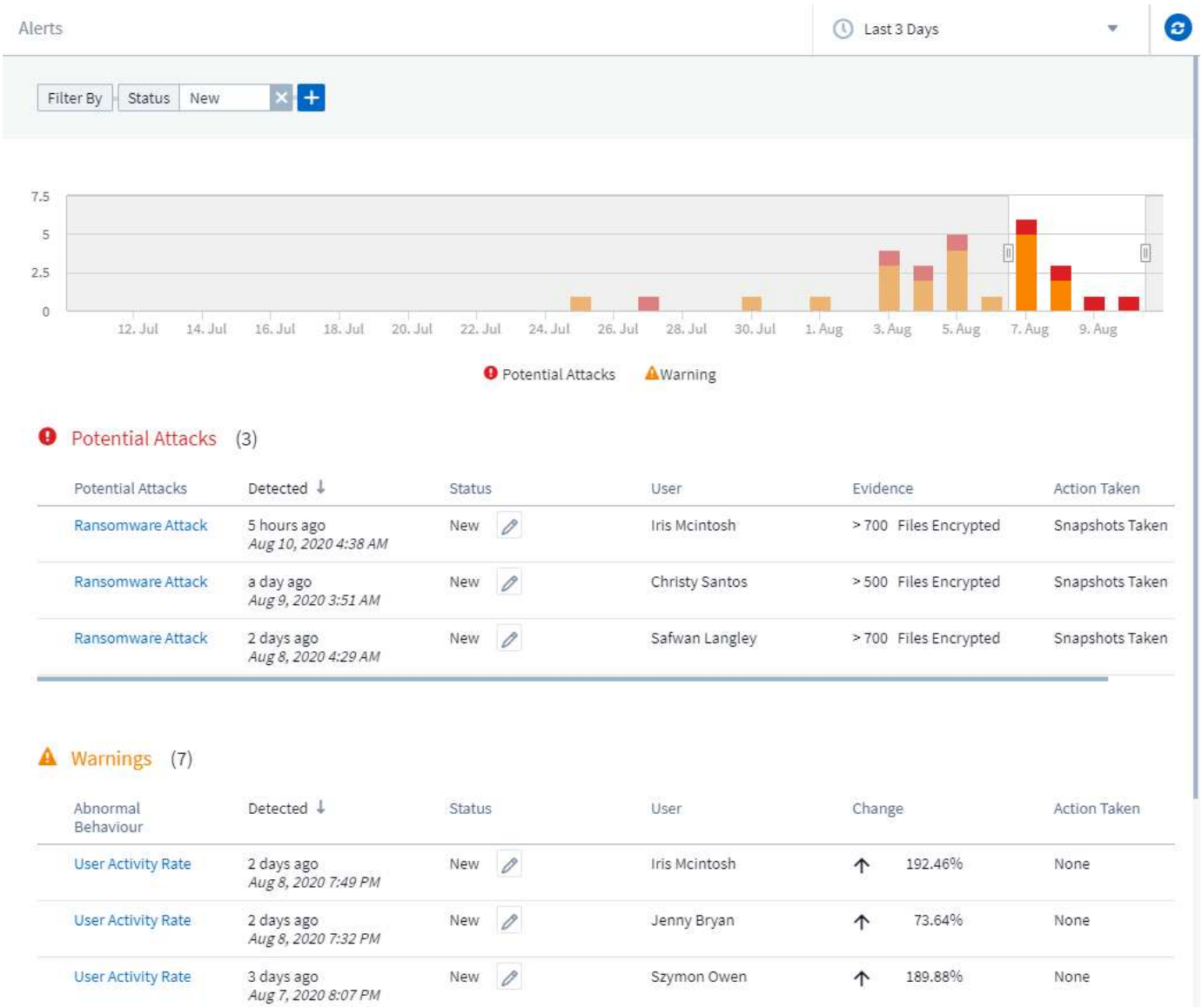
Fehlerbehebung

Frage	Antwort
Wenn ich dieses Skript auf einer SVM ausführe, die bereits für die Workload-Sicherheit konfiguriert ist, verwendet es einfach die bestehende fpolicy-Konfiguration auf der SVM oder richtet es eine temporäre ein und führt den Prozess aus?	Der Event Rate Checker kann auch für eine bereits für Workload Security konfigurierte SVM einwandfrei ausgeführt werden. Es sollte keine Auswirkungen geben.
Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann?	Ja. Bearbeiten Sie einfach das Skript und ändern Sie die maximale Anzahl der SVMs von 5 in eine beliebige Zahl.
Wenn ich die Anzahl der SVMs vergrössern möchte, wird sich damit die Ausführung des Skripts verlängern?	Nein Das Skript wird für maximal 5 Minuten ausgeführt, selbst wenn die Anzahl der SVMs erhöht wird.
Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann?	Ja. Sie müssen das Skript bearbeiten und die maximale Anzahl an SVMs von 5 in eine beliebige andere Maximalzahl ändern.
Wenn ich die Anzahl der SVMs vergrössern möchte, wird sich damit die Ausführung des Skripts verlängern?	Nein Das Skript läuft für maximal 5 Minuten, selbst wenn die Anzahl der SVMs erhöht wird.

Was passiert, wenn ich die Ereignisratsprüfung mit einem vorhandenen Agenten durchführe?	Wenn Sie die Ereignisratenprüfung für einen bereits vorhandenen Agenten ausführen, kann dies zu einer Erhöhung der Latenz auf der SVM führen. Diese Erhöhung ist temporär, während die Ereignisratenprüfung ausgeführt wird.

Meldungen

Die Seite „Workload Security Alerts“ zeigt eine Zeitleiste aktueller Angriffe und/oder Warnungen an und ermöglicht Ihnen, Details zu jedem Problem anzuzeigen.



Alarm

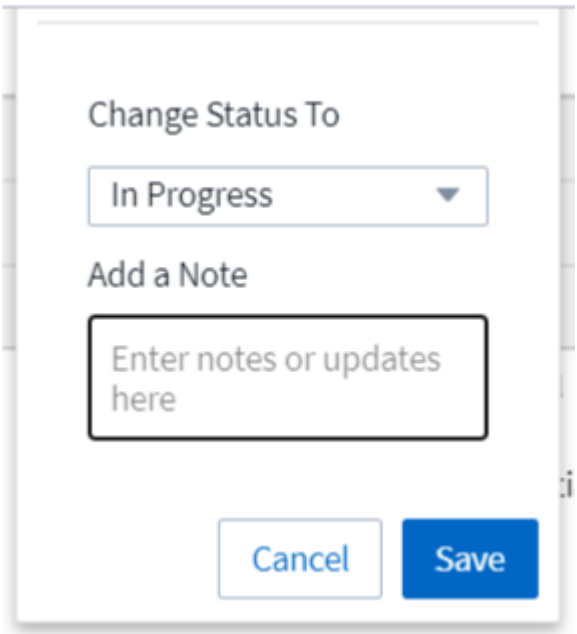
In der Alarmliste wird ein Diagramm angezeigt, in dem die Gesamtanzahl der potenziellen Angriffe und/oder Warnungen angezeigt wird, die im ausgewählten Zeitraum angehoben wurden, gefolgt von einer Liste der Angriffe und/oder Warnungen, die in diesem Zeitraum aufgetreten sind. Sie können den Zeitbereich ändern, indem Sie die Schieberegler für Startzeit und Endzeit in der Grafik anpassen.

Für jede Meldung wird Folgendes angezeigt:

Potentielle Angriffe:

- Der *Potential Attack*-Typ (z. B. Ransomware oder Sabotage)
- Datum und Uhrzeit des potenziellen Angriffs wurde *entdeckt*
- Der *Status* der Warnmeldung:
  - **Neu**: Dies ist der Standard für neue Warnmeldungen.
  - **In Bearbeitung**: Der Alarm wird von einem Teammitglied oder Mitgliedern untersucht.
  - **Behoben**: Der Alarm wurde von einem Teammitglied als gelöst markiert.
  - **Abgeschieden**: Der Alarm wurde als falsch positives oder erwartetes Verhalten abgewiesen.

    Ein Administrator kann den Status der Warnmeldung ändern und eine Notiz hinzufügen, um die Untersuchung zu unterstützen.



- Der *User*, dessen Verhalten die Warnung ausgelöst hat
- *Nachweis* des Angriffs (zum Beispiel wurde eine große Anzahl von Dateien verschlüsselt)
- Die *Aktion wurde ausgeführt* (zum Beispiel wurde ein Snapshot erstellt)

Warnungen:

- Das *anormale Verhalten*, das die Warnung ausgelöst hat
- Das Datum und die Uhrzeit, zu der das Verhalten erkannt wurde_
- Der *Status* der Warnmeldung (Neu, wird ausgeführt usw.)
- Der *User*, dessen Verhalten die Warnung ausgelöst hat
- Eine Beschreibung des *Change* (z. B. eine abnormale Erhöhung des Dateizugriffs)
- Die *Aktion Ausgeführt*

Filteroptionen

Sie können Warnungen nach folgenden Kriterien filtern:

- Der *Status* der Warnmeldung
- Spezifischer Text in der *Note*
- Die Art von *attacks/Warnings*
- Der_Benutzer_, dessen Aktionen die Warnung/Warnung ausgelöst haben

Die Seite „Warndetails“

Sie können auf der Seite mit den Warnmeldungen auf einen Alarm-Link klicken, um eine Detailseite für die Meldung zu öffnen. Die Alarmdetails können je nach Angriffstyp oder Alarmtyp variieren. Eine Seite mit den Details zum Angriff durch Ransomware kann beispielsweise folgende Informationen enthalten:

Zusammenfassung:

- Angriffstyp (Ransomware, Sabotage) und Alarm-ID (zugewiesen durch Workload-Sicherheit)
- Datum und Uhrzeit des Angriffs
- Es wurde eine Aktion ausgeführt (beispielsweise ein automatischer Snapshot erstellt. Die Zeit des Snapshots wird direkt unter der Zusammenfassung angezeigt)
- Status (Neu, in Bearbeitung usw.)

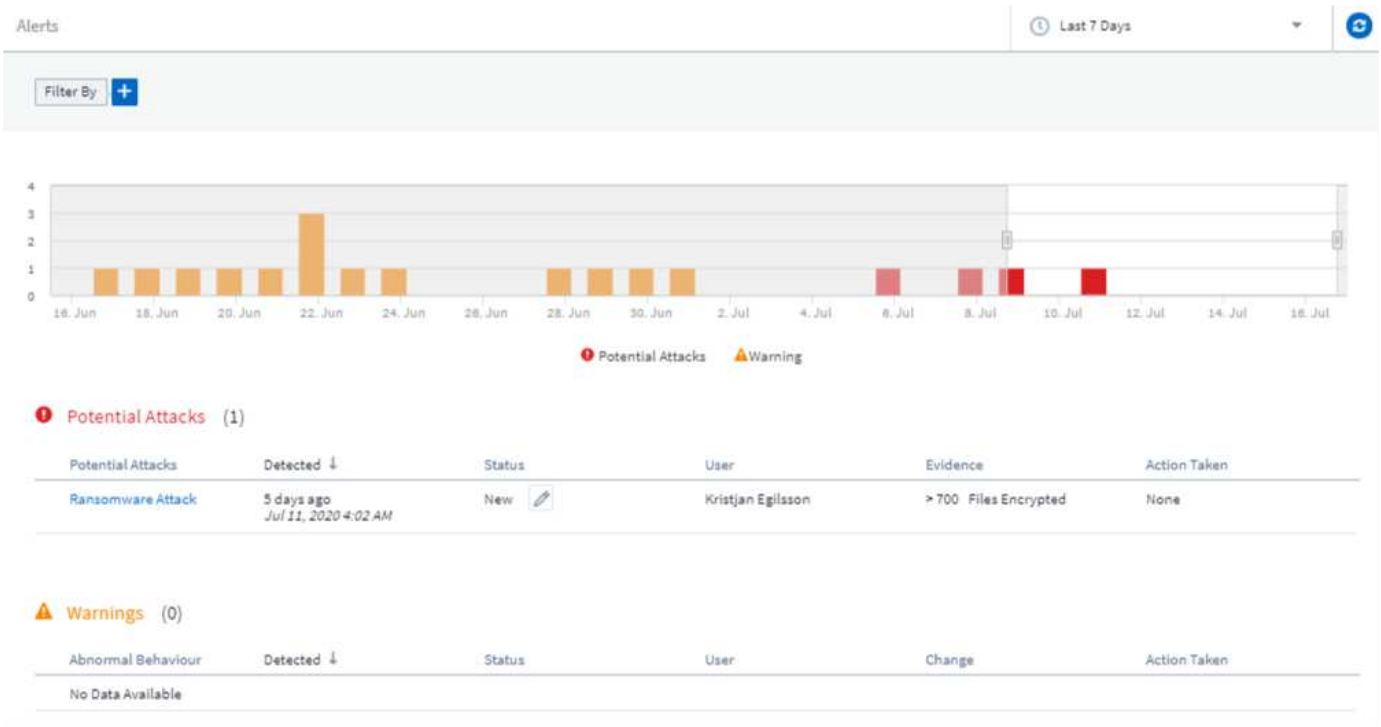
Abschnitt „Angriffsergebnisse“:

- Anzahl der betroffenen Volumes und Dateien
- Eine begleitende Zusammenfassung der Detektion
- Ein Diagramm mit Dateiaktivitäten während des Angriffs

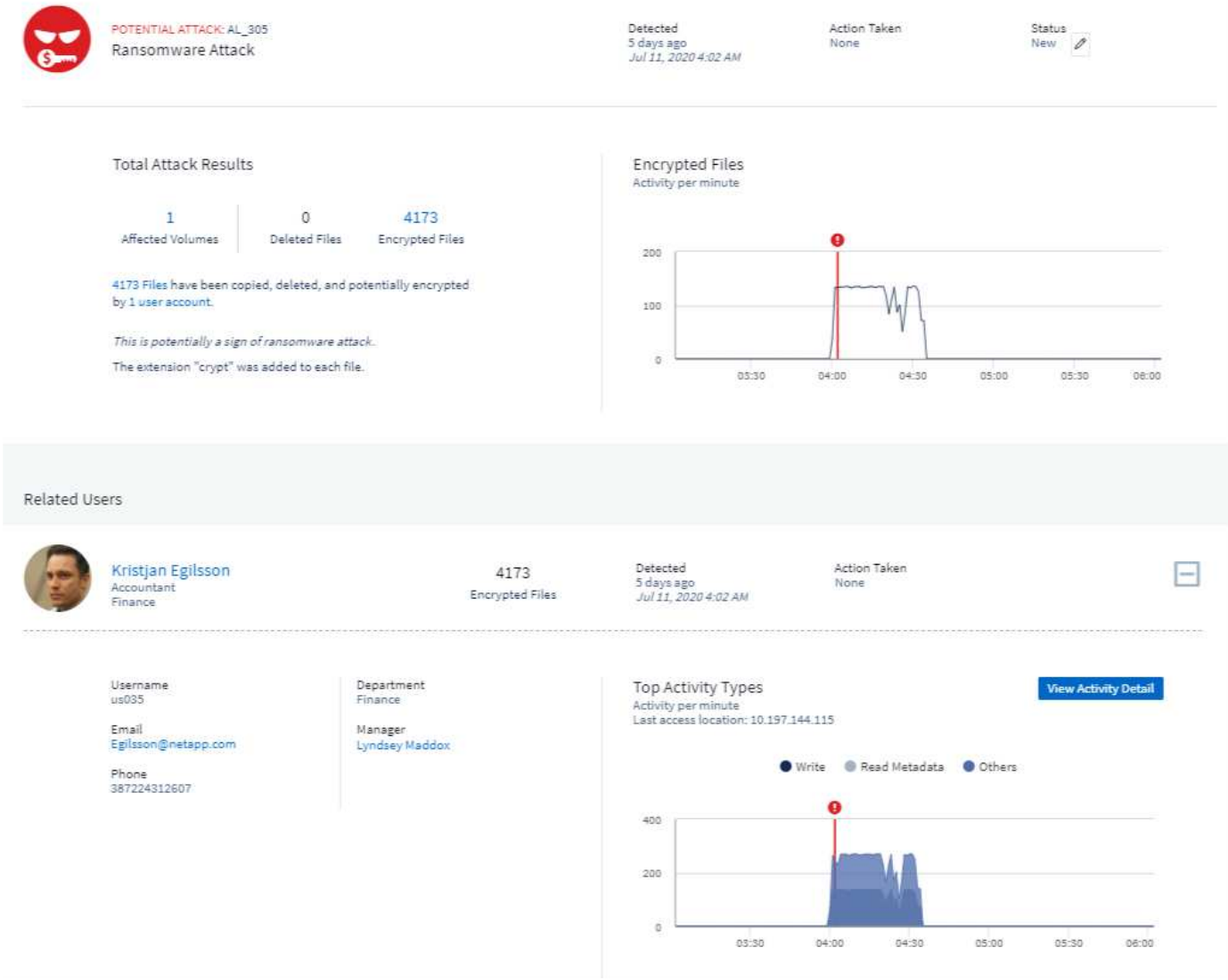
Abschnitt „Verwandte Benutzer“:

In diesem Abschnitt werden Details zu dem Benutzer angezeigt, der an dem potenziellen Angriff beteiligt ist, einschließlich einer Grafik der Top-Aktivität für den Benutzer.

Seite zu Warnungen (Dieses Beispiel zeigt einen potenziellen Ransomware-Angriff
auf):



Detailseite (dieses Beispiel zeigt einen potenziellen Ransomware-Angriff.):

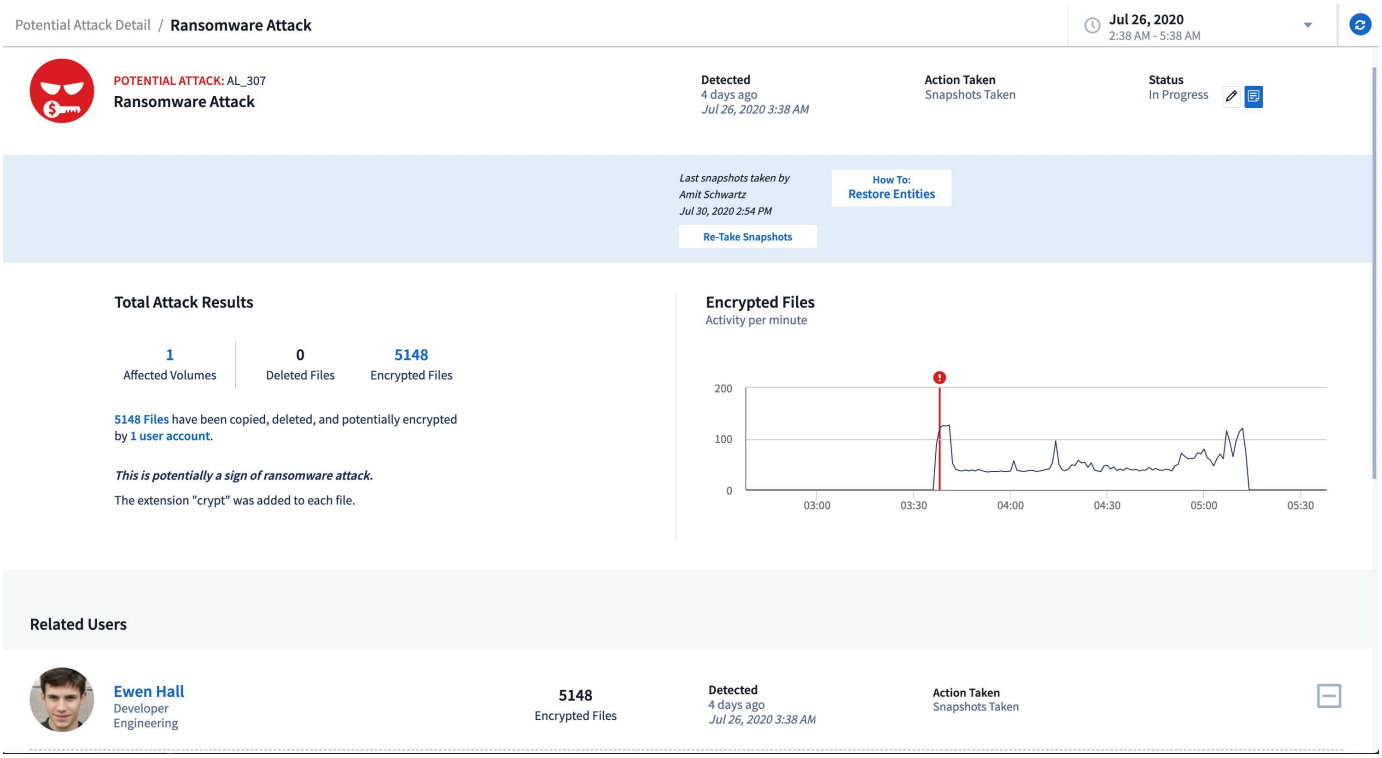


Snapshot Aktion durchführen

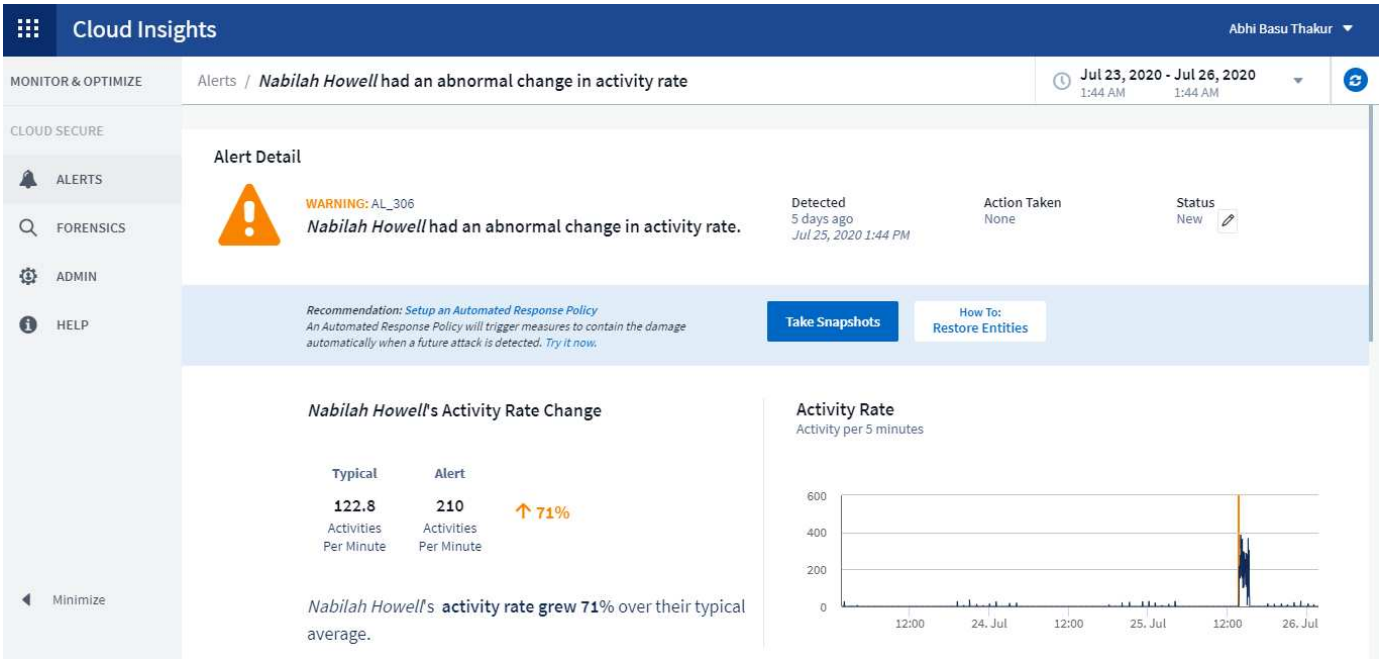
Workload Security schützt Ihre Daten, indem bei Erkennung schädlicher Aktivitäten automatisch ein Snapshot erstellt wird. So wird sichergestellt, dass Ihre Daten sicher gesichert werden.

Sie können definieren "Automatisierte Antwortrichtlinien" Die einen Snapshot machen, wenn Ransomware-Angriff oder eine andere abnormale Benutzeraktivität erkannt wird. Sie können einen Snapshot auch manuell von der Warnungsseite aus erstellen.

Automatische
Momentaufnahme:



Manuelle Momentaufnahme:



Warnbenachrichtigungen

Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an eine Benachrichtigungsliste gesendet. Um Warnungsempfänger zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse ein.

Aufbewahrungsrichtlinie

Warnungen und Warnungen werden 13 Monate lang aufbewahrt. Warnungen und Warnungen, die älter als 13

Monate sind, werden gelöscht. Wenn die Workload-Sicherheitsumgebung gelöscht wird, werden auch alle mit der Umgebung verknüpften Daten gelöscht.

Fehlerbehebung

Problem:	Versuchen Sie Das:
Es besteht die Situation, dass ONTAP stündliche Snapshots pro Tag erstellt. Wirken sich Workload Security (WS)-Snapshots darauf aus? Wird WS-Schnappschuss den stündlichen Schnappschuss-Platz machen? Wird der stündliche StandardSnapshot angehalten?	Arbeitslastsicherheit Schnappschüsse werden die stündlichen Schnappschüsse nicht beeinflussen. WS-Schnappschüsse nehmen nicht den stündlichen Snapshot-Platz und das sollte so weitergehen wie zuvor. Der standardmäßige stündliche Snapshot wird nicht angehalten.
Was geschieht, wenn die Maximalanzahl der Snapshots in ONTAP erreicht wird?	Wenn die maximale Anzahl an Snapshots erreicht wird, schlägt das nachfolgende Erstellen eines Snapshots fehl, und die Workload-Sicherheit weist eine Fehlermeldung auf, dass der Snapshot voll ist. Benutzer müssen Snapshot-Richtlinien definieren, um die ältesten Snapshots zu löschen, sonst werden keine Snapshots erstellt. Ab ONTAP 9.3 und älteren Versionen kann ein Volume bis zu 255 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein Volume bis zu 1023 Snapshot Kopien enthalten. Weitere Informationen finden Sie in der ONTAP-Dokumentation "Richtlinie zum Löschen von Snapshots wird festgelegt".
Workload Security kann überhaupt keine Snapshots erstellen.	Stellen Sie sicher, dass die Rolle, die zum Erstellen von Snapshots verwendet wird, Link hat: proper Rechte zugewiesen. Stellen Sie sicher, dass *csrole* mit entsprechenden Zugriffsrechten für die Erstellung von Snapshots erstellt wird: Security Login role create -vserver <vservername> -role csrolle -cmddirname „Volume Snapshot“ -Access all
Snapshots versagen bei älteren Warnmeldungs-Warnungen auf SVMs, die aus der Workload Security entfernt und anschließend wieder hinzugefügt wurden. Für neue Warnmeldungen, die nach dem erneuten Hinzufügen der SVM auftreten, werden Snapshots erstellt.	Dies ist ein seltenes Szenario. Falls dies der Fall ist, melden Sie sich bei ONTAP an und erstellen Sie die Snapshots manuell, um die älteren Meldungen zu erhalten.
Auf der Seite „ Details der Warnmeldung “ wird die Meldung „Letzter Versuch fehlgeschlagen“ unter der Schaltfläche „*Take Snapshot*“ angezeigt. Wenn Sie den Fehler bewegen, wird „API-Befehl aufrufen hat Timeout für den Datensammler mit id“ angezeigt.	Dies kann passieren, wenn ein Datensammler zur Workload-Sicherheit über SVM Management IP hinzugefügt wird, wenn sich die LIF der SVM in ONTAP in „*dedisabled* State“ befindet. Aktivieren Sie die bestimmte LIF in ONTAP und lösen Sie _Snapshot manuell aus der Workload-Sicherheit aus. Die Aktion „Snapshot“ wird dann erfolgreich ausgeführt.

Forensik

Forensik - Alle Aktivitäten

Auf der Seite Alle Aktivitäten können Sie die Aktionen verstehen, die für Einheiten in der Workload-Sicherheitsumgebung durchgeführt werden.

Alle Aktivitätsdaten Werden Untersucht

Klicken Sie auf **Forensics > Vorgangsforensics** und klicken Sie auf die Registerkarte **Alle Aktivitäten**, um die Seite Alle Aktivitäten aufzurufen. Diese Seite bietet einen Überblick über Aktivitäten in Ihrer Umgebung und hebt die folgenden Informationen hervor:

- Ein Diagramm mit „*Aktivitätsverlauf*“ (Zugriff pro Minute/pro 5 Minuten/pro 10 Minuten basierend auf dem ausgewählten globalen Zeitbereich)

  Sie können das Diagramm vergrößern, indem Sie ein Rechteck im Diagramm herausziehen. Die gesamte Seite wird geladen, um den vergrößerten Zeitbereich anzuzeigen. Wenn der Zoom vergrößert wird, wird eine Schaltfläche angezeigt, mit der der Benutzer zoomen kann.

- Ein Diagramm mit „*Aktivitätstypen*“. Um die Vorgangshistorie-Daten nach Aktivitätstyp zu erhalten, klicken Sie auf den entsprechenden x-Achse-Label-Link.
- Ein Diagramm der Aktivität auf_Entity Types_. Um Vorgangsdaten nach Entitätstyp zu erhalten, klicken Sie auf den entsprechenden Link für die X-Achse-Bezeichnung.
- Eine Liste der Daten „*Alle Aktivitäten*“

Die Tabelle **Alle Aktivitäten** enthält die folgenden Informationen. Beachten Sie, dass standardmäßig nicht alle dieser Spalten angezeigt werden. Sie können Spalten auswählen, die angezeigt werden sollen, indem Sie auf das Zahnradsymbol klicken.

- Die **Zeit**, auf die ein Unternehmen zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der * Benutzer*, der mit einem Link auf das Entity zugegriffen hat "Benutzerinformationen".
- Die **Aktivität**, die der Benutzer durchgeführt hat. Folgende Typen werden unterstützt:
  - **Gruppeneigentum ändern** - Gruppeneigentum ist von Datei oder Ordner geändert. Weitere Informationen zu Gruppeneigentum finden Sie unter "Dieser Link."
  - **Eigentümer ändern** - das Eigentum an Datei oder Ordner wird zu einem anderen Benutzer geändert.
  - **Berechtigung ändern** - Datei- oder Ordnerrechte wurde geändert.
  - **Erstellen** - Erstellen Sie Datei oder Ordner.
  - **Löschen** - Datei oder Ordner löschen. Wenn ein Ordner gelöscht wird, werden *delete* Ereignisse für alle Dateien in diesem Ordner und Unterordnern abgerufen.
  - **Lesen** - Datei wird gelesen.
  - **Metadaten lesen** - nur bei Option zur Ordnerüberwachung. Wird beim Öffnen eines Ordners unter Windows erzeugt oder „ls“ innerhalb eines Ordners unter Linux ausgeführt.
  - **Umbenennen** - Umbenennen Sie die Datei oder den Ordner.
  - **Schreiben** - Daten werden in eine Datei geschrieben.
  - **Metadaten schreiben** - Dateimetadaten werden geschrieben, zum Beispiel, Berechtigung geändert.
  - **Andere Änderung** - jedes andere Ereignis, das oben nicht beschrieben wird. Alle nicht zugeordneten Ereignisse werden dem Aktivitätstyp „andere Änderung“ zugeordnet. Gilt für Dateien und Ordner.

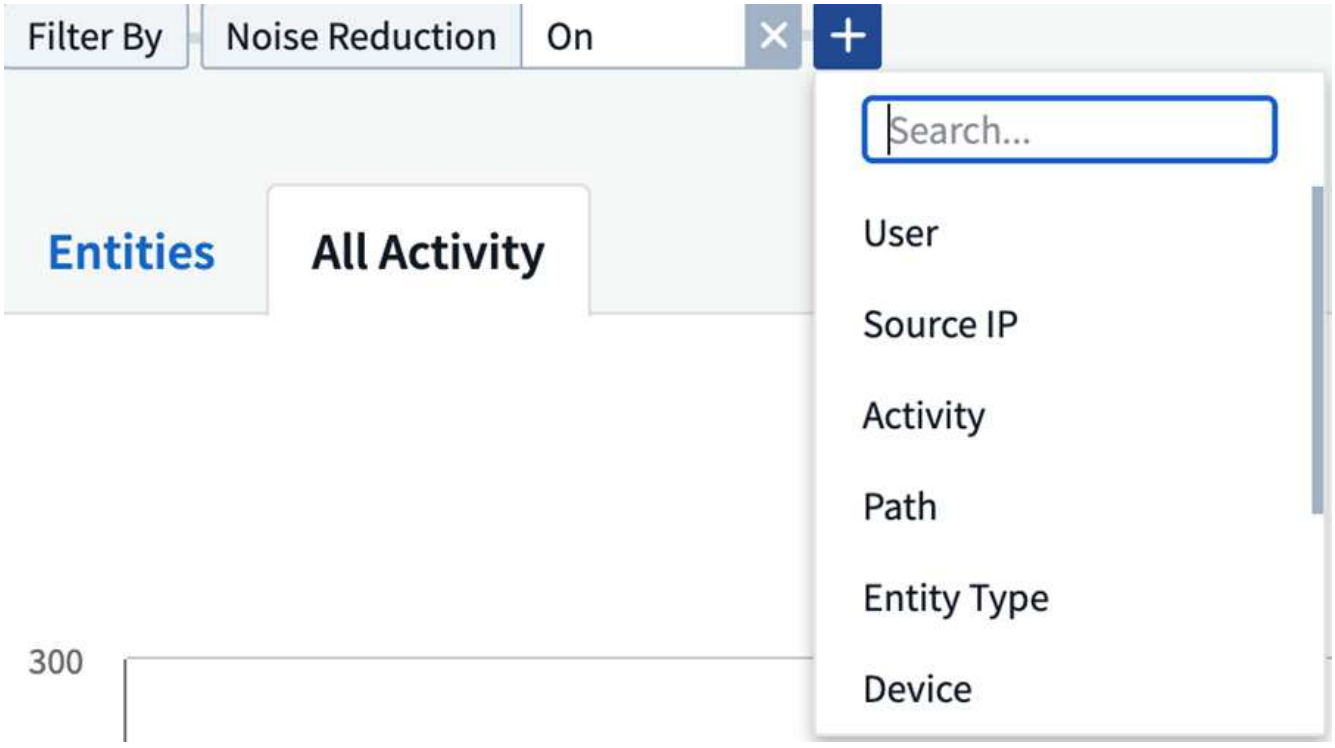
- Der **Pfad** zur Entität mit einem Link zum "Entity Detail-Daten"
- **Entity Type**, einschließlich der Endung Entity (d. h. Datei) (.doc, .docx, .tmp usw.)
- Das **Gerät**, in dem sich die Entitäten befinden
- Das **Protokoll** zum Abrufen von Ereignissen.
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.
- Das **Volumen**, in dem sich die Entitäten befinden. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.

Filtern Forensischer Vorgangshistorie-Daten

Es gibt zwei Methoden, mit denen Sie Daten filtern können.

1. Bewegen Sie den Mauszeiger über das Feld in der Tabelle, und klicken Sie auf das angezeigte Filtersymbol. Der Wert wird den entsprechenden Filtern in der oberen Liste *Filter by* hinzugefügt.
2. Filtern Sie die Daten, indem Sie das Feld *Filter by* eingeben:

   Wählen Sie den entsprechenden Filter aus dem oberen Widget ‘Filtern nach’ aus, indem Sie auf die Schaltfläche **[+]** klicken:



   Geben Sie den Suchtext ein

   Drücken Sie die Eingabetaste, oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

Sie können forensische Aktivitätsdaten nach folgenden Feldern filtern:

- Der Typ **Aktivität**.

- **Quell-IP**, auf die das Element zugegriffen wurde. Sie müssen eine gültige Quell-IP-Adresse in doppelten Anführungszeichen angeben, z. B. „10.1.1.1.“. Unvollständige IPs wie „10.1.1.**“, „10.1.**.*“ usw. funktionieren nicht.
- **Protokoll** zum Abrufen protokollspezifischer Aktivitäten.
- **Benutzername** des Benutzers, der die Aktivität ausführt. Sie müssen den genauen Benutzernamen angeben, um sie zu filtern. Die Suche mit teilweisen Nutzernamen oder teilweisen Nutzernamen, vorfixiert oder mit ‘*’ abgestickt, funktioniert nicht.
- **Rauschunterdrückung** zum Filtern von Dateien, die in den letzten 2 Stunden vom Benutzer erstellt werden. Sie wird auch zum Filtern temporärer Dateien (z. B. .tmp-Dateien) verwendet, auf die der Benutzer Zugriff hat.
- **Domain** des Benutzers, der die Aktivität ausführt. Sie müssen die **genaue Domain** angeben, um zu filtern. Die Suche nach einer partiellen Domäne oder einer partiellen Domäne mit Präfix oder Suffix mit Platzhalter ('*') funktioniert nicht. *None* kann angegeben werden, um nach fehlender Domain zu suchen.

Die folgenden Felder unterliegen speziellen Filterregeln:

- **Entity Type**, mit Entity (File) Extension - es ist vorzuziehen, den genauen Entity-Typ in Anführungszeichen anzugeben. Beispiel: _ „Txt“_.
- **Pfad** der Entity - Verzeichnispfad-Filter (Pfadstring endet mit /) für schnellere Ergebnisse werden bis zu 4 Verzeichnisse empfohlen. Beispiel: */Home/userX/nested1/nested2/* ODER *“/Home/userX/nested1/nested2/“*. Weitere Informationen finden Sie in der folgenden Tabelle.
- **User** die Aktivität durchführen - es ist vorzuziehen, den genauen Benutzer in Anführungszeichen anzugeben. Beispiel: _ „Administrator“_.
- **Gerät** (SVM), in dem sich Entitäten befinden
- **Volumen**, in dem sich Entitäten befinden
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird.

Die vorhergehenden Felder unterliegen beim Filtern folgenden Kriterien:

- Der genaue Wert sollte in Anführungszeichen liegen: Beispiel: "suchtext"
- Platzhalter-Strings dürfen keine Anführungszeichen enthalten: Beispiel: suchtext, *suchtext*, filtert nach Zeichenfolgen, die ‘seartext’ enthalten.
- String mit einem Präfix, Beispiel: suchtext* , sucht alle Strings, die mit ‘seartext’ beginnen.

Beispiele Für Forensik-Filter Für Aktivitäten:

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Performance-Assessment	Kommentar
Pfad = /Home/userX/nested1/nested2/ oder /Home/userX/nested1/nested2/* oder "/Home/userX/nested1/nested2/"	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Schnell	Verzeichnissuchen bis zu 4 Verzeichnisse werden schnell sein.

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Performance-Assessment	Kommentar
Pfad = /Home/userX/nested1/ oder /Home/userX/nested1/* oder "/Home/userX/nested1/"	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Schnell	Verzeichnissuchen bis zu 4 Verzeichnisse werden schnell sein.
Pfad = /Home/userX/nested1/Test* oder /Home/userX/nested1/Test	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Pfad regex(Test* könnte Datei ODER Verzeichnis ODER beides bedeuten)	Langsamer	Die Suche nach Verzeichnis+Datei ist langsamer als bei Verzeichnissuchen.
Pfad = /Home/userX/nested1/nested2/nested3/ oder /Home/userX/nested1/nested2/nested3/* oder "/Home/userX/nested1/nested2/nested3/"	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Langsamer	Mehr als 4 Verzeichnissuchen sind langsamer zu suchen.
Pfad=*userX/nested1/Test*	Rekursive Abfrage aller Dateien und Ordner unter der angegebenen Platzhalterpfad-Zeichenfolge (Test* kann Datei ODER Verzeichnis ODER beides bedeuten)	Langsam	Führende Platzhaltersuche sind langsamste Suchvorgänge.
Alle anderen nicht pfadbasierten Filter. Benutzer- und Entitätstyp-Filter, die in Anführungszeichen empfohlen werden, z. B. Benutzer=„Administrator“ Entitätstyp=„txt“		Schnell	

HINWEIS:

1. Die Anzahl der Aktivitäten, die neben dem Symbol „Alle Aktivitäten“ angezeigt wird, wird auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst. In einem Zeitraum von _1. September 10:15 bis 7. September 10:15 werden die Aktivitätszahlen vom 1. September 10:00 bis 7. September 10:30 Uhr angezeigt.
2. Ebenso werden die Zählmetriken in Aktivitätstypen, Aktivität auf Entitätstypen und Aktivitätsverlauf auf 30 Minuten abgerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst.

Forensische Vorgangshistorie-Daten Sortieren

Sie können Daten aus dem Aktivitätsverlauf nach *Zeit, Benutzer, Quell-IP, Aktivität,* und *Entitätstyp* sortieren. Standardmäßig wird die Tabelle nach absteigender_Time_-Reihenfolge sortiert, was bedeutet, dass die

neuesten Daten zuerst angezeigt werden. Die Sortierung ist für die Felder *Device* und *Protocol* deaktiviert.

Benutzerhandbuch für asynchrone Exporte

Überblick

Die Funktion „asynchrone Exporte“ in „Storage Workload Security“ wurde für die Verarbeitung großer Datenexporte entwickelt.

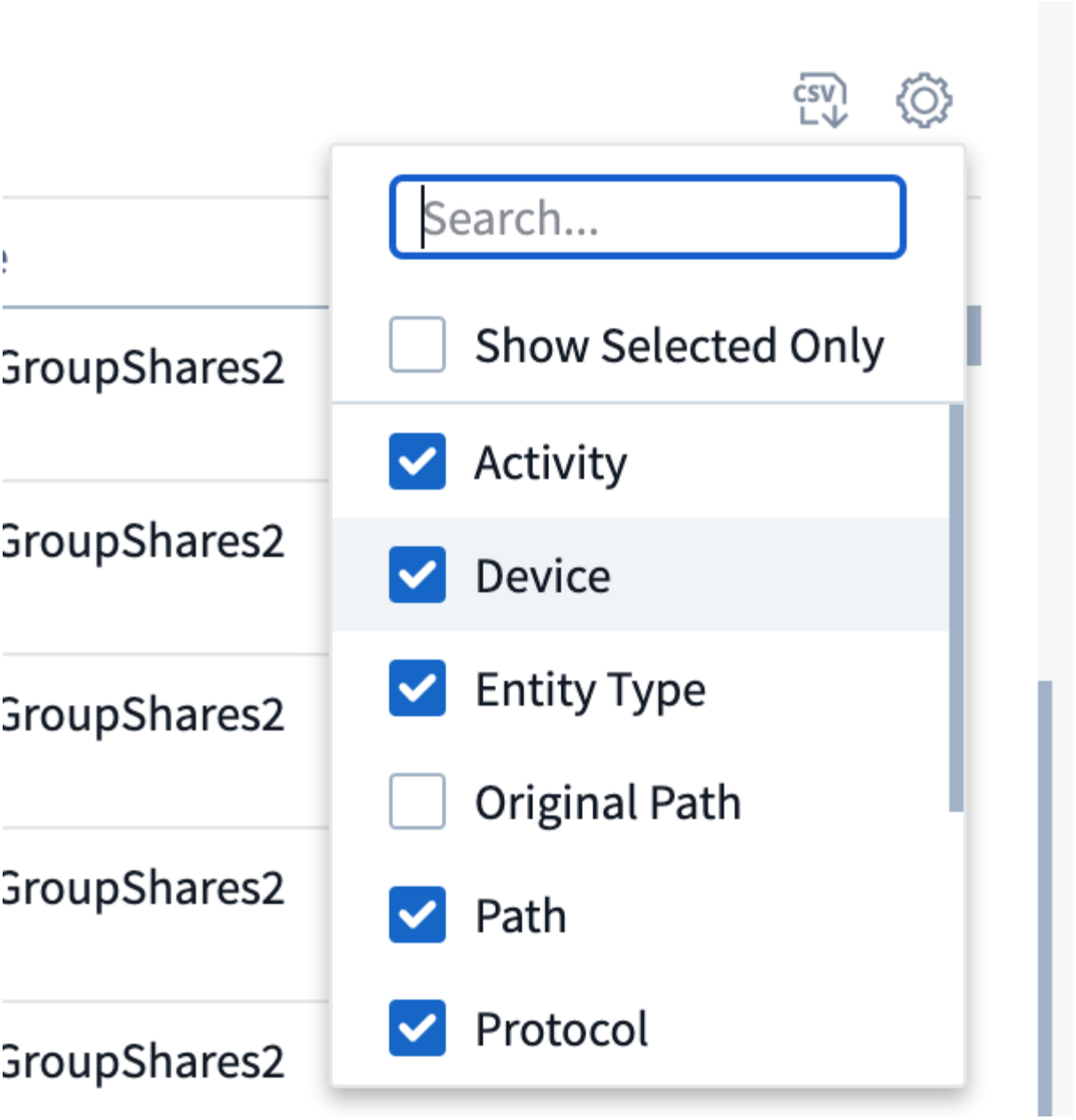
Schritt-für-Schritt-Anleitung: Daten mit asynchronen Exporten exportieren

1. **Export starten**: Wählen Sie die gewünschte Zeitdauer und Filter für den Export aus und klicken Sie auf den Export-Button.
2. **Wait for Export to complete**: Die Verarbeitungszeit kann von ein paar Minuten bis zu einigen Stunden betragen. Unter Umständen müssen Sie die Seite „Forensik“ einige Male aktualisieren. Sobald der Exportauftrag abgeschlossen ist, wird die Schaltfläche "Letzten Export CSV-Datei herunterladen" aktiviert.
3. **Download**: Klicken Sie auf den Button "Download Last created Export file", um die exportierten Daten im .zip-Format zu erhalten. Diese Daten können heruntergeladen werden, bis der Benutzer einen anderen asynchronen Export initiiert oder 3 Tage vergangen sind, je nachdem, was zuerst eintritt. Die Schaltfläche bleibt aktiviert, bis ein anderer asynchroner Export gestartet wird.
4. **Einschränkungen**:
    - Die Anzahl asynchroner Downloads ist derzeit auf 1 pro Benutzer und 3 pro Mandant begrenzt.
    - Die exportierten Daten sind auf maximal 1 Million Datensätze begrenzt.

Ein Beispielskript zum Extrahieren forensischer Daten über API ist auf dem Agenten unter */opt/NetApp/CloudSecure/Agent/Export-script/* vorhanden. Weitere Informationen zum Skript finden Sie in der Infodatei an dieser Stelle.

Spaltenauswahl für Alle Aktivitäten

In der Tabelle *Alle Aktivitäten* werden standardmäßig ausgewählte Spalten angezeigt. Um die Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle und wählen Sie aus der Liste der verfügbaren Spalten aus.



Aufbewahrung Des Aktivitätsverlaufs

Der Aktivitätsverlauf wird 13 Monate lang in aktiven Workload-Sicherheitsumgebungen aufbewahrt.

Anwendbarkeit von Filtern in Forensics Seite

Filtern	Das macht es	Beispiel	Gilt für diese Filter	Gilt nicht für diese Filter	Ergebnis
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	Auto*03172022 Wenn der Suchtext Bindestrich oder Unterstrich enthält, geben Sie den Ausdruck in Klammern an, z. B. (svm*) für die Suche nach svm-123	Benutzer, PFAD, Einheitstyp, Gerät, Volume, ursprünglicher Pfad		Gibt alle Ressourcen zurück, die mit „Auto“ beginnen und mit „03172022“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	AutoSabotageUser1_03172022?	Benutzer, Einheitstyp, Gerät, Volume		Gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 usw. zurück
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022	Benutzer, Domäne, PFAD, Entitätstyp, ursprünglicher Pfad		Gibt eine beliebige von AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT automatisch BefreiUser4_03162022	Benutzer, Domäne, PFAD, Entitätstyp, ursprünglicher PFAD	Gerät	Gibt alles zurück, was nicht mit "AutoBefreiUser4_03162022" beginnt
Keine	Sucht in allen Feldern nach Null-Werten	Keine	Domäne		Gibt Ergebnisse an, bei denen das Zielfeld leer ist

Pfadsuche/Original-Pfadsuche

Suchergebnisse mit und ohne / werden unterschiedlich sein

/AutoDir1/AutoFile	Funktioniert
AutoDir1/AutoFile	Funktioniert nicht
/AutoDir1/AutoFile (Dir1)	Dir1 partielle Substring funktioniert nicht
„/AutoDir1/AutoFile03242022“	Genaue Suche funktioniert

Auto*03242022	Funktioniert nicht
AutoSabotageUser1_03172022?	Funktioniert nicht
/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1	Funktioniert
NICHT /AutoFile03242022	Funktioniert nicht
*	Zeigt alle Einträge an

Lokale Root-SVM-Benutzeraktivitäten ändern sich

Wenn ein lokaler Root-SVM-Benutzer eine Aktivität ausführt, wird die IP des Clients, auf dem die NFS-Freigabe gemountet ist, jetzt im Benutzernamen berücksichtigt, der sowohl auf forensischen Aktivitäten als auch auf Benutzeraktivitäts-Seiten als Root@<ip-address-of-the-client> angezeigt wird.

Beispiel:

- Wenn SVM-1 von Workload Security überwacht wird und der Root-Benutzer dieser SVM die Freigabe auf einem Client mit der IP-Adresse 10.197.12.40 mountet, lautet der auf der Seite für forensische Aktivitäten angezeigte Benutzername *root@10.197.12.40*.
- Wenn dieselbe SVM-1 in einen anderen Client mit der IP-Adresse 10.197.12.41 eingebunden wird, lautet der auf der Seite für forensische Aktivitäten angezeigte Benutzername *root@10.197.12.41*.

*• Dies wird getan, um NFS-Root-Benutzeraktivität durch IP-Adresse zu trennen. Zuvor wurde die gesamte Aktivität als vom *root*-Benutzer durchgeführt betrachtet, ohne IP-Unterscheidung.

Fehlerbehebung

Problem	Versuchen Sie Dies

In der Tabelle „Alle Aktivitäten“ in der Spalte ‘Benutzer“ wird der Benutzername wie folgt angezeigt: „ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” oder LDAP:default:80038003“	Mögliche Gründe sind: 1. Es wurden noch keine User Directory Collectors konfiguriert. Um einen hinzuzufügen, gehen Sie zu **Workload Security > Collectors > User Directory Collectors** und klicken Sie auf **+User Directory Collector**. Wählen Sie *Active Directory* oder *LDAP Directory Server*. 2. Ein Benutzerverzeichnissammler wurde konfiguriert, ist jedoch angehalten oder befindet sich im Fehlerzustand. Bitte gehen Sie zu **Collectors > User Directory Collectors** und überprüfen Sie den Status. Siehe "Fehlerbehebung für Benutzerverzeichnissammler" Der Dokumentation für Tipps zur Fehlerbehebung. Nach der ordnungsgemäßen Konfiguration wird der Name innerhalb von 24 Stunden automatisch behoben. Wenn die Lösung immer noch nicht behoben wird, überprüfen Sie, ob Sie den korrekten Benutzer-Data Collector hinzugefügt haben. Stellen Sie sicher, dass der Benutzer tatsächlich Teil des hinzugefügten Active Directory/LDAP Directory Servers ist.
Einige NFS-Ereignisse werden in der UI nicht angezeigt.	Überprüfen Sie Folgendes: 1. Ein Benutzer-Verzeichnis-Collector für AD-Server mit POSIX-Attributen sollte mit dem unixid-Attribut ausgeführt werden, das über UI aktiviert ist. 2. Jeder Benutzer, der NFS-Zugang macht, sollte angezeigt werden, wenn er in der Benutzerseite von UI 3 durchsucht wird. RAW-Ereignisse (Ereignisse, für die der Benutzer noch nicht erkannt wurde) werden für NFS 4 nicht unterstützt. Anonymer Zugriff auf den NFS-Export wird nicht überwacht. 5. Stellen Sie sicher, dass die NFS-Version in weniger als NFS4.1 verwendet wird.
Nachdem Sie einige Buchstaben mit einem Platzhalterzeichen wie Sternchen (*) in die Filter auf den Seiten Forensics *All Activity* oder *entities* eingegeben haben, werden die Seiten sehr langsam geladen.	Ein Sternchen (*) in der Suchzeichenfolge sucht nach allem. Führende Platzhalterzeichenfolgen wie *<*searchTerm*>* oder *<*searchTerm*>** führen jedoch zu einer langsamen Abfrage. Um eine bessere Leistung zu erzielen, verwenden Sie stattdessen Präfix-Strings im Format <*searchTerm*>* (mit anderen Worten: Fügen Sie das Sternchen (*) *nach* einem Suchbegriff hinzu). Beispiel: Verwenden Sie den String *testvolume** anstatt **testvolume* oder **Test*Volume*. Verwenden Sie eine Verzeichnissuche, um alle Aktivitäten unterhalb eines bestimmten Ordners rekursiv anzuzeigen (hierarchische Suche). Z.B. werden unter /path1/path2/path3/ oder „/path1/path2/path3/“ alle Vorgänge rekursiv unter /path1/path2/path3 aufgelistet. Alternativ können Sie die Option „zum Filter hinzufügen“ unter der Registerkarte „Alle Aktivitäten“ verwenden.

Bei der Verwendung eines Pfadfilters tritt ein Fehler „Anfrage fehlgeschlagen mit Statuscode 500/503“ auf.	Versuchen Sie, einen kleineren Datumsbereich zum Filtern von Datensätzen zu verwenden.
Die forensische Benutzeroberfläche lädt Daten langsam, wenn der *PATH*-Filter verwendet wird.	Verzeichnispfad-Filter (Pfadstring endet mit /) für schnellere Ergebnisse werden bis zu 4 Verzeichnisse empfohlen. Beispiel: Wenn der Verzeichnispfad /AAA/BBB/CCC/DDD ist, versuchen Sie, nach /AAA/BBB/CCC/DDD/ oder „/AAA/BBB/CCC/DDD/“ zu suchen, um Daten schneller zu laden.

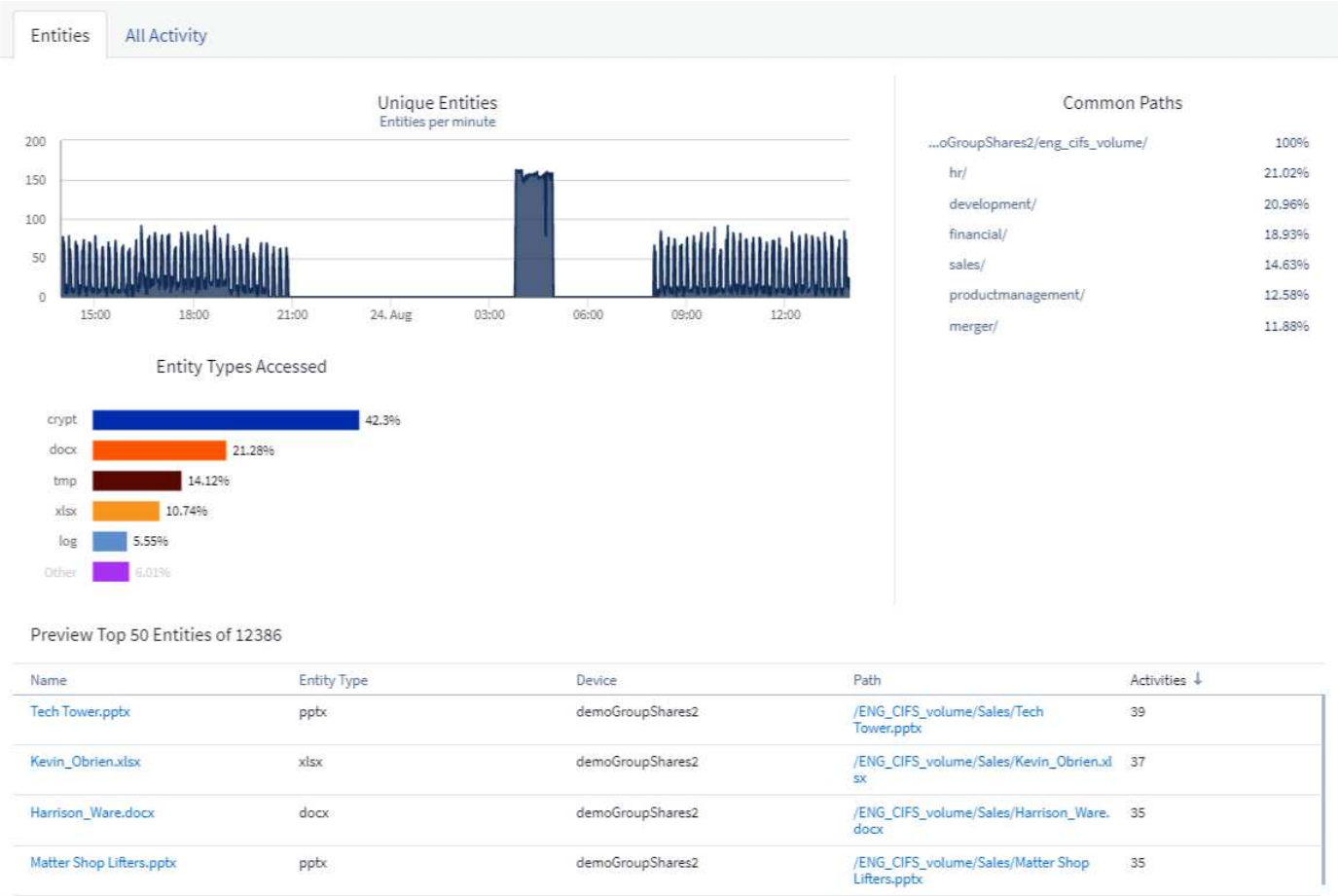
Seite Mit Forensischen Einheiten

Die Seite Forensics Entities enthält detaillierte Informationen über die Aktivität der Entität in Ihrer Umgebung.

Untersuchung Von Informationen Zur Einheit

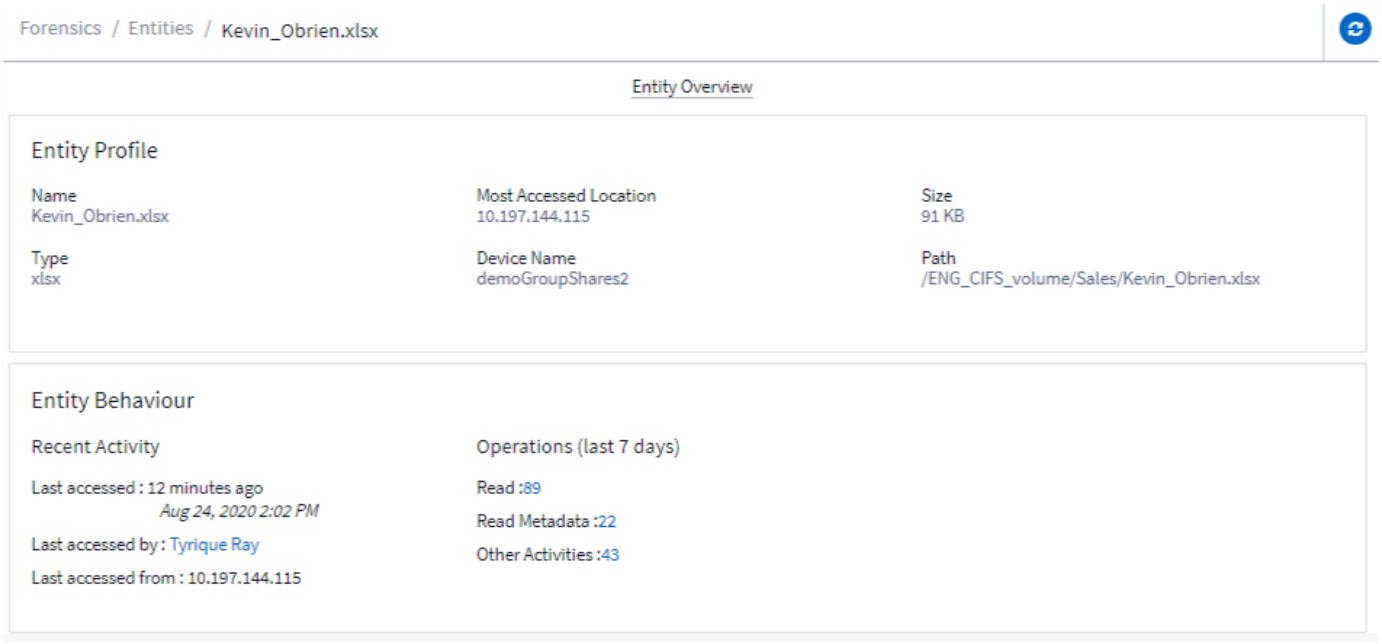
Klicken Sie auf **Forensics > Vorgangsforensics**, und klicken Sie auf die Registerkarte *Entities*, um die Seite Entities aufzurufen.

Auf dieser Seite erhalten Sie einen Überblick über die Aktivitäten der Einheit in Ihrer Umgebung, und Sie können die folgenden Informationen hervorheben: * Ein Diagramm mit_eindeutigen Entitäten_ Zugriffsberechtigung pro Minute * Ein Diagramm mit_Entity-Typen, auf die zugegriffen wurde_ * Eine Aufschlüsselung der_Common Paths_ * Eine Liste der *Top 50 Entities* von der Gesamtanzahl der Entitäten



Durch Klicken auf eine Entität in der Liste wird eine Übersichtsseite für die Entität geöffnet, auf der ein Profil

der Entität mit Details wie Name, Typ, Gerätename, IP-Adresse und Pfad sowie das Entity-Verhalten wie Benutzer, IP, Und die Zeit, zu der das Unternehmen zuletzt aufgerufen wurde.



Übersicht Über Forensische Benutzer

Informationen zu jedem Benutzer finden Sie in der Benutzerübersicht. Verwenden Sie diese Ansichten, um Benutzereigenschaften, zugehörige Einheiten und aktuelle Aktivitäten zu verstehen.

Benutzerprofil

Zu den Benutzerprofilinformationen gehören die Kontaktinformationen und der Standort des Benutzers. Das Profil enthält folgende Informationen:

- Name des Benutzers
- E-Mail-Adresse des Benutzers
- Benutzermanager
- Telefonkontakt für den Benutzer
- Standort des Benutzers

Benutzerverhalten

Die Informationen zum Benutzerverhalten identifizieren aktuelle Aktivitäten und Vorgänge, die vom Benutzer durchgeführt werden. Zu diesen Informationen gehören:

- Aktuelle Aktivität
  - Letzter Zugriffsort
  - Aktivitätsdiagramm
  - Meldungen
- Betrieb der letzten sieben Tage

- Anzahl an Operationen

Intervall Aktualisieren

Die Benutzerliste wird alle 12 Stunden aktualisiert.

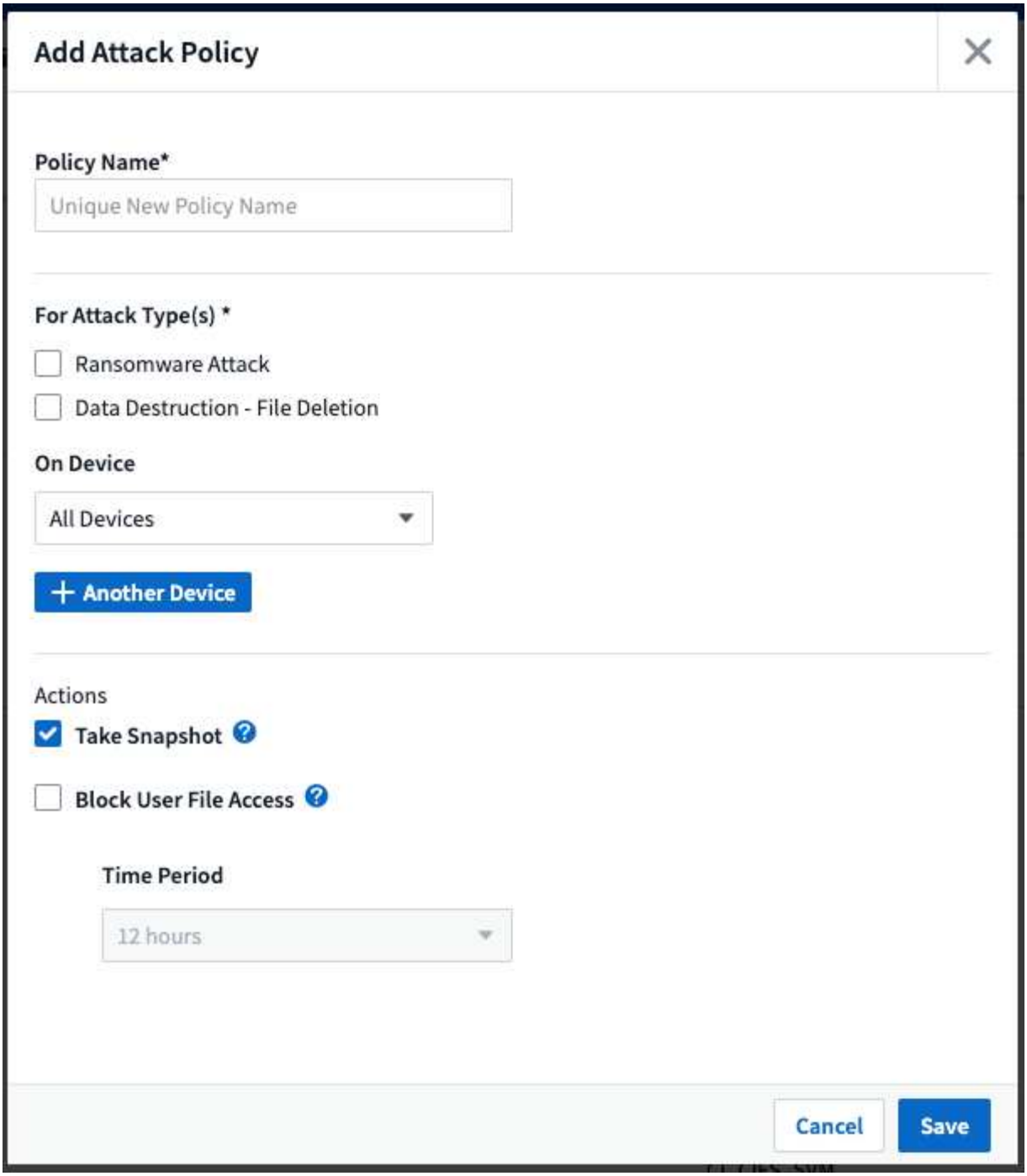
Aufbewahrungsrichtlinie

Wenn die Benutzerliste nicht erneut aktualisiert wird, wird sie 13 Monate lang aufbewahrt. Nach 13 Monaten werden die Daten gelöscht. Wenn die Workload-Sicherheitsumgebung gelöscht wird, werden alle der Umgebung zugeordneten Daten gelöscht.

Automatisierte Antwortrichtlinien

Antwortrichtlinien lösen Aktionen aus, wie z. B. das Erstellen eines Snapshots oder das Einschränken des Benutzerzugriffs bei einem Angriff oder einem anormalen Benutzerverhalten.

Sie können Richtlinien für bestimmte Geräte oder alle Geräte festlegen. Um eine Antwortrichtlinie festzulegen, wählen Sie **Admin > Automatische Antwortrichtlinien** aus und klicken Sie auf die entsprechende Schaltfläche **+Policy**. Sie können Richtlinien für Angriffe oder Warnungen erstellen.



Sie müssen die Richtlinie mit einem eindeutigen Namen speichern.

Um eine automatische Antwortzeit zu deaktivieren (z. B. Snapshot erstellen), überprüfen Sie einfach die Aktion und speichern Sie die Richtlinie.

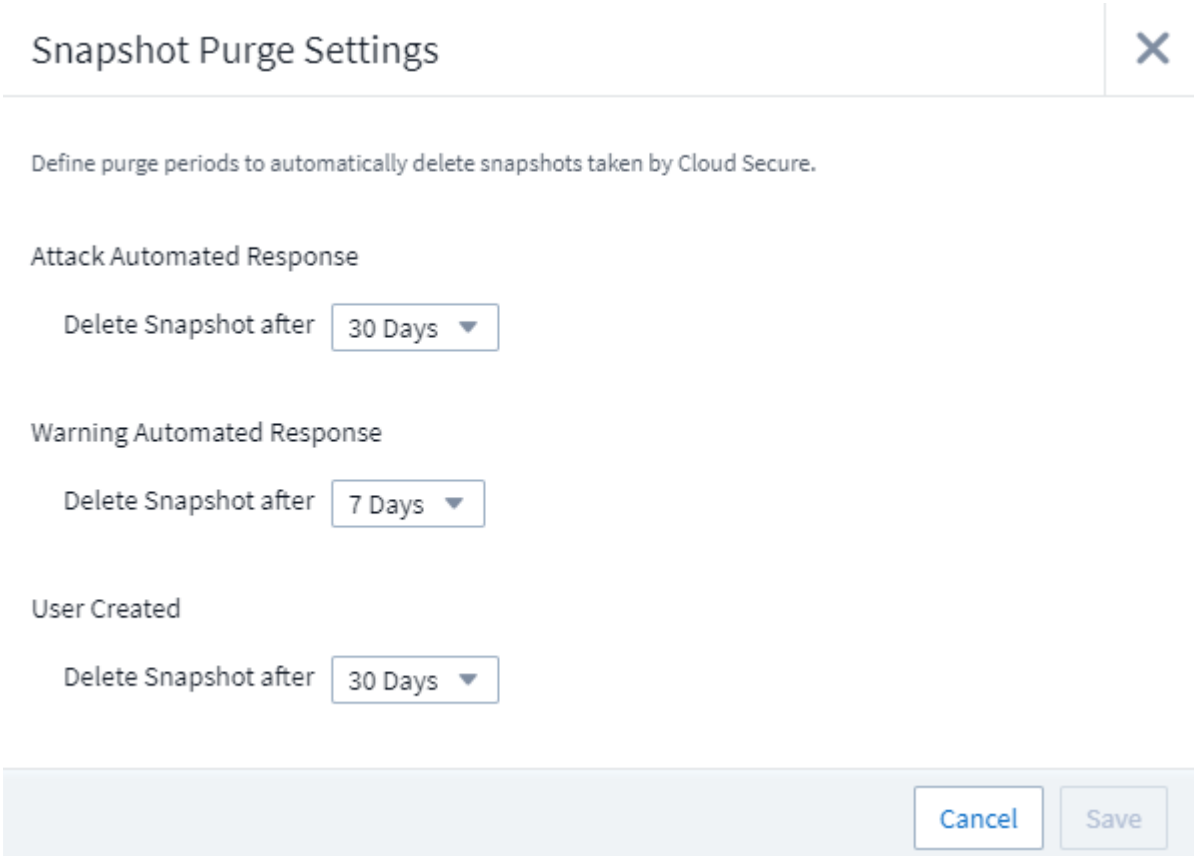
Wenn eine Warnung für die angegebenen Geräte (oder alle Geräte, falls ausgewählt) ausgelöst wird, erstellt die Richtlinie zur automatischen Reaktion einen Snapshot Ihrer Daten. Sie können den Snapshot-Status auf der sehen "Details zu Warnmeldungen".

Siehe "Einschränken Des Benutzerzugriffs" Seite für weitere Details zur Einschränkung des Benutzerzugriffs durch IP.

Sie können eine Richtlinie für automatische Reaktionen ändern oder anhalten, indem Sie die Option im

Dropdown-Menü der Richtlinie auswählen.

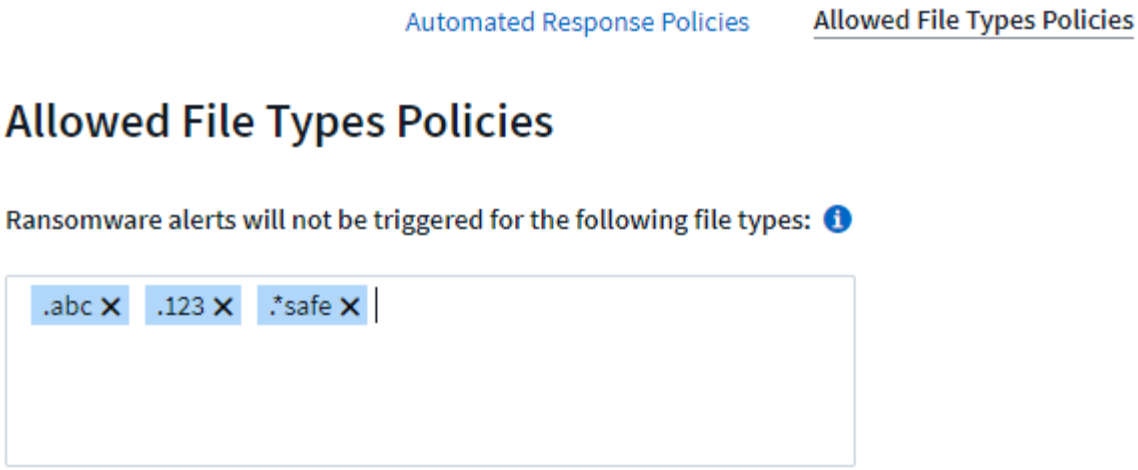
Workload Security löscht automatisch Snapshots einmal pro Tag auf Basis der Snapshot-Einstellungen.



Richtlinien Für Zulässige Dateitypen

Wenn ein Ransomware-Angriff auf eine bekannte Dateierweiterung erkannt wird und auf dem Bildschirm „Alerts“ Warnmeldungen generiert werden, kann diese Dateiendung zu einer Liste „Allowed file types_“ hinzugefügt werden, um unnötige Warnmeldungen zu vermeiden.

Navigieren Sie zu **Workload-Sicherheit > Richtlinien**, und wechseln Sie zur Registerkarte *allowed File Type Policies*.



Nach dem Hinzufügen zur Liste *allowed file types* wird für diesen zulässigen Dateityp keine Ransomware-Angriffswarnung generiert. Beachten Sie, dass die *allowed File Types*-Richtlinie nur für die Ransomware-Erkennung gilt.

Wenn beispielsweise eine Datei namens *Test.txt* in *Test.txt.abc* umbenannt wird und Workload Security einen Ransomware-Angriff aufgrund der Erweiterung *.abc* erkennt, kann die Erweiterung *.abc* zur Liste *allowed file types* hinzugefügt werden. Nachdem sie in die Liste aufgenommen wurde, werden Ransomware-Angriffe gegen Dateien mit der Erweiterung *.abc* nicht mehr ausgelöst.

Zulässige Dateitypen sind exakte Übereinstimmungen (z. B. ".abc") oder Ausdrücke (z. B. ".**type", ".type**" oder "**type**"). Ausdrücke der Typen ".a*c", ".p*f" werden nicht unterstützt.

Integration in ONTAP Autonomous Ransomware Protection

Die Funktion ONTAP Autonomous Ransomware Protection (ARP) verwendet Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Dateiaktivitäten proaktiv zu erkennen und zu warnen, die auf einen Ransomware-Angriff hinweisen könnten.

Weitere Details und Lizenzanforderungen zu ARP finden Sie "Hier".

Workload Security ist in ONTAP integriert, um ARP-Ereignisse zu empfangen, und bietet zusätzliche Analysen und automatische Antwortebenen.

Workload Security erhält die ARP-Ereignisse vom ONTAP und ergreift die folgenden Maßnahmen:

1. Korreliert Ereignisse der Volume-Verschlüsselung mit den Benutzeraktivitäten, um zu ermitteln, wer den Schaden verursacht.
2. Implementierung von Richtlinien zur automatischen Reaktion (falls definiert)
3. Bietet forensische Funktionen:
   - Ermöglichen Sie Kunden die Durchführung von Untersuchungen zu Datensicherheitsverletzungen.
   - Erkennen Sie, welche Dateien betroffen waren, sodass das Recovery schneller erfolgt und Untersuchungen zu Datensicherheitsverletzungen durchgeführt werden können.

Voraussetzungen

1. Minimale ONTAP-Version: 9.11.1
2. ARP-aktivierte Volumes. Einzelheiten zur Aktivierung von ARP finden Sie "Hier". ARP muss über den OnCommand System Manager aktiviert sein. Workload Security kann ARP nicht aktivieren.
3. Workload Security Collector sollte über Cluster-IP hinzugefügt werden.
4. Für diese Funktion sind Anmeldedaten auf Cluster-Ebene erforderlich. Das bedeutet, dass beim Hinzufügen der SVM Anmeldedaten für die Cluster-Ebene verwendet werden müssen.

Benutzerberechtigungen erforderlich

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, befolgen Sie die folgenden Schritte, um Workload Security-Berechtigungen zum Sammeln von ARP-bezogenen Informationen aus ONTAP zu erteilen.

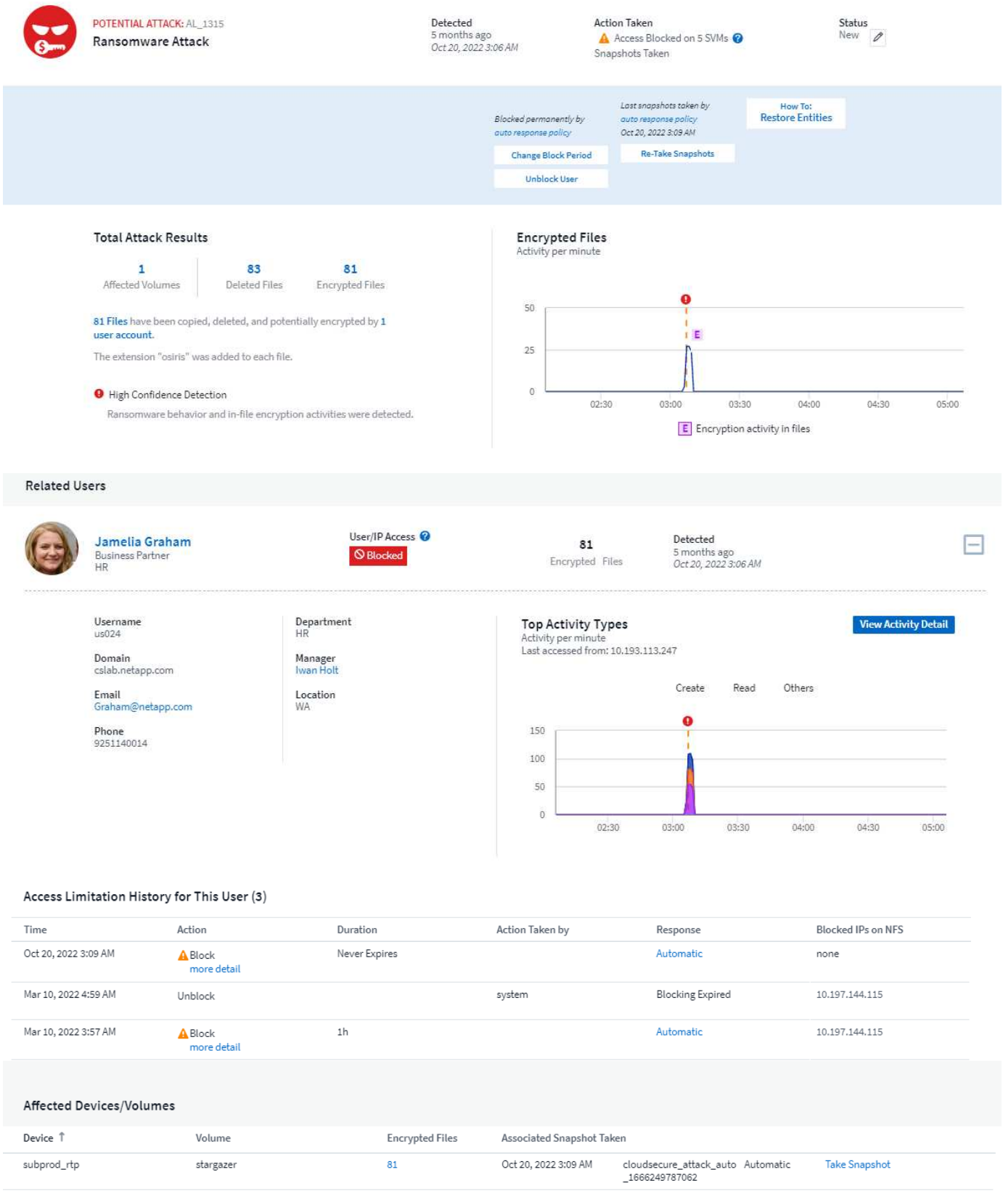
Führen Sie für *csuser* mit Cluster-Anmeldedaten folgende Schritte in der ONTAP-Befehlszeile aus:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Weitere Informationen zur Konfiguration anderer "ONTAP-Berechtigungen".

Beispielalarm

Im Folgenden wird eine Beispielwarnung angezeigt, die aufgrund eines ARP-Ereignisses generiert wurde:



Ein hochvertrauliches Banner zeigt auf, dass der Angriff das Verhalten von Ransomware zusammen mit Dateiverschlüsselungsaktivitäten gezeigt hat. Das Diagramm der verschlüsselten Dateien gibt den Zeitstempel an, mit dem die Volume-Verschlüsselungsaktivität von der ARP-Lösung erkannt wurde.

Einschränkungen

Wenn eine SVM nicht durch Workload-Sicherheit überwacht wird, aber durch ONTAP ARP-Ereignisse generiert werden, dann werden die Ereignisse weiterhin durch die Workload-Sicherheit empfangen und angezeigt. Es werden jedoch keine forensischen Informationen bezüglich der Warnmeldung und auch keine Benutzerzuordnung erfasst oder angezeigt.

Fehlerbehebung

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

Problem:	Auflösung:
E-Mail-Alarme werden 24 Stunden nach einem Angriff empfangen. In der UI werden die Warnmeldungen 24 Stunden vor dem Eingang der E-Mails bei Data Infrastructure Insights Workload Security angezeigt.	Wenn ONTAP das Ereignis „*Ransomware Detected*“ (Ransomware Detected_) an Data Infrastructure Insights Workload Security (d. h. Workload-Sicherheit) sendet, wird die E-Mail gesendet. Das Ereignis enthält eine Liste von Angriffen und Zeitstempel. Die Workload Security UI zeigt den Warnungszeitstempel der ersten angegriffenen Datei an. ONTAP sendet das *Ransomware Detected* Ereignis an Dateninfrastrukturerkennungen, wenn eine bestimmte Anzahl von Dateien codiert wird. Daher kann es einen Unterschied geben zwischen dem Zeitpunkt, zu dem die Warnung in der UI angezeigt wird, und dem Zeitpunkt, zu dem die E-Mail gesendet wird.

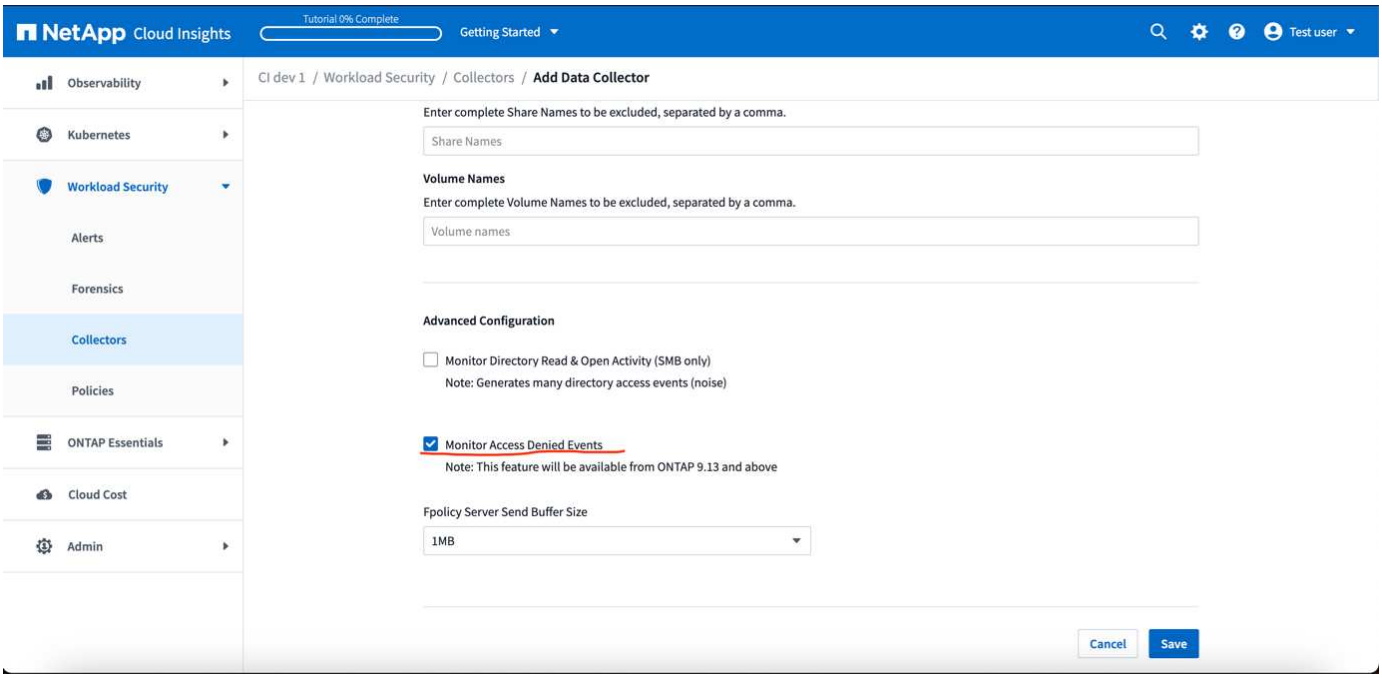
Integration mit ONTAP-Zugriff verweigert

Die ONTAP-Zugriffsverweigerung verwendet Workload-Analysen in NAS-Umgebungen (NFS und SMB), um proaktiv fehlgeschlagene Dateivorgänge zu erkennen und zu warnen (d. h. Benutzer, die versuchen, einen Vorgang auszuführen, für den sie keine Berechtigung haben). Diese Benachrichtigungen über fehlgeschlagene Dateioperationen – insbesondere bei sicherheitsrelevanten Fehlern – werden auch dazu beitragen, Insider-Angriffe frühzeitig zu blockieren.

Einblicke in die Dateninfrastruktur Workload Security lässt sich in ONTAP integrieren, um Ereignisse mit Zugriffsverweigerung zu empfangen und eine zusätzliche Analyse- und automatische Antwortebene bereitzustellen.

Voraussetzungen

- Minimale ONTAP-Version: 9.13.0.
- Ein Workload Security-Administrator muss die Funktion Zugriff verweigert aktivieren, während er einen neuen Collector hinzufügt oder vorhandene Collector bearbeitet, indem er das Kontrollkästchen *Zugriff verweigert überwachen* unter Erweiterte Konfiguration aktiviert.



Benutzerberechtigungen erforderlich

Wenn der Data Collector mithilfe der Anmeldeinformationen für die Clusteradministration hinzugefügt wird, sind keine neuen Berechtigungen erforderlich.

Wenn der Collector mithilfe eines benutzerdefinierten Benutzers (z. B. *csuser*) mit den Berechtigungen für den Benutzer hinzugefügt wird, führen Sie die folgenden Schritte aus, um Workload Security die erforderliche Berechtigung zur Registrierung für Ereignisse mit Zugangsverweigerung bei ONTAP zu erteilen.

Führen Sie für csuser mit *Cluster*-Anmeldeinformationen die folgenden Befehle über die ONTAP-Befehlszeile aus. Beachten Sie, dass *csrestrole* eine benutzerdefinierte Rolle ist und *csuser* ein benutzerdefinierter ONTAP-Benutzer ist.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

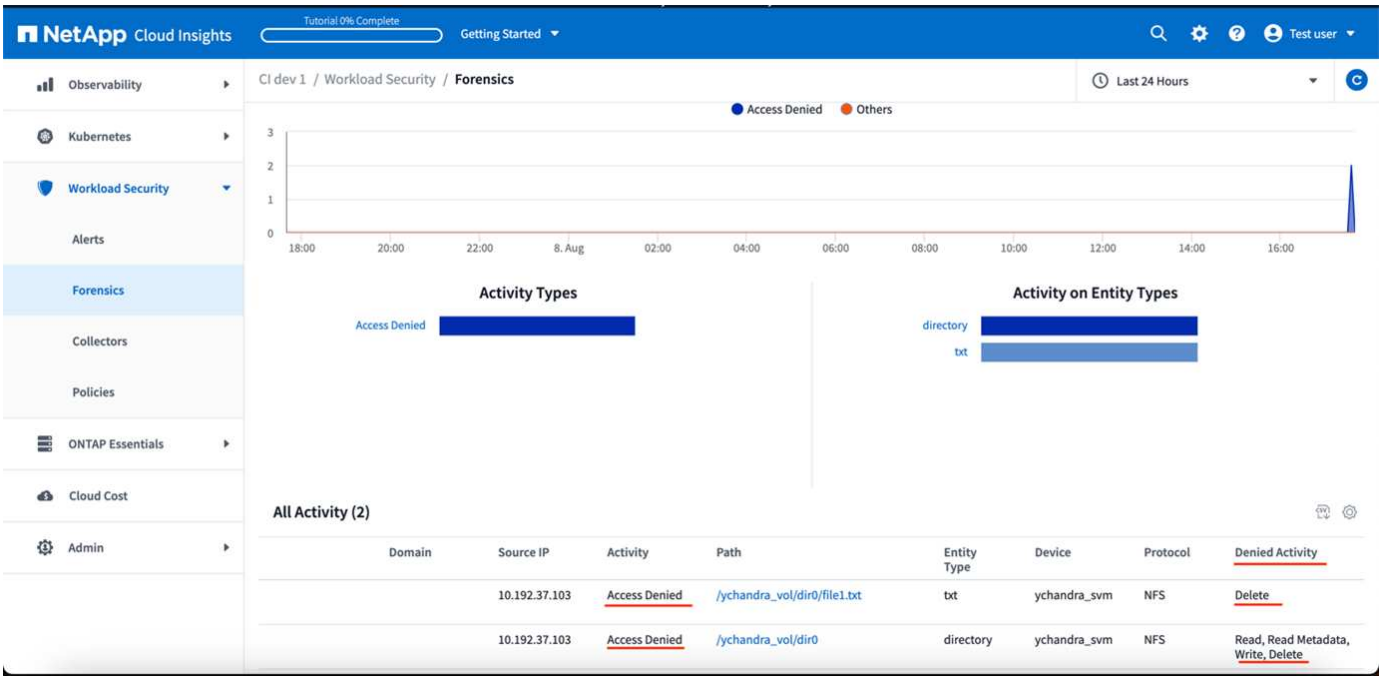
Führen Sie für csuser mit *SVM*-Anmeldeinformationen die folgenden Befehle über die ONTAP-Befehlszeile aus:

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Weitere Informationen zur Konfiguration anderer "ONTAP-Berechtigungen".

Zugriff verweigert Ereignisse

Sobald Ereignisse vom ONTAP-System erfasst wurden, werden auf der Seite Forensik für Workload-Sicherheit Ereignisse mit Zugriffsverweigerung angezeigt. Zusätzlich zu den angezeigten Informationen können Sie die fehlenden Benutzerberechtigungen für eine bestimmte Operation anzeigen, indem Sie die Spalte *gewünschte Aktivität* aus dem Zahnradsymbol zur Tabelle hinzufügen.



Blockieren Des Benutzerzugriffs

Sobald ein Angriff erkannt wurde, kann Workload Security den Angriff beenden, indem der Benutzerzugriff auf das Dateisystem blockiert wird. Der Zugriff kann automatisch mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden.

Beim Blockieren des Benutzerzugriffs sollten Sie einen Sperrzeitraum festlegen. Nach Ende des ausgewählten Zeitraums wird der Benutzerzugriff automatisch wiederhergestellt. Das Zugriffssperre wird sowohl für SMB- als auch für NFS-Protokolle unterstützt.

Benutzer ist direkt für SMB gesperrt und die IP-Adresse der Host Machines, die den Angriff verursachen, wird für NFS blockiert. Diese Computer-IP-Adressen dürfen nicht auf alle Storage Virtual Machines (SVMs) zugreifen, die durch Workload Security überwacht werden.

Zum Beispiel, sagen wir, Workload Security verwaltet 10 SVMs und die automatische Antwortrichtlinie ist für vier dieser SVMs konfiguriert. Wenn der Angriff in einer der vier SVMs stammt, wird der Zugriff des Benutzers in allen 10 SVMs blockiert. Auf der ursprünglichen SVM wird noch ein Snapshot erstellt.

Falls vier SVMs mit einer für SMB konfigurierten SVM und eine für NFS konfigurierte SVM und die übrigen beiden für NFS und SMB konfiguriert sind, werden alle SVMs blockiert, wenn der Angriff aus einer der vier SVMs stammt.

Voraussetzungen für die Sperrung des Benutzerzugriffs

Für diese Funktion sind Anmeldedaten auf Cluster-Ebene erforderlich.

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *cscuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, führen Sie die folgenden Schritte aus, um Workload Security-Berechtigungen zum Blockieren des Benutzers zu erteilen.

Führen Sie für CSuser mit Cluster-Anmeldedaten die folgenden Schritte in der ONTAP-Befehlszeile aus:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Überprüfen Sie unbedingt den Abschnitt Berechtigungen der "Konfiguration des ONTAP SVM Data Collector" Zu.

Wie wird die Funktion aktiviert?

- Navigieren Sie in Workload Security zu **Workload Security > Policies > Automated Response Policies**. Wählen Sie **+Angriffsrichtlinie**.
- Wählen Sie *Benutzerdateizugriff blockieren*.

Wie richten Sie die automatische Sperrung des Benutzerzugriffs ein?

- Erstellen Sie eine neue Angriffsrichtlinie oder bearbeiten Sie eine vorhandene Angriffsrichtlinie.
- Wählen Sie die SVMs aus, auf denen die Angriffsrichtlinie überwacht werden soll.
- Klicken Sie auf das Kontrollkästchen „Benutzerdateizugriff blockieren“. Die Funktion wird aktiviert, wenn diese Option ausgewählt ist.
- Wählen Sie unter „Zeitraum“ die Zeit aus, bis die Blockierung angewendet werden soll.
- Um die automatische Blockierung von Benutzern zu testen, können Sie einen Angriff über ein simulieren "Simuliertes Skript".

Wie kann man wissen, ob es blockierte Benutzer im System gibt?

- Auf der Seite Alarmlisten wird ein Banner oben auf dem Bildschirm angezeigt, falls ein Benutzer blockiert ist.
- Durch Klicken auf das Banner gelangen Sie zur Seite „Benutzer“, wo die Liste der blockierten Benutzer angezeigt wird.

- Auf der Seite „Benutzer“ befindet sich eine Spalte mit dem Namen „Benutzer/IP-Zugriff“. In dieser Spalte wird der aktuelle Status der Benutzerblockierung angezeigt.

Benutzerzugriff manuell einschränken und verwalten

- Sie können zu den Warnungsdetails oder Benutzerdetails gehen und einen Benutzer dann manuell von diesen Bildschirmen blockieren oder wiederherstellen.

Verlauf Der Benutzerzugriffsbeschränkung

Auf der Seite Warnungsdetails und Benutzerdetails im Bedienfeld können Sie eine Prüfung des Zugriffsbegrenzungsverlaufs des Benutzers anzeigen: Zeit, Aktion (Blockieren, Entsperren), Dauer, Aktion ausgeführt von, Manuelle/automatische und betroffene IPs für NFS.

Wie wird die Funktion deaktiviert?

Sie können die Funktion jederzeit deaktivieren. Wenn es eingeschränkte Benutzer im System gibt, müssen Sie zuerst den Zugriff wiederherstellen.

- Navigieren Sie in Workload Security zu **Workload Security > Policies > Automated Response Policies**. Wählen Sie **+Angriffsrichtlinie**.
- Deaktivieren Sie die Option *Benutzerdateizugriff blockieren*.

Die Funktion wird von allen Seiten ausgeblendet.

Manuelle Wiederherstellung der IPs für NFS

Führen Sie die folgenden Schritte aus, um IP-Adressen von ONTAP manuell wiederherzustellen, wenn Ihre Workload-Sicherheitsstudie abläuft oder wenn der Agent/Collector nicht verfügbar ist.

1. Listen Sie alle Exportrichtlinien auf einer SVM auf.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Löschen Sie die Regeln über alle Richtlinien auf der SVM, die als Client Match „cloudSecure_rule“ haben, indem Sie den entsprechenden RegelIndex angeben. Workload-Sicherheitsregel liegt in der Regel bei 1.

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Stellen Sie sicher, dass die Sicherheitsregel für Workloads gelöscht
wird (optionaler Schritt zur Bestätigung).
```

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Benutzer für SMB manuell wiederherstellen

Führen Sie die folgenden Schritte aus, um alle Benutzer von ONTAP manuell wiederherzustellen, wenn Ihre Testversion für die Workload-Sicherheit abläuft oder wenn der Agent/Collector nicht verfügbar ist.

Sie können die Liste der in Workload Security blockierten Benutzer auf der Benutzer-Listenseite abrufen.

1. Melden Sie sich mit Cluster_admin_-Anmeldedaten beim ONTAP Cluster an (wo Sie die Blockierung von Benutzern aufheben möchten). (Bei Amazon FSX melden Sie sich mit FSX-Anmeldeinformationen an).
2. Führen Sie den folgenden Befehl aus, um alle durch Workload Security für SMB blockierten Benutzer in allen SVMs aufzulisten:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

In der obigen Ausgabe wurden 2 Benutzer (US030, US040) mit Domain CSLAB blockiert.

1. Führen Sie den folgenden Befehl aus, um den Benutzer zu entsperren, wenn Sie die Position aus der obigen Ausgabe identifiziert haben:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Bestätigen Sie, dass die Sperrung der Benutzer aufgehoben wird, indem
Sie den folgenden Befehl ausführen:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Für die zuvor blockierten Benutzer sollten keine Einträge angezeigt werden.

Fehlerbehebung

Problem	Versuchen Sie Dies
Einige der Benutzer werden nicht eingeschränkt, obwohl es einen Angriff gibt.	1. Stellen Sie sicher, dass sich der Data Collector und der Agent für die SVMs im Status *running* befinden. Workload Security kann keine Befehle senden, wenn der Data Collector und der Agent angehalten sind. 2. Dies liegt daran, dass der Benutzer möglicherweise von einem Computer mit einer neuen IP-Adresse auf den Speicher zugegriffen hat, die zuvor nicht verwendet wurde. Die Einschränkung erfolgt über die IP-Adresse des Hosts, über den der Benutzer auf den Speicher zugreift. Überprüfen Sie in der UI (Warndetails > Zugriffsbegrenzungsverlauf für diesen Benutzer > betroffene IP-Adressen) die Liste der eingeschränkten IP-Adressen. Wenn der Benutzer von einem Host aus auf Speicher zugreift, der eine andere IP als die eingeschränkten IP hat, kann der Benutzer weiterhin über die nicht eingeschränkte IP auf den Speicher zugreifen. Wenn der Benutzer versucht, von den Hosts, deren IP-Adressen eingeschränkt sind, auf den Speicher zuzugreifen, wird nicht zugegriffen werden können.
Manuelles Klicken auf Zugriff beschränken gibt „IP-Adressen dieses Benutzers wurden bereits eingeschränkt“.	Die zu beschränkte IP wird bereits von einem anderen Benutzer eingeschränkt.
Richtlinie konnte nicht geändert werden. Grund: Nicht autorisiert für diesen Befehl.	Überprüfen Sie, ob Sie cscuser verwenden, dass dem Benutzer Berechtigungen wie oben beschrieben erteilt werden.
Benutzer (IP-Adresse) Blockieren für NFS funktioniert, aber für SMB / CIFS, sehe ich eine Fehlermeldung: “SID to DomainName Transformation fehlgeschlagen. Grund-Timeout: Socket wurde nicht hergestellt“	Dies kann vorkommen, dass *csuser* nicht über die Berechtigung verfügt, ssh auszuführen. (Stellen Sie die Verbindung auf Cluster-Ebene sicher, und stellen Sie dann sicher, dass der Benutzer ssh ausführen kann.) *Csuser* Rolle erfordert diese Berechtigungen. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blockingFühren Sie für *csuser* mit Cluster-Anmeldeinformationen über die ONTAP-Befehlszeile Folgendes aus: Sicherheits-Login Rolle create -role csrole -cmddirname "vserver Export-Policy rule" -Access all Security Login role create -role csrdirname set -Access all Security Login role create -role csrole -cmddirname "vserver cifs Session" -Access all Security Login role create -role csrole -cmddirname "vserver Services Access-Check Authentication Translate" -Access all Security Login Rolle create -role csrole -cmddirname "vserver Name-Mapping" -Access all Wenn *csuser* nicht verwendet wird und wenn Admin-Benutzer auf Cluster-Ebene verwendet wird, stellen Sie sicher, dass der Admin-Benutzer SSH-Berechtigung für ONTAP hat.

Problem	Versuchen Sie Dies
Ich erhalte die Fehlermeldung *SID Translate failed. Grund:255:Fehler: Befehl fehlgeschlagen: Nicht autorisiert für diesen Befehl Fehler: "Access-Check" ist kein erkannter Befehl*, wenn ein Benutzer blockiert werden sollte.	Dies kann passieren, wenn *csuser* nicht über die richtigen Berechtigungen verfügt. Weitere Informationen finden Sie unter "Voraussetzungen für die Sperrung des Benutzerzugriffs" . Nach dem Anwenden der Berechtigungen wird empfohlen, den ONTAP-Datensammler und den Benutzerverzeichnisdatensammler neu zu starten. Die erforderlichen Berechtigungsbefehle sind unten aufgeführt. ---- Sicherheits-Login Rolle create -role csrole -cmddirname "vserver Export-Policy rule" -Access all Security Login role create -role csrdirname set -Access all Security Login role create -role csrole -cmddirname "vserver cifs Session" -Access all Security Login role create -role csrole -cmddirname "vserver Services Access-Check Authentication Translate" -Access all Security Login Role create -role csrole -cmddirname „vserver Name-Mapping“ -Access all ----

Workload Security: Simulation eines Angriffs

Mithilfe der Anweisungen auf dieser Seite können Sie einen Angriff für das Testen oder Demonieren der Workload-Sicherheit mithilfe des im Lieferumfang enthaltenen Skripts Ransomware Simulation simulieren.

Dinge zu beachten, bevor Sie beginnen

- Das Ransomware-Simulationsskript funktioniert nur auf Linux.
- Das Skript wird mit den Installationsdateien des Workload Security Agent bereitgestellt. Sie ist auf jedem Computer verfügbar, auf dem ein Workload Security Agent installiert ist.
- Sie können das Skript auf dem Workload Security Agent-Rechner selbst ausführen; es ist nicht erforderlich, einen anderen Linux-Rechner vorzubereiten. Wenn Sie jedoch das Skript lieber auf einem anderen System ausführen möchten, kopieren Sie einfach das Skript und führen es dort aus.

Mindestens 1,000 Beispieldateien haben

Dieses Skript sollte auf einer SVM mit einem Ordner ausgeführt werden, der Dateien verschlüsselt. Es wird empfohlen, mindestens 1,000 Dateien in diesem Ordner und allen Unterordnern zu haben. Die Dateien dürfen nicht leer sein. Erstellen Sie die Dateien nicht und verschlüsseln Sie sie mit demselben Benutzer. Workload Security berücksichtigt diese Aktivität mit niedrigem Risiko und erzeugt daher keine Warnmeldung (d. h. der gleiche Benutzer ändert die Dateien, die er gerade erstellt hat).

Siehe unten für Anweisungen zu "Programmgesteuertes Erstellen nicht leerer Dateien".

Richtlinien vor dem Ausführen des Simulators:

1. Stellen Sie sicher, dass verschlüsselte Dateien nicht leer sind.
2. Vergewissern Sie sich, dass Sie > 50 Dateien verschlüsseln. Eine kleine Anzahl von Dateien wird ignoriert.

3. Führen Sie keinen Angriff mit demselben Benutzer mehrmals durch. Nach ein paar Mal lernt Workload Security dieses Benutzerverhalten kennen und geht davon aus, dass es sich um das normale Verhalten des Benutzers handelt.
4. Verschlüsseln Sie keine Dateien, die gerade von demselben Benutzer erstellt wurden. Das Ändern einer Datei, die gerade von einem Benutzer erstellt wurde, wird nicht als riskante Aktivität betrachtet. Verwenden Sie stattdessen Dateien, die von einem anderen Benutzer erstellt wurden, ODER warten Sie ein paar Stunden zwischen Erstellung und Verschlüsselung der Dateien.

Bereiten Sie das System vor

Zunächst das Zielvolumen auf die Maschine montieren. Sie können entweder ein NFS-Mount oder einen CIFS-Export mounten.

So mounten Sie den NFS-Export in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Mounten Sie NFS Version 4.1 nicht; es wird von FPolicy nicht unterstützt.

So mounten Sie CIFS in Linux:

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Richten Sie als Nächstes einen Data Collector ein:
```

1. Konfigurieren Sie den Workload Security Agent, falls er noch nicht ausgeführt wurde.
2. Konfigurieren Sie den SVM-Datensammler, falls noch nicht geschehen.

Führen Sie das Skript Ransomware Simulator aus

1. Melden Sie sich (ssh) beim Workload Security Agent-Rechner an.
2. Navigieren Sie zu: */opt/netapp/cloudSecure/Agent/install*
3. Rufen Sie das Simulator-Skript ohne Parameter auf, um die Verwendung zu sehen:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Verschlüsseln Sie Ihre Testdateien

Um die Dateien zu verschlüsseln, führen Sie den folgenden Befehl aus:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

Stellen Sie Dateien wieder her

Führen Sie zum Entschlüsseln den folgenden Befehl aus:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Führen Sie das Skript mehrmals aus

Nachdem ein Ransomware-Angriff für einen Benutzer generiert wurde, wechseln Sie zu einem anderen Benutzer, um einen zusätzlichen Angriff zu generieren. Workload Security erlernt das Benutzerverhalten und warnt bei wiederholten Ransomware-Angriffen innerhalb kurzer Zeit für denselben Benutzer nicht.

Dateien programmatisch erstellen

Bevor Sie die Dateien erstellen, müssen Sie zunächst die Verarbeitung des Datensammlers anhalten oder anhalten.
Führen Sie die folgenden Schritte aus, bevor Sie den Datensammler zum Agenten hinzufügen. Wenn Sie den Datensammler bereits hinzugefügt haben, bearbeiten Sie einfach den Datensammler, geben Sie ein ungültiges Kennwort ein und speichern Sie es. Dadurch wird der Datensammler vorübergehend in einen Fehlerzustand versetzt. HINWEIS: Achten Sie darauf, dass Sie das ursprüngliche Passwort beachten!

Die empfohlene Option ist to "Unterbrechen Sie den Collector" Bevor Sie Ihre Dateien erstellen.]

Bevor Sie die Simulation ausführen, müssen Sie zuerst Dateien hinzufügen, die verschlüsselt werden sollen. Sie können die zu verschlüsselenden Dateien entweder manuell in den Zielordner kopieren oder die Dateien mithilfe eines Skripts (siehe Beispiel unten) programmatisch erstellen. Kopieren Sie mindestens 1,000 Dateien, unabhängig von der verwendeten Methode.

Wenn Sie die Dateien programmatisch erstellen möchten, gehen Sie wie folgt vor:

1. Melden Sie sich im Feld Agent an.
2. Mounten Sie einen NFS-Export aus der SVM des Filers auf die Agent Maschine. CD in diesen Ordner.
3. Erstellen Sie in diesem Ordner eine Datei mit dem Namen createfiles.sh
4. Kopieren Sie die folgenden Zeilen in diese Datei.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Speichern Sie die Datei.
6. Stellen Sie sicher, dass Sie die Berechtigung für die Ausführung der Datei ausführen:

```
 chmod 777 ./createfiles.sh
. Ausführen des Skripts:
```

```
./createfiles.sh
```

Im aktuellen Ordner werden 1000 Dateien erstellt.

7. Aktivieren Sie den Datensammler erneut

   Wenn Sie den Datensammler in Schritt 1 deaktiviert haben, bearbeiten Sie den Datensammler, geben Sie das richtige Passwort ein, und speichern Sie es. Stellen Sie sicher, dass der Datensammler wieder in Betrieb ist.

8. Wenn Sie den Collector angehalten haben, bevor Sie diese Schritte ausführen, müssen Sie Folgendes tun "Nehmen Sie die Sammlung wieder auf".

Konfigurieren von E-Mail-Benachrichtigungen für Warnungen, Warnungen und den Zustand des Agent/Data Source Collectors

Um die Empfänger von Benachrichtigungen für die Workload-Sicherheit zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse in die entsprechenden Abschnitte ein.

Potenzielle Angriffs- und Warnhinweise

Um Benachrichtigungen zu potenziellen Angriffen zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „ potenzielle Angriffswarnungen senden “ ein. Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an die Benachrichtigungsliste gesendet.

Um _Warnhinweise zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „ Warnhinweise senden “ ein.

Statusüberwachung von Agent und Data Collector

Sie können den Zustand von Agenten und Datenquellen über Benachrichtigungen überwachen.

Um Benachrichtigungen zu erhalten, wenn ein Agent oder Datenquellensammler nicht funktioniert, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „*Data Collection Health Alerts*“ ein.

Beachten Sie Folgendes:

- Zustandswarnmeldungen werden erst gesendet, nachdem der Agent/Sammler mindestens eine Stunde lang die Meldung beendet hat.
- Es wird nur eine E-Mail-Benachrichtigung an die vorgesehenen Empfänger in einem bestimmten Zeitraum von 24 Stunden gesendet, auch wenn der Agent oder der Datensammler länger getrennt ist.
- Bei einem Agent-Fehler wird eine Warnung gesendet (nicht eine pro Collector). Die E-Mail enthält eine Liste aller betroffenen SVMs.
- Active Directory-Sammlung Fehler wird als Warnung gemeldet; es hat keine Auswirkungen auf Ransomware-Erkennung.
- Die Setup-Liste „erste Schritte“ enthält jetzt eine neue Phase „*E-Mail-Benachrichtigungen konfigurieren*“.

Empfangen Von Agent- Und Data Collector-Upgrade-Benachrichtigungen

- Geben Sie in „Data Collection Health Alerts“ die E-Mail-ID(s) ein.
- Das Kontrollkästchen „Upgrade-Benachrichtigungen aktivieren“ wird aktiviert.
- Die E-Mail-Benachrichtigungen für Agent- und Data Collector-Upgrades werden einen Tag vor dem geplanten Upgrade an die E-Mail-IDs gesendet.

Fehlerbehebung

Problem:	**Teste das:**
E-Mail-IDs sind in den „Data Collector Health Alerts“ vorhanden, ich erhalte jedoch keine Benachrichtigungen.	Benachrichtigungs-E-Mails werden von der NetApp-Data-Infrastructure-Insights-Domain gesendet, d. h. von *accounts@service.cloudinsights.NetApp.com*. Einige Unternehmen blockieren eingehende E-Mails, wenn sie von einer externen Domäne stammen. Stellen Sie sicher, dass externe Benachrichtigungen aus NetApp-Dateninfrastrukturdomänen auf die Whitelist gesetzt sind.

Workload-Sicherheits-API

Die Workload-Sicherheits-API ermöglicht NetApp Kunden und unabhängigen Software-Anbietern (ISVs) die Integration der Workload-Sicherheit in andere Applikationen wie CMDB- oder andere Ticketsysteme.

Anforderungen für API-Zugriff:

- Ein API-Zugriffstoken-Modell wird verwendet, um den Zugriff zu gewähren.
- Das Management von API-Token wird von Workload Security-Benutzern mit der Administratorrolle durchgeführt.

API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Workload Security anmelden und zu **Admin > API Access** navigieren. Klicken Sie auf den Link **API Documentation**. Die API-Dokumentation ist Swagger-basiert, die eine kurze Beschreibung und Verwendungsinformationen für die API enthält und Sie können es in Ihrer Umgebung ausprobieren.

Wenn Sie die Forensics Activity API aufrufen, verwenden Sie die API cloudSecure_forensics.activities.**v2**. Wenn Sie mehrere Aufrufe zu dieser API ausführen, stellen Sie sicher, dass die Aufrufe nacheinander und nicht parallel erfolgen. Mehrere parallele Aufrufe können dazu führen, dass die API-Zeit abgeht.

API-Zugriffs-Tokens

Bevor Sie die Workload Security API verwenden, müssen Sie ein oder mehrere **API Access Token** erstellen. Access Tokens gewähren Leseberechtigungen. Sie können auch die Ablauffrist für jedes Access Token festlegen.

So erstellen Sie ein Access Token:

- Klicken Sie auf **Admin > API Access**
- Klicken Sie auf **+API Access Token**
- Geben Sie **Tokenname** Ein
- Geben Sie **Token Expiration** An

Ihr Token kann nur während des Erstellungsvorgangs in die Zwischenablage kopiert und gespeichert werden. Token können nicht abgerufen werden, nachdem sie erstellt wurden. Daher wird dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche API-Zugriffstoken kopieren zu klicken, bevor Sie den Bildschirm zur Token-Erstellung schließen können.

Sie können Token deaktivieren, aktivieren und widerrufen. Deaktivierte Token können aktiviert werden.

Tokens gewähren aus Kundensicht allgemeinen Zugang zu APIs und verwalten den Zugriff auf APIs im Umfang ihrer eigenen Umgebung.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Access Token dann als Berechtigung, wenn es die Ziel-API anruft. Das

übergebene Token informiert die API, dass der Inhaber des Tokens berechtigt ist, auf die API zuzugreifen und bestimmte Aktionen basierend auf dem Umfang auszuführen, den während der Autorisierung gewährt wurde.

Der HTTP-Header, in dem das Access Token übergeben wird, ist **X-CloudInsights-ApiKey:**

Verwenden Sie zum Abrufen von Lagerbeständen beispielsweise Folgendes:

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
Wobei _<API_Access_Token>_ das Token ist, das Sie bei der Erstellung des
API-Zugriffsschlüssels gespeichert haben.
```

Detaillierte Informationen finden Sie im Link *API Documentation* unter **Admin > API Access**.

Skript zum Extrahieren von Daten über die API

Workload Security-Agenten enthalten ein Exportskript, um parallele Aufrufe an die v2-API zu ermöglichen, indem sie den angeforderten Zeitraum in kleinere Stapel aufteilen.

Das Skript befindet sich unter */opt/NetApp/CloudSecure/Agent/Export-script*. Eine README-Datei im selben Verzeichnis enthält Anweisungen zur Verwendung.

Hier ist ein Beispielbefehl zum Aufrufen des Skripts:

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

Key Parameters: - `--iteration_interval 12`: Teilt den gewünschten Zeitbereich in Intervalle von 12 Stunden auf. - `--num_workers 3`: Holt diese Intervalle parallel mit 3 Threads.

Fehlerbehebung

Fehlerbehebung Bei Allgemeinen Problemen Mit Data Infrastructure Insights

Hier finden Sie Vorschläge für die Fehlerbehebung Data Infrastructure Insights.

Siehe auch "Fehlerbehebung Bei Problemen Mit Der Linux-Erfassungseinheit" Und "Fehlerbehebung Bei Problemen Mit Der Windows-Erfassungseinheit".

Probleme bei der Anmeldung

Problem:	Teste das:
Data Infrastructure Insights meldet sich automatisch alle 6 Stunden ab	Dies ist auf deaktivierte Browser-Cookies von Drittanbietern zurückzuführen. Benutzer können ihren Browser so konfigurieren, dass alle Drittanbieter-Cookies aktiviert werden, oder eine engere Ausnahmeliste verwenden, um nur diejenigen für Data Infrastructure Insights zu aktivieren. Beispiel: Browser-Einstellungen öffnen Wählen Sie die Option "Alle Cookies zulassen". **ODER** Wählen Sie „Cookies von Drittanbietern blockieren“ und fügen Sie Ausnahmen für *[*.]auth0.com* und *[*.]NetApp.com* hinzu. Microsoft Edge follows das gleiche Format für Ausnahmen wie Chrome. In Firefox werden Cookie-Ausnahmen einfach als *auth0.com* und *netapp.com* bezeichnet.
Ich habe ein BlueXP Konto, kann mich aber nicht bei BlueXP anmelden.	Öffnen Sie ein Ticket von https://mysupport.netapp.com/site/help. Wählen Sie die Kategorie „blueXP.netapp.com > Probleme mit Account/Login“ oder „bluexp.netapp.com > Probleme mit der Federation“ aus. Diese betreffen speziell Probleme oder Fragen zu BlueXP. Für alle anderen Fragen zum technischen Support von Data Infrastructure Insights wenden Sie sich an "NetApp Support".
Ich wurde zu Data Infrastructure Insights eingeladen, aber ich erhalte eine Nachricht „nicht autorisiert“.	Überprüfen Sie, ob Sie sich für ein BlueXP Konto registriert haben oder ob Ihr Unternehmen SSO-Anmeldedaten mit BlueXP verwendet. Überprüfen Sie, ob Ihre E-Mail-Adresse für Ihr BlueXP -Profil mit der E-Mail-Adresse übereinstimmt, die in Ihrer Begrüßungs-E-Mail zu Einblicke von Dateninfrastruktur Stimmt die E-Mail nicht überein, fordern Sie eine neue Einladung mit der richtigen E-Mail-Adresse an.

Problem:	Teste das:
Ich habe mich bei BlueXP abgemeldet und wurde automatisch bei „Data Infrastructure Insights“ abgemeldet.	Bei Single Sign On (SSO) über NetApp-Cloud-Services werden alle Sitzungen zu Dateninfrastruktur-Einblicken abgehört. Wenn Sie Zugriff auf mehrere Konten für Data Infrastructure Insights haben, werden alle aktiven Sitzungen bei einer beliebigen Abmeldung abmeldet. Melden Sie sich erneut an, um auf Ihr Konto zuzugreifen.
Ich wurde nach einigen Tagen automatisch abgemeldet.	Für NetApp Cloud-Konten muss alle paar Tage eine erneute Authentifizierung durchgeführt werden (die aktuelle BlueXP Einstellung beträgt 7 Tage). Melden Sie sich erneut an, um auf Ihr Konto zuzugreifen.
Ich erhalte eine Fehlermeldung „Anmeldung nicht mehr zulässig“.	Wenden Sie sich an Ihren Account-Administrator, um den Zugriff auf Data Infrastructure Insights zu überprüfen. Überprüfen Sie, ob Ihre E-Mail-Adresse für Ihr BlueXP -Profil mit der E-Mail-Adresse übereinstimmt, die in Ihrer Begrüßungs-E-Mail zu Einblicke von Dateninfrastruktur
Andere Anmeldefehler	Testen Sie den Inkognito-Modus in Chrome, oder löschen Sie den Browserverlauf, Cookies und Cache. Versuchen Sie es mit einem anderen Browserprofil (d.h. Chrome - Person hinzufügen).

Andere Probleme

Frage:	Antwort:
Meine Qtree-Hard-Quoten werden korrekt in Abfragen angezeigt, aber meine Soft Quotas werden als Gesamtkapazität des Volumes angezeigt. Ist das richtig?	Nur harte Kontingente - die entweder manuell festgelegt oder durch Trident eingestellt sind - werden als festgelegte Kontingente angezeigt; wenn keine harten Kontingente angegeben werden, wird die Qtree-Kapazität die interne Volume-Kapazität sein.
Ich habe sowohl eine weiche als auch eine harte Quote manuell im selben Qtree eingestellt, aber die insgesamt darstellende Kapazität ist die harte Quote; ist das richtig?	Ja, wenn eine harte Quote angegeben wird, wird diese als Gesamtkapazität angezeigt.
Bei der Eingabe eines Cognos Report-Zeitplans endet manchmal ein zusätzliches „m“ in der Zeitplanung. Wenn ich die Zeit beispielsweise als „02:15 PM“ eingebe, kann ein zusätzliches Zeichen hinzugefügt werden: „02:15 PMM“ (oder PMM). Wenn ich draußen klicke, ändert es sich zu "2:15 AM". Ich kann den Bericht speichern, aber wenn ich den gespeicherten Bericht erneut öffne, wird die Zeitplanzeit als AM (d. h. morgens) angezeigt, unabhängig davon, ob ich in der Zeitplanzeit AM oder PM eingegeben habe.	Geben Sie die Zeitplanzeit erneut ein. Achten Sie dabei darauf, nicht die vollständigen Zeichen „AM“ oder „PM“ einzugeben. Es reicht aus, „A“ für „AM“ oder „P“ für „PM“ einzugeben. Wenn das zusätzliche Zeichen nicht angezeigt wird, wird die Zeitplanzeit korrekt eingestellt.

Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im "NetApp Knowledge Base" (Support-Anmeldung erforderlich).

Weitere Support-Informationen finden Sie auf der Seite Data Infrastructure Insights"Unterstützung".

Wenn Sie über ein aktives Abonnement von Data Infrastructure Insights verfügen, können Sie die folgenden Support-Optionen nutzen:

"Telefon"
"Support-Ticket"

Weitere Informationen finden Sie im "Support-Dokumentation Zu Data Infrastructure Insights".

Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Linux

Hier finden Sie Vorschläge zur Fehlerbehebung bei Problemen mit Akquisitionseinheiten auf einem Linux-Server.

Problem:	**Teste das:**
AU-Status auf der Seite **Observability > Collectors** auf der Registerkarte **Acquisition Units** zeigt "Certificate Expired" oder "Certificate Recanned" an.	Klicken Sie auf das Menü rechts neben der AU und wählen Sie **Verbindung wiederherstellen**. Befolgen Sie die Anweisungen, um Ihre Erfassungseinheit wiederherzustellen: 1. Beenden Sie den AU-Dienst (Acquisition Unit). Klicken Sie auf die Schaltfläche *Stop-Befehl kopieren*, um den Befehl schnell in die Zwischenablage zu kopieren, und fügen Sie diesen Befehl anschließend in eine Eingabeaufforderung auf dem Erfassungsgerät ein. 2. Erstellen Sie eine Datei mit dem Namen „Token“ im Ordner */var/lib/netapp/nebinsights/acq/conf* auf der AU. 3. Klicken Sie auf die Schaltfläche *Token kopieren* und fügen Sie dieses Token in die von Ihnen erstellte Datei ein. 4. Starten Sie den AU-Service. Klicken Sie auf die Schaltfläche *Copy Restart Command*, und fügen Sie den Befehl in eine Eingabeaufforderung auf der AU ein.
Berechtigung beim Starten des Serverdienstes für die Erfassungseinheit verweigert	Wenn die AU auf SELINUX installiert ist, sollte SE auf den Modus *Permissive* eingestellt werden. *Forcieren* -Modus wird nicht unterstützt. Starten Sie den AU-Dienst erneut, nachdem SELINUX den Modus „Permissiv“ eingestellt hat. "Weitere Informationen .".
Serveranforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Akquisitionsgruppenserver oder Ihre VM die Anforderungen erfüllt "Anforderungen"

Netzwerkanforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server/Ihre VM über eine SSL-Verbindung über Port 443 auf Ihre Data Infrastructure Insights-Umgebung (<environment-name>.c01.cloudinsights.NetApp.com) zugreifen kann. Versuchen Sie es mit folgenden Befehlen: *Ping <environment-name>.c01.cloudinsights.NetApp.com traceroute <environment-name>.c01.cloudinsights.NetApp.com curl https://<environment-name>.c01.cloudinsights.NetApp.com wget https://<environment-name>.c01.cloudinsights.NetApp.com*
Proxy-Server nicht ordnungsgemäß konfiguriert	Überprüfen Sie Ihre Proxy-Einstellungen und deinstallieren/installieren Sie die Software für die Acquisition Unit, falls erforderlich, um die richtigen Proxy-Einstellungen einzugeben. 1. Versuchen Sie "Curl". Beziehen Sie sich auf "man Curl" Informationen/Dokumentation zu Proxys: --preproxy, --Proxy-* (das ist ein Platzhalter "*", da Curl viele Proxy-Einstellungen unterstützt). 2. Versuchen Sie "wget". In der Dokumentation finden Sie Proxy-Optionen.
Installation der Erfassungseinheit in Data Infrastructure Insights mit Anmeldefehlern beim Starten des Erfassungsservice (und sichtbar im acq.log) fehlgeschlagen.	Dies kann durch die Einbeziehung von Sonderzeichen in die Proxy-Anmeldeinformationen verursacht werden. Deinstallieren Sie AU (*sudo nebundinsights-uninstall.sh*) und installieren Sie sie erneut, ohne Sonderzeichen zu verwenden.
Linux: Fehlende Bibliothek / Datei nicht gefunden	Stellen Sie sicher, dass Ihr Linux Acquisition Unit Server/VM über alle erforderlichen Bibliotheken verfügt. Zum Beispiel muss die Bibliothek *unzip* auf dem Server installiert sein. Um die Bibliothek *unzip* zu installieren, führen Sie den Befehl **sudo yum install unzip** aus, bevor Sie das Installationsskript für die Erfassungseinheit ausführen
Berechtigungsprobleme	Stellen Sie sicher, dass Sie als Benutzer mit *sudo* Berechtigungen angemeldet sind
Akquisition Nicht Ausgeführt:	Sammeln Sie die acq.log aus /opt/netapp/cloudinsights/acq/logs (Linux) Neustart des Acquisition Service: Sudo cloudinsights-service.sh restart Übernahme
Probleme Bei Der Datenerfassung:	Senden Sie einen Fehlerbericht von der Data Collector-Startseite, indem Sie auf die Schaltfläche „Fehlerbericht senden“ klicken

Status: Herzschlag Fehlgeschlagen	Die Acquisition Unit (AU) sendet zur Erneuerung des Leasingvertrags alle 60 Sekunden einen Heartbeat an Data Infrastructure Insights. Wenn der Heartbeat-Anruf aufgrund eines Netzwerkproblems oder einer nicht reagierenden Data Infrastructure Insights fehlschlägt, wird die Leasingzeit des AU nicht aktualisiert. Wenn die Leasingzeit der AU abläuft, zeigt Data Infrastructure Insights den Status „Heartbeat failed“ an. Schritte zur Fehlerbehebung: Prüfen Sie die Netzwerkverbindung zwischen dem Server der Akquisitionseinheit und CloudInsights. Prüfen Sie, ob der Dienst für die Erfassungseinheit ausgeführt wird. Wenn der Dienst nicht ausgeführt wird, starten Sie den Dienst. Überprüfen Sie im Log der Acquisition Unit (/var/log/netapp/nebinsights/acq/acq.log), ob Fehler aufgetreten sind.
Ich sehe die Meldung „Heartbeat Error:“	Dieser Fehler kann auftreten, wenn eine Netzwerkunterbrechung vorliegt, die dazu führt, dass die Kommunikation zwischen der Erfassungseinheit und der Data Infrastructure Insights-Umgebung länger als eine Minute unterbrochen wird. Überprüfen Sie, ob die Verbindung zwischen AU und Data Infrastructure Insights stabil und aktiv ist.
Bei der Neuinstallation der Acquisition Unit sehe ich „ValueError: Dateikontext für /opt/netapp/Cloudinsights(/.*)? Bereits definiert“.	Auf einem System mit SELinux wird möglicherweise nach dieser Fehlermeldung angezeigt `cloudinsights-uninstall.sh -p` Wurde ausgeführt und die Erfassungseinheit muss neu installiert werden. Ausführen des Befehls `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` Sollte das Problem beheben und die Meldung entfernen.

Überlegungen zu Proxys und Firewalls

Wenn Ihr Unternehmen die Proxy-Nutzung für den Internetzugang benötigt, müssen Sie möglicherweise das Proxy-Verhalten Ihres Unternehmens kennen und bestimmte Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Beachten Sie Folgendes:

- Erstens blockiert Ihr Unternehmen standardmäßig den Zugriff und erlaubt ausschließlich den Zugriff auf bestimmte Websites/Domänen durch Ausnahme? Wenn dies der Fall ist, müssen Sie die folgende Domäne der Ausnahmeliste hinzufügen:

  ```
  *.cloudinsights.netapp.com
  ```

  Ihre Data Infrastructure Insights Acquisition Unit sowie Ihre Interaktionen in einem Webbrowser mit Data Infrastructure Insights gehen alle zu Hosts mit diesem Domänennamen.

- Zweitens versuchen einige Proxys, TLS/SSL-Prüfungen durchzuführen, indem sie Webseiten von Data Infrastructure Insights mit digitalen Zertifikaten imitieren, die nicht von NetApp generiert wurden. Das Sicherheitsmodell der Data Infrastructure Insights Acquisition Unit ist mit diesen Technologien

grundsätzlich nicht kompatibel. Sie benötigen außerdem den oben genannten Domänennamen, der von dieser Funktionalität ausgenommen ist, damit sich die Data Infrastructure Insights Acquisition Unit erfolgreich bei Data Infrastructure Insights anmelden und die Datenerkennung erleichtern kann.

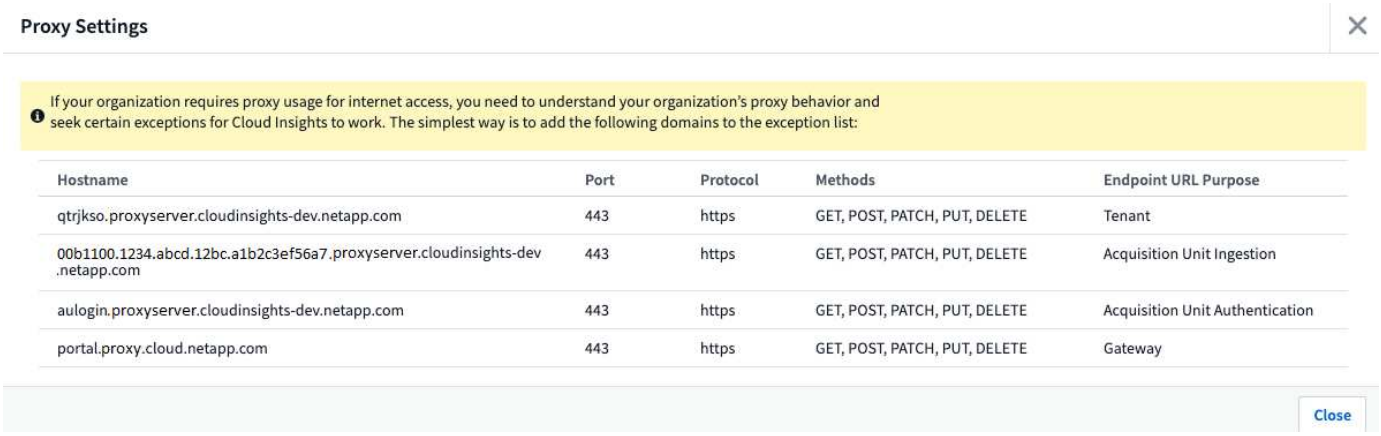
Wenn der Proxy für die Verkehrsinspektion eingerichtet ist, muss die Data Infrastructure Insights-Umgebung einer Ausnahmeliste in der Proxy-Konfiguration hinzugefügt werden. Das Format und die Einrichtung dieser Ausnahmeliste variieren je nach Proxy-Umgebung und -Tools. Im Allgemeinen müssen Sie jedoch die URLs der Data Infrastructure Insights-Server zu dieser Ausnahmeliste hinzufügen, damit die AU ordnungsgemäß mit diesen Servern kommunizieren kann.

Am einfachsten fügen Sie dazu die Data Infrastructure Insights-Domäne selbst der Ausnahmeliste hinzu:

```
 *.cloudinsights.netapp.com
Wenn der Proxy nicht für die Verkehrsprüfung eingerichtet ist, kann eine
Ausnahmeliste erforderlich sein oder nicht. Wenn Sie sich nicht sicher
sind, ob Sie Data Infrastructure Insights zu einer Ausnahmeliste
hinzufügen müssen, oder wenn aufgrund der Proxy- und/oder Firewall-
Konfiguration Probleme bei der Installation oder Ausführung von Data
Infrastructure Insights auftreten, wenden Sie sich an Ihr Proxy-
Verwaltungsteam, um die Verarbeitung des SSL-Abhörens durch den Proxy
einzurichten.
```

Anzeigen von Proxy-Endpunkten

Sie können Ihre Proxy-Endpunkte anzeigen, indem Sie beim Onboarding auf den Link **Proxy-Einstellungen** klicken oder auf der Seite **Hilfe > Support** den Link unter *Proxy-Einstellungen* wählen. Eine Tabelle wie die folgende wird angezeigt. Wenn Sie Workload Security in Ihrer Umgebung haben, werden auch die konfigurierten Endpunkt-URLs in dieser Liste angezeigt.



Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im "NetApp Knowledge Base" (Support-Anmeldung erforderlich).

Weitere Support-Informationen finden Sie auf der Seite Data Infrastructure Insights"Unterstützung".

Fehlerbehebung bei Problemen mit der Erfassungseinheit unter Windows

Hier finden Sie Vorschläge zur Fehlerbehebung bei Problemen mit Akquisitionseinheiten auf einem Windows-Server.

Problem:	Teste das:
AU-Status auf der Seite **Observability > Collectors** auf der Registerkarte **Acquisition Units** zeigt "Certificate Expired" oder "Certificate Recanned" an.	Klicken Sie auf das Menü rechts neben der AU und wählen Sie **Verbindung wiederherstellen**. Befolgen Sie die Anweisungen, um Ihre Erfassungseinheit wiederherzustellen: 1. Beenden Sie den AU-Dienst (Acquisition Unit). Klicken Sie auf die Schaltfläche *Stop-Befehl kopieren*, um den Befehl schnell in die Zwischenablage zu kopieren, und fügen Sie diesen Befehl anschließend in eine Eingabeaufforderung auf dem Erfassungsgerät ein. 2. Erstellen Sie eine Datei namens "Token" im Ordner *c:\Programme\Cloud Insights\Acquisition Unit\conf* auf der AU. 3. Klicken Sie auf die Schaltfläche *Token kopieren* und fügen Sie dieses Token in die von Ihnen erstellte Datei ein. 4. Starten Sie den AU-Service. Klicken Sie auf die Schaltfläche *Copy Restart Command*, und fügen Sie den Befehl in eine Eingabeaufforderung auf der AU ein.
Serveranforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Akquisitionsgruppenserver oder Ihre VM die Anforderungen erfüllt "Anforderungen"
Netzwerkanforderungen nicht erfüllt	Stellen Sie sicher, dass Ihr Acquisition Unit-Server/Ihre VM über eine SSL-Verbindung über Port 443 auf Ihre Data Infrastructure Insights-Umgebung (<environment-name>.c01.cloudinsights.NetApp.com) zugreifen kann. Versuchen Sie es mit folgenden Befehlen: *Ping <environment-name>.c01.cloudinsights.NetApp.com traceroute <environment-name>.c01.cloudinsights.NetApp.com curl https://<environment-name>.c01.cloudinsights.NetApp.com wget https://<environment-name>.c01.cloudinsights.NetApp.com*
Proxy-Server nicht ordnungsgemäß konfiguriert	Überprüfen Sie Ihre Proxy-Einstellungen und deinstallieren/installieren Sie die Software für die Acquisition Unit, falls erforderlich, um die richtigen Proxy-Einstellungen einzugeben. 1. Versuchen Sie "Curl". Beziehen Sie sich auf "man Curl" Informationen/Dokumentation zu Proxys: --preproxy, --Proxy-* (das ist ein Platzhalter "*", da Curl viele Proxy-Einstellungen unterstützt). 2. Versuchen Sie "wget". In der Dokumentation finden Sie Proxy-Optionen.

Installation der Erfassungseinheit in Data Infrastructure Insights mit Anmeldefehlern beim Starten des Erfassungsservice (und sichtbar im acq.log) fehlgeschlagen.	Dies kann durch die Einbeziehung von Sonderzeichen in die Proxy-Anmeldeinformationen verursacht werden. Deinstallieren Sie AU (*sudo nebundinsights-uninstall.sh*) und installieren Sie sie erneut, ohne Sonderzeichen zu verwenden.
Berechtigungsprobleme	Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind
Akquisition Wird Nicht Ausgeführt	Informationen finden Sie im Ordner acq.log im Verzeichnis *<install>\Cloud Insights\Acquisition Unit\log*. Starten Sie die Akquisition über Windows Services neu
Probleme Bei Der Datenerfassung	Senden Sie einen Fehlerbericht von der Data Collector-Startseite, indem Sie auf die Schaltfläche „Fehlerbericht senden“ klicken
Status: Herzschlag Fehlgeschlagen	Die Acquisition Unit (AU) sendet zur Erneuerung des Leasingvertrags alle 60 Sekunden einen Heartbeat an Data Infrastructure Insights. Wenn der Heartbeat-Anruf aufgrund eines Netzwerkproblems oder einer nicht reagierenden Data Infrastructure Insights fehlschlägt, wird die Leasingzeit des AU nicht aktualisiert. Wenn die Leasingzeit der AU abläuft, zeigt Data Infrastructure Insights den Status „Heartbeat failed“ an. Schritte zur Fehlerbehebung: * Überprüfen Sie die Netzwerkverbindung zwischen Acquisition Unit Server und CloudInsights. * Prüfen Sie, ob der Dienst „Erfassungseinheit“ ausgeführt wird. Wenn der Dienst nicht ausgeführt wird, starten Sie den Dienst. * Überprüfen Sie im Protokoll der Erfassungseinheit (<Install dir>:\Programme\Cloud Insights\Acquisition Unit\log\acq.log), ob Fehler auftreten.
Ich sehe eine Meldung „Heartbeat Error:“	Dieser Fehler kann auftreten, wenn eine Netzwerkunterbrechung vorliegt, die dazu führt, dass die Kommunikation zwischen der Erfassungseinheit und der Data Infrastructure Insights-Umgebung länger als eine Minute unterbrochen wird. Überprüfen Sie, ob die Verbindung zwischen AU und Data Infrastructure Insights stabil und aktiv ist.

Überlegungen zu Proxys und Firewalls

Wenn Ihr Unternehmen die Proxy-Nutzung für den Internetzugang benötigt, müssen Sie möglicherweise das Proxy-Verhalten Ihres Unternehmens kennen und bestimmte Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Beachten Sie Folgendes:

- Erstens blockiert Ihr Unternehmen standardmäßig den Zugriff und erlaubt ausschließlich den Zugriff auf bestimmte Websites/Domänen durch Ausnahme? Wenn dies der Fall ist, müssen Sie der Ausnahmeliste die folgende Domäne hinzufügen:

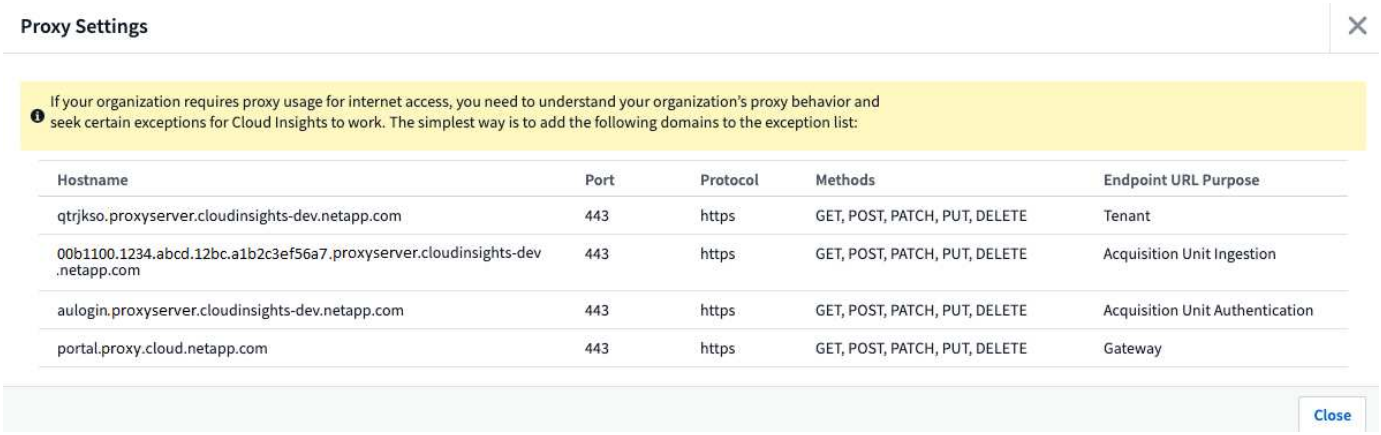
```
*.cloudinsights.netapp.com
```

Ihre Data Infrastructure Insights Acquisition Unit sowie Ihre Interaktionen in einem Webbrowser mit Data Infrastructure Insights gehen alle zu Hosts mit diesem Domänennamen.

- Zweitens versuchen einige Proxys, TLS/SSL-Prüfungen durchzuführen, indem sie Webseiten von Data Infrastructure Insights mit digitalen Zertifikaten imitieren, die nicht von NetApp generiert wurden. Das Sicherheitsmodell der Data Infrastructure Insights Acquisition Unit ist mit diesen Technologien grundsätzlich nicht kompatibel. Sie benötigen außerdem den oben genannten Domänennamen, der von dieser Funktionalität ausgenommen ist, damit sich die Data Infrastructure Insights Acquisition Unit erfolgreich bei Data Infrastructure Insights anmelden und die Datenerkennung erleichtern kann.

Anzeigen von Proxy-Endpunkten

Sie können Ihre Proxy-Endpunkte anzeigen, indem Sie beim Onboarding auf den Link **Proxy-Einstellungen** klicken oder auf der Seite **Hilfe > Support** den Link unter *Proxy-Einstellungen* wählen. Eine Tabelle wie die folgende wird angezeigt. Wenn Sie Workload Security in Ihrer Umgebung haben, werden auch die konfigurierten Endpunkt-URLs in dieser Liste angezeigt.



Ressourcen

Weitere Tipps zur Fehlerbehebung finden Sie im "NetApp Knowledge Base" (Support-Anmeldung erforderlich).

Weitere Support-Informationen finden Sie auf der Seite Data Infrastructure Insights"Unterstützung".

Recherchieren eines fehlgeschlagenen Datensammlers

Wenn ein Datensammler über eine Fehlermeldung und eine hohe oder mittlere Auswirkung verfügt, müssen Sie dieses Problem anhand der Datensammler-Übersichtsseite mit den verknüpften Informationen untersuchen.

Gehen Sie wie folgt vor, um die Ursache für fehlgeschlagene Datensammler zu ermitteln. Fehlermeldungen der Datensammler werden im Menü **Admin** und auf der Seite **installierte Datensammler** angezeigt.

Schritte

1. Klicken Sie Auf **Admin** > **Datensammler** > **Installierte Datensammler**.
2. Klicken Sie auf den verknüpften Namen des defekten Datensammlers, um die Seite Zusammenfassung zu

öffnen.

3. Auf der Seite Zusammenfassung können Sie im Bereich Kommentare alle Hinweise lesen, die von einem anderen Techniker hinterlassen wurden, der möglicherweise auch diesen Fehler untersucht hat.
4. Notieren Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniskleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unter der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol Fehlerdetails rechts neben der Meldung.

   Die Fehlerdetails enthalten den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, die verwendeten Informationen und Vorschläge, was versucht werden kann, das Problem zu beheben.

7. Im Bereich Geräte, die von diesem Data Collector gemeldet werden, können Sie die Liste filtern, um nur Geräte von Interesse anzuzeigen. Sie können dann auf den verknüpften **Name** eines Geräts klicken, um die Asset-Seite für dieses Gerät anzuzeigen.
8. Wenn Sie zur Übersichtsseite des Datensammlers zurückkehren, überprüfen Sie im Bereich **Letzte Änderungen anzeigen** unten auf der Seite, um zu sehen, ob die letzten Änderungen das Problem verursacht haben könnten.

Data Infrastructure Insights Data Collector Support Matrix

Die Data Collector Support Matrix bietet Referenz für Data Collectors, die von Data Infrastructure Insights unterstützt werden, einschließlich Hersteller- und Modellinformationen.

HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 20850_R2 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400C HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 InServ F400 InServ T400 InServ T800 InServ V400	3.1.1 (MU1) 3.1.2 (MU3) 3.1.3 (MU1) 3.1.3 (MU2) 3.1.3 (MU3) 3.2.1 (MU3) 3.2.1 (MU5) 3.2.2 3.2.2 (MU2) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 (MU1) 3.3.1 (MU2) 3.3.1 (MU5) 3.3.2 3.3.2 (MU1) 4.4.1 Freigabetyp: Standard Support Release 4.5.11 Versionstyp: Extended Support Release 4.5.3 Versionstyp: Extended Support Release 4.5.7 Versionstyp: Extended Support Release 9.5.8 Versionstyp: Extended Support Release

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Protokoll-Controller	Implementiert	SSH	
		Storage-Port	Implementiert	SSH	
		Typ	Lücke	SSH	
	Volume-Maske	Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Storage-Port	Implementiert	SSH	
		Typ	Lücke	SSH	
	Volumenreferenz	Name	Implementiert	SSH	
		Storage-Ip	Implementiert	SSH	
	WWN-Alias	Host-Aliase	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		Quelle	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					und Schreibvorgänge auf allen
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz Schreiben	Implementiert	SMI-S	
		„Ausstehend“	Implementiert	SMI-S	Insgesamt ausstehend

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
3PAR SMI-S	SMI-S	HTTP/HTTPS	5988/5989		Richtig	Richtig	Richtig	Richtig
3PAR-CLI	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

Amazon AWS EC2

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
1 2014-10-01

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
660					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Disk	VirtualisierungsDisk OID	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Virtuelle Machine	Implementiert	HTTPS	
	Host	Host-Betriebssystem	Implementiert	HTTPS	
		IPS	Implementiert	HTTPS	
		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		OID	Implementiert	HTTPS	
	Info	Api-Beschreibung	Implementiert	HTTPS	
		Api-Name	Implementiert	HTTPS	
		Api-Version	Implementiert	HTTPS	
		Name der Datenquelle	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Ersteller-ID	Implementiert	HTTPS	
		Erstellschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

					auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz Schreiben	Implementiert	HTTPS	
	vm	Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		Gesamtzahl der CPU-Auslastung	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		DiskIops.total	Implementiert	HTTPS	
		Festplatten-IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Festplattendurchsatz	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	Gesamtauslesen des Festplattendurchsatzes
		Festplattendurchsatz Schreiben	Implementiert	HTTPS	
		IP-Durchsatz Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	IP-Durchsatz insgesamt
		IpThrughput.write	Implementiert	HTTPS	
		Gesamte Speicherauslastung	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EC2 API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Amazon AWS S3

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
S3	1 2010-08-01

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Festplatten)			
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage-Pool	In Dwh-Kapazität Einbeziehen	Implementiert	HTTPS	Ein Weg von ACQ zu cotnrol, die Stroage Pools sind interessant in DWH Kapazität
		Name	Implementiert	HTTPS	
		Kapazität der physischen Festplatte (MB)	Implementiert	HTTPS	Wird als Rohkapazität für den Storage-Pool verwendet
		Raid-Gruppe	Implementiert	HTTPS	Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	HTTPS	Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning Wird Unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
Performance	Internes Volumen	Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		Objekte Gesamt	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
S3-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Microsoft Azure NetApp Files

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle
1 2019-06-01	Azure NetApp Dateien

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Daten			
		Verwendete Kapazität	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	IOPS Lesen	Implementiert		Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert		
		IOPS Schreiben	Implementiert		
		Durchsatz Beim Lesen	Implementiert		
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert		

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Azure NetApp Files REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Brocade Fibre Channel Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
178.0 183.0 Brocade 200E Brocade 300E Brocade 3900 Brocade 4024 Integriert Brocade 48000 Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Integriert Brocade 6505 Brocade 6510 Brocade 6520 Brocade 6548 Brocade 7800 Brocade 7840 Brocade DCX Brocade DCX-4S Backbone Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade M5424 integriert Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v5.3.2c V6.2.1b V6.2.2g V6.3.2 v6.4.1a v6.4.2 v6.4.2a V7.0.0 V7.0.1b v7.1.0c v7.3.0c v7.3.1d v7.4.1d v7.4.1f v7.4.2a v7.4.2c v7.4.2d v7.4.2g v7.4.2g_cvr_824494_01 v7.4.2h v7.4.2j1 v8.0.2a v8.0.2c v8.0.2d V8.1.2g V8.1.2j V8.1.2K v8.2.0 v8.2.0b v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3a1 v8.2.3b v8.2.3c v8.2.3c1 v9.0.0b v9.0.1a v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1_01 v9.1.1b

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Zone	Zonenname	Implementiert	SSH	
	Zonenmitglied	Typ	Lücke	SSH	
		WWN	Implementiert	SSH	
	Zonenfunktionen	Aktive Konfiguration	Implementiert	SSH	
		Konfigurationsname	Implementiert	SSH	
		Standardverhalten Für Zoneneinzug	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Verkehrsrahmenrate	Implementiert	SNMP	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verkehrsrahmenrate	Implementiert	SNMP	
		Durchschnittliche Bildgröße	Implementiert	SNMP	Durchschnittliche Größe des Datenverkehrs
		TX-Rahmen	Implementiert	SNMP	Durchschnittliche Größe des Verkehrsaufkommens
		Traffic-Rate	Implementiert	SNMP	
		Gesamte Datenverkehrrate	Implementiert	SNMP	
		Traffic-Rate	Implementiert	SNMP	
		Traffic-Auslastung	Implementiert	SNMP	
		Traffic-Auslastung	Implementiert	SNMP	Gesamte Traffic-Auslastung
		Traffic-Auslastung	Implementiert	SNMP	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		Richtig	Richtig	Richtig	Richtig
Brocade SSH	SSH	SSH	22		Falsch	Falsch	Richtig	Richtig
Konfiguration des Datenquellenassistenten	Manuelle Eingabe				Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Brocade Network Advisor HTTP

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
14.4.1 14.4.3 14.4.4 14.4.5	Brocade 5300 Brocade 6510 Brocade 6520 Brocade 6548 Brocade DCX 8510-8 Brocade G620 DS-6620B EMC CONNECTRIX ED-DCX8510-8B	v7.2.1a v7.3.1a v7.4.1b v7.4.2d v8.2.3b v8.2.3c v9.0.1a v9.0.1b v9.0.1e1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
690					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Switch-Status	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
		WWN	Implementiert	HTTP/S	
	Unbekannt	Treiber	Implementiert	HTTP/S	
		Firmware	Implementiert	HTTP/S	
		Hersteller	Implementiert	HTTP/S	
		Modell	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	
	WWN-Alias	Host-Aliase	Implementiert	HTTP/S	
		Objekttyp	Implementiert	HTTP/S	
		Quelle	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	
	Zone	Zonenname	Implementiert	HTTP/S	
	Zonenmitglied	Typ	Lücke	HTTP/S	
		WWN	Implementiert	HTTP/S	
	Zonenfunktionen	Aktive Konfiguration	Implementiert	HTTP/S	
		Konfigurationsname	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance	Port	BbCreditZero.total	Implementiert	HTTP/S	
		BB-Guthaben	Implementiert	HTTP/S	
		BbCreditZeroMs	Implementiert	HTTP/S	
		PortErrors.class3Discard	Implementiert	HTTP/S	
		PortErrors.crc	Implementiert	HTTP/S	
		Port-Fehler	Implementiert	HTTP/S	
		Port-Fehler	Implementiert	HTTP/S	Port-Fehler aufgrund des kurzen Rahmens
		PortErrors.linkAusfall	Implementiert	HTTP/S	Verbindungsfehler bei Port-Fehlern
		Port-Fehler	Implementiert	HTTP/S	Port-Fehler signalisieren Verlust
		Port-Fehler	Implementiert	HTTP/S	Port-Fehler Synchronisierungsverlust
		Port-Fehler	Implementiert	HTTP/S	Port-Fehler-Zeitüberschreitung verwerfen
		Port-Fehler	Implementiert	HTTP/S	Gesamtanzahl an Port-Fehlern
		Traffic-Rate	Implementiert	HTTP/S	
		Gesamte Datenverkehrrate	Implementiert	HTTP/S	
		Traffic-Rate	Implementiert	HTTP/S	
		Traffic-Auslastung	Implementiert	HTTP/S	
		Traffic-Auslastung	Implementiert	HTTP/S	Gesamte Traffic-Auslastung
		Traffic-Auslastung	Implementiert	HTTP/S	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Brocade Network Advisor REST-API	HTTP/HTTPS	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Brocade FOS REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Brocade 6505 Brocade G720 Brocade X6-8	v8.2.3c v8.2.3c1 v9.0.1e1 v9.1.1b

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		WWN	Implementiert	HTTPS	
	Zone	Zonenname	Implementiert	HTTPS	
	Zonenmitglied	Typ	Lücke	HTTPS	
		WWN	Implementiert	HTTPS	
	Zonenfunktionen	Aktive Konfiguration	Implementiert	HTTPS	
		Konfigurationsname	Implementiert	HTTPS	
		Standardverhalten Für Zoneneinzug	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Gesamte Traffic Frame Rate	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktionsattribute**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchschnittliche Bildgröße	Implementiert	HTTPS	Durchschnittliche Größe des Datenverkehrs
		TX-Rahmen	Implementiert	HTTPS	Durchschnittliche Größe des Verkehrsaufkommens
		Traffic-Rate	Implementiert	HTTPS	
		Gesamte Datenverkehrrate	Implementiert	HTTPS	
		Traffic-Rate	Implementiert	HTTPS	
		Traffic-Auslastung	Implementiert	HTTPS	
		Traffic-Auslastung	Implementiert	HTTPS	Gesamte Traffic-Auslastung
		Traffic-Auslastung	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
BROCADE FOS REST-API	HTTPS		443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Cisco MDS und Nexus Fabric Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
8978-E04 CN1610 DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9134-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C56128P N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-6454	3.3 (1c) 4.1 (3a) 5.0(1a) 5.0(3)N2(3.11e) 5.0(3)N2(3.23o) 5.0(3)N2(4.01d) 5.0(3)N2(4.04e) 5.0(3)N2(4.13e) 5.0(3)N2(4.13i) 5.0(3)N2(4.21e) 5.0(3)N2(4.21j) 5.0(3)N2(4,21k) 5.0(3)N2(4,22c) 5.0 (8) 5.2 (2d) 5.2(3)N2(2,28 g) 5.2 (6a) 5.2 (8) 5.2 (8b) 5.2 (8c) 5.2 (8d) 5.2 (8f) 5.2 (8 g) 5.2 (8 Std.) 5.2(8i) 6.2(1) 6.2 (11) 6.2 (11b) 6.2 (11c) 6.2 (11e) 6.2 (13) 6.2 (13a) 6.2 (15) 6.2 (17) 6.2 (19) 6.2 (21) 6.2 (23) 6.2 (25) 6.2 (27) 6.2 (29) 6.2 (31) 6.2 (33) 6.2 (5) 6.2 (5a) 6.2 (7) 6.2 (9) 6.2 (9a) 6.2 (9c) 7.3(0)D1(1) 7.3(0)DY(1) 7.3(1)DY(1) 7.3(1)N1(1) 7.3(13)N1(1) 7.3(6)N1(1)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	SNMP	
		VSAN aktiviert	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Unbekannt	Treiber	Implementiert	SNMP	
		Firmware	Implementiert	SNMP	
		Erzeugt	Implementiert	SNMP	
		Hersteller	Implementiert	SNMP	
		Modell	Implementiert	SNMP	
		Name	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
	WWN-Alias	Host-Aliase	Implementiert	SNMP	
		Objekttyp	Implementiert	SNMP	
		Quelle	Implementiert	SNMP	
		WWN	Implementiert	SNMP	
	Zone	Zonenname	Implementiert	SNMP	
		Zonentyp	Implementiert	SNMP	
	Zonenmitglied	Typ	Lücke	SNMP	
		WWN	Implementiert	SNMP	
	Zonenfunktionen	Aktive Konfiguration	Implementiert	SNMP	
		Konfigurationsname	Implementiert	SNMP	
		Standardverhalten Für Zoneneinzug	Implementiert	SNMP	
		Steuerung Zusammenführen	Implementiert	SNMP	
		WWN	Implementiert	SNMP	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Gesamte Traffic Frame Rate	Implementiert	SNMP	
Produkt	**Kategorie**	**Funktionsattribute**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchschnittliche Bildgröße	Implementiert	SNMP	Durchschnittliche Größe des Datenverkehrs
		TX-Rahmen	Implementiert	SNMP	Durchschnittliche Größe des Verkehrsaufkommens
		Traffic-Rate	Implementiert	SNMP	
		Gesamte Datenverkehrrate	Implementiert	SNMP	
		Traffic-Rate	Implementiert	SNMP	
		Traffic-Auslastung	Implementiert	SNMP	
		Traffic-Auslastung	Implementiert	SNMP	Gesamte Traffic-Auslastung
		Traffic-Auslastung	Implementiert	SNMP	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Cisco SNMP	SNMP	SNMPv1 (nur Inventar), SNMPv2, SNMPv3	161		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Cohesity

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
C2500 C2505 C4000 Compute-Node C4600 C5036 C5066 C6025 C6035 C6055 PXG1 UCS-C240M5H10	6.5.1f_Release-20210913_13f6a4bf 6.5.1f_u1_Release-20211027_9e4e40cb 6.6.0d_u6_Release-20221204_c03629f0 6.8.1_Release-20220807_6c9115ef 6.8.1_u1_Release-20221022_6f58ed2a 6.8.1_u2_Release-20230412_5ced2ed3 6.8.1_u3_Release-20230509_1e641b74 7.0_u1_Release-20230222_8995f044

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
710					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Wird Unterstützt			interne Volume Thin Provisioning für die Volume-Ebene
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere zusätzlich Informationen**
		Insgesamt Zugewiesene Kapazität	Implementiert		
		Insgesamt Genutzte Kapazität	Implementiert		Gesamtkapazität in MB
		Typ	Lücke		
		Einheitliche	Implementiert		Handelt es sich um ein Gerät zur Storage-Virtualisierung?
		Verschlüsselt	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

	Implementiert			Durchsatz Beim Lesen	Implementiert
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
	IOPS insgesamt	Implementiert			Latenz – Schreiben
	Implementiert			Auslastung Insgesamt	Implementiert
			Storage Pool Festplatte	IOPS Lesen	Implementiert
		Anzahl der Lese-IOPS auf der Festplatte		IOPS Schreiben	Implementiert
				Durchsatz Beim Lesen	Implementiert
				Durchsatz Schreiben	Implementiert
				Gesamtdurchsatz	Implementiert
		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s		IOPS insgesamt	Implementiert

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Cohesity REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC Celerra (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
NS-480FC NSX VG8 VNX5200 VNX5300 VNX5400 VNX5600 VNX7600	5.5.38-1 6.0.65-2 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.21-303 8.1.9-155

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Ebene zusätzlich unterstützt
		Insgesamt	Implementiert	SSH	
Produkt	**Kategorie**	**Zugehöriges Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Insgesamt Genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Einheitliche	Implementiert	SSH	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Celerra-CLI	SSH	SSH			Richtig	Falsch	Richtig	Richtig

Zurück nach oben

EMC CLARiiON (NaviCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
6.23 6.26 6.28 7.30 7.32 7.33	AX4-5F8 CX3-20f CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.710 04.30.000.5.525 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.236 05.33.009.5.238 05.33.009.6.305 05.33.021.5.256 05.33.021.5.266 2.23.50.5.710 3.26.20.5.011 3.26.40.5.029

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Speicherpool-Id	Implementiert	CLI	
		Thin Provisioning	Implementiert	CLI	
		Typ	Lücke	CLI	
		UUID	Implementiert	CLI	
		Genutzte Kapazität	Implementiert	CLI	
	Volume-Zuordnung	LUN	Implementiert	CLI	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	CLI	
		Storage-Port	Implementiert	CLI	
		Typ	Lücke	CLI	
	Volume-Maske	Initiator	Implementiert	CLI	
		Protokoll-Controller	Implementiert	CLI	
		Storage-Port	Implementiert	CLI	
		Typ	Lücke	CLI	
	Volumenmitglied	Kapazität	Implementiert	CLI	Verwendete Kapazität des Snapshot in MB
		Name	Implementiert	CLI	
		Rang	Implementiert	CLI	
		Gesamtbruttokapazität	Implementiert	CLI	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	CLI	Redundanzebene
		Speicherpool-Id	Implementiert	CLI	
		Genutzte Kapazität	Implementiert	CLI	
	WWN-Alias	Host-Aliase	Implementiert	CLI	
		IP	Implementiert	CLI	
		Objekttyp	Implementiert	CLI	
		Quelle	Implementiert	CLI	
		WWN	Implementiert	CLI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Auslastung Insgesamt	Implementiert	CLI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Cache-Trefferverhältnis Lesen	Implementiert	CLI	
		Cache-Trefferverhältnis Insgesamt	Implementiert	CLI	
		Cache-Trefferverhältnis Schreiben	Implementiert	CLI	
		Bruttokapazität	Implementiert	CLI	
		Gesamtkapazität	Implementiert	CLI	
		Genutzte Kapazität	Implementiert	CLI	
		Verhältnis Der Verwendeten Kapazität	Implementiert	CLI	
		IOPS Lesen	Implementiert	CLI	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	CLI	
		IOPS Schreiben	Implementiert	CLI	
		Latenzleseszeit	Implementiert	CLI	
		Latenz Insgesamt	Implementiert	CLI	
		Latenz – Schreiben	Implementiert	CLI	
		Teilweise Blockielles Verhältnis	Implementiert	CLI	
		Durchsatz Beim Lesen	Implementiert	CLI	
		Gesamtdurchsatz	Implementiert	CLI	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	CLI	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Navi CLI	CLI		6389,2162,2163,443 (HTTPS)/80 (HTTP)		Richtig	Richtig	Richtig	Falsch

Zurück nach oben

EMC Data Domain (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
DD VE DD2200 DD2500 DD3300 DD4200 DD6300 DD6800 DD6900 DD7200 DD9300 DD9400 DD9500 DD9800 DD990 DD9900	6.1.2.051-633576 6.1.2.20-606786 6.1.2.50-632120 6.2.0.30-629757 6.2.0.35-635767 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.0-1017741 7.10.1.0-1042928 7.2.0.30-663847 7.2.0.50-671975 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.6.0.20-689174 7.6.0.30-690691 7.7.0.7-1007134 7.7.1.10-1011247 7.7.2.011-1011427 7.7.2.10-1011249 7.7.3.0-1011963 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.8.0.0-1008134

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		„Rohkapazität zu „nutzbar“			Konvertierung von nutzbarer Kapazität zur Rohkapazität
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Speicherpool-Id	Implementiert	SSH	
		Thin Provisioning Wird Unterstützt	Implementiert	SSH	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	SSH	
		Insgesamt Genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Einheitliche	Implementiert	SSH	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Data Domain CLI	SSH	SSH	22		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC ECS

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
ECS	3.6.1.1 3.6.1.3 3.6.2.1 3.6.2.4 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.5 3.8.0.1 3.8.0.2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		tung des Node nutzbar in MB			
		Kapazitätsnutzung des Nodes in MB	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktionsattribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage-Pool	In Dwh-Kapazität Einbeziehen	Implementiert	HTTPS	Ein Weg von ACQ zu cotnrol, die Stroage Pools sind interessant in DWH Kapazität
		Name	Implementiert	HTTPS	
		Kapazität der physischen Festplatte (MB)	Implementiert	HTTPS	Wird als Rohkapazität für den Storage-Pool verwendet
		Raid-Gruppe	Implementiert	HTTPS	Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	HTTPS	Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning Wird Unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	HTTPS	
		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

					auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut schreiben**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	Bereitgestellte Kapazität	Implementiert	HTTPS	
		Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert	HTTPS	Als Zeitreihe gemeldet
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EMC ECS REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Dell EMC Isilon und PowerScale Rest

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 NL410 S210 X210 X400 X410	9.1.0.11 9.1.0.6 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.16 9.2.1.19 9.2.1.21 9.2.1.6 9.2.1.7 9.2.1.9 9.4.0.11 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.5 9.4.0.7 9.5.0.3 v8.0.0.4 v8.0.0.6 v8.0.0.7 V8.1.2.0 v8.2.2.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	HTTPS	Verhältnis zur Konvertierung von nutzbarer
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Zugewiesene Kapazität Am Snapshot	Lücke	HTTPS	Zugewiesene Kapazität von Snapshots in MB
		Verwendete Snapshot-Kapazität	Implementiert	HTTPS	
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning Wird Unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	HTTPS	
		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Verwendeten Snapshot-Technologie			
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
REST-API von EMC Isilon und PowerScale	HTTPS		443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Dell EMC Isilon/PowerScale (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
A200 A2000 A300 F200 F800 F900 H400 H500 H600 H700 NL400 NL410 S210 X200 X210 X400 X410	9.1.0.10 9.1.0.12 9.1.0.16 9.1.0.18 9.1.0.19 9.1.0.7 9.2.1.11 9.2.1.13 9.2.1.15 9.2.1.22 9.2.1.7 9.2.1.9 9.3.0.3 9.4.0.0 9.4.0.10 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.6 9.4.0.7 v7.1.1.8 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 V8.1.2.0 v8.2.2.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Ebene zusätzlich unterstützt
		Insgesamt	Implementiert	SSH	

Produkt	Kategorie	Zugehöriges Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Insgesamt Genutzte Kapazität	Implementiert	SSH	Gesamtkapazität in MB
		Typ	Lücke	SSH	
		Einheitliche	Implementiert	SSH	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz Schreiben	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	Bereitgestellte Kapazität	Implementiert	SSH	
		Bruttokapazität	Implementiert	SSH	
		Gesamtkapazität	Implementiert	SSH	
		Genutzte Kapazität	Implementiert	SSH	
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert	SSH	Als Zeitreihe gemeldet
		Verhältnis Der Verwendeten Kapazität	Implementiert	SSH	
		Gesamtkapazität Daten	Implementiert	SSH	
		Genutzte Kapazität Von Daten	Implementiert	SSH	
		Reservierte Snapshot-Kapazität	Implementiert	SSH	
		Verwendete Snapshot-Kapazität	Implementiert	SSH	
		Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie	Implementiert	SSH	Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Isilon SSH	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

EMC PowerStore REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5000X PowerStore 9000T PowerStore 9200T	2.0.1.3 2.1.1.0 2.1.1.1 3.0.0.1 3.2.0.0 3.2.0.1 3.2.1.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke		
		Einheitliche	Implementiert		Handelt es sich um ein Gerät zur

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen?
	Datenmenge	Kapazität	Implementiert		Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert		
		Name	Implementiert		
		Gesamtbruttokapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-Id	Implementiert		
		Thin Provisioning	Implementiert		
		Typ	Lücke		
		UUID	Implementiert		
		Genutzte Kapazität	Implementiert		
		QoS: Richtlinie	Implementiert		
	Volume-Zuordnung	LUN	Implementiert		Der Name der Backend-lun
		Maskierung Erforderlich	Implementiert		
		Protokoll-Controller	Implementiert		
		Storage-Port	Implementiert		
		Typ	Lücke		
	Volume-Maske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Typ	Lücke		
	WWN-Alias	Host-Aliase	Implementiert		
		Objekttyp	Implementiert		
		Quelle	Implementiert		
		WWN	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

			und Schreibvorgänge auf allen		
Produkt	**Kategorie**	**Funktion/Attribut**	**Statistiken** (Festplatten) in MB/s	**Verwendetes Protokoll**	**Weitere Informationen**
	Implementiert			Datenmenge	Bruttokapazität
	Implementiert				Gesamtkapazität
	Implementiert				Genutzte Kapazität
	Implementiert				Verhältnis Der Verwendeten Kapazität
	Implementiert				IOPS Lesen
	Implementiert		Anzahl der Lese-IOPS auf der Festplatte		IOPS insgesamt
	Implementiert				IOPS Schreiben
	Implementiert				Latenzleseszeit
	Implementiert				Latenz Insgesamt
	Implementiert				Latenz – Schreiben
	Implementiert				Durchsatz Beim Lesen
	Implementiert				Gesamtdurchsatz
	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s		Durchsatz Schreiben

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EMC POWERSTORE REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC RecoverPoint (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
RecoverPoint	5.1.P1(c.175) 5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(Std.97)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

		Festplatten)			
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Storage-Node	Speichergröße	Lücke	HTTPS	Gerätespeicher in MB
		Modell	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Prozessoranzahl	Implementiert	HTTPS	Geräte-CPU
		Seriennummer	Implementiert	HTTPS	
		Bundesland	Implementiert	HTTPS	Kostenloser Text, der den Gerätestatus beschreibt
		UUID	Implementiert	HTTPS	
		Version	Implementiert	HTTPS	Softwareversion
	Storage-Synchronisierung	Modus	Implementiert	HTTPS	
		Modus Enum	Implementiert	HTTPS	
		Quell-Storage	Implementiert	HTTPS	
		Quell-Volume	Implementiert	HTTPS	
		Bundesland	Implementiert	HTTPS	Kostenloser Text, der den Gerätestatus beschreibt
		Staatsummen	Implementiert	HTTPS	
		Ziel-Storage	Implementiert	HTTPS	
		Ziel-Volume	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die Storage-Effizienz verändert

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
RecoverPoint-REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC ScaleIO und PowerFlex REST

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
ScaleIO	R2_6.11000.113 R2_6.11000.115 R3_0.1400.101 R3_5.1200.104 R3_6.500.113 R3_6.700.103

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen?**
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Host-IPs	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
					Schreibvorgänge auf allen Festplatten) in MB/s
		IOPS insgesamt	Implementiert		
	Datenmenge	Bruttokapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		IOPS Lesen	Implementiert		Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert		
		IOPS Schreiben	Implementiert		
		Durchsatz Beim Lesen	Implementiert		
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert		

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EMC ScaleIO und PowerFlex REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC Symmetrix CLI

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
V10.0.0.0 V10.0.1.0 V7.6.2.67 V8.3.0.22 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.18 V9.1.0.5 V9.1.0.6 V9.2.0.0 V9.2.1.0 V9.2.1.1 V9.2.1.2 V9.2.2.0 V9.2.3.0 V9.2.3.1 V9.2.3.4 V9.2.3.5 V9.2.3.6 V9.2.4.1 V9.2.4.2	DMX3-24 DMX4-24 PMax2000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5773.198.142 (168D0000) Build 5 5876.272.177 (16F40000) Build 39 5876.286.194 (16F40000) Build 115 5876.309.196 (16F40000) Build 162 5977.1131.1131(17590000) Build 551 5977.1151.1151(17590000) Build 45 5977.1151.1151(17590000) Build 59 5977.1151.1151(17590000) Build 60 5977.1151.1151(17590000) Build 9 5978.479.479 (175A0000) Build 195 5978.711.711 (175A0000) Build 113 5978.711.711 (175A0000) Build 139 5978.711.711 (175A0000) Build 149 5978.711.711 (175A0000) Build 194 5978.711.711 (175A0000) Build 196 5978.711.711 (175A0000) Build 220 5978.711.711 (175A0000) Build 239 5978.711.711 (175A0000) Build 252 5978.711.711 (175A0000) Build 267 5978.711.711 (175A0000) Build 278 5978.711.711 (175A0000) Build 287 5978.711.711 (175A0000) Build 335 5978.711.711 (175A0000) Build 365 5978.711.711 (175A0000) Build 366 5978.711.711 (175A0000) Build 388 5978.711.711 (175A0000) Build 416 5978.711.711 (175A0000) Build 436 5978.711.711 (175A0000) Build 438 5978.711.711 (175A0000) Build 448

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert		
		Storage-Port	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status Lücke**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volumenmitglied	Automatisiertes Tiering	Implementiert		Gibt an, ob dieser storagepool an Auto-Tiering mit anderen Pools beteiligt ist
		Kapazität	Implementiert		Verwendete Kapazität des Snapshot in MB
		Zylinder	Implementiert		
		Name	Implementiert		
		Rang	Implementiert		
		Gesamtbruttokapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert		Redundanzebene
		Speicherpool-Id	Implementiert		
		UUID	Implementiert		
		Genutzte Kapazität	Implementiert		
	Volumenreferenz	Name	Implementiert		
		Storage-Ip	Implementiert		
	WWN-Alias	Host-Aliase	Implementiert		
		Objekttyp	Implementiert		
		Quelle	Implementiert		
		WWN	Implementiert		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					und Schreibvorgänge auf allen
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	Weiteren) in MB/s **Informationen**
		Durchsatz Schreiben	Implementiert		
		„Ausstehend“	Implementiert		Insgesamt ausstehend

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
symcli	CLI		2707		Richtig	Richtig	Richtig	Richtig
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		Richtig	Falsch	Falsch	Richtig

Zurück nach oben

Dell Unisphere REST

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
V10.0.0.5 V10.0.1.3 V9.2.1.6 V9.2.3.20 V9.2.3.22 V9.2.3.4 V9.2.4.1	PowerMax_2000 PowerMax_2500 PowerMax_8000 VMAX250F VMAX950F	5978.479.479 Build 350 5978.711.711 Build 252 5978.711.711 Build 278 Build 278 5978.711.711 Build 287 5978.711.711 Build 329 Build 329 5978.711.711 Build 365 5978.711.711 Build 365 Build 365 5978.711.711 Build 376 5978.711.711 Build 388 Build 388 5978.711.711 Build 416 5978.711.711 Build 435 5978.711.711 Build 448 5978.711.711 Build 461 Build 461 5978.711.711 Build 481 Build 481 5978.711.711 Build 484 5978.711.711 Build 484 Build 484 5978.711.711 Build 502 6079.125.0 Build 53 Build 53 6079.175.0 Build 0 Build 0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
840					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	WWN-Alias	Host-Aliase	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	
		Quelle	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Schreiben				
	Implementiert	HTTPS		Datenmenge	Bruttokapazität
	Implementiert	HTTPS			Gesamtkapazität
	Implementiert	HTTPS			Genutzte Kapazität
	Implementiert	HTTPS			Verhältnis Der Verwendeten Kapazität
	Implementiert	HTTPS			KapazitätRatio geschrieben
	Implementiert	HTTPS			IOPS Lesen
	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte		IOPS insgesamt
	Implementiert	HTTPS			IOPS Schreiben
	Implementiert	HTTPS			Latenzleseszeit
	Implementiert	HTTPS			Latenz Insgesamt
	Implementiert	HTTPS			Latenz – Schreiben
	Implementiert	HTTPS			Durchsatz Beim Lesen
	Implementiert	HTTPS			Gesamtdurchsatz
	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s		Durchsatz Schreiben

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Dell Unisphere-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC VNX (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VNX5300 VNX5400 VNX5700 VNX5800	05.33.009.5.231 7.1.76-4 7.1.80-3 8.1.9-232

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
850					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Storage-Port	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	SSH	
	Volume-Maske	Storage-Port	Implementiert	SSH	
		Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Typ	Lücke	SSH	
	WWN-Alias	Quelle	Implementiert	SSH	
		Host-Aliase	Implementiert	SSH	
		WWN	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		IP	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Auslastung Insgesamt	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage	Fehlerhafte Bruttokapazität	Implementiert	SSH	
		Bruttokapazität	Implementiert	SSH	
		Freie Rohkapazität	Implementiert	SSH	RAW capapCity of Spare Disks (Summe aller freien Festplatten)
		Storage Pools: Kapazität	Implementiert	SSH	
		IOPS Sonstiges	Implementiert	SSH	
		IOPS Lesen	Implementiert	SSH	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	SSH	
		IOPS Schreiben	Implementiert	SSH	
		Latenzleseszeit	Implementiert	SSH	
		Latenz Insgesamt	Implementiert	SSH	
		Latenz – Schreiben	Implementiert	SSH	
		Durchsatz Beim Lesen	Implementiert	SSH	
		Gesamtdurchsatz	Implementiert	SSH	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	SSH	
	Storage-Node	IOPS Lesen	Implementiert	SSH	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	SSH	
		IOPS Schreiben	Implementiert	SSH	
		Auslastung Insgesamt	Implementiert	SSH	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
VNX SSH UND CLI	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

EMC VNXe und Unity Unisphere (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Unity 300 Unity 300F Unity 350F Unity 380 Unity 380F Unity 400 Unity 400F Unity 450F Unity 480F Unity 500 Unity 550F Unity 600 Unity 600F Unity 650F Unity 680F Unity 880 VNXe3200	3.1.17.10223906 3.1.17.10229825 4.1.2.9257522 4.2.1.9535982 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.2.2.0.6.201 5.3.0.0.5.120

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Ziel-Volume	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die Storage-Effizienz verwendet

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

			und Schreibvorgänge auf allen		
Produkt	**Kategorie**	**Funktion/Attribut**	**Festplatten) in MB/s**	**Verwendetes Protokoll**	**Weitere Informationen**
	Implementiert	HTTPS		Datenmenge	Bruttokapazität
	Implementiert	HTTPS			Gesamtkapazität
	Implementiert	HTTPS			Genutzte Kapazität
	Implementiert	HTTPS			Verhältnis Der Verwendeten Kapazität
	Implementiert	HTTPS			IOPS Lesen
	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte		IOPS insgesamt
	Implementiert	HTTPS			IOPS Schreiben
	Implementiert	HTTPS			Latenz Insgesamt
	Implementiert	HTTPS			Durchsatz Beim Lesen
	Implementiert	HTTPS			Gesamtdurchsatz
	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s		Durchsatz Schreiben

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
VNXe und Unisphere CLI	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC VPLEX

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VPLEX	5.4.1.00.00.07 5.4.1.01.00.05 6.2.0.03.00.02 6.2.0.04.00.07 6.2.0.05.00.11 6.2.0.07.00.02

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		UUID	Implementiert	HTTP/S	
		Einheitliche	Implementiert	HTTP/S	Handelt es sich um ein Gerät zur
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen?**
	Volume-Zuordnung	LUN	Implementiert	HTTP/S	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTP/S	
		Storage-Port	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Volume-Maske	Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Storage-Port	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz Schreiben	Implementiert	SSH	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	Bereitgestellte Kapazität	Implementiert	SSH	
		Gesamtkapazität	Implementiert	SSH	
		Genutzte Kapazität	Implementiert	SSH	
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert	SSH	Als Zeitreihe gemeldet
		Verhältnis Der Verwendeten Kapazität	Implementiert	SSH	
		Sonstige Gesamtkapazität	Implementiert	SSH	
		Andere Genutzte Kapazität	Implementiert	SSH	
	Datenmenge	Bruttokapazität	Implementiert	SSH	
		Gesamtkapazität	Implementiert	SSH	
		IOPS insgesamt	Implementiert	SSH	
		Latenzleseszeit	Implementiert	SSH	
		Latenz Insgesamt	Implementiert	SSH	
		Latenz – Schreiben	Implementiert	SSH	
		Durchsatz Beim Lesen	Implementiert	SSH	
		Gesamtdurchsatz	Implementiert	SSH	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	SSH	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EMC VPLEX-CLI	SSH	SSH	22		Richtig	Richtig	Richtig	Richtig
EMC VPLEX-API	HTTP/HTTPS	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

EMC XtremIO (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
6.2.1 6.2.2 6.3.1 6.3.2 6.3.3 6.4.0	1 Bricks und 125 TB 1 Bricks und 24 TB 1 Bricks und 26 TB 1 Bricks und 31 TB 1 Bricks und 62 TB 1 Bricks und 8 TB 1 X 10 TB 1 X 20 TB 1 X 40 TB 2 Bricks und 52 TB 2 Bricks und 62 TB 2 Bricks und 76TB 2 Bricks und 83 TB 2 X 10 TB 2 X 20 TB 2 X 40 TB 3 Bricks und 251 TB 3 Bricks und 283 TB 4 Bricks und 125 TB 4 Bricks und 503 TB 4 Bricks und 628 TB 4 Bricks und 754 TB 4 X 20 TB 4 X 40 TB 6 X 20 TB	4.0.27-1 4.0.31-11 6.1.0-99_X2 6.3.3-8_X2 6.4.0-22_X2 6.4.0-36_Hotfix_2_X2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Ziel-Volume	Implementiert	HTTPS	
		Technologie	Implementiert	HTTPS	Technologie, die Storage-Effizienz verwendet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		Festplattengröße	Implementiert	HTTPS	Kommagetrennte Liste der Festplattengrößen (GB)
		Festplattengeschwindigkeit	Implementiert	HTTPS	Kommagetrennte Liste von Festplattengeschwindigkeiten (rpm)
		Festplattentyp	Nicht Verfügbar	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzebene
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		UUID	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamtkapazität Daten	Implementiert	HTTPS	
		Genutzte Kapazität Daten	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Teilweise Blockielles Verhältnis	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
EMC XTREMIO REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp E-Series

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2600 2660 2680 2702 2704 2.800 MRD. 2804 2806 3000 5480 5486 5488 5504 5564 5600 5700 5700B 6000	08.40.60.01 8.10.14.0 8.20.11.0 8.20.27.0 8.20.30.0 8.20.5.0 8.20.8.0 8.25.14.0 8.25.6.0 8.30.1.0 8.40.0.1 8.40.0.3 8.40.20.0 8.40.30.3 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.20.0 8.50.0.3 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	RMI	
		Einheitliche	Implementiert	RMI	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Kapazität	Implementiert	RMI	Verwendete Kapazität des Snapshot in MB
		Festplattentyp	Nicht Verfügbar	RMI	
		Name	Implementiert	RMI	
		Gesamtbruttokapazität	Implementiert	RMI	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	RMI	Redundanzebene
		Speicherpool-Id	Implementiert	RMI	
		Thin Provisioning	Implementiert	RMI	
		Typ	Lücke	RMI	
		UUID	Implementiert	RMI	
		Genutzte Kapazität	Implementiert	RMI	
		Einheitliche	Implementiert	RMI	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
		Geschriebene Kapazität	Implementiert	RMI	Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde
	Volume-Zuordnung	LUN	Implementiert	RMI	Der Name der Backend-lun
		Storage-Port	Implementiert	RMI	
		Typ	Lücke	RMI	
	Volume-Maske	Initiator	Implementiert	RMI	
		Storage-Port	Implementiert	RMI	
		Typ	Lücke	RMI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					und Schreibvorgänge auf allen
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz Schreiben	Implementiert	RMI	Weiteren) in MB/s

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
SANtricity API	RMI	TCP			Richtig	Richtig	Falsch	Falsch

Zurück nach oben

Google Cloud Computing

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
v1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		OID	Implementiert	HTTPS	
	Info	Api-Beschreibung	Implementiert	HTTPS	
		Api-Name	Implementiert	HTTPS	
		Api-Version	Implementiert	HTTPS	
		Name der Datenquelle	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Ersteller-ID	Implementiert	HTTPS	
		Erstellschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Schreiben	Implementiert	HTTPS	
	vm	Gesamtkapazität	Implementiert	HTTPS	
		Gesamtzahl der CPU-Auslastung	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		DiskIops.total	Implementiert	HTTPS	
		Festplatten-IOPS Schreiben	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Festplattendurchsatz	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	Gesamtauslesen des Festplattendurchsatzes
		Festplattendurchsatz Schreiben	Implementiert	HTTPS	
		IP-Durchsatz Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	IP-Durchsatz insgesamt
		IpThrughput.write	Implementiert	HTTPS	
		Gesamte Speicherauslastung	Implementiert	HTTPS	
		swapRate.inRate	Implementiert	HTTPS	
		Swap-Rate	Implementiert	HTTPS	
		Gesamtpausenrate	Implementiert	HTTPS	
		Legen Sie die Wartezeit fest	Implementiert	HTTPS	Warten auf geplante Zeit in Prozent

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Google Compute-Plattform REST-API	HTTPS		443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

HDS HCP (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Hitachi Content Platform	9.3.7.2 9.5.0.121

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

		Durchsatz Schreiben	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut insgesamt**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	Gesamtkapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		Bereitgestellte Kapazität	Implementiert		
		Genutzte Kapazität	Implementiert		
		Bruttokapazität	Implementiert		
		Kapazitätsgrenze	Implementiert		
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert		Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
HDS HCP REST API	HTTPS	HTTPS	9090		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

HiCommand Device Manager

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
7.6.1 8.7.7 8.8.1 8.8.3 8.8.5	DF850MH DF850S HM800 HM850 P9500 RAID700 RAID800 VSP5000 XP24000 XP7	0983/A-H 0988/H-S DKC: 60-08-22 DKC: 60-08-65 DKC: 70-06-46 DKC: 70-06-67-00/00 DKC: 80-06-80 DKC: 80-06-82-00/00 DKC: 80-06-86-00/00 DKC: 80-06-87 DKC: 80-06-88-00/00 DKC: 80-06-91 DKC: 80-06-91-00/00 DKC: 80-06-93-00/00 DKC: 83-05-45-40/00 DKC: 83-05-45-60/00 DKC: 83-05-46-60/00 DKC: 83-05-47-60/00 DKC: 83-05-48-40/00 DKC: 83-05-48-60/00 DKC: 88-08-08-60/00 DKC: 88-08-09-60/00 DKC: 90-08-81-00/00 DKC: 90-08-83-00/01 SVP: 60-08-21/00 SVP: 60-08-54/00 SVP: 70-06-32/00 SVP: 70-06-51/00 SVP: 80-06-76/02 SVP: 80-06-78/00 SVP: 80-06-81/00 SVP: 80-06-82/00 SVP: 80-06-83/00 SVP: 80-06-86/00 SVP: 80-06-88/00 SVP: 83-05-49-40/00 SVP: 83-05-49-60/00 SVP: 83-05-50-60/00 SVP: 83-05-51-60/00 SVP: 83-05-52-40/00 SVP: 83-05-52-60/00 SVP: 88-08-10-60/00 SVP: 88-08-11-60/00 SVP: 90-08-81/00 SVP: 90-08-83/00

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Speicherpool-Id	Implementiert	HDS-XML-API	
		Thin Provisioning Typ	Implementiert	HDS-XML-API	
		Tiering	Lücke	HDS-XML-API	
		Genutzte Kapazität	Implementiert	HDS-XML-API	
		Einheitliche	Implementiert	HDS-XML-API	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
	Volume-Zuordnung	LUN	Implementiert	HDS-XML-API	Der Name der Backend-lun
		Maskierung Erforderlich	Implementiert	HDS-XML-API	
		Protokoll-Controller	Implementiert	HDS-XML-API	
		Storage-Port	Implementiert	HDS-XML-API	
	Volume-Maske	Initiator	Implementiert	HDS-XML-API	
		Protokoll-Controller	Implementiert	HDS-XML-API	
		Storage-Port	Implementiert	HDS-XML-API	
	Volumenmitglied	Name	Implementiert	HDS-XML-API	
		Speicherpool-Id	Implementiert	HDS-XML-API	
		Rang	Implementiert	HDS-XML-API	
		Zylinder	Implementiert	HDS-XML-API	
		Kapazität	Implementiert	HDS-XML-API	Verwendete Kapazität des Snapshot in MB
		Gesamtbruttokapazität	Implementiert	HDS-XML-API	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Genutzte Kapazität	Implementiert	HDS-XML-API	
	WWN-Alias	Host-Aliase	Implementiert	HDS-XML-API	
		Objekttyp	Implementiert	HDS-XML-API	
		Quelle	Implementiert	HDS-XML-API	
		WWN	Implementiert	HDS-XML-API	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazitätsgrenze	Implementiert	Export/CLI	
		Kapazitätsverhältnis	Implementiert	Export/CLI	Als Zeitreihe gemeldet
Produkt	**Kategorie**	**Funktion/Attribut festsetzen**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Latenz Insgesamt	Implementiert	Export/CLI	
		IOPS Lesen	Implementiert	Export/CLI	Anzahl der Lese-IOPS auf der Festplatte
		Latenzleseszeit	Implementiert	Export/CLI	
		Cache-Trefferverhältnis Lesen	Implementiert	Export/CLI	
		IOPS Schreiben	Implementiert	Export/CLI	
		Cache-Trefferverhältnis Insgesamt	Implementiert	Export/CLI	
		Cache-Trefferverhältnis Schreiben	Implementiert	Export/CLI	
		Durchsatz Beim Lesen	Implementiert	Export/CLI	
		Durchsatz Schreiben	Implementiert	Export/CLI	
		Gesamtdurchsatz	Implementiert	Export/CLI	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		IOPS insgesamt	Implementiert	Export/CLI	
		Latenz – Schreiben	Implementiert	Export/CLI	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Exportdienstprogramm (USPV) / SNM CLI (AMS)	Export/CLI				Falsch	Falsch	Falsch	Falsch
HiCommand Device Manager-XML-API	HDS-XML-API	HTTP/HTTPS	2001		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Hitachi Ops Center (Hds)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
VSP 5100 VSP 5500 VSP F1500 VSP F600 VSP G800	80-06-92-00/00:01-65-03/05 83-05-46-60/00:01-65-03/05 83-05-47-40/00:01-65-03/05 83-05-48-40/00:01-65-03/05 90-08-81-00/00:01-65-03/05 90-08-82-00/00:01-65-03/05

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Ziel-Storage	Implementiert		
		Technologie	Implementiert		Technologie, die Storage-Effizienz verwendet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Kapazität	Implementiert		Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert		
		Name	Implementiert		
		Schutzart	Implementiert		
		Gesamtbruttokapazität	Implementiert		Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-Id	Implementiert		
		Thin Provisioning	Implementiert		
		Typ	Lücke		
		Genutzte Kapazität	Implementiert		
		Komprimierung Aktiviert	Implementiert		
	Volume-Zuordnung	LUN	Implementiert		Der Name der Backend-lun
		Maskierung Erforderlich	Implementiert		
		Protokoll-Controller	Implementiert		
		Storage-Port	Implementiert		
		Typ	Lücke		
	Volume-Maske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Storage-Port	Implementiert		
		Typ	Lücke		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					
950					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Schreibvorgänge auf allen Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		IOPS insgesamt	Implementiert		
	Storage Pool Festplatte	Gesamtkapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		Bereitgestellte Kapazität	Implementiert		
		Genutzte Kapazität	Implementiert		
		Bruttokapazität	Implementiert		
		Kapazitätsgrenze	Implementiert		
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert		Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Hitachi Ops Center REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

HDS HNAS (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
G600 G800 HNAS 4080 HNAS 4100 N800	13.9.6918.05 14.5.7413.01 14.6.7520.04

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Geschützte Kapazität			in MB
		Insgesamt	Implementiert	SSH	
Produkt	**Kategorie**	**Zugehöriges Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Kapazität			
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	SSH	Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
HDS HNAS CLI	SSH	SSH	22		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

HPE Nimble/Alletra 6000 Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
v1	6030 AF1000 AF20Q AF3000 AF40 AF5000 CS1000 CS300 CS3000 CS500 CS5000 HF20 HF20H HF40 HF60	5.0.10.0-742719-opt 5.0.7.0-604814-opt 5.0.8.0-677726-opt 5.2.1.1000-1017822-opt 5.2.1.400-796142-opt 5.2.1.600-841103-opt 5.2.1.700-882343-opt 5.2.1.800-930936-opt 5.2.1.900-1003439-opt 6.0.0.300-956221-opt 6.0.0.400-991061-opt 6.1.1.200-1020304-opt 6.1.1.300-1028597-opt

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Typ	Lücke	HTTPS	
	WWN-Alias	Host-Aliase	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	
		Quelle	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Schreiben	Implementiert	HTTPS	
	Datenmenge	Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		Gesamteinsparungen Durch Komprimierung	Implementiert	HTTPS	
		Speicherersparnis Durch Komprimierung	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
HP NIMBLE REST API	HTTPS	HTTPS	5392		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

Huawei OceanStor (REST/HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
5300 V5 5500 V3 5500 V5 5800 V3 Dorado 5000 V6 SAS Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V600R003C00 V600R005C03

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzebene
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Latenz – Schreiben	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Cache-Trefferverhältnis Lesen	Implementiert	HTTPS	
		Cache-Trefferverhältnis Insgesamt	Implementiert	HTTPS	
		Cache-Trefferverhältnis Schreiben	Implementiert	HTTPS	
		Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Huawei OceanStor REST-API	HTTPS	HTTPS	8088		Richtig	Richtig	Richtig	Richtig
Huawei OceanStor Performance REST API	HTTPS	HTTPS	8088		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

IBM Cleversafe

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		UUID	Implementiert	HTTPS	
		Version	Implementiert	HTTPS	Softwareversion
Produkt	**Kategorie**	**Management-Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Management-IP-Adressen	Implementiert	HTTPS	
	Storage-Pool	In Dwh-Kapazität Einbeziehen	Implementiert	HTTPS	Ein Weg von ACQ zu cotnrol, die Stroage Pools sind interessant in DWH Kapazität
		Name	Implementiert	HTTPS	
		Kapazität der physischen Festplatte (MB)	Implementiert	HTTPS	Wird als Rohkapazität für den Storage-Pool verwendet
		Raid-Gruppe	Implementiert	HTTPS	Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	HTTPS	Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning Wird Unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	HTTPS	
		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
IBM CLEVERSAFE REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

IBM DS 8K (DSCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2107-951 2107-961 2107-985 2107-996	7.6.31.4250 7.7.51.1400 7.8.57.18 7.9.21.91 7.9.32.126

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Volume-Maske	Initiator	Implementiert	DSNI	
		Protokoll-Controller	Implementiert	DSNI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Storage-Port	Implementiert	DSNI	
	WWN-Alias	Host-Aliase	Implementiert	DSNI	
		Host-Betriebssystem	Implementiert	DSNI	
		Objekttyp	Implementiert	DSNI	
		Quelle	Implementiert	DSNI	
		WWN	Implementiert	DSNI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Auslastung Insgesamt	Implementiert	DSNI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Cache-Trefferverhältnis Lesen	Implementiert	DSNI	
		Cache-Trefferverhältnis Insgesamt	Implementiert	DSNI	
		Cache-Trefferverhältnis Schreiben	Implementiert	DSNI	
		Bruttokapazität	Implementiert	DSNI	
		Gesamtkapazität	Implementiert	DSNI	
		IOPS Lesen	Implementiert	DSNI	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	DSNI	
		IOPS Schreiben	Implementiert	DSNI	
		Latenzleseszeit	Implementiert	DSNI	
		Latenz Insgesamt	Implementiert	DSNI	
		Latenz – Schreiben	Implementiert	DSNI	
		Durchsatz Beim Lesen	Implementiert	DSNI	
		Gesamtdurchsatz	Implementiert	DSNI	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	DSNI	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Konfiguration des Datenquellenassistenten	Manuelle Eingabe				Richtig	Richtig	Richtig	Richtig
IBM DS-CLI	DSNI	DSNI			Richtig	Richtig	Richtig	Richtig

Zurück nach oben

IBM PowerVM (SSH)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1004					

		Name	Implementiert	SSH	
		OID	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut Typ	Status Lücke	Verwendetes Protokoll	Weitere Informationen
	Virtual Machine	Dns-Name	Implementiert	SSH	
		Gaststaat	Implementiert	SSH	
		Host-OID	Implementiert	SSH	
		IPS	Implementiert	SSH	
		MOID	Implementiert	SSH	
		Speicher	Implementiert	SSH	
		Name	Implementiert	SSH	
		OID	Implementiert	SSH	
		BETRIEBSSYSTEM	Implementiert	SSH	
		Stromzustand	Implementiert	SSH	
		Zeit Für Statusänderungen	Implementiert	SSH	
		Prozessoren	Implementiert	SSH	
	VirtualMachine Disk	OID	Implementiert	SSH	
		VirtualisierungsDisk OID	Implementiert	SSH	
		OID der Virtual Machine	Implementiert	SSH	
	Host	Host-Cpu-Anzahl	Implementiert	SSH	
		Host-Installierter Speicher	Implementiert	SSH	
		Host-Modell	Implementiert	SSH	
		Anzahl der NIC	Implementiert	SSH	
		IPS	Implementiert	SSH	
		Hersteller	Implementiert	SSH	
		Name	Implementiert	SSH	
		OID	Implementiert	SSH	
		Plattformtyp	Implementiert	SSH	
	Info	Name der Datenquelle	Implementiert	SSH	Info
		Datum	Implementiert	SSH	
		Ersteller-ID	Implementiert	SSH	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
SSH-Zugriff auf die IBM Hardware Management Console	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

IBM SVC (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
2072-12F 2072-12 G 2072-2N4 2072-324 2072-3H4 2072-3N4 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-624 2076-724 2076-824 2076-AF6 2076-AFF 2077-24F 2077-424 2078-12F 2078-224 2078-24C 2078-24F 2078-324 2078-424 2078-4H4 2078 G 2078-AF3 4657-924 4662-12 G 4662-6H2 4666-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AE2 9848-AF7 9848-AF8 9848-AG8 SERVICE	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.5.0.11 7.5.0.12 7.7.1.8 7.8.1.14 7.8.1.6 7.8.1.8 8.2.1.10 8.2.1.11 8.2.1.14 8.2.1.9 8.3.1.1 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.6 8.4.0.7 8.4.0.8 8.4.0.9 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.5.2.2 8.5.3.1 8.5.4.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1008					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität			
		Einheitliche	Implementiert	SSH	Handelt es sich um ein Gerät zur
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen?**
		Geschriebene Kapazität	Implementiert	SSH	Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde
		Komprimierung Aktiviert	Implementiert	SSH	
		Verschlüsselt	Implementiert	SSH	
	Volume-Zuordnung	LUN	Implementiert	SSH	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	SSH	
		Storage-Port	Implementiert	SSH	
	Volume-Maske	Initiator	Implementiert	SSH	
		Protokoll-Controller	Implementiert	SSH	
		Storage-Port	Implementiert	SSH	
		Typ	Lücke	SSH	
	WWN-Alias	Host-Aliase	Implementiert	SSH	
		Objekttyp	Implementiert	SSH	
		Quelle	Implementiert	SSH	
		WWN	Implementiert	SSH	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					und Schreibvorgänge auf allen
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz Schreiben	Implementiert	SSH	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
IBM SVC-CLI	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

IBM XIV UND A9000 (XIVCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
415 A14	10.2.4.e 12.3.2.c

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Typ	Lücke	XIV CLI	
		Einheitliche	Implementiert	XIV CLI	Handelt es sich um ein Gerät zur
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen?**
	Datenmenge	Kapazität	Implementiert	XIV CLI	Verwendete Kapazität des Snapshot in MB
		DiskGroup	Implementiert	XIV CLI	Typ Der Festplattengruppe
		Festplattentyp	Nicht Verfügbar	XIV CLI	
		Name	Implementiert	XIV CLI	
		Qtree-Id	Implementiert	XIV CLI	Eindeutige id des qtree
		Gesamtbruttokapazität	Implementiert	XIV CLI	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	XIV CLI	Redundanzebene
		Speicherpool-Id	Implementiert	XIV CLI	
		Thin Provisioning	Implementiert	XIV CLI	
		Typ	Lücke	XIV CLI	
		Genutzte Kapazität	Implementiert	XIV CLI	
		Komprimierung Aktiviert	Implementiert	XIV CLI	
	Volume-Zuordnung	LUN	Implementiert	XIV CLI	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	XIV CLI	
	Volume-Maske	Initiator	Implementiert	XIV CLI	
		Protokoll-Controller	Implementiert	XIV CLI	
	WWN-Alias	Host-Aliase	Implementiert	XIV CLI	
		Host-Betriebssystem	Implementiert	XIV CLI	
		Objekttyp	Implementiert	XIV CLI	
		Quelle	Implementiert	XIV CLI	
		WWN	Implementiert	XIV CLI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					
1028					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Bruttokapazität	Implementiert	DSNI	
		Kapazitätsverhältnis Zu Festsetzen	Implementiert	DSNI	Als Zeitreihe gemeldet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Latenz Insgesamt	Implementiert	DSNI	
		Latenzleseszeit	Implementiert	DSNI	
		IOPS Schreiben	Implementiert	DSNI	
		Speicherersparnis Durch Komprimierung	Implementiert	DSNI	
		Durchsatz Beim Lesen	Implementiert	DSNI	
		IOPS insgesamt	Implementiert	DSNI	
		Latenz – Schreiben	Implementiert	DSNI	
		IOPS Lesen	Implementiert	DSNI	Anzahl der Lese-IOPS auf der Festplatte
		Cache-Trefferverhältnis Lesen	Implementiert	DSNI	
		Gesamteinsparungen Durch Komprimierung	Implementiert	DSNI	
		Cache-Trefferverhältnis Insgesamt	Implementiert	DSNI	
		Cache-Trefferverhältnis Schreiben	Implementiert	DSNI	
		Durchsatz Schreiben	Implementiert	DSNI	
		Gesamtdurchsatz	Implementiert	DSNI	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
IBM DS-CLI	DSNI	DSNI			Richtig	Richtig	Richtig	Richtig
IBM XIV CLI	XIV CLI	TCP	7778		Richtig	Falsch	Richtig	Falsch

Zurück nach oben

Infiniat Infinibox (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
F6230 F6240 F6303 F6304	6.0.31.0 7.0.14.20

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1032					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					(Summe aller Festplatten im Array)
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Kapazität	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		Storage-Port	Implementiert	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		Storage-Port	Implementiert	HTTPS	
	WWN-Alias	Quelle	Implementiert	HTTPS	
		Host-Aliase	Implementiert	HTTPS	
		WWN	Implementiert	HTTPS	
		Objekttyp	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Infinidat REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Microsoft Azure Computing

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
1 2018-06-01

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Hersteller	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		OID	Implementiert	HTTPS	
	Info	Api-Beschreibung	Implementiert	HTTPS	
		Api-Name	Implementiert	HTTPS	
		Api-Version	Implementiert	HTTPS	
		Name der Datenquelle	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Ersteller-ID	Implementiert	HTTPS	
		Erstellschlüssel	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					
1044					

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktionsname/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	vm	Gesamtzahl der CPU-Auslastung	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		DiskIops.total	Implementiert	HTTPS	
		Festplatten-IOPS Schreiben	Implementiert	HTTPS	
		Festplattendurchsatz	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	Gesamtauslesen des Festplattendurchsatzes
		Festplattendurchsatz Schreiben	Implementiert	HTTPS	
		IP-Durchsatz Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	IP-Durchsatz insgesamt
		IpThrughput.write	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Microsoft Azure Compute-REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Microsoft Hyper-V

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Bereitgestellte Kapazität	Implementiert	WMI	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Bereitgestellte Kapazität	Implementiert	WMI	
	VirtualMachine Disk	OID	Implementiert	WMI	
		VirtualisierungsDisk OID	Implementiert	WMI	
		OID der Virtual Machine	Implementiert	WMI	
	Host	Host-Cpu-Anzahl	Implementiert	WMI	
		Host-Cpu-Geschwindigkeit	Implementiert	WMI	
		Host Domain	Implementiert	WMI	
		Host-Installierter Speicher	Implementiert	WMI	
		Host-Modell	Implementiert	WMI	
		Anzahl der NIC	Implementiert	WMI	
		NIC-Geschwindigkeit	Implementiert	WMI	
		IPS	Implementiert	WMI	
		Hersteller	Implementiert	WMI	
		Name	Implementiert	WMI	
		OID	Implementiert	WMI	
		Plattformtyp	Implementiert	WMI	
	ISCSI-Node	Host-Aliase	Implementiert	WMI	
		Node-Name	Implementiert	WMI	
		OID	Implementiert	WMI	
		Typ	Lücke	WMI	
	Info	Name der Datenquelle	Implementiert	WMI	Info
		Datum	Implementiert	WMI	
		Ersteller-ID	Implementiert	WMI	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	vm	Gesamtkapazität	Implementiert	WS-Verwaltung	
		Genutzte Kapazität	Implementiert	WS-Verwaltung	
		Verhältnis Der Verwendeten Kapazität	Implementiert	WS-Verwaltung	
		Gesamtzahl der CPU-Auslastung	Implementiert	WS-Verwaltung	
		IOPS Lesen	Implementiert	WS-Verwaltung	Anzahl der Lese-IOPS auf der Festplatte
		DiskIops.total	Implementiert	WS-Verwaltung	
		Festplatten-IOPS Schreiben	Implementiert	WS-Verwaltung	
		Latenz Insgesamt	Implementiert	WS-Verwaltung	
		Festplattendurchsatz	Implementiert	WS-Verwaltung	
		Durchsatz Beim Lesen	Implementiert	WS-Verwaltung	Gesamtauslesen des Festplattendurchsatzes
		Festplattendurchsatz Schreiben	Implementiert	WS-Verwaltung	
		IP-Durchsatz Lesen	Implementiert	WS-Verwaltung	
		Gesamtdurchsatz	Implementiert	WS-Verwaltung	IP-Durchsatz insgesamt
		IpThrughput.write	Implementiert	WS-Verwaltung	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
PowerShell	WS-Verwaltung	HTTP	5985		Richtig	Falsch	Falsch	Richtig
WMI	WMI	WMI	135		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

NetApp 7-Modus

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
1.12 1.14 1.17 1.19 1.20 1.21	FAS2040 FAS2050 FAS2220 FAS2240-2 FAS2240-4 FAS2520 FAS2554 FAS3140 FAS3160 FAS3210 FAS3220 FAS3240 FAS3250 FAS3270 FAS6240 FAS6290 FAS8020 FAS8040 FAS8060 FAS8080 N6070 N6240 V3240	7.3.6 8.1.1 7-Mode 8.1.3P2 7-Mode 8.1.4P1 7-Mode 8.1.4P10 7-Mode 8.1.4P9D18 7-Mode 8.2.1 7-Mode 8.2.2 7-Mode 8.2.3 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.4 7-Mode 8.2.4P2 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.4P6 7-Mode 8.2.5 7-Mode 8.2.5P1 7-Mode 8.2.5P2 7-Mode 8.2.5P4 7-Mode 8.2.5P5 7-Mode 8.2P3 7-Mode 8.2P4 7-Mode Data ONTAP Version 7.3.3 Data ONTAP Version 7.3.4 Data ONTAP Version 8.2.5 7-Mode

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Zuordnung				Backend-lun
		Protokoll-Controller	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke		
	Volume-Maske	Initiator	Implementiert		
		Protokoll-Controller	Implementiert		
		Storage-Port	Implementiert		
		Typ	Lücke		

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Auslastung Insgesamt	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Auslastung Schreiben	Implementiert		
	Datenmenge	Bruttokapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Genutzte Kapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		I/O-Dichte für Lesevorgänge	Implementiert		
		I/O-Dichte insgesamt	Implementiert		
		Schreib-I/O-Dichte	Implementiert		
		IOPS Lesen	Implementiert		Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert		
		IOPS Schreiben	Implementiert		
		Latenzleseszeit	Implementiert		
		Latenz Insgesamt	Implementiert		
		Latenz – Schreiben	Implementiert		
		Teilweise Blockielles Verhältnis	Implementiert		
		Durchsatz Beim Lesen	Implementiert		
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert		
		„Ausstehend“	Implementiert		Insgesamt ausstehend

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp 7 Modus ZAPI	ZAPI	ZAPI			Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp Cloud Volumes Service

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
AWS Cloud Volumes	v1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazität der physischen	Implementiert		Wird als Rohkapazität für
Produkt	**Kategorie**	**Funktionsname/API**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert		Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Cloud Volumes Service REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Amazon FSX für NetApp ONTAP

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
FSX für ONTAP	Data ONTAP

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Virtual Machine Storage Pool lRef	Speicherpool-Id	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Virtual Machine Volume Ref	Kapazität	Implementiert	HTTPS	
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		DiskGroup	Implementiert	HTTPS	Typ Der Festplattengruppe
		Verbindungspfad	Implementiert	HTTPS	
		Zuletzt Bekannte Zugriffszeit	Implementiert	HTTPS	Zuletzt Know Zugriff auf das Volume
		Name	Implementiert	HTTPS	
		Qtree-Id	Implementiert	HTTPS	Eindeutige id des qtree
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
		UUID	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verschlüsselt	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Leistung	Storage	Fehlerhafte Festplatten	Implementiert	HTTPS	
	Storage-Node	Cache-Trefferverhältnis Insgesamt	Implementiert	HTTPS	
		Insgesamt Ausgetauschte Festplatten-Lesevorgang	Implementiert	HTTPS	
		Auslastung Insgesamt	Implementiert	HTTPS	
	Qtree		Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ONTAP-API	HTTP/HTTPS	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp Clustered Data ONTAP 8.1 und höher

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
AFF-A150 AFF A200 AFF-A220 AFF-A250 AFF A300 AFF A320 AFF-A400 AFF-A700 AFF A700s AFF A800 AFF-A900 AFF C190 AFF-C250 AFF-C400 AFF-C800 AFF8020 AFF8040 AFF8060 AFF8080 CDvM100 CDvM200 DM5000H FAS2240-2 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS6220 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX V6240	8.2.3P5 8.3.0 8.3.1 8.3.1P2 8.3.2 8.3.2P12 8.3.2P2 8.3.2P5 9.0.1 9.1.0 9.1.0P1 9.1.0P10 9.1.0P11 9.1.0P12 9.1.0P14 9.1.0P15 9.1.0P17 9.1.0P19 9.1.0P20 9.1.0P5 9.1.0P7 9.1.0P8 9.10.0 9.10.1 9.10.1P1 9.10.1P10 9.10.1P11 9.10.1P12 9.10.1P13 9.10.1P2 9.10.1P3 9.10.1P4 9.10.1P5 9.10.1P6 9.10.1P7 9.10.1P8 9.10.1P9 911.0P1 9.11.1 9.11.1P1 9.11.1P10 9.11.1P2 9.11.1P3 9.11.1P4 9.11.1P5 9.11.1P6 9.11.1P7 9.11.1P8 9.11.1P9 9.11.1X12 9.11.1X26 9.12.1 9.12.1P1 9,12.1P2

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Virtualisierung?
		Verschlüsselt	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		QoS begrenzt IOPS	Implementiert	HTTPS	
		QoS begrenzt MB/S	Implementiert	HTTPS	
		Qos-Limit: Raw	Implementiert	HTTPS	
		QoS: Richtlinie	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Festplatten) in MB/s
Produkt	**Kategorie**	**Funktion/Attribut schreiben**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		I/O-Dichte für Lesevorgänge	Implementiert	HTTPS	
		I/O-Dichte insgesamt	Implementiert	HTTPS	
		Schreib-I/O-Dichte	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Teilweise Blockielles Verhältnis	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
NetApp ONTAP-API	HTTP/HTTPS	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp SolidFire 8.1 oder höher

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF38410 SF4805 SF9605 SF9608 FCN001 H300S H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 H610S2 SF19210 SF38410 SF4805 SF9605	11.1.0.72 11.5.0.63 11.7.0.76 11.8.0.23 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		IOPS			
		qos-Minimum für IOPS	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		QoS: Richtlinie	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Maskierung Erforderlich	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Sonstige Gesamtkapazität	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribute**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		Gesamteinsparungen Durch Komprimierung	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Latenzleseszeit	Implementiert	HTTPS	
		Latenz Insgesamt	Implementiert	HTTPS	
		Latenz – Schreiben	Implementiert	HTTPS	
		Teilweise Blockielles Verhältnis	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	
		Auslastung Insgesamt	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
SolidFire REST-API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp StorageGRID (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Modelle	Firmware-Versionen
3.0 3.2 3.3 3.4 3.5	Webscale	11.2.0 11.4.0 11.4.0.3 11.4.0.4 11.5.0.1 11.5.0.11 11.5.0.2 11.5.0.3 11.5.0.6 11.5.0.7 11.5.0.8 11.5.0.9 11.6.0 11.6.0.1 11.6.0.10 11.6.0.2 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		tung des Knotens verwendete Metadaten in MB			
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Standortname	Implementiert	HTTPS	
	Storage-Pool	In Dwh-Kapazität Einbeziehen	Implementiert	HTTPS	Ein Weg von ACQ zu cotnrol, die Stroage Pools sind interessant in DWH Kapazität
		Name	Implementiert	HTTPS	
		Kapazität der physischen Festplatte (MB)	Implementiert	HTTPS	Wird als Rohkapazität für den Storage-Pool verwendet
		Raid-Gruppe	Implementiert	HTTPS	Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt
		Verhältnis „Rohkapazität“ zu „nutzbar“	Implementiert	HTTPS	Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning Wird Unterstützt	Implementiert	HTTPS	Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt
		Insgesamt Zugewiesene Kapazität	Implementiert	HTTPS	
		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

					Festplatten)
		Storage Pools: Kapazität	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Bruttokapazität	Implementiert		
	Storage-Node	Kapazitätsauslastung Des Node Erlaubte Metadaten	Implementiert		
		Kapazitätsauslastung Des Nodes Insgesamt	Implementiert		
		Nutzbare Node-Kapazitätsauslastung	Implementiert		
		Verwendete Node-Kapazitätsauslastung	Implementiert		
		Node-Kapazitätsauslastung Verwendete Metadaten	Implementiert		
		Durchsatz Beim Lesen	Implementiert		
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert		
	Storage Pool Festplatte	Bereitgestellte Kapazität	Implementiert		
Bruttokapazität		Implementiert			Gesamtkapazität
Implementiert				Genutzte Kapazität	Implementiert
			Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert	
Als Zeitreihe gemeldet		Verhältnis Der Verwendeten Kapazität	Implementiert		

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
StorageGRID REST API	HTTPS	HTTPS	443		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

Nutanix Storage (REST)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
HPE DL360-8 G10 NX-3060-G6 NX-3170-G6 NX-8035-G6 NX-8150-G7 HPE DL360-8 G10 HPE DL380-12 G10 NX-3060-G5 NX-3170-G7 NX-5155-G6 NX-8035-G6 NX-8035-G7 NX-8150-G7 NX-8150-G8	6.5.1.6 6.5.2 6.5.2.5 6.5.2.6 6.5.2.7 6.5.3 6.5.3.1

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1158					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

					Ebene zusätzlich unterstützt
		Insgesamt	Implementiert	HTTPS	
Produkt	**Kategorie**	**Zugehöriges Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Insgesamt Genutzte Kapazität	Implementiert	HTTPS	Gesamtkapazität in MB
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
	Datenmenge	Kapazität	Implementiert	HTTPS	Verwendete Kapazität des Snapshot in MB
		Verbindungspfad	Implementiert	HTTPS	
		Name	Implementiert	HTTPS	
		Qtree-Id	Implementiert	HTTPS	Eindeutige id des qtree
		Gesamtbruttokapazität	Implementiert	HTTPS	Gesamte Rohkapazität (Summe aller Festplatten im Array)
		Redundanz	Implementiert	HTTPS	Redundanzebene
		Speicherpool-Id	Implementiert	HTTPS	
		Thin Provisioning	Implementiert	HTTPS	
		UUID	Implementiert	HTTPS	
	Volume-Zuordnung	LUN	Implementiert	HTTPS	Der Name der Backend-lun
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	
	Volume-Maske	Initiator	Implementiert	HTTPS	
		Protokoll-Controller	Implementiert	HTTPS	
		Storage-Port	Implementiert	HTTPS	
		Typ	Lücke	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

			und Schreibvorgänge auf allen		
Produkt	**Kategorie**	**Funktion/Attribut**	**Festplatten) in MB/s**	**Verwendetes Protokoll**	**Weitere Informationen**
	Implementiert	HTTPS		Datenmenge	IOPS Lesen
	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte		IOPS insgesamt
	Implementiert	HTTPS			IOPS Schreiben
	Implementiert	HTTPS			Latenzleseszeit
	Implementiert	HTTPS			Latenz Insgesamt
	Implementiert	HTTPS			Latenz – Schreiben
	Implementiert	HTTPS			Durchsatz Beim Lesen
	Implementiert	HTTPS			Gesamtdurchsatz
	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s		Durchsatz Schreiben

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Nutanix REST API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

OPENSTACK (REST-API/SSH)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1172					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Node-Name	Implementiert	HTTPS	
		OID	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut Typ	Status	Verwendetes Protokoll	Weitere Informationen
			Lücke	HTTPS	
	Info	Name der Datenquelle	Implementiert	HTTPS	Info
		Datum	Implementiert	HTTPS	
		Ersteller-ID	Implementiert	HTTPS	
		Erstellschlüssel	Implementiert	HTTPS	
Performance	Datastore	Gesamtkapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		Bereitgestellte Kapazität	Implementiert		
		Genutzte Kapazität	Implementiert		
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert		Als Zeitreihe gemeldet
	Host	Gesamtzahl der CPU-Auslastung	Implementiert		
		Gesamte Speicherauslastung	Implementiert		
	Virtuelles Laufwerk	Latenzleseszeit	Implementiert		
		Latenz Insgesamt	Implementiert		
		Latenz – Schreiben	Implementiert		

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
OpenStack REST API	HTTPS	HTTPS	443		Richtig	Falsch	Richtig	Richtig
OpenStack SSH	SSH	SSH	22		Richtig	Falsch	Richtig	Richtig

Zurück nach oben

Oracle ZFS (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
Sun ZFS Storage 7330 Sun ZFS Storage 7335 Sun ZFS Storage 7350 Sun ZFS Storage 7370 Sun ZFS Storage 7420 Sun ZFS Storage 7430 Sun ZFS Storage 7450	1-1.1 1-1.2 1-1.3 1-1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.35 2013.06.05.8.37 2013.06.05.8.47 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.6 2013.06.05.8.7

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Genutzte Kapazität	Implementiert	HTTP/S	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Volume-Zuordnung	LUN	Implementiert	HTTP/S	Der Name der Backend-lun
		Storage-Port	Implementiert	HTTP/S	
		Maskierung Erforderlich	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Volume-Maske	Storage-Port	Implementiert	HTTP/S	
		Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Cache-Trefferverhältnis Insgesamt	Implementiert		
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Auslastung Insgesamt	Implementiert		
	Storage Pool Festplatte	IOPS insgesamt	Implementiert		
		Gesamtkapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		Gesamtkapazität Daten	Implementiert		
		Bereitgestellte Kapazität	Implementiert		
		Genutzte Kapazität Von Daten	Implementiert		
		Genutzte Kapazität	Implementiert		
		Andere Genutzte Kapazität	Implementiert		
		Bruttokapazität	Implementiert		
		Kapazitätsverhältnis Zu Hoch Festsetzen	Implementiert		Als Zeitreihe gemeldet
		Verwendete Snapshot-Kapazität	Implementiert		
		Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie	Implementiert		Als Zeitreihe gemeldet

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
ORACLE ZFS REST API	HTTP/HTTPS	HTTP/HTTPS	215		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Pure Storage FlashArray (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

Modelle	Firmware-Versionen
DFSC1 FA-420 FA-450 FA-C40R3 FA-C60 FA-C60R3 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X50R2 FA-X50R3 FA-X70R2 FA-X70R3 FA-X90R2 FA-X90R3 FA-XL130 FA-XL170 FA-m10r2 FA-m20 FA-m20r2 FA-m50 FA-m50r2 FA-m70 FA-m70r2 FA-x70	4.8.8 5.3.14 5.3.15 5.3.17 5.3.18 5.3.20 5.3.21 5.3.6 5.3.8 6.1.10 6.1.11 6.1.13 6.1.14 6.1.15 6.1.17 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.1.5 6.2.13 6.2.7 6.2.9 6.3.10 6.3.11 6.3.12 6.3.2 6.3.5 6.3.6 6.3.7 6.3.9 6.4.3 6.4.4 6.4.5

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1192					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Protokoll-Controller	Implementiert	HTTP/S	
		Storage-Port	Implementiert	HTTP/S	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTP/S	
	Volume-Maske	Initiator	Implementiert	HTTP/S	
		Protokoll-Controller	Implementiert	HTTP/S	
		Storage-Port	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	WWN-Alias	Host-Aliase	Implementiert	HTTP/S	
		Objekttyp	Implementiert	HTTP/S	
		Quelle	Implementiert	HTTP/S	
		WWN	Implementiert	HTTP/S	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					
1200					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Kapazitätsverhältnis Der Verwendeten	Implementiert		Als Zeitreihe gemeldet
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Datenmenge	Bruttokapazität	Implementiert		
		Gesamtkapazität	Implementiert		
		Genutzte Kapazität	Implementiert		
		Verhältnis Der Verwendeten Kapazität	Implementiert		
		IOPS Lesen	Implementiert		Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert		
		IOPS Schreiben	Implementiert		
		Latenzleseszeit	Implementiert		
		Latenz Insgesamt	Implementiert		
		Latenz – Schreiben	Implementiert		
		Durchsatz Beim Lesen	Implementiert		
		Gesamtdurchsatz	Implementiert		Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert		

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Pure Storage REST-API	HTTP/HTTPS	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Red hat RHV (REST)

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1204					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Disk	OID der Virtual Machine	Implementiert	HTTP/S	
Produkt	**Kategorie**	**Funktion/Attribut ist OID**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Host	OID	Implementiert	HTTP/S	
		Name	Implementiert	HTTP/S	
		IPS	Implementiert	HTTP/S	
		Plattformtyp	Implementiert	HTTP/S	
		Host-Installierter Speicher	Implementiert	HTTP/S	
		Hersteller	Implementiert	HTTP/S	
		Host-Modell	Implementiert	HTTP/S	
		Host-Cpu-Anzahl	Implementiert	HTTP/S	
		Host-Cpu-Geschwindigkeit	Implementiert	HTTP/S	
		Anzahl der NIC	Implementiert	HTTP/S	
		NIC-Geschwindigkeit	Implementiert	HTTP/S	
	ISCSI-Node	OID	Implementiert	HTTP/S	
		Node-Name	Implementiert	HTTP/S	
		Typ	Lücke	HTTP/S	
	Info	Name der Datenquelle	Implementiert	HTTP/S	Info
		Ersteller-ID	Implementiert	HTTP/S	
		Datum	Implementiert	HTTP/S	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Red hat RHEV REST API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Rubrik Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen	Firmware-Versionen
v5.3	5.3.3-p1-19391 6.0.3-p3-13584 7.0.2-p4-15876 7.0.3-p1-15949 8.0.3-p2-22743

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Zugewiesene Kapazität			
		Insgesamt Kapazität	Implementiert	HTTPS	Gesamtkapazität
Produkt	**Kategorie**	**Sensitive/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Typ	Lücke	HTTPS	
		Einheitliche	Implementiert	HTTPS	Handelt es sich um ein Gerät zur Storage-Virtualisierung?
		Effektiv Genutzte Kapazität In Prozent	Implementiert	HTTPS	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Durchsatz Schreiben	Implementiert	HTTPS	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Storage Pool Festplatte	Bruttokapazität	Implementiert	HTTPS	
		Gesamtkapazität	Implementiert	HTTPS	
		Genutzte Kapazität	Implementiert	HTTPS	
		Verhältnis Der Verwendeten Kapazität	Implementiert	HTTPS	
		Genutzte Kapazität Von Daten	Implementiert	HTTPS	
		IOPS Lesen	Implementiert	HTTPS	Anzahl der Lese-IOPS auf der Festplatte
		IOPS insgesamt	Implementiert	HTTPS	
		IOPS Schreiben	Implementiert	HTTPS	
		Andere Genutzte Kapazität	Implementiert	HTTPS	
		Verwendete Snapshot-Kapazität	Implementiert	HTTPS	
		Durchsatz Beim Lesen	Implementiert	HTTPS	
		Gesamtdurchsatz	Implementiert	HTTPS	Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s
		Durchsatz Schreiben	Implementiert	HTTPS	

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
Rubrik Storage REST API	HTTPS	HTTPS	443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

NetApp HCI Virtual Center

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
VMware vCenter Server 6.7.0 Build-10244857 VMware vCenter Server 6.7.0 Build-14368073 VMware vCenter Server 7.0.3 Build-19234570 VMware vCenter Server 7.0.3 Build-20150588 VMware vCenter Server 7.0.3 Build-20395099 VMware vCenter Server 7.0.3 Build-20990077 VMware vCenter Server 7.0.3 Build-21477706 VMware vCenter Server 7.0.3 Build-21784236 VMware vCenter Server 8.0.1 Build-21815093

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1218					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Bereitgestellte Kapazität	Implementiert	Web-Services	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	VirtualMachine Disk	OID	Implementiert	Web-Services	
		VirtualisierungsDisk OID	Implementiert	Web-Services	
		OID der Virtual Machine	Implementiert	Web-Services	
	Host	Host-Cpu-Anzahl	Implementiert	Web-Services	
		Host-Cpu-Geschwindigkeit	Implementiert	Web-Services	
		Host Domain	Implementiert	Web-Services	
		Host-Installierter Speicher	Implementiert	Web-Services	
		Host-Modell	Implementiert	Web-Services	
		Anzahl der NIC	Implementiert	Web-Services	
		NIC-Geschwindigkeit	Implementiert	Web-Services	
		IPS	Implementiert	Web-Services	
		Hersteller	Implementiert	Web-Services	
		Name	Implementiert	Web-Services	
		OID	Implementiert	Web-Services	
		Plattformtyp	Implementiert	Web-Services	
	ISCSI-Node	Host-Aliase	Implementiert	Web-Services	
		Node-Name	Implementiert	Web-Services	
		OID	Implementiert	Web-Services	
		Typ	Lücke	Web-Services	
	Info	Api-Beschreibung	Implementiert	Web-Services	
		Api-Name	Implementiert	Web-Services	
		Api-Version	Implementiert	Web-Services	
		Client-Api-Name	Implementiert	Web-Services	
		Client-Api-Version	Implementiert	Web-Services	
		Name der Datenquelle	Implementiert	Web-Services	Info
		Datum	Implementiert	Web-Services	
		Ersteller-ID	Implementiert	Web-Services	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		ipThruput.write	Implementiert	Web-Services	
		Gesamte	Implementiert	Web-Services	
Produkt	**Kategorie**	**Funktion/Attribution**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		swapRate.inRate	Implementiert	Web-Services	
		Swap-Rate	Implementiert	Web-Services	
		Gesamtpausenrate	Implementiert	Web-Services	
		Legen Sie die Wartezeit fest	Implementiert	Web-Services	Warten auf geplante Zeit in Prozent

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST-API	Web-Services	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

VMware Cloud auf AWS

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
VMware vCenter Server 7.0.3 Build-20532039 VMware vCenter Server 7.0.3 Build-20870699 VMware vCenter Server 8.0.0 Build-21709157

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					
1226					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

	Disk	OID der Virtual Machine	Implementiert	Web-Services	
Produkt	**Kategorie**	**Funktion/Attribut ist**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	Host	OID	Implementiert	Web-Services	
		Name	Implementiert	Web-Services	
		IPS	Implementiert	Web-Services	
		Host Domain	Implementiert	Web-Services	
		Plattformtyp	Implementiert	Web-Services	
		Host-Installierter Speicher	Implementiert	Web-Services	
		Hersteller	Implementiert	Web-Services	
		Host-Modell	Implementiert	Web-Services	
		Host-Cpu-Anzahl	Implementiert	Web-Services	
		Host-Cpu-Geschwindigkeit	Implementiert	Web-Services	
		Anzahl der NIC	Implementiert	Web-Services	
		NIC-Geschwindigkeit	Implementiert	Web-Services	
	Info	Name der Datenquelle	Implementiert	Web-Services	Info
		Ersteller-ID	Implementiert	Web-Services	
		Datum	Implementiert	Web-Services	
		Api-Name	Implementiert	Web-Services	
		Api-Version	Implementiert	Web-Services	
		Api-Beschreibung	Implementiert	Web-Services	
		Client-Api-Name	Implementiert	Web-Services	
		Client-Api-Version	Implementiert	Web-Services	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Gesamtzahl der CPU-Auslastung	Implementiert	Web-Services	
		Legen Sie die	Implementiert	Web-Services	Warten auf
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		DiskIops.total	Implementiert	Web-Services	
		Gesamtpausenrate	Implementiert	Web-Services	
		Durchsatz Beim Lesen	Implementiert	Web-Services	Gesamtauslesen des Festplattendurchsatzes

Von diesem Datensammler verwendete Management-APIs:

API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST-API	Web-Services	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

VMware vSphere (Web Services)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen
VMware ESXi 6.0.0 Build-10719132
VMware ESXi 6.0.0 Build-2494585
VMware ESXi 6.0.0 Build-5572656
VMware ESXi 6.0.0 Build-9313334
VMware ESXi 6.5.0 Build-14990892
VMware ESXi 6.5.0 Build-5969303
VMware ESXi 7.0.0 Build-15843807
VMware ESXi 7.0.3 Build-20036589
VMware ESXi 7.0.3 Build-20328353
VMware ESXi 7.0.3 Build-20842708
VMware vCenter Server 5.0.0 Build-3073236
VMware vCenter Server 5.0.0 Build-455964
VMware vCenter Server 5.0.0 Build-623373
VMware vCenter Server 5.1.0 Build-3814779
VMware vCenter Server 5.5.0 Build-1750787
VMware vCenter Server 5.5.0 Build-2442329
VMware vCenter Server 5.5.0 Build-3000241
VMware vCenter Server 5.5.0 Build-3252642
VMware vCenter Server 5.5.0 Build-3721164
VMware vCenter Server 5.5.0 Build-4180647
VMware vCenter Server 5.5.0 Build-6516310
VMware vCenter Server 5.5.0 Build-9911218
VMware vCenter Server 6.0.0 Build-13638472
VMware vCenter Server 6.0.0 Build-14510545
VMware vCenter Server 6.0.0 Build-2776511
VMware vCenter Server 6.0.0 Build-3634793
VMware vCenter Server 6.0.0 Build-3634794
VMware vCenter Server 6.0.0 Build-5960847
VMware vCenter Server 6.0.0 Build-7924803
VMware vCenter Server 6.0.0 Build-8803875
VMware vCenter Server 6.0.0 Build-9313458
VMware vCenter Server 6.5.0 Build-10964411
VMware vCenter Server 6.5.0 Build-15679215
VMware vCenter Server 6.5.0 Build-17590285
VMware vCenter Server 6.5.0 Build-17994927
VMware vCenter Server 6.5.0 Build-18499837
VMware vCenter Server 6.5.0 Build-18711281
VMware vCenter Server 6.5.0 Build-19261680
VMware vCenter Server 6.5.0 Build-20510539
VMware vCenter Server 6.5.0 Build-7119157
VMware vCenter Server 6.7.0 Build-10244857
VMware vCenter Server 6.7.0 Build-11727113
VMware vCenter Server 6.7.0 Build-13007421
VMware vCenter Server 6.7.0 Build-13639324
VMware vCenter Server 6.7.0 Build-14368073
VMware vCenter Server 6.7.0 Build-15129973
VMware vCenter Server 6.7.0 Build-15679289
VMware vCenter Server 6.7.0 Build-17137327
VMware vCenter Server 6.7.0 Build-18010599
VMware vCenter Server 6.7.0 Build-18485185
VMware vCenter Server 6.7.0 Build-18831049
VMware vCenter Server 6.7.0 Build-19299595
VMware vCenter Server 6.7.0 Build-19832247
VMware vCenter Server 6.7.0 Build-19832280

Von diesem Datensammler unterstützte Produkte:

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
grundlage					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Bereitgestellte Kapazität	Implementiert	Web-Services	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
	VirtualMachine Disk	OID	Implementiert	Web-Services	
		VirtualisierungsDisk OID	Implementiert	Web-Services	
		OID der Virtual Machine	Implementiert	Web-Services	
	Host	Host-Cpu-Anzahl	Implementiert	Web-Services	
		Host-Cpu-Geschwindigkeit	Implementiert	Web-Services	
		Host Domain	Implementiert	Web-Services	
		Host-Installierter Speicher	Implementiert	Web-Services	
		Host-Modell	Implementiert	Web-Services	
		Anzahl der NIC	Implementiert	Web-Services	
		NIC-Geschwindigkeit	Implementiert	Web-Services	
		IPS	Implementiert	Web-Services	
		Hersteller	Implementiert	Web-Services	
		Name	Implementiert	Web-Services	
		OID	Implementiert	Web-Services	
		Plattformtyp	Implementiert	Web-Services	
	ISCSI-Node	Host-Aliase	Implementiert	Web-Services	
		Node-Name	Implementiert	Web-Services	
		OID	Implementiert	Web-Services	
		Typ	Lücke	Web-Services	
	Info	Api-Beschreibung	Implementiert	Web-Services	
		Api-Name	Implementiert	Web-Services	
		Api-Version	Implementiert	Web-Services	
		Client-Api-Name	Implementiert	Web-Services	
		Client-Api-Version	Implementiert	Web-Services	
		Name der Datenquelle	Implementiert	Web-Services	Info
		Datum	Implementiert	Web-Services	
		Ersteller-ID	Implementiert	Web-Services	

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
Performance					

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen

		Festplattendurchsatz Schreiben	Implementiert	Web-Services	
Produkt	**Kategorie**	**Funktion/Attribut**	**Status**	**Verwendetes Protokoll**	**Weitere Informationen**
		Durchsatz lesen	Implementiert	Web-Services	
		Gesamtdurchsatz	Implementiert	Web-Services	IP-Durchsatz insgesamt
		IpThrughput.write	Implementiert	Web-Services	
		Gesamte Speicherauslastung	Implementiert	Web-Services	
		swapRate.inRate	Implementiert	Web-Services	
		Swap-Rate	Implementiert	Web-Services	
		Gesamtpausenrate	Implementiert	Web-Services	
		Legen Sie die Wartezeit fest	Implementiert	Web-Services	Warten auf geplante Zeit in Prozent

Von diesem Datensammler verwendete Management-APIs:

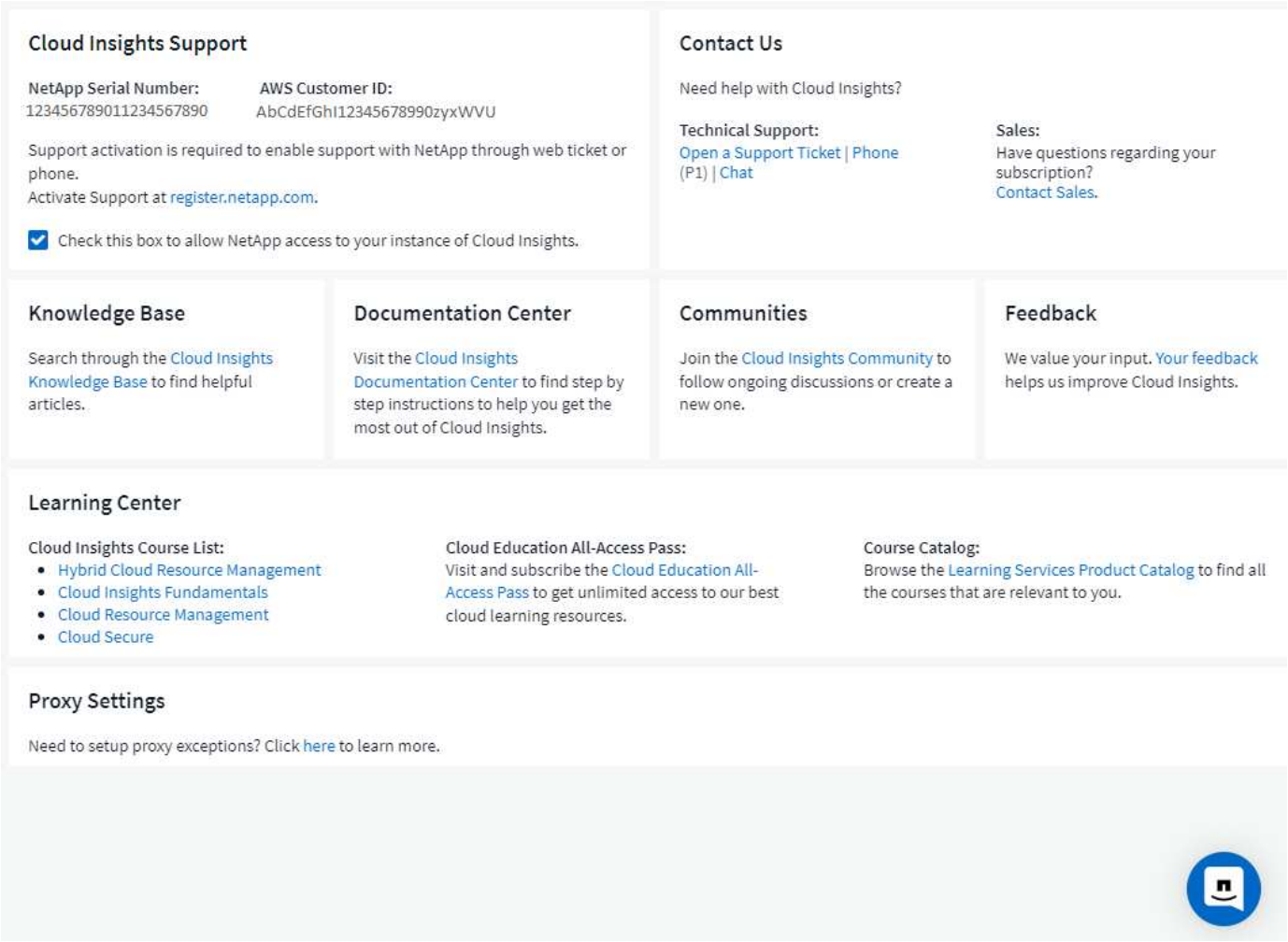
API	Verwendetes Protokoll	Verwendetes Transportschicht-Protokoll	Eingehende Ports verwendet	Verwendete ausgehende Ports	Unterstützt Authentifizierung	Erfordert nur die „Schreibgeschützt“-Anmeldedaten	Unterstützung Von Verschlüsselung	Firewall-freundlich (statische Ports)
VMware REST-API	Web-Services	HTTP/HTTPS	80/443		Richtig	Richtig	Richtig	Richtig

Zurück nach oben

Referenzsupport

Support Wird Angefordert

Sie können auf Supportoptionen in Data Infrastructure Insights zugreifen, indem Sie auf **Hilfe > Support** klicken. Welche Support-Optionen Ihnen zur Verfügung stehen, hängt von Ihrer Data Infrastructure Insights Edition ab.



Aktivieren der Supportberechtigung

Data Infrastructure Insights bietet Self-Service- und E-Mail-Support im Testmodus. Sobald Sie den Service abonniert haben, wird dringend empfohlen, den Supportanspruch zu aktivieren. Durch die Aktivierung der Supportberechtigung können Sie über den Online-Chat, das Web-Ticketing-System und das Telefon auf den technischen Support zugreifen. Der Standard-Support-Modus ist bis zum Abschluss der Registrierung Self-Service. Siehe Details unten.

Während des ersten Abonnements generiert Ihre Data Infrastructure Insights Instanz eine 20-stellige NetApp-Seriennummer, die mit „950“ beginnt. Diese NetApp Seriennummer steht für das Abonnement von Data Infrastructure Insights, das Ihrem Konto zugeordnet ist. Sie müssen die NetApp Seriennummer registrieren, um die Support-Berechtigung zu aktivieren. Wir bieten zwei Optionen für die Support-Registrierung:

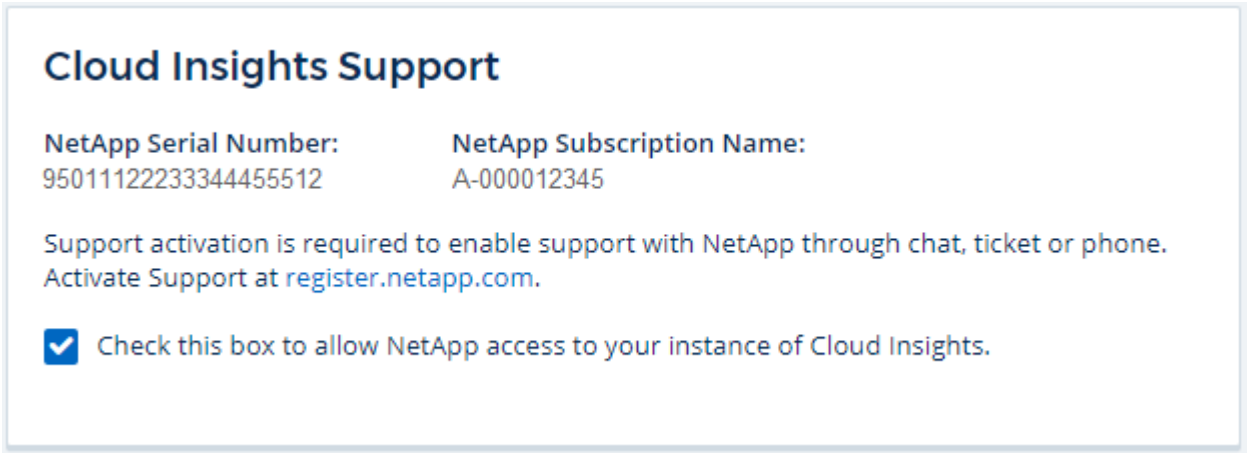
1. Benutzer mit vorvorhandenem NetApp Support Site (NSS) SSO-Konto (z. B. aktueller NetApp Kunde)

2. Neuer NetApp Kunde ohne vorbestehendes NSS SSO-Konto (NetApp Support Site

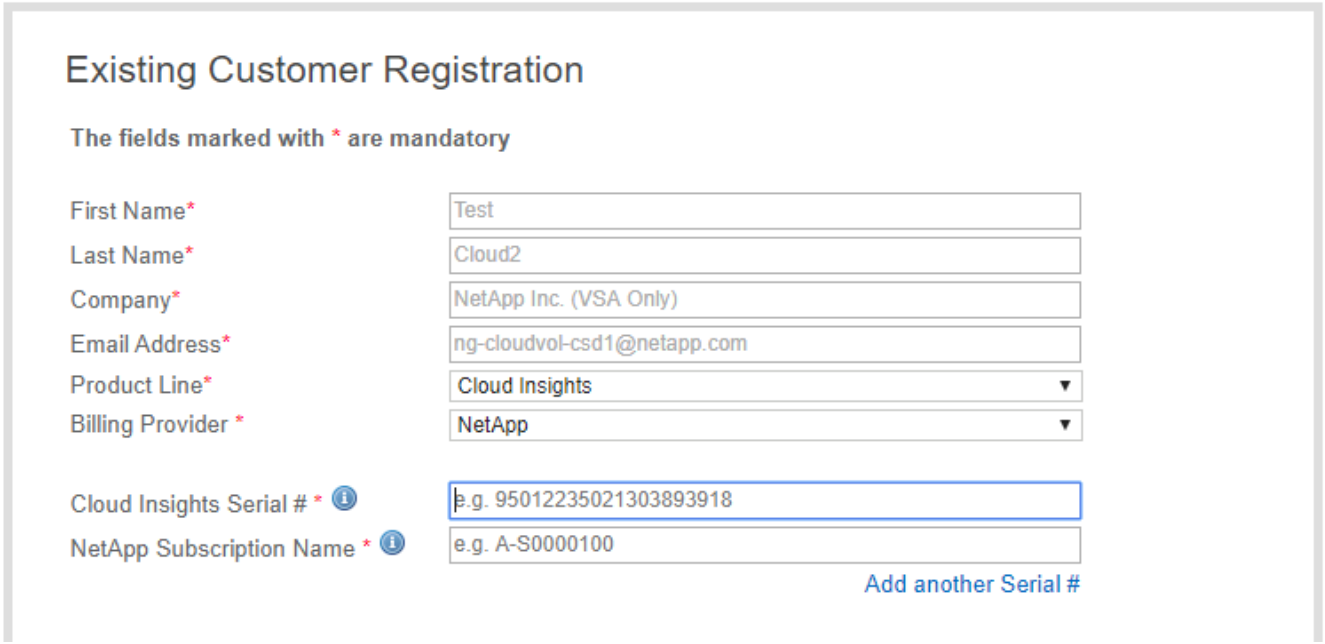
Option 1: Schritte für einen Benutzer mit einem zuvor bestehenden NSS SSO-Konto (NetApp Support Site

Schritte

1. Öffnen Sie die Website für die Registrierung von NetApp https://register.netapp.com
2. Wählen Sie „Ich bin bereits als NetApp-Kunde registriert“ und wählen Sie als Produktlinie „*Data Infrastructure Insights*“. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus, und geben Sie Ihre Seriennummer und den Namen Ihres NetApp-Abonnements oder Ihre AWS Kunden-ID an. Verwenden Sie hierzu in der Insights Benutzeroberfläche der Dateninfrastruktur das Menü „Hilfe > Support“:



3. Füllen Sie das bestehende Registrierungsformular aus und klicken Sie auf **Absenden**.

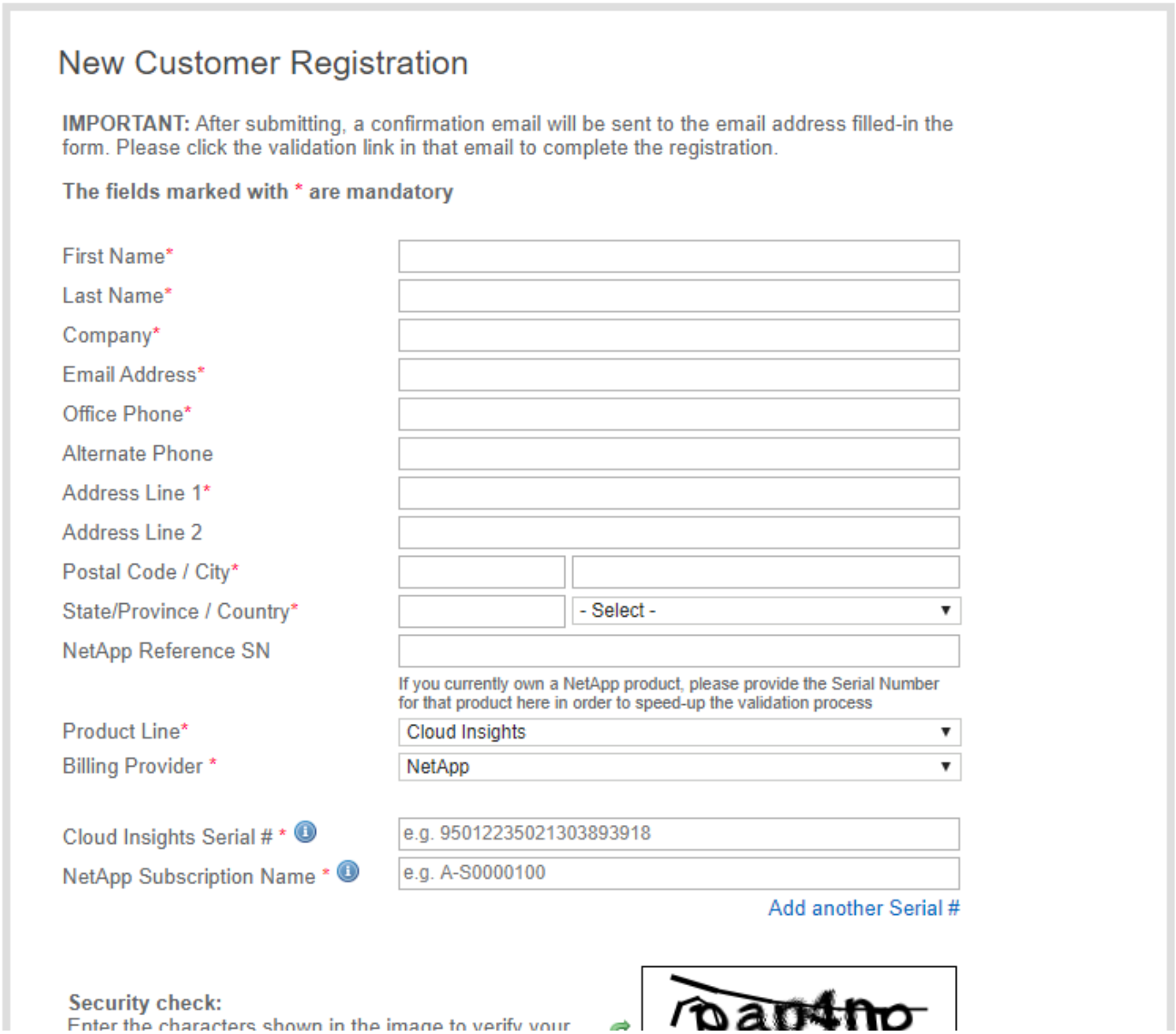


4. Wenn keine Fehler auftreten, wird der Benutzer auf eine Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. Die E-Mail-Adresse, die mit dem NSS SSO-Benutzernamen verbunden ist, der für die Registrierung verwendet wird, erhält innerhalb von wenigen Minuten eine E-Mail mit der Angabe „Ihr Produkt ist jetzt für Support berechtigt“.
5. Dies ist eine einmalige Registrierung für die Seriennummer des Data Infrastructure Insights NetApp.

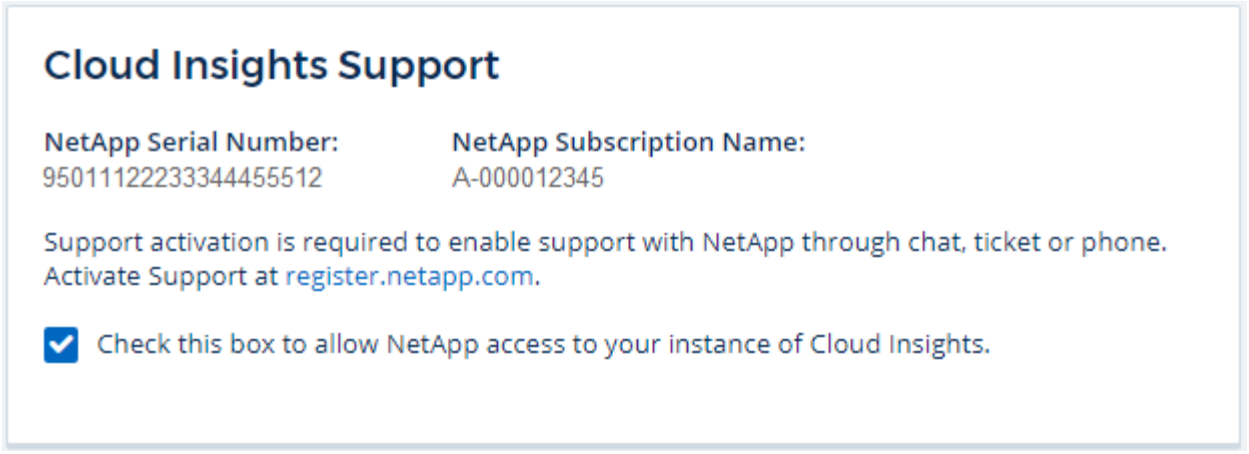
Option 2: Schritte für einen neuen NetApp Kunden ohne vorbestehendes NSS-SSO-Konto (NetApp Support Site

Schritte

1. Öffnen Sie die Website für die Registrierung von NetApp https://register.netapp.com
2. Wählen Sie „Ich bin kein registrierter NetApp Kunde“ und füllen Sie die erforderlichen Informationen im folgenden Beispielformular aus:



1. Wählen Sie *Data Infrastructure Insights* als Produktlinie aus. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus, und geben Sie Ihre Seriennummer und den Namen Ihres NetApp-Abonnements oder Ihre AWS Kunden-ID an. Verwenden Sie hierzu in der Insights Benutzeroberfläche der Dateninfrastruktur das Menü „Hilfe > Support“:



2. Wenn keine Fehler auftreten, wird der Benutzer auf eine Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. Die E-Mail-Adresse, die mit dem NSS SSO-Benutzernamen verbunden ist, der für die Registrierung verwendet wird, erhält innerhalb weniger Stunden eine E-Mail mit der Angabe „Ihr Produkt ist jetzt für Support berechtigt“.
3. Als neuer NetApp Kunde müssen Sie außerdem ein NSS-Benutzerkonto für die zukünftige Registrierung auf der NetApp Support Site erstellen und auf das Support-Portal für den Chat des technischen Supports und die Ticketausstellung im Web zugreifen. Dieser Link befindet sich unter https://mysupport.netapp.com/eservice/public/now.do. Sie können die neu registrierte Data Infrastructure Insights Seriennummer zur Verfügung stellen, um diesen Prozess zu beschleunigen.
4. Dies ist eine einmalige Registrierung für die Seriennummer des Data Infrastructure Insights NetApp.

Abrufen Von Support-Informationen

NetApp unterstützt Data Infrastructure Insights auf verschiedene Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledgebase-Artikel (KB) oder die NetApp Community. Für Benutzer, die eine der Data Infrastructure Insights Editions (Basic*, Standard, Premium) abonniert haben, steht der technische Support per Telefon oder Web-Ticketing zur Verfügung. Für Webticket und die Case-Verwaltung ist ein NSS-Konto (NetApp Support Site) erforderlich.

*Der Support ist bei Basic Edition verfügbar, sofern alle NetApp Speichersysteme mindestens auf Premium Support Level abgedeckt sind.

Self-Service-Support:

Diese Support-Optionen sind im Testmodus verfügbar und stehen rund um die Uhr kostenlos zur Verfügung:

- **Knowledgebase**

+ durch Klicken auf die Links in diesem Abschnitt gelangen Sie zur NetApp Knowledgebase, in der Sie relevante Artikel, Anleitungen und vieles mehr durchsuchen können.

- **"Dokumentation"**

  Durch Klicken auf den Link Dokumentation gelangen Sie zu diesem Dokumentationszentrum.

- **"Community"**

  Durch Klicken auf den Community-Link gelangen Sie zur NetApp Data Infrastructure Insights Community, in der Sie sich mit Kollegen und Experten austauschen können.

Außerdem gibt es einen Link**"Feedback"**, den Sie uns zur Verbesserung der Einblicke aus der Dateninfrastruktur zur Verfügung stellen können.

Abonnementunterstützung

Wenn Sie zusätzlich zu den oben aufgeführten Self-Support-Optionen ein Abonnement für Data Infrastructure Insights oder bezahlten Support für überwachte NetApp Produkte und Services haben, können Sie gemeinsam mit einem NetApp Support Engineer das Problem lösen.

Sie müssen sich registrieren, um Aktivieren Sie den Support Für NetApp Cloud-Produkte. Registrieren Sie sich unter NetApp "Support-Registrierung Für Cloud-Datenservices".

Es wird dringend empfohlen, das Kontrollkästchen zu aktivieren, damit NetApp-Support-Techniker während der Support-Sitzung auf die Data Infrastructure Insights-Umgebung zugreifen können. So kann der Techniker das Problem beheben und es schnell beheben. Wenn Ihr Problem behoben ist oder Ihre Support-Sitzung beendet wurde, können Sie das Kontrollkästchen deaktivieren.

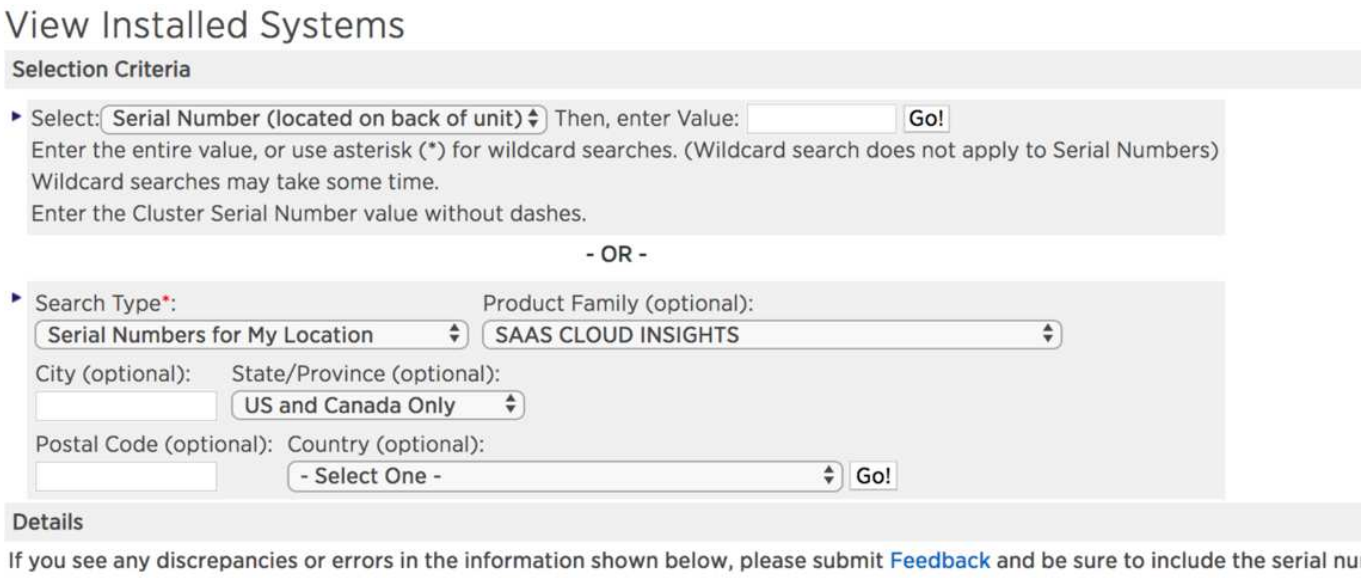
Sie können Unterstützung durch eine der folgenden Methoden anfordern. Um die folgenden Support-Optionen nutzen zu können, benötigen Sie ein aktives Abonnement von Data Infrastructure Insights:

- "* Telefon*"
- **"Support-Ticket"**
- **Chat** - Sie werden mit NetApp-Support-Mitarbeiter für Unterstützung (nur an Wochentagen) verbunden werden. Der Chat ist über die Menüoption **Hilfe > Live Chat** in der oberen rechten Ecke eines Bildschirms Data Infrastructure Insights verfügbar.

Sie können auch Unterstützung für den Vertrieb anfordern, indem Sie auf die klicken **"Vertrieb Kontaktieren"** Verlinken:

Ihre Data Infrastructure Insights Seriennummer wird im Service über das Menü **Hilfe > Support** angezeigt. Wenn beim Zugriff auf den Service Probleme auftreten und Sie zuvor eine Seriennummer bei NetApp registriert haben, können Sie sich wie folgt auf der NetApp Support-Website Ihre Liste mit Seriennummern von Data Infrastructure Insights anzeigen lassen:

- Melden Sie sich bei mysupport.netapp.com an
- Verwenden Sie auf der Menüregisterkarte Produkte > Meine Produkte die Produktfamilie „SaaS Data Infrastructure Insights“, um alle Ihre registrierten Seriennummern zu finden:



Data Infrastructure Insights Data Collector Support Matrix

Informationen und Details zu unterstützten Datensammlern können Sie im anzeigen oder herunterladen**Data Infrastructure Insights Data Collector Support Matrix**, Rolle=„extern“.

Learning Center

Unabhängig von Ihrem Abonnement führt **Hilfe > Support** Links zu verschiedenen Kursangeboten der NetApp University, damit Sie die Erkenntnisse über Ihre Dateninfrastruktur optimal nutzen können. Erfahren Sie mehr darüber!

Data Collector Reference - Infrastruktur

Anbieterspezifische Referenz

Die Themen in diesem Abschnitt enthalten anbieterspezifische Referenzinformationen. In den meisten Fällen ist die Konfiguration eines Datensammlers einfach. In einigen Fällen benötigen Sie möglicherweise zusätzliche Informationen oder Befehle, um den Datensammler richtig zu konfigurieren.

Klicken Sie im Menü links auf einen **Anbieter**, um Informationen zu ihren Datensammlern anzuzeigen.

Amazon EC2 Data Collector konfigurieren

Data Infrastructure Insights verwendet den Amazon EC2 Datensammler, um Bestands- und Performance-Daten von EC2-Instanzen zu erfassen.

Anforderungen

Um Daten von Amazon EC2 Geräten zu erfassen, müssen Sie folgende Informationen haben:

- Sie müssen eine der folgenden Optionen aufweisen:

    - Die **IAM-Rolle** für Ihr Amazon EC2 Cloud-Konto, wenn Sie IAM-Rollenauthentifizierung verwenden. Die IAM-Rolle gilt nur, wenn die Acquisition Unit auf einer AWS-Instanz installiert ist.
    - Die **IAM Access Key**-ID und der geheime Zugriffsschlüssel für Ihr Amazon EC2 Cloud-Konto bei Verwendung der IAM Access Key-Authentifizierung.
- Sie müssen über die Berechtigung „Listenorganisation“ verfügen
- Port 443 HTTPS
- EC2-Instanzen können als Virtual Machine oder (weniger natürlich) als Host gemeldet werden. EBS Volumes können sowohl von der VM als virtualisierte Festplatte genutzt werden als auch als Datenspeicher, die die Kapazität der virtuellen Festplatte bereitstellen.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID (z. B. AKIAIOSFODN7EXAMPLE) und einem geheimen Zugriffsschlüssel (z. B. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Sie verwenden Zugriffsschlüssel, um programmatische Anfragen zu signieren, die Sie an EC2 vornehmen, wenn Sie die Amazon EC2 SDKs, REST oder Abfrage-API-Operationen verwenden. Diese Schlüssel werden mit Ihrem Vertrag von Amazon zur Verfügung gestellt.

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
AWS Region	Wählen Sie die Region AWS
IAM-Rolle	Nur zur Verwendung bei Übernahme auf einer AU in AWS. Siehe unten für weitere Informationen über IAM-Rolle.
AWS IAM Access Key-ID	Geben Sie die AWS IAM-Zugriffsschlüssel-ID ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden.
AWS IAM Secret Access Key	Geben Sie den AWS IAM-Schlüssel für den geheimen Zugriff ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden.
Ich verstehe, dass mir AWS API-Anfragen nach	Überprüfen Sie dies, um zu überprüfen, ob AWS Sie für API-Anfragen abfragt, die durch die Data Infrastructure Insights Umfrage gemacht wurden.

Erweiterte Konfiguration

Feld	Beschreibung
Zusätzliche Regionen Einschließen	Geben Sie zusätzliche Bereiche an, die in die Abfrage einbezogen werden sollen.
Accountübergreifende Rolle	Rolle für den Zugriff auf Ressourcen in unterschiedlichen AWS Konten.
Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Wählen Sie „exclude“ oder „include“, um VMs nach Tags zu filtern	Geben Sie an, ob VM’s by Tags beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn ‘include’ ausgewählt ist, kann das Feld Tag-Schlüssel nicht leer sein.

Feld	Beschreibung
Markieren Sie Schlüssel und Werte, nach denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Tag**, um die VMs (und die zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte von Tags auf der VM entsprechen, einzuschließen bzw. auszuschließen. Tag-Schlüssel erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM solange gefiltert, wie sie dem Tag-Schlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 1800
CloudWatch Agent Metrics Namespace	Namespace in EC2/EBS zur Erfassung von Daten Wenn die Namen der Standardmetriken in diesem Namespace geändert werden, kann Data Infrastructure Insights diese umbenannten Daten möglicherweise nicht erfassen. Es wird empfohlen, die standardmäßigen metrischen Namen zu belassen.

IAM-Zugriffsschlüssel

Zugriffsschlüssel sind langfristige Anmeldedaten für einen IAM-Benutzer oder den Root-Benutzer des AWS-Kontos. Mit Zugriffsschlüsseln werden programmatische Anfragen an die AWS CLI oder die AWS API (direkt oder über das AWS SDK) signieren.

Zugriffsschlüssel bestehen aus zwei Teilen: Einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Wenn Sie die Authentifizierung *IAM Access Key* verwenden (im Gegensatz zur Authentifizierung von *IAM Role*), müssen Sie für die Authentifizierung von Anfragen sowohl den Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel gemeinsam verwenden. Weitere Informationen finden Sie in der Amazon-Dokumentation auf "Zugriffsschlüssel".

IAM-Rolle

Bei der Verwendung der Authentifizierung über *IAM-Rolle* (im Gegensatz zur IAM-Zugriffsschlüsselauthentifizierung) müssen Sie sicherstellen, dass die von Ihnen erstellte oder angegebene Rolle über die entsprechenden Berechtigungen verfügt, die für den Zugriff auf Ihre Ressourcen erforderlich sind.

Wenn Sie beispielsweise eine IAM-Rolle mit dem Namen *InstanceEc2ReadOnly* erstellen, müssen Sie die Richtlinie einrichten, um allen EC2-Ressourcen für diese IAM-Rolle schreibgeschützten Zugriff auf EC2-Listen zu gewähren. Außerdem müssen Sie STS (Security Token Service)-Zugriff gewähren, damit diese Rolle Rollenübergreifende Konten übernehmen kann.

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie sie beim Erstellen einer neuen EC2-Instanz oder einer vorhandenen EC2-Instanz anhängen.

Nachdem Sie die IAM-Rolle *InstanceEc2ReadOnly* an eine EC2-Instanz angehängt haben, können Sie die temporären Anmeldedaten über die Metadaten der Instanz per IAM-Rollennamen abrufen und verwenden, um von jeder auf dieser EC2-Instanz ausgeführten Anwendung auf AWS-Ressourcen zuzugreifen.

Weitere Informationen finden Sie in der Amazon-Dokumentation auf "IAM-Rollen".

Hinweis: Die IAM-Rolle kann nur verwendet werden, wenn die Acquisition Unit in einer AWS-Instanz ausgeführt wird.

Zuordnen von Amazon Tags zu Annotationen zu Data Infrastructure Insights

Der Amazon EC2 Datensammler enthält eine Option zum Ausfüllen von Anmerkungen zu Data Infrastructure Insights mit auf EC2 konfigurierten Tags. Die Anmerkungen müssen genau wie die EC2-Tags benannt werden. Data Infrastructure Insights füllt immer Anmerkungen vom gleichen Namen aus und versucht, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) zu füllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht füllt, kann es erforderlich sein, die Anmerkung zu entfernen und sie als Texttyp neu zu erstellen.

Bei AWS muss die Groß-/Kleinschreibung nicht beachtet werden, während bei Data Infrastructure Insights die Groß-/Kleinschreibung nicht beachtet werden muss. Wenn Sie in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“, „OWNER“ und „OWNER“ in EC2 erstellen, werden alle EC2-Variationen von „Owner“ der „Owner“ in der Annotation von Cloud Insight mit der Bezeichnung „OWNER“ zusammengefasst.

Zusätzliche Regionen Einschließen

Im Abschnitt AWS Data Collector **Erweiterte Konfiguration** können Sie das Feld * zusätzliche Regionen* so einstellen, dass zusätzliche durch Komma oder Semikolon getrennte Bereiche einbezogen werden. Standardmäßig ist dieses Feld auf ***US-.**** gesetzt, das auf allen US AWS Regionen sammelt. Um in *all* Regionen zu sammeln, setzen Sie dieses Feld auf ***.**. Ist das Feld **zusätzliche Regionen** leer, sammelt der Datensammler die im Feld **AWS Region** angegebenen Werte, wie im Abschnitt **Konfiguration** angegeben.

Erfassung über AWS Child-Konten

Data Infrastructure Insights unterstützt die Erfassung von untergeordneten Konten für AWS innerhalb eines einzigen AWS-Datensammlers. Die Konfiguration dieser Sammlung erfolgt in der AWS-Umgebung:

- Sie müssen jedes Child-Konto so konfigurieren, dass eine AWS Rolle zugewiesen wird, die es der Haupt-Account-ID ermöglicht, über das Children-Konto auf EC2 Details zuzugreifen.
- Für jedes untergeordnete Konto muss der Rollenname mit demselben String konfiguriert sein.
- Geben Sie diese Zeichenfolge für den Rollennamen im Abschnitt Data Infrastructure Insights AWS Data Collector **Advanced Configuration** im Feld **Cross Account role** ein.
- Das Konto, auf dem der Collector installiert ist, muss über *Delegate Access Administrator* Privileges verfügen. "AWS-Dokumentation"Weitere Informationen finden Sie im.

Best Practice: Es wird dringend empfohlen, dem EC2-Hauptkonto die vordefinierte Richtlinie *AmazonEC2ReadOnlyAccess* zuzuweisen. Außerdem sollte dem in der Datenquelle konfigurierten Benutzer mindestens die vordefinierte Richtlinie *AWSOrganizationsReadOnlyAccess* zugewiesen sein, um AWS abzufragen.

Im Folgenden finden Sie Informationen zur Konfiguration Ihrer Umgebung, damit Data Infrastructure Insights von untergeordneten AWS-Konten erfasst werden kann:

"Tutorial: Delegieren des Zugriffs über AWS Konten mithilfe von IAM-Rollen"

"AWS Setup: Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto bereitstellen, das Sie besitzen"

"Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Amazon FSX für NetApp ONTAP Datensammler

Dieser Datensammler erfasst Bestands- und Performance-Daten von Amazon FSX für NetApp ONTAP. Dieser Datensammler wird in den gesamten Serviceregionen von Data Infrastructure Insights inkrementell zur Verfügung gestellt. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn das Symbol für diesen Collector in Ihrer Data Infrastructure Insights Environment nicht angezeigt wird.

Für diesen Dateninfrastrukturüberblick ist ein ONTAP-Benutzer mit einer Rolle *Filesystem-scoped* erforderlich. In der AWS "Rollen und Regeln" Dokumentation finden Sie weitere Informationen zu verfügbaren Optionen. AWS unterstützt derzeit nur eine Art Benutzerrolle mit Filesystem Scope, nämlich *fsxadmin*. Dies ist die geeignete Rolle für den Data Infrastructure Insights Collector. Dem Benutzer sollten auch alle drei dieser Anwendungen zugewiesen sein: http, ontapi, ssh.

Terminologie

Data Infrastructure Insights erfasst Inventar- und Performance-Daten aus dem FSX-NetApp-Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
LUN	Datenmenge
Datenmenge	Internes Volumen

FSX-NetApp – Terminologie

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den FSX-NetApp Storage Asset Landing Pages finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen, diskreten Modellnamen in diesem Cluster.
- Anbieter – AWS
- Seriennummer: Die Seriennummer des Arrays.
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Rohkapazität: Die Summe aus 2 des gesamten SSD-Speichers, der dem FSX-Dateisystem zugewiesen ist
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.
- IOPS – die Summe der IOPS aller Volumes, die in diesem Storage-Pool zugewiesen sind.
- Durchsatz – der Gesamtdurchsatz aller Volumes, die in diesem Storage-Pool zugewiesen sind.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Konto mit der Rolle „fsxadmin“ haben, wobei drei Anwendungen zugewiesen sind - ssh, ontapi, http
- Zu den Kontodetails gehören Benutzername und Passwort.
- Anforderungen an den Hafen: 443

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domain-Name des NetApp Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp Cluster

Erweiterte Kennzahlen

Dieser Datensammler sammelt die folgenden erweiterten Metriken aus dem FSX für NetApp ONTAP Storage:

- fpolicy
- nfsv3
- nfsv3:Node
- nfsv4
- nfsv4_1
- nfsv4_1:Node
- nfsv4:Node
- Policy_Group
- Qtree
- Datenmenge
- Workload_Volume

Beachten Sie, dass FSX CLI- und API-Befehle einige Kapazitätswerte abrufen, die Data Infrastructure Insights ZAPI nicht sammelt, so dass bestimmte Kapazitätswerte (z. B. für Speicherpools) in Data Infrastructure

Insights anders sein können als sie auf dem FSX selbst sind.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des Azure Compute-Datensammlers

Data Infrastructure Insights verwendet den Compute-Datensammler Azure, um Inventar- und Performance-Daten aus Azure Computing-Instanzen zu erfassen.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren.

- Port-Anforderung: 443 HTTPS
- Azure OAuth 2.0 Redirect URI (login.microsoftonline.com)

- Azure Management Rest-IP (management.azure.com)
- Azure Resource Manager IP (management.core.windows.net)
- Azure Service Principal Application (Client)-ID (Reader-Rolle erforderlich)
- Azure Service Principal Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen ein Azure-Konto für die Erkennung von Data Infrastructure Insights einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten. https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure Service Principal Application (Client)-ID (Reader-Rolle erforderlich)	Anmelde-ID bei Azure. Erfordert Zugriff auf die Leserrolle.
Azure-Mandanten-ID	Microsoft Mandanten-ID
Authentifizierungsschlüssel Des Azure Service Principal	Anmeldeauthentifizierungsschlüssel
Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt	Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt.

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Wählen Sie „exclude“ oder „include“, um VMs nach Tags zu filtern	Geben Sie an, ob VM’s by Tags beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn ‘include’ ausgewählt ist, kann das Feld Tag-Schlüssel nicht leer sein.
Markieren Sie Schlüssel und Werte, nach denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Tag**, um die VMs (und die zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte von Tags auf der VM entsprechen, einzuschließen bzw. auszuschließen. Tag-Schlüssel erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM solange gefiltert, wie sie dem Tag-Schlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector

Supportmatrix".

Broadcom

Datensammler Brocade Network Advisor

Dateninfrastrukturanalysen verwenden den Datensammler Brocade Netzwerkberater, um Bestands- und Performancedaten von Brocade-Switches zu erfassen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Brocade Netzwerkberater-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Logischer Switch	Logischer Switch

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit führt Verbindungen zu TCP-Port 443 auf dem BNA-Server ein. BNA-Server muss Version 14.2.1 oder höher ausführen.
- IP-Adresse des Brocade Network Advisor Servers
- Benutzername und Kennwort für ein Administratorkonto
- Port-Anforderung: HTTP/HTTPS 443

Konfiguration

Feld	Beschreibung
Brocade Network Advisor Server IP	IP-Adresse des Network Advisor-Servers
Benutzername	Benutzername für den Switch
Benutzername	Administrator-Benutzername
Passwort	Administratorpasswort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Standardport 443) oder HTTP (Standardport 80)
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Passwort	Passwort für den Switch
Abfrageintervall für Bestand (min)	Der Standardwert ist 40
Access Gateway Melden	Aktivieren Sie diese Option, um Geräte im Access Gateway-Modus einzubeziehen
Leistungsintervall (Sek.)	Der Standardwert ist 1800

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Sie erhalten eine Meldung, dass mehr als 1 Knoten am Access Gateway-Port angemeldet ist, oder Datensammler kann das Access Gateway-Gerät nicht erkennen.	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und dass alle verbundenen WWNs erwartet werden. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen erfasst die Akquisition des Core Fabric Switch die NPV Geräte-Daten.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Brocade FC Switch

Dateninfrastruktur Insights verwendet die SSH-Datenquelle (Brocade FC Switch), um eine Bestandsaufnahme für Brocade- oder umbenannte Switch-Geräte zu erkennen, auf denen die Firmware des Factsored Operating System (FOS) 4.2 und höher ausgeführt wird. Geräte werden sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Brocade FC Switch-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Zone	Zone
Logischer Switch	Logischer Switch
Virtual Volume	Datenmenge
LSAN-Zone zu erreichen	IVR-Zone

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die Data Infrastructure Insights Acquisition Unit (AU) initiiert Verbindungen zu TCP-Port 22 auf Brocade-Switches, um Bestandsdaten zu sammeln. Die AU wird auch Verbindungen zu UDP Port 161 für die Sammlung von Leistungsdaten initiieren.
- Es muss eine IP-Verbindung zu allen Switches in der Fabric vorhanden sein. Wenn Sie das Kontrollkästchen Alle Switches in der Fabric ermitteln aktivieren, identifiziert Data Infrastructure Insights alle Switches in der Fabric, benötigt jedoch IP-Konnektivität zu diesen zusätzlichen Switches, um sie zu erkennen.
- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können PuTTY (Open Source Terminal Emulator) verwenden, um den Zugriff zu bestätigen.
- Die Ports 161 und 162 müssen offen sein für alle Switches im Fabric für SNMP-Performance-Abfragen.
- SNMP Read-Only Community String

Konfiguration

Feld	Beschreibung
Switch-IP	IP-Adresse oder vollqualifizierter Domänenname des EFC-Servers
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch
SNMP	SNMP-Version
SNMP-Community-Zeichenfolge	SNMP read-only Community String verwendet, um auf den Switch zugreifen
SNMP-Benutzername	SNMP-Benutzername
SNMP-Kennwort	SNMP-Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Fabric-Name	Der Fabric-Name wird vom Data Collector gemeldet. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden.

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 15.
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen
Admin-Domänen Aktiv	Wählen Sie, wenn Sie Admin-Domains verwenden
MPR-Daten abrufen	Wählen Sie diese Option aus, um Routing-Daten von Ihrem Multiprotokoll-Router zu erhalten.
Trapping Aktivieren	Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren.
Mindestzeit zwischen Traps (s)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen. Der Standardwert ist 10.
Erkennung aller Switches in der Fabric	Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen
Entscheiden Sie sich für HBA vs Zonenaliase	Wählen Sie, ob HBA- oder Zonenaliasen bevorzugt werden sollen
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
SNMP-Auth-Protokoll	SNMP-Authentifizierungsprotokoll (nur SNMP v3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort (nur SNMP v3)
SNMP wird erneut verwendet	Anzahl der SNMP-Wiederholungsversuche

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Die Bestandsaufnahme der Brocade Datenquelle schlägt mit dem Fehler fehl: <date> <time> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Fehler 2 von 2: <datasource Name> [Interner Fehler] - das Modell für das Gerät konnte nicht generiert werden <IP>. Fehler beim Erkennen der Eingabeaufforderung ([Gerätename <Name>]: Fehler beim Generieren des Modells für Gerät <IP> nicht möglich. Fehler beim Erkennen der Eingabeaufforderung)	Das Problem kann verursacht werden, wenn der Brocade Switch mit einer Eingabeaufforderung zu lange zurückgibt und damit die Standardzeitüberschreitung von 5 Sekunden überschreitet. Versuchen Sie in den Einstellungen für die erweiterte Konfiguration des Datensammlers in Data Infrastructure Insights, das *SSH Banner Wait Timeout (sec)* auf einen höheren Wert zu erhöhen.
Fehler: „Data Infrastructure Insights received invalid Chassis role“	Vergewissern Sie sich, dass dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Gehäuserolle erteilt wurde.

Problem:	Versuchen Sie dies:
Fehler: „IP-Adresse des Gehäuses nicht stimmt überein“	Ändern Sie die Konfiguration der Datenquelle, um die Gehäuse-IP-Adresse zu verwenden.
Sie erhalten eine Meldung, dass mehr als 1 Knoten am Access Gateway-Port angemeldet ist	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und dass alle verbundenen WWNs erwartet werden. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen erfasst die Akquisition des Core Fabric Switch die NPV Geräte-Daten.
Performance-Erfassung schlägt mit „Timeout beim Senden der SNMP-Anforderung“ fehl.	Je nach Abfragevariablen und Switch-Konfiguration können einige Abfragen das Standard-Timeout überschreiten. "Weitere Informationen".

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Brocade FOS REST Data Collector

Data Infrastructure Insights verwendet den Brocade FOS REST Collector, um Bestand und Performance für Brocade-Switch-Geräte mit FabricOS (FOS) Firmware 8.2 und höher zu ermitteln.

Bitte beachten Sie: FOS' Standard "user"-Ebene ist nicht ausreichend leistungsfähig, damit Data Infrastructure Insights alle logischen Aspekte eines Geräts anzeigen kann - wir benötigen ein Benutzerkonto mit aktivierter "Chassis Role" sowie Berechtigungen für alle auf einem Switch konfigurierten virtuellen Fabrics.

Hier ist ein Beispiel dafür, wie Sie ein Benutzerkonto mit den geringsten Berechtigungen für die Verwendung von Data Infrastructure Insights in einer SSH-Sitzung auf einem FOS-Gerät erstellen können:

UserConfig --add NetAppCIUser -r user -l 1-128 -c user -p Qwerty!

Dadurch wird ein User „NetAppCIUser“ mit einem Passwort von „Qwerty!“ eingerichtet. Dieser Benutzer hat die „user“-Rolle (-r) für alle 128 möglichen virtuellen Fabrics (-l). Dieser Benutzer verfügt zusätzlich über die erforderliche „Chassis“-Rolle (-c) mit zugewiesenem Zugriff auf Benutzerebene.

Standardmäßig versucht dieser Collector, alle FOS-Geräte zu ermitteln, die Teil aller Fabrics sind, zu denen der Switch gehört.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Brocade FOS REST Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Zone	Zone

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Logischer Switch	Logischer Switch
LSAN-Zone zu erreichen	IVR-Zone

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Es muss eine TCP-Verbindung zu allen Switches in der Fabric vorhanden sein. Dieser Datensammlertyp versucht nahtlos sowohl HTTP als auch HTTPS für jedes Gerät in der Fabric. Wenn Sie das Kontrollkästchen *Discover all Switches in the Fabric* aktivieren, identifiziert Data Infrastructure Insights alle Switches in der Fabric; es benötigt jedoch TCP-Konnektivität zu diesen zusätzlichen Switches, um sie zu erkennen.
- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können den Zugriff über die Webschnittstelle des Geräts bestätigen.

Konfiguration

Feld	Beschreibung
Switch-IP	IP-Adresse oder vollständig qualifizierter Domänenname des FOS-Switches
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch

Erweiterte Konfiguration

Feld	Beschreibung
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IPv4-Adressen, die von der Abfrage ausgeschlossen werden sollen.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60.
Erkennung aller Switches in der Fabric	Wählen Sie diese Option aus, um alle Switches in der Fabric zu ermitteln.
Entscheiden Sie sich für HBA vs Zonenaliase	Wählen Sie aus, ob HBA- oder Zonenaliase bevorzugt werden sollen.
Verbindungstyp	HTTP oder HTTPS.
Beachten Sie, dass diese Einstellung nur ändert, welches Protokoll-CI zuerst pro Gerät verwendet. CI versucht automatisch, das andere Protokoll zu verwenden, wenn die Standardeinstellung fehlschlägt	TCP-Port überschreiben
Geben Sie einen Port an, wenn der Standardwert nicht verwendet wird.	Leistungsintervall (Sek.)

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Die Testfunktion warnt mich, dass ein Protokoll nicht zugänglich ist	Ein bestimmtes Brocade FOS 8.2+ Gerät will nur über HTTP oder HTTPS sprechen - wenn ein Switch ein digitales Zertifikat installiert hat, wirft der Switch HTTP-Fehler auf, wenn man versucht, mit unverschlüsseltem HTTP gegen HTTPS zu kommunizieren. Die Testfunktion versucht die Kommunikation mit HTTP und HTTPS - wenn der Test Ihnen mitteilt, dass ein Protokoll erfolgreich ist, können Sie den Collector sicher speichern und sich keine Sorgen machen, dass das andere Protokoll nicht erfolgreich war - der Collector versucht beide Protokolle während der Sammlung und schlägt nur fehl, wenn keines funktioniert.
Fehler: „Data Infrastructure Insights received invalid Chassis role“	Vergewissern Sie sich, dass dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Gehäuserolle erteilt wurde.
Fehler: „IP-Adresse des Gehäuses nicht stimmt überein“	Ändern Sie die Konfiguration der Datenquelle, um die Gehäuse-IP-Adresse zu verwenden.
Die Inventur schlägt mit einer 403 Verbotenen fehl	Dies kann einfach schlechte Anmeldeinformationen sein, oder es kann bezeichnend sein, dass Sie versuchen, eine nicht ausreichend leistungsstarke Rolle zu verwenden - denken Sie daran, dass Benutzer auf Benutzerebene nicht über das erforderliche Recht auf „Gehäuserolle“ verfügen oder den Zugriff auf nicht standardmäßige virtuelle Fabrics anzeigen.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Cisco MDS Fabric Switches Datensammler

Data Infrastructure Insights verwendet den Data Collector der Cisco MDS-Fabric-Switches zur Bestandsaufnahme von Cisco MDS-Fabric-Switches sowie einer Vielzahl von Cisco Nexus FCoE-Switches, auf denen der FC-Service aktiviert ist.

Darüber hinaus können Sie mit diesem Datensammler viele Modelle von Cisco-Geräten im NPV-Modus entdecken.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Cisco FC Switch-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
VSAN	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
Name Server-Eintrag	Name Server-Eintrag
Inter-VSAN Routing-Zone (IVR	IVR-Zone

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Eine IP-Adresse eines Switches in der Fabric oder den einzelnen Switches
- Chassis-Erkennung für die Fabric-Erkennung
- Bei Verwendung von SNMP V2, nur lesbare Community-String
- Port 161 wird für den Zugriff auf das Gerät verwendet

Konfiguration

Feld	Beschreibung
Cisco Switch IP	IP-Adresse oder vollqualifizierter Domain-Name des Switches
SNMP-Version	Wählen Sie V1, V2 oder V3 aus. Für Leistungserfassung ist V2 oder höher erforderlich.
SNMP-Community-Zeichenfolge	SNMP Read-Only-Community-String zum Zugriff auf den Switch (gilt nicht für SNMP v3)
Benutzername	Benutzername für den Switch (nur SNMP v3)
Passwort	Passwort für den Switch (nur SNMPv3)

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten)
SNMP-Auth-Protokoll	SNMP-Authentifizierungsprotokoll (nur SNMPv3)
SNMP-Datenschutzprotokoll	SNMP-Datenschutzprotokoll (nur SNMPv3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort
SNMP wird erneut verwendet	Anzahl der SNMP-Wiederholungsversuche
SNMP-Timeout (ms)	SNMP-Timeout (Standard 5000 ms)

Feld	Beschreibung
Trapping Aktivieren	Wählen Sie, um das Überfüllen zu aktivieren. Wenn Sie Trapping aktivieren, müssen Sie auch SNMP-Benachrichtigungen aktivieren.
Mindestzeit zwischen Traps (s)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden)
Alle Fabric Switches Erkennen	Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IP-Adressen, die von der Abfrage ausgeschlossen werden sollen
Enthaltene Geräte	Kommagetrennte Liste der Geräte-IPs, die in Abfrage aufgenommen werden sollen
Überprüfen Sie Den Gerätetyp	Wählen Sie diese Option aus, um nur die Geräte zu akzeptieren, die sich explizit als Cisco-Geräte bewerben
Erster Alias-Typ	Geben Sie eine erste Präferenz für die Auflösung des Alias an. Wählen Sie aus folgenden Optionen: **Device Alais** Dies ist ein benutzerfreundlicher Name für einen Port WWN (PWWN), der bei Bedarf in allen Konfigurationsbefehlen verwendet werden kann. Alle Switches der Produktfamilie Cisco MDS 9000 unterstützen Distributed Device Alias Services (Geräte-Aliase). **Keine** meldet keinen Alias. **Port Description** Eine Beschreibung, um den Port in einer Liste von Ports zu identifizieren. **Zone Alias (all)** Ein benutzerfreundlicher Name für einen Port, der nur für die aktive Konfiguration verwendet werden kann. Dies ist die Standardeinstellung.
Typ Des Zweiten Alias	Geben Sie eine zweite Vorliebe für die Auflösung des Alias an
Dritter Aliastyp	Geben Sie eine dritte Präferenz für die Auflösung des Alias an
Aktivieren Sie die Unterstützung für den SANTAP-Proxy-Modus	Wählen Sie aus, ob Ihr Cisco Switch SANTAP im Proxy-Modus verwendet. Wenn Sie EMC RecoverPoint verwenden, verwenden Sie wahrscheinlich SANTAP.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden)

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Gehäuse konnte nicht erkannt werden. Es wurden keine Switches gefunden	• Ping the device with the IP Configured • Melden Sie sich mit der Cisco Device Manager-GUI am Gerät an • Melden Sie sich über CLI beim Gerät an • Versuchen Sie, SNMP Walk auszuführen
Fehler: Gerät ist kein Cisco MDS Switch	• Vergewissern Sie sich, dass die für das Gerät konfigurierte IP-Adresse der Datenquelle richtig ist • Melden Sie sich über die Cisco Device Manager-GUI am Gerät an • Melden Sie sich über die CLI an
Fehler: Data Infrastructure Insights kann den WWN des Switches nicht abrufen.	Hierbei handelt es sich möglicherweise nicht um einen FC- oder FCoE-Switch, dessen Unterstützung möglicherweise nicht möglich ist. Stellen Sie sicher, dass der in der Datenquelle konfigurierte IP/FQDN wirklich ein FC/FCoE-Switch ist.
Fehler: Es wurden mehrere Knoten gefunden, die beim NPV Switch Port angemeldet sind	Deaktivieren Sie die direkte Akquisition des NPV-Schalters
Fehler: Verbindung zum Schalter konnte nicht hergestellt werden	• Stellen Sie sicher, dass das Gerät EINGESCHALTET ist • Überprüfen Sie die IP-Adresse und den Zuhörport • Ping the device • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an • Melden Sie sich über CLI beim Gerät an • Ausführen von SNMP Walk

Leistung

Problem:	Versuchen Sie dies:
Fehler: Leistungsaufnahme wird von SNMP v1 nicht unterstützt	• Datenquelle bearbeiten und Switch-Performance deaktivieren • Datenquelle und Switch-Konfiguration ändern, um SNMP v2 oder höher zu verwenden

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Cohesity SmartFiles

Dieser REST-API-basierte Collector erwirbt ein Cohesity-Cluster, das die „Ansichten“ (als interne Data Infrastructure Insights Volumes) und die verschiedenen Nodes erkennt und Performance-Metriken sammelt.

Konfiguration

Feld	Beschreibung
Cohesity Cluster-IP	IP-Adresse des Cohesity-Clusters
Benutzername	Benutzername für den Cohesity Cluster
Passwort	Passwort, das für den Cohesity Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Port, der für die TCP-Kommunikation mit dem Cohesity-Cluster verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Leistungsintervall (min)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 900 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell

Datensammler der Dell EMC XC-Serie

Data Infrastructure Insights verwendet diesen Datensammler, um Bestands- und Leistungsinformationen für die Dell Speicherarrays der EMC XC-Serie zu ermitteln.

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	IP-Adresse des XC-Servers
Benutzername	Benutzername für den XC-Server
Passwort	Passwort, das für den XC-Server verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Port, der für die TCP-Kommunikation mit dem XC-Server verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Leistungsintervall (min)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell EMC

DELL EMC Data Domain-Datensammler

Dieser Datensammler erfasst Bestands- und Performance-Informationen von DELL EMC Data Domain Deduplizierungs-Storage-Systemen. Zur Konfiguration dieses Datensammlers sind spezifische Konfigurationsanweisungen und Nutzungsempfehlungen zu beachten.

Terminologie

Data Infrastructure Insights bezieht die folgenden Bestandsinformationen aus dem Data Domain-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Array Erledigen	Storage
FC-Port	Port
File-System	Internes Volumen
Kontingente	Kontingente
NFS- und CIFS-Freigabe	Dateifreigabe

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In diesem Datencolletor sind dies möglicherweise nicht alle Fälle.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- IP-Adresse des Data Domain-Geräts
- Schreibgeschützter Benutzername und Kennwort für den Data Domain-Speicher
- SSH-Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des Data Domain-Speicherarrays
Benutzername	Der Benutzername für das Data Domain-Speicherarray
Passwort	Das Kennwort für das Data Domain-Speicherarray

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.
SSH-Port	SSH-Service-Port

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des EMC ECS-Datensammlers

Dieser Datensammler erfasst Bestands- und Performancedaten von EMC ECS Speichersystemen. Für die Konfiguration benötigt der Datensammler eine IP-Adresse oder einen Hostnamen des ECS-Clusters sowie einen Benutzernamen und ein Passwort.

Dell EMC ECS wird mit einer anderen Rate von Raw TB zu Managed Units gemessen. Alle 40 TB unformatierte ECS-Kapazität wird als 1 geladen "Verwaltete Einheit (ME)".

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem ECS-Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Mandant	Storage-Pool
Eimer	Internes Volumen
Festplatte	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Eine IP-Adresse oder ein Hostname des ECS-Clusters
- Benutzername und Passwort für das ECS-System
- Port 4443 (HTTPS). Erfordert ausgehende Verbindungen zum TCP-Port 4443 auf dem ECS-System.

Konfiguration

Feld	Beschreibung
ECS Host	IP-Adresse oder vollqualifizierter Domain-Name des ECS-Systems

Feld	Beschreibung
ECS-Host-Port	Port, der für die Kommunikation mit ECS Host verwendet wird
ECS-Benutzer-ID	Benutzer-ID für ECS
Passwort	Passwort wird für ECS verwendet

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 360 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Leistung

Problem:	Versuchen Sie dies:
Fehler: Es wurden nicht genügend Daten erfasst.	• Prüfen Sie den Zeitstempel der Sammlung in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend • Warten Sie länger
Fehler: Das Abfrageintervall für die Performance ist zu groß.	Überprüfen Sie den Sammlungs-Zeitstempel in der Protokolldatei €{logfile} und ändern Sie das Abfrageintervall entsprechend

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell EMC PowerScale Datensammler

Data Infrastructure Insights verwendet den SSH-Datensammler Dell EMC PowerScale (ehemals Isilon), um Bestands- und Performance-Daten aus PowerScale-out-NAS-Speicher zu erfassen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
File-System	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- Administrator Berechtigungen für den PowerScale-Speicher
- IP-Adresse des PowerScale-Clusters
- SSH-Zugriff auf Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des PowerScale-Clusters
Benutzername	Benutzername für den PowerScale-Cluster
Passwort	Passwort, das für den PowerScale-Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
SSH-Port	SSH-Service-Port. Der Standardwert ist 22.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Befehle, die für die rollenbasierte Administration nicht aktiviert sind, benötigen Root-Benutzerzugriff“	* Überprüfen Sie, dass der Benutzer über die Berechtigungen verfügt, um die folgenden Befehle auf dem Gerät auszuführen: > isi Version osselease > isi Status -q > isi Status -n > isi Devices -d %s > isi Lizenz * Überprüfen Sie, dass die im Assistenten verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
„Interner Fehler“ mit Fehlermeldungen “Befehl <Ihr Befehl> Ausführen fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>. Sudo Befehl ausführen Berechtigungsproblem“	Überprüfen Sie, ob der Benutzer über sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Rest-Datensammler Dell EMC Isilon/PowerScale

Data Infrastructure Insights verwendet den REST-Datensammler Dell EMC Isilon/PowerScale, um Bestands- und Performance-Daten von Dell EMC Isilon- oder PowerScale-Speicher zu erfassen. Dieser Collector unterstützt Arrays, auf denen OneFS 8.0.0+ ausgeführt wird.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
OneFS File System	Internes Volumen
OneFS File System	Storage-Pool
Qtree	Qtree

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- Ein Benutzerkonto und ein Passwort. Dieses Konto muss nicht Administrator/Root sein, aber Sie MÜSSEN Ihrem Servicekonto eine beträchtliche Anzahl an schreibgeschützten Berechtigungen gewähren - siehe Tabelle unten

- IP-Adresse / Fully Qualified Domain Name des Dell EMC Isilon / PowerScale Clusters
- HTTPS-Zugriff auf Port 8080
- Isilon/PowerScale-Cluster mit OneFS 8.0.0 oder höher

Berechtigungsname	Beschreibung	r(Lesen) oder rw (Lesen+Schreiben)
ISI_PRIV_LOGIN_PAPI	Plattform-API	r
ISI_PRIV_SYS_TIME	Zeit	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Berechtigung	r
ISI_PRIV_DEVICES	Geräte	r
ISI_PRIV_EVENT	Ereignis	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Netzwerk	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Konfigurieren Sie die Plattform-API	r
ISI_PRIV_QUOTA	Kontingente	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	SMB	r
ISI_PRIV_STATISTICS	Statistiken	r
ISI_PRIV_SWIFT	Swift	r
ISI_PRIV_JOB_ENGINE	Job-Engine	r

Konfiguration

Feld	Beschreibung
Isilon IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domain-Name des Isilon-Speichers
Benutzername	Benutzername für Isilon
Passwort	Passwort, das für Isilon verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 8080.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.

Feld	Beschreibung
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Befehle, die für die rollenbasierte Administration nicht aktiviert sind, benötigen Root-Benutzerzugriff“	* Überprüfen Sie, dass der Benutzer über die Berechtigungen verfügt, um die folgenden Befehle auf dem Gerät auszuführen: > isi Version osselease > isi Status -q > isi Status -n > isi Devices -d %s > isi Lizenz * Überprüfen Sie, dass die im Assistenten verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
„Interner Fehler“ mit Fehlermeldungen “Befehl <Ihr Befehl> Ausführen fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>. Sudo Befehl ausführen Berechtigungsproblem“	Überprüfen Sie, ob der Benutzer über sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell EMC PowerStore-Datensammler

Der EMC PowerStore Data Collector sammelt Bestandsdaten aus dem EMC PowerStore-Speicher. Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Der EMC PowerStore Datensammler erfasst die Replikationsbeziehungen zwischen Volume und Volume, die PowerStore über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicher-Array für jeden PowerStore-Cluster und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Storage-Pool- oder Volume-Daten erfasst.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Host	Host
Host_Volume_Zuordnung	Host_Volume_Zuordnung
Hardware (es hat Laufwerke unter „extra_Details“-Objekt): Laufwerke	Festplatte

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Appliance	Storage Pool
Cluster	Storage Array Durchführt
Knoten	StorageNode
fc_Port	Port
Datenmenge	Datenmenge
InternalVolume	File_System

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort

Konfiguration

Feld	Beschreibung
PowerStore Gateway(s)	IP-Adressen oder vollqualifizierte Domain-Namen des PowerStore-Speichers
Benutzername	Benutzername für PowerStore
Passwort	Passwort, das für PowerStore verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 443
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.

Die PowerStore Performance-Sammlung von Cloud Insight nutzt die 5-minütigen Granularitätsquelldaten von PowerStore. Daher fragt Data Infrastructure Insights diese Daten alle fünf Minuten ab. Dies ist nicht konfigurierbar.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell EMC RecoverPoint Data Collector

Der primäre Anwendungsfall des EMC RecoverPoint Data Collector ist die Ermittlung von Replikationsbeziehungen zwischen Volumes, die von der RecoverPoint-Speicher-

Appliance unterstützt werden. Dieser Sammler entdeckt auch das RecoverPoint-Gerät selbst. Bitte beachten Sie, dass Dell/EMC eine VMware Backup-Lösung für VMs--„RecoverPoint for VMs“ verkauft, die von diesem Collector nicht unterstützt wird

Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Der EMC RecoverPoint Data Collector sammelt die Replikationsbeziehungen zwischen Volume und Volume, die RecoverPoint über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicher-Array für jeden RecoverPoint-Cluster an und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Storage-Pool- oder Volume-Daten erfasst.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- REST-API-Zugriff über Port 443

Konfiguration

Feld	Beschreibung
Adresse von RecoverPoint	IP-Adresse oder vollqualifizierter Domain-Name des RecoverPoint-Clusters
Benutzername	Benutzername für das RecoverPoint-Cluster
Passwort	Passwort, das für den RecoverPoint-Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port für die Verbindung mit dem RecoverPoint-Cluster
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.
Ausgeschlossene Cluster	Kommagetrennte Liste von Cluster-IDs oder Namen, die beim Abfragen ausgeschlossen werden sollen.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

DELL EMC ScaleIO/PowerFlex-Datensammler

Der Datensammler ScaleIO/PowerFlex erfasst Bestandsdaten aus ScaleIO und PowerFlex-Speicher. Für die Konfiguration benötigt dieser Datensammler die

ScaleIO/PowerFlex-Gateway-Adresse sowie einen Admin-Benutzernamen und ein Passwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Datensammler ScaleIO/PowerFlex. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
MDM-Cluster (Meta Data Manager	Storage
SDS (ScaleIO/PowerFlex Data Server)	Storage-Node
Storage-Pool	Storage-Pool
Datenmenge	Datenmenge
Gerät	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Schreibgeschützter Zugriff auf das Admin-Benutzerkonto
- Port-Anforderung: HTTPS-Port 443

Konfiguration

Feld	Beschreibung
ScaleIO/PowerFlex-Gateway(s)	IP-Adressen oder FQDNs von ScaleIO/PowerFlex Gateways, getrennt durch Komma (,) oder Semikolon (;)
Benutzername	Admin-Benutzername für die Anmeldung beim ScaleIO/PowerFlex-Gerät
Passwort	Passwort für die Anmeldung beim ScaleIO/PowerFlex-Gerät

Erweiterte Konfiguration

Klicken Sie auf das Kontrollkästchen Inventar, um die Bestandssammlung zu aktivieren.

Feld	Beschreibung
HTTPS-Port	443
Abfrageintervall für Bestand (min)	Der Standardwert ist 60.
Verbindungs-Timeout (s)	Der Standardwert ist 60.

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des EMC Unity Data Collector

DER DELL EMC Unity (ehemals VNXe)-Datensammler bietet Bestandsunterstützung für VNXe Unified Storage-Arrays. Data Infrastructure Insights unterstützt derzeit iSCSI- und NAS-Protokolle.

Anforderungen

- Der Unity Data Collector ist CLI-basiert. Sie müssen Unisphere for Unity CLI (uemcli.exe) auf der Erfassungseinheit installieren, in der sich Ihr VNXe Data Collector befindet.
- uemcli.exe verwendet HTTPS als Transportprotokoll, sodass die Erfassungseinheit in der Lage sein muss, HTTPS-Verbindungen zur Unity zu initiieren.
- IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
- Sie müssen mindestens einen schreibgeschützten Benutzer zur Verwendung durch den Datensammler haben.
- HTTPS am Port 443 ist erforderlich
- Der EMC Unity Data Collector bietet NAS- und iSCSI-Unterstützung für die Bestandsaufnahme. Fibre-Channel-Volumes werden erkannt, Data Infrastructure Insights jedoch keine Berichte zu FC-Mapping, -Masking oder -Speicherports.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem Unity-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage Array Durchführt	Storage
Prozessor	Storage-Node
Storage-Pool	Storage-Pool
Allgemeine Informationen zu iSCSI Block, VMware VMFS	Share
Remote-Replikationssystem	Synchronisierung
ISCSI-Node	ISCSI-Ziel-Node
ISCSI-Initiator	ISCSI-Target-Initiator

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Konfiguration

Feld	Beschreibung
Unity Storage	IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
Benutzername	Benutzername für das Unity-Gerät
Passwort	Kennwort für das Unity-Gerät
Vollständiger Pfad zur ausführbaren UEMCLI	Vollständiger Pfad zum Ordner mit der ausführbaren Datei *uemcli.exe*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten
Unity-CLI-Port	Port, der für die Unity-CLI verwendet wird
Leistungsintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Externes Dienstprogramm konnte nicht ausgeführt werden“ mit Fehlermeldungen „Unisphere executable uemcli konnte nicht gefunden werden“	* Korrekte IP-Adresse, Benutzername und Kennwort überprüfen * Bestätigen Sie, dass Unisphere CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass das Unisphere CLI-Installationsverzeichnis in der Datenquelle korrekt ist * Bestätigen Sie, dass die IP-Adresse der VNXe in der Konfiguration der Datenquelle korrekt ist. Öffnen Sie in der Data Infrastructure Insights Acquisition Unit eine CMD und wechseln Sie in das konfigurierte Installationsverzeichnis: €{INSTALLDIR. Versuchen Sie, eine Verbindung zum VNXe-Gerät herzustellen, indem Sie Folgendes eingeben: Uemcli -d <Ihre IP> -U <Ihre ID> /sys/General show

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler der Dell EMC VMAX- und PowerMax-Gerätefamilie

Data Infrastructure Insights erkennt EMC VMAX- und PowerMax-Speicher-Arrays mithilfe der symcli-Befehle von Solutions Enabler in Verbindung mit einem vorhandenen Solutions Enabler-Server in Ihrer Umgebung. Der vorhandene Solutions Enabler-Server verfügt über eine Verbindung zum VMAX/PowerMax-Speicher-Array über den Zugriff auf

Gatekeeper-Volumes.

Anforderungen

Bevor Sie diesen Datensammler konfigurieren, sollten Sie sicherstellen, dass Data Infrastructure Insights über TCP-Verbindungen zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. Data Infrastructure Insights ermittelt alle Symmetrix-Arrays, die auf diesem Server „lokal“ sind, wie in der Ausgabe „symcfg list“ dieses Servers dargestellt.

- Die Anwendung EMC Solutions Enabler (CLI) mit SMI-S Provider muss auf dem Acquisition Unit-Server installiert sein. Die Version muss mit der Version übereinstimmen oder niedriger als die auf dem Solutions Enabler Server ausgeführte Version sein.
- Eine ordnungsgemäß konfigurierte Datei {installdir}\EMC\SYMAPI\config\netcnfg ist erforderlich. Diese Datei definiert Dienstnamen für Solutions Enabler-Server sowie die Zugriffsmethode (SECURE / NOSECURE /ANY).
- Wenn Sie eine Lese-/Schreiblatenz auf Speicherknotenebene benötigen, muss der SMI-S-Provider mit einer laufenden Instanz der UNISPHERE for VMAX-Anwendung kommunizieren.
- IP-Adresse des Management Solutions Enabler Servers
- Administratorberechtigungen auf dem Solutions Enabler (SE)-Server
- Schreibgeschützter Benutzername und Kennwort für die SE-Software
- DIE UNISPHERE for VMAX-Anwendung muss ausgeführt werden und Statistiken für die EMC VMAX- und PowerMax-Speicher-Arrays sammeln, die von der SMI-S Provider-Installation gemanagt werden
- Zugriffsvalidierung für die Leistung: In einem Webbrowser auf Ihrer Acquisition Unit gehen Sie zu *https://<SMI-S Hostname oder IP>:5989/ecomconfig*, wobei „SMI-S Hostname or IP“ die IP-Adresse oder den Hostnamen Ihres SMI-S Servers ist. Diese URL ist für ein Verwaltungsportal für den Service EMC SMI-S (auch bekannt als „ECOM“) vorgesehen. Sie erhalten ein Login-Popup.
- Berechtigungen müssen in der Daemon-Konfigurationsdatei des Solutions Enabler Servers deklariert werden, die üblicherweise hier zu finden ist: */var/symapi/config/daemon_Users*

  Hier ist eine Beispieldatei mit den richtigen Cisys Berechtigungen.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
#############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus der EMC VMAX/PowerMax-Datenquelle. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Festplattengruppe	Festplattengruppe
Storage	Array-Storage
Direktor	Storage-Node
Geräte-Pool, Storage-Ressourcen-Pool (SRP)	Storage-Pool
Gerät TDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Konfiguration

Hinweis: Wenn die SMI-S-Benutzerauthentifizierung nicht aktiviert ist, werden die Standardwerte im Data Infrastructure Insights Datensammler ignoriert.

Feld	Beschreibung
Name Des Service	Dienstname wie in der Datei *netcnfg* angegeben
Vollständiger Pfad zur CLI	Vollständiger Pfad zu dem Ordner, der die Symmetrix CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Bestandsfilter Geräteliste	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen

Feld	Beschreibung
Verbindungs-Caching	Wählen Sie die Methode zum Zwischenspeichern von Verbindungen: * LOCAL bedeutet, dass der Cloud Insights Acquisition-Dienst auf dem Solutions Enabler-Server ausgeführt wird, der über eine Fibre-Channel-Verbindung zu den Symmetrix-Arrays verfügt, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. Dies ist möglicherweise in einigen Konfigurationen der Remote Acquisition Unit (rau) zu sehen. * REMOTE_CACHED ist der Standard und sollte in den meisten Fällen verwendet werden. Hierbei werden die NETCNFG-Dateieinstellungen verwendet, um eine Verbindung über IP mit dem Solutions Enabler-Server herzustellen. Dieser muss über eine Fibre-Channel-Verbindung zu den Symmetrix-Arrays verfügen, die Sie ermitteln möchten, und hat Zugriff auf Gatekeeper-Volumes. * Wenn DIE OPTIONEN REMOTE_CACHED CLI-Befehle fehlschlagen, verwenden Sie DIE REMOTE-Option. Denken Sie daran, dass es den Erfassungsprozess verlangsamen wird (möglicherweise auf Stunden oder sogar Tage in extremen Fällen). Die NETCNFG-Dateieinstellungen werden weiterhin für eine IP-Verbindung zum Solutions Enabler-Server verwendet, der über Fibre Channel-Verbindungen zu den erkannten Symmetrix-Arrays verfügt. **Hinweis:** Diese Einstellung ändert nicht das Verhalten von Data Infrastructure Insights in Bezug auf die Arrays, die von der Ausgabe „symcfg list“ als REMOTE aufgeführt werden. Data Infrastructure Insights sammelt nur Daten zu Geräten, die mit diesem Befehl als LOKAL angezeigt werden.
SMI-S-Protokoll	Protokoll für die Verbindung mit dem SMI-S-Provider. Zeigt auch den verwendeten Standardport an.
SMIS-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
SMI-S-Benutzername	Benutzername für den SMI-S Provider Host
SMI-S-Passwort	Benutzername für den SMI-S Provider Host
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen (standardmäßig 1000 Sekunden)
hoose 'exclude' oder 'include', um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Erfassen von Performancedaten einbezogen oder ausgeschlossen werden soll
Geräteliste Für Leistungsfilter	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Fehler: Die angeforderte Funktion ist derzeit nicht lizenziert	Installieren Sie die SYMAPI-Serverlizenz.
Fehler: Es wurden keine Geräte gefunden	Stellen Sie sicher, dass Symmetrix-Geräte vom Solutions Enabler-Server verwaltet werden: - Führen Sie die symcfg-Liste -V aus, um die Liste der konfigurierten Symmetrix-Geräte anzuzeigen.
Fehler: Ein angeforderter Netzwerkdienst wurde in der Servicedatei nicht gefunden	Stellen Sie sicher, dass der Solutions Enabler Service Name die netcnfg-Datei für Solutions Enabler definiert hat. Diese Datei befindet sich in der Regel unter SYMAPI\config\ in der Installation des Solutions Enabler-Clients.
Fehler: Die Handshake des Remote-Clients/Servers ist fehlgeschlagen	Überprüfen Sie die letzten speichersrvd.log*-Dateien auf dem Solutions Enabler-Host, den wir zu entdecken versuchen.
Fehler: Allgemeiner Name im Clientzertifikat ungültig	Bearbeiten Sie die Datei *Hosts* auf dem Solutions Enabler-Server, damit der Hostname der Acquisition Unit wie in der storsrvd.log auf dem Solutions Enabler-Server angegeben auf der IP-Adresse auflöst.
Fehler: Die Funktion konnte keinen Speicher abrufen	Stellen Sie sicher, dass genügend freier Speicherplatz im System vorhanden ist, um Solutions Enabler auszuführen
Fehler: Solutions Enabler konnte nicht alle erforderlichen Daten bereitstellen.	Untersuchen Sie den Integritätsstatus und das Lastprofil von Solutions Enabler
Fehler: • Der CLI-Befehl "symcfg list -tdev" gibt bei der Erfassung mit Solutions Enabler 7.x von einem Solutions Enabler Server 8.x. möglicherweise falsche Daten zurück • Der CLI-Befehl „symcfg list -srp“ kann bei der Erfassung mit Solutions Enabler 8.1.0 oder früher von einem Solutions Enabler Server 8.3 oder höher falsche Daten zurückgeben.	Vergewissern Sie sich, dass Sie die gleiche Solutions Enabler-Hauptversion verwenden

Problem:	Versuchen Sie dies:
Ich sehe Datenerhebungsfehler mit der Meldung "unbekannter Code"	Sie können diese Meldung sehen, wenn die Berechtigungen nicht in der Daemon-Konfigurationsdatei des Solutions Enabler Servers deklariert sind (siehe Anforderungen Oben). Hierbei wird davon ausgegangen, dass die Version Ihres SE-Clients mit Ihrer SE-Serverversion übereinstimmt. Dieser Fehler kann auch auftreten, wenn der Benutzer *cisys* (der Solutions Enabler-Befehle ausführt) nicht mit den erforderlichen Daemon-Berechtigungen in der Konfigurationsdatei /var/symapi/config/daemon_users konfiguriert wurde. Um dies zu beheben, bearbeiten Sie die Datei /var/symapi/config/daemon_users und stellen Sie sicher, dass der cisys-Benutzer über die für den storapid-Daemon angegebene <all>-Berechtigung verfügt. Beispiel: 14:11:25 # tail /var/symapi/config/daemon_users … Cisys storapid <all>

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Dell EMC VNX Block Storage (NaviCLI

Data Infrastructure Insights verwendet den Dell EMC VNX Block Storage (NaviSec) Data Collector (ehemals CLARiiON) zur Erfassung von Bestands- und Performance-Daten.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem EMC VNX Block Storage Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage	Storage
Storage Processor	Storage-Node
Dieser Pool, RAID-Gruppe	Storage-Pool
LUN	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

Zur Datenerfassung müssen die folgenden Anforderungen erfüllt sein:

- Eine IP-Adresse jedes VNX-Blockspeicherprozessors
- Schreibgeschützter Navisphere-Benutzername und Kennwort für die VNX-Block-Speicher-Arrays

- Naviseccli muss auf der Data Infrastructure Insights AU installiert sein
- Zugriffsvalidierung: Führen Sie NaviSecCLI von der Data Infrastructure Insights AU zu jedem Array mit dem Benutzernamen und Passwort aus.
- Port-Anforderungen: 80, 443
- Naviseccli Version sollte mit dem neuesten FLARE-Code auf Ihrem Array entsprechen
- Zur Performance muss die Statistik-Protokollierung aktiviert sein.

Syntax der Navisphere Befehlszeilenschnittstelle

NaviSECCLI.exe -h <IP-Adresse> -user <user> -password <password> -scope <scope,use 0 for global Scope> -Port <use 443 by default> Command

Konfiguration

Feld	Beschreibung
VNX Block Storage-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des VNX-Blockspeichers
Benutzername	Name, der für die Anmeldung beim VNX-Block-Speichergerät verwendet wird.
Passwort	Passwort zur Anmeldung beim VNX-Block-Speichergerät.
CLI-Pfad zu NaviSECCLI.exe	Vollständiger Pfad zum Ordner mit der ausführbaren Datei *naviseccli.exe*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Umfang	Der Umfang des sicheren Clients. Die Standardeinstellung ist Global.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: • Agent Wird Nicht Ausgeführt • Naviseccli konnte nicht gefunden werden • Fehler beim Ausführen eines Befehls	• Vergewissern Sie sich, dass Navisphere CLI auf der Cloud Insight Acquisition Unit installiert ist • Sie haben die Option „Secure Client verwenden“ im Assistenten für die Konfiguration des Datensammlers nicht ausgewählt und haben keine nicht sichere Version der Navisphere CLI installiert. • Vergewissern Sie sich, dass das Navisphere CLI-Installationsverzeichnis in der Data Collector-Konfiguration korrekt ist • Vergewissern Sie sich, dass die IP-Adresse des VNX-Blockspeichers in der Data Collector-Konfiguration korrekt ist: • Aus der Abteilung Data Infrastructure Insights Acquisition: ◦ Öffnen Sie eine CMD. ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Versuchen Sie, eine Verbindung mit dem VNX-Blockspeichergerät herzustellen, indem Sie „navicli -h} ip {getagent“ eingeben (ersetzen Sie die {ip} durch die tatsächliche IP).
Fehler: 4.29 emc235848 emc241018 getall konnte keine Host-Alias-Info analysieren	Dies wird wahrscheinlich durch eine FLARE 29-Fehlerproblematik der Host-Initiator-Datenbank auf dem Array selbst verursacht. Siehe EMC Knowledge Base Artikel: Emc235848, emc241018. Sie können auch prüfen https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Fehler: Die Meta-LUNs können nicht abgerufen werden. Fehler beim Ausführen von java -jar navicli.jar	• Ändern der Datensammlerkonfiguration zur Verwendung des sicheren Clients (empfohlen) • Installieren Sie navicli.jar im CLI-Pfad zu navicli.exe ODER NaviSECCLI.exe • Hinweis: navicli.jar ist ab EMC Navisphere Version 6.26 veraltet • Das navicli.jar steht möglicherweise auf http://powerlink.emc.com zur Verfügung
Fehler: Speicherpools melden keine Festplatten auf dem Serviceprozessor bei der konfigurierten IP-Adresse	Konfigurieren Sie den Datensammler mit beiden Service-Prozessor-IPs, getrennt durch Komma

Problem:	Versuchen Sie dies:
Fehler: Fehler bei nicht übereinstimmender Revision	• Dies wird normalerweise durch die Aktualisierung der Firmware auf dem VNX-Blockspeichergerät verursacht, aber nicht durch die Aktualisierung der Installation von NaviCLI.exe. Dies kann auch dadurch verursacht werden, dass verschiedene Geräte mit unterschiedlichen Firmwares installiert sind, aber nur eine CLI (mit einer anderen Firmware-Version). • Vergewissern Sie sich, dass sowohl das Gerät als auch der Host identische Versionen der Software ausführen: ◦ Öffnen Sie in der Data Infrastructure Insights Acquisition Unit ein Befehlszeilenfenster ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Stellen Sie eine Verbindung mit dem CLARiiON-Gerät her, indem Sie „navicli -h <ip> getagent“ eingeben. ◦ Achten Sie auf die Versionsnummer auf den ersten Zeilen. Beispiel: „Agent Rev: 6.16.2 (0.1)“ ◦ Suchen und vergleichen Sie die Version in der ersten Zeile. Beispiel: „Navisphere CLI Revision 6.07.00.04.07“
Fehler: Nicht Unterstützte Konfiguration - Keine Fibre-Channel-Ports	Das Gerät ist nicht mit Fibre-Channel-Ports konfiguriert. Aktuell werden nur FC-Konfigurationen unterstützt. Überprüfen Sie, ob diese Version/Firmware unterstützt wird.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

DATENSAMMLUNG FÜR DELL EMC VNX File (ehemals Celerra Unified Storage System

Dieser Datensammler erfasst Bestandsinformationen vom VNX File Storage System. Für die Konfiguration benötigt dieser Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem VNX File Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Celerra Network Server/Celerra Storage-Pool	Storage-Pool
File-System	Internes Volumen
Data Mover	Controller
Auf einem Data Mover gemountet	Dateifreigabe
CIFS- und NFS-Exporte	Share
Festplatten-Volume	Back-End LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren:

- Die IP-Adresse des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- SSH-Port 22

Konfiguration

Feld	Beschreibung
VNX-Datei-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Dateigeräts
Benutzername	Name, der zum Anmelden am VNX-Speichergerät verwendet wird
Passwort	Passwort zur Anmeldung beim VNX-Speichergerät

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Fortfahren nicht möglich, während die DART-Aktualisierung ausgeführt wird	Mögliche Lösung: Unterbrechen Sie den Datensammler, und warten Sie, bis die DART-Aktualisierung abgeschlossen ist, bevor Sie eine andere Erfassungsanforderung versuchen.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des Dell EMC VNX Unified Data Collectors

Für die Konfiguration benötigt der Dell EMC VNX Unified (SSH)-Datensammler die IP-Adresse der Control Station sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Festplattenordner	Festplattengruppe
File-System	Internes Volumen
Storage	Storage
Storage Processor	Storage-Node
Speicherpool, RAID-Gruppe	Storage-Pool
LUN	Datenmenge
Data Mover	Controller
Auf einem Data Mover gemountet	Dateifreigabe
CIFS- und NFS-Exporte	Share
Festplatten-Volume	Back-End LUN

Anforderungen

Sie benötigen Folgendes, um den VNX (SSH) Data Collector zu konfigurieren:

- VNX-IP-Adresse und Anmeldeinformationen an der Celerra Control Station.
- Nur-Lese-Benutzername und Kennwort.
- Der Datensammler kann NaviCLI/NaviSecCLI Befehle gegen das Backend-Array ausführen, das die DART OS NAS Heads verwendet

Konfiguration

Feld	Beschreibung
VNX-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname der VNX Control Station
Benutzername	Benutzername für die VNX Control Station
Passwort	Kennwort für die VNX Control Station

Erweiterte Konfigiration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Leistungsintervall (Sek.).	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des EMC VPLEX-Datensammlers

Dieser Datensammler erfasst Bestands- und Performancedaten von EMC VPLEX-Speichersystemen. Zur Konfiguration benötigt der Datensammler eine IP-Adresse des VPLEX-Servers und ein Domain-Konto auf Administratorebene.

> Die Performance-Erfassung von Data Infrastructure Insights aus VPLEX-Clustern erfordert, dass der Performance-Archivierungsservice betriebsbereit ist, um die CSV-Dateien und Protokolle zu füllen, die Data Infrastructure Insights über SCP-basierte Dateikopien abruft. NetApp hat beobachtet, dass viele Updates der VPLEX-Firmware-Upgrades/Management Station diese Funktionen nicht mehr betriebsbereit machen werden. Kunden, die ein solches Upgrade planen, fragen Dell/EMC möglicherweise proaktiv, ob ihr geplantes Upgrade diese Funktion nicht mehr funktionsfähig bleibt. Wenn ja, wie kann sie die IT neu aktivieren, um Lücken bei der Performance-Sichtbarkeit zu minimieren? Der VPLEX-Performance-Code von Cloud Insight bewertet bei jeder Umfrage, ob alle erwarteten Dateien vorhanden sind und ob sie ordnungsgemäß aktualisiert werden. Fehlen oder sind sie veraltet, protokolliert Data Infrastructure Insights Fehler bei der Performance-Erfassung.

Terminologie

Data Infrastructure Insightst erfasst die folgenden Bestandsinformationen aus dem VPLEX-Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Motor	Storage-Node
Gerät, Systemumfang	Back-End Storage-Pool
Virtual Volume	Datenmenge
Front-End-Port, Back-End-Port	Port
Verteiltes Gerät	Storage-Synchronisierung
Übersicht Storage	Volume Map, Volume Mask
Storage Volume	Back-End LUN

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
ITLS	Back-End-Pfad

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Eine IP-Adresse der VPLEX Management Console
- Domänenkonto auf Administratorebene für den VPLEX-Server
- Port 443 (HTTPS): Erfordert eine ausgehende Verbindung zum TCP-Port 443 auf der VPLEX-Managementstation.
- Für die Leistung können Sie den schreibgeschützten Benutzernamen und das Kennwort für den ssh/scp-Zugriff verwenden.
- Für die Leistung ist Port 22 erforderlich.

Konfiguration

Feld	Beschreibung
IP-Adresse der VPLEX Management Console	IP-Adresse oder vollqualifizierter Domänenname der VPLEX Management Console
Benutzername	Benutzername für VPLEX-CLI
Passwort	Passwort, das für die VPLEX-CLI verwendet wird
Remote-IP-Adresse für die Performance	Performance Remote IP-Adresse der VPLEX Management Console
Performance Remote User Name	Performance Remote-Benutzername der VPLEX Management Console
Kennwort Für Das Remote-Netzwerk Der Performance	Remote-Kennwort für die Performance der VPLEX Management Console

Erweiterte Konfiguration

Feld	Beschreibung
Kommunikations-Port	Für VPLEX-CLI verwendeter Port. Der Standardwert ist 443.
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.
Anzahl der Verbindungsversuche	Der Standardwert ist 3.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 600 Sekunden.
Anzahl Wiederholungen	Der Standardwert ist 2.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Leistung

Problem:	Versuchen Sie dies:
Fehler: VPLEX-Performance für Version unter 5.3 wird nicht unterstützt.	Aktualisieren Sie VPLEX auf 5.3 oder höher
Fehler: Es wurden nicht genügend Daten erfasst.	• Prüfen Sie den Zeitstempel der Sammlung in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend • Warten Sie länger
Fehler: Unbefristete Log-Dateien werden nicht aktualisiert.	Wenden Sie sich an den EMC Support, um die Aktualisierung der unbefristeten Protokolldateien zu aktivieren
Fehler: Das Abfrageintervall für die Performance ist zu groß.	Überprüfen Sie den Sammlungs-Zeitstempel in der Protokolldatei €{logfile} und ändern Sie das Abfrageintervall entsprechend
Fehler: Performance Remote IP-Adresse der VPLEX Management Console ist nicht konfiguriert.	Bearbeiten Sie die Datenquelle, um die Performance Remote IP-Adresse der VPLEX Management Console festzulegen.
Fehler: Keine Leistungsdaten vom Director gemeldet	• Überprüfen Sie, ob die System-Performance-Monitore ordnungsgemäß ausgeführt werden • Bitte wenden Sie sich an den EMC Support, um die Aktualisierung der Protokolldateien des Systems Performance Monitor zu ermöglichen

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Dell EMC XtremeIO-Datensammler

Der EMC XtremIO Data Collector erwirbt Bestands- und Performance-Daten vom EMC XtremIO Storage-System.

Anforderungen

Zum Konfigurieren des EMC XtremIO (HTTP) Datensammlers sind folgende Funktionen erforderlich:

- Die Host-Adresse des XtremIO Management Servers (XMS)
- Ein Konto mit Administratorrechten
- Zugriff auf Port 443 (HTTPS)

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem EMC XtremIO Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese

Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte (SSD)	Festplatte
Cluster	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Ziel-FC-Initiator	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

- Die XMS-Host-IP-Adresse des XtremIO Management Servers (XMS)
- Administratorbenutzername und -Passwort für den XtremIO

Konfiguration

Feld	Beschreibung
XMS-Host	IP-Adresse oder vollqualifizierter Domain-Name des XtremIO Management Servers
Benutzername	Benutzername für den XtremIO Management Server
Passwort	Passwort für den XtremIO Management Server

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port für die Verbindung mit dem XtremIO Management Server. Der Standardwert ist 443.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Fujitsu ETERNUS Datensammler

Der Fujitsu ETERNUS-Datensammler erfasst Bestandsdaten über administrativen Zugriff

auf das Speichersystem.

Terminologie

Data Infrastructure Insights bezieht die folgenden Bestandsinformationen aus dem Fujitsu ETERNUS Storage. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid-Gruppe	Storage-Pool
Standard-Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV), Flexible Tier Volume (FTV), Wide Striping Volume (WSV)	Datenmenge
Channel-Adapter	Controller

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diese Datensammlung möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Eine IP-Adresse des ETERNUS-Speichers, die nicht durch Komma getrennt werden kann
- Benutzername und Passwort der SSH-Administration
- Port 22
- Stellen Sie sicher, dass die Seitenscrollen deaktiviert ist (clienv-show-more-Scroll deaktiviert)

Konfiguration

Feld	Beschreibung
IP-Adresse des ETERNUS-Speichers	IP-Adresse des ETERNUS-Speichers
Benutzername	Benutzername für ETERNUS-Speicher
Passwort	Passwort für den ETERNUS-Speicher

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Fehler beim Abrufen von Daten“ mit Fehlermeldungen „Error Finding prompt CLI“ oder „Error Finding prompt at the end of Shell results“	Wahrscheinlich verursacht durch: Speichersystem hat Seite Scrollen aktiviert. Mögliche Lösung: * Versuchen Sie, den Bildlauf zu deaktivieren, indem Sie den folgenden Befehl ausführen: Clienv-show-more -scroll disable
„Verbindungsfehler“ mit Fehlermeldungen „konnte eine SSH-Verbindung zum Storage nicht instanziieren“ oder „Verbindung zum VirtualCenter konnte nicht hergestellt werden“	Wahrscheinliche Ursachen: * Falsche Anmeldeinformationen. * Falsche IP-Adresse. * Netzwerkproblem. * Storage kann ausgefallen oder nicht mehr reagiert werden. Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit dem Speicher über SSH Client zu kommunizieren.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp Google Compute Data Collector

Dieser Datensammler unterstützt Inventar- und Performance-Erfassung aus Google Compute Cloud-Plattformkonfigurationen. Dieser Sammler wird versuchen, alle Computing-Ressourcen in allen Projekten innerhalb einer Google-Organisation zu entdecken. Wenn Sie über mehrere Google-Unternehmen verfügen, die Sie mit Data Infrastructure Insights ermitteln möchten, möchten Sie pro Unternehmen einen Data Infrastructure Insights Collector implementieren.

Konfiguration

Feld	Beschreibung
Organisation-ID	Die Organisations-ID, die Sie mit diesem Sammler entdecken möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCP-Projekte nach IDs zu filtern	Wenn Sie einschränken möchten, welche Projektressourcen in Data Infrastructure Insights einfließen.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie in oder aus der Erkennung filtern möchten, hängt vom Wert des Werts "Ausschließen"… ab. Die Standardliste ist leer
Client-ID	Client-ID für die Konfiguration der Google Cloud Platform
Kopieren Sie den Inhalt Ihrer Google Credential-Datei hier	Kopieren Sie Ihre Google-Anmeldedaten für das Cloud-Plattform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Wählen Sie „Exclude“ oder „include“, um VMs nach Etiketten filtern zu können	Geben Sie an, ob VM’s by Labels beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn ‘include’ ausgewählt ist, kann das Feld Label Key nicht leer sein.
Bezeichnungsschlüssel und Werte, auf denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Label**, um die VMs (und zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte der Labels auf der VM entsprechen, einzuschließen bzw. auszuschließen. Etikettenschlüssel ist erforderlich, Etikettenwert ist optional. Wenn der Etikettenwert leer ist, wird die VM solange gefiltert, wie sie dem Etikettenschlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 1800 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

HP Enterprise

HP Enterprise Alletra 9000 / Primera Storage Datensammler

Data Infrastructure Insights verwendet den Datensammler HP Enterprise Alletra 9000 / HP Enterprise Primera (ehemals 3PAR) zur Ermittlung von Bestand und Leistung.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Feld	Beschreibung
Physisches Laufwerk	Festplatte
Storage-System	Storage
Controller-Node	Storage-Node
Gemeinsame Bereitstellungsgruppe	Storage-Pool
Virtual Volume	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- IP-Adresse oder FQDN des InServ-Clusters
- Für den Bestand können Sie den schreibgeschützten Benutzernamen und das Kennwort für den StoreServ Server verwenden
- Für eine bessere Leistung können Sie den Benutzernamen und das Kennwort für Lese- und Schreibvorgänge auf dem StoreServ Server verwenden
- Port-Anforderungen: 22 (Bestandsaufnahme), 5988 oder 5989 (Performance-Sammlung) [Hinweis: Leistung wird für StoreServ OS 3.x+ unterstützt]
- Bei der Erfassung der Performance bestätigen Sie, dass SMI-S durch Anmeldung am Array über SSH aktiviert ist.

Konfiguration

Feld	Beschreibung
Storage-IP-Adresse	Speicher-IP-Adresse oder vollqualifizierter Domain-Name des StoreServ-Clusters
Benutzername	Benutzername für den StoreServ Server
Passwort	Passwort, das für den StoreServ Server verwendet wird
SMI-S-Benutzername	Benutzername für den SMI-S Provider Host
SMI-S-Passwort	Passwort, das für den SMI-S Provider-Host verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
SMI-S-Konnektivität	Protokoll für die Verbindung mit dem SMI-S-Provider
SMI-S-Standardport überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport von SMI-S Connectivity. Andernfalls geben Sie den zu verwendenden Verbindungsport ein
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Der Befehl „showsys“ gibt kein Ergebnis zurück.	Führen Sie „showsys“ und „showversion -A“ über die Befehlszeile aus und prüfen Sie, ob die Version vom Array unterstützt wird.

Leistung

Problem:	Versuchen Sie dies:
Verbindung oder Anmeldung fehlgeschlagen. Fehler bei der Initialisierung des Providers.	Ein Name eines rein numerischen Arrays kann Probleme mit dem SMI-S-Server verursachen. Versuchen Sie, den Namen des Arrays zu ändern.
Der konfigurierte SMI-S-Benutzer verfügt über keine Domäne	Gewähren Sie dem konfigurierten SMI-S-Benutzer entsprechende Domänenberechtigungen
Data Infrastructure Insights gibt an, dass keine Verbindung zum SMI-S-Service hergestellt bzw. angemeldet werden kann.	Vergewissern Sie sich, dass es keine Firewall zwischen der CI AU und dem Array gibt, die die CI AU daran versperren würde, TCP-Verbindungen zu 5988 oder 5989 zu machen. Sobald das geschehen ist, und wenn Sie bestätigt haben, dass es keine Firewall gibt, sollten Sie SSH auf das Array, und verwenden Sie den "showcim" Befehl zu bestätigen. Überprüfen Sie, dass: * Dienst aktiviert ist * HTTPS-Port sollte 5989 sein. Wenn alle diese sind, können Sie versuchen, „stopcim“ und dann ein „startcim“, um den CIM neu zu starten (d.h. SMI-S-Service).

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

HP Enterprise Command View-Datensammler

Der HP Enterprise Command View Advanced Edition Data Collector unterstützt die Erkennung von XP- und P9500-Arrays über den Command View Advanced Edition-Server (CVAE). Data Infrastructure Insights kommuniziert über die standardmäßige Command View API mit CVAE, um Inventar- und Performance-Daten zu erfassen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem HP Enterprise Command View-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
PDEV	Festplatte
Journalpool	Festplattengruppe
Storage Array Durchführt	Storage
Port Controller	Storage-Node
Array-Gruppe, DP-Pool	Storage-Pool

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Logische Einheit, LDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse des CVAE-Servers
- Schreibgeschützter Benutzername und Kennwort für die CVAE-Software und die Peer-Rechte
- Port-Anforderung: 2001

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.
  - Das Export-Tool (Export.exe) muss in die Data Infrastructure Insights AU kopiert und an einen Speicherort extrahiert werden. Stellen Sie unter CI Linux aus sicher, dass „cisys“ Berechtigungen gelesen und ausgeführt hat.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- AMS-Leistung:
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) wird auf der Data Infrastructure Insights AU installiert.
- Netzwerkanforderungen
  - Die Exportwerkzeuge sind Java-basiert und verwenden RMI, um mit dem Array zu sprechen. Diese Tools sind möglicherweise nicht für die Firewall geeignet, da sie auf jedem Aufruf dynamisch die Quell- und Ziel-TCP-Ports aushandeln können. Außerdem verhalten sich die Export-Tools der verschiedenen Modell-Arrays im Netzwerk möglicherweise unterschiedlich - Fragen Sie HPE nach den Anforderungen Ihres Modells

Konfiguration

Feld	Beschreibung
Command View Server	IP-Adresse oder vollqualifizierter Domain-Name des Command View Servers
Benutzername	Benutzername für den Command View Server.
Passwort	Passwort, das für den Command View-Server verwendet wird.

Feld	Beschreibung
GERÄTE – VSP G1000 (R800), VSP (R700), HUS VM (HM700) UND USP-SPEICHER	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit Export Utility JAR-Dateien
SNM2Geräte - WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array's IP: IP address of the Storage * Storage Navigator CLI Pfad: SNM2 CLI Pfad * Konto Authentifizierung gültig: Wählen Sie gültige Konto Authentifizierung * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für Leistung	Andere Leistungsoptionen überschreiben
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers
Tuning-Manager-Port	Port, der für Tuning Manager verwendet wird
Benutzername Für Tuning Manager	Benutzername für Tuning Manager
Kennwort Für Tuning-Manager	Passwort für Tuning Manager

Hinweis: Bei HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

Erweiterte Konfiguration

Feld	Beschreibung
Command View Server Port	Port, der für den Command View Server verwendet wird
HTTPS aktiviert	Wählen Sie diese Option aus, um HTTPS zu aktivieren
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Schließen Sie Geräte aus oder schließen Sie sie ein	Kommagetrennte Liste der Geräte-IDs oder Array-Namen, die einbezogen oder ausgeschlossen werden sollen
Abfrage-Host-Manager	Wählen Sie diese Option aus, um den Hostmanager abzufragen
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Benutzer hat nicht genügend Berechtigung	Verwenden Sie ein anderes Benutzerkonto, das über mehr Berechtigungen verfügt oder die Berechtigung des Benutzerkontos, das im Datensammler konfiguriert ist, erhöht
Fehler: Speicherliste ist leer. Entweder sind Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto, das mehr Berechtigungen hat, oder erhöhen Sie die Berechtigung des Benutzerkontos
Fehler: HDS Speicher-Array wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HP CommandView AE nicht aktualisiert wird.

Leistung

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Exportdienstprogramm auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Data Collectors korrekt ist * Öffnen Sie einen CMD und das Kennwort in der Konfiguration des Data Collectors * Bestätigen Sie, dass die Export Utility-Version mit der Speicher-Microcode-Version kompatibel ist * aus der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD - Aufforderung zur Installation mit dem folgenden Ordner konfigurieren: runWin.bat
Fehler: Export Tool-Anmeldung für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt ist * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.

Problem:	Versuchen Sie dies:
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Exportdienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird nicht von Speicher-Navigator Modular CLI unterstützt	* Nur unterstützte Storage-Arrays konfigurieren. * Verwenden Sie „Filter Device List“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicher-Array nicht gemeldet von Inventory * Konfigurationsfehler:Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Exportdienstprogramms. * Prüfen Sie, ob Speicher-Array in Frage in Command View Server konfiguriert ist * Festlegen des Performance-Abfrageintervalls als mehrere 60 Sekunden.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen von auPerform Befehl * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Speicherort in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Data Collectors korrekt ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Version kompatibel ist mit Microcode-Version des Speicher-Arrays konfiguriert im Data Collector * von der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD-Eingabeaufforderung und führen Sie den folgenden Befehl aus:
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im Command View-Server konfiguriert ist
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern * Ausführen des Befehls „set=STONAVM_HOME=.“ * Ausführen des Befehls „auunitref“ * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP * enthält. Wenn die Ausgabe nicht die Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern - Befehl „set=STONAVM_HOME= ausführen.“ - Ausführen des Befehls „auunitaddAuto -ip €{ip}“. Ersetzen Sie{ip} durch echtes IP

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

HPE Alletra 6000 Datensammler

Der HP Enterprise Alletra 6000 (vormals Nimble) Datensammler unterstützt Bestands- und Performancedaten von Alletra 6000 Storage Arrays.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dieser Sammlung. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Array Erledigen	Storage
Festplatte	Festplatte
Datenmenge	Datenmenge
Pool	Storage-Pool
Initiator	Storage-Host-Alias
Controller	Storage-Node
Fibre Channel-Schnittstelle	Controller

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zum Erfassen von Bestands- und Konfigurationsdaten aus dem Speicher-Array müssen Sie Folgendes haben:

- Das Array muss installiert und konfiguriert sein und über den Client über seinen vollständig qualifizierten Domänennamen (FQDN) oder die Array-Management-IP-Adresse erreichbar sein.
- Auf dem Array muss NimbleOS 2.3.x oder höher ausgeführt werden.
- Sie müssen einen gültigen Benutzernamen und ein Kennwort für das Array mit der Rolle „Operator“ besitzen. Die „Gast“-Rolle verfügt nicht über ausreichenden Zugriff, um Initiator-Konfigurationen zu verstehen.
- Port 5392 muss auf dem Array geöffnet sein.

Zum Erfassen von Performance-Daten aus dem Speicher-Array müssen Sie Folgendes haben:

- Auf dem Array muss NimbleOS 4.0.0 oder höher ausgeführt werden
- Für das Array müssen Volumes konfiguriert sein. Die einzige Performance-API, die NimbleOS bietet, gilt für Volumes. Alle Statistiken zu Data Infrastructure Insights Berichten werden aus den Statistiken zu Volumes abgeleitet

Konfiguration

Feld	Beschreibung
Array-Management-IP-Adresse	Vollständig qualifizierter Domain-Name (FQDN) oder Array-Management-IP-Adresse.
Benutzername	Benutzername für das Array
Passwort	Kennwort für das Array

Erweiterte Konfiguration

Feld	Beschreibung
Port	Der von Nimble REST API verwendete Port. Der Standardwert ist 5392.

Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.

Hinweis: Das Standard-Performance-Abfrageintervall beträgt 300 Sekunden und kann nicht geändert werden. Dies ist das einzige von HPE Alletra 6000 unterstützte Intervall.

Hitachi Data Systems (Hds)

Datensammler der Hitachi Vantara Command Suite

Der Datensammler der Hitachi Vantara Command Suite unterstützt den HiCommand Device Manager-Server. Data Infrastructure Insights kommuniziert über die standardmäßige HiCommand API mit dem HiCommand Device Manager-Server.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Datensammler der Hitachi Vantara Command Suite. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
PDEV	Festplatte
Journalpool	Festplattengruppe
Storage Array Durchführt	Storage
Port Controller	Storage-Node
Array-Gruppe, HDS Pool	Storage-Pool
Logische Einheit, LDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Storage

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name – kommt direkt aus dem Attribut „Name“ des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- Modell - kommt direkt aus dem „arrayType“-Attribut des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- Anbieter – HDS
- Family - kommt direkt aus dem Attribut „arrayFamily“ des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- IP – hierbei handelt es sich um die Management-IP-Adresse des Arrays, keine vollständige Liste aller IP-Adressen im Array

- Rohkapazität: Ein base2-Wert, der die Summe der Gesamtkapazität aller Festplatten in diesem System darstellt, unabhängig von der Festplattenrolle.

Storage-Pool

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Pool Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Typ: Der Wert hier ist einer von:
  - RESERVIERT – Wenn dieser Pool für andere Zwecke als Datenvolumes, i.e, Journaling, Snapshots bestimmt ist
  - Thin Provisioning – wenn es sich um einen HDP-Pool handelt
  - RAID-Gruppe – aus ein paar Gründen werden Sie diese wahrscheinlich nicht sehen:

    Data Infrastructure Insights ist ein starker Standpunkt, um zu vermeiden, dass bei allen Kosten eine doppelte Kapazität gezählt wird. Auf HDS muss man normalerweise RAID-Gruppen von Festplatten erstellen, Pool-Volumes auf diesen RAID-Gruppen erstellen und Pools (oft HDP, könnte aber besonderer Zweck sein) aus diesen Pool Volumes erstellen. Wenn Data Infrastructure Insights sowohl die zugrunde liegenden RAID-Gruppen wie auch die Pools meldet, würde die Summe ihrer Rohkapazität die Summe der Festplatten erheblich übersteigen.

  Stattdessen verkleinert der Datensammler HDS Command Suite von Data Infrastructure Insights die Größe von RAID-Gruppen willkürlich nach der Kapazität von Pool Volumes. Dies kann dazu führen, dass Data Infrastructure Insights die RAID-Gruppe überhaupt nicht meldet. Darüber hinaus werden alle resultierenden RAID-Gruppen so gekennzeichnet, dass sie in der Data Infrastructure Insights WebUI nicht sichtbar sind, aber sie fließen in das Data Warehouse (DWH) von Data Infrastructure Insights ein. Der Zweck dieser Entscheidungen ist es, UI-Gerinnung für Dinge zu vermeiden, die den meisten Benutzern egal sind – wenn Ihr HDS-Array RAID-Gruppen mit 50 MB frei hat, können Sie diesen freien Speicherplatz wahrscheinlich nicht für ein sinnvolles Ergebnis nutzen.

- Node – k. A., da HDS Pools nicht an einen bestimmten Node gebunden sind
- Redundanz: Der RAID-Level des Pools. Möglicherweise mehrere Werte für einen HDP-Pool, die aus mehreren RAID-Typen bestehen
- Kapazität % - der Prozentsatz, der für die Datenverwendung des Pools verwendet wird, wobei die verwendete GB und die gesamte logische GB-Größe des Pools verwendet werden
- Überzuviel Kapazität - ein abgeleiteter Wert, der angibt, „die logische Kapazität dieses Pools wird durch diesen Prozentsatz überzeichnet, aufgrund der Summe der logischen Volumes, die die logische Kapazität des Pools um diesen Prozentsatz überschreiten“
- Snapshot - zeigt die Kapazität an, die für die Snapshot-Nutzung in diesem Pool reserviert ist

Storage-Node

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf den HDS Storage Node Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name: Der Name des Front-End-Director (FED) oder Channel-Adapters auf monolithischen Arrays oder der Name des Controllers auf einem modularen Array. Ein bestimmtes HDS-Array verfügt über zwei oder mehr Storage-Nodes
- Volumes – die Volume-Tabelle zeigt jedes Volume an, das einem beliebigen Port dieses Speicherknoten zugeordnet ist

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse des HiCommand Device Manager-Servers
- Schreibgeschützter Benutzername und Kennwort für die HiCommand Device Manager-Software und Peer-Berechtigungen
- Port-Anforderungen: 2001 (http) oder 2443 (https)
- Melden Sie sich mit Benutzernamen und Kennwort bei der HiCommand Device Manager-Software an
- Überprüfen Sie den Zugriff auf HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/Service/StorageManager

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.
  - Das Export-Tool (Export.exe) muss in die Data Infrastructure Insights AU kopiert werden.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- AMS-Leistung:
  - NetApp empfiehlt dringend, ein dediziertes Dienstkonto auf AMS-Arrays zu erstellen, damit Dateninfrastrukturdaten zum Abrufen von Leistungsdaten verwendet werden können. Storage Navigator ermöglicht nur ein Benutzerkonto, das gleichzeitig mit dem Array angemeldet ist. Wenn Data Infrastructure Insights dasselbe Benutzerkonto wie Verwaltungsskripte oder HiCommand verwendet, kann es dazu kommen, dass Data Infrastructure Insights, Verwaltungsskripte oder HiCommand aufgrund der Beschränkung der gleichzeitigen Anmeldung eines Benutzerkontos nicht mit dem Array kommunizieren kann
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Data Infrastructure Insights AU installiert werden.

Konfiguration

Feld	Beschreibung
HiCommand Server	IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers
Benutzername	Benutzername für den HiCommand Device Manager-Server.
Passwort	Passwort, das für den HiCommand Device Manager-Server verwendet wird.

Feld	Beschreibung
GERÄTE – VSP G1000 (R800), VSP (R700), HUS VM (HM700) UND USP-SPEICHER	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit Export Utility JAR-Dateien
SNM2Geräte - WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array's IP: IP address of the Storage * Storage Navigator CLI Pfad: SNM2 CLI Pfad * Konto Authentifizierung gültig: Wählen Sie gültige Konto Authentifizierung * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für Leistung	Andere Leistungsoptionen überschreiben
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers
Tuning Manager-Port Überschreiben	Wenn leer, verwenden Sie den Standardport im Feld Tuning Manager für Performance auswählen. Geben Sie andernfalls den zu verwendenden Port ein
Benutzername Für Tuning Manager	Benutzername für Tuning Manager
Kennwort Für Tuning-Manager	Passwort für Tuning Manager

Hinweis: Bei HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an
HiCommand Server-Port	Port, der für den HiCommand Device Manager verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Geräteliste filtern	Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
Ausfuhrzeitlimit in Sekunden	Zeitüberschreitung beim Exportieren der Dienstprogrammfunktion. Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Benutzer hat nicht genügend Berechtigung	Verwenden Sie ein anderes Benutzerkonto, das über mehr Berechtigungen verfügt oder die Berechtigung des Benutzerkontos, das im Datensammler konfiguriert ist, erhöht
Fehler: Speicherliste ist leer. Entweder sind Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto, das mehr Berechtigungen hat, oder erhöhen Sie die Berechtigung des Benutzerkontos
Fehler: HDS Speicher-Array wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array nicht in HDS HiCommand aktualisiert wird.

Leistung

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Exportdienstprogramm auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Data Collectors korrekt ist * Öffnen Sie einen CMD und das Kennwort in der Konfiguration des Data Collectors * Bestätigen Sie, dass die Export Utility-Version mit der Speicher-Microcode-Version kompatibel ist * aus der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD - Aufforderung zur Installation mit dem folgenden Ordner konfigurieren: runWin.bat
Fehler: Export Tool-Anmeldung für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt ist * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.

Problem:	Versuchen Sie dies:
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Exportdienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird nicht von Speicher-Navigator Modular CLI unterstützt	* Nur unterstützte Storage-Arrays konfigurieren. * Verwenden Sie „Filter Device List“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicher-Array nicht gemeldet von Inventory * Konfigurationsfehler:Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Exportdienstprogramms. * Prüfen Sie, ob Speicher-Array in Frage in HiCommand Server konfiguriert ist * Festlegen des Performance-Abfrageintervalls als mehrere 60 Sekunden.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen von auPerform Befehl * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Speicherort in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Data Collectors korrekt ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Version kompatibel ist mit Microcode-Version des Speicher-Arrays konfiguriert im Data Collector * von der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD-Eingabeaufforderung und führen Sie den folgenden Befehl aus:
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im HiCommand-Server konfiguriert ist
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Öffnen Sie Eingabeaufforderung und ändern Sie das Verzeichnis auf den konfigurierten Pfad * Führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP enthält * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis auf den konfigurierten Pfad - Führen Sie den Befehl „set=STONAVM_HOME=“ aus. - Führen Sie den Befehl „auunitaddauto -ip <ip>“ aus. Ersetzen Sie <ip> durch die richtige IP.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfiguration des Hitachi Vantara NAS Data Collector

Der Hitachi Vantara NAS Data Collector ist ein Bestands- und Konfigurationsdatensammler, der die Erkennung von HDS NAS-Clustern unterstützt. Data Infrastructure Insights unterstützt die Erkennung von NFS- und CIFS-Freigaben, Filesystemen (interne Volumes) und Spanns (Storage-Pools).

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem HNAS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Ebene	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Span	Storage-Pool
Systemlaufwerk	Back-End Lun
File System	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort - Berechtigungsebene: Supervisor
- Hinweis: Dieser Datensammler ist SSH-basiert, also muss die AU, die auf dem HNAS selbst SSH-Sitzungen auf TCP 22 oder auf der Systemverwaltungseinheit (SMU) initiieren können, mit der das Cluster verbunden ist.

Konfiguration

Feld	Beschreibung
HNAS-Host	IP-Adresse oder vollqualifizierter Domain-Name des HNAS Management Host
Benutzername	Benutzername für HNAS CLI
Passwort	Passwort, das für HNAS-CLI verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 30 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Fehler beim Verbinden“ mit Fehlermeldungen „Fehler beim Einrichten des Shell-Kanals:“ oder „Fehler beim Öffnen des Shell-Kanals“	Wahrscheinlich verursacht durch Probleme mit der Netzwerkverbindung oder SSH ist falsch konfiguriert. Bestätigen Sie die Verbindung mit dem alternativen SSH-Client
„Timeout“ oder „Fehler beim Abrufen von Daten“ mit Fehlermeldungen „Befehl: XXX hat Timeout.“	* Versuchen Sie den Befehl mit dem alternativen SSH-Client * Erhöhen Sie die Zeitüberschreitung
„Fehler beim Verbindungsaufbau“ oder „Ungültige Anmeldeinformationen“ mit Fehlermeldungen „konnte nicht mit dem Gerät kommunizieren:“	* IP-Adresse prüfen * Benutzername und Passwort überprüfen * Verbindung mit alternativem SSH-Client bestätigen

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Hitachi Ops Center

Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Bestands- und Performancedaten mehrerer Speichergeräte zuzugreifen. Eine Bestandsaufnahme und Kapazitätserkennung muss in Ihrer Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Zur Performance-Erfassung muss zusätzlich „Analyzer“ implementiert sein.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Systeme	Storage
Datenmenge	Datenmenge
Paritätsgruppen	Speicherpool (RAID), Festplattengruppen
Festplatte	Festplatte
Storage-Pool	Speicherpool (Thin, SNAP)
Externe Paritätsgruppen	Speicherpool (Backend), Festplattengruppen
Port	Storage-Node → Controller-Node →-Port
Host-Gruppen	Volume-Zuordnung und -Maskierung
Volume-Paare	Storage-Synchronisierung

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse oder Hostname des Ops Center-Servers, der die „Common Services“-Komponente hostet
- Root/sysadmin Benutzerkonto und Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center Komponenten gehostet werden. HDS hat KEINE REST-API-Unterstützung für LDAP/SSO-Benutzer bis Ops Center 10.8+ implementiert

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

Das HDS Ops Center „Analyzer“-Modul muss installiert sein Storage Arrays müssen das Ops Center-Modul „Analyzer“ speisen

Konfiguration

Feld	Beschreibung
Hitachi Ops Center-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, der die Komponente „Allgemeine Dienste“ hostet
Benutzername	Benutzername für den Ops-Center-Server.
Passwort	Passwort, das für den Ops-Center-Server verwendet wird.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Port 443) ist der Standard
TCP-Port überschreiben	Geben Sie den zu verwendenden Port an, wenn nicht der Standardport
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Geräteliste filtern	Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Infiniat InfiniBox Datensammler

Der Datensammler Infinibei InfiniBox (HTTP) wird verwendet, um Inventarinformationen vom Infiniat InfiniBox-Speichersystem zu sammeln.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Infinidat Infinibox Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Knoten	Controller
Dateisystem	Internes Volumen
Dateisystem	Dateifreigabe
Dateisystem-Exporte	Share

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers.

- IP-Adresse oder FQDN des InfiniBox-Managementknoten
- Admin-Benutzer-ID und Passwort
- Port 443 über REST API

Konfiguration

Feld	Beschreibung
InfiniBox Host	IP-Adresse oder vollqualifizierter Domainname des InfiniBox Management Node
Benutzername	Benutzername für InfiniBox Management Node
Passwort	Passwort für den InfiniBox Management-Knoten

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port zur Verbindung mit InfiniBox-Server. Der Standardwert ist 443.
Abfrageintervall Für Bestand	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Huawei OceanStor Datensammler

Data Infrastructure Insights nutzt den Huawei OceanStor (REST/HTTPS) Datensammler zur Ermittlung von Inventar und Leistung für Huawei OceanStor und OceanStor Dorado Speicher.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
File-System	Internes Volumen
Controller	Storage-Node
FC-Port (zugeordnet)	Volume-Zuordnung
Host FC Initiator (zugeordnet)	Volume-Maske
NFS/CIFS-Freigabe	Share
ISCSI-Link-Ziel	ISCSI-Ziel-Node
ISCSI-Link-Initiator	ISCSI-Initiator-Node
Festplatte	Festplatte
LUN	Datenmenge

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Anforderungen erforderlich:

- IP-Adresse des Geräts
- Anmeldeinformationen für den Zugriff auf OceanStor Geräte-Manager
- Port 8088 muss verfügbar sein

Konfiguration

Feld	Beschreibung
OceanStor Host-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des OceanStor Device Managers
Benutzername	Name, der zur Anmeldung beim OceanStor Device Manager verwendet wird
Passwort	Passwort zur Anmeldung beim OceanStor Device Manager

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port zur Verbindung mit dem OceanStor Device Manager. Der Standardwert ist 8088.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.).	Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

IBM

IBM Cleversafe Datensammler

Data Infrastructure Insights nutzt diesen Datensammler, um Bestands- und Leistungsdaten für IBM Cleversafe-Speichersysteme zu ermitteln.

IBM Cleversafe wird mit einer anderen Raw TB zu Managed Unit Rate gemessen. Alle 40 TB unformatierte IBM Cleversafe Kapazität wird als 1 geladen "Verwaltete Einheit (ME)".

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem IBM Cleversafe Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Manager-IP oder Host-Name	IP-Adresse oder Hostname des Management-Node
Benutzername	Benutzername für das Benutzerkonto mit Superuser- oder Systemadministrator-Rolle
Passwort	Kennwort für das Benutzerkonto mit Superuser- oder Systemadministrator-Rolle

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen
HTTP-Verbindungszeitlimit (Sek.)	HTTP-Zeitüberschreitung in Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

IBM CS Datensammler

Data Infrastructure Insights nutzt diesen Datensammler zur Ermittlung von Bestands- und Leistungsdaten für IBM CS-Speichersysteme.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem IBM CS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem IBM CS-Array verwendet wird. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Abfrageintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler der IBM System Storage DS8000-Serie

Der IBM DS (CLI) Datensammler unterstützt die Erfassung von Bestands- und Performancedaten für DS6xxx- und DS8xxx-Geräte.

DS3xxx-, DS4xxx- und DS5xxx-Geräte werden vom unterstütztNetApp E-Series Datensammler". Unterstützte Modelle und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem IBM DS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplattenmodul	Festplatte
Storage-Bild	Storage
Extent-Pool	Storage-Node
Festes Block-Volume	Datenmenge
Host FC Initiator (zugeordnet)	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen möglicherweise nicht alle Fälle für diese Datensammlung dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren:

- IP-Adresse jedes DS-Arrays
- Schreibgeschützter Benutzername und Kennwort auf jedem DS-Array
- Software von Drittanbietern, die auf der Data Infrastructure Insights AU installiert ist: IBM *dscli*
- Zugriffsvalidierung: Führen Sie die Befehle *dscli* mit dem Benutzernamen und Passwort aus
- Port-Anforderungen: 80, 443 und 1750

Konfiguration

Feld	Beschreibung
DS-Speicher	IP-Adresse oder vollqualifizierter Domain-Name des DS-Geräts
Benutzername	Benutzername für die DS-CLI
Passwort	Kennwort für die DS-CLI
Dscli ausführbare Datei-Pfad	Vollständiger Pfad zur ausführbaren Datei *dscli*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen (min). Der Standardwert ist 40.
Anzeigename Für Speicher	Name des IBM DS-Speicherarrays
Inventory Exclude Devices	Kommagetrennte Liste von Geräteseriennummer, die von der Bestandserfassung ausgeschlossen werden sollen
Leistungsintervall (Sek.)	Der Standardwert ist 300.
Typ Des Leistungsfilters	Enthalten: Daten, die nur von Geräten in der Liste erfasst werden. Ausschließen: Es werden keine Daten von diesen Geräten erfasst
Geräteliste Für Leistungsfilter	Kommagetrennte Liste der Geräte-IDs, die die Leistungssammlung einschließen oder ausschließen sollen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler mit CMUC00192E, CMUC00191E oder CMUC00190E	* Eingabe von Anmeldeinformationen und IP-Adresse überprüfen. * Versuchen Sie, mit dem Array über die Web-Management-Konsole https://<ip>:8452/DS8000/Console zu kommunizieren. Ersetzen Sie <ip> durch konfigurierte IP-Adresse für den Data Collector.
Fehler: * Programm kann nicht ausgeführt werden * Fehler beim Ausführen des Befehls	* Aus Data Infrastructure Insights Acquisition Unit Öffnen Sie eine CMD * Open CLI.CFG-Datei in CLI's Home dir/lib und überprüfen Sie die Eigenschaft Java_INSTALL, bearbeiten Sie den Wert, der Ihrer Umgebung entspricht * Java-Version auf diesem Rechner anzeigen, indem Sie "java -Version" eingeben * Ping die IP-Adresse des IBM-Speichergeräts, das im CLI-Befehl ausgegeben wurde. * Wenn alle oben genannten gut funktioniert haben, dann führen Sie manuell einen CLI-Befehl aus

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des IBM PowerVM-Datensammlers

Der IBM PowerVM (SSH) Datensammler wird verwendet, um Informationen über virtuelle Partitionen zu sammeln, die auf IBM POWER Hardware-Instanzen ausgeführt werden, die von einer Hardware Management Console (HMC) verwaltet werden.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen von den virtuellen Partitionen, die auf IBM POWER Hardware-Instanzen ausgeführt werden. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Hdisk	Virtuelles Laufwerk
Managed System	Host
LPAR, VIO Server	Virtual Machine
Volume-Gruppe	Datastore
Physisches Volume	LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen die folgenden Anforderungen erfüllt sein:

- IP-Adresse der Hardware Management Console (HMC)

- Benutzername und Passwort, die Zugriff auf die Hardware Management Console (HMC) über SSH ermöglichen
- Port-Anforderung SSH-22
- Zeigen Sie Berechtigungen auf allen Verwaltungssystemen und Sicherheitsdomänen logischer Partitionen an

  Der Benutzer muss darüber hinaus über die Berechtigung View für HMC-Konfigurationen und die Möglichkeit verfügen, VPD-Informationen für die Sicherheitsgruppierung der HMC-Konsole zu sammeln. Der Benutzer muss außerdem den Zugriff auf den virtuellen IO-Server-Befehl unter der Sicherheitsgruppierung der logischen Partition zulassen. Es ist eine bewährte Vorgehensweise, von einer Rolle eines Bedieners zu beginnen und dann alle Rollen zu entfernen. Schreibgeschützte Benutzer auf dem HMC haben keine Berechtigungen zum Ausführen von Proxed-Befehlen auf AIX-Hosts.

- Die Best Practice von IBM besteht darin, dass die Geräte von zwei oder mehr HMCs überwacht werden. Beachten Sie, dass dies dazu führen kann, dass OnCommand Insight doppelte Geräte meldet. Daher wird dringend empfohlen, redundante Geräte zur Liste „Geräte ausschließen“ in der erweiterten Konfiguration für diesen Datensammler hinzuzufügen.

Konfiguration

Feld	Beschreibung
IP-Adresse für Hardware Management Console (HMC)	IP-Adresse oder vollqualifizierter Domänenname der PowerVM Hardware Management Console
HMC-Benutzer	Benutzername für die Hardware Management Console
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.
SSH-Port	Port, der für SSH zu PowerVM verwendet wird
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird
Anzahl Wiederholungen	Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme
Geräte Ausschließen	Kommagetrennte Liste von Geräte-IDs oder zu schließenden Anzeigenamen

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des IBM SAN Volume Controller-Datensammlers

Der IBM SAN Volume Controller (SVC)-Datensammler sammelt Bestands- und Performancedaten mithilfe von SSH und unterstützt eine Vielzahl von Geräten, auf denen das SVC-Betriebssystem ausgeführt wird.

Die Liste der unterstützten Geräte umfasst Modelle wie SVC, v7000, v5000 und v3700. Unterstützte Modelle und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem IBM SVC-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
Mdisk-Gruppe	Storage-Pool
Vdisk	Datenmenge
Mdisk	Back-End-LUNs und -Pfade

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

- IP-Adresse jedes SVC-Clusters
- Port 22 verfügbar
- Schreibgeschützter Benutzername und Kennwort

Performance-Anforderungen Erfüllt

- SVC-Konsole, die für jeden SVC-Cluster obligatorisch und für das Foundation-Paket für die SVC-Erkennung erforderlich ist
- Mit den Anmeldedaten ist nur Administratorzugriff erforderlich, um Performance-Dateien von Cluster-Nodes auf den Konfigurations-Node zu kopieren.
- Aktivieren Sie die Datensammlung, indem Sie über SSH eine Verbindung zum SVC-Cluster herstellen und ausführen: *Svctask startstats -Interval 1*

  Hinweis: Alternativ können Sie die Datenerfassung über die SVC Management-Benutzeroberfläche aktivieren.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adressen	IP-Adressen oder vollqualifizierte Domain-Namen des SVC-Speichers
Benutzername Des Inventurbenutzers	Benutzername für die SVC-CLI
Inventurpasswort	Passwort für die SVC-CLI

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.
Um dumpte Statistikdateien zu bereinigen	Aktivieren Sie dieses Kontrollkästchen, um heruntergelegte Statistikdateien zu bereinigen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurations-Node ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurations-Node ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfiguration des IBM XIV/A9000 Datensammlers

Der Datensammler IBM XIV und A9000 (CLI) verwendet die XIV-Befehlszeilenschnittstelle, um Bestandsdaten zu sammeln, während die Performance erfasst wird, indem SMI-S-Aufrufe zum XIV/A9000 Array ausführt, auf dem ein SMI-S-Provider über Port 7778 ausgeführt wird.

Terminologie

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage-System	Storage

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Datenmenge	Datenmenge

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen die folgenden Anforderungen erfüllt sein:

- Port-Anforderung: TCP-Port 7778
- Schreibgeschützter Benutzername und Kennwort
- Das XIV CLI muss auf der AU installiert sein

Performance-Anforderungen erfüllt

Im Folgenden sind Anforderungen für die Performance-Erfassung aufgeführt:

- SMI-S Agent 1.4 oder höher
- SMI-S-kompatibler CIMService auf Array. Bei den meisten XIV Arrays ist standardmäßig ein Cimserver installiert.
- Für den Cimserver muss eine Benutzeranmeldung bereitgestellt werden. Die Anmeldung muss vollständigen Lesezugriff auf die Arraykonfiguration und -Eigenschaften haben.
- SMI-S-Namespace. Der Standardwert ist root/ibm. Dies ist im Cimserver konfigurierbar.
- Port-Anforderungen: 5988 für HTTP, 5989 für HTTPS.
- Unter folgendem Link finden Sie Informationen zur Erstellung eines Kontos für die SMI-S-Performance-Sammlung: https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Konfiguration

Feld	Beschreibung
XIV IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des XIV Storage
Benutzername	Benutzername für den XIV Storage
Passwort	Passwort für den XIV-Speicher
Vollständiger Pfad zu XIV CLI Directory	Vollständiger Pfad zum Ordner mit der XIV CLI
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
SMI-S-Protokoll	Protokoll für die Verbindung mit dem SMI-S-Provider. Zeigt auch den Standardport an.

Feld	Beschreibung
SMI-S-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Benutzername	Benutzername für den SMI-S Provider Host
Passwort	Kennwort für den SMI-S Provider-Host
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Lenovo Datensammler

Data Infrastructure Insights verwendet den Lenovo Datensammler zur Ermittlung von Bestands- und Leistungsdaten für Lenovo HX-Speichersysteme.

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Externe IP-Adresse des Prism
- Administrator-Benutzername und -Passwort
- TCP-Port-Anforderung: 9440

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port für die Verbindung zum Array. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Microsoft

Konfigurieren des Azure NetApp Files-Datensammlers

Data Infrastructure Insights verwendet den Azure NetApp Files Datensammler zur Erfassung von Bestands- und Performance-Daten.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren.

- Port-Anforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Principal Client-ID für den Azure-Service (Benutzerkonto)
- Azure Service Principal Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen ein Azure-Konto für die Erkennung von Data Infrastructure Insights einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure Service Principal Client-ID	Anmelde-ID bei Azure
Azure Mandanten-ID	Azure Mandanten-ID
Authentifizierungsschlüssel Des Azure Service Principal	Anmeldeauthentifizierungsschlüssel
Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt	Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt.

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60

Fehlerbehebung

- Die von Ihrem ANF-Datensammler verwendeten Anmeldedaten dürfen keinen Zugriff auf Azure-Abonnements haben, die ANF-Volumes enthalten.
- Wenn der Zugang zum Reader dazu führt, dass die Leistensammlung fehlschlägt, versuchen Sie, den Zugriff auf Mitarbeiter auf Ressourcengruppenebene zu gewähren.

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Microsoft Hyper-V Datensammler

Der Microsoft Hyper-V Datensammler erfasst Bestands- und Performancedaten aus der virtualisierten Server Computing-Umgebung. Dieser Datensammler kann einen eigenständigen Hyper-V-Host oder einen gesamten Cluster erkennen und einen Collector pro eigenständigen Host oder Cluster erstellen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Microsoft Hyper-V (WMI). Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Cluster Shared Volumes (CSV), Partition Volume	Datastore
Internet SCSI-Gerät, Multi Path SCSI LUN	LUN
Fibre Channel-Port	Port

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Für die Hyper-V muss Port 5985 geöffnet sein, damit Daten erfasst und Remote-Zugriff/-Management erfolgen können.
- IP-Adresse oder FQDN des Clusters oder Standalone-Hypervisors. Die Verwendung des unverankerten Cluster-Hostnamens oder der IP ist wahrscheinlich der zuverlässigste Ansatz im Vergleich dazu, den Collector nur auf einen bestimmten Knoten in einem Cluster zu verweisen.
- Benutzerkonto auf administrativer Ebene, das für alle Hypervisoren im Cluster funktioniert.
- WinRM muss aktiviert sein und alle Hypervisoren abhören
- Port-Anforderungen: Port 135 über WMI & Dynamic TCP Ports zugewiesen 1024-65535 für Windows 2003 und älter und 49152-65535 für Windows 2008.

- DNS-Auflösung muss erfolgreich sein, auch wenn der Datensammler nur auf eine IP-Adresse verweist
- Für jeden Hyper-V Hypervisor muss für jede VM, auf jedem Host, „Resource Metering“ aktiviert sein. Dadurch kann jeder Hypervisor bei jedem Gast mehr Daten für Data Infrastructure Insights zur Verfügung haben. Wenn diese Einstellung nicht festgelegt ist, werden für jeden Gast weniger Performance-Metriken erfasst. Weitere Informationen zur Ressourcenmessung finden Sie in der Microsoft-Dokumentation:

  "Hyper-V Übersicht zur Ressourcenmessung"

  "Aktivieren-VMressourcenMetering"

Für den Hyper-V-Datensammler ist eine Windows Acquisition Unit erforderlich.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adresse oder fließender Cluster-FQDN	Die IP-Adresse oder der vollständig qualifizierte Domänenname für das Cluster oder ein eigenständiger Hypervisor ohne Cluster
Benutzername	Administrator-Benutzername für den Hypervisor
Passwort	Kennwort für den Hypervisor
DNS-Domain-Suffix	Das Hostnamen-Suffix, das mit dem einfachen Hostnamen kombiniert wird, um den FQDN eines Hypervisors zu rendern

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp

NetApp Cloud Volumes ONTAP Datensammler

Dieser Datensammler unterstützt die Bestandserfassung aus Cloud Volumes ONTAP-Konfigurationen.

Konfiguration

Feld	Beschreibung
NetApp Management-IP-Adresse	IP-Adresse für Cloud Volumes ONTAP
Benutzername	Benutzername für Cloud Volumes ONTAP

Feld	Beschreibung
Passwort	Passwort für den oben genannten Benutzer

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS empfohlen. Zeigt außerdem den Standardport an.
Kommunikations-Port Überschreiben	Port zu verwenden, wenn nicht standardmäßig.
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Inventurzählung Der Threads	Anzahl der gleichzeitigen Threads.
Erzwingen von TLS für HTTPS	TLS über HTTPS erzwingen
Netzgruppen Automatisch Suchen	Netzgruppen Automatisch Suchen
Netzgruppenerweiterung	Wählen Sie Shell oder Datei aus
HTTP-Lesezeit Sekunden	Der Standardwert ist 30 Sekunden
Antworten als UTF-8 erzwingen	Antworten als UTF-8 erzwingen
Leistungsintervall (min)	Der Standardwert ist 900 Sekunden.
Performance-Threads Anzahl	Anzahl der gleichzeitigen Threads.
Erweiterte Zähldatensammlung	Aktivieren Sie diese Option, damit Data Infrastructure Insights die erweiterten Metriken aus der folgenden Liste erfasst.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp Cloud Volumes Services für AWS Data Collector

Dieser Datensammler unterstützt die Bestandserfassung von NetApp Cloud Volumes Services für AWS Konfigurationen.

Konfiguration

Feld	Beschreibung
Region Von Cloud Volumes	Region der NetApp Cloud Volumes Services für AWS
API-Schlüssel	API-Schlüssel für Cloud Volumes
Geheimer Schlüssel	Geheimen Schlüssel von Cloud Volumes

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Ich habe einen Fehler wie diesen erhalten: 'Anfrage konnte nicht ausgeführt werden: Verbindung zu <Endpunkt der AWS-Region>:8080 [<Endpunkt der AWS-Region>/Endpunkt der AWS-Region IP>] fehlgeschlagen: Verbindung abgelaufen: https://<AWS-Region ABRUFEN Endpunkt-FQDN>:8080/v1/Speicher/IPRanges HTTP/1.1'	Das"Proxy", das von Data Infrastructure Insights zur Kommunikation mit der Acquisition Unit verwendet wird, kommuniziert nicht zwischen Data Infrastructure Insights und dem Data Collector selbst. Hier sind einige Dinge, die Sie versuchen können: Stellen Sie sicher, dass die Erfassungseinheit in der Lage ist, den fqdn aufzulösen und den erforderlichen Port zu erreichen. Vergewissern Sie sich, dass kein Proxy erforderlich ist, um den angegebenen Endpunkt in der Fehlermeldung zu erreichen. Curl kann verwendet werden, um die Kommunikation zwischen der Akquisitionseinheit und dem Endpunkt zu testen. Stellen Sie sicher, dass Sie für diesen Test **nicht** einen Proxy verwenden. Beispiel: Root@acquisitionunit# curl -s -H Accept:Application/json -H "Content-type: Application/json" -H API-key:<API-Schlüssel in den Daten-Collector-Anmeldeinformationen verwendet -H secret-key:<SECRET key used in the Data Collector credentials> -X GET https://<AWS Regional Endpoint>:8080/v1/Storage/IPRanges Siehe dieses "NetApp KB-Artikel".

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler der NetApp ONTAP Datenmanagement-Software

Diese Datensammlung erfasst Bestands- und Performancedaten von Storage-Systemen mit ONTAP unter Verwendung von schreibgeschützten API-Aufrufen eines ONTAP-Kontos. Dieser Datensammler erstellt auch einen Datensatz in der Cluster-Anwendungsregistrierung, um den Support zu beschleunigen.

Terminologie

Data Infrastructure Insights erfasst Inventar- und Performance-Daten aus dem ONTAP Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

Terminologie für ONTAP Datenmanagement

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für ONTAP Storage-Assets finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer: Die Seriennummer des Arrays. Bei Cluster-Architektur Storage-Systemen wie ONTAP Datenmanagement, ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes.
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Microcode-Version – Firmware.
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt.
- Verwendet Flash Pool – Ja/kein Wert: Verfügen in diesem SATA/SAS-basierten Pool über SSDs zur Caching-Beschleunigung?
- Redundanz: RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.

- Überprovisionierung der Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der Prozentwert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet. ONTAP in MetroCluster Konfigurationen zeigen dies wahrscheinlich, während andere ONTAP Konfigurationen weniger sind.
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Auch viele Arrays Replikationsimplementierungen können die Festplattenauslastung steigern, während sie nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch.
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen.
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node.
- Speicher: Sockel 2 Speicher, falls verfügbar.
- Auslastung – bei ONTAP handelt es sich um einen Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie nachhaltige Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – abgeleitet aus ONTAP ZAPI-Aufrufen des Node-Objekts.
- Latenz: Direkt aus ONTAP ZAPI-Aufrufen des Node-Objekts abgeleitet.
- Durchsatz – abgeleitet direkt aus ONTAP ZAPI-Aufrufen des Node-Objekts.
- Prozessoren: Anzahl der CPUs

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützte API-Aufrufe konfiguriert ist.
- Zu den Kontodetails gehören Benutzername und Passwort.
- Port-Anforderungen: 80 oder 443
- Kontoberechtigungen:

- Nur den Rollennamen in der ontapi-Anwendung auf den Standard-Vserver lesen
- Möglicherweise benötigen Sie zusätzliche optionale Schreibberechtigungen. Siehe Hinweis über Berechtigungen unten.

- ONTAP Lizenzanforderungen:
  - FCP-Lizenz und zugeordnete/maskierte Volumes sind für die Fibre-Channel-Erkennung erforderlich

Berechtigungsanforderungen für das Sammeln von ONTAP-Switch-Metriken

Data Infrastructure Insights bietet die Möglichkeit, ONTAP-Cluster-Switch-Daten als Option in den Collector-Erweiterte KonfigurationEinstellungen zu erfassen. Zusätzlich zur Aktivierung dieser Funktion im Data Infrastructure Insights Collector müssen Sie das ONTAP-System* selbst so konfigurieren, dass "Switch-Informationen"die korrekten BerechtigungenEinstellungen vorgenommen werden, damit die Switch-Daten an Data Infrastructure Insights gesendet werden können.

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domain-Name des NetApp Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Die Standardeinstellung ist HTTPS
Kommunikations-Port Überschreiben	Geben Sie einen anderen Port an, wenn Sie den Standardwert nicht verwenden möchten
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Für TLS für HTTPS	TLS nur als Protokoll bei Verwendung von HTTPS zulassen
Netzgruppen Automatisch Suchen	Aktivieren Sie die automatische Suche der Netzgruppe nach den Regeln für die Exportrichtlinie
Netzgruppenerweiterung	Erweiterungsstrategie Für Netzgruppen: Wählen Sie_file_ oder_Shell_. Der Standardwert ist *shell*.
HTTP-Lesezeit Sekunden	Der Standardwert ist 30
Antworten als UTF-8 erzwingen	Erzwingt den Datensammler-Code, um Antworten aus der CLI als in UTF-8 zu interpretieren
Leistungsintervall (Sek.)	Der Standardwert ist 900 Sekunden.

Feld	Beschreibung
Erweiterte Zähldatensammlung	ONTAP Integration aktivieren. Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Wählen Sie die gewünschten Zähler aus der Liste aus.
Kennzahlen Für Cluster-Switch	Erfassung von Cluster-Switch-Daten durch Data Infrastructure Insights Beachten Sie, dass Sie zusätzlich zur Aktivierung dieser Funktion auf der Seite Dateninfrastruktureinblicke auch das ONTAP-System so konfigurieren müssen"Switch-Informationen", dass die korrekten BerechtigungenEinstellungen vorgenommen werden, damit die Switch-Daten an Dateninfrastruktureinblicke gesendet werden können. Siehe „Ein Hinweis zu Berechtigungen“ weiter unten.

ONTAP-Leistungskennzahlen

Mehrere ONTAP Modelle bieten Stromkennzahlen für Einblicke in die Dateninfrastruktur, die für Monitoring oder Warnmeldungen genutzt werden können. Die unten aufgeführten Listen unterstützter und nicht unterstützter Modelle sind nicht umfassend, sollten jedoch einige Hinweise enthalten. Wenn ein Modell in der gleichen Familie wie ein Modell auf der Liste ist, sollte der Support identisch sein.

Unterstützte Modelle:

A200
A220
A250
A300
A320
A400
A700
A700s
A800
A900
C190
FAS2240-4
FAS2552
FAS2650
FAS2720
FAS2750
FAS8200
FAS8300
FAS8700
FAS9000

Nicht Unterstützte Modelle:

FAS2620
FAS3250
FAS3270
FAS500f
FAS6280

FAS/ALL FLASH FAS 8020
FAS/ALL FLASH FAS 8040
FAS/ALL FLASH FAS 8060
FAS/ALL FLASH FAS 8080

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP Dashboards von Data Infrastructure Insights auf erweiterten ONTAP-Zählern basieren, müssen Sie im Abschnitt Erweiterte Konfiguration des Datensammlers **Advanced Counter Data Collection** aktivieren.

Sie sollten außerdem sicherstellen, dass die Schreibberechtigung für die ONTAP-API aktiviert ist. Dafür ist in der Regel ein Konto auf Cluster-Ebene mit den erforderlichen Berechtigungen erforderlich.

Um ein lokales Konto für Dateninfrastrukturanalysen auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clusterverwaltungsadministrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und die Befehle *diagnoseebene* müssen aktiviert sein.
2. Erstellen Sie mit den folgenden Befehlen eine schreibgeschützte Rolle.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Sobald Sie den Befehl create ausgeführt haben, werden Sie aufgefordert, ein Passwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Wenn AD/LDAP-Konto verwendet wird, sollte der Befehl sein

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Wenn Sie Cluster-Switch-Daten erfassen:
```

```
 security login rest-role create -role ci_readonly -api
/api/network/ethernet -access readonly
Die daraus resultierende Rolle und Benutzeranmeldung sieht folgendermaßen
aus: Die tatsächliche Ausgabe kann variieren:
```

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------ --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1::security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Wenn die ONTAP-Zugriffssteuerung nicht korrekt eingestellt ist, können die REST-Aufrufe von Data Infrastructure Insights fehlschlagen, was zu Datenlücken für das Gerät führt. Wenn Sie sie beispielsweise auf dem Dateninfrastruktursammler aktiviert haben, aber die Berechtigungen auf dem ONTAP nicht konfiguriert haben, schlägt die Erfassung fehl. Wenn die Rolle zuvor auf der ONTAP definiert ist und Sie die Rest-API-Fähigkeiten hinzufügen, stellen Sie außerdem sicher, dass *http* der Rolle hinzugefügt wird.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
Cluster-Version ist < 8.1	Die unterstützte Version für das Cluster-Minimum ist 8.1. Upgrade auf die unterstützte Mindestversion.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
Fehler: „7 Modus Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diese Datensammler benutzen, um 7 Modus Filer zu entdecken. Ändern Sie die IP, um stattdessen auf cdot Cluster zu verweisen.
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.

Problem:	Versuchen Sie dies:
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.

Leistung

Problem:	Versuchen Sie dies:
„Fehler beim Sammeln der Leistung aus ZAPI“ Fehler	Dies liegt normalerweise daran, dass perfstat nicht ausgeführt wird. Versuchen Sie auf jedem Knoten den folgenden Befehl: > *System Node systemshell -Node * -command „spmctl -h cmd -stop; spmctl -h cmd -exec“*

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp ONTAP REST-Datensammler

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Bestände, EMS-Protokolle und Performance-Daten von Speichersystemen mit ONTAP 9.14.1 und höher. Verwenden Sie für ONTAP-Systeme mit früheren Versionen den ZAPI-basierten Collector-Typ „NetApp ONTAP-Datenverwaltungssoftware“.

> ⓘ Der ONTAP REST Collector kann als Ersatz für den früheren ONTAPI-basierten Collector verwendet werden. Daher kann es bei den gesammelten oder berichteten Metriken zu Unterschieden kommen. Weitere Informationen zu den Unterschieden zwischen ONTAPI und REST finden Sie im "ONTAP 9.14.1 ONTAPI-to-REST-Zuordnung" Dokumentation.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass Administratorberechtigungen erforderlich sind, wenn Sie einen neuen REST-Benutzer/eine neue REST-Rolle erstellen.
  - Zu ihren Funktionen gehören in erster Linie Leseanforderungen. Für die Registrierung im ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich, damit sich Dateninfrastruktur Insights registrieren kann. Siehe *Hinweis zu Berechtigungen* direkt unten.

- ONTAP Version 9.14.1 oder höher.
- Anforderungen an den Hafen: 443

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP-Dashboards von Data Infrastructure Insights auf erweiterten ONTAP-Zählern basieren, sollten Sie **Enable Advanced Counter Data Collection** im Abschnitt Data Collector Advanced Configuration aktivieren.

Um ein lokales Konto für Dateninfrastrukturanalysen auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clusterverwaltungsadministrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und die Befehle *diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des vservers vom Typ *admin* ab. Sie werden diesen Namen in nachfolgenden Befehlen verwenden.

```
 vserver show -type admin
. Erstellen Sie eine Rolle mit den folgenden Befehlen:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Sobald Sie den Befehl create ausgeführt haben, werden Sie aufgefordert, ein Passwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Wenn AD/LDAP-Konto verwendet wird, sollte der Befehl sein

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Die daraus resultierende Rolle und Benutzeranmeldung sieht folgendermaßen
aus: Die tatsächliche Ausgabe kann variieren:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migration

Gehen Sie wie folgt vor, um von einem früheren ONTAP (ontapi)-Datensammler zum neueren ONTAP-REST-Collector zu migrieren:

1. Fügen Sie den REST Collector hinzu. Es wird empfohlen, Informationen für einen anderen Benutzer einzugeben als für den vorherigen Collector konfiguriert. Verwenden Sie zum Beispiel den Benutzer, der im Abschnitt Berechtigungen oben angegeben ist.
2. Unterbrechen Sie den vorherigen Collector, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector Daten für mindestens 30 Minuten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ angezeigt werden.
4. Nach der Ruhezeit sollten Sie Ihre Daten stabilisieren sehen, während der REST-Collector weiterhin zu erfassen.

Sie können diesen Vorgang verwenden, um zum vorherigen Collector zurückzukehren, wenn Sie möchten.

Konfiguration

Feld	Beschreibung
ONTAP-Management-IP-Adresse	Die IP-Adresse oder der vollständig qualifizierte Domänenname des NetApp-Clusters. Muss Cluster-Management-IP/FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Kennwort	Passwort für NetApp Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zähldatensammlung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
Aktivieren Sie die EMS-Ereigniserfassung	Wählen Sie diese Option aus, um die Ereignisdaten des ONTAP-EMS-Protokolls einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (s)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Performance-Daten aus dem ONTAP Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen
Storage Virtual Machine/Vserver	Storage Virtual Machine

Terminologie für ONTAP Datenmanagement

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für ONTAP Storage-Assets finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – die Array-UUID
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Microcode-Version – Firmware.

- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt.
- Verwendet Flash Pool – Ja/kein Wert: Verfügen in diesem SATA/SAS-basierten Pool über SSDs zur Caching-Beschleunigung?
- Redundanz: RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.
- Überprovisionierung der Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der Prozentwert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet. ONTAP in MetroCluster Konfigurationen zeigen dies wahrscheinlich, während andere ONTAP Konfigurationen weniger sind.
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Auch viele Arrays Replikationsimplementierungen können die Festplattenauslastung steigern, während sie nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch.
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen.
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node.

- Speicher: Sockel 2 Speicher, falls verfügbar.
- Auslastung – bei ONTAP handelt es sich um einen Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie nachhaltige Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Latenz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Durchsatz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Prozessoren: Anzahl der CPUs

ONTAP-Leistungskennzahlen

Mehrere ONTAP Modelle bieten Stromkennzahlen für Einblicke in die Dateninfrastruktur, die für Monitoring oder Warnmeldungen genutzt werden können. Die unten aufgeführten Listen unterstützter und nicht unterstützter Modelle sind nicht umfassend, sollten jedoch einige Hinweise enthalten. Wenn ein Modell in der gleichen Familie wie ein Modell auf der Liste ist, sollte der Support identisch sein.

Unterstützte Modelle:

A200
A220
A250
A300
A320
A400
A700
A700s
A800
A900
C190
FAS2240-4
FAS2552
FAS2650
FAS2720
FAS2750
FAS8200
FAS8300
FAS8700
FAS9000

Nicht Unterstützte Modelle:

FAS2620
FAS3250
FAS3270
FAS500f
FAS6280
FAS/ALL FLASH FAS 8020
FAS/ALL FLASH FAS 8040
FAS/ALL FLASH FAS 8060

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Beim Versuch, einen ONTAP-REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest API bei 10.193.70.14 ist nicht verfügbar: 10.193.70.14 Fehler beim ABRUFEN VON /API/Cluster: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem Oldeer ONTAP-Array), z. B. ONTAP 9.6), das keine REST-API-Funktionen hat. ONTAP 9.14.1 ist die minimale ONTAP-Version, die vom ONTAP REST Collector unterstützt wird. Bei den ONTAP-Versionen vor dem REST sind die Antworten auf „400 schlechte Anfragen“ zu erwarten. Für ONTAP-Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, können Sie die folgende ähnliche Meldung sehen: Konfiguration: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist verfügbar: Cheryl5-Cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ist aber nicht von der Mindestversion 9.14.1.
Ich sehe leere oder „0“ Metriken, wo der ONTAP ontapi Collector Daten anzeigt.	ONTAP REST enthält keine Kennzahlen, die nur intern auf dem ONTAP System verwendet werden. Systemaggregate werden beispielsweise nicht von ONTAP REST erfasst, sondern nur SVM vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Kennzahlen, bei denen keine oder leere Daten gemeldet werden können: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Storage: Die meisten Metriken sind eine Auflutung der Kennzahlen für das interne Volume und werden von den oben genannten Auswirkungen beeinflusst. Storage Virtual Machines: REST meldet keine anderen SVM-Typen als „Daten“ (z. B. „Cluster“, „gmt“, „Node“). Sie können auch eine Änderung in der Darstellung von Diagrammen bemerken, die Daten enthalten, aufgrund der Änderung des standardmäßigen Performance-Abfragezeitraums von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Plotten.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp Data ONTAP mit 7-Mode Datensammler

Bei Storage-Systemen mit Data ONTAP Software im 7-Mode verwenden Sie den 7-Mode Datensammler, der mit der CLI Kapazitäts- und Performance-Daten bezieht.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Data Collector von NetApp 7-Mode. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Dieser Datensammler ist "Veraltet".

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Filer	Storage
Filer	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren und zu verwenden:

- IP-Adressen des FAS Storage Controllers und des Partners.
- Port 443
- Ein benutzerdefinierter Benutzername und Passwort für den Admin-Level für den Controller und den Partner-Controller mit den folgenden Rollenfunktionen für 7-Mode:
  - „api-*“: Nutzen Sie diese, um OnCommand Insight die Ausführung aller NetApp Storage-API-Befehle zu ermöglichen.
  - „login-http-admin“: Hiermit kann OnCommand Insight über HTTP eine Verbindung mit dem NetApp Storage herstellen.
  - „Security-API-vfiler“: Nutzen Sie dies, um OnCommand Insight zu ermöglichen, NetApp Storage API Befehle auszuführen, um vFiler Einheitsinformationen abzurufen.
  - „cli-Optionen“: Hier können Sie Storage-Systemoptionen lesen.
  - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
  - „cli-df“: Verwenden Sie dies, um freien Speicherplatz anzuzeigen.
  - „cli-ifconfig“: Verwenden Sie diese, um Schnittstellen und IP-Adressen anzuzeigen.

Konfiguration

Feld	Beschreibung
Adresse des Storage-Systems	IP-Adresse oder vollqualifizierter Domain-Name für das NetApp Storage-System
Benutzername	Benutzername für das NetApp Storage-System
Passwort	Passwort für das NetApp Storage-System
Adresse des HA-Partners im Cluster	IP-Adresse oder vollqualifizierter Domain-Name für den HA-Partner
Benutzername des HA-Partners in Cluster	Benutzername für den HA-Partner
Passwort des HA Partner Filer in Cluster	Passwort für den HA-Partner

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Storage-Systemverbindung

Als Alternative zur Nutzung des Standard-Administrationsbenutzers für diesen Datensammler können Sie einen Benutzer mit Administratorrechten direkt auf den NetApp Storage-Systemen konfigurieren, sodass dieser Datensammler Daten von NetApp Storage-Systemen erfassen kann.

Für die Verbindung zu NetApp Storage-Systemen muss der Benutzer, der beim Erwerb der Haupt-pfiler angegeben ist (auf dem das Speichersystem vorhanden ist), die folgenden Bedingungen erfüllen:

- Der Benutzer muss auf vfiler0 (root Filer/pfiler) sein.

  Storage-Systeme werden beim Erwerb der Haupt-Filer erworben.

- Mit den folgenden Befehlen werden die Fähigkeiten der Benutzerrolle definiert:
  - „api-*“: Damit kann Dateninfrastruktur Insights alle NetApp Storage API-Befehle ausführen.

    Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.

  - „login-http-admin“: Hiermit können Dateninfrastruktureinblicke über HTTP eine Verbindung zum NetApp-Speicher herstellen. Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.
  - Security-API-vfiler: Verwenden Sie diese, damit Dateninfrastruktur Insights NetApp Storage API-Befehle ausführen kann, um Informationen über die vFiler Einheit abzurufen.
  - „cli-Opes“: Zum Befehl „Opes“, der für Partner-IP und aktivierte Lizenzen verwendet wird.

- „cli-lun“: Greifen Sie auf diesen Befehl zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
- „cli-df“: Für „df -s“, „df -r“, „df -A -r“ und für die Anzeige des freien Speicherplatzes
- „cli-ifconfig“: Für „ifconfig -a“ Befehl und verwendet für das Abrufen von Filer IP Adresse.
- "cli-rdfile": Für den Befehl "rdfile /etc/netgroup" und für das Abrufen von Netzgruppen verwendet.
- „cli-Datum“: Für den Befehl „Datum“ und mit dem vollständigen Datum für das Abrufen von Snapshot Kopien.
- „cli-Snap“: Für den Befehl „Snap list“ und zum Abrufen von Snapshot Kopien verwendet.

Wenn cli-Datum oder cli-Snap Berechtigungen nicht bereitgestellt werden, kann die Erfassung abgeschlossen werden. Snapshot Kopien werden jedoch nicht gemeldet.

Um eine 7-Mode Datenquelle erfolgreich zu erhalten und keine Warnungen auf dem Speichersystem zu generieren, sollten Sie eine der folgenden Befehlstrings verwenden, um Ihre Benutzerrollen zu definieren. Der zweite hier aufgeführte String ist eine optimierte Version des ersten:

- login-http-admin,API-*,Security-API-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-Snap,_
- login-http-admin,API-*,Security-API-vfile,cli-

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
Fehler „Befehl konnte nicht ausgeführt werden“	Prüfen Sie, ob der Benutzer auf dem Gerät über die folgenden Berechtigungen verfügt: • API-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-Operations • cli-rdfile • cli-Snap • Login-http-admin • Security-API-vfiler überprüfen Sie auch, ob die ONTAP-Version von Data Infrastructure Insights unterstützt wird, und überprüfen Sie, ob die verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
Cluster-Version ist < 8.1	Die unterstützte Version für das Cluster-Minimum ist 8.1. Upgrade auf die unterstützte Mindestversion.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
Fehler: „7 Modus Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diese Datensammler benutzen, um 7 Modus Filer zu entdecken. Ändern Sie IP, um stattdessen auf cdot Filer zu verweisen.

Problem:	Versuchen Sie dies:
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte Verbindung zum ZAPI nicht herstellen	IP/Port-Konnektivität prüfen und ZAPI-Konfiguration bestätigen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
Socket-Zeitüberschreitungsfehler mit ZAPI	Prüfen Sie die Filer-Konnektivität und/oder erhöhen Sie die Zeitüberschreitung.
„C-Modus-Cluster werden nicht durch den 7-Mode-Datenquelle unterstützt“-Fehler	Überprüfen Sie die IP und ändern Sie die IP in ein 7-Mode-Cluster.
Fehler „Verbindung zum vFiler konnte nicht hergestellt werden“	Überprüfen Sie, ob die Fähigkeiten des Erwerbs von Benutzern mindestens folgende Fähigkeiten enthalten: api-* Security-API-vfiler Login-http-admin Bestätigen Sie, dass Filer mindestens ONTAPI Version 1.7 läuft.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler für die NetApp E-Series ältere SANtricity API

Der Datensammler für die ältere SANtricity-API der NetApp E-Series erfasst Inventar- und Performance-Daten. Der Collector unterstützt die Firmware 7.x+ unter Verwendung derselben Konfigurationen und meldet dieselben Daten.

Terminologie

Cloud Insight erfasst die folgenden Bestandsinformationen aus dem NetApp E-Series Data Collector. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Volume-Gruppe	Festplattengruppe
Storage Array Durchführt	Storage
Controller	Storage-Node
Volume-Gruppe	Storage-Pool
Datenmenge	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Terminologie der E-Series (Landing Page)

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Asset-Landing-Pages der NetApp E-Series finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer: Die Seriennummer des Arrays. Bei Storage-Systemen der Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet
- Microcode-Version – Firmware
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen Volumes durch.
- Durchsatz – der Gesamthost des Arrays mit Blick auf den Durchsatz. Data Infrastructure Insights wird im Idealfall direkt aus dem Array bezogen, falls nicht verfügbar, und fasst den Durchsatz der Volumes zusammen, um diesen Wert abzuleiten
- Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Thin Provisioning“ oder „RAID-Gruppe“ sein
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt

- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz: RAID-Level oder Schutzschema. E-Series berichtet „RAID 7“ für DDP Pools
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz. Zu diesen beiden Werten zählen die „Erhaltung“ der Kapazität der E-Series, was sowohl in Zahlen als auch in Prozent höher ist als die der E-Series eigenen Benutzeroberfläche angezeigt werden kann
- Überprovisionierung der Kapazität: Wenn Sie mithilfe von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der prozentuale Wert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Außerdem können viele Arrays Replikationsimplementierungen die Festplattenauslastung steigern, während sie nicht als Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Wenn Festplatten-IOPS auf einer bestimmten Plattform nicht verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPS für alle Volumes in diesem Speicherpool bezogen
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn der Festplattendurchsatz auf einer bestimmten Plattform nicht verfügbar ist, wird dieser Wert für alle Volumes in diesem Speicherpool aus der Summe des Volumes abgerufen

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node
- Speicher: Sockel 2 Speicher, falls verfügbar
- Auslastung – im Allgemeinen eine CPU-Auslastungsnummer, oder im Fall von NetApp ONTAP, ein Controller-Stressindex. Die Auslastung ist derzeit für die NetApp E-Series nicht verfügbar
- IOPS: Eine Zahl, die die Host-gestützten IOPS auf diesem Controller repräsentiert. Idealerweise direkt aus dem Array bezogen. Wenn nicht verfügbar, wird der Wert berechnet, indem alle IOPS für Volumes zusammengefasst werden, die ausschließlich zu diesem Node gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Antwortzeit auf diesem Controller repräsentiert. Wenn nicht verfügbar, wird er idealerweise direkt aus dem Array bezogen. Wird das System dann berechnet, wenn die gewichtete IOPS-Berechnung aus den Volumes durchgeführt wird, die ausschließlich zu diesem Node gehören.
- Durchsatz: Eine Zahl, die den Host-basierten Durchsatz auf diesem Controller repräsentiert. Falls nicht verfügbar, wird der gesamte Durchsatz aus dem Array bezogen, wenn er nicht verfügbar ist, wird er

berechnet, indem der gesamte Durchsatz für Volumes zusammengefasst wird, die ausschließlich zu diesem Node gehören.

- Prozessoren: Anzahl der CPUs

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Port-Anforderung 2463

Konfiguration

Feld	Beschreibung
Kommagetrennte Liste der Array-SANtricity-Controller-IPs	IP-Adressen und/oder vollqualifizierte Domain-Namen für die Array Controller

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 30 Minuten
Leistungsintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp E-Series REST-Datensammler

Der REST-Datensammler der NetApp E-Series erfasst Inventar- und Performance-Daten. Der Collector unterstützt die Firmware 7.x+ unter Verwendung derselben Konfigurationen und meldet dieselben Daten. Der REST Collector überwacht den Verschlüsselungsstatus von Speicherpools sowie den Verschlüsselungsstatus zugehöriger Festplatten und Volumes und bietet CPU-Auslastung von Speicherknoten als Performance-Zähler - Funktionalität, die nicht im älteren Collector der SANtricity E-Series bereitgestellt wird.

Terminologie

Cloud Insight erfasst mithilfe von REST die folgenden Inventarinformationen der NetApp E-Series: Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Volume-Gruppe	Festplattengruppe
Storage Array Durchführt	Storage
Controller	Storage-Node

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Volume-Gruppe	Storage-Pool
Datenmenge	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Dieser Collector unterstützt nur Arrays mit E-Series-Modellen mit **nativen REST-API-Funktionen**. Die E-Series Organisation liefert eine Array-externe, installierbare REST API-Distribution für ältere E-Series Arrays, die dieses Szenario nicht unterstützt. Benutzer mit älteren Arrays sollten weiterhin den "E-Series SANtricity API"Collector von Data Infrastructure Insights verwenden.
- Das Feld „E-Series Controller IP-Adressen“ unterstützt eine durch Kommas getrennte Zeichenfolge von 2 IP/Hostnamen. Der Collector versucht intelligent, den zweiten IP/Hostnamen zu verwenden, wenn der erste nicht zugänglich ist.
- HTTPS-Port: Der Standardwert ist 8443.

Konfiguration

Feld	Beschreibung
IP-Adressen der E-Series Controller	Kommagetrennte IP-Adressen und/oder vollständig qualifizierte Domänennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 30 Minuten
Leistungsintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Terminologie der E-Series (Landing Page)

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Asset-Landing-Pages der NetApp E-Series finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer: Die Seriennummer des Arrays. Bei Storage-Systemen der Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet
- Microcode-Version – Firmware

- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen Volumes durch.
- Durchsatz – der Gesamthost des Arrays mit Blick auf den Durchsatz. Data Infrastructure Insights wird im Idealfall direkt aus dem Array bezogen, falls nicht verfügbar, und fasst den Durchsatz der Volumes zusammen, um diesen Wert abzuleiten
- Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Thin Provisioning“ oder „RAID-Gruppe“ sein
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz: RAID-Level oder Schutzschema. E-Series berichtet „RAID 7“ für DDP Pools
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz. Zu diesen beiden Werten zählen die „Erhaltung“ der Kapazität der E-Series, was sowohl in Zahlen als auch in Prozent höher ist als die der E-Series eigenen Benutzeroberfläche angezeigt werden kann
- Überprovisionierung der Kapazität: Wenn Sie mithilfe von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der prozentuale Wert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Außerdem können viele Arrays Replikationsimplementierungen die Festplattenauslastung steigern, während sie nicht als Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Wenn Festplatten-IOPS auf einer bestimmten Plattform nicht verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPS für alle Volumes in diesem Speicherpool bezogen
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn der Festplattendurchsatz auf einer bestimmten Plattform nicht verfügbar ist, wird dieser Wert für alle Volumes in diesem Speicherpool aus der Summe des Volumes abgerufen

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover

ausgeführt wird, ist er allgemein zu sehen

- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node
- Speicher: Sockel 2 Speicher, falls verfügbar
- Auslastung – im Allgemeinen eine CPU-Auslastungsnummer, oder im Fall von NetApp ONTAP, ein Controller-Stressindex. Die Auslastung ist derzeit für die NetApp E-Series nicht verfügbar
- IOPS: Eine Zahl, die die Host-gestützten IOPS auf diesem Controller repräsentiert. Idealerweise direkt aus dem Array bezogen. Wenn nicht verfügbar, wird der Wert berechnet, indem alle IOPS für Volumes zusammengefasst werden, die ausschließlich zu diesem Node gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Antwortzeit auf diesem Controller repräsentiert. Wenn nicht verfügbar, wird er idealerweise direkt aus dem Array bezogen. Wird das System dann berechnet, wenn die gewichtete IOPS-Berechnung aus den Volumes durchgeführt wird, die ausschließlich zu diesem Node gehören.
- Durchsatz: Eine Zahl, die den Host-basierten Durchsatz auf diesem Controller repräsentiert. Falls nicht verfügbar, wird der gesamte Durchsatz aus dem Array bezogen, wenn er nicht verfügbar ist, wird er berechnet, indem der gesamte Durchsatz für Volumes zusammengefasst wird, die ausschließlich zu diesem Node gehören.
- Prozessoren: Anzahl der CPUs

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Konfigurieren des Datensammlers des NetApp HCI-Verwaltungsservers

Der Datensammler des NetApp HCI-Verwaltungsservers sammelt Informationen zum NetApp HCI-Host und benötigt schreibgeschützte Berechtigungen auf allen Objekten innerhalb des Verwaltungsservers.

Dieser Datensammler erwirbt nur vom **NetApp HCI Management Server**. Um Daten aus dem Storage-System zu erfassen, müssen Sie außerdem den konfigurieren "NetApp SolidFire" Datensammler.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Festplatte
Host	Host
Virtual Machine	Virtual Machine
Datastore	Datastore

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
LUN	Datenmenge
Fibre-Channel-Port	Port

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die für diesen Datensammler möglicherweise nicht alle Fälle darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse des NetApp HCI-Verwaltungsservers
- Schreibgeschützter Benutzername und Kennwort für den NetApp HCI-Verwaltungsserver
- Schreibgeschützte Berechtigungen für alle Objekte im NetApp HCI-Verwaltungsserver.
- SDK-Zugriff auf den NetApp HCI-Verwaltungsserver – in der Regel bereits eingerichtet.
- Port-Anforderungen: http-80 HTTPS-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim NetApp HCI-Verwaltungsserver an
  - Überprüfen Sie, ob das SDK aktiviert ist: telnet <vc_ip> 443

Einrichtung und Verbindung

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
NetApp HCI Storage Cluster MVIP	Management Virtual IP-Adresse
SolidFire-Management-Node (mNode)	Management-Node-IP-Adresse
Benutzername	Benutzername für den Zugriff auf den NetApp HCI-Verwaltungsserver
Passwort	Passwort für den Zugriff auf den NetApp HCI-Verwaltungsserver
VCenter-Benutzername	Benutzername für vCenter
VCenter Passwort	Passwort für vCenter

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm Erweiterte Konfiguration die Option **VM Performance**, um Leistungsdaten zu sammeln. Bestandserfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Deafult ist 20
Filtern von VMs nach	Wählen Sie EINEN CLUSTER-, DATACENTER- oder ESX-HOST aus
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob VMs ein- oder ausgeschlossen werden sollen
Geräteliste Filtern	Liste der zu filternden VMs (durch Komma getrennt oder durch Semikolon getrennt, wenn Komma im Wert verwendet wird) für die Filterung nur nach ESX_HOST, CLUSTER und DATACENTER
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	**Versuchen Sie dies:**
Fehler: Liste einschließen, um VMs zu filtern, darf nicht leer sein	Wenn Liste einschließen ausgewählt ist, geben Sie gültige DataCenter-, Cluster- oder Hostnamen an, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter bei IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit Virtual Center über Infrastructure Client zu kommunizieren. * Versuchen Sie, mit Virtual Center über Managed Object Browser (z. B. MOB) zu kommunizieren.
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe Versionshinweise zu JDK 7 Update 40 unter "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp SolidFire All-Flash Array Datensammler

Der NetApp SolidFire All-Flash Array Data Collector unterstützt die Bestandsaufnahme und Performance der iSCSI- und Fibre Channel SolidFire-Konfigurationen.

Der SolidFire Datensammler nutzt die SolidFire REST API. Die Erfassungseinheit, in der sich der Datensammler befindet, muss in der Lage sein, HTTPS-Verbindungen zum TCP-Port 443 an der SolidFire-Cluster-Management-IP-Adresse zu initiieren. Der Datensammler benötigt Zugangsdaten, die in der Lage sind, REST-API-Abfragen auf dem SolidFire Cluster zu erstellen.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem Datensammler für rein Flash-basierte NetApp SolidFire Arrays: Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
Datenmenge	Datenmenge
Fibre-Channel-Port	Port
Volume Access Group, LUN-Zuweisung	Volume-Zuordnung
ISCSI-Sitzung	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers:

- Management Virtual IP-Adresse
- Schreibgeschützter Benutzername und Anmeldeinformationen
- Port 443

Konfiguration

Feld	Beschreibung
Management Virtual IP-Adresse (MVIP)	Management-virtuelle IP-Adresse des SolidFire-Clusters
Benutzername	Name, der zur Anmeldung im SolidFire Cluster verwendet wird
Passwort	Passwort, das zur Anmeldung beim SolidFire Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie den Verbindungstyp

Feld	Beschreibung
Kommunikations-Port	Für NetApp API verwendeter Port
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten
Leistungsintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Wenn SolidFire einen Fehler meldet, wird er in Data Infrastructure Insights wie folgt angezeigt:

Beim Versuch, Daten abzurufen, wurde eine Fehlermeldung von einem SolidFire-Gerät empfangen. Der Aufruf war <method> (<parameterString>). Die Fehlermeldung vom Gerät war (überprüfen Sie die Bedienungsanleitung des Geräts): <message>

Wo?

- Die ←Methode> ist eine HTTP-Methode, z. B. GET oder PUT.
- Der <parameterString> ist eine kommagetrennte Liste von Parametern, die im REST-Aufruf enthalten waren.
- Die Meldung <message> ist das Gerät, das als Fehlermeldung zurückgegeben wurde.

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

NetApp StorageGRID Datensammler

Der NetApp StorageGRID Datensammler unterstützt Inventar- und Performance-Sammlung aus StorageGRID Konfigurationen.

StorageGRID wird mit einem eigenen Raw TB für die gemanagte Einheit gemessen. Jede unformatierte StorageGRID-Kapazität von 40 TB wird als 1 berechnet "Verwaltete Einheit (ME)".

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem NetApp StorageGRID-Collector. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
StorageGRID	Storage
Knoten	Knoten
Mandant	Storage-Pool
Eimer	Internes Volumen

Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- StorageGRID-Host-IP-Adresse
- Ein Benutzername und ein Passwort für einen Benutzer, dem die Rollen Metric Query und Tenant Access zugewiesen sind
- Port 443

Konfiguration

Feld	Beschreibung
StorageGRID-Host-IP-Adresse	Management der virtuellen IP-Adresse der StorageGRID Appliance
Benutzername	Name, der zur Anmeldung bei der StorageGRID Appliance verwendet wird
Passwort	Passwort, das zur Anmeldung bei der StorageGRID Appliance verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Leistungsintervall (Sek.)	Der Standardwert ist 900 Sekunden

Single Sign On (SSO)

Der "StorageGRID" Firmware-Versionen verfügen über entsprechende API-Versionen; 3.0 API und neuere Versionen unterstützen Single Sign On (SSO)-Anmeldung.

Die Firmware-Version	API-Version	Unterstützung von Single Sign On (SSO)
11.1	2	Nein
11.2	3.0	Ja.
11.5	3.3	Ja.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Nutanix NX-Datensammler

Data Infrastructure Insights nutzt den Nutanix Datensammler zur Erkennung von Bestands- und Performancedaten für Nutanix NX-Speichersysteme.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Nutanix Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses

Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Nutanix Container	Internes Volumen
Nutanix Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Schreibgeschützter Benutzername und Kennwort, sofern keine Volume_groups verwendet werden, sind in diesem Fall Administratorbenutzername und Passwort erforderlich
- Port-Anforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP Port für die Verbindung mit dem Nutanix Array. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.
Abfrageintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

OpenStack Data Collector

Der OpenStack (REST API/KVM) Data Collector erfasst Bestandsdaten für alle OpenStack Instanzen und optional VM-Performance-Daten.

Anforderungen

- IP-Adresse des OpenStack Controllers
- Anmeldeinformationen für OpenStack Admin-Rollen und Zugriff auf den Linux-KVM-Hypervisor. Wenn Sie das Administratorkonto oder die entsprechenden Administratorrechte nicht verwenden, müssen Sie die Standardrichtlinien mithilfe von „Trial and Error“ ermitteln, um sich für Ihre Benutzer-ID für Datensammler zu entspannen.
- Das OpenStack Gnocchi-Modul muss für die Performance-Erfassung installiert und konfiguriert sein. Die Konfiguration von Gnocchi erfolgt durch Bearbeiten der Nova.conf-Datei für jeden Hypervisor und anschließenden Neustart des Nova Compute Service auf jedem Hypervisor. Die Optionsnamen ändern sich für verschiedene OpenStack Versionen:
  - Icehouse
  - Juno
  - Kilo
  - Freiheit
  - Mitaka
  - Newton
  - Kata
- Für CPU-Statistiken muss „Compute_Monitors=ComputeDriverCPUMonitor“ in /etc/Nova/Nova.conf auf Computing-Knoten eingeschaltet werden.
- Port-Anforderungen:
  - 5000 für http und 13000 für https, für den Keystone Service
  - 22 für KVM SSH
  - 8774 für Nova Compute Service
  - 8776 für Cinder Block Service
  - 8777 für Gnocchi Performance Service
  - 9292 für Glance Image Service **Hinweis** der Port bindet sich an den spezifischen Dienst, und der Dienst kann auf dem Controller oder einem anderen Host in größeren Umgebungen ausgeführt werden.

Konfiguration

Feld	Beschreibung
OpenStack-Controller-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des OpenStack Controllers
OpenStack Administrator	Benutzername für einen OpenStack Admin
OpenStack Passwort	Passwort, das für den OpenStack Admin verwendet wird
OpenStack Administrator-Mandant	Mandantenname des OpenStack Administrator
KVM-Sudo-Benutzer	KVM sudo Benutzername
Wählen Sie „Kennwort“ oder „OpenSSH-Schlüsseldatei“, um den Anmeldeinformationstyp anzugeben	Anmeldeinformationstyp, der für die Verbindung zum Gerät über SSH verwendet wird

Feld	Beschreibung
Vollständiger Pfad zum privaten Bestandsschlüssel	Vollständiger Pfad zum privaten Bestandsschlüssel
KVM-Sudo-Kennwort	KVM-Sudo-Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Aktivieren der Erkennung des Hypervisor-Inventars über SSH	Aktivieren Sie diese Option, um die Erkennung des Hypervisor-Inventars über SSH zu aktivieren
OpenStack Admin-URL-Port	OpenStack Admin-URL-Port
Verwenden Sie HTTPS	Überprüfen Sie, ob sicheres HTTP verwendet wird
SSH-Port	Port, der für SSH verwendet wird
SSH-Prozess wird erneut ausgeführt	Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Konfigurationsfehler“ mit Fehlermeldungen beginnen mit „Policy lässt nicht zu“ oder „Sie sind nicht autorisiert“	* ip-Adresse prüfen * Benutzername und Passwort überprüfen

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler der Oracle ZFS Storage Appliance

Data Infrastructure Insights verwendet den Datensammler der Oracle ZFS Storage Appliance zur Erfassung von Bestands- und Leistungsdaten.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen mit dem Oracle ZFS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte (SSD)	Festplatte
Cluster	Storage

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Controller	Storage-Node
LUN	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Initiator, Ziel	Volume-Maske
Share	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

- Host-Namen für den ZFS-Controller-1 und den ZFS-Controller-2
- Administrator-Benutzername und -Passwort
- Port-Anforderung: 215 HTTP/HTTPS

Erforderliche Performance-Metriken

Oracle ZFS Appliances stellen Storage-Verwaltungen große Flexibilität zur Erfassung von Performance-Statistiken zur Verfügung. Data Infrastructure Insights erwartet, dass Sie in einem Hochverfügbarkeitspaar *each* Controller konfiguriert haben, um die folgenden Kennzahlen zu erfassen:

- smb2.OPS[Freigabe]
- nfs3.OPS[Freigabe]
- nfs4.OPS[Share]
- nfs4-1.OPS[Share]

Wird ein Controller diese oder alle Funktionen nicht erfassen, führt dies wahrscheinlich dazu, dass Data Infrastructure Insights den Workload auf den „internen Volumes“ nicht oder nur unzureichend meldet.

Konfiguration

Feld	Beschreibung
ZFS Controller-1-Hostname	Host Name für Storage Controller 1
ZFS Controller-2-Hostname	Host-Name für Storage Controller 2
Benutzername	Benutzername für das Benutzerkonto des Speichersystemadministrators
Passwort	Kennwort für das Administratorbenutzerkonto

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an

Feld	Beschreibung
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Abfrageintervall für den Bestand	Der Standardwert beträgt 60 Sekunden
Leistungsintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“	ZFS-Benutzerkonto und -Passwort validieren
„Konfigurationsfehler“ mit Fehlermeldung „REST Service ist deaktiviert“	Vergewissern Sie sich, dass DER REST-Dienst auf diesem Gerät aktiviert ist.
„Konfigurationsfehler“ mit Fehlermeldung „Benutzer nicht autorisiert für Befehl“	Dieser Fehler ist wahrscheinlich darauf zurückzuführen, dass bestimmte Rollen (z. B. „Advanced_Analytics“) für den konfigurierten Benutzer nicht enthalten sind. Durch die Anwendung des Analysebereichs für den Benutzer mit schreibgeschützter Rolle kann der Fehler behoben werden. Führen Sie hierzu folgende Schritte aus: 1. Bewegen Sie auf dem ZFS-System im Bildschirm Konfiguration → Benutzer die Maus über die Rolle und doppelklicken Sie, um die Bearbeitung zu ermöglichen 2. Wählen Sie im Dropdown-Menü „Bereich“ die Option „Analyse“ aus. Eine Liste der möglichen Eigenschaften wird angezeigt. 3. Klicken Sie auf das Kontrollkästchen am oberen Ende, um alle drei Eigenschaften auszuwählen. 4. Klicken Sie auf der rechten Seite auf die Schaltfläche Hinzufügen. 5. Klicken Sie oben rechts im Popup-Fenster auf die Schaltfläche Übernehmen. Das Popup-Fenster wird geschlossen.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Pure Storage FlashArray

Data Infrastructure Insights verwendet den Pure Storage FlashArray Datensammler zur Erfassung von Bestands- und Performance-Daten.

Terminologie

Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die gängigste Terminologie für die Ressource angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk (SSD)	Festplatte
Array Erledigen	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Initiator, Ziel	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- IP-Adresse des Storage-Systems
- Benutzername und Kennwort für das Administratorkonto des Pure Storage-Systems.
- Port-Anforderung: HTTP/HTTPS 80/443

Konfiguration

Feld	Beschreibung
FlashArray Host-IP-Adresse	IP-Adresse des Storage-Systems
Benutzername	Benutzername mit Administratorrechten
Passwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie HTTP oder HTTPS. Zeigt auch den Standardport an.
TCP-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten

Feld	Beschreibung
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Richtlinie lässt nicht zu“ oder „Sie sind nicht autorisiert“	Validierung des Pure Benutzerkontos und Passworts über die Pure http Schnittstelle

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Datensammler Red hat Virtualization

Data Infrastructure Insights verwendet den Datensammler Red hat Virtualization zur Erfassung von Bestandsdaten aus virtualisierten Linux- und Microsoft Windows-Workloads.

Terminologie

Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die gängigste Terminologie für die Ressource angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Storage Domain	Datastore
Logische Einheit	LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- IP-Adresse des RHEV-Servers über Port 443 über REST-API
- Nur-Lese-Benutzername und Kennwort
- RHEV Version 3.0+

Konfiguration

Feld	Beschreibung
RHEV-Server-IP-Adresse	IP-Adresse des Storage-Systems
Benutzername	Benutzername mit Administratorrechten
Passwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Kommunikationsschnittstelle	Port, der für die HTTPS-Kommunikation mit RHEV verwendet wird
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Rubrik CDM Data Collector

Data Infrastructure Insights erfasst mithilfe des Rubrik Datensammlers Inventar- und Performance-Daten von Rubrik Storage Appliances.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Datensammler Rubrik. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage, Storage-Pool
Knoten	Storage-Node
Festplatte	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 zum Cluster Rubrik. Ein Collector pro Cluster.
- IP-Adresse des Rubrik Clusters.

- Benutzername und Passwort für das Cluster.
- Rubrik Cluster IP-Adresse oder Hostname.
- Für die Basisauthentifizierung müssen ein Benutzername und ein Passwort für das Cluster eingegeben werden. Wenn Sie die Service Account-basierte Authentifizierung bevorzugen, benötigen Sie ein Dienstkonto, einen geheimen Schlüssel und eine Unternehmens-ID
- Port-Anforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
IP	IP-Adresse des Clusters Rubrik
Benutzername	Benutzername für das Cluster
Passwort	Passwort für das Cluster

Erweiterte Konfiguration

Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Ich erhielt die Nachricht, dass mehr als ein Speicher erstellt wird.	Überprüfen Sie, ob das Cluster ordnungsgemäß konfiguriert ist und der Collector auf ein einzelnes Cluster verweist.
Ich erhielt eine Warnung, dass die Disk API mehr Daten zurückgegeben hat	Wenden Sie sich an den Support, um zusätzliche Daten zu erhalten.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

VMware vSphere Data Collector konfigurieren

Der Datensammler für VMware vSphere erfasst Performance- und Konfigurationsinformationen für die VM-Gast- und ESXi Hosts und erfordert schreibgeschützte Privileges für alle Objekte in vSphere. Ab August 2024 werden bei vSphere Collector zusätzlich Protokollmeldungen aus vSphere-Umgebungen und einige VMware-spezifische Kennzahlen integriert. Beachten Sie bitte, dass Data Infrastructure Insights nur Informationen zu VMware-Protokollen aus Umgebungen mit vSphere 8.0.1 oder höher abrufen kann. Ebenso werden die anbieterspezifischen Metriken nur für vSphere 7+-Umgebungen unterstützt. Daher können Sie das Kontrollkästchen Protokolle und/oder anbieterspezifische Metriken für einen bestimmten Collector deaktivieren, wenn

auf eine ältere vSphere-Instanz verwiesen wird.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem VMware vSphere-Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Festplatte
Host	Host
Virtual Machine	Virtual Machine
Datastore	Datastore
LUN	Datenmenge
Fibre-Channel-Port	Port

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die für diesen Datensammler möglicherweise nicht alle Fälle darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse des Virtual Center-Servers
- Schreibgeschützter Benutzername und Kennwort in Virtual Center
- Für alle Objekte im Virtual Center benötigen wir schreibgeschützte Berechtigungen.
- SDK-Zugriff auf dem Virtual Center-Server – in der Regel bereits eingerichtet.
- Port-Anforderungen: http-80 HTTPS-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim Virtual Center Client an
  - Überprüfen Sie, ob das SDK aktiviert ist: telnet <vc_ip> 443

Einrichtung und Verbindung

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
IP-Adresse für Virtual Center	IP-Adresse des Virtual Center
Benutzername	Benutzername für den Zugriff auf das Virtual Center

Feld	Beschreibung
Passwort	Passwort für den Zugriff auf das Virtual Center

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm Erweiterte Konfiguration die Option **VM Performance**, um Leistungsdaten zu sammeln. Bestandserfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20
Filtern von VMs	Wählen Sie EINEN CLUSTER-, DATACENTER- oder ESX-HOST aus
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Filterliste erstellen (CLUSTER, DATACENTER und/oder ESX_HOST)
Anzahl der Wiederholungen	Der Standardwert ist 3
Kommunikations-Port	Der Standardwert ist 443
Geräteliste Filtern…	Diese Liste muss aus exakten String-Übereinstimmungen bestehen. Wenn Sie nach ESX_HOST filtern möchten, müssen Sie eine kommagetrennte Liste mit den genauen „Namen“ Ihrer ESX-Hosts erstellen, wie in Data Infrastructure Insights und vSphere gemeldet. Bei diesen „Namen“ handelt es sich entweder um IP-Adressen, einfache Hostnamen oder vollqualifizierte Domain-Namen (FQDNs) – dies wird durch den Namen dieser Hosts bestimmt, als sie ursprünglich zu vSphere hinzugefügt wurden. Verwenden Sie bei der Filterung nach CLUSTER die von CI auf Hypervisoren gemeldeten Cluster-Namen im Stil von Data Infrastructure Insights – Data Infrastructure Insights setzt den vSphere-Cluster-Namen mit dem vSphere-Datacenter-Namen und einem Schrägstrich voraus – „DC1/clusterA“ ist der Cluster-Name Data Infrastructure Insights würde über einen Hypervisor in ClusterA im Rechenzentrum DC1 berichten.
Leistungsintervall (Sek.)	Der Standardwert ist 300

Zuordnen von VMware Tags zu Annotationen zu Data Infrastructure Insights

Der VMware Datensammler ermöglicht das Befüllen von Data Infrastructure Insights Annotationen mit Tags, die auf VMware konfiguriert sind. Die Annotationen müssen genau mit den VMware Tags benannt werden. Data Infrastructure Insights füllt immer Anmerkungen vom gleichen Namen aus und versucht, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) zu füllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht füllt, kann es erforderlich sein, die Anmerkung zu entfernen und sie als Texttyp neu zu erstellen.

Achten Sie darauf, dass bei VMware Tags die Groß-/Kleinschreibung beachtet wird, während bei Data Infrastructure Insights die Tags nicht beachtet werden müssen. Wenn Sie in Data Infrastructure Insights eine Annotation mit dem Namen „BESITZER“ und Tags mit den Namen „EIGENTÜMER“, „Eigentümer“ und

„Eigentümer“ in VMware erstellen, würden alle diese Variationen von „Eigentümer“ auch der Annotation von Cloud Insight zugeordnet.

Beachten Sie Folgendes:

- Data Infrastructure Insights veröffentlicht derzeit nur automatisch Supportinformationen für NetApp-Geräte.
- Da diese Support-Informationen in Anmerkungsform gespeichert sind, können Sie sie abfragen oder in Dashboards verwenden.
- Wenn ein Benutzer den Anmerkungswert überschreibt oder leert, wird der Wert erneut automatisch gefräst, wenn Data Infrastructure Insights die Anmerkungen aktualisiert, die er einmal täglich tut.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Liste einschließen, um VMs zu filtern, darf nicht leer sein	Wenn Liste einschließen ausgewählt ist, geben Sie gültige DataCenter-, Cluster- oder Hostnamen an, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter bei IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit Virtual Center über den VMware Infrastructure Client zu kommunizieren. * Versuchen Sie, mit Virtual Center über Managed Object Browser (z. B. MOB) zu kommunizieren.
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe Versionshinweise zu JDK 7 Update 40 unter "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Data Collector Reference - Dienste

Erfassung Von Node-Daten

Data Infrastructure Insights sammelt Kennzahlen aus dem Knoten, auf dem Sie einen Agenten installieren.

Installation

1. Wählen Sie unter **Observability > Collectors** ein Betriebssystem/eine Plattform aus. Beachten Sie, dass durch die Installation eines Datensammlers für die Integration (Kubernetes, Docker, Apache usw.) auch die Erfassung von Node-Daten konfiguriert wird.
2. Befolgen Sie die Anweisungen, um den Agenten zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden als Node-Kennzahlen erfasst:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten Dateisystem	Node-UUID-Gerätetyp	Node-IP Node-Name Node OS-Modus	Freie Inodes Free Inodes Total Inodes Used Total Used Total Used Total Used
Node-Festplatte	Node-UUID-Festplatte	Node-IP Node-Name Node OS	I/O-Zeit insgesamt IOPS in Bearbeitung Lesen von Bytes (pro s) Lesezeit insgesamt Lesevorgänge (pro s) gewichtete I/O-Zeit insgesamt Schreibbyte (pro s) Schreibzeit Gesamtzahl Schreibvorgänge (pro s) Aktuelle Festplattenwarteschlange Länge Schreibzeit I/O-Zeit
Node-CPU	Node-UUID-CPU	Node-IP Node-Name Node OS	System CPU Usage User CPU Usage Idle CPU Usage Prozessor CPU Usage Interrupt CPU Usage DPC CPU Usage

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten	Node-UUID	Node-IP Node-Name Node OS	Kernel Boot Time Kernel Context Switches (per sec) Kernel Entropy Available Kernel Interrupts (per sec) Kernel processes Forked (per sec) Arbeitsspeicher Aktiver Speicher Verfügbar Gesamter Verfügbarer Speicher Gepufferter Speicher Im Cache Speicherlimit Speicher Speicher Bereitgestellt Als Speicher Schmutziger Speicher Freier Speicher Hoher Freier Speicher Hoher Gesamtspeicher Riesige Seitengröße Speicher Riesige Seiten Freier Speicher Riesige Seiten Gesamt Speicher Niedriger Freier Speicher Niedriger Speicher Gemappter Speicher Seitentabellen Speicher Gemeinsam Genutzter Speicher Slab Speicher Austausch Gecachten Speicher Austausch Freier Speicher Austausch Gesamt Speicher Verwendeter Gesamt-Speicher Verwendeter Speicher Vmalloc Chunk Speicher Vmalloc Gesamt-Speicher Vmalloc Verwendeter Speicher Wired Memory Writeback Total Memory Writeback Tmp Speicher Cache Fehler Speicheranforderung Null Fehler Speicherseiten Fehler Speicherseiten Fehler Speicherseiten-Speicher-Seiten-Speicher Nicht Gepageter Speicher Paged Memory Cache Core Memory Standby Cache Normaler Speicher Standby Cache Reserve Memory Transition Fehler Prozesse Blockierte Prozesse Dead Processes

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Node-Netzwerk	UUID der Netzwerkschnittstelle-Node	Node Name Node-IP Node OS	Bytes Empfangene Bytes Gesendete Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Paketfehler Empfangen Pakete Empfangene Fehler Pakete Empfangene Pakete Empfangene Pakete Empfangen Pakete

Einrichtung

Informationen zur Einrichtung und Fehlerbehebung finden Sie im "Konfigurieren eines Agenten" Seite.

ActiveMQ Data Collector

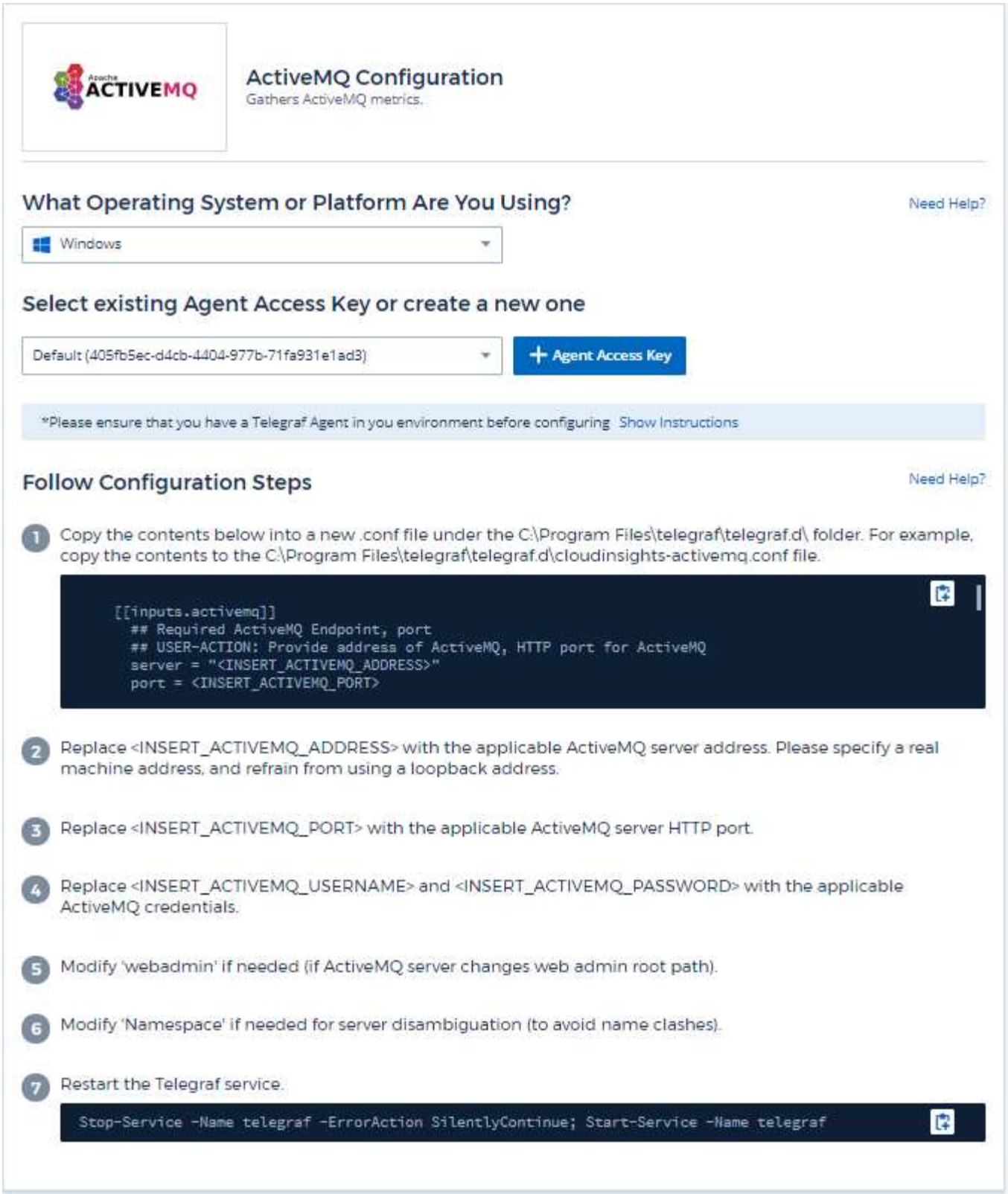
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus ActiveMQ zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie ActiveMQ.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "ActiveMQ-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
ActiveMQ-Warteschlange	Namespace Queue Port Server	Node Name Node-IP-Node-UUID	Anzahl Der Warteschlange Anzahl Der Kunden Anzahl Der Ausgleiche Anzahl Warteschlange Größe
ActiveMQ-Abonnenten	Namespace für Client-ID-Verbindungs-ID-Port-Server	Ist Active Destination Node Name Node IP Node UUID Node OS Selector Subscription	Anzahl Der Entsandten Absendete Warteschlange Anzahl Der Abgesandten Warteschlange Größe Anzahl Der Warteschlange Anzahl Der Ausstehenden Warteschlange Größe
ActiveMQ-Thema	Thema Port Server Namespace	Node Name Node-IP-Node-UUID-Node-OS	Anzahl Der Ausgleichen Anzahl Der Verbraucher Größe Der Anzahl Der Warteschlangen

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Apache Data Collector

Dieser Datensammler ermöglicht die Erfassung von Daten von Apache-Servern in Ihrer Umgebung.

Voraussetzungen

- Sie müssen Ihren Apache HTTP Server einrichten und ordnungsgemäß ausführen lassen
- Sie müssen über sudo- oder Administratorberechtigungen auf Ihrem Agent-Host/VM verfügen
- In der Regel ist das Apache *mod_Status*-Modul so konfiguriert, dass eine Seite am Speicherort '/Server-Status?Auto' des Apache-Servers angezeigt wird. Die Option *ExtendedStatus* muss aktiviert sein, um alle verfügbaren Felder zu erfassen. Informationen zum Konfigurieren des Servers finden Sie in der Apache-Moduldokumentation: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

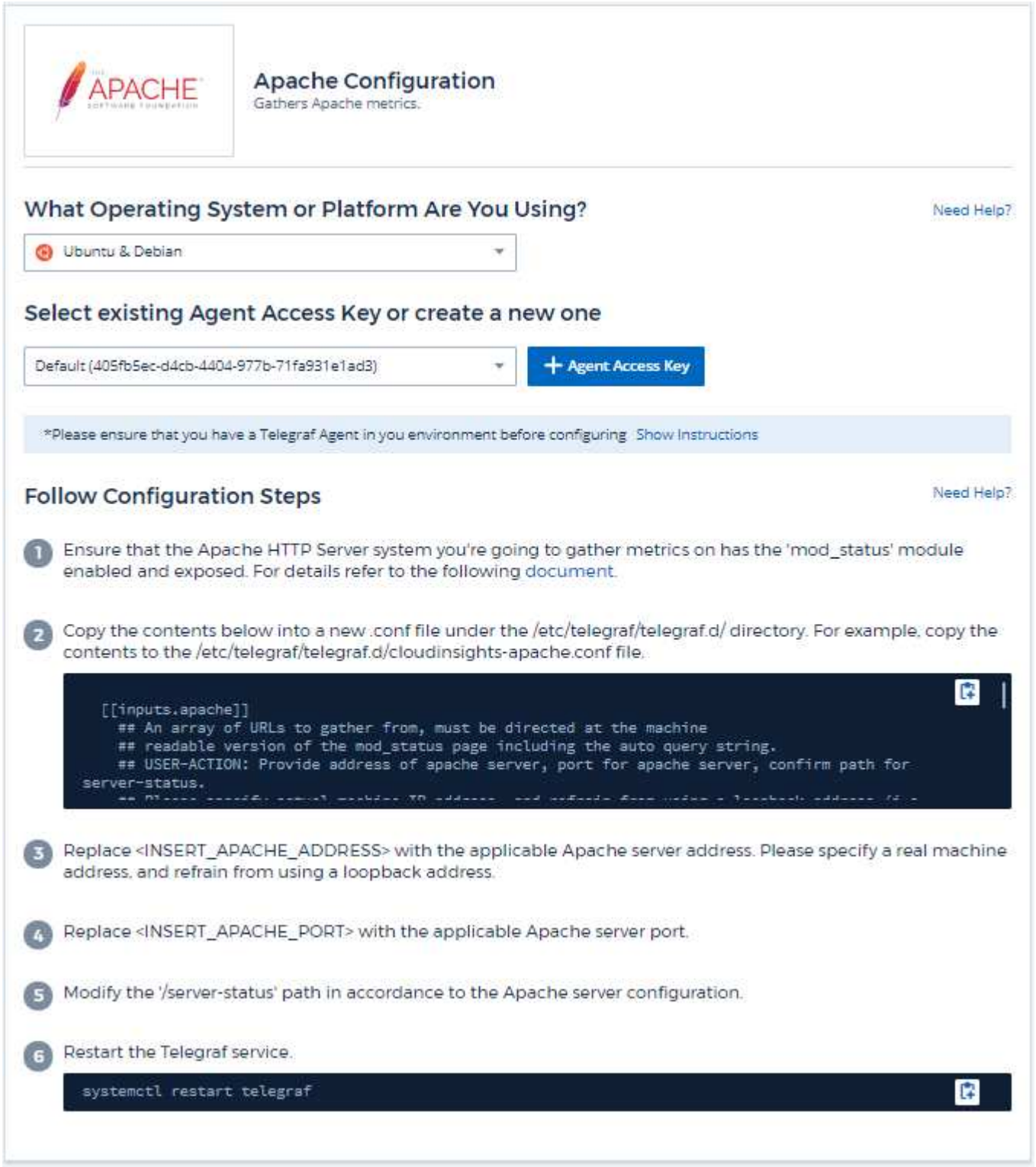
1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Apache.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-

Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Telegraf-Plugin für Apache's HTTP Server setzt auf das 'mod_Status'-Modul, um aktiviert zu werden. Wenn diese Option aktiviert ist, wird Apache HTTP Server einen HTML-Endpunkt anzeigen, der in Ihrem Browser angezeigt oder für die Extraktion des Status aller Apache HTTP Server-Konfigurationen gepatzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen Apache HTTP Server Version 2.4.38 entwickelt.

Aktivieren von mod_Status:

Das Aktivieren und Bereitstellen der 'mod_Status'-Module umfasst zwei Schritte:

- Modul wird aktivieren
- Legen Sie Statistiken aus dem Modul fest

Modul aktivieren:

Das Laden von Modulen wird durch die Konfigurationsdatei unter '/usr/local/apache/conf/httpd.conf' gesteuert. Bearbeiten Sie die config-Datei und heben Sie die folgenden Zeilen aus:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Statistiken aus dem Modul offenlegen:

Die Offenlegung von 'mod_Status' wird durch die Konfigurationsdatei unter '/usr/local/apache2/conf/extra/httpd-info.conf' gesteuert. Stellen Sie sicher, dass Sie in dieser Konfigurationsdatei Folgendes haben (mindestens sind weitere Richtlinien vorhanden):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Detaillierte Anweisungen zum Modul „MOD_Status“ finden Sie im "Apache-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Apache	Namespace-Server	Node-IP-Knotenname-Port-Parent Server-Konfiguration der übergeordnete Server-Generation der MPM-Generation wird angehalten	Beschäftigte Arbeiter Bytes pro Anfrage Bytes pro Sekunde CPU Kinder System CPU Kinder Benutzer CPU Last CPU System CPU System CPU Benutzer asynchrone Verbindungen Schließen Asynchronous Connections am Leben Asynchronous Connections Writing connections Total Duration per Request Idle Workers Load Average (Last 1m) Load Average (Last 15m) Load Average (Last Average (Last 5m) Prozesse Anfragen pro Sekunde Gesamtzugriff Gesamtdauer Gesamtdauer KBytes Scoreboard schließen Scoreboard DNS Lookups Scoreboard abschließen Scoreboard-Idle Cleanup Scoreboard halten am Leben Scoreboard Logging Scoreboard öffnen Scoreboard lesen Scoreboard senden Scoreboard Starting Scoreboard warten

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Consul Data Collector

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Consul zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Konsul.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert "Installieren Sie

einen Agenten" Ihrer Umgebung zu unterstützen.

Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen auf dem Bildschirm Consul Configuration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Einrichtung

Informationen finden Sie unter "Dokumentation für Konsul".

Objekte und Zähler für Konsul

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Konsul	Namespace-ID-Service-Node prüfen	Node-IP Node OS Node UUID Node Name Service Name Check Name Service Service ID Status	Warnung Bei Kritischem Durchgang

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Couchbase Data Collector

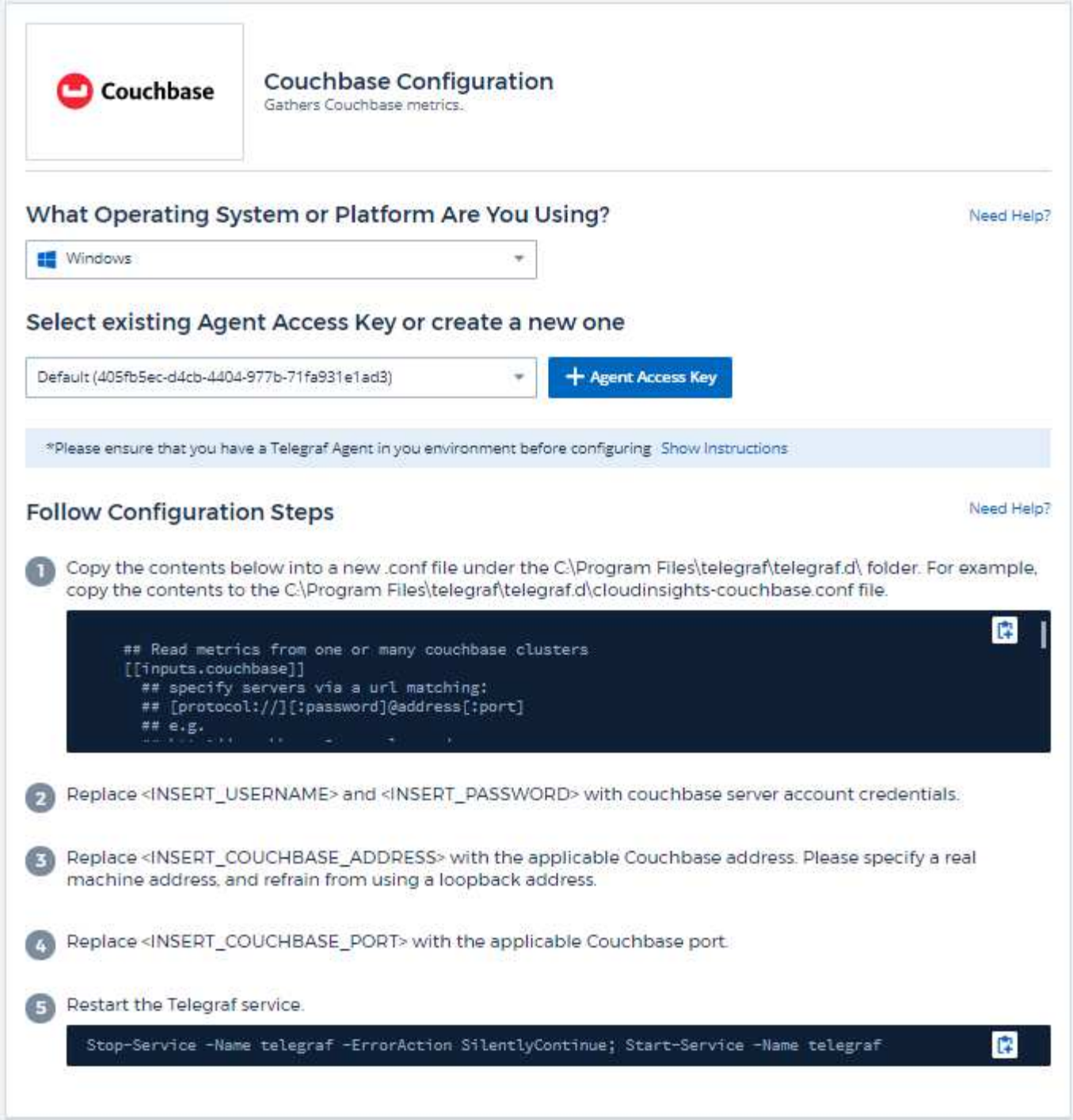
Data Infrastructure Insights nutzt diesen Datensammler zur Erfassung von Kennzahlen aus Couchbase.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Couchbase.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Couchbase Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Couchbase Node	Namespace Cluster Couchbase Node-Hostname	Node Name Node-IP	Speicher Insgesamt
Couchbase Bucket	Namespace-Bucket-Cluster	Node Name Node-IP	Daten Verwendete Daten Abrufen Verwendete Elemente Anzahl Verwendete Elemente Speicher Verwendete Operationen Pro Sekunde Kontingent Verwendet

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

CouchDB Data Collector

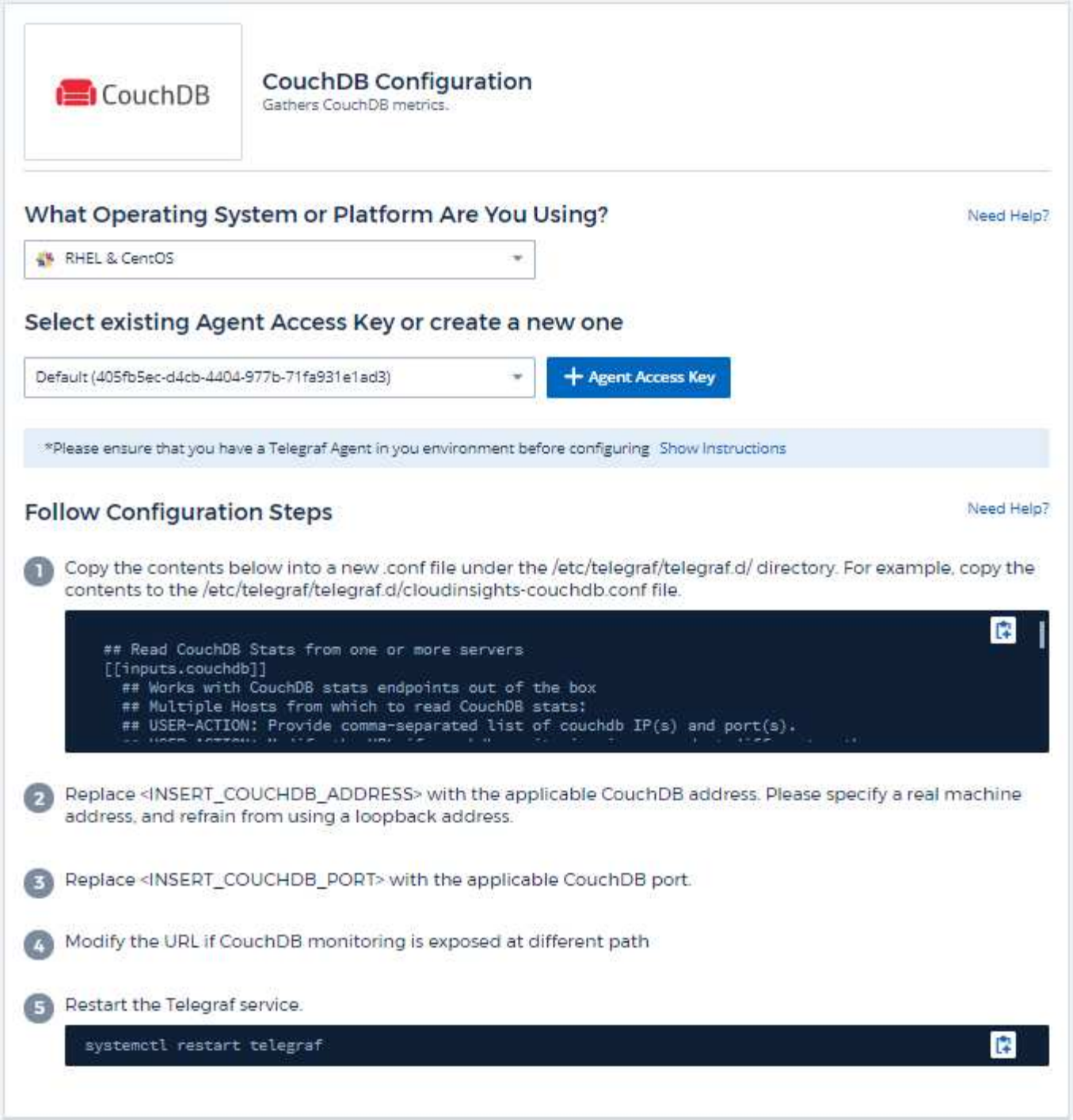
Data Infrastructure Insights nutzt diesen Datensammler, um Metriken von CouchDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie CouchDB.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "CouchDB-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
CouchDB	Namespace-Server	Node Name Node-IP	Authentifizierung Cache Treffer Authentifizierung Cache Fräulein Datenbank liest Datenbank schreibt Datenbanken Open OS Files Max Anfragenzeit Min Anfragestzeit httpd Request Methoden httpd Request Methoden httpd Request löschen httpd Request Methods Get httpd Request Methods Head httpd Request Methods Post httpd Request Methods Put Status Codes 200 Status Codes 201 Statuscodes 202 Statuscodes 301 Statuscodes 304 Statuscodes 400 Statuscodes 401 Statuscodes 403 Statuscodes 404 Statuscodes 405 Statuscodes 409 Statuscodes 412 Statuscodes 500

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Docker Data Collector

Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus Docker zu sammeln.

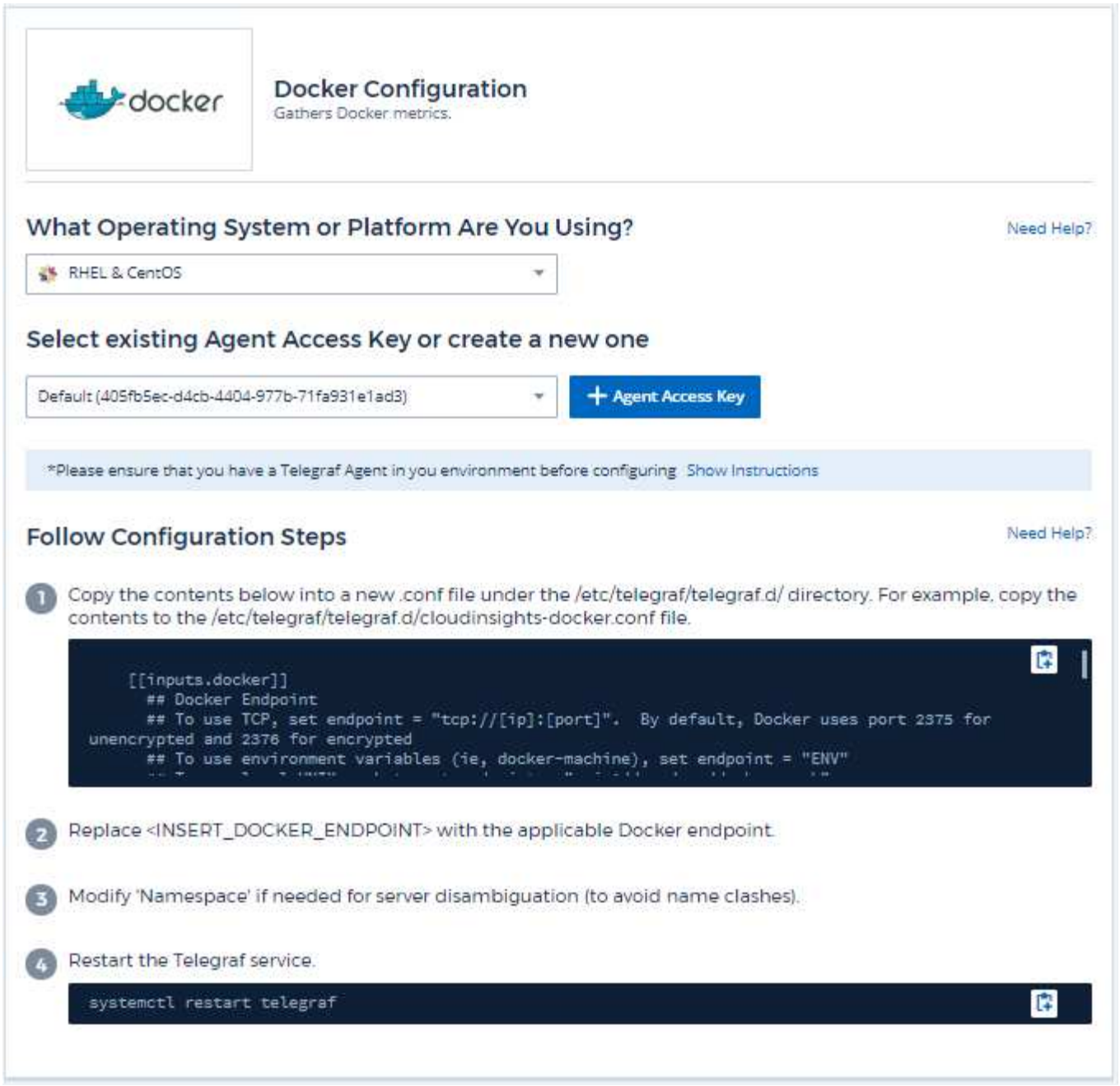
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Für Docker:

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert "Installieren Sie einen Agenten" Ihrer Umgebung zu unterstützen.

   Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen im Bildschirm Docker-Konfiguration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Telegraf-Input-Plug-in für Docker erfasst Kennzahlen über einen bestimmten UNIX-Socket oder einen TCP-Endpunkt.

Kompatibilität

Die Konfiguration wurde mit Docker Version 1.12.6 entwickelt.

Einrichtung

Zugriff auf Docker über einen UNIX-Socket

Wenn der Telegraf-Agent auf bareMetal läuft, fügen Sie den telegraf Unix-Benutzer zur Docker Unix-Gruppe hinzu, indem Sie Folgendes ausführen:

```
 sudo usermod -aG docker telegraf
Wenn der Telegraf-Agent in einem Kubernetes Pod ausgeführt wird, legen Sie
den Docker Unix-Socket offen, indem Sie den Socket als Volume in den POD
einbilden und das Volume dann in /var/run/docker.sock mounten. Fügen Sie
zum Beispiel der PodSpec Folgendes hinzu:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Fügen Sie dann dem Container Folgendes hinzu:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Beachten Sie, dass das Installationsprogramm von Data Infrastructure Insights für die Kubernetes-Plattform diese Zuordnung automatisch übernimmt.

Zugriff auf Docker über einen TCP-Endpunkt

Docker verwendet standardmäßig Port 2375 für unverschlüsselte Zugriffe und Port 2376 für verschlüsselten Zugriff.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Engine	Docker Engine Für Namespace	Node Name Node-IP-Node-UUID Node OS Kubernetes Cluster Docker-Versionseinheit	Speichercontainer Container verwendete Container ausgeführt Container gestoppt CPUs Gehroutinen Bilder Listener Ereignisse verwendete Datei Deskriptoren Daten verfügbar Daten insgesamt verwendete Metadaten Verfügbare Metadaten insgesamt verwendete Pool Blocksize

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container	Namespace Container-Name Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes Container-Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes IO Config Kubernetes IO-Konfiguration gesehen Kubernetes IO-Konfiguration Quelle OpenShift IO SCC Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Kompose Service Pod Vorlage Hash Controller Revision Hash Pod Vorlage Erstellung Lizenz Schema Build Date Schema Lizenz Schema Name Schema URL Schema VCS URL Schema Vendor Schema Version Schema Schema Schema Version Maintainer Customer Pod Kubernetes StatefulSet Pod Name Tenant WebConsole Architektur autoritäre Quelle URL Build Datum RH Build Host RH Component Distribution Scope Installation Release Run Zusammenfassung Uninstall Ref Type Vendor Version Health Status	Speicher Aktiv Anonymer Speicher Aktiv Speicher Cache Hierarchischer Grenzwert Speicher Inaktiver Anonymer Speicher Inaktiver Speicher Speicherlimit Arbeitsspeicher Gemappter Speicher Max Nutzung Speicherseitenfehler Speicherseite Hauptfehler Speicher Im Speicher Ausgepeitet Speicher Resident Set Größe Speicher Resident Set Größe Riesige Speicher Gesamt Aktiv Anonymer Speicher Gesamt Active File Memory Gesamt Cache Speicher Inaktiver Anonymer Speicher Gesamt Inaktiver Speicher Gesamt Mapped File Memory Total Page Fault Memory Total Page Major Fehler Memory Total Paged In Memory Total Paged Out Memory Total Resident Set Größe Speicher Gesamt Resident Set Größe Riesige Speicher Gesamt Nicht entfernen Speicher nicht entfernen Speichernutzung Speichernutzung Prozent Exit Code OOM tötete PID bei fehlender Streak gestartet

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Block IO	Namespace Container Name Device Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes Container-Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes Config Kubernetes Config gesehen Kubernetes Config Quelle OpenShift SCC Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Schema Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema Lizenz Schema Name Schema Vendor Customer Pod Kubernetes StatprofSet Pod Name Tenant WebConsole Build Date License Vendor Architecture authorited Source URL RH Build Host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Typ Version Schema URL Schema VCS Schema Version Container ID	IO Service Bytes rekursiv Async IO Service Bytes rekursiv IO lesen Service Bytes rekursiv Sync IO Service Bytes rekursiv IO Service Bytes rekursiv Schreib IO Serviced rekursive Async E/A Serviced rekursive Read IO Serviced rekursive Sync IO Serviced rekursive Total IO Serviced rekursive Write

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX-reduzierte RX-Bytes RX-Fehler RX-Pakete TX reduzierte TX-Bytes TX-Fehler TX-Pakete

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container-CPU	Namespace Container Name CPU Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Kubernetes-Konfiguration Kubernetes-Konfiguration Kubernetes-KonfigurationSCC-Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes-Container-Name Kubernetes Docker Typ Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Node OS Kubernetes Cluster Docker Version Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema License Schema Name Schema Hersteller-Pod Kubernetes StatprofSet Pod Name Tenant WebConsole Build Date License Vendor Architecture authorited Source URL RH Build Host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Typ Version Schema URL Schema VCS Schema VCS URL Schema Version Container ID	Drosselungszeiträume Drosselung Gedrosselte Perioden Drosselung Gedrosselte Zeitnutzung Im Kernel-Modus Nutzung Im Benutzermodus Auslastung Prozent Nutzung Des Systems Gesamt

Fehlerbehebung

Problem:	Versuchen Sie dies:
Ich sehe meine Docker-Kennzahlen in Data Infrastructure Insights nicht, nachdem ich die Anweisungen auf der Konfigurationsseite befolgt habe.	Prüfen Sie die Telegraf-Agentenprotokolle, um zu sehen, ob es folgenden Fehler meldet: E! Fehler im Plugin [inputs.docker]: Berechtigung verweigert beim Versuch, eine Verbindung zum Docker Daemon-Socket herzustellen.Falls dies der Fall ist, ergreifen Sie die erforderlichen Schritte, um den Telegraf-Agent-Zugriff auf den Docker Unix-Sockel wie oben angegeben zu ermöglichen.

Weitere Informationen finden Sie im "Unterstützung" Seite.

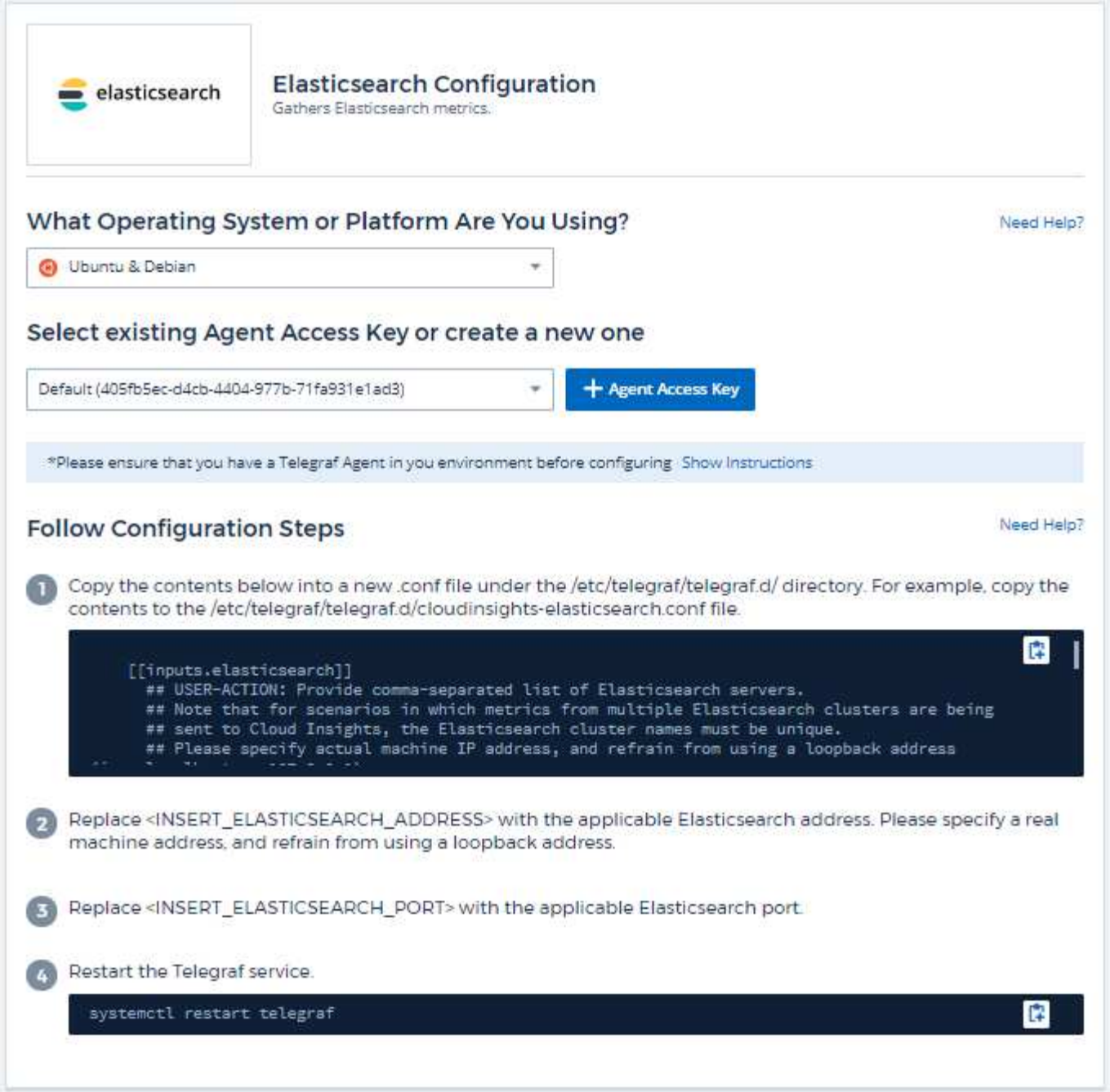
Elasticsearch Data Collector

Data Infrastructure Insights verwendet diesen Datensammler zum Erfassen von Kennzahlen aus Elasticsearch.

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Elasticsearch.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Elasticsearch-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Cluster	Namespace-Cluster	Node-IP Node-Name Cluster-Status	Gesamtknotenanzahl Gesamtknotenanzahl Dateidatenmenge (Bytes) Dateidatenfreiwert (Bytes) Dateisystem-Daten gesamt (Bytes) JVM Threads BS zugewiesene Prozesse Betriebssystem Verfügbare Prozessoren Betriebssystem Mem Free (Bytes) Betriebssystem Mem Free OS Mem Total (Bytes) verwendetes Betriebssystem Mem verwendeter Prozess CPU Indexes Abschlussgröße (Bytes) Indizes Anzahl Indizes Indexen Anzahl Indizes Indizes Docs gelöschte Indizes Feld Datendiktionen Indices Field Data Memory Size (Bytes) Indizes Abfrage Cache-Anzahl Indizes Cache Größe Indizes Anzahl Segmente Anzahl Indizes Segmente Doc Values Speicher (Bytes) Indizes Shards Index Primärarten AVG Indizes Shards Index Primärindizes Indizes Max Indizes Shards Index Primärindizes Index Indizes Min Indizes. Indizes Shards Index Replication Avg Indizes Shards Index Replication Max Indizes Shards Index Replikation Min Indizes Shards durchschn. Indizes Shards Max Indizes Shards Primaries Indizes Indizes Shards Replication Indizes Shards Storage-Größe (Bytes)

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Node	Namespace Cluster es Node ID es Node IP es Node	Zone-ID	Machine Learning Enabled Machine Learning Memory Machine Learning Max Open Jobs X-Pack installierte Breakers Accounting Estimated Size (Bytes) Breakers Accounting Limit Size (Bytes) Breakers Accounting Overhead Breakers Accounting Tripped Breakers Field Data Estimated Size (Bytes) Breakers Field Data Overhead Breakers Field Data Tripped Breakers Field Data Breakers Field Data Stimulated Size (Bytes) Breakers in-Flight Limit Size (Bytes) Breakers in-Flight Overhead Breakers in-Flight Dripped Breakers Parent Estimated Size (Bytes) Breakers Parent Limit Size (Bytes) Breakers Parent Overhead Breakers Parent Tripped Breakers Request Estimated Size (Bytes) Breakers Request availed Filesystem Data available (Bytes) Filesystem Data Free (Bytes) Filesystem Data Total (Bytes) Dateisystem IO Stats Devices Ops Filesystem IO Stats Devices (kb) Schreib-I/O-Stats-Geräte Lese-Ops-Filesystem IO Statistik-Geräte EITE (kb) Dateisystem IO Stats Devices Write Ops Dateisystem IO Stats Total Ops Filesystem IO Stats Total Read (kb) Filesystem IO Stats Read Ops-Filesystem – IO-Statistik (KB) Dateisystem-IO-Stats-Write-Ops-Filesystem Least Usage Estimate Available (Bytes)

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Flik Data Collector

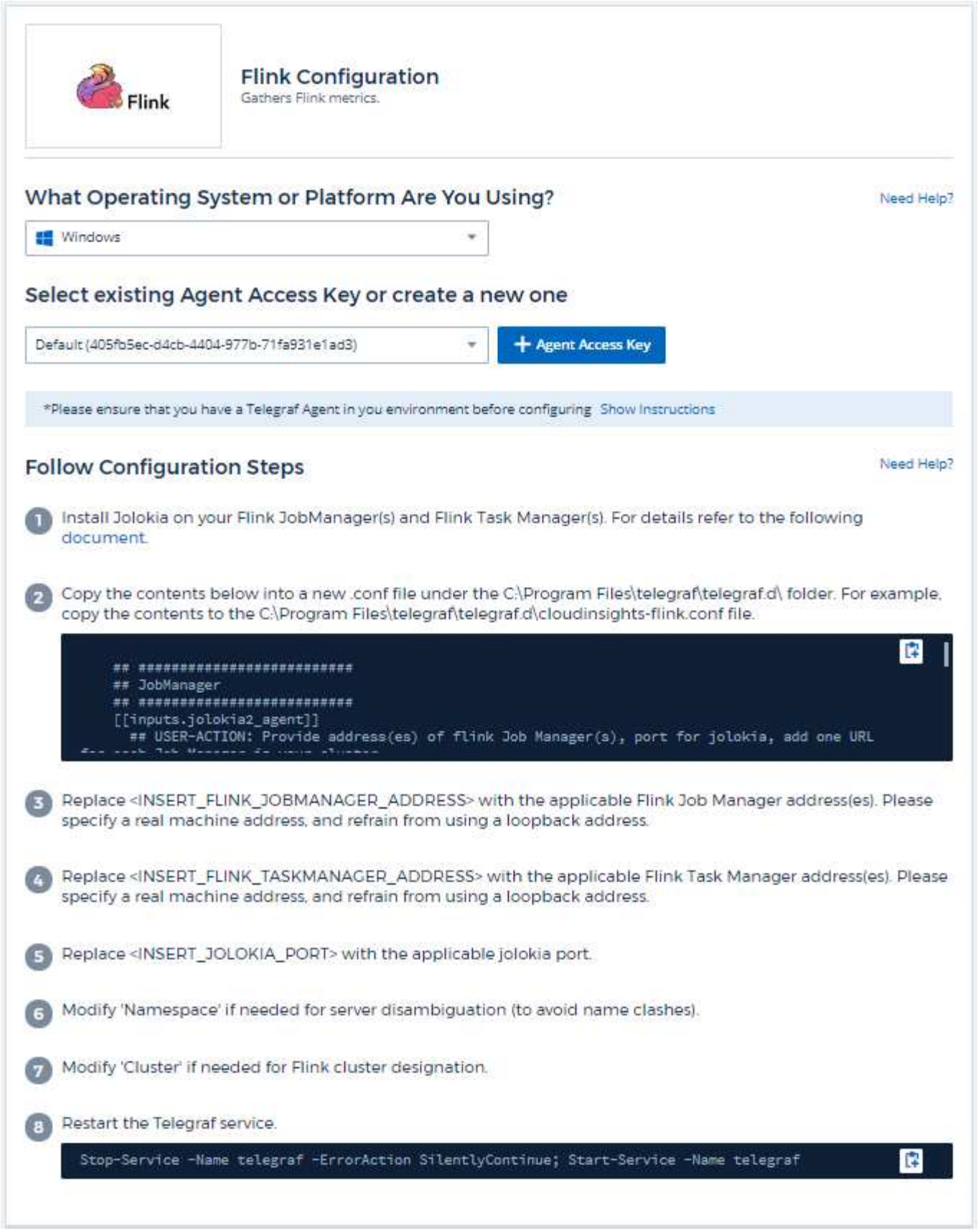
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Flink zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie „Flink“.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Eine vollständige Flink-Implementierung umfasst die folgenden Komponenten:

JobManager: Das Primärsystem Flik. Koordiniert eine Reihe von TaskManagers. In einer Konfiguration mit hoher Verfügbarkeit verfügt das System über mehr als einen JobManager. Taskmanager: Hier werden Flik-Operatoren ausgeführt. Das Flink Plugin basiert auf dem telegraf Jolokia Plugin. Als Voraussetzung für die Erfassung von Informationen aus allen Flik-Komponenten muss JMX auf allen Komponenten konfiguriert und über Jolokia freigelegt werden.

Kompatibilität

Die Konfiguration wurde gegen die Version 1.7 von Flink entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war "Jolokia Agent 1.6.0".

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/flink/lib/' platziert wird.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia API freigegeben wird, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den JobManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Taskmanager

So konfigurieren Sie TaskManager(s), um die Jolokia-API zu öffnen, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den TaskManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Manager	Cluster Namespace-Server	Node Name Task-Manager-ID-Knoten-IP	Netzwerk verfügbar Speichersegmente Netzwerk Speichersegmente Speichersegmente Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Thread Count Daemon Thread Count Thread Count Spitzenanzahl Thread Count Thread Count Insgesamt Gestartet
Druckauftrag Einflken	Job-ID des Cluster-Namespace-Servers	Node Name Job Name Node-IP Letzte Checkpoint External Path-Neustartzeit	Ausfall Vollneustarts Last Checkpoint Alignment Buffered Last Checkpoint Duration Last Checkpoint Size Anzahl der abgeschlossenen Checkpoints Anzahl der fehlgeschlagenen Checkpoints Anzahl der laufenden Checkpoints Anzahl der Kontrollpunkte Betriebszeit

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Job Manager	Cluster Namespace-Server	Node Name Node-IP	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scravenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Number Registrierte Task-Manager Anzahl laufende Jobs Taskleisten verfügbare Task-Steckplätze Gesamt-Thread-Anzahl Daemon-Thread-Anzahl Maximale Anzahl Der Threads Anzahl Der Threads Insgesamt Begonnen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik-Aufgabe	Cluster Namespace Job-ID Task-ID	Server Node Name Job Name Sub Task-Index Task-Versuch-ID Task-Versuch Nummer Task-Name Task-Manager-ID Knoten-IP Aktuelle Eingabe-Wasserzeichen	Puffer in Pool Nutzung Buffers in Warteschlange Länge Buffer Out Pool Nutzung Buffer Out Queue Länge Anzahl Puffer in Lokale Anzahl Buffers in Local per Second Anzahl Puffer in Local per second Rate Anzahl Puffer in Remote Number Buffers in Remote per second Anzahl Puffer in Remote per second Anzahl der Puffer in Remote per Anzahl Der Auspuffer Anzahl Der Auspuffer Pro Sekunde Anzahl Auspuffer Pro Sekunde Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokale Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Remote Number Bytes In Remote Per Second Anzahl Bytes In Remote Pro Sekunde Rate Anzahl Bytes Out Anzahl Bytes Out Pro Sekunde Anzahl Bytes Out Pro Sekunde Anzahl Datensätze In Number Datensätze In Per Second Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Pro Sekunde

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Operator	Cluster Namespace Job-ID Operator-ID Task-ID	Server Node Name Job Name Operator Name Sub Task-Index Task-Versuch-ID Task-Versuch-Nummer Task-Name Task-Manager-ID-Knoten-IP	Aktuelle Eingabe Watermark Current Output Watermark Number Records In Number Records In Per Second Count Anzahl Datensätze In Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Anzahl Datensätze Aus Pro Sekunde Anzahl Verspätete Datensätze Verworfen Zugewiesene Partitionen Bytes Verbrauchte Rate Commit Latenz Durchschn. Commit-Latenz Max. Commit Rate Commits faciert fehlgeschlagene Verbindungen Close Rate Verbindungsanzahl Verbindungserzeugung Rate Anzahl Abholen Latenz durchschn. Abholen Max. Abholen Rate Abholen Größe Max. Abholen Drosselzeit durchschn. Abrufdauer Max. Heartbeat Rate Incoming Byte Rate I/O-Zeit durchschn. (Ns) I/O Wartezeit I/O Wartezeit durchschn. (Ns) Verbindungsrate Verbindungszeit durchschn. Letzter Heartbeat ago Netzwerk-I/O-Rate ausgehende Byte-Datensätze verbrauchte Rate Datensätze lag max. Datensätze pro Anforderung durchschn. Anfragemgröße Durchschnittl. Anfragengröße max. Ansprechrate Wählen Rate Synchronisierungszeit durchschn. Heartbeat Antwort Zeit Max. Verbindungszeit Max. Synchronisierungszeit

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Hadoop Data Collector

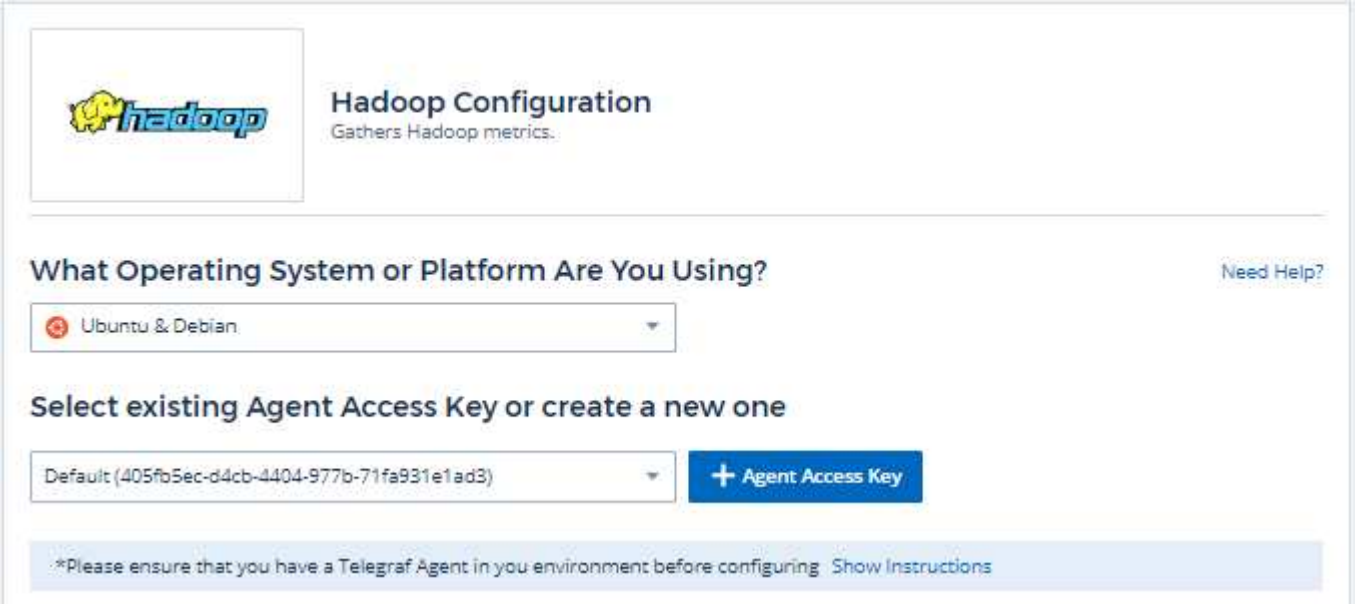
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus Hadoop zu sammeln.

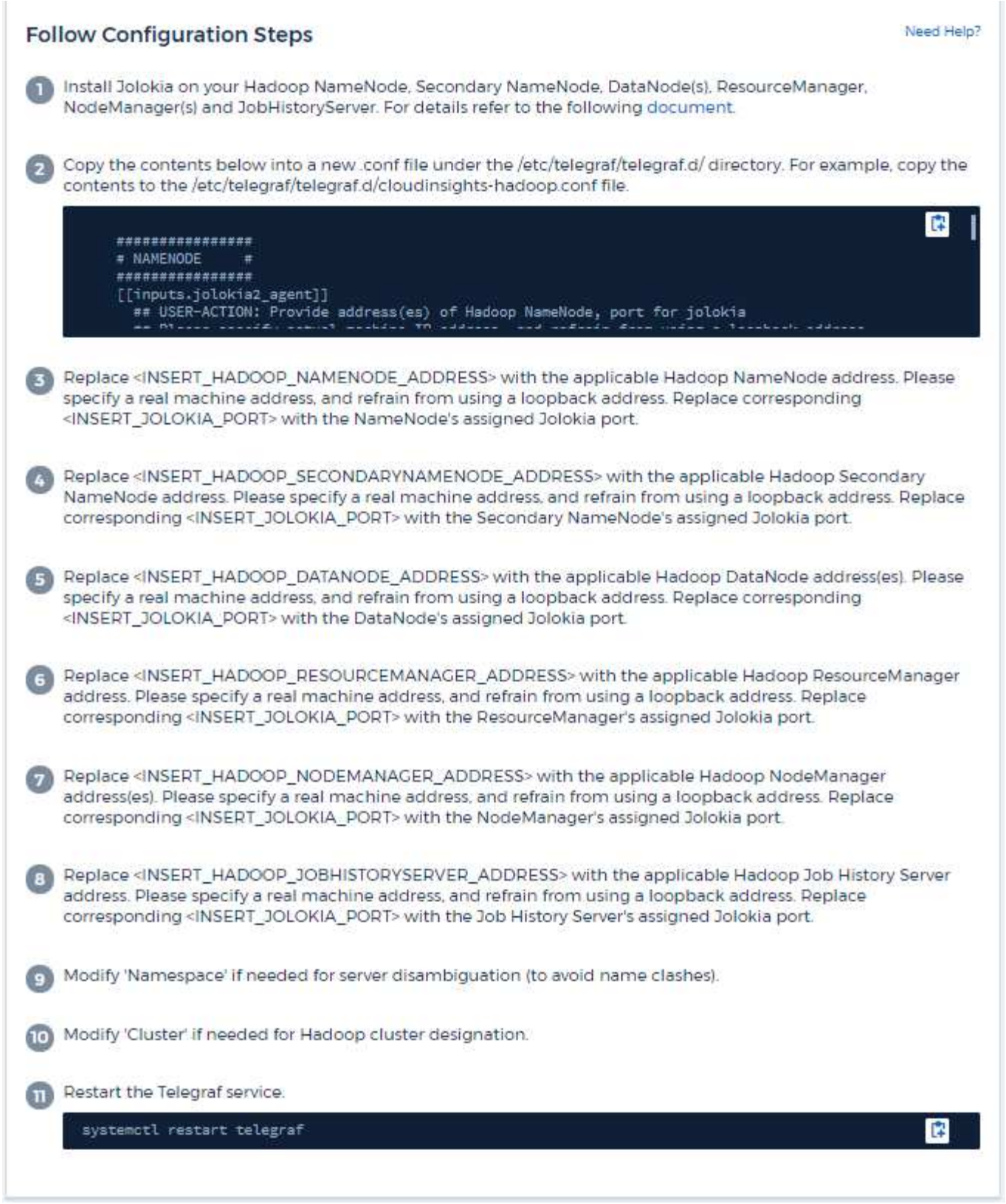
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Für Hadoop.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.





Einrichtung

Eine vollständige Hadoop Implementierung umfasst die folgenden Komponenten:

- NameNode: Das primäre System Hadoop Distributed File System (HDFS) Koordiniert eine Reihe von DataNodes.

- Sekundärer NameNode: Ein warmer Failover für den NameNode. In Hadoop erfolgt die Heraufstufung auf NameNode nicht automatisch. Secondary NameNode sammelt Informationen von NameNode, damit sie bei Bedarf heraufgestuft werden können.
- DataNode: Tatsächlicher Eigentümer von Daten.
- ResourceManager: Das primäre Computersystem (Yarn). Koordiniert eine Reihe von NodeManagers.
- NodeManager: Die Ressource für Computing. Aktueller Speicherort für das Ausführen von Anwendungen.
- JobHistorieServer: Verantwortlich für die Bearbeitung aller Anfragen im Zusammenhang mit der Jobhistorie.

Das Hadoop Plugin basiert auf dem telegraf Jolokia Plugin. Um Informationen aus allen Hadoop Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Die Konfiguration wurde mit Hadoop Version 2.9 entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war "Jolokia Agent 1.6.0".

Die nachfolgende Anleitung setzt voraus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter der Adresse '/opt/hadoop/lib/' abgelegt wird.

NameNode

Um NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie unter <HADOOP_HOME>/etc/hadoop/hadoop-env.sh Folgendes einrichten:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Sekundärer NameNode

Um den sekundären NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

DataNode

Um die DataNodes so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager

Um den ResourceManager so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

NodeManager

Um die NodeManagers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

JobGeschichteServer

Um den JobHistorieServer so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Sekundärer Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Compile Info Version	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info-Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NodeManager	Cluster Namespace-Server	Node Name Node-IP	Container Zugewiesener Speicher Zugewiesener Speicher Zuweisen Oportunistic Virtual Cores Allocchortunistic Virtual Cores Zugeordnete Speichernutzung Verfügbare Kerne Verfügbare Verzeichnisse Bad Lokale Verzeichnisse Bad Log Cache Größe Vor Clean Container Starten Dauer Durchschn. Dauer Container Starten Dauer Anzahl Operationen Container Abgeschlossen Container Container Container Container Container Container Inting Container Killed Containers Started Containers Container Reiniting Container gerollt zurück auf Fehler-Container ausgeführt Plattenauslastung gut Lokale Verzeichnisse Datenträgernutzung gut Log-Verzeichnisse Bytes gelöscht Private Bytes gelöscht Öffentliche Container mit opportunistischen Bytes gelöscht Gesamtanzahl Shuffle Verbindungen Shuffle Ausgabe Bytes Shuffle Outputs fehlgeschlagen Shuffle Outputs OK GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact Count GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact Time GC Gesamtdauer Extra Sleep Time Logs Anzahl Protokolle Fatal Count Protokolle Warnungszahl Speicher Heap Max

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop ResourceManager	Cluster Namespace-Server	Node Name Node-IP	AnwendungMaster-Startverzögerung durchschn. AnwendungMaster-Startverzögerung AnwendungMaster-Register Verzögerung durchschn. AnwendungMaster Register Verzögerung Nummer NodeManager Aktive Nummer NodeManager Decomissierte Nummer NodeManager Decomissioning Nummer NodeManager Lost Number NodeManager neu gestartet Nummer NodeManager Herunterfahren Nummer NodeManager Healthy Number NodeManager Memory Limit NodeManager Virtual Cores Limit used Capacity Active Applications Active Users Aggregierter Container Zugewiesene Aggregatcontainer Freigegebene Aggregate-Speicher Sekunden Ersatz Für Aggregat-Node Lokale Container Zugewiesene Aggregat-Aus Switch-Container Zugewiesenes Aggregat Ack Lokale Container Zugewiesenes Aggregat Virtuelle Kerne Sekunden Vorweggenommen Container Zugewiesener Speicher Zugewiesene Virtuelle Kerne Applikationsversuch Erster Container-Zuweisungsverzögerung Durchschn. Time Application-Versuch Erste Containerzuordnungsverzögerung Anzahl der Anwendungen Abgeschlossene Anwendungen Anwendungen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop DataNode	Cluster Namespace-Server	Node Name Node-IP Cluster-ID-Version	Transceiver-Anzahl überträgt in Bearbeitung Cache Kapazität Cache verwendete Kapazität DFS verwendete geschätzte Kapazität verloren Gesamt Letztes Volume Ausfall Rate Blöcke Anzahl gecachte Blöcke Anzahl fehlgeschlagener Cache-Blöcke Anzahl nicht in Cache-Blöcke Anzahl nicht übertragene Volumes Anzahl Restkapazität GC-Kopien Anzahl GC-Mark Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnschwellenwert überschritten GC-Zeit Kopieren GC-Zeit GC-Markierungen Sweep Compact Time GC Gesamt Extra Sleep Time Logs Anzahl Protokolle tödliche Anzahl Protokolle Info Anzahl Protokolle Warnungszahl Speicher Heap-Speicher Heap Max Speicher Heap verwendeter Speicher Max Speicher nicht Heap-belegt Speicher Nicht Heap Max Speicher Nicht Heap Verwendet Threads Blockiert Threads Neue Threads Runnable Threads Beendet Threads Timed Warting Threads Wartend

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Transaktions-ID Letzte geschriebene Zeit seit Letzte geladen Edits HA State File System Status Block Pool ID Cluster ID Compile Info unterschiedliche Version Anzahl Version	Block Kapazität Blöcke Gesamtkapazität genutzte Gesamtkapazität nicht DFS-Blöcke beschädigt geschätzte Kapazität verloren Gesamtblöcke Überschuss Herzschläge abgelaufen Dateien Gesamt File System Lock Queue Länge Blöcke fehlende Blöcke fehlende Replizierung mit Faktor 1 Clients Aktive Daten Knoten Dead Data Nodes Deaktivieren Dead Data Nodes Decommissioning Live Data Nodes Decomissieren Verschlüsselungszonen Anzahl Daten Knoten, die Wartungsdateien unter Baudaten Knoten eingeben in Wartung Daten Knoten leben in Wartung Daten Knoten Live-Speicher Inches Replikation Ausstehende Timeouts Datenknoten Nachricht Ausstehende Blöcke Ausstehende Löschblöcke ausstehende Replikationsblöcke Ausstehende Replikationsblöcke Ausstehende Replikationsblöcke mehrere verschobene Blöcke geplante Snapshot-Verzeichnisse Daten-Nodes veraltete Dateien Gesamt Last Sync Anzahl der gesamten Transaktionen seit letzten Checkpoint-Transaktionen seit Last Log Roll-Blocks UnderReplicated Volume Failures gesamte Synchronisierungszeiten Gesamtes Objekt Max Operationen hinzufügen Operationen Snapshots zulassen Batched Operations Block Queued Operations Block

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop JobGeschichteServer	Cluster Namespace-Server	Node Name Node-IP	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info-Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

HAProxy Data Collector

Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von HAProxy zu sammeln.

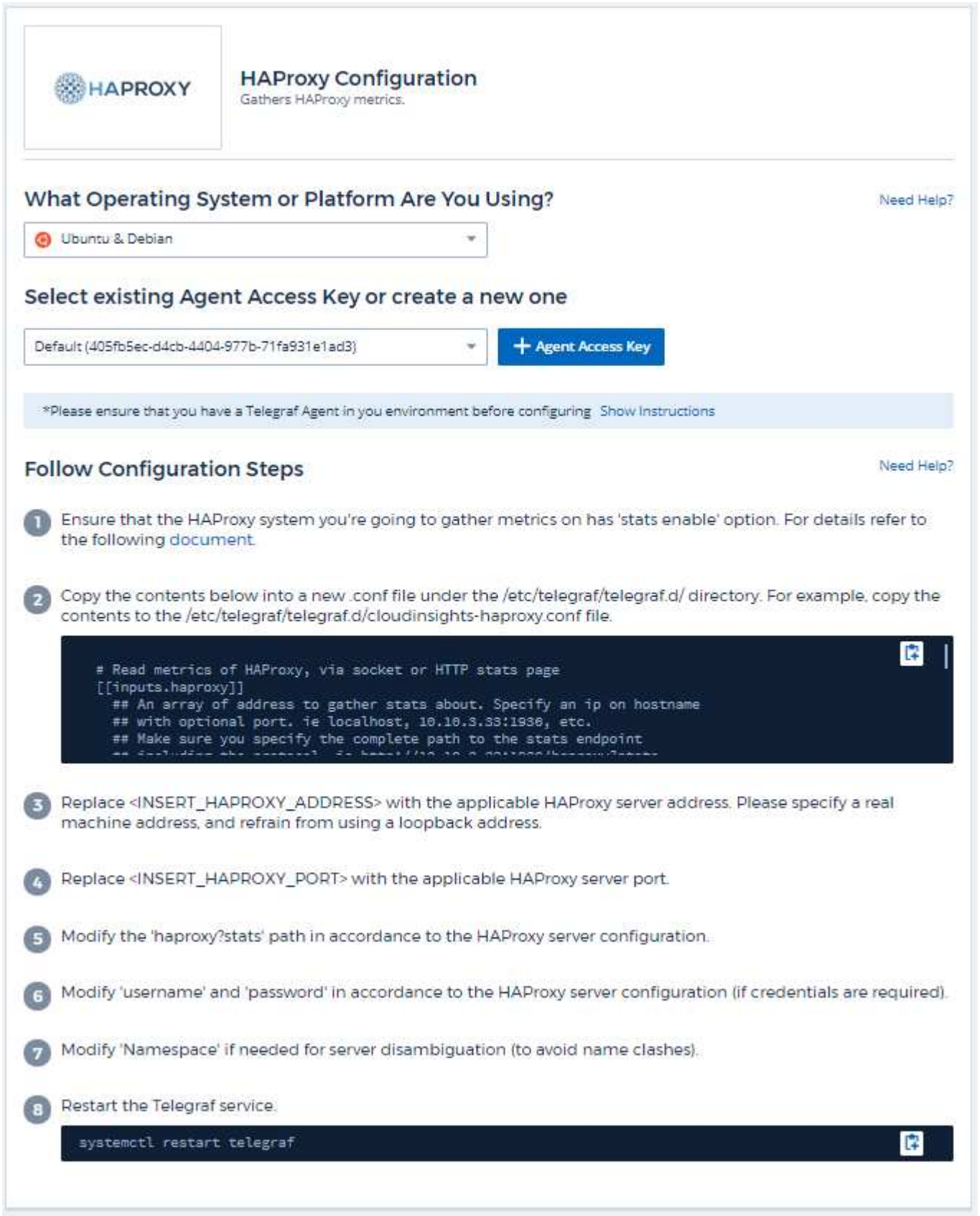
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie HAProxy.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Telegraf's Plugin für HAProxy setzt auf HAProxy Stats Aktivierung. Diese Konfiguration ist in HAProxy integriert, ist jedoch nicht sofort aktiviert. Wenn HAProxy aktiviert ist, wird ein HTML-Endpunkt angezeigt, der in Ihrem Browser angezeigt werden kann oder für die Extraktion des Status aller HAProxy-Konfigurationen abgekratzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen HAProxy-Version 1.9.4 entwickelt.

Einrichtung:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt 'Standards' die folgenden Zeilen hinzu: Verwenden Sie Ihren eigenen Benutzer/Ihr Passwort und/oder die haproxy-URL:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Im Folgenden finden Sie eine vereinfachte Beispiel-Konfigurationsdatei mit aktivierten Statistiken:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Vollständige und aktuelle Anweisungen finden Sie im "HAProxy-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy Frontend	Namespace-Adressenproproxy	Node-IP-Knotenname Proxy-ID-Modus Prozess-id Sitzungen Ratenlimit Server-id Sitzungen Limit Status	Bytes in Bytes Out Cache Hits Cache Lookups Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes Out Komprimierung Reaktionen Verbindungsrate Verbindungsrate Max Verbindungen insgesamt Anträge, die von der Verbindung abgelehnt werden Rule Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheitsbedenken Anfragen abgelehnt durch Session Rule Requests erfragt Fehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten andere Anfragen Abfangen Sitzungen Rate Sitzungen Max Anfragen Rate Max Anfragen Rate Max Anforderungen Total Sessions Sitzungen Max Sitzungen Antworten Neuschreibung Total Requests

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Server	Namespace-Adresse-Proxy-Server	Node-IP-Knotenname Check Time to Finish Check Fall Configuration Check Health Value Check RISE Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server Status Weight	Aktive Server Backup Server Bytes in Bytes Out Downs Check Downs Check Fails Client abgebrochen Verbindungen Verbindung Verbindung Durchschnittliche Zeit Ausfallzeit Gesamt Denied Responses Verbindungsfehler Antwort 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Durchschnittliche Zeit Sitzungen pro Zweite Sitzungen pro Sekunde Max. Wiederverwendbarkeit der Verbindung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max Server Transfer bricht Sitzungen gesamte Sitzungen Gesamtzeit Durchschnittliche Anforderungen Redispatches Anfragen Wiederholungen Anfragen Neuschreibung Anfragen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Back-End	Namespace-Adressenproproxy	Node-IP-Node-Name Proxy-ID Letzte Änderung Zeit Letzte Sitzung Zeitmodus Prozess-id Server-id Sitzungen Limit Status Gewicht	Aktive Server Backup Server Bytes in Bytes Out Cache Aufrufe Cache Lookups überprüfen Downs Client abbricht Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes out Komprimierungsantworten Verbindung Durchschnittliche Zeit Ausfallzeit Total Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheit Bedenken Verbindungsfehler Antworten Reaktion 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Warteschlange Durchschnittliche Zeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamt Verbindungswiederverwendung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragung Abtreibungen Sitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Anträge Neu Schreiben

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

JVM Data Collector

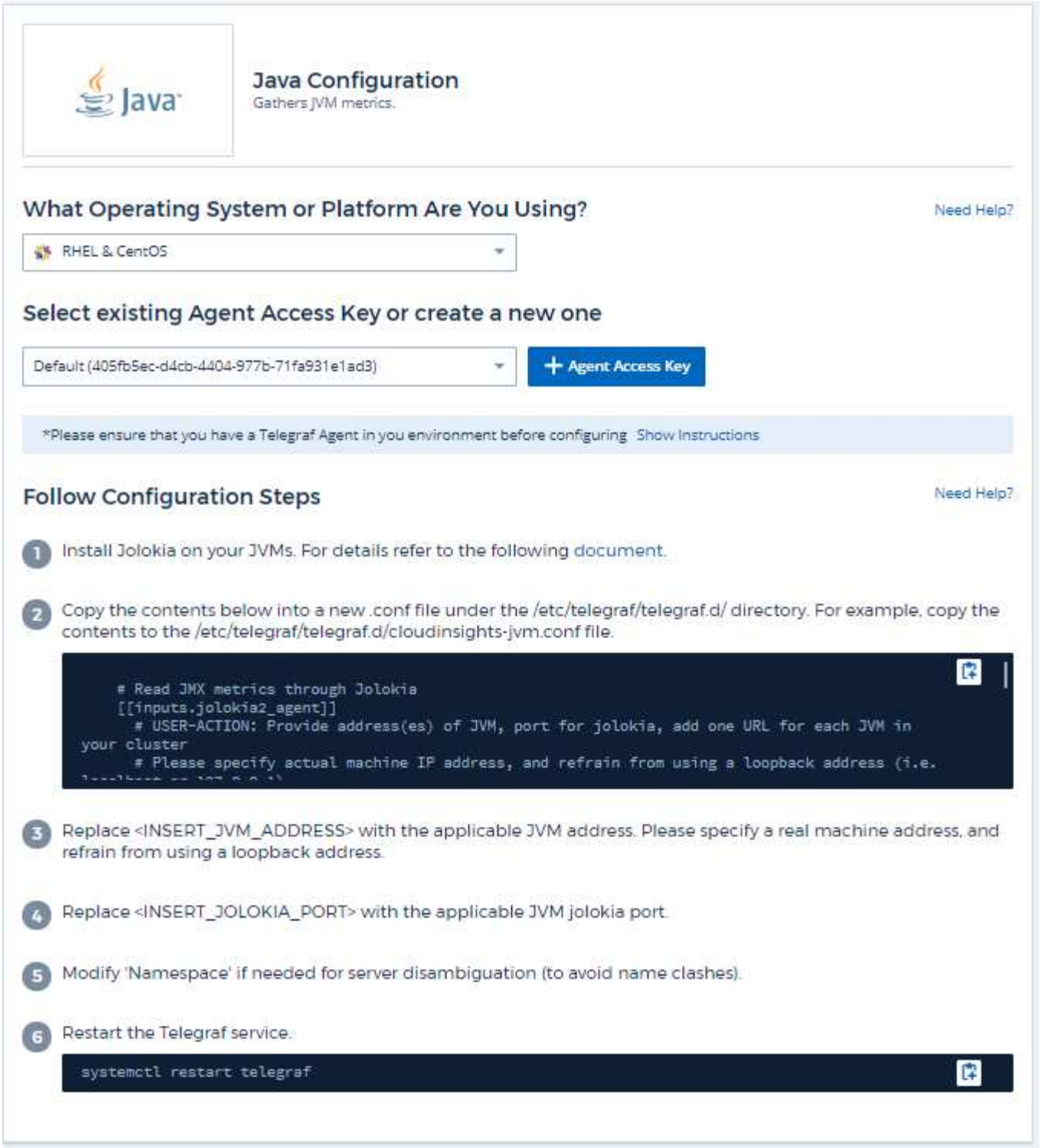
Data Infrastructure Insights verwendet diesen Datensammler zur Erfassung von Kennzahlen aus JVM.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie JVM.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "JVM-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
JVM	Namespace-JVM	OS Architektur OS Name OS Version Laufzeit Spezifikation Laufzeit Spezifikation Hersteller Laufzeit Spezifikation Version Uptime Laufzeit VM Name Laufzeit VM Anbieter Laufzeit VM Version Node Name Node IP	Class Loaded Class Loaded Class Memory Unloaded Memory Heap Init Memory Heap used Max Memory Heap Used Memory Non Heap Innit Memory Non Heap Max Memory nicht Heap Used Memory Objects Ausstehende Fertigstellung von Betriebssystemprozessoren verfügbar Betriebssystem engagierte virtuelle Speichergröße OS Kostenlos Physikalische Speichergröße OS Freier Swap Speicherplatz Größe OS Max Datei Descriptor Anzahl OS Open File Descriptors Anzahl Betriebssystem Prozessor CPU Load OS CPU Time OS System CPU Load OS System Load Average OS Gesamt Physical Memory Size OS Gesamt Swap Space Size Thread Daemon Anzahl der Threads Spitzenanzahl Thread Count Thread Total Started Count Garbage Collector Copy Collection Count Garbage Collector Copy Collection Time Garbage Collector Sammlung von Mark-Sweep Sammlungszeit Zeitabfälle Collector G1 Sammlung der Alten Generation Speicherbage Collector G1 Zeitabbage der Jungen Generation Sammlungszähler Garbage Collector G1 Young Generation Collection Time Garbage Collector Zeitabfälle Sammlung der aktuellen Mark-Sweep Sammlung Zeitgarage Collector Parallel Collection Count Garbage Collector Parallel

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Kafka Data Collector

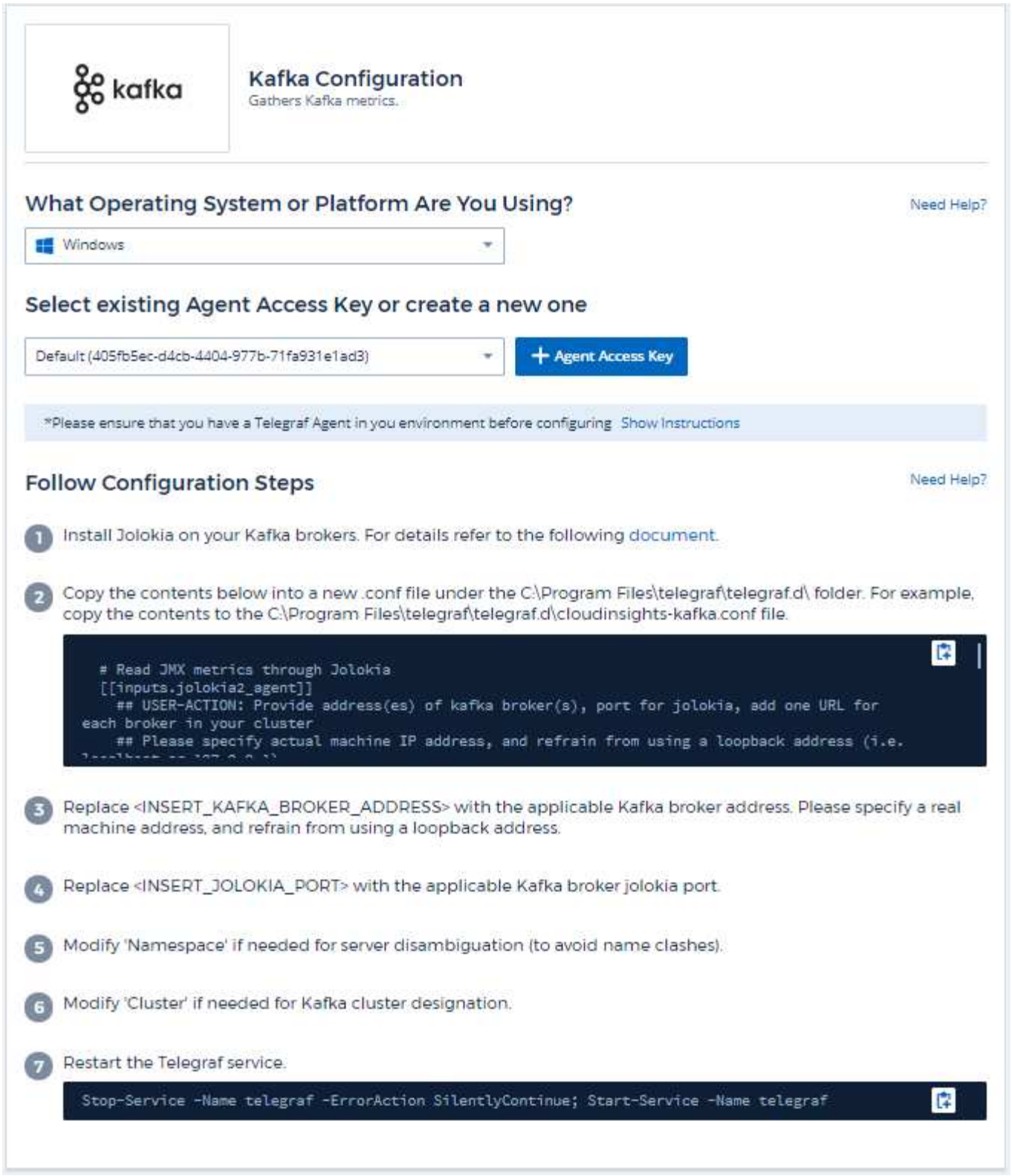
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen aus Kafka zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kafka.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Kafka Plugin basiert auf dem telegraf's Jolokia Plugin. Um Informationen aus allen Kafka-Brokern zu sammeln, muss JMX über Jolokia auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Konfiguration wurde gegen Kafka Version 0.11.0 entwickelt.

Einrichtung

Alle Anweisungen unten Nehmen wir an, dass Ihr Installationsort für kafka '/opt/kafka' ist. Sie können die nachfolgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version die Jolokia Agent jar-Datei muss sein "Heruntergeladen". Die gegen die Version getestete war Jolokia Agent 1.6.0.

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/kafka/libs/' abgelegt wird.

Kafka Brokers

Um Kafka Brokers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie in <KAFKA_HOME>/bin/kafka-Server-Start.sh kurz vor dem Anruf „kafka-run-class.sh“ Folgendes hinzufügen:

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Beachten Sie, dass das obige Beispiel 'Hostname -i' verwendet, um die Umgebungsvariable 'RMI_HOSTNAME' einzurichten. In mehreren IP-Maschinen muss dies optimiert werden, um die IP, die Sie für RMI-Verbindungen interessieren, zu erfassen.

Sie können einen anderen Port für JMX (9999 oben) und Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss. Sie können die Option '-Dcom.sun.management.jmxremote.authenticate=false' verwenden, wenn Sie nicht authentifizieren möchten. Nutzung auf eigenes Risiko.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kafka Broker	Cluster Namespace Broker	Node Name Node-IP	Replikatmanager Fetcher Max Lag Zookeeper Client-Verbindungen Zookeeper Client-Verbindungen (15 m Rate) Zookeeper Client-Verbindungen (5 m Rate) Zookeeper Client-Verbindungen (mittlere Rate) Zookeeper Client-Verbindungen (1 m Rate) Anzahl der Threads des Replikatmanagers Anzahl der Threads Anzahl der Threads Anzahl der Threads Anzahl der aktuellen Lesevorgänge Anzahl der insgesamt gestarteten Offline-Partitionen Anfragen Gesamtzeit (50. Perzentil) Anfragen produzieren Gesamtzeit (75. Perzentil) Anfragen produzieren Gesamtzeit (98 Perzentil) Anfragen produzieren Gesamtzeit (999. Perzentil) Erstellen von Anfragen Gesamtzeit (9th Perzentil) Erstellen von Anfragen Gesamt Zeit produzieren Anfragen Gesamt Zeit produzieren Max produzieren Anfragen Gesamt Zeit Mittelwert produzieren Anfragen Gesamtzeit Min Erzeugungsanforderunge n Total Zeit Max Gesamtzeit Gesamt Zeit Stddev Replica Manager ISR reduziert Replikatmanager verkleinert ISR (15 m Rate) Replica Manager ISR reduziert (5 m Rate) Replica Manager ISR reduziert (Mittlere Rate) Replica Manager ISR-Shrink (1-m-Rate) Anforderung Handler durchschn. Leerlaufanfrage (15-m-Rate) Anforderung

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Kibana Data Collector

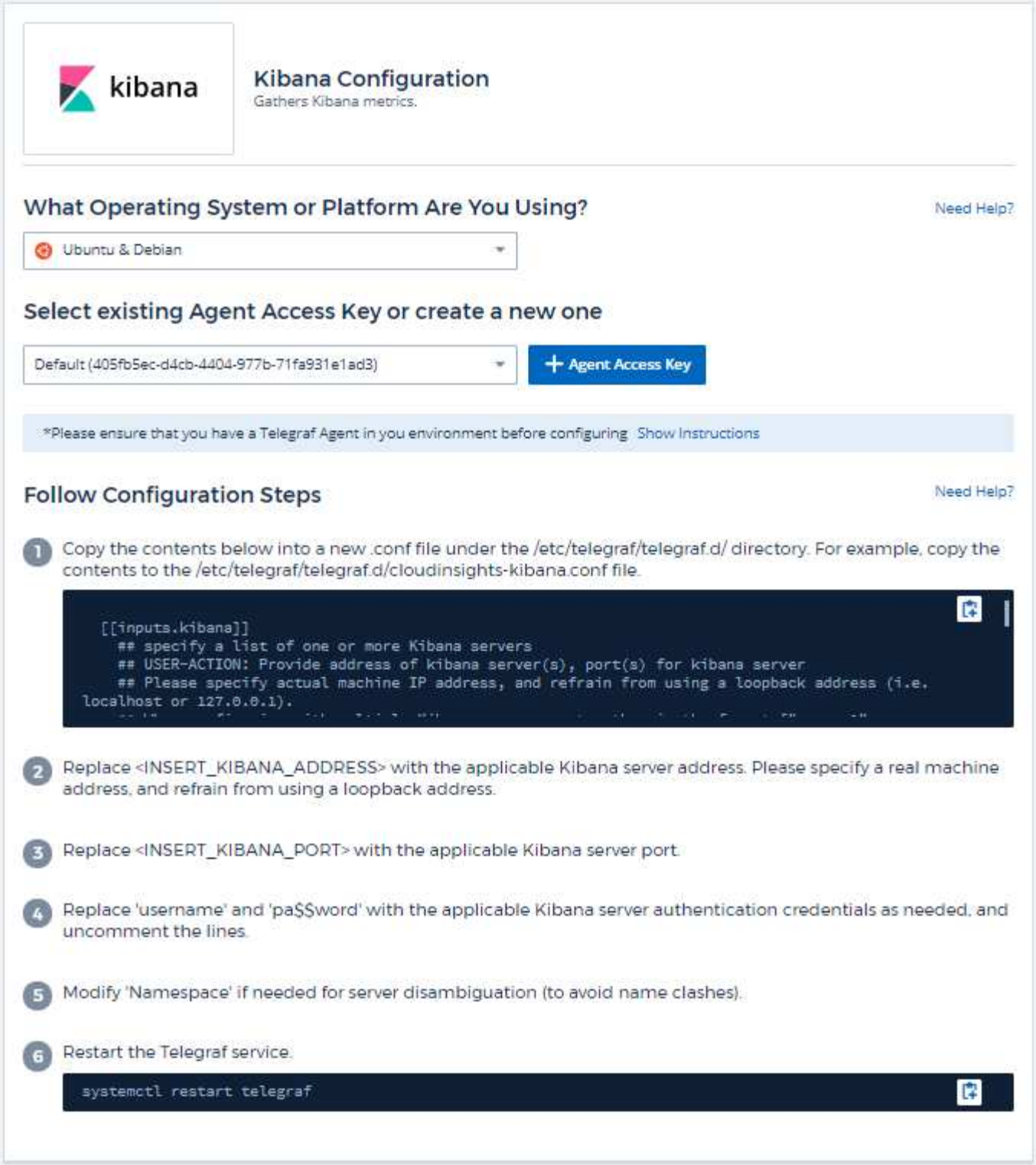
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Kibana zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kibana.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Kibana Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kibana	Namespace-Adresse	Versionsstatus des Node-IP-Node-Namens	Gleichzeitige Verbindungen Heap Max Heap verwendete Anforderungen pro Sekunde Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

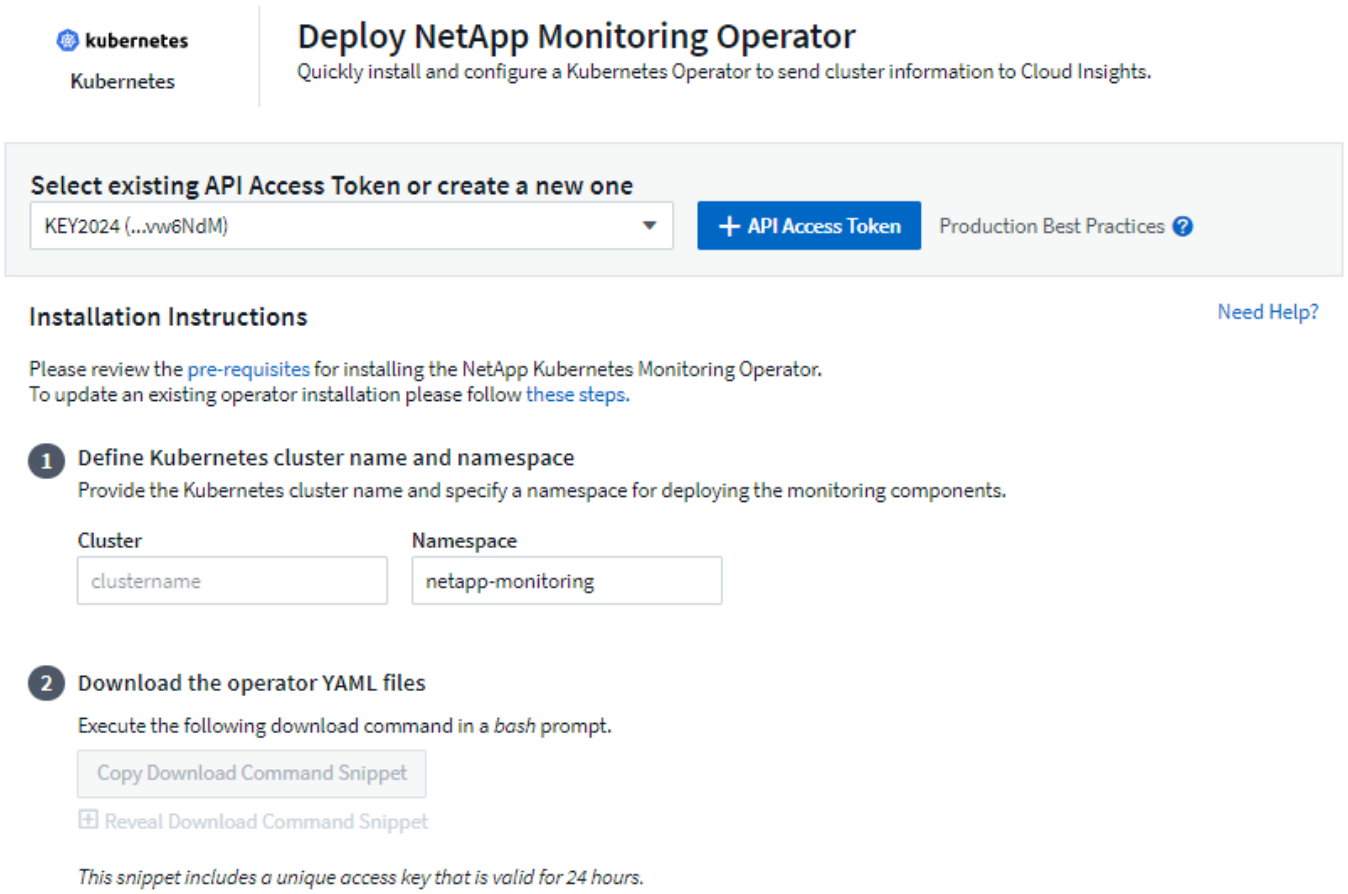
Installation und Konfiguration des Kubernetes Monitoring Operator

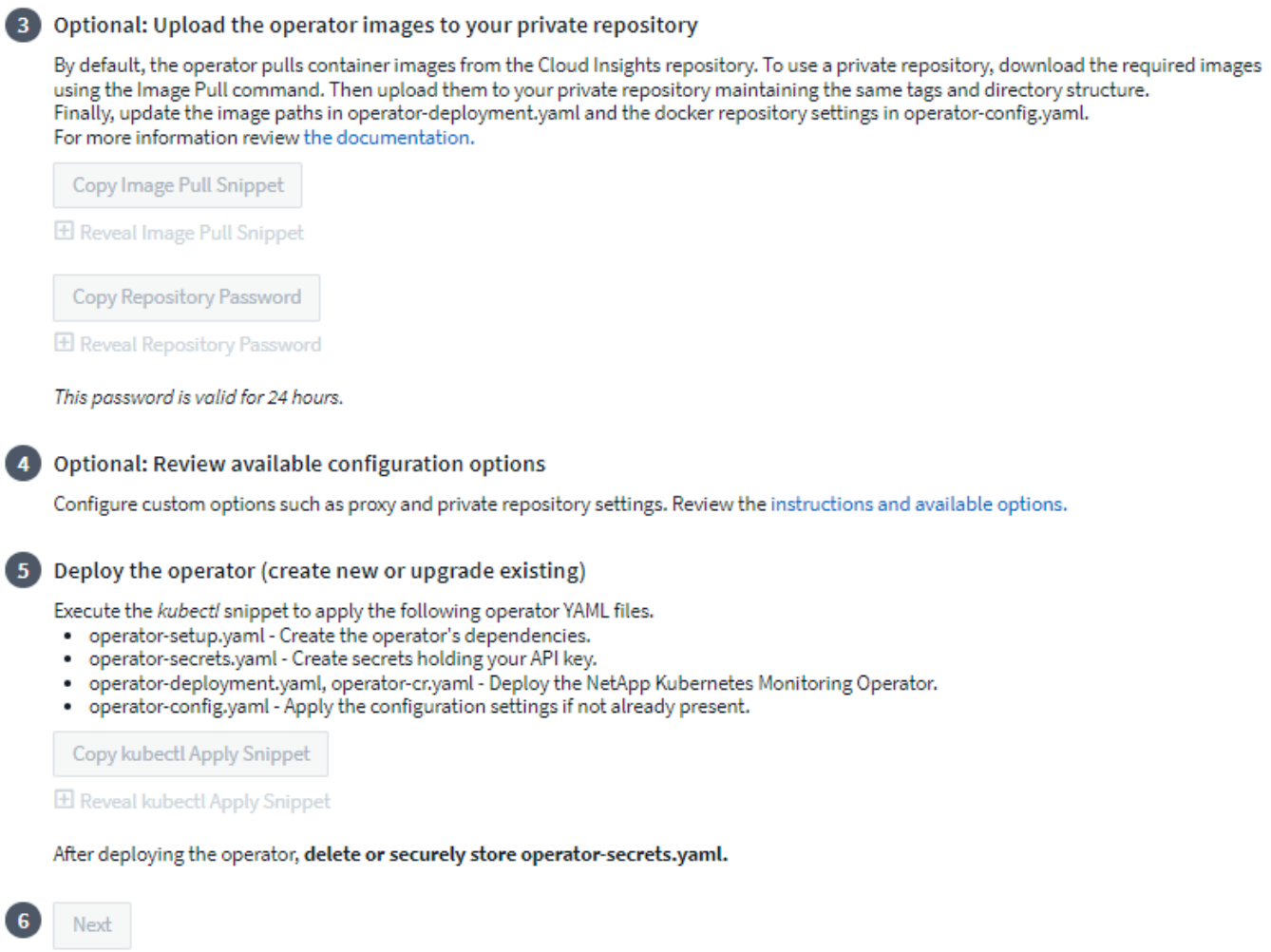
Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung an. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Bevor Sie den Kubernetes Monitoring Operator installieren

Siehe "Voraussetzungen" Dokumentation vor der Installation oder dem Upgrade des Kubernetes Monitoring Operator.

Installieren des Kubernetes Monitoring Operator





Schritte zum Installieren des Kubernetes Monitoring Operator Agent auf Kubernetes:

1. Geben Sie einen eindeutigen Cluster-Namen und einen eindeutigen Namespace ein. Wenn Sie es sind Aktualisierung Verwenden Sie aus einem früheren Kubernetes-Operator den gleichen Cluster-Namen und Namespace.
2. Sobald diese eingegeben wurden, können Sie den Download-Befehl-Snippet in die Zwischenablage kopieren.
3. Fügen Sie das Snippet in ein *bash* Fenster ein und führen Sie es aus. Die Installationsdateien des Bedieners werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und für 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie das optionale Bild-Pull-Snippet, fügen Sie es in eine *bash*-Shell ein und führen Sie es aus. Nachdem die Bilder gezogen wurden, kopieren Sie sie in Ihr privates Repository. Stellen Sie sicher, dass Sie dieselben Tags und Ordnerstrukturen beibehalten. Aktualisieren Sie die Pfade in *Operator-Deployment.yaml* sowie die Einstellungen des Docker-Repository in *Operator-config.yaml*.
5. Prüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen, z. B. Proxy- oder private Repository-Einstellungen. Sie können mehr über lesen "Konfigurationsoptionen".
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie den kubectl Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation wird automatisch ausgeführt. Klicken Sie anschließend auf die Schaltfläche „*Next*“.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche „*Next*“. Achten Sie darauf, auch die Datei *Operator-Secrets.yaml* zu löschen oder sicher zu speichern.

Wenn Sie einen Proxy verwenden, lesen Sie mehr über Proxy wird konfiguriert.

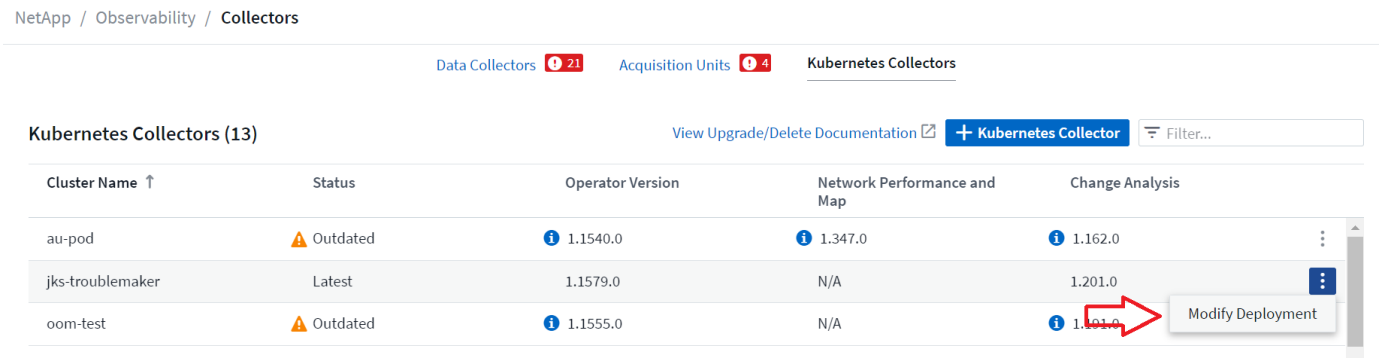
Wenn Sie über ein benutzerdefiniertes Repository verfügen, lesen Sie mehr über Ein benutzerdefiniertes/privates Docker-Repository verwenden.

Kubernetes-Monitoring-Komponenten

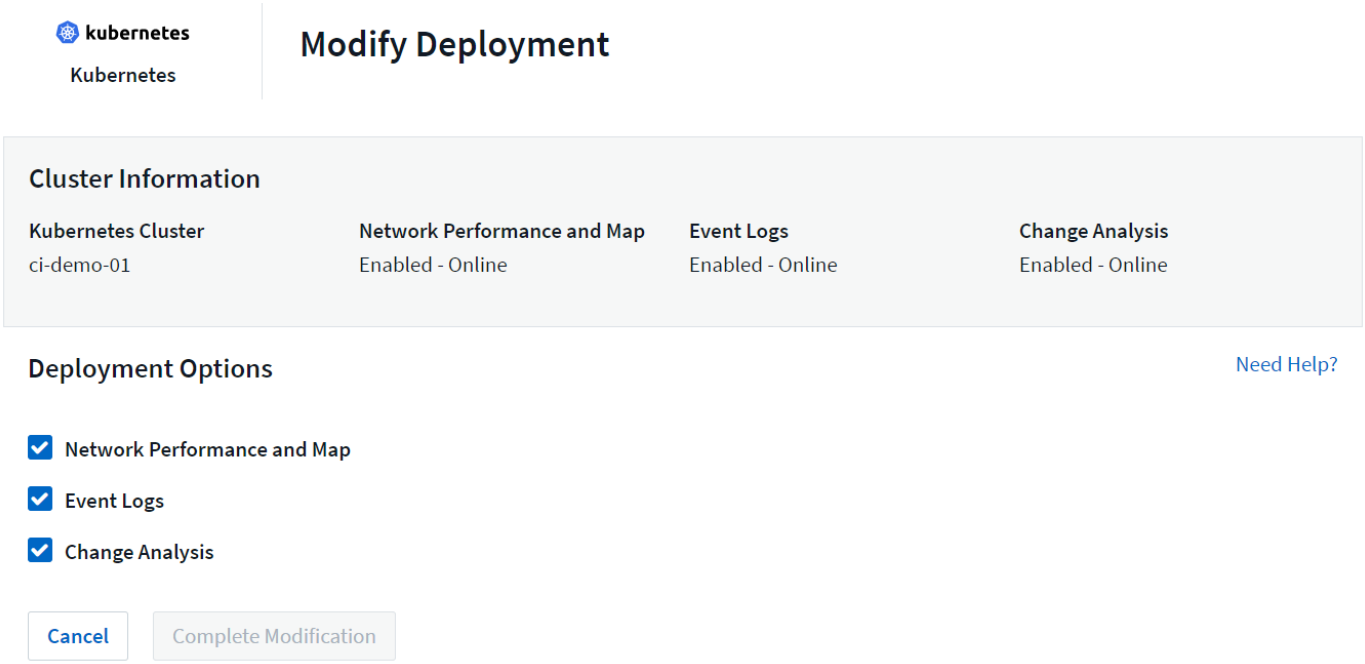
Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Monitoring-Komponenten:

- Cluster-Kennzahlen
- Netzwerkleistung und -Zuordnung (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben aufgeführten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie sich entscheiden, keine Komponente für einen bestimmten Collector zu benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Collector-Menü „drei Punkte“ rechts auf dem Bildschirm *Modify Deployment* auswählen.



Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht es Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.



Aktualisierung

Upgrade auf den neuesten Kubernetes Monitoring Operator

Ermitteln Sie, ob eine AgentConfiguration bei dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardwert *netapp-Monitoring* ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
Wenn eine AgentConfiguration vorhanden ist:
```

- Installieren Der letzte Operator über den vorhandenen Operator.
  - Stellen Sie sicher, dass Sie es sind Die neuesten Container-Bilder werden angezeigt Wenn Sie ein benutzerdefiniertes Repository verwenden.

Wenn AgentConfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Cluster-Namen (wenn Ihr Namespace nicht das standardmäßige NetApp-Monitoring ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Erstellen Sie eine Sicherung des bestehenden Operators (wenn Ihr
Namespace nicht der Standard-netapp-Überwachung ist, ersetzen Sie den
entsprechenden Namespace):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>> Der
vorhandene Operator.
* <<installing-the-kubernetes-monitoring-operator,Installieren>> Der
neueste Operator.
```

- Verwenden Sie denselben Cluster-Namen.
- Nachdem Sie die neuesten Operator YAML-Dateien heruntergeladen haben, können Sie alle in Agent_Backup.yaml gefundenen Anpassungen vor der Bereitstellung an den heruntergeladenen Operator-config.yaml übertragen.
- Stellen Sie sicher, dass Sie es sind Die neuesten Container-Bilder werden angezeigt Wenn Sie ein benutzerdefiniertes Repository verwenden.

Anhalten und Starten des Kubernetes Monitoring Operator

So beenden Sie den Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

Um den Kubernetes Monitoring Operator zu entfernen

Beachten Sie, dass der Standard-Namespace für den Kubernetes Monitoring Operator „netapp-Monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Überwachungsoperators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Wenn der Überwachungsoperator in seinem eigenen dedizierten Namespace bereitgestellt wurde, löschen Sie den Namespace:

```
 kubectl delete ns <NAMESPACE>
Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt, verwenden
Sie die folgenden Anweisungen, um ältere Versionen des
Überwachungsoperators zu deinstallieren.
```

Führen Sie jeden der folgenden Befehle in der Reihenfolge aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle Nachrichten ‘object not found’ zurückgeben. Diese Meldungen können sicher ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Sicherheitskontextbeschränkung erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert seine eigenen kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.

Informationen über Kube-State-Metrics finden Sie unter "Auf dieser Seite".

Konfigurieren/Anpassen des Bedieners

Diese Abschnitte enthalten Informationen zur Anpassung Ihrer Bedienerkonfiguration, zur Arbeit mit Proxy, zur Verwendung eines benutzerdefinierten oder privaten Docker-Repositorys oder zur Arbeit mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource bearbeiten, bevor Sie den Operator bereitstellen, indem Sie die Datei *Operator-config.yaml* bearbeiten. Diese Datei enthält kommentierte Beispiele für Einstellungen. Siehe Liste von "Verfügbare Einstellungen" Für die neueste Version des Bedieners.

Sie können diese Ressource auch bearbeiten, nachdem der Operator bereitgestellt wurde, indem Sie den folgenden Befehl verwenden:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Um festzustellen, ob die bereitgestellte Version des Operators
AgentConfiguration unterstützt, führen Sie den folgenden Befehl aus:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Wenn die Meldung „Fehler vom Server (notfound)“ angezeigt wird, muss Ihr
Bediener aktualisiert werden, bevor Sie die AgentConfiguration verwenden
können.
```

Proxy-Unterstützung Wird Konfiguriert

Es gibt zwei Stellen, an denen Sie einen Proxy in Ihrer Umgebung verwenden können, um den Kubernetes Monitoring Operator zu installieren. Es kann sich um dieselben oder separate Proxy-Systeme handelt:

- Proxy wird während der Ausführung des Installationscode-Snippets (mit „Curl“) benötigt, um das System zu verbinden, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights-Umgebung
- Der vom Kubernetes Ziel-Cluster benötigte Proxy für die Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur ist erforderlich

Wenn Sie einen Proxy für eine oder beide dieser Optionen verwenden, müssen Sie zur Installation des Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights-Umgebung möglich ist. Wenn Sie über einen Proxy verfügen und von dem Server/der VM, von dem aus Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, legen Sie vor der Installation des Operators die Umgebungsvariablen *http_Proxy/https_Proxy* fest. In einigen Proxy-Umgebungen müssen Sie möglicherweise auch die Variable *no_Proxy Environment* festlegen.

Um die Variablen festzulegen, führen Sie die folgenden Schritte auf Ihrem System aus * bevor* den Kubernetes Monitoring Operator installiert:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:
   a. Wenn der Proxy, der eingerichtet wird, keine Authentifizierung (Benutzername/Passwort) aufweist, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der Proxy, der eingerichtet wird, über Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie folgenden Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Wenn der Proxy, der für das Kubernetes-Cluster zur Kommunikation mit der Insights Umgebung Ihrer

Dateninfrastruktur verwendet wird, verwendet wird, installieren Sie den Kubernetes Monitoring Operator, nachdem Sie alle diese Anweisungen gelesen haben.

Konfigurieren Sie den Proxy-Abschnitt von AgentConfiguration in Operator-config.yaml, bevor Sie den Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker Repositorys

Standardmäßig zieht der Kubernetes Monitoring Operator Container-Images aus dem Repository Data Infrastructure Insights. Wenn Sie ein Kubernetes-Cluster als Ziel für das Monitoring verwenden und der Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder der Container-Registrierung zieht, müssen Sie den Zugriff auf die Container konfigurieren, die vom Kubernetes Monitoring Operator benötigt werden.

Führen Sie das „Image Pull Snippet“ aus der NetApp Monitoring Operator Installationskachel aus. Dieser Befehl meldet sich beim Repository Data Infrastructure Insights an, zieht alle Image-Abhängigkeiten für den Operator ab und meldet sich vom Repository Data Infrastructure Insights ab. Wenn Sie dazu aufgefordert werden, geben Sie das angegebene temporäre Repository-Passwort ein. Mit diesem Befehl werden alle vom Bediener verwendeten Bilder heruntergeladen, einschließlich optionaler Funktionen. Nachfolgend sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Core Operator-Funktionalität und Kubernetes Monitoring

- netapp Monitoring
- ci-kube-rbac-Proxy
- ci-ksm
- ci-telegraf

- Distroless-root-user

Ereignisprotokoll

- ci-Fluent-Bit
- ci-kubernetes-Event-Exporteur

Netzwerkleistung und -Zuordnung

- ci-Netz-Beobachter

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in das private/lokale/unternehmenseigene Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Images in Ihrem Repository mit denen im Data Infrastructure Insights Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Monitoring-Operators in Operator-Deployment.yaml, und ändern Sie alle Bildverweise, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie die AgentConfiguration in Operator-config.yaml, um die neue Position des Docker-Repo zu berücksichtigen. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher ausführen, müssen Sie die AgentConfiguration in *Operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift kann zusätzliche Sicherheitsstufen implementieren, die den Zugriff auf einige Kubernetes-Komponenten blockieren könnten.

Ein Hinweis über Geheimnisse

Um die Berechtigung für den Kubernetes Monitoring Operator zum Anzeigen der geheimen Daten im gesamten Cluster zu entfernen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *Operator-Setup.yaml*:

```
 ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Wenn es sich um ein Upgrade handelt, löschen Sie auch die Ressourcen aus Ihrem Cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Wenn die Änderungsanalyse aktiviert ist, ändern Sie die Optionen *AgentConfiguration* oder *Operator-config.yaml*, um den Änderungsmanagementabschnitt zu entkommentieren und *kindsToIgnoreFromWatch: '"Secrets"* im Bereich Change-Management aufzunehmen. Notieren Sie sich das Vorhandensein und die Position von einfachen und doppelten Anführungszeichen in dieser Zeile.

```
# change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Überprüfen Von Kubernetes Prüfsummen

Das Installationsprogramm von Data Infrastructure Insights Agent führt Integritätsprüfungen durch, einige Benutzer möchten jedoch möglicherweise ihre eigenen Überprüfungen durchführen, bevor heruntergeladene Artefakte installiert oder angewendet werden. Um einen nur-Download-Vorgang durchzuführen (im Gegensatz zum Standard-Download-and-install), können diese Benutzer den Agent-Installation Befehl erhalten von der UI und entfernen Sie die nachhängbare "Installation" Option.

Führen Sie hierzu folgende Schritte aus:

1. Kopieren Sie das Agent Installer-Snippet wie angewiesen.
2. Anstatt das Snippet in ein Befehlsfenster einzufügen, fügen Sie es in einen Texteditor ein.
3. Entfernen Sie den nachfolgenden „--install“ aus dem Befehl.
4. Kopieren Sie den gesamten Befehl aus dem Texteditor.
5. Fügen Sie es nun in Ihr Befehlsfenster ein (in einem Arbeitsverzeichnis) und führen Sie es aus.
    - Download und Installation (Standard):

```
 installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download --install
** Nur Download:
```

```
installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download
```

Mit dem Befehl „nur herunterladen“ werden alle erforderlichen Artefakte aus Data Infrastructure Insights in das Arbeitsverzeichnis heruntergeladen. Die Artefakte umfassen, dürfen aber nicht beschränkt sein auf:

- Ein Installationsskript
- Einer Umgebungsdatei
- YAML-Dateien
- Eine signierte Prüfsumme-Datei (sha256.signed)
- Eine PEM-Datei (netapp_cert.pem) zur Signaturverifizierung

Das Installationsskript, die Umgebungsdatei und die YAML-Dateien können mittels Sichtprüfung verifiziert werden.

Die PEM-Datei kann durch Bestätigung des Fingerabdrucks wie folgt verifiziert werden:

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
Genauer gesagt,
```

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
Die signierte Prüfsummendatei kann mit der PEM-Datei verifiziert werden:
```

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die
Agenteninstallation durch Ausführen von gestartet werden:
```

```
sudo -E -H ./<installation_script_name> --install
```

Toleranzen und Verfleckungen

Die DemonSets *netapp-CI-telegraf-ds*, *netapp-CI-Fluent-Bit-ds* und *netapp-CI-net-Observer-l4-ds* müssen für jeden Node im Cluster einen Pod planen, damit Daten auf allen Nodes korrekt erfasst werden. Der Operator wurde so konfiguriert, dass er einige bekannte **Fehler** toleriert. Wenn Sie auf Ihren Nodes benutzerdefinierte Taints konfiguriert haben und damit verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie für diese Taints eine **Toleration** erstellen "In der *AgentConfiguration*". Wenn Sie auf alle Nodes im Cluster benutzerdefinierte Taints angewendet haben, müssen Sie der Operator-Bereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Weitere Informationen zu Kubernetes "Tönungen und Tolerationen".

Kehren Sie zum zurück **"NetApp Kubernetes Monitoring Operator Installation** Seite"

Fehlerbehebung

Bei Problemen beim Einrichten des Kubernetes Monitoring Operator sollten Sie Folgendes versuchen:

Problem:	Versuchen Sie dies:
Ich sehe keinen Hyperlink/Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End Storage-Gerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Storage-Servers konfiguriert.	Befolgen Sie die Schritte, um den bestehenden Telegraf-Agent zu deinstallieren, und installieren Sie dann den neuesten Telegraf-Agent erneut. Sie müssen Telegraf Version 2.0 oder höher verwenden. Der Kubernetes-Cluster-Storage muss aktiv durch Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie dies:
Ich sehe Nachrichten in den Protokollen, die folgendermaßen aussehen: E0901 15:21:39.962145 1 Reflector.go:178] k8s.io/kube-State-metrics/internal/Store/Builder.go:352: Konnte *v1.MutatingWebhookKonfiguration: Der Server konnte die angeforderte Ressource nicht finden E0901 15:21:43.168161 1 Reflector.go:178] k8s.io/kube-State-metrics/internal/Store/Builder.go:352: Fehler beim Auflisten von *v1.Lease: Der Server konnte die angeforderte Ressource nicht finden (get Leases.Coordination.k8s.io) Usw.	Diese Nachrichten können auftreten, wenn Sie kube-State-Metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. So erhalten Sie die Kubernetes-Version: *Kubectl Version* So erhalten Sie die kube-State-metrics-Version: *Kubectl get deploy/kube-State-metrics -o jsonpath='{..image}'* Um zu verhindern, dass diese Meldungen stattfinden, können Benutzer ihre Bereitstellung von kube-State-Metrics ändern, um die folgenden Leasings zu deaktivieren: *Mutatingwebhookkonfigurationen* *Validatingwebhookkonfigurationen* *Volumeattachments-Ressourcen* Genauer gesagt können sie das folgende CLI-Argument verwenden: Ressourcen=zertifiziertigningrequests,configmaps,cronjobs,demonsets, Bereitstellungen,Endpunkte,horizontalpodautoscalers,ingresses,Jobs,limitranges, Namespaces,Netzwerkrichtlinien,Nodes,persistent Volumeclaims,persistent Volumes, poddisruptionbudgets,Pods,Replikasets,Replikationcontroller,resourcequotas, Secrets,Services,Statefulsets,Storageclasses Die Standardressourcenliste lautet: „Zertificatezigningrequest,configmaps,cronjobs,demonsets,Bereitstellungen, Endpunkte,horizontalpodautoscalers,ingresses,Jobs,Leases,limitranges, mutatingwebhookkonfigurationen,Namespaces,Netzwerkrichtlinien,Nodes,persistent Volumeclaims,persistent,Volumes,poddisruptionbudgets,Pods,Replikasets,resourcequotas,Secrets,Services,statectorSets,statectoresets Validatingwebhookkonfigurationen, Volumeanhänge“

Problem:	Versuchen Sie dies:
Ich sehe Fehlermeldungen von Telegraf wie die folgenden, aber Telegraf startet und läuft: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Startete den Plugin-gesteuerten Server-Agent für die Berichterstattung von Kennzahlen in InfluxDB. Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„konnte kein Cache-Verzeichnis erstellen. /Etc/telegraf/.Cache/snowflake, err: Mkdir /etc/telegraf/.ca Che: Erlaubnis verweigert. Ignored\n“ func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:120“ Okt. 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„Öffnen fehlgeschlagen. Ignoriert. Open /etc/telegraf/.Cache/snowflake/ocsp_response_Cache .json: Nicht so Datei oder Verzeichnis\n“ func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:120“ Okt. 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z i! Telegraf 1.19.3 Starten	Dies ist ein bekanntes Problem. Siehe "Dieser GitHub-Artikel" Entnehmen. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.
Auf Kubernetes berichten meine Telegraf POD(s) die folgende Fehlermeldung: "Fehler bei der Verarbeitung von mountstats-Info: Mountstats-Datei konnte nicht geöffnet werden: /Hostfs/proc/1/mountstats, Fehler: Open /hostfs/proc/1/mountstats: Berechtigung verweigert"	Wenn SELinux aktiviert und durchgesetzt wird, wird wahrscheinlich verhindert, dass die Telegraf PODs auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen. Um diese Einschränkung zu überwinden, bearbeiten Sie die Agentkonfiguration und aktivieren Sie die runPrivileged-Einstellung. Weitere Informationen finden Sie im "OpenShift-Anweisungen".
Auf Kubernetes meldet mein Telegraf ReplicaSet POD den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Konnte keypair /etc/kubernetes/pki/etcd/Server.crt:/etc/kubernetes/pki /etcd/Server.key nicht laden: Öffnen /etc/kubernetes/pki/etcd/Server.crt: Datei oder Verzeichnis nicht vorhanden	Der Pod Telegraf ReplicaSet soll auf einem Knoten ausgeführt werden, der als Master oder für etc bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master/etcd-Knoten eine Tönungswalle haben. Fügen Sie in diesem Fall die erforderlichen Verträgungen in das Telegraf ReplicaSet, telegraf-rs ein. Bearbeiten Sie beispielsweise das ReplicaSet… Kubectl bearbeiten rs telegraf-rs …Und fügen Sie die entsprechenden Toleranzen in die Spezifikation ein. Starten Sie anschließend den Pod ReplicaSet neu.

Problem:	Versuchen Sie dies:
Ich habe eine PSP/PSA Umgebung. Hat dies Auswirkungen auf meinen Überwachungsperator?	Wenn Ihr Kubernetes-Cluster mit Pod-Sicherheitsrichtlinie (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie ein Upgrade auf den aktuellen Kubernetes Monitoring Operator durchführen. Führen Sie die folgenden Schritte aus, um auf den aktuellen Bediener mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren Der vorherige Überwachungsoperator: Kubectl delete Agent-Monitoring-netapp -n netapp-Monitoring Kubectl löschen ns netapp-Monitoring Kubectl löschen crd agents.monitoring.netapp.com Kubectl delete clusterrole Agent-Manager-role Agent-Proxy-role Agent-metrics-reader Kubectl delete clusterrolebinding Agent-Manager-rolebinding Agent-Proxy-rolebinding Agent-Cluster-admin-rolebinding 2. Installieren Die neueste Version des Überwachungsbedieners.
Ich habe Probleme beim Versuch, den Operator bereitzustellen, und ich habe PSP/PSA in Gebrauch.	1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: Kubectl -n <name-space>-Bearbeitungsagent 2. Markieren Sie "Sicherheit-Politik-aktiviert" als "falsch". Dadurch werden Pod-Sicherheitsrichtlinien und Pod-Sicherheitszulassung deaktiviert und der Bediener kann die Bereitstellung durchführen. Bestätigen Sie die Bestätigung mit folgenden Befehlen: Kubectl get psp (sollte zeigen, dass die Pod-Sicherheitsrichtlinie entfernt wurde) Kubectl get all -n <namespace> (sollte zeigen, dass nichts gefunden wird)
„ImagePullBackoff“-Fehler erkannt	Diese Fehler können auftreten, wenn Sie über ein benutzerdefiniertes oder privates Docker-Repository verfügen und den Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass er es richtig erkennt. Weitere Informationen Info zur Konfiguration für benutzerdefinierte/private Repo.

Problem:	Versuchen Sie dies:
Ich habe ein Problem mit der Installation meines Monitoring-Bedieners, und die aktuelle Dokumentation hilft mir nicht, es zu lösen.	Erfassen oder notieren Sie die Ausgabe der folgenden Befehle, und wenden Sie sich an den technischen Support. ``` kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true ```
NET-Observer (Workload Map)-Pods im Operator Namespace befinden sich in CrashLoopBackOff	Diese Pods entsprechen dem Workload Map-Datensammler für Network Observability. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die minimale Kernel-Version zu bestätigen. Beispiel: ---- {„CI-Tenant-id“:„your-Tenant-id“,„Collector-Cluster“:„your-k8s-Cluster-Name“,„environment“:„prod“,„Level“:„error“,„msg“:„failed in validation. Grund: Kernelversion 3.10.0 ist kleiner als die minimale Kernelversion von 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • Net-Observer PODs benötigen die Linux Kernel Version mindestens 4.18.0. Überprüfen Sie die Kernel-Version mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 sind
Pods werden im Operator Namespace ausgeführt (Standard: netapp-Monitoring), es werden jedoch keine Daten in der UI für die Workload-Zuordnung oder Kubernetes-Metriken in Abfragen angezeigt	Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Rechner mit Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.

Problem:	Versuchen Sie dies:
Einige der Net-Observer-Pods im Namespace Operator befinden sich im Status „Ausstehend“	NET-Observer ist ein DemonSet und führt in jedem Knoten des K8s-Clusters einen Pod aus. • Beachten Sie den Pod, der sich im Status „Ausstehend“ befindet, und prüfen Sie, ob ein Ressourcenproblem für CPU oder Speicher vorliegt. Stellen Sie sicher, dass der erforderliche Arbeitsspeicher und die erforderliche CPU im Knoten verfügbar sind.
Ich sehe Folgendes in meinen Protokollen sofort nach der Installation des Kubernetes Monitoring Operator: [inputs.prometheus] Fehler im Plugin: Fehler beim Erstellen einer HTTP-Anforderung an http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.Cluster.local: Kein solcher Host	Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert ist und der Pod „*telegraf-rs*“ vor dem Einschalten des Pod „*ksm*“ steht. Diese Meldungen sollten beendet werden, sobald alle Pods ausgeführt werden.
Ich sehe keine Kennzahlen für die Kubernetes-Kronjobs, die in meinem Cluster vorhanden sind, erfasst.	Überprüfen Ihrer Kubernetes Version (d. h. `kubectl version`). Wenn es v1.20.x oder niedriger ist, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator implementierte Version von kube-State-Metrics unterstützt nur v1.cronjob. Bei Kubernetes 1.20.x und niedriger befindet sich die Ressource cronjob unter v1beta.cronjob. Daher können kube-State-Metriken die Ressource cronjob nicht finden.
Nach der Installation des Bedieners geben die telegraf-ds-Pods CrashLoopBackOff ein und die POD-Protokolle zeigen „su: Authentication failure“ an.	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und setzen Sie *dockerMetricCollectionEnabled* auf false. Weitere Informationen finden Sie im "Konfigurationsoptionen". HINWEIS: Wenn Sie Data Infrastructure Insights Federal Edition verwenden, können Benutzer mit Einschränkungen hinsichtlich der Verwendung von *su* keine Docker-Metriken sammeln, da der Zugriff auf den Dockersockel entweder den telegraf-Container als root ausführen muss oder *su* verwenden muss, um den telegraf-Benutzer zur Docker-Gruppe hinzuzufügen. Docker metric Collection und die Verwendung von *su* sind standardmäßig aktiviert; um beides zu deaktivieren, entfernen Sie den Eintrag *telegraf.Docker* in der *AgentConfiguration*-Datei: … Spec: … telegraf: … - Name: docker Run-Mode: - DemonSet Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCK_PLACEHOLDER Wert: unix:///run/Docker.Sock … …

Problem:	Versuchen Sie dies:
Ich sehe wiederholte Fehlermeldungen wie die folgenden in meinen Telegraf-Protokollen: E! [Agent] Fehler beim Schreiben in Outputs.http: Post "https://<tenant_url>/Rest/v1/Lake/ingest/influxdb": Kontext-Deadline überschritten (Client. Zeitüberschreitung beim Warten auf Header überschritten)	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und erhöhen Sie *outputTimeout* auf 10s. Weitere Informationen finden Sie im Abschnitt des Bedieners "Konfigurationsoptionen".
Ich vermisse *involvedobject* Daten für einige Event Logs.	Stellen Sie sicher, dass Sie die Schritte im befolgt haben "Berechtigungen" Abschnitt oben.
Wieso werden zwei Monitoring Operator Pods ausgeführt, einer mit dem Namen netapp-CI-Monitoring-Operator-<pod> und der andere mit dem Namen Monitoring-Operator-<pod>?	Seit dem 12. Oktober 2023 hat Data Infrastructure Insights den Betreiber refaktorisiert, um unseren Benutzern besser dienen zu können. Damit diese Änderungen vollständig umgesetzt werden, müssen Sie Entfernen Sie den alten Bedienerund Installieren Sie den neuen.
Meine kubernetes-Ereignisse haben unerwartet aufgehört, Daten bei Infrastruktur-Insights zu melden.	Rufen Sie den Namen des POD für den Event-Exporter ab: `kubectl -n netapp-monitoring get pods`
grep event-exporter	awk '{print $1}'
sed 's/event-exporter./event-exporter/` Es sollte entweder „netapp-CI-Event-Exporteur“ oder „Event-Exporteur“ sein. Bearbeiten Sie anschließend den Monitoring-Agent `kubectl -n netapp-monitoring edit agent`, Und legen Sie den Wert für LOG_FILE so fest, dass der entsprechende POD-Name für den Event-Exporter im vorherigen Schritt angezeigt wird. Genauer gesagt sollte LOG_FILE auf "/var/log/Containers/netapp-CI-Event-exporteur.log" oder "/var/log/Containers/Event-exporteur*.log" gesetzt werden …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativ kann man auch Deinstallieren Und Neu installieren Der Agent.	Ich sehe POD(s), die vom Kubernetes-Monitoring-Operator bereitgestellt werden, aufgrund unzureichender Ressourcen.

Problem:	Versuchen Sie dies:
Weitere Informationen finden Sie im Kubernetes Monitoring Operator "Konfigurationsoptionen" Um die CPU- und/oder Speichergrenzen je nach Bedarf zu erhöhen.	Durch ein fehlendes Image oder eine ungültige Konfiguration wurden die netapp-CI-kube-State-metrics Pods nicht gestartet oder nicht einsatzbereit gemacht. Jetzt bleibt StatefulSet stecken und Konfigurationsänderungen werden nicht auf die Pods mit den netapp-CI-kube-State-Metriken angewendet.
Das StatefulSet befindet sich in A "Defekt" Bundesland. Nachdem Sie Konfigurationsprobleme behoben haben, springen die netapp-CI-kube-State-metrics-Pods an.	Pods mit netapp-CI-kube-Status-Metriken können nicht gestartet werden, nachdem ein Kubernetes Operator Upgrade ausgeführt wurde. Es wird ErrImagePull geworfen (es konnte nicht das Image entfernt werden).
Versuchen Sie, die Pods manuell zurückzusetzen.	„Event disorded as being alder then maxEventAgeSeconds“ Meldungen werden für meinen Kubernetes Cluster unter Log Analysis beobachtet.
Ändern Sie den Operator *agentkonfiguration*, und erhöhen Sie die Erweiterung *Event-exporteur-maxEventAgeSeconds* (d. h. auf 60s), *Event-exporteur-kubeQPS* (d. h. auf 100) und *Event-exporteur-kubeBurst* (d. h. auf 500). Weitere Informationen zu diesen Konfigurationsoptionen finden Sie im "Konfigurationsoptionen" Seite.	Telegraf warnt vor unzureichenden, abschließbaren Speichern oder stürzt ab.

Weitere Informationen finden Sie im "Unterstützung" Oder auf der "Data Collector Supportmatrix".

Memcached Data Collector

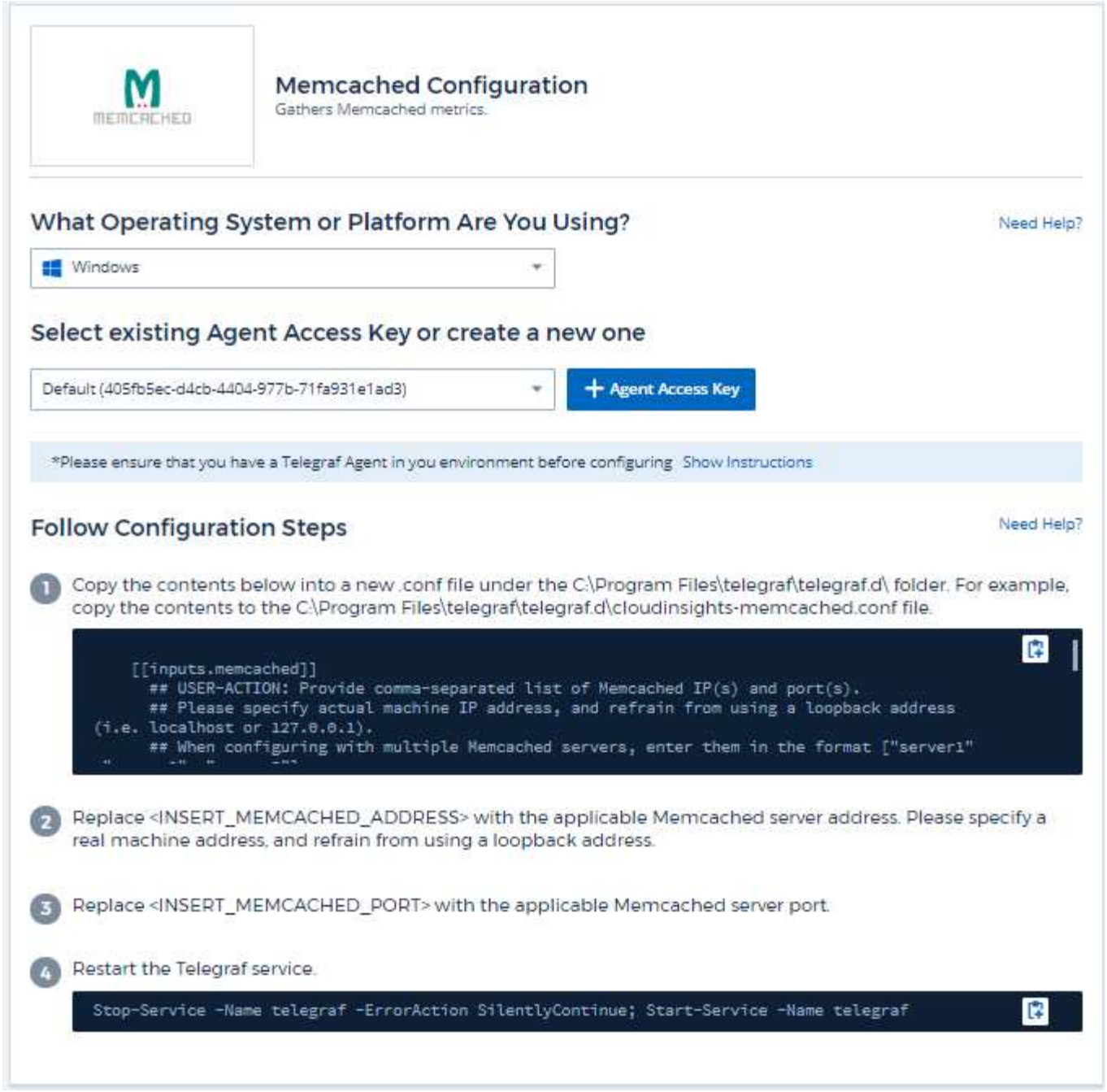
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen aus Memcached zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Memcached.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Wiki mit Memcached".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Gememcachte	Namespace-Server	Node-IP-Node-Name	Akzeptieren von Verbindungen verarbeitet Authentifizierungsanforderungen fehlgeschlagene Authentifizierungen verwendete Bytes (pro Sekunde) geschriebene Bytes (pro Sek.) CAS Badval CAS Hits CAS Misses Flush Reqs (pro Sek.) Get Reqs (pro Sek.) Set Reqs (pro Sek.) Touch Reqs (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Verbindungen öffnen Aktuelle gespeicherte Objekte Decr fordert Zugriffe (pro Sek.) Decr fordert Fehlschläge (pro Sek.) Löschen von Anfragen Treffer (pro Sek.) Löschen von Anfragen Fehlschläge (pro Sek.) entfernte Objekte gültige Abtreibungen abgelaufene Objekte Get Hits (pro Sek.) Get Misses (pro Sek.) Gebrauchte Hash Bytes Hash-Bytes erweitert Hash Power Level Inc. Hash Power Level Inc. Zugriffe (pro Sek.) Infr Anfragen Misses (pro Sek.) Server Max Bytes anhören deaktiviert Num zurückgewonnener Mitarbeiter Threads Anzahl geöffnete Verbindungen Gesamtzahl der gespeicherten Elemente Touch Hits Touch Misses Server Uptime

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

MongoDB Data Collector

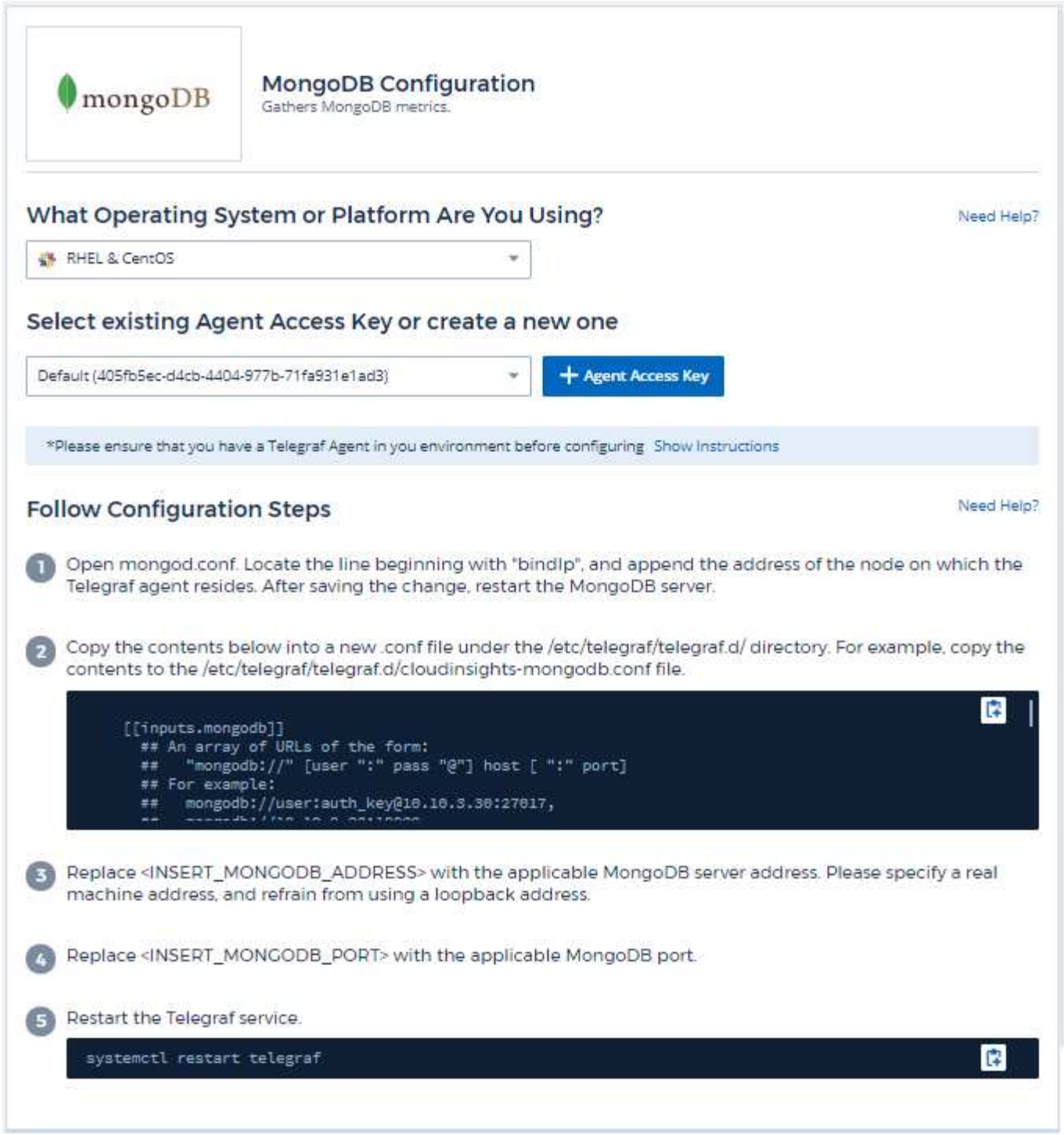
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von MongoDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MongoDB.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "MongoDB Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB	Namespace-Hostname		

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB Datenbank	Name der Namespace-Hostname-Datenbank		

Fehlerbehebung

Informationen können im gefunden werden "Unterstützung" Seite.

MySQL Data Collector

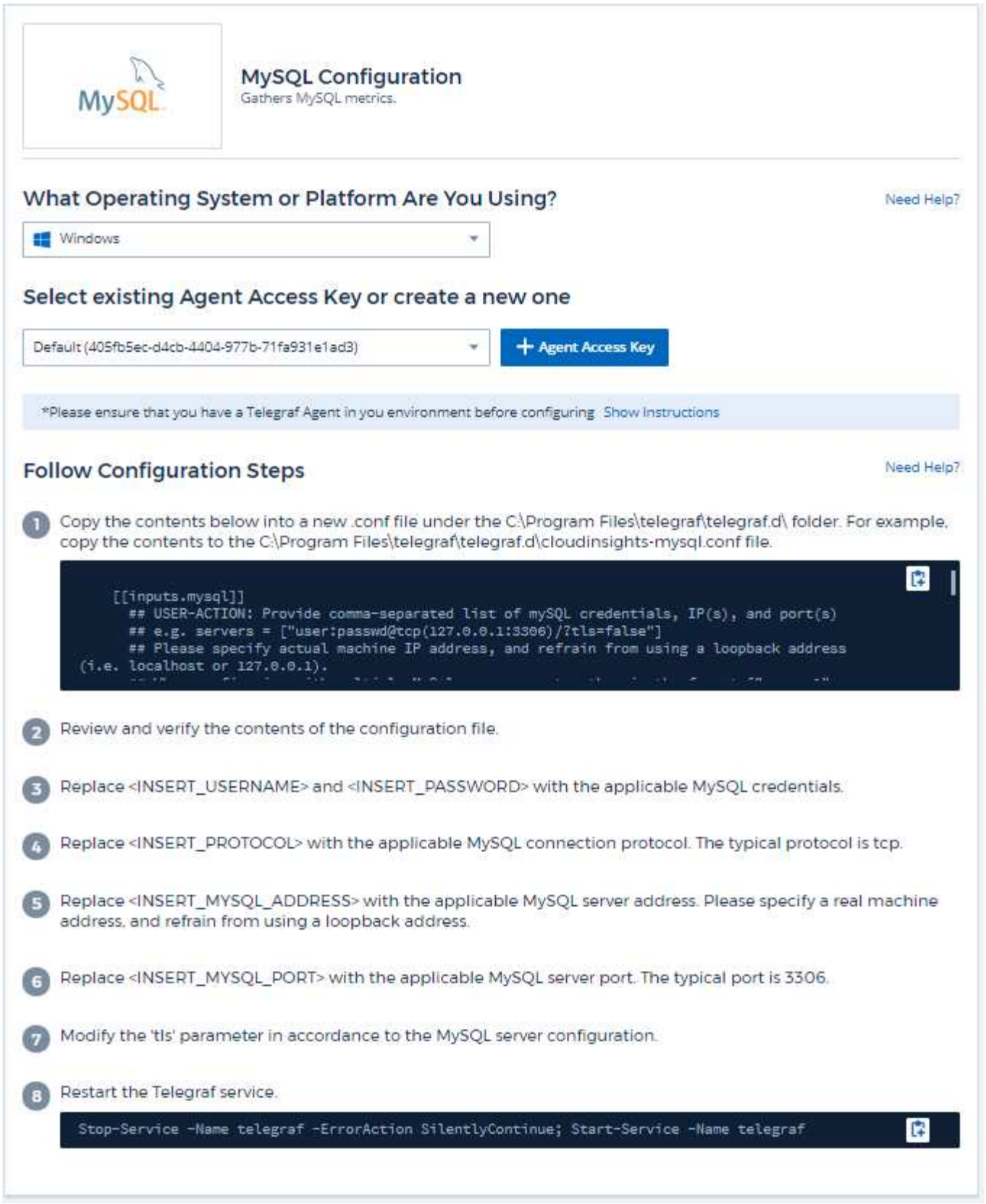
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus MySQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MySQL.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "MySQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MySQL	Namespace für MySQL Server	Node-IP-Node-Name	Abgebrochene Clients (pro s) abgebrochene Verbindungen (pro s) RX Byte (pro s) TX Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Alter Ereignisbefehle Alter Funktion Befehle Alter Instanz Befehle Alter Prozedur Befehle Alter Server Befehle Alter Tabelle Befehle Alter Tablespace Befehle Alter Benutzer Befehle Analyse Befehle Zuweisen zu Keycache-Befehlen Begin-Befehle Binlog-Befehle Aufruf Procedure-Befehle DB-Befehle Change Master befiehlt Change Repl Filter Befehle Check Commands Prüfsummenbefehle Befehle Commit-Befehle DB-Befehle erstellen Ereignisbefehle erstellen Befehle erstellen Index-Befehle erstellen Maßnahmen-Befehle erstellen Serverbefehle erstellen Trigger-Befehle erstellen UDF-Befehle erstellen Benutzerbefehle erstellen Befehle anzeigen erstellen Dealloc SQL-Verbindungsfehler akzeptieren erstellte tmp-Disk-Tabellen verzögerte Fehler Flush-Befehle Handler Commit Innodb Buffer Pool Bytes Daten Schlüsselblöcke Nicht Gespült Schlüssel Leseanforderungen Schlüssel Schreib Schlüssel Schreibvorgänge Max Ausführungszeit Überschritten Max Verwendete Verbindungen Open Files Performance Schema Konten Lost Prepared Stmt Count Qcache Freie Blöcke

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Netstat Data Collector

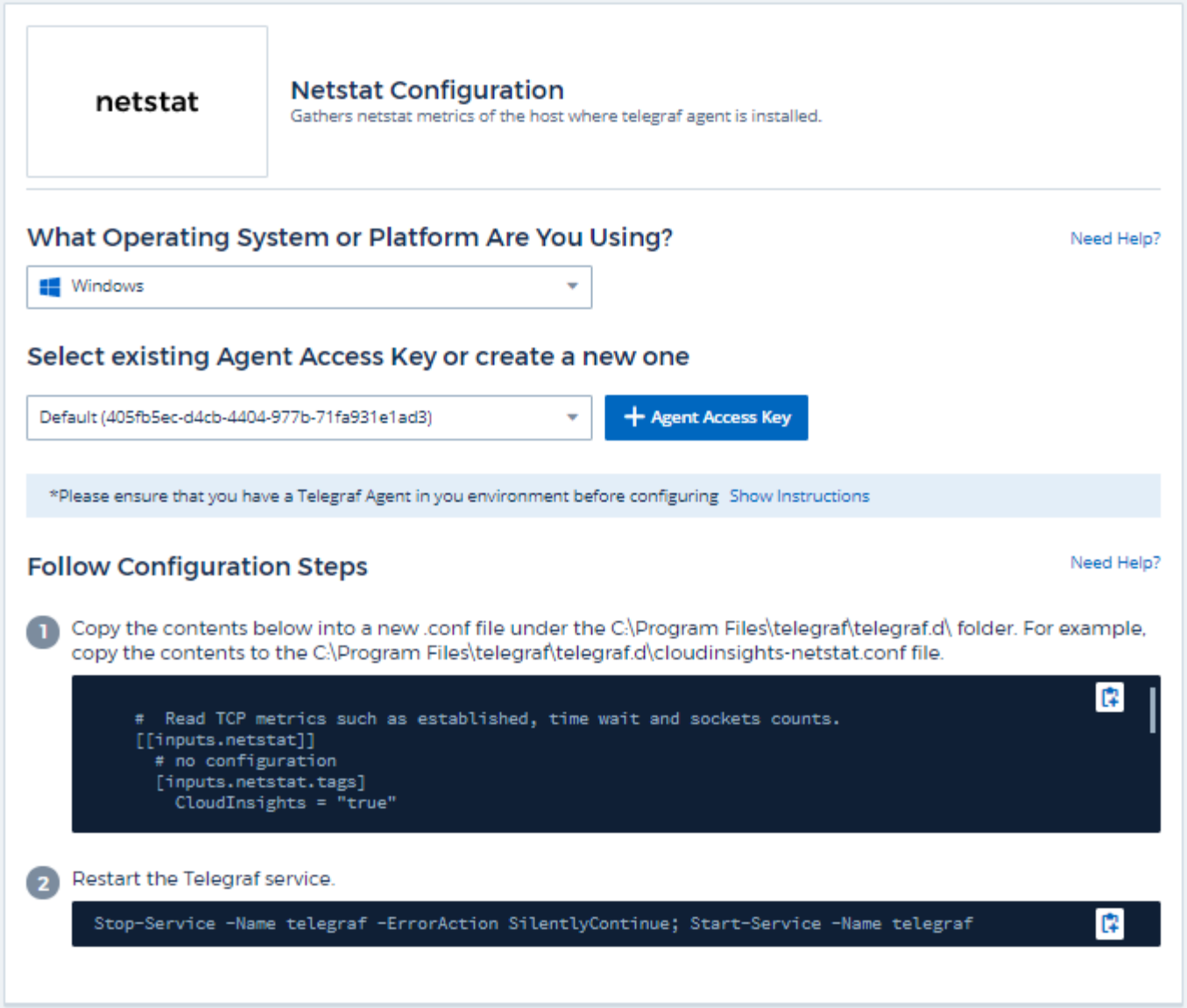
Data Infrastructure Insights verwendet diesen Datensammler, um netstat-Metriken zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Netstat.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Netstat	Node-UUID	Node-IP-Node-Name	

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Nginx Data Collector

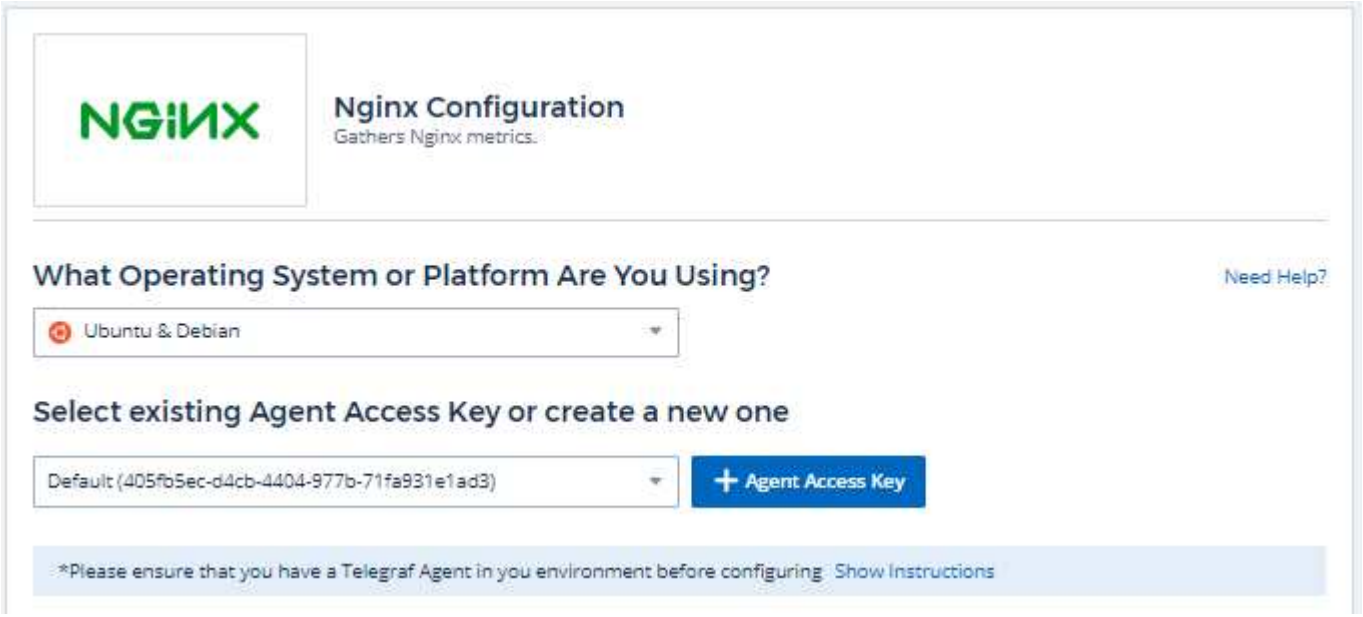
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Nginx zu sammeln.

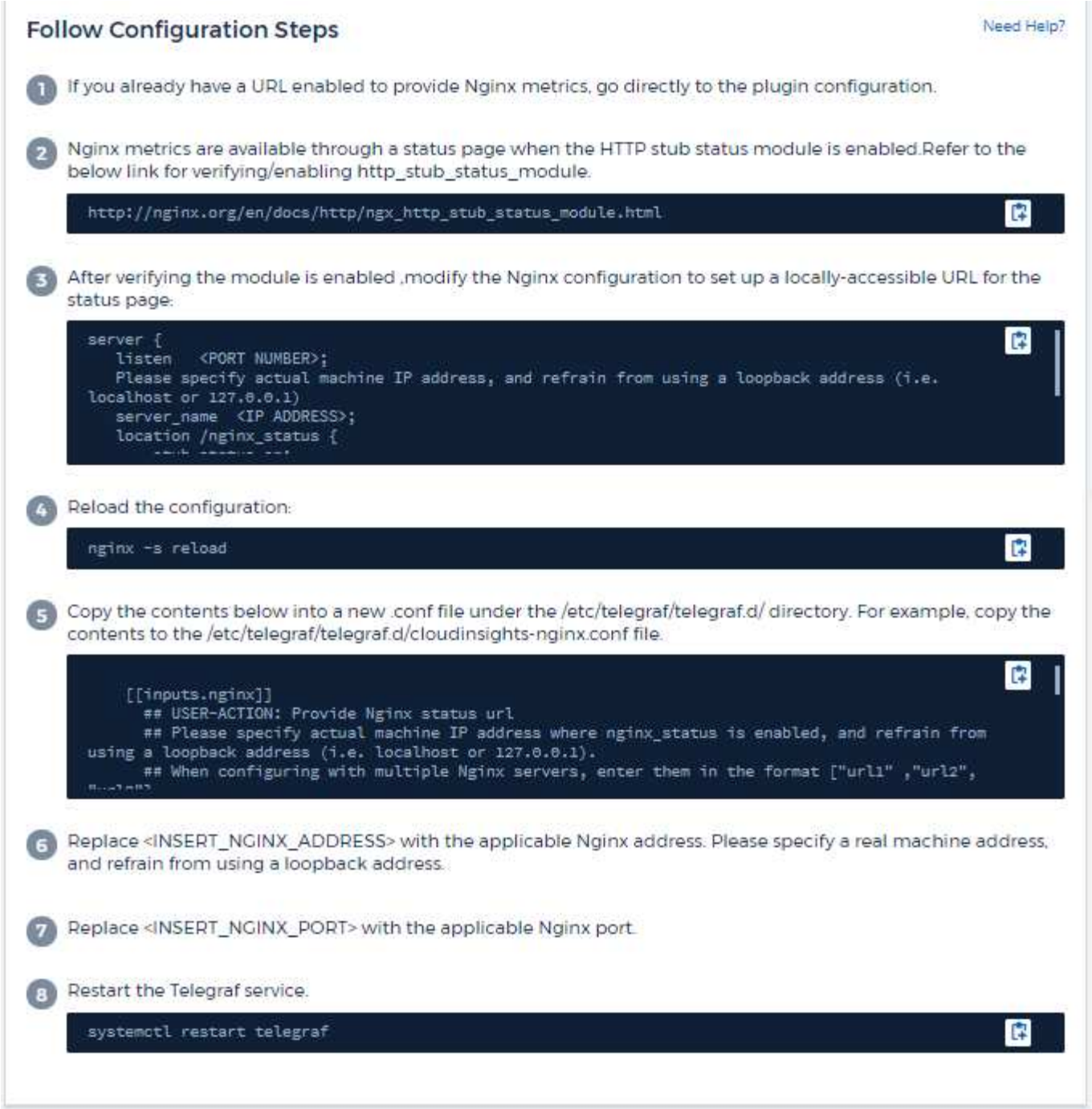
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Nginx.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.





Einrichtung

Für die nginx-metrische Sammlung ist Nginx erforderlich "http_stub_Status_Module" Aktiviert sein.

Weitere Informationen finden Sie im "Nginx-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Nginx	Namespace-Server	Node-IP-Node-Name-Port	Akzeptiert Aktive Bearbeitet Leseanforderungen, Die Auf Das Schreiben Warten

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

PostgreSQL Data Collector

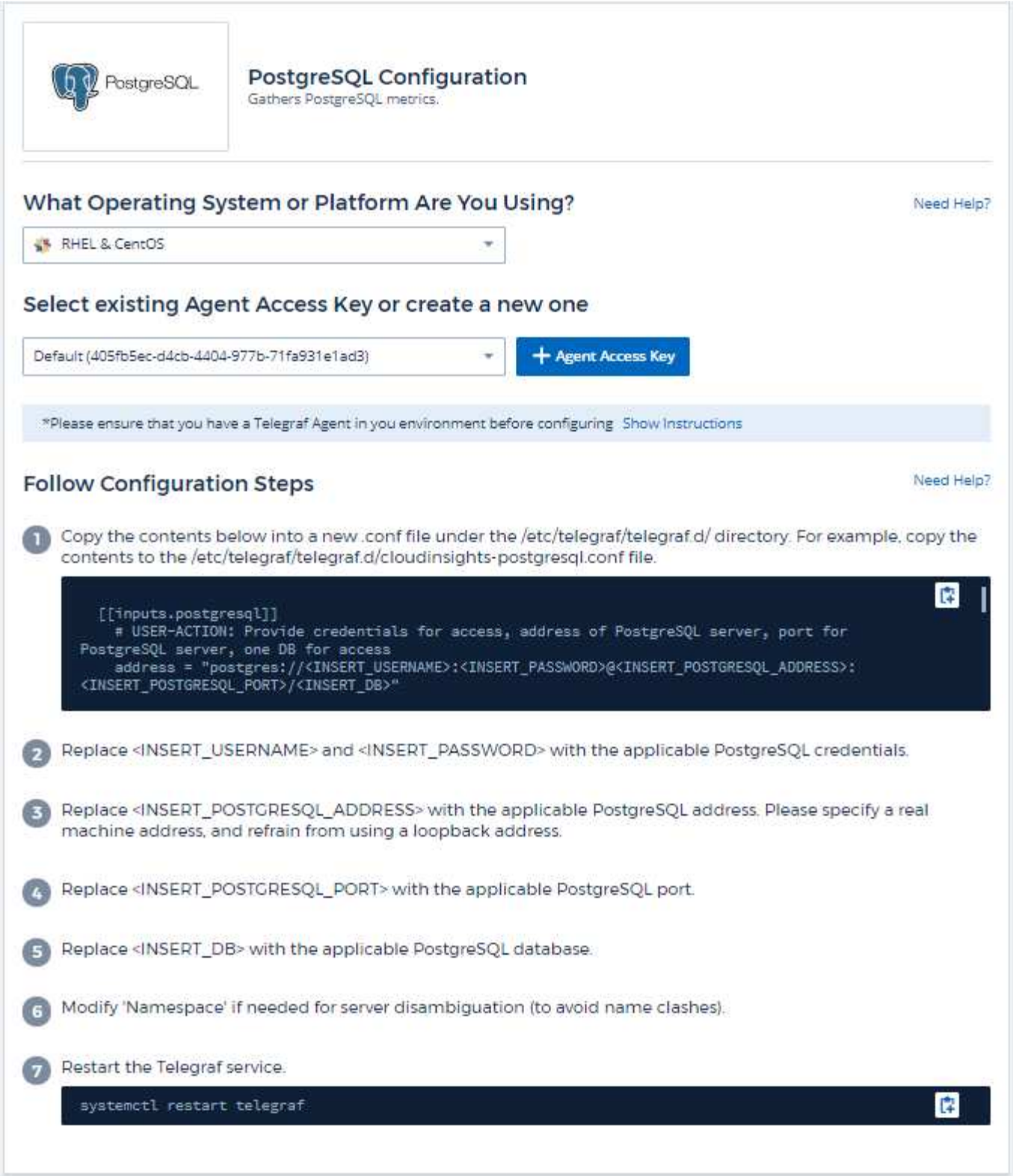
Data Infrastructure Insights nutzt diesen Datensammler, um Metriken aus PostgreSQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie PostgreSQL.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "PostgreSQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
PostgreSQL Server	Namespace-Datenbankserver	Node Name Node-IP	Puffer Zugeordnete Buffers Back-End-Puffer Dateisynchronisation Buffers Checkpoint Puffer Clean Checkpoints Sync Time Checkpoints Write Time Checkpoints Requests Checkpoints Timed Max Geschrieben Sauber
PostgreSQL Datenbank	Namespace-Datenbankserver	Datenbank OID Node Name Node IP	Blöcke Lesezeit Blöcke Write Time Blocks Treffer Blöcke Liest Konflikte Deadlocks Client-Nummer Temp-Dateien Bytes Temp-Dateien Anzahl Zeilen Gelöschte Zeilen Abgeholt Zeilen Zeilenanzahl Zeilenanzahl Zeilenanzahl Zeilenumeinfügen Letzte Transaktionen Letzte Transaktionen Übertragen Rollbacks

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Puppet Agent Data Collector

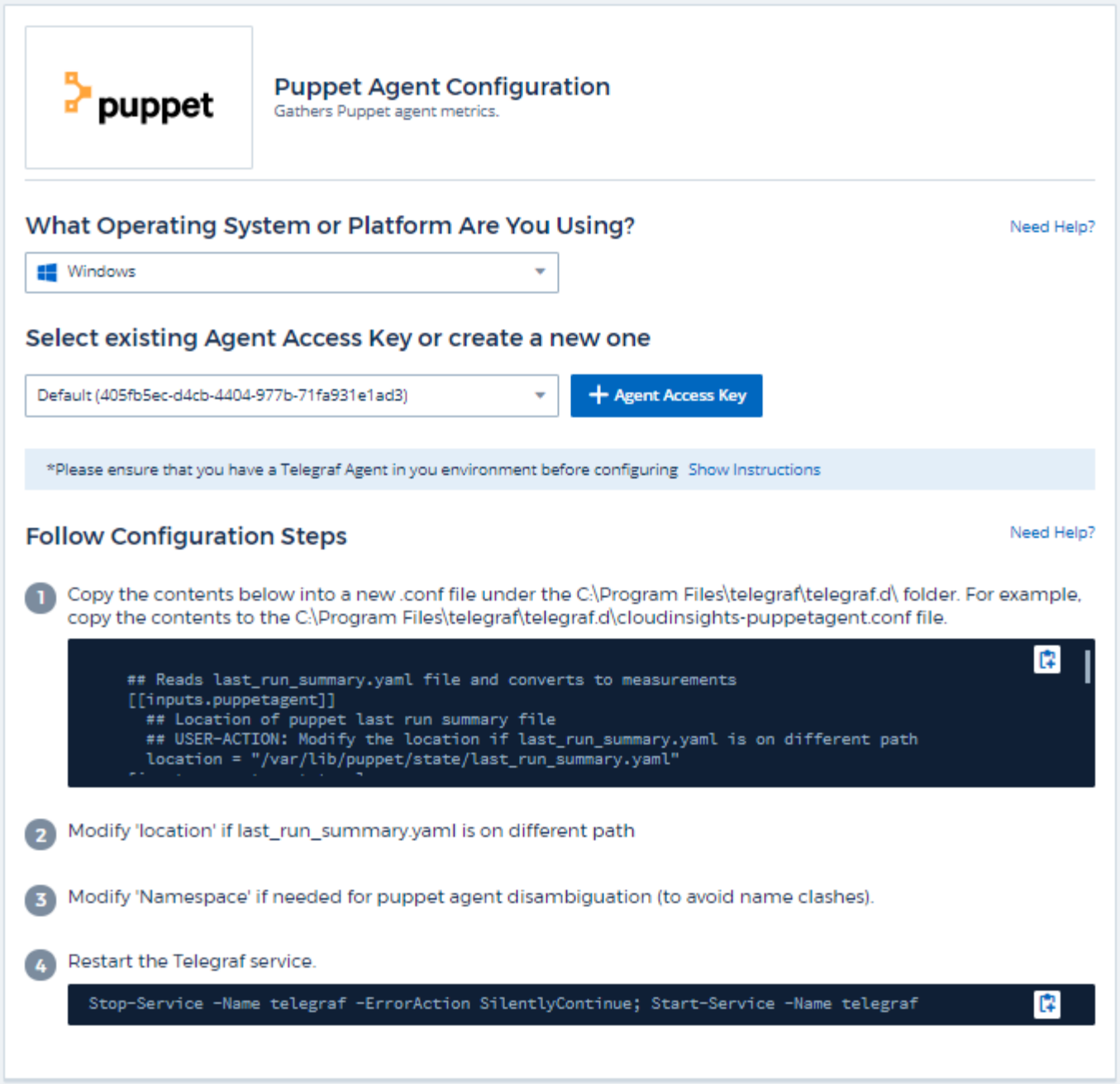
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen von Puppet Agent zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Puppet.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Puppet-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:

Puppet Agent	Namespace-Node-UUID	Node Name Ort Node-IP-Version Konfigstring Version Puppet	Änderungen Total Events Failure Ereignisse Success Events Summe Ressourcen Geänderte Ressourcen Fehlgeschlagen Ressourcen Konnten Nicht Neu Starten Ressourcen Outofsync Ressourcen Neustart Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Abruf Configtime Cron Time Exec Time File Time Filebucket Time Lastrun Time Package Time Zeitplanzeit Service Time Sshauorizedkey Time Total Time User

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Redis Data Collector

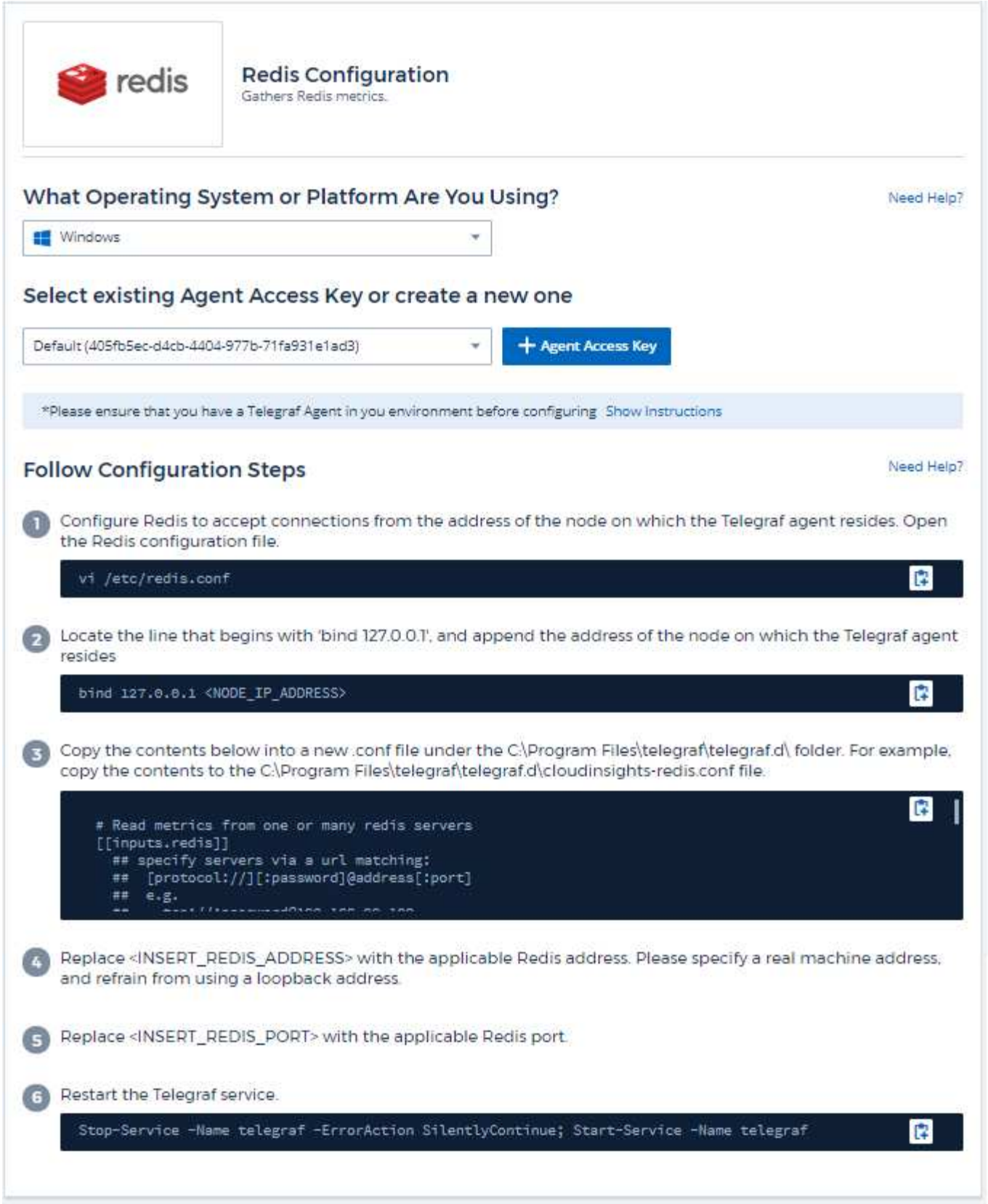
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen von Redis zu sammeln. Redis ist ein Open Source, in-Memory Data Structure Store, der als Datenbank-, Cache- und Nachrichten-Broker verwendet wird und die folgenden Datenstrukturen unterstützt: Strings, Hash-Funktionen, Listen, Sätze und mehr.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie „Redis“.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "Redis-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Redis	Namespace-Server		

Fehlerbehebung

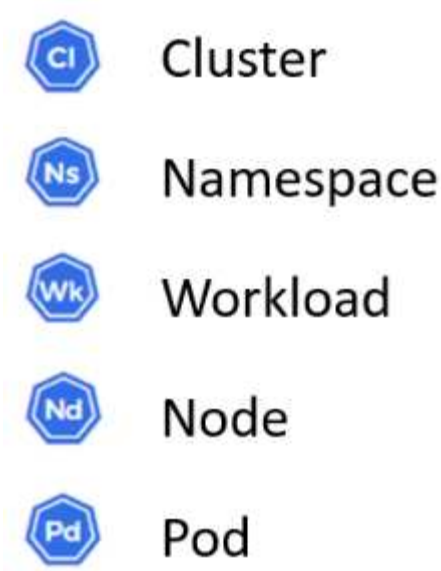
Weitere Informationen finden Sie im "Unterstützung" Seite.

Objekt Symbol Referenz

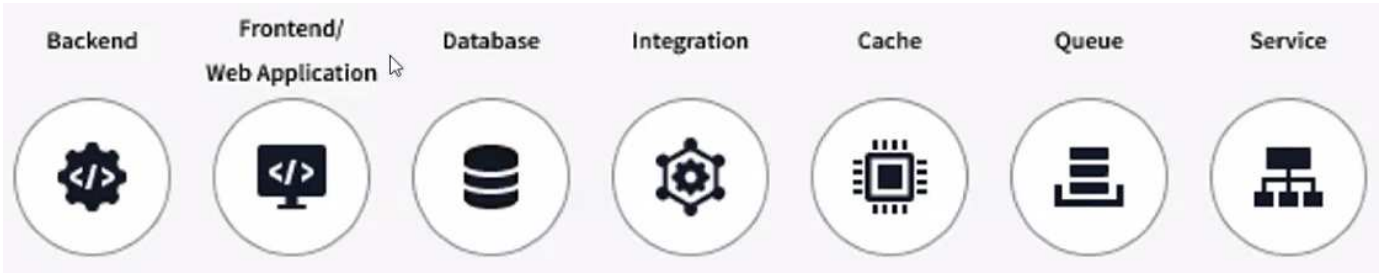
In Data Infrastructure Insights verwendete Objektsymbole:

Infrastruktursymbole:

Kubernetes-Symbole:



Symbole für die Kubernetes-Netzwerkleistungsüberwachung und -Zuordnung:



Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweise zu Dateninfrastruktureinblicken (ehemals Cloud Insights)"

"Hinweis zur Workload-Sicherheit (ehemals Cloud Secure)"