



Referenz & Support

Data Infrastructure Insights

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/de-de/data-infrastructure-insights/concept_requesting_support.html on February 03, 2026. Always check docs.netapp.com for the latest.

Inhalt

Referenz & Support	1
Support anfordern	1
Supportanspruch aktivieren	1
Supportinformationen erhalten	4
Data Infrastructure Insights Datensammler-Supportmatrix	5
Datensammlerreferenz – Infrastruktur	6
Anbieterspezifische Referenz	6
Konfigurieren des Amazon EC2-Datensammlers	6
Amazon FSx for NetApp ONTAP Datenkollektor	9
Konfigurieren des Azure-Compute-Datensammlers	12
Broadcom	13
Cisco MDS Fabric Switches Datensammler	21
Cohesity SmartFiles-Datensammler	24
Dell	25
Dell EMC	25
Fujitsu Eternus Datensammler	52
NetApp Google Compute-Datenkollektor	53
Google Cloud NetApp Volumes Datensammler	54
HP Unternehmen	56
Hitachi-Datensysteme	64
Infinidat InfiniBox Datensammler	72
Huawei OceanStor Datensammler	74
IBM	75
Lenovo Datensammler	82
Microsoft	83
NetApp	86
Nutanix NX-Datensammler	127
Oracle ZFS Storage Appliance-Datenkollektor	128
Pure Storage FlashArray-Datensammler	130
Red Hat Virtualization-Datenkollektor	131
Rubrik CDM-Datensammler	132
Konfigurieren des VMware VSphere-Datenkollektors	134
Datensammlerreferenz – Dienste	137
Knotendatenerfassung	137
ActiveMQ-Datensammler	140
Apache-Datensammler	142
Konsul-Datensammler	145
Couchbase-Datensammler	146
CouchDB-Datensammler	148
Docker-Datensammler	150
Elasticsearch-Datensammler	158
Flink-Datensammler	160
Hadoop-Datensammler	167

HAProxy-Datensammler	172
JVM-Datensammler	180
Kafka-Datensammler	184
Kibana-Datensammler	187
Installation und Konfiguration des Kubernetes Monitoring Operators	189
Memcached-Datensammler	210
MongoDB-Datensammler	213
MySQL-Datensammler	215
Netstat-Datensammler	220
Nginx-Datensammler	221
PostgreSQL-Datensammler	224
Puppet Agent-Datensammler	226
Redis-Datensammler	228
Objektsymbolreferenz	230
Infrastruktursymbole:	230
Kubernetes-Symbole:	230
Überwachung der Netzwerkleistung von Kubernetes und Kartensymbole:	231

Referenz & Support

Support anfordern

Sie können auf die verfügbaren Supportoptionen in Data Infrastructure Insights zugreifen, indem Sie **Hilfe > Support** auswählen.

Support

When opening a support ticket please include the URL of the client tenant.

Technical Support:
[Open a Support Ticket](#) | [Phone\(P1\)](#)


Sales:
Have questions regarding your subscription? [Contact Sales](#).

Support Entitlement

Data Infrastructure Insights Serial Number:
111222333444555666777888999

Data Infrastructure Insights Subscription Name:
DII-1701-NetApp

Support Level:
Not registered - [Register Now](#)

☐ Allow NetApp access to your Data Infrastructure Insights Environment. 

Feedback

We value your input. [Your feedback](#) helps us improve Data Infrastructure Insights.

Documentation

Documentation Center:
Visit the [Data Infrastructure Insights Documentation Center](#) to find any step by step instructions to help you get the most out of Data Infrastructure Insights.

Knowledge Base:
Search through the [Data Infrastructure Insights Knowledge Base](#) to find helpful articles.

What's New:
See [What's New with Data Infrastructure Insights](#) to find recent product updates and changes.

API Access:
To integrate Data Infrastructure Insights with other applications see the [Data Infrastructure Insights API List and documentation](#).

Proxy Settings

Need to setup proxy exceptions? Click [here](#) to learn more.

Learning Center

Data Infrastructure Insights Course List:

- [Hybrid Cloud Resource Management](#)
- [Data Infrastructure Insights Fundamentals](#)
- [Cloud Resource Management](#)

Cloud Education All-Access Pass:
Visit and subscribe the [Cloud Education All-Access Pass](#) to get unlimited access to our best cloud learning resources.

Course Catalog:
Browse the [Learning Services Product Catalog](#) to find all the courses that are relevant to you.

Supportanspruch aktivieren

Data Infrastructure Insights bietet im Testmodus Self-Service- und E-Mail-Support. Sobald Sie den Dienst abonniert haben, wird dringend empfohlen, den Supportanspruch zu aktivieren. Durch die Aktivierung der Supportberechtigung erhalten Sie Zugriff auf den technischen Support über das Web-Ticketsystem und per Telefon. Der Standard-Supportmodus ist Selbstbedienung, bis die Registrierung abgeschlossen ist. Sehen [Details](#) unten.

Während des ersten Abonnementvorgangs generiert Ihre Data Infrastructure Insights -Instanz eine 20-stellige NetApp -Seriennummer, die mit „950“ beginnt. Diese NetApp Seriennummer stellt das mit Ihrem Konto verknüpfte Data Infrastructure Insights -Abonnement dar. Sie müssen die NetApp Seriennummer registrieren, um den Supportanspruch zu aktivieren. Wir bieten zwei Möglichkeiten zur Support-Registrierung:

1. Benutzer mit bereits vorhandenem NetApp Support Site (NSS) SSO-Konto (z. B. aktueller NetApp Kunde)
2. Neuer NetApp Kunde ohne bereits vorhandenes SSO-Konto für die NetApp Support Site (NSS)

Option 1: Schritte für einen Benutzer mit einem bereits vorhandenen NetApp Support Site (NSS) SSO-Konto

Schritte

1. Navigieren Sie zur NetApp -Registrierungswebsite <https://register.netapp.com>

2. Wählen Sie „Ich bin bereits als NetApp -Kunde registriert“ und wählen Sie *Data Infrastructure Insights* als Produktlinie. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS-Kunden-ID ein, indem Sie auf das Menü „Hilfe > Support“ in der Benutzeroberfläche von Data Infrastructure Insights verweisen:

Cloud Insights Support

NetApp Serial Number: 95011122233344455512	NetApp Subscription Name: A-000012345
--	---

Support activation is required to enable support with NetApp through chat, ticket or phone.
Activate Support at register.netapp.com.

☒ Check this box to allow NetApp access to your instance of Cloud Insights.

3. Füllen Sie das Registrierungsformular für Bestandskunden aus und klicken Sie auf **Senden**.

Existing Customer Registration

The fields marked with * are mandatory

First Name*	<input type="text" value="Test"/>
Last Name*	<input type="text" value="Cloud2"/>
Company*	<input type="text" value="NetApp Inc. (VSA Only)"/>
Email Address*	<input type="text" value="ng-cloudvol-csd1@netapp.com"/>
Product Line*	<input type="text" value="Cloud Insights"/>
Billing Provider *	<input type="text" value="NetApp"/>
Cloud Insights Serial # * ⓘ	<input type="text" value="e.g. 95012235021303893918"/>
NetApp Subscription Name * ⓘ	<input type="text" value="e.g. A-S0000100"/>

[Add another Serial #](#)

4. Wenn keine Fehler auftreten, wird der Benutzer auf die Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. An die E-Mail-Adresse, die mit dem für die Registrierung verwendeten NSS SSO-Benutzernamen verknüpft ist, wird innerhalb weniger Minuten eine E-Mail mit der Meldung „Für Ihr Produkt besteht jetzt Anspruch auf Support“ gesendet.
5. Dies ist eine einmalige Registrierung für die Data Infrastructure Insights NetApp -Seriennummer.

Option 2: Schritte für einen neuen NetApp Kunden ohne bereits vorhandenes NetApp Support Site (NSS) SSO-Konto

Schritte

1. Navigieren Sie zur NetApp -Registrierungswebsite <https://register.netapp.com>
2. Wählen Sie „Ich bin kein registrierter NetApp -Kunde“ und geben Sie die erforderlichen Informationen im

folgenden Beispielformular ein:

New Customer Registration

IMPORTANT: After submitting, a confirmation email will be sent to the email address filled-in the form. Please click the validation link in that email to complete the registration.

The fields marked with * are mandatory

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Company*	<input type="text"/>
Email Address*	<input type="text"/>
Office Phone*	<input type="text"/>
Alternate Phone	<input type="text"/>
Address Line 1*	<input type="text"/>
Address Line 2	<input type="text"/>
Postal Code / City*	<input type="text"/>
State/Province / Country*	<input type="text"/> - Select - ▼
NetApp Reference SN	<input type="text"/>
If you currently own a NetApp product, please provide the Serial Number for that product here in order to speed-up the validation process	
Product Line*	Cloud Insights ▼
Billing Provider *	NetApp ▼
Cloud Insights Serial # * ⓘ	<input type="text"/> e.g. 95012235021303893918
NetApp Subscription Name * ⓘ	<input type="text"/> e.g. A-S0000100

[Add another Serial #](#)

Security check:

Enter the characters shown in the image to verify your



1. Wählen Sie *Data Infrastructure Insights* als Produktlinie aus. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS-Kunden-ID ein, indem Sie auf das Menü „Hilfe > Support“ in der Benutzeroberfläche von Data Infrastructure Insights verweisen:

Cloud Insights Support

NetApp Serial Number:
95011122233344455512

NetApp Subscription Name:
A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone.
Activate Support at register.netapp.com.



Check this box to allow NetApp access to your instance of Cloud Insights.

2. Wenn keine Fehler auftreten, wird der Benutzer auf die Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. An die E-Mail-Adresse, die mit dem für die Registrierung verwendeten NSS SSO-Benutzernamen verknüpft ist, wird innerhalb weniger Stunden eine E-Mail mit der Meldung „Für Ihr Produkt besteht jetzt Anspruch auf Support“ gesendet.
3. Als neuer NetApp Kunde müssen Sie außerdem ein Benutzerkonto für die NetApp Support Site (NSS) für zukünftige Registrierungen und den Zugriff auf das Support-Portal für technischen Support und Web-Ticketing erstellen. Dieser Link befindet sich unter <https://mysupport.netapp.com/eservice/public/now.do> . Sie können Ihre neu registrierte Data Infrastructure Insights -Seriennummer angeben, um den Vorgang zu beschleunigen.
4. Dies ist eine einmalige Registrierung für die Data Infrastructure Insights NetApp Seriennummer.

Supportinformationen erhalten

NetApp bietet auf vielfältige Weise Unterstützung für Data Infrastructure Insights . Umfangreiche kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, beispielsweise Knowledgebase-Artikel (KB) oder die NetApp Community. Für Benutzer, die Data Infrastructure Insights abonniert haben, steht technischer Support per Telefon oder Webticket zur Verfügung. Für Webtickets und das Fallmanagement ist ein SSO-Konto der NetApp Support Site (NSS) erforderlich.

Self-Service-Support:

Diese Supportoptionen sind im Testmodus verfügbar und stehen rund um die Uhr kostenlos zur Verfügung:

- **Wissensdatenbank**

Wenn Sie auf die Links in diesem Abschnitt klicken, gelangen Sie zur NetApp Knowledgebase, wo Sie relevante Artikel, Anleitungen und mehr durchsuchen können.

- **"Dokumentation" ***

Wenn Sie auf den Link „Dokumentation“ klicken, gelangen Sie zu diesem Dokumentationscenter.

- **"Gemeinschaft" ***

Wenn Sie auf den Community-Link klicken, gelangen Sie zur NetApp Data Infrastructure Insights -Community, wo Sie sich mit Kollegen und Experten vernetzen können.

Es gibt auch einen Link zum Angeben **"Rückmeldung"** um uns bei der Verbesserung von Data Infrastructure Insights zu unterstützen.

Abonnement-Support

Wenn Sie über ein Data Infrastructure Insights Abonnement oder kostenpflichtigen Support für überwachte NetApp -Produkte oder -Services verfügen, können Sie zusätzlich zu den oben genannten Optionen zur Selbstunterstützung mit einem NetApp Supporttechniker zusammenarbeiten, um Ihr Problem zu lösen.



Sie müssen sich registrieren, um [Support aktivieren](#) für NetApp Cloud-Produkte. Um sich zu registrieren, gehen Sie zu NetApp's "[Registrierung für den Support von Cloud Data Services](#)".

Es wird dringend empfohlen, das Kontrollkästchen zu aktivieren, um einem NetApp -Supporttechniker während Ihrer Supportsession Zugriff auf Ihren Data Infrastructure Insights Mandanten zu gewähren. Dadurch kann der Techniker das Problem beheben und Ihnen helfen, es schnell zu lösen. Wenn Ihr Problem gelöst oder Ihre Support-Sitzung beendet ist, können Sie das Kontrollkästchen deaktivieren.

Sie können mit einer der folgenden Methoden Support anfordern. Sie müssen über ein aktives Data Infrastructure Insights -Abonnement verfügen, um diese Supportoptionen nutzen zu können:

- ["Telefon"](#)
- ["Support-Ticket"](#)

Sie können auch Vertriebsunterstützung anfordern, indem Sie auf den Link **Vertrieb kontaktieren** klicken.

Ihre Data Infrastructure Insights Seriennummer ist innerhalb des Dienstes im Menü **Hilfe > Support** sichtbar. Wenn Sie Probleme beim Zugriff auf den Dienst haben und zuvor eine Seriennummer bei NetApp registriert haben, können Sie Ihre Liste der Data Infrastructure Insights Seriennummern auch wie folgt auf der NetApp Support-Site anzeigen:

- 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:

View Installed Systems

Selection Criteria

- Select: Then, enter Value:
Enter the entire value, or use asterisk (*) for wildcard searches. (Wildcard search does not apply to Serial Numbers)
Wildcard searches may take some time.
Enter the Cluster Serial Number value without dashes.

- OR -

- Search Type*: Product Family (optional):
City (optional): State/Province (optional):
Postal Code (optional): Country (optional):

Details

If you see any discrepancies or errors in the information shown below, please submit [Feedback](#) and be sure to include the serial nu

Data Infrastructure Insights Datensammler-Supportmatrix

Informationen und Details zu unterstützten Datensammlern können Sie im* [Data Infrastructure Insights Datensammler-Supportmatrix*](#), [role=](#) .

Unabhängig von Ihrem Abonnement finden Sie unter **Hilfe > Support** Links zu mehreren Kursangeboten der NetApp University, die Ihnen dabei helfen, Data Infrastructure Insights optimal zu nutzen. Schauen Sie sich an!

Datensammlerreferenz – Infrastruktur

Anbieterspezifische Referenz

Die Themen in diesem Abschnitt bieten anbieterspezifische Referenzinformationen. In den meisten Fällen ist die Konfiguration eines Datensammlers unkompliziert. 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 dessen Datensammlern anzuzeigen.

Konfigurieren des Amazon EC2-Datensammlers

Data Infrastructure Insights verwendet den Amazon EC2-Datensammler, um Bestands- und Leistungsdaten von EC2-Instances zu erfassen.

Anforderungen

Um Daten von Amazon EC2-Geräten zu erfassen, benötigen Sie die folgenden Informationen:

- Sie müssen über eines der folgenden Elemente verfügen:
 - Die **IAM-Rolle** für Ihr Amazon EC2-Cloud-Konto, wenn Sie die IAM-Rollenauthentifizierung verwenden. Die IAM-Rolle gilt nur, wenn Ihre Erfassungseinheit auf einer AWS-Instanz installiert ist.
 - Die **IAM-Zugriffsschlüssel-ID** und der geheime Zugriffsschlüssel für Ihr Amazon EC2-Cloud-Konto, wenn Sie die IAM-Zugriffsschlüssel-Authentifizierung verwenden.
- Sie müssen über die Berechtigung „Organisation auflisten“ verfügen
- Port 443 HTTPS
- EC2-Instanzen können als virtuelle Maschine oder (weniger natürlich) als Host gemeldet werden. EBS-Volumes können sowohl als von der VM verwendete VirtualDisk als auch als DataStore gemeldet werden, der die Kapazität für die VirtualDisk bereitstellt.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID (z. B. AKIAIOSFODNN7EXAMPLE) und einem geheimen Zugriffsschlüssel (z. B. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Sie verwenden Zugriffsschlüssel, um programmgesteuerte Anfragen zu signieren, die Sie an EC2 stellen, wenn Sie die Amazon EC2 SDKs, REST oder Query-API-Operationen verwenden. Diese Schlüssel werden Ihnen 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	AWS-Region auswählen

Feld	Beschreibung
IAM-Rolle	Nur zur Verwendung, wenn es auf einer AU in AWS erworben wurde. Weitere Informationen finden Sie weiter unten IAM-Rolle .
AWS IAM-Zugriffsschlüssel-ID	Geben Sie die AWS IAM-Zugriffsschlüssel-ID ein. Erforderlich, wenn Sie keine IAM-Rolle verwenden.
Geheimer AWS IAM-Zugriffsschlüssel	Geben Sie den geheimen AWS IAM-Zugriffsschlüssel ein. Erforderlich, wenn Sie keine IAM-Rolle verwenden.
Mir ist bekannt, dass AWS mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass AWS Ihnen die API-Anfragen in Rechnung stellt, die durch Data Infrastructure Insights -Polling gestellt werden.

Erweiterte Konfiguration

Feld	Beschreibung
Zusätzliche Regionen einschließen	Geben Sie zusätzliche Regionen an, die in die Abfrage einbezogen werden sollen.
Cross-Account-Rolle	Rolle für den Zugriff auf Ressourcen in verschiedenen AWS-Konten.
Inventarabfrageintervall (min)	Der Standardwert ist 60
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Tags zu filtern	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Tags ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Tag-Schlüssel“ nicht leer sein.
Tag-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf + Tag filtern , um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Tags auf der VM übereinstimmen. Tag-Schlüssel ist erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM gefiltert, solange sie mit dem Tag-Schlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800
Namespace für CloudWatch-Agent-Metriken	Namespace in EC2/EBS, aus dem Daten gesammelt werden sollen. Beachten Sie, dass Data Infrastructure Insights diese umbenannten Daten möglicherweise nicht erfassen kann, wenn die Namen der Standardmetriken in diesem Namespace geändert werden. Es wird empfohlen, die Standardmetrikenamen beizubehalten.

IAM-Zugriffsschlüssel

Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Benutzer oder den Stammbenutzer des AWS-Kontos. Zugriffsschlüssel werden verwendet, um programmgesteuerte Anfragen an die AWS CLI oder

AWS API zu signieren (direkt oder mithilfe des AWS SDK).

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Wenn Sie die Authentifizierung mit *IAM-Zugriffsschlüssel* verwenden (im Gegensatz zur Authentifizierung mit *IAM-Rolle*), müssen Sie zur Authentifizierung von Anfragen sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel zusammen verwenden. Weitere Informationen finden Sie in der Amazon-Dokumentation unter "[Zugriffsschlüssel](#)".

IAM-Rolle

Wenn Sie die Authentifizierung mit *IAM-Rolle* verwenden (im Gegensatz zur Authentifizierung mit *IAM-Zugriffsschlüssel*), müssen Sie sicherstellen, dass die von Ihnen erstellte oder angegebene Rolle über die entsprechenden Berechtigungen für den Zugriff auf Ihre Ressourcen verfügt.

Wenn Sie beispielsweise eine IAM-Rolle mit dem Namen *InstanceEc2ReadOnly* erstellen, müssen Sie die Richtlinie so einrichten, dass EC2 für diese IAM-Rolle die schreibgeschützte Listenzugriffsberechtigung für alle EC2-Ressourcen erhält. Zusätzlich müssen Sie STS (Security Token Service)-Zugriff gewähren, damit diese Rolle kontoübergreifend Rollen übernehmen darf.

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie sie anhängen, wenn Sie eine neue EC2-Instanz oder eine vorhandene EC2-Instanz erstellen.

Nachdem Sie die IAM-Rolle *InstanceEc2ReadOnly* an eine EC2-Instanz angehängt haben, können Sie die temporären Anmeldeinformationen über die Instanzmetadaten anhand des IAM-Rollenamens abrufen und sie verwenden, um mit jeder auf dieser EC2-Instanz ausgeführten Anwendung auf AWS-Ressourcen zuzugreifen.

Weitere Informationen finden Sie in der Amazon-Dokumentation unter "[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 Data Infrastructure Insights -Anmerkungen

Der Amazon EC2-Datensammler enthält eine Option, mit der Sie Data Infrastructure Insights -Anmerkungen mit auf EC2 konfigurierten Tags füllen können. Die Anmerkungen müssen genau wie die EC2-Tags benannt sein. Data Infrastructure Insights füllt immer gleichnamige Textanmerkungen aus und unternimmt den bestmöglichen Versuch, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) auszufüllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht ausfüllen kann, kann es erforderlich sein, die Anmerkung zu entfernen und als Texttyp neu zu erstellen.

Beachten Sie, dass bei AWS die Groß- und Kleinschreibung beachtet wird, während bei Data Infrastructure Insights die Groß- und Kleinschreibung nicht beachtet wird. Wenn Sie also in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“ und in EC2 Tags mit den Namen „OWNER“, „Owner“ und „owner“ erstellen, werden alle EC2-Varianten von „owner“ der Annotation „OWNER“ von Cloud Insight zugeordnet.

Zusätzliche Regionen einschließen

Im Abschnitt **Erweiterte Konfiguration** des AWS Data Collector können Sie das Feld **Zusätzliche Regionen einschließen** so festlegen, dass zusätzliche Regionen eingeschlossen werden, getrennt durch Komma oder Semikolon. Standardmäßig ist dieses Feld auf **us-.*** eingestellt, wodurch alle US-amerikanischen AWS-Regionen erfasst werden. Um in *allen* Regionen zu sammeln, setzen Sie dieses Feld auf **.***. Wenn das Feld **Zusätzliche Regionen einschließen** leer ist, sammelt der Datensammler Daten für die im Feld **AWS-Region** angegebenen Assets, wie im Abschnitt **Konfiguration** angegeben.

Sammeln von AWS-Unterkonten

Data Infrastructure Insights unterstützt die Erfassung untergeordneter Konten für AWS innerhalb eines einzelnen AWS-Datensammlers. Die Konfiguration für diese Sammlung wird in der AWS-Umgebung durchgeführt:

- Sie müssen jedes untergeordnete Konto so konfigurieren, dass es über eine AWS-Rolle verfügt, die der Hauptkonto-ID den Zugriff auf EC2-Details des untergeordneten Kontos ermöglicht.
- Für jedes untergeordnete Konto muss der Rollename als dieselbe Zeichenfolge konfiguriert sein.
- Geben Sie diese Rollennamenzeichenfolge in den Abschnitt **Erweiterte Konfiguration** des Data Infrastructure Insights AWS Data Collector im Feld **Kontoübergreifende Rolle** ein.
- Das Konto, unter dem der Collector installiert ist, muss über die Berechtigung „Delegierter Zugriffsadministrator“ verfügen. Siehe die ["AWS-Dokumentation"](#) für weitere Informationen.

Best Practice: Es wird dringend empfohlen, dem EC2-Hauptkonto die von AWS vordefinierte Richtlinie *AmazonEC2ReadOnlyAccess* zuzuweisen. Außerdem sollte dem in der Datenquelle konfigurierten Benutzer mindestens die vordefinierte Richtlinie *AWSOrganizationsReadOnlyAccess* zugewiesen sein, um AWS abfragen zu können.

Im Folgenden finden Sie Informationen zum Konfigurieren Ihrer Umgebung, damit Data Infrastructure Insights Daten von untergeordneten AWS-Konten erfassen kann:

["Tutorial: Zugriff über AWS-Konten hinweg mithilfe von IAM-Rollen delegieren"](#)

["AWS-Setup: Bereitstellen des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto, das Ihnen gehört"](#)

["Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"](#)

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Amazon FSx for NetApp ONTAP Datenkollektor

Dieser Datensammler erfasst Bestands- und Leistungsdaten von Amazon FSx for NetApp ONTAP. Dieser Datensammler wird schrittweise in allen Serviceregionen von Data Infrastructure Insights verfügbar gemacht. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie das Symbol für diesen Collector in Ihrer Data Infrastructure Insights -Umgebung nicht sehen.



Dieser Data Infrastructure Insights Collector erfordert einen ONTAP Benutzer mit einer *Filesystem-Scoped*-Rolle. Bitte überprüfen Sie die AWS ["Rollen und Regeln"](#) Informationen zu verfügbaren Optionen finden Sie in der Dokumentation. Derzeit unterstützt AWS nur eine Art von Benutzerrolle mit Dateisystembereich, nämlich *fsxadmin*. Dies ist die geeignete Rolle für den Data Infrastructure Insights -Collector. Dem Benutzer sollten außerdem alle drei dieser Anwendungen zugewiesen sein: http, ontapi, ssh.

Terminologie

Data Infrastructure Insights erfasst Bestands- und Leistungsdaten vom FSx- NetApp Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
LUN	Volumen
Volumen	Internes Volumen

FSx- NetApp -Terminologie

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der FSx- NetApp Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Modellnamen innerhalb dieses Clusters.
- Anbieter – AWS
- Seriennummer – Die Seriennummer des Arrays.
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Rohkapazität – Basis-2-Summe des gesamten dem FSx-Dateisystem zugewiesenen SSD-Speichers.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- IOPS – die Summe der IOPs aller diesem Speicherpool zugewiesenen Volumes.
- Durchsatz – der Gesamtdurchsatz aller diesem Speicherpool zugewiesenen Volumes.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Konto mit der Rolle „fsxadmin“ haben, dem drei Anwendungen zugewiesen sind

- ssh, ontapi, http
- Zu den Kontodetails gehören Benutzername und Passwort.
- Portanforderungen: 443

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domänenname des NetApp -Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp -Cluster

Erweiterte Metriken

Dieser Datensammler sammelt die folgenden erweiterten Metriken aus dem FSx für NetApp ONTAP -Speicher:

- fpolicy
- nfsv3
- nfsv3:Knoten
- nfsv4
- nfsv4_1
- nfsv4_1:Knoten
- nfsv4:Knoten
- Richtliniengruppe
- qtree
- Volumen
- Arbeitslastvolumen

Beachten Sie, dass FSx CLI- und API-Befehle einige Kapazitätswerte abrufen, die Data Infrastructure Insights ZAPI nicht erfasst. Daher können bestimmte Kapazitätswerte (z. B. für Speicherpools) in Data Infrastructure Insights anders sein als auf dem FSx selbst.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.

Problem:	Versuchen Sie Folgendes:
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen 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: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des Azure-Compute-Datensammlers

Data Infrastructure Insights verwendet den Azure Compute-Datensammler, um Bestands- und Leistungsdaten von Azure Compute-Instanzen zu erfassen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen.

- Portanforderung: 443 HTTPS
- Azure OAuth 2.0-Umleitungs-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 (Leserrolle erforderlich)
- Azure-Dienstprinzipal-Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen für die Data Infrastructure Insights Erkennung ein Azure-Konto einrichten.

Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Anwendung in Azure registrieren, verfügen Sie über die erforderlichen Anmeldeinformationen, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Unter dem folgenden Link wird beschrieben, wie Sie das Konto für die Erkennung 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 (Leserrolle erforderlich)	Anmelde-ID für Azure. Erfordert Zugriff mit der Rolle „Leser“.
Azure-Mandanten-ID	Microsoft-Mandanten-ID
Azure-Dienstprinzipalauthentifizierungsschlüssel	Login-Authentifizierungsschlüssel
Mir ist bekannt, dass Microsoft mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass Microsoft Ihnen für API-Anfragen, die durch Insight-Polling gestellt werden, eine Rechnung stellt.

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Tags zu filtern	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Tags ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Tag-Schlüssel“ nicht leer sein.
Tag-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf + Tag filtern , um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüsseln und Werten filtern, die mit den Schlüsseln und Werten der Tags auf der VM übereinstimmen. Tag-Schlüssel ist erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM gefiltert, solange sie mit dem Tag-Schlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Broadcom

Brocade Network Advisor-Datensammler

Data Infrastructure Insights verwendet den Brocade Network Advisor-Datensammler, um Bestands- und Leistungsdaten von Brocade -Switches zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade Network Advisor-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten

verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Logischer Switch	Logischer Switch

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 auf dem BNA-Server. Auf dem BNA-Server muss Version 14.2.1 oder höher ausgeführt werden.
- IP-Adresse des Brocade Network Advisor-Servers
- Benutzername und Kennwort für ein Administratorkonto
- Portanforderung: 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	Administratorkennwort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Standardport 443) oder HTTP (Standardport 80)
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Passwort	Passwort für den Switch
Inventarabfrageintervall (min)	Der Standardwert ist 40
Bericht Access Gateway	Aktivieren Sie dieses Kontrollkästchen, um Geräte in den Access Gateway-Modus einzuschließen
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Sie erhalten eine Meldung, dass mehr als ein Knoten am Access Gateway-Port angemeldet ist oder dass der Datensammler das Access Gateway-Gerät nicht erkennen kann.	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und ob alle angeschlossenen WWNs den Erwartungen entsprechen. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen werden die NPV-Gerätedaten durch die Erfassung des Core Fabric Switch erfasst.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Brocade FC Switch-Datenkollektor

Data Infrastructure Insights verwendet die Datenquelle Brocade FC Switch (SSH), um den Bestand für Brocade oder umbenannte Switch-Geräte zu ermitteln, auf denen die Factored Operating System (FOS)-Firmware 4.2 und höher ausgeführt wird. Es werden Geräte sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade FC Switch-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
Virtuelles Volume	Volumen
LSAN-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die Data Infrastructure Insights Acquisition Unit (AU) initiiert Verbindungen zum TCP-Port 22 auf Brocade -Switches, um Inventardaten zu erfassen. Die AU initiiert außerdem Verbindungen zum UDP-Port 161, um Leistungsdaten zu erfassen.
- Es muss eine IP-Konnektivität zu allen Switches im Fabric bestehen. Wenn Sie das Kontrollkästchen „Alle

Switches im Fabric erkennen“ aktivieren, identifiziert Data Infrastructure Insights alle Switches im Fabric. Allerdings ist für die Erkennung dieser zusätzlichen Switches eine IP-Verbindung erforderlich.

- Für alle Switches im Fabric ist global dasselbe Konto erforderlich. Sie können PuTTY (Open Source-Terminalemulator) verwenden, um den Zugriff zu bestätigen.
- Die Ports 161 und 162 müssen für alle Switches im Fabric für die SNMP-Leistungsabfrage geöffnet sein.
- SNMP-Nur-Lese-Community-String

Konfiguration

Feld	Beschreibung
IP wechseln	IP-Adresse oder vollqualifizierter Domänenname des EFC-Servers
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch
SNMP	SNMP-Version
SNMP-Community-String	SNMP-schreibgeschützte Community-Zeichenfolge für den Zugriff auf den Switch
SNMP-Benutzername	SNMP-Benutzername
SNMP-Passwort	SNMP-Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Stoffname	Vom Datensammler zu meldender Stoffname. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 15.
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen
Aktive Admin-Domänen	Wählen Sie aus, ob Sie Admin-Domänen verwenden
MPR-Daten abrufen	Wählen Sie diese Option aus, um Routingdaten von Ihrem Multiprotokoll-Router abzurufen.
Überfüllung aktivieren	Wählen Sie diese Option, um die Erfassung beim Empfang eines SNMP-Traps vom Gerät zu aktivieren. Wenn Sie „Trapping aktivieren“ auswählen, müssen Sie auch SNMP aktivieren.
Mindestzeit zwischen Traps (Sek.)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen. Der Standardwert ist 10.
Entdecken Sie alle Switches im Fabric	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen
Wählen Sie HBA gegenüber Zonenaliasen	Wählen Sie, ob HBA- oder Zonenalias bevorzugt werden sollen

Feld	Beschreibung
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
SNMP-Authentifizierungsprotokoll	SNMP-Authentifizierungsprotokoll (nur SNMP v3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort (nur SNMP v3)
SNMP-Wiederholungen	Anzahl der SNMP-Wiederholungsversuche

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Die Inventarerfassung der Brocade -Datenquelle schlägt mit folgendem Fehler fehl: <Datum> <Uhrzeit> FEHLER [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Fehler 2 von 2: <Datenquellenname> [Interner Fehler] – Das Modell für Gerät <IP> konnte nicht generiert werden. Fehler beim Erkennen der Eingabeaufforderung ([Gerätename <Name>]: Das Modell für Gerät <IP> konnte nicht generiert werden. Fehler bei der Eingabeaufforderung)	Das Problem kann dadurch verursacht werden, dass der Brocade -Switch zu lange braucht, um mit einer Eingabeaufforderung zurückzukehren, und das Standard-Timeout von 5 Sekunden überschreitet. Versuchen Sie, in den erweiterten Konfigurationseinstellungen des Datensammlers in Data Infrastructure Insights den Wert <i>SSH-Banner-Wartezeitüberschreitung (Sek.)</i> auf einen höheren Wert zu erhöhen.
Fehler: „Data Infrastructure Insights hat eine ungültige Chassis-Rolle erhalten“	Überprüfen Sie, ob dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Chassis-Rolle erteilt wurde.
Fehler: „Nicht übereinstimmende Gehäuse-IP-Adresse“	DII unterstützt grundsätzlich KEINE Netzwerkadressübersetzung oder Portadressübersetzung zwischen der Erfassungseinheit und Geräten. DII erkennt möglicherweise, dass der Hostname/die IP-Adresse in der Collector-Konfiguration NICHT mit einer der Adressen übereinstimmt, die das Gerät zu haben glaubt.
Erhalten Sie eine Meldung, dass mehr als ein Knoten am Access Gateway-Port angemeldet ist	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und ob alle angeschlossenen WWNs den Erwartungen entsprechen. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen werden die NPV-Gerätedaten durch die Erfassung des Core Fabric Switch erfasst.

Problem:	Versuchen Sie Folgendes:
Fehler:Maximale Remote-Sitzungen für die Anmeldung...	FOS hat unterschiedliche Beschränkungen für die Anzahl unterstützter gleichzeitiger SSH-Sitzungen pro Benutzerrolle. Die SSH-Sitzung von DII zu diesem Gerät wird bei der Anmeldung wegen Verletzung dieser Grenzwerte abgelehnt. Dies kann ein Zeichen dafür sein, dass Sie doppelte Sammler haben, die denselben Vermögenswert entdecken, was vermieden werden sollte

Performance

Problem:	Versuchen Sie Folgendes:
Die Leistungserfassung schlägt mit der Meldung „Zeitüberschreitung beim Senden der SNMP-Anforderung“ fehl.	Abhängig von Abfragevariablen und Switch-Konfiguration können einige Abfragen das Standard-Timeout überschreiten. "Weitere Informationen" .
Die Leistungserfassung schlägt fehl mit ... Zeilenduplikate in der SNMP-Tabelle gefunden ...	DII hat fehlerhafte SNMP-Antworten erkannt. Sie verwenden wahrscheinlich FOS 8.2.3e. Aktualisieren Sie auf 8.2.3e2 oder höher.
Leistungserfassungen schlagen mit ...Unbekanntem Benutzernamen... fehl	Sie haben Ihren DII-Collector mit einem „SNMP-Benutzernamen“-Wert konfiguriert, der nicht in einen der SNMPv3-Benutzersteckplätze passt. Durch das einfache Erstellen eines Benutzers auf Brocade FOS wird dieser NICHT unbedingt als SNMPv3-Benutzer aktiviert – Sie müssen ihn in einem der v3-Benutzerslots platzieren.
Leistungserfassungen schlagen mit ...Nicht unterstützte Sicherheitsstufe... fehl.	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 konfiguriert, jedoch mit Verschlüsselungs- (auch Datenschutz-) und/oder Autorisierungseinstellungen, die auf dem betreffenden Gerät nicht aktiviert sind.
Die Leistungserfassung schlägt fehl mit ... Leeres Datenschutzkennwort ist nur für das Datenschutzprotokoll NONE zulässig	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 mit einem Verschlüsselungs- bzw. Datenschutzprotokoll (AES usw.) konfiguriert, aber Sie haben einen leeren Wert für „SNMP-Datenschutzkennwort“, sodass DII keine verschlüsselten SNMPv3-Datenflüsse mit diesem Gerät aushandeln kann.
Die Leistungserfassung schlägt mitVF:nn fehl, Fehler: Kein Zugriff...	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 auf einem Gerät mit mehreren aktivierten virtuellen Fabrics konfiguriert, aber der SNMPv3-Benutzer verfügt NICHT über Rechte für VF NN. DII unterstützt keine teilweise Erkennung eines physischen Assets. Sie sollten DII immer proaktiv Zugriff auf alle 128 möglichen VFs gewähren, da DII immer versucht, Leistungsdaten für alle vorhandenen VFs auf einem bestimmten physischen Gerät abzurufen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Brocade FOS REST-Datenkollektor

Data Infrastructure Insights verwendet den Brocade FOS REST-Collector, um Inventar und Leistung für Brocade -Switch-Geräte mit FabricOS (FOS)-Firmware 8.2 und höher zu ermitteln. Bitte beachten Sie, dass frühe 8.2-FOS-Versionen möglicherweise REST-API-Fehler aufweisen. Es wird dringend empfohlen, die neuste FOS-Version auszuführen, die Ihre Plattform unterstützt.

Bitte beachten Sie: Die standardmäßige „Benutzer“-Ebene von FOS ist für Data Infrastructure Insights nicht leistungsfähig genug, um alle logischen Aspekte eines Geräts anzuzeigen. Wir benötigen ein Benutzerkonto mit aktivierter „Chassis-Rolle“ sowie Berechtigungen für alle auf einem Switch konfigurierten virtuellen Fabrics.

Hier ist ein Beispiel, wie Sie ein Benutzerkonto mit den geringsten Berechtigungen für die Verwendung von Data Infrastructure Insights in einer SSH-Sitzung mit einem FOS-Gerät erstellen können:

```
userConfig --add NetAppCIUser -r Benutzer -l 1-128 -c Benutzer -p Qwerty!
```

Dadurch wird ein Benutzer „NetAppCIUser“ mit dem Kennwort „Qwerty!“ erstellt. Dieser Benutzer hat die Rolle „Benutzer“ (-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 erkennen, die Teil aller Fabrics sind, zu denen der Switch gehört.

Bitte beachten Sie: Der standardmäßige schreibgeschützte Benutzer „Benutzer“ von FOS verfügt NICHT über Anzeigeberechtigungen für alle virtuellen Fabrics und auch nicht über Berechtigungen für die „Chassis-Rolle“. Dies bedeutet, dass die Erfolgsaussichten bei der Verwendung von „Benutzer“ mit Data Infrastructure Insights gering sind, da hierfür sowohl die physische als auch die logische Konfiguration des FOS-Geräts bekannt sein muss.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Brocade FOS REST-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
Virtuelles Gewebe, physisches Gewebe	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
LSAN-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuzuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Es muss eine TCP-Konnektivität zu allen Switches im Fabric bestehen. Dieser Datensammlertyp probiert nahtlos sowohl HTTP als auch HTTPS für jedes Gerät im Fabric aus. Wenn Sie das Kontrollkästchen „Alle Switches im Fabric erkennen“ aktivieren, identifiziert Data Infrastructure Insights alle Switches im Fabric. Allerdings ist für die Erkennung dieser zusätzlichen Switches eine TCP-Verbindung erforderlich.
- Für alle Switches im Fabric ist global dasselbe Konto erforderlich. Sie können den Zugriff über die Weboberfläche des Geräts bestätigen.

Konfiguration

Feld	Beschreibung
IP wechseln	IP-Adresse oder vollqualifizierter Domänenname des FOS-Switches
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch

Erweiterte Konfiguration

Feld	Beschreibung
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IPv4-Adressen, die von der Abfrage ausgeschlossen werden sollen.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 60.
Entdecken Sie alle Switches im Fabric	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen.
Wählen Sie HBA gegenüber Zonenaliasen	Wählen Sie, ob HBA- oder Zonenalias bevorzugt werden sollen.
Anschlussart	HTTP oder HTTPS.
Beachten Sie, dass diese Einstellung nur ändert, welches Protokoll CI zuerst pro Gerät zu verwenden versucht. CI versucht automatisch das entgegengesetzte Protokoll, wenn die Standardeinstellung fehlschlägt.	TCP-Port überschreiben
Geben Sie einen Port an, wenn Sie nicht den Standardport verwenden.	Leistungsabfrageintervall (Sek.)

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Die Testfunktion warnt mich, dass auf ein Protokoll nicht zugegriffen werden kann	Ein bestimmtes Brocade FOS 8.2+-Gerät möchte nur über HTTP oder HTTPS kommunizieren. Wenn auf einem Switch ein digitales Zertifikat installiert ist, gibt der Switch HTTP-Fehler aus, wenn versucht wird, mit ihm über unverschlüsseltes HTTP statt HTTPS zu kommunizieren. Die Testfunktion versucht, sowohl mit HTTP als auch mit HTTPS zu kommunizieren. Wenn der Test ergibt, dass ein Protokoll erfolgreich ist, können Sie den Collector sicher speichern und müssen sich keine Sorgen machen, dass das andere Protokoll nicht erfolgreich war. Der Collector versucht während der Erfassung beide Protokolle und schlägt nur fehl, wenn keines von beiden funktioniert.
Fehler: Inventarisierung schlägt mit 401 Unauthorized fehl...Ungültiger Sitzungsschlüssel...	Dies ist ein eindeutiger Fehler in einigen sehr frühen 8.2 FOS-Versionen wie 8.2.1c, die die HTTP-Basisauthentifizierung NICHT richtig unterstützen. Upgrade auf eine spätere Version 8.2 oder 9.*
Fehler: „Data Infrastructure Insights hat eine ungültige Chassis-Rolle erhalten“	Überprüfen Sie, ob dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Chassis-Rolle erteilt wurde.
Fehler: „Nicht übereinstimmende Gehäuse-IP-Adresse“	Ändern Sie die Datenquellenkonfiguration, um die IP-Adresse des Gehäuses zu verwenden.
Die Inventur schlägt mit der Fehlermeldung „403 Forbidden“ fehl	Dies können einfach ungültige Anmeldeinformationen sein oder ein Hinweis darauf, dass Sie versuchen, eine Rolle mit unzureichenden Befugnissen zu verwenden. Bedenken Sie, dass Benutzer auf der Ebene „Benutzer“ NICHT über die erforderlichen Rechte für die „Chassis-Rolle“ verfügen oder keinen Anzeigenzugriff auf nicht standardmäßige virtuelle Fabrics haben.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Cisco MDS Fabric Switches Datensammler

Data Infrastructure Insights verwendet den Datensammler von Cisco MDS Fabric Switches, um den Bestand für Cisco MDS Fabric Switches sowie eine Vielzahl von Cisco Nexus FCoE-Switches zu ermitteln, auf denen der FC-Dienst aktiviert ist.

Darüber hinaus können Sie mit diesem Datensammler viele Modelle von Cisco -Geräten entdecken, die im NPV-Modus laufen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Cisco FC Switch-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Schalten	Schalten
Hafen	Hafen
VSAN	Stoff
Zone	Zone
Logischer Switch	Logischer Switch
Nameserver-Eintrag	Nameserver-Eintrag
Inter-VSAN-Routing (IVR)-Zone	IVR-Zone

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse eines Switches im Fabric oder einzelner Switches
- Chassis-Erkennung, um die Fabric-Erkennung zu ermöglichen
- Bei Verwendung von SNMP V2: schreibgeschützter Community-String
- Port 161 wird für den Zugriff auf das Gerät verwendet

Konfiguration

Feld	Beschreibung
Cisco Switch-IP	IP-Adresse oder vollqualifizierter Domänenname des Switches
SNMP -Version	Wählen Sie V1, V2 oder V3. Für die Leistungserfassung ist V2 oder höher erforderlich.
SNMP-Community-String	SNMP-Nur-Lese-Community-String für den Zugriff auf den Switch (gilt nicht für SNMP v3)
Benutzername	Benutzername für den Switch (nur SNMP v3)
Passwort	Für den Switch verwendetes Passwort (nur SNMPv3)

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen (Standard 40 Minuten)
SNMP-Authentifizierungsprotokoll	SNMP-Authentifizierungsprotokoll (nur SNMPv3)
SNMP-Datenschutzprotokoll	SNMP-Datenschutzprotokoll (nur SNMPv3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort
SNMP-Wiederholungen	Anzahl der SNMP-Wiederholungsversuche
SNMP-Zeitüberschreitung (ms)	SNMP-Timeout (Standard 5000 ms)

Feld	Beschreibung
Überfüllung aktivieren	Wählen Sie diese Option, um das Trapping zu aktivieren. Wenn Sie Trapping aktivieren, müssen Sie auch SNMP-Benachrichtigungen aktivieren.
Mindestzeit zwischen Traps (Sek.)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard 10 Sekunden)
Entdecken Sie alle Fabric Switches	Wählen Sie diese Option aus, um alle Switches im Fabric zu erkennen
Ausgeschlossene Geräte	Durch Kommas getrennte Liste von Geräte-IPs, die von der Abfrage ausgeschlossen werden sollen
Enthaltene Geräte	Durch Kommas getrennte Liste der Geräte-IPs, die in die Abfrage einbezogen werden sollen
Gerätetyp prüfen	Wählen Sie diese Option aus, um nur die Geräte zu akzeptieren, die sich ausdrücklich als Cisco -Geräte ausgeben
Erster Aliastyp	Geben Sie eine erste Präferenz für die Auflösung des Alias an. Wählen Sie aus Folgendem: Device Alias Dies ist ein benutzerfreundlicher Name für einen Port-WWN (pWWN), der bei Bedarf in allen Konfigurationsbefehlen verwendet werden kann. Alle Switches der Cisco MDS 9000-Familie unterstützen Distributed Device Alias Services (Gerätealias). Keine Kein Alias melden. Portbeschreibung Eine Beschreibung zur Identifizierung des Ports in einer Portliste. Zonenalias (alle) Ein benutzerfreundlicher Name für einen Port, der nur für die aktive Konfiguration verwendet werden kann. Dies ist die Standardeinstellung.
Zweiter Aliastyp	Geben Sie eine zweite Präferenz für die Auflösung des Alias an
Dritter Aliastyp	Geben Sie eine dritte Präferenz für die Auflösung des Alias an
Aktivieren Sie die SANTap-Proxy-Modus-Unterstützung	Wählen Sie aus, ob Ihr Cisco Switch SANTap im Proxy-Modus verwendet. Wenn Sie EMC RecoverPoint verwenden, verwenden Sie wahrscheinlich SANTap.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen (Standard 300 Sekunden)

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Chassis konnte nicht erkannt werden – es wurden keine Switches erkannt	<ul style="list-style-type: none"> • Pingen Sie das Gerät mit der konfigurierten IP an. • Melden Sie sich über die GUI des Cisco Device Managers beim Gerät an. • Melden Sie sich über die CLI beim Gerät an. • Versuchen Sie, SNMP Walk auszuführen.
Fehler: Gerät ist kein Cisco MDS-Switch	<ul style="list-style-type: none"> • Stellen Sie sicher, dass die für das Gerät konfigurierte Datenquellen-IP richtig ist. • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an. • Melden Sie sich über die CLI beim Gerät an.
Fehler: Data Infrastructure Insights kann den WWN des Switches nicht abrufen.	Dies ist möglicherweise kein FC- oder FCoE-Switch und wird daher möglicherweise nicht unterstützt. Stellen Sie sicher, dass es sich bei der in der Datenquelle konfigurierten IP/FQDN tatsächlich um einen FC/FCoE-Switch handelt.
Fehler: Es wurden mehrere Knoten gefunden, die am NPV-Switch-Port angemeldet sind.	Deaktivieren Sie die direkte Erfassung des NPV-Schalters
Fehler: Es konnte keine Verbindung zum Switch hergestellt werden	<ul style="list-style-type: none"> • Stellen Sie sicher, dass das Gerät aktiv ist. • Überprüfen Sie die IP-Adresse und den Abhörport. • Pingen Sie das Gerät an. • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an. • Melden Sie sich über die CLI beim Gerät an. • Führen Sie einen SNMP-Walk aus.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Leistungserfassung wird von SNMP v1 nicht unterstützt	<ul style="list-style-type: none"> • Datenquelle bearbeiten und Switch-Leistung deaktivieren • Datenquelle und Switch-Konfiguration ändern, um SNMP v2 oder höher zu verwenden

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Cohesity SmartFiles-Datensammler

Dieser auf REST-API basierende Collector erwirbt einen Cohesity-Cluster, erkennt die „Ansichten“ (als interne Volumes von Data Infrastructure Insights) und die verschiedenen Knoten und sammelt Leistungsmetriken.

Konfiguration

Feld	Beschreibung
Cohesity-Cluster-IP	IP-Adresse des Cohesity-Clusters
Benutzername	Benutzername für den Cohesity-Cluster
Passwort	Für den Cohesity-Cluster verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die TCP-Kommunikation mit dem Cohesity-Cluster verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (min)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 900 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell

Datensammler der Dell EMC XC-Serie

Data Infrastructure Insights verwendet diesen Datensammler, um Bestands- und Leistungsinformationen für die Speicher-Arrays der Dell EMC XC-Serie zu ermitteln.

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	IP-Adresse des XC-Servers
Benutzername	Benutzername für den XC-Server
Passwort	Für den XC-Server verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die TCP-Kommunikation mit dem XC-Server verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (min)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC

DELL EMC Data Domain-Datenkollektor

Dieser Datensammler sammelt Bestands- und Leistungsinformationen von DELL EMC Data Domain-Deduplizierungsspeichersystemen. Zum Konfigurieren dieses Datensammlers müssen Sie bestimmte Konfigurationsanweisungen und Verwendungsempfehlungen befolgen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Data Domain-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Anordnung	Storage
FC-Anschluss	Hafen
Dateisystem	Internes Volumen
Quote	Quote
NFS- und CIFS-Freigabe	Dateifreigabe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- IP-Adresse des Data Domain-Geräts
- Nur-Lese-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
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
SSH-Port	SSH-Dienstport

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Konfigurieren des EMC ECS-Datenkollektors

Dieser Datensammler erfasst Bestands- und Leistungsdaten von EMC ECS-Speichersystemen. Zur Konfiguration benötigt der Datensammler eine IP-Adresse oder den Hostnamen des ECS-Clusters sowie einen Benutzernamen und ein Passwort.



Dell EMC ECS wird zu einem anderen Preis als Raw TB und Managed Unit berechnet. Jede 40 TB unformatierte ECS-Kapazität wird als 1 berechnet ["Verwaltete Einheit \(MU\)"](#).

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom ECS-Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
Mieter	Speicherpool
Eimer	Internes Volumen
Scheibe	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse oder ein Hostname des ECS-Clusters
- Ein Benutzername und ein Passwort für das ECS-System
- Port 4443 (HTTPS). Erfordert ausgehende Konnektivität zum TCP-Port 4443 auf dem ECS-System.

Konfiguration

Feld	Beschreibung
ECS-Host	IP-Adresse oder vollqualifizierter Domänenname des ECS-Systems

Feld	Beschreibung
ECS-Host-Port	Für die Kommunikation mit dem ECS-Host verwendeter Port
ECS-Benutzer-ID	Benutzer-ID für ECS
Passwort	Für ECS verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert beträgt 360 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Nicht genügend Daten gesammelt.	* Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend. * Warten Sie länger
Fehler: Das Leistungsabfrageintervall ist zu groß.	Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei <code>logfile</code> und ändern Sie das Abfrageintervall entsprechend

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC PowerScale-Datenkollektor

Data Infrastructure Insights verwendet den SSH-Datensammler Dell EMC PowerScale (früher Isilon), um Bestands- und Leistungsdaten vom PowerScale-Scale-Out-NAS-Speicher zu erfassen.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Dateisystem	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- Administratorberechtigungen 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	Für den PowerScale-Cluster verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
SSH-Port	SSH-Dienstport. Der Standardwert ist 22.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Für die rollenbasierte Verwaltung nicht aktivierte Befehle erfordern Root-Benutzerzugriff“	* Überprüfen Sie, ob der Benutzer über die Berechtigung verfügt, die folgenden Befehle auf dem Gerät auszuführen: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Überprüfen Sie, ob die im Assistenten verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen
„Interner Fehler“ mit Fehlermeldungen „Ausführung des Befehls <Ihr Befehl> fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>.“ Problem mit der Berechtigung zum Ausführen des Sudo-Befehls“	Stellen Sie sicher, dass der Benutzer über Sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC Isilon/PowerScale REST-Datensammler

Data Infrastructure Insights verwendet den Dell EMC Isilon/PowerScale REST-Datensammler, um Bestands- und Leistungsdaten vom Dell EMC Isilon- oder PowerScale-Speicher zu erfassen. Dieser Collector unterstützt Arrays mit OneFS 8.0.0+.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
OneFS-Dateisystem	Internes Volumen
OneFS-Dateisystem	Speicherpool
Qtree	Qtree

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen:

- Ein Benutzerkonto und ein Passwort. Dieses Konto muss NICHT admin/root sein, aber Sie MÜSSEN Ihrem Dienstkonto eine beträchtliche Anzahl von Leseberechtigungen erteilen – siehe Tabelle unten
- IP-Adresse / vollqualifizierter Domänenname 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	Authentifizierung	R
ISI_PRIV_ROLE	Privileg	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 der Plattform-API	R
ISI_PRIV_QUOTA	Quote	R
ISI_PRIV_SMARTPOOLS	SmartPools	R
ISI_PRIV_SMB	KMU	R
ISI_PRIV_STATISTICS	Statistiken	R
ISI_PRIV_SWIFT	Schnell	R
ISI_PRIV_JOB_ENGINE	Job-Engine	R

Konfiguration

Feld	Beschreibung
Isilon-IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des Isilon-Speichers
Benutzername	Benutzername für Isilon
Passwort	Für Isilon verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 8080.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 20.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Für die rollenbasierte Verwaltung nicht aktivierte Befehle erfordern Root-Benutzerzugriff“	* Überprüfen Sie, ob der Benutzer über die Berechtigung verfügt, die folgenden Befehle auf dem Gerät auszuführen: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Überprüfen Sie, ob die im Assistenten verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen
„Interner Fehler“ mit Fehlermeldungen „Ausführung des Befehls <Ihr Befehl> fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>.“ Problem mit der Berechtigung zum Ausführen des Sudo-Befehls“	Stellen Sie sicher, dass der Benutzer über Sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC PowerStore-Datenkollektor

Der EMC PowerStore-Datenkollektor sammelt Bestandsinformationen vom EMC PowerStore-Speicher. Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Der EMC PowerStore-Datenkollektor erfasst die Volume-zu-Volume-Replikationsbeziehungen, die PowerStore über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicherarray für jeden PowerStore-Cluster und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Speicherpool- oder Volumedaten erfasst.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Gastgeber	Gastgeber
Host-Volume-Zuordnung	Host-Volume-Zuordnung
Hardware (es hat Laufwerke unter dem Objekt "extra_details"): Laufwerke	Scheibe
Gerät	Speicherpool
Cluster	Speicher-Array
Node	Speicherknoten

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
fc_port	Hafen
Volumen	Volumen
Internes Volumen	Dateisystem

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse oder vollqualifizierter Domänenname des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen

Konfiguration

Feld	Beschreibung
PowerStore-Gateway(s)	IP-Adressen oder vollqualifizierte Domännennamen des PowerStore-Speichers
Benutzername	Benutzername für PowerStore
Passwort	Für PowerStore verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 443
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Die PowerStore-Leistungssammlung von Cloud Insight nutzt die Quelldaten von PowerStore mit einer Granularität von 5 Minuten. Daher fragt Data Infrastructure Insights diese Daten alle fünf Minuten ab, und dies ist nicht konfigurierbar.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Dell EMC RecoverPoint-Datensammler

Der Hauptanwendungsfall des EMC RecoverPoint-Datensammlers besteht darin, Volume-zu-Volume-Replikationsbeziehungen zu ermitteln, die das RecoverPoint-Speichergerät ermöglicht. Dieser Collector erkennt auch das Recoverpoint-Gerät selbst. Bitte beachten Sie, dass Dell/EMC eine VMware-Backup-Lösung für VMs verkauft – „RecoverPoint für VMs“ – die von diesem Collector nicht unterstützt wird.

Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Der EMC RecoverPoint-Datenkollektor erfasst die Volume-zu-Volume-Replikationsbeziehungen, die RecoverPoint über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicherarray für jeden RecoverPoint-Cluster und sammelt Inventardaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Speicherpool- oder Volumedaten erfasst.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse oder vollqualifizierter Domänenname des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen
- REST-API-Zugriff über Port 443

Konfiguration

Feld	Beschreibung
Adresse von RecoverPoint	IP-Adresse oder vollqualifizierter Domänenname des RecoverPoint-Clusters
Benutzername	Benutzername für den RecoverPoint-Cluster
Passwort	Für den RecoverPoint-Cluster verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	Für die Verbindung mit dem Recoverpoint-Cluster verwendeter TCP-Port
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.
Ausgeschlossene Cluster	Durch Kommas getrennte Liste von Cluster-IDs oder -Namen, die beim Polling ausgeschlossen werden sollen.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

DELL EMC ScaleIO / PowerFlex-Datensammler

Der ScaleIO/PowerFlex-Datensammler sammelt Bestandsinformationen vom ScaleIO- und PowerFlex-Speicher. Zur Konfiguration benötigt dieser Datensammler die ScaleIO/PowerFlex-Gateway-Adresse sowie einen Administrator-Benutzernamen und ein Administrator-Passwort.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom ScaleIO/PowerFlex-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
MDM-Cluster (Metadaten-Manager)	Storage
SDS (ScaleIO/PowerFlex-Datenserver)	Speicherknoten
Speicherpool	Speicherpool
Volumen	Volumen
Gerät	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Nur-Lese-Zugriff auf das Admin-Benutzerkonto
- Portanforderung: HTTPS-Port 443

Konfiguration

Feld	Beschreibung
ScaleIO/PowerFlex-Gateway(s)	IP-Adressen oder FQDNs von ScaleIO/PowerFlex-Gateways, getrennt durch Komma (,) oder Semikolon (;)
Benutzername	Administrator-Benutzername für die Anmeldung beim ScaleIO/PowerFlex-Gerät
Passwort	Kennwort zur Anmeldung beim ScaleIO/PowerFlex-Gerät

Erweiterte Konfiguration

Klicken Sie auf das Kontrollkästchen Inventar, um die Inventarerfassung zu aktivieren.

Feld	Beschreibung
HTTPS-Port	443
Inventarabfrageintervall (min)	Der Standardwert ist 60.
Verbindungs-Timeout (Sek.)	Der Standardwert ist 60.

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des EMC Unity-Datenkollektors

Der Datensammler DELL EMC Unity (ehemals VNXe) bietet Inventarunterstützung für VNXe Unified Storage Arrays. Data Infrastructure Insights unterstützt derzeit iSCSI- und NAS-Protokolle.

Anforderungen

- Der Unity-Datensammler ist CLI-basiert. Sie müssen die Unisphere für Unity-CLI (uemcli.exe) auf der Erfassungseinheit installieren, auf der sich Ihr VNXe-Datensammler befindet.
- uemcli.exe verwendet HTTPS als Transportprotokoll, daher muss die Erfassungseinheit in der Lage sein, HTTPS-Verbindungen zur Unity herzustellen.
- IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
- Für die Verwendung durch den Datensammler müssen Sie mindestens über einen schreibgeschützten Benutzer verfügen.
- HTTPS auf Port 443 ist erforderlich
- Der EMC Unity-Datenkollektor bietet NAS- und iSCSI-Unterstützung für die Bestandsaufnahme. Fibre-Channel-Volumes werden erkannt, Data Infrastructure Insights meldet jedoch keine FC-Zuordnung, Maskierung oder Speicherports.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Unity-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Speicher-Array	Storage
Prozessor	Speicherknoten
Speicherpool	Speicherpool
Allgemeine iSCSI-Blockinformationen, VMware VMFS	Aktie
Replikations-Remotesystem	Synchronisation
iSCSI-Knoten	iSCSI-Zielknoten
iSCSI-Initiator	iSCSI-Zielinitiator

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Konfiguration

Feld	Beschreibung
Unity-Speicher	IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts

Feld	Beschreibung
Benutzername	Benutzername für das Unity-Gerät
Passwort	Passwort für das Unity-Gerät
Vollständiger Pfad zur ausführbaren UEMCLI	Vollständiger Pfad zum Ordner, der die ausführbare Datei <i>uemcli.exe</i> enthält

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten
Unity CLI-Port	Für die Unity CLI verwendeter Port
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Ausführen des externen Dienstprogramms“ mit der Fehlermeldung „Ausführbare Unisphere-Uemcli konnte nicht gefunden werden“	<ul style="list-style-type: none"> * Überprüfen Sie, ob die IP-Adresse, der Benutzername und das Kennwort korrekt sind. * Bestätigen Sie, dass Unisphere CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass das Installationsverzeichnis von Unisphere CLI in der Datenquellenkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des VNxe in der Konfiguration der Datenquelle korrekt ist. <p>Öffnen Sie in der Data Infrastructure Insights Acquisition Unit eine CMD und wechseln Sie zum konfigurierten Installationsverzeichnis: <code>\${INSTALLDIR}</code>. Versuchen Sie, eine Verbindung mit dem VNxe-Gerät herzustellen, indem Sie Folgendes eingeben: <code>uemcli -d <Ihre IP> -u <Ihre ID> /sys/general show</code></p>

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Datensammler der Dell EMC VMAX- und PowerMax-Gerätefamilie

Data Infrastructure Insights erkennt EMC VMAX- und PowerMax-Speicher-Arrays mithilfe von Solutions Enabler-Symcli-Befehlen in Verbindung mit einem vorhandenen Solutions Enabler-Server in Ihrer Umgebung. Der vorhandene Solutions Enabler-Server verfügt über eine Verbindung zum VMAX/PowerMax-Speicherarray durch Zugriff auf Gatekeeper-Volumes.

Anforderungen

Bevor Sie diesen Datensammler konfigurieren, sollten Sie sicherstellen, dass Data Infrastructure Insights über eine TCP-Konnektivität zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. Data Infrastructure Insights erkennt alle Symmetrix-Arrays, die für diesen Server „lokal“ sind, wie in der Ausgabe „symcfg list“ von diesem Server zu sehen ist.

- Der EMC Solutions Enabler (CLI) mit der SMI-S-Provider-Anwendung muss auf dem Acquisition Unit-Server installiert sein und die Version muss mit der auf dem Solutions Enabler-Server ausgeführten Version übereinstimmen oder älter 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-Anbieter mit einer laufenden Instanz der UNISPHERE für VMAX-Anwendung kommunizieren.
- IP-Adresse des verwaltenden Solutions Enabler-Servers
- Administratorberechtigungen auf dem Solutions Enabler (SE)-Server
- Nur-Lese-Benutzername und Passwort für die SE-Software
- Die UNISPHERE für VMAX-Anwendung muss ausgeführt werden und Statistiken für die EMC VMAX- und PowerMax-Speicherarrays sammeln, die von der SMI-S Provider-Installation verwaltet werden.
- Zugriffsvalidierung für die Leistung: Gehen Sie in einem Webbrowser auf Ihrer Erfassungseinheit zu <https://<SMI-S-Hostname oder IP>:5989/ecomconfig>, wobei „SMI-S-Hostname oder IP“ die IP-Adresse oder der Hostname Ihres SMI-S-Servers ist. Diese URL führt zu einem Verwaltungsportal für den EMC SMI-S-Dienst (auch bekannt als „ECOM“). Sie erhalten ein Anmelde-Popup.
- Berechtigungen müssen in der Daemon-Konfigurationsdatei des Solutions Enabler-Servers deklariert werden, die sich normalerweise hier befindet: `/var/symapi/config/daemon_users`

Hier ist eine Beispieldatei mit den richtigen Cisy-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 stordaeon
control
###      operations (e.g., shutdown).
#####
#####
# smith      storrdfd
cisy storapid <all>
```

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen aus der EMC VMAX/PowerMax-Datenquelle. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses

Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Datenträgergruppe	Datenträgergruppe
Storage	Array-Speicher
Direktor	Speicherknoten
Gerätepool, Speicherressourcenpool (SRP)	Speicherpool
Gerät TDev	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Konfiguration

Hinweis: Wenn die SMI-S-Benutzerauthentifizierung nicht aktiviert ist, werden die Standardwerte im Data Infrastructure Insights -Datenkollektor ignoriert.

Feld	Beschreibung
Dienstname	Dienstname wie in der Datei <i>netcnfg</i> angegeben
Vollständiger Pfad zur CLI	Vollständiger Pfad zum Ordner, der die Symmetrix CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Inventarfilter-Geräteliste	Durch Kommas getrennte Liste der ein- oder auszuschließenden Geräte-IDs

Feld	Beschreibung
Verbindungs-Caching	Wählen Sie die Verbindungs-Caching-Methode: * LOKAL bedeutet, dass der Cloud Insights Acquisition-Dienst auf dem Solutions Enabler-Server ausgeführt wird, der über Fibre Channel-Konnektivität zu den Symmetrix-Arrays verfügt, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. Dies kann bei einigen Remote Acquisition Unit (RAU)-Konfigurationen auftreten. * REMOTE_CACHED ist die Standardeinstellung und sollte in den meisten Fällen verwendet werden. Dabei werden die NETCNFG-Dateieinstellungen verwendet, um über IP eine Verbindung zum Solutions Enabler-Server herzustellen, der über Fibre Channel-Konnektivität zu den Symmetrix-Arrays verfügen muss, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. * Falls die Option REMOTE_CACHED dazu führt, dass CLI-Befehle fehlschlagen, verwenden Sie die Option REMOTE. Bedenken Sie, dass sich der Erfassungsprozess dadurch verlangsamt (in Extremfällen möglicherweise um Stunden oder sogar Tage). Die NETCNFG-Dateieinstellungen werden weiterhin für eine IP-Verbindung zum Solutions Enabler-Server verwendet, der über Fibre Channel-Konnektivität zu den erkannten Symmetrix-Arrays verfügt. Hinweis: Diese Einstellung ändert nicht das Verhalten von Data Infrastructure Insights in Bezug auf die Arrays, die in der Ausgabe „symcfg list“ als REMOTE aufgeführt sind. Data Infrastructure Insights sammelt Daten nur auf Geräten, die durch diesen Befehl als LOKAL angezeigt werden.
SMI-S-Protokoll	Für die Verbindung mit dem SMI-S-Anbieter verwendetes Protokoll. Zeigt auch den verwendeten Standardport an.
SMIS-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
SMI-S-Benutzername	Benutzername für den SMI-S Provider-Host
SMI-S-Passwort	Benutzername für den SMI-S Provider-Host
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen (Standard 1000 Sekunden)
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Erfassen von Leistungsdaten ein- oder ausgeschlossen werden soll.
Leistungsfilter-Geräteliste	Durch Kommas getrennte Liste der ein- oder auszuschließenden Geräte-IDs

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
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 für die Verwaltung durch den Solutions Enabler-Server konfiguriert sind: – Führen Sie <code>symcfg list -v</code> aus, um die Liste der konfigurierten Symmetrix-Geräte anzuzeigen.
Fehler: Ein angeforderter Netzwerkdienst wurde in der Dienstdatei nicht gefunden	Stellen Sie sicher, dass der Solutions Enabler-Dienstname in der <code>Netcnfg</code> -Datei für Solutions Enabler definiert ist. Diese Datei befindet sich normalerweise unter <code>SYMAPI\config\</code> in der Solutions Enabler-Clientinstallation.
Fehler: Der Remote-Client/Server-Handshake ist fehlgeschlagen	Überprüfen Sie die aktuellsten <code>storsrvd.log*</code> -Dateien auf dem Solutions Enabler-Host, den wir ermitteln möchten.
Fehler: Allgemeiner Name im Client-Zertifikat ungültig	Bearbeiten Sie die Datei <code>hosts</code> auf dem Solutions Enabler-Server, sodass der Hostname der Erfassungseinheit in die IP-Adresse aufgelöst wird, die im <code>storsrvd.log</code> auf dem Solutions Enabler-Server gemeldet wird.
Fehler: Die Funktion konnte keinen Speicher abrufen	Stellen Sie sicher, dass im System genügend freier Speicher zur Ausführung von Solutions Enabler verfügbar ist
Fehler: Solutions Enabler konnte nicht alle erforderlichen Daten bereitstellen.	Untersuchen Sie den Gesundheitszustand und das Lastprofil von Solutions Enabler
Fehler: • Der CLI-Befehl „ <code>symcfg list -tdev</code> “ gibt möglicherweise falsche Daten zurück, wenn er mit Solutions Enabler 7.x von einem Solutions Enabler-Server 8.x erfasst wird. • Der CLI-Befehl „ <code>symcfg list -srp</code> “ gibt möglicherweise falsche Daten zurück, wenn er mit Solutions Enabler 8.1.0 oder früher von einem Solutions Enabler-Server 8.3 oder höher erfasst wurde.	Stellen Sie sicher, dass Sie dieselbe Hauptversion von Solutions Enabler verwenden

Problem:	Versuchen Sie Folgendes:
Ich sehe Datenerfassungsfehler mit der Meldung: „unbekannter Code“	Diese Meldung wird möglicherweise angezeigt, wenn in der Daemon-Konfigurationsdatei des Solutions Enabler-Servers keine Berechtigungen deklariert sind (siehe Anforderungen über.) Dies setzt voraus, dass Ihre SE-Clientversion mit Ihrer SE-Serverversion übereinstimmt. Dieser Fehler kann auch auftreten, wenn der Benutzer <i>cisys</i> (der Solutions Enabler-Befehle ausführt) in der Konfigurationsdatei <code>/var/symapi/config/daemon_users</code> nicht mit den erforderlichen Daemon-Berechtigungen konfiguriert wurde. Um dies zu beheben, bearbeiten Sie die Datei <code>/var/symapi/config/daemon_users</code> und stellen Sie sicher, dass der Cisys-Benutzer über die Berechtigung <code><all></code> für den Storapid-Daemon verfügt. Beispiel: 14:11:25 # tail <code>/var/symapi/config/daemon_users ... cisys storapid <all></code>

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC VNX Block Storage (NaviCLI)-Datenkollektor

Data Infrastructure Insights verwendet den Datensammler Dell EMC VNX Block Storage (NaviSec) (ehemals CLARiiON), um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom EMC VNX Block Storage-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Storage	Storage
Speicherprozessor	Speicherknoten
Dieser Pool, RAID-Gruppe	Speicherpool
LUN	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

Für die Datenerhebung müssen folgende Voraussetzungen erfüllt sein:

- Eine IP-Adresse jedes VNX-Blockspeicherprozessors
- Schreibgeschützter Navisphere-Benutzername und -Passwort für die VNX-Blockspeicher-Arrays

- NaviSecCli muss auf der Data Infrastructure Insights AU installiert sein
- Zugriffsvalidierung: Führen Sie NaviSecCLI von der Data Infrastructure Insights AU mit dem Benutzernamen und dem Kennwort für jedes Array aus.
- Portanforderungen: 80, 443
- Die NaviSecCLI-Version sollte dem neuesten FLARE-Code auf Ihrem Array entsprechen
- Aus Leistungsgründen muss die Statistikprotokollierung aktiviert sein.

Syntax der NaviSphere-Befehlszeilenschnittstelle

naviseccli.exe -h <IP-Adresse> -user <Benutzer> -password <Passwort> -scope <Bereich, verwenden Sie 0 für den globalen Bereich> -port <verwenden Sie standardmäßig 443> Befehl

Konfiguration

Feld	Beschreibung
VNX-Blockspeicher-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Blockspeichers
Benutzername	Name, der für die Anmeldung beim VNX-Blockspeichergerät verwendet wird.
Passwort	Kennwort zum Anmelden beim VNX-Blockspeichergerät.
CLI-Pfad zu naviseccli.exe	Vollständiger Pfad zum Ordner, der die ausführbare Datei <i>naviseccli.exe</i> enthält

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40 Minuten.
Umfang	Der sichere Clientbereich. Die Standardeinstellung ist „Global“.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
<p>Fehler:</p> <ul style="list-style-type: none"> • Agent wird nicht ausgeführt • Naviseccli konnte nicht gefunden werden • Kein Befehl konnte ausgeführt werden 	<ul style="list-style-type: none"> • Bestätigen Sie, dass NaviSphere CLI auf der Cloud Insight Acquisition Unit installiert ist • Sie haben im Konfigurationsassistenten des Datensammlers nicht die Option „Sicheren Client verwenden“ ausgewählt und keine nicht sichere Version von Navisphere CLI installiert. • Bestätigen Sie, dass das NaviSphere CLI-Installationsverzeichnis in der Datensammlerkonfiguration korrekt ist • Bestätigen Sie, dass die IP des VNX-Blockspeichers in der Datensammlerkonfiguration korrekt ist: • Von der Data Infrastructure Insights Acquisition Unit: <ul style="list-style-type: none"> ◦ 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 {ip} durch die tatsächliche IP).
<p>Fehler: 4.29 emc235848 emc241018 getall Fehler beim Parsen der Host-Alias-Informationen</p>	<p>Dies wird wahrscheinlich durch ein FLARE 29-Beschädigungsproblem der Host-Initiator-Datenbank auf dem Array selbst verursacht. Siehe EMC-Wissensdatenbankartikel: emc235848, emc241018. Sie können auch überprüfen https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128</p>
<p>Fehler: Meta-LUNs konnten nicht abgerufen werden. Fehler beim Ausführen von java -jar navicli.jar</p>	<ul style="list-style-type: none"> • Ändern Sie die Datensammlerkonfiguration, um den sicheren Client zu verwenden (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. • Die navicli.jar ist möglicherweise verfügbar auf http://powerlink.emc.com
<p>Fehler: Speicherpools melden keine Datenträger auf dem Serviceprozessor unter der konfigurierten IP-Adresse</p>	<p>Konfigurieren Sie den Datensammler mit beiden Serviceprozessor-IPs, getrennt durch ein Komma</p>

Problem:	Versuchen Sie Folgendes:
Fehler: Revisionskonflikt	<ul style="list-style-type: none"> • Dies wird normalerweise dadurch verursacht, dass die Firmware auf dem VNX-Blockspeichergerät aktualisiert wird, nicht jedoch die Installation von NaviCLI.exe. Dies kann auch daran liegen, dass auf verschiedenen Geräten unterschiedliche Firmwares vorhanden sind, aber nur eine CLI (mit einer anderen Firmware-Version) installiert ist. • Stellen Sie sicher, dass auf dem Gerät und dem Host identische Versionen der Software ausgeführt werden: <ul style="list-style-type: none"> ◦ 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. ◦ Suchen Sie in den ersten Zeilen nach der Versionsnummer. 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. Derzeit werden nur FC-Konfigurationen unterstützt. Überprüfen Sie, ob diese Version/Firmware unterstützt wird.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

DELL EMC VNX File (früher Celerra Unified Storage System) Datenkollektor

Dieser Datensammler ruft Inventarinformationen vom VNX File Storage System ab. Zur Konfiguration benötigt dieser Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Passwort.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom VNX File-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Celerra-Netzwerkserver/Celerra-Speicherpool	Speicherpool
Dateisystem	Internes Volumen
Datenverschieber	Regler
Auf einem Data Mover gemountetes Dateisystem	Dateifreigabe
CIFS- und NFS-Exporte	Aktie
Datenträgervolumen	Backend-LUN

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie Folgendes:

- Die IP-Adresse des Speicherprozessors
- Benutzername und Kennwort nur zum Lesen
- SSH-Port 22

Konfiguration

Feld	Beschreibung
VNX-Datei-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Dateigeräts
Benutzername	Name, der für die Anmeldung beim VNX-Dateigerät verwendet wird
Passwort	Kennwort zum Anmelden beim VNX-Dateigerät

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (Minuten)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Fortfahren nicht möglich, während DART-Update läuft	Mögliche Lösung: Halten Sie den Datensammler an und warten Sie, bis das DART-Upgrade abgeschlossen ist, bevor Sie eine weitere Erfassungsanforderung versuchen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des Dell EMC VNX Unified-Datenkollektors

Zur 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 erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Datenträgerordner	Datenträgergruppe
Dateisystem	Internes Volumen
Storage	Storage
Speicherprozessor	Speicherknoten
Speicherpool, RAID-Gruppe	Speicherpool
LUN	Volumen
Datenverschieber	Regler
Auf einem Data Mover gemountetes Dateisystem	Dateifreigabe
CIFS- und NFS-Exporte	Aktie
Datenträgervolumen	Backend-LUN

Anforderungen

Zum Konfigurieren des VNX (SSH)-Datenkollektors benötigen Sie Folgendes:

- VNX-IP-Adresse und Anmeldeinformationen für die Celerra Control Station.
- Benutzername und Passwort sind schreibgeschützt.
- Der Datensammler kann NaviCLI/NaviSecCLI-Befehle auf dem Backend-Array ausführen, indem er die DART OS NAS-Köpfe nutzt.

Konfiguration

Feld	Beschreibung
VNX-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname der VNX Control Station
Benutzername	Benutzername für die VNX Control Station
Passwort	Passwort für die VNX Control Station

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Leistungsabfrageintervall (Sek.).	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des EMC VPLEX-Datenkollektors

Dieser Datensammler erfasst Bestands- und Leistungsdaten von EMC VPLEX-Speichersystemen. Zur Konfiguration benötigt der Datensammler eine IP-Adresse des VPLEX-Servers und ein Domänenkonto auf Administratorebene.



Für die Leistungserfassung von Data Infrastructure Insights aus Vplex-Clustern muss der Leistungsarchivdienst betriebsbereit sein, um die CSV-Dateien und Protokolle zu füllen, die Data Infrastructure Insights über SCP-basierte Dateikopien abrufen. NetApp hat festgestellt, dass diese Funktionalität bei vielen Vplex-Firmware-Upgrades/Management-Station-Updates nicht mehr funktioniert. Kunden, die solche Upgrades planen, möchten Dell/EMC möglicherweise proaktiv fragen, ob diese Funktionalität durch das geplante Upgrade nicht mehr funktionsfähig ist, und wenn ja, wie sie sie wieder aktivieren können, um Lücken in der Leistungstransparenz zu minimieren. Der Vplex-Leistungscod von Cloud Insight prüft bei jeder Abfrage, ob alle erwarteten Dateien vorhanden sind und ob sie ordnungsgemäß aktualisiert werden. Wenn sie fehlen oder veraltet sind, protokolliert Data Infrastructure Insights Leistungserfassungsfehler.

Terminologie

Data Infrastructure Insightst erhält die folgenden Bestandsinformationen vom VPLEX-Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage
Motor	Speicherknoten
Gerät, Systemumfang	Backend-Speicherpool
Virtuelles Volume	Volumen
Front-End-Port, Back-End-Port	Hafen
Verteiltes Gerät	Speichersynchronisierung
Speicheransicht	Volumenkarte, Volumenmaske
Speichervolumen	Backend-LUN

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
ITLs	Backend-Pfad

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Eine IP-Adresse der VPLEX-Verwaltungskonsole
- Domänenkonto auf Administratorebene für den VPLEX-Server
- Port 443 (HTTPS). Erfordert ausgehende Konnektivität zum TCP-Port 443 auf der VPLEX-Verwaltungsstation.
- Aus Leistungsgründen sind Benutzername und Kennwort für den SSH-/SCP-Zugriff schreibgeschützt.
- Aus Leistungsgründen ist Port 22 erforderlich.

Konfiguration

Feld	Beschreibung
IP-Adresse der VPLEX-Verwaltungskonsole	IP-Adresse oder vollqualifizierter Domänenname der VPLEX-Verwaltungskonsole
Benutzername	Benutzername für VPLEX CLI
Passwort	Für VPLEX CLI verwendetes Kennwort
Leistung Remote-IP-Adresse	Leistung Remote-IP-Adresse der VPLEX-Verwaltungskonsole
Performance Remote-Benutzername	Leistung Remote-Benutzername der VPLEX-Verwaltungskonsole
Performance Remote-Passwort	Leistungs-Remotekennwort der VPLEX-Verwaltungskonsole

Erweiterte Konfiguration

Feld	Beschreibung
Kommunikationsanschluss	Für VPLEX CLI verwendeter Port. Der Standardwert ist 443.
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.
Anzahl der Verbindungsversuche	Der Standardwert ist 3.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 600 Sekunden.
Anzahl der Wiederholungsversuche	Der Standardwert ist 2.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Benutzerauthentifizierung fehlgeschlagen.	Stellen Sie sicher, dass Ihre Anmeldeinformationen für dieses Gerät korrekt sind.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: Die VPLEX-Leistung für Versionen unter 5.3 wird nicht unterstützt.	Aktualisieren Sie VPLEX auf 5.3 oder höher
Fehler: Nicht genügend Daten gesammelt.	• Prüfen Sie den Erfassungszeitstempel in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend. • Warten Sie länger
Fehler: Perpetual-Log-Dateien werden nicht aktualisiert.	Bitte kontaktieren Sie den EMC-Support, um die Aktualisierung der permanenten Protokolldateien zu aktivieren
Fehler: Das Leistungsabfrageintervall ist zu groß.	Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei <code>logfile</code> und ändern Sie das Abfrageintervall entsprechend
Fehler: Die Remote-IP-Adresse der VPLEX-Verwaltungskonsole ist nicht konfiguriert.	Bearbeiten Sie die Datenquelle, um die Performance-Remote-IP-Adresse der VPLEX-Verwaltungskonsole festzulegen.
Fehler: Keine Leistungsdaten vom Direktor gemeldet	• Überprüfen Sie, ob die Systemleistungsmonitore ordnungsgemäß ausgeführt werden. • Wenden Sie sich an den EMC-Support, um die Aktualisierung der Protokolldateien des Systemleistungsmonitors zu ermöglichen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Dell EMC XtremIO-Datenkollektor

Der EMC XtremIO-Datenkollektor erfasst Bestands- und Leistungsdaten vom EMC XtremIO-Speichersystem.

Anforderungen

Zum Konfigurieren des EMC XtremIO (HTTP)-Datenkollektors benötigen Sie:

- Die Hostadresse des XtremIO Management Servers (XMS)
- Ein Konto mit Administratorrechten
- Zugriff auf Port 443 (HTTPS)

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom EMC XtremIO-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie

für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieser Datenquelle die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplatte (SSD)	Scheibe
Cluster	Storage
Regler	Speicherknoten
Volumen	Volumen
LUN-Karte	Volumenkarte
Ziel-FC-Initiator	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

- Die Host-IP-Adresse des XtremIO Management Server (XMS)
- Administratorbenutzername und -kennwort für XtremIO

Konfiguration

Feld	Beschreibung
XMS-Host	IP-Adresse oder vollqualifizierter Domänenname des XtremIO-Managementsservers
Benutzername	Benutzername für den XtremIO-Managementserver
Passwort	Kennwort für den XtremIO-Managementserver

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem XTremIO-Verwaltungsserver verwendet wird. Der Standardwert ist 443.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Fujitsu Eternus Datensammler

Der Fujitsu Eternus-Datenkollektor erfasst Inventardaten mithilfe des Administratorzugriffs auf das Speichersystem.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen vom Fujitsu Eternus-Speicher. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid-Gruppe	Speicherpool
Standard-Volume, Snap-Daten-Volume (SDV), Snap-Daten-Pool-Volume (SDPV), Thin-Provisioning-Volume (TPV), Flexible-Tier-Volume (FTV), Wide-Striping-Volume (WSV)	Volumen
Kanaladapter	Regler

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Eine IP-Adresse des Eternus-Speichers, die nicht durch Kommas getrennt sein darf
- Benutzername und Kennwort auf SSH-Administrationsebene
- Port 22
- Stellen Sie sicher, dass das Scrollen der Seite deaktiviert ist (clienv-show-more-scroll disable)

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
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Abrufen der Daten“ mit den Fehlermeldungen „Fehler beim Suchen der Eingabeaufforderung CLI“ oder „Fehler beim Suchen der Eingabeaufforderung am Ende der Shell-Ergebnisse“	Wahrscheinliche Ursache: Im Speichersystem ist das Scrollen von Seiten aktiviert. Mögliche Lösung: * Versuchen Sie, das Scrollen der Seite zu deaktivieren, indem Sie den folgenden Befehl ausführen: <code>set clienv-show-more -scroll disable</code>
„Verbindungsfehler“ mit den Fehlermeldungen „Fehler beim Herstellen einer SSH-Verbindung zum Speicher“ oder „Fehler beim Herstellen einer Verbindung zu VirtualCenter“	Mögliche Ursachen: * Falsche Anmeldeinformationen. * Falsche IP-Adresse. * Netzwerkproblem. * Der Speicher ist möglicherweise ausgefallen oder reagiert nicht. Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den SSH-Client mit dem Speicher zu kommunizieren.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp Google Compute-Datenkollektor

Dieser Datensammler unterstützt die Bestands- und Leistungserfassung von Google Compute-Cloud-Plattformkonfigurationen. Dieser Collector versucht, alle Rechenressourcen in allen Projekten einer Google-Organisation zu ermitteln. Wenn Sie mehrere Google-Organisationen haben, die Sie mit Data Infrastructure Insights ermitteln möchten, sollten Sie pro Organisation einen Data Infrastructure Insights -Collector bereitstellen.

Anforderungen für Dienstkonten

- Sie müssen ein Dienstkonto erstellen, indem Sie den Anweisungen in ["Erstellen/Verwalten von Dienstkonten"](#) . Ein solches Dienstkonto wird durch eine eindeutige ID identifiziert, die als *clientId* bezeichnet wird und als Benutzername verwendet wird.
- Erstellen Sie außerdem einen Dienstkontoschlüssel, indem Sie den Anweisungen in ["Erstellen/Verwalten von Dienstkontoschlüsseln"](#) . Dieser Schlüssel kann als JSON-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.
- Das Dienstkonto muss auf *compute.readonly*, *monitoring.read* und *cloud-platform* beschränkt sein.

Konfiguration

Feld	Beschreibung
Organisations-ID	Die Organisations-ID, die Sie mit diesem Collector ermitteln möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann

Feld	Beschreibung
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCP-Projekte nach IDs zu filtern	Wenn Sie einschränken möchten, welche Projektressourcen in Data Infrastructure Insights eingebracht werden.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie je nach Wert des Werts „Wählen Sie ‚Ausschließen‘ ...“ in die Erkennung ein- oder ausfiltern möchten. Die Standardliste ist leer
Client-ID	Client-ID für die Google Cloud Platform-Konfiguration
Kopieren Sie den Inhalt Ihrer Google-Anmeldeinformationsdatei und fügen Sie ihn hier ein.	Kopieren Sie Ihre Google-Anmeldeinformationen für das Cloud Platform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Wählen Sie „Ausschließen“ oder „Einschließen“, um VMs nach Labels zu filtern.	Geben Sie an, ob VMs beim Sammeln von Daten anhand von Labels ein- oder ausgeschlossen werden sollen. Wenn „Einschließen“ ausgewählt ist, darf das Feld „Beschriftungsschlüssel“ nicht leer sein.
Label-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf + Bezeichnung filtern , um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüssel und Werten filtern, die mit den Schlüssel und Werten der Bezeichnungen auf der VM übereinstimmen. Der Beschriftungsschlüssel ist erforderlich, der Beschriftungswert ist optional. Wenn der Labelwert leer ist, wird die VM gefiltert, solange sie mit dem Labelschlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 1800 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Google Cloud NetApp Volumes Datensammler

Dieser Datensammler unterstützt die Bestands- und Leistungserfassung von Google Cloud NetApp Volumes -Konfigurationen. Der Collector erkennt NetApp -Volumes und Speicherressourcen in allen Projekten innerhalb einer Google-Organisation. Wenn Sie mehrere Google-Organisationen haben, die Sie mit Data Infrastructure Insights überwachen möchten, stellen Sie einen Collector pro Organisation bereit.

Anforderungen für Dienstkonten

- Sie müssen ein Dienstkonto erstellen, indem Sie den Anweisungen in ["Erstellen/Verwalten von"](#)

Dienstkonto" . Dieses Dienstkonto wird durch eine eindeutige ID identifiziert, die als *clientId* bezeichnet wird und als Benutzername verwendet wird.

- Erstellen Sie außerdem einen Dienstkontoschlüssel, indem Sie den Anweisungen in "[Erstellen/Verwalten von Dienstkontoschlüsseln](#)" . Dieser Schlüssel kann als JSON-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.
- Das Dienstkonto muss auf *compute.readonly*, *monitoring.read* und *cloud-platform* beschränkt sein.

Konfiguration

Feld	Beschreibung
Organisations-ID	Die Organisations-ID, die Sie mit diesem Collector ermitteln möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCNV-Assets nach Standort zu filtern	Die Standardeinstellung ist „Ausschließen“, da dieser Collector standardmäßig alle GCNV-Volumes weltweit innerhalb Ihrer Organisation ermitteln soll.
GCNV-Standorte ausschließen/einschließen	Dies ist standardmäßig leer und wird in Verbindung mit der Option „Wählen Sie ‚Ausschließen‘ oder ‚Einschließen‘“ verwendet. Wenn Sie Assets nur in bestimmten Regionen entdecken möchten, verwenden Sie diese beiden Optionen, um den Umfang dieses Collectors einzuschränken.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie je nach Wert des Werts „Wählen Sie ‚Ausschließen‘ ...“ in die Erkennung ein- oder ausfiltern möchten. Die Standardliste ist leer
Client-ID	Client-ID für die Google Cloud Platform-Konfiguration
Kopieren Sie den Inhalt Ihrer Google-Anmeldeinformationsdatei und fügen Sie ihn hier ein.	Kopieren Sie Ihre Google-Anmeldeinformationen für das Cloud Platform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Verwenden Sie den AU-Proxy für REST-API-Aufrufe	Wählen Sie diese Option, damit der Collector denselben Proxy verwendet wie die Erfassungseinheit, auf der sich der Collector befindet. Standardmäßig ist dies deaktiviert, was bedeutet, dass der Collector versucht, HTTPS-API-Aufrufe direkt an Google zu senden.

Feld	Beschreibung
Label-Schlüssel und -Werte zum Filtern von VMs	Klicken Sie auf + Bezeichnung filtern , um auszuwählen, welche VMs (und zugehörigen Datenträger) ein-/ausgeschlossen werden sollen, indem Sie nach Schlüssel und Werten filtern, die mit den Schlüssel und Werten der Bezeichnungen auf der VM übereinstimmen. Der Beschriftungsschlüssel ist erforderlich, der Beschriftungswert ist optional. Wenn der Labelwert leer ist, wird die VM gefiltert, solange sie mit dem Labelschlüssel übereinstimmt.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

HP Unternehmen

HP Enterprise Alletra 9000 / Primera Storage Datensammler

Data Infrastructure Insights verwendet den Datensammler HP Enterprise Alletra 9000 / HP Enterprise Primera (früher 3PAR), um Inventar und Leistung zu ermitteln.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Feld	Beschreibung
Physische Festplatte	Scheibe
Speichersystem	Storage
Controller-Knoten	Speicherknoten
Gemeinsame Bereitstellungsguppe	Speicherpool
Virtuelles Volume	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- IP-Adresse oder FQDN des InServ-Clusters
- Für die Bestandsaufnahme sind Benutzername und Kennwort für den StoreServ-Server schreibgeschützt.

- Aus Leistungsgründen Lese-/Schreibzugriff auf den Benutzernamen und das Kennwort für den StoreServ-Server
- Portanforderungen: 22 (Inventarerfassung), 5988 oder 5989 (Leistungserfassung) [Hinweis: Leistung wird für StoreServ OS 3.x+ unterstützt]
- Bestätigen Sie zur Leistungserfassung, dass SMI-S aktiviert ist, indem Sie sich per SSH beim Array anmelden.

Konfiguration

Feld	Beschreibung
Speicher-IP-Adresse	Speicher-IP-Adresse oder vollqualifizierter Domänenname des StoreServ-Clusters
Benutzername	Benutzername für den StoreServ-Server
Passwort	Für den StoreServ-Server verwendetes Kennwort
SMI-S-Benutzername	Benutzername für den SMI-S Provider-Host
SMI-S-Passwort	Für den SMI-S-Provider-Host verwendetes Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
SMI-S-Konnektivität	Für die Verbindung mit dem SMI-S-Provider verwendetes Protokoll
SMI-S-Standardport überschreiben	Wenn leer, verwenden Sie den Standardport von SMI-S Connectivity, andernfalls geben Sie den zu verwendenden Verbindungsport ein
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Der Befehl „showsys“ gibt kein Ergebnis zurück.	Führen Sie „showsys“ und „showversion -a“ von der Befehlszeile aus und prüfen Sie, ob die Version vom Array unterstützt wird.

Performance

Problem:	Versuchen Sie Folgendes:
Verbindung oder Anmeldung fehlgeschlagen. Die Initialisierung des Anbieters ist fehlgeschlagen.	Ein rein numerischer Array-Name kann Probleme mit dem SMI-S-Server verursachen. Versuchen Sie, den Array-Namen zu ändern.
Der konfigurierte SMI-S-Benutzer hat keine Domäne	Gewähren Sie dem konfigurierten SMI-S-Benutzer entsprechende Domänenberechtigungen
Data Infrastructure Insights gibt an, dass keine Verbindung zum SMI-S-Dienst hergestellt bzw. keine Anmeldung möglich ist.	Stellen Sie sicher, dass sich zwischen der CI AU und dem Array keine Firewall befindet, die die CI AU daran hindern würde, TCP-Verbindungen zu 5988 oder 5989 herzustellen. Wenn dies erledigt ist und Sie bestätigt haben, dass keine Firewall vorhanden ist, sollten Sie per SSH auf das Array zugreifen und zur Bestätigung den Befehl „showcim“ verwenden. Überprüfen Sie, ob: * der Dienst aktiviert ist * HTTPS aktiviert ist * der HTTPS-Port 5989 sein sollte. Wenn dies alles der Fall ist, können Sie versuchen, „stopcim“ und dann „startcim“ auszuführen, um das CIM (d. h. den SMI-S-Dienst) neu zu starten.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

HP Enterprise Command View-Datensammler

Der HP Enterprise Command View Advanced Edition-Datensammler unterstützt die Erkennung von XP- und P9500-Arrays über den Command View Advanced Edition (CVAE)-Server. Data Infrastructure Insights kommuniziert mit CVAE über die standardmäßige Command View-API, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom HP Enterprise Command View-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
PDEV	Scheibe
Zeitschriftenpool	Datenträgergruppe
Speicher-Array	Storage
Port-Controller	Speicherknoten
Array-Gruppe, DP-Pool	Speicherpool
Logische Einheit, LDEV	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse des CVAE-Servers
- Nur-Lese-Benutzername und Passwort für die CVAE-Software und Peer-Berechtigungen
- Portanforderung: 2001

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

- HDS USP-, USP V- und VSP-Leistung
 - Performance Monitor muss lizenziert sein.
 - Der Überwachungsschalter muss aktiviert sein.
 - Das Exporttool (Export.exe) muss in die Data Infrastructure Insights AU kopiert und an einen Speicherort extrahiert werden. Stellen Sie auf CI Linux AUs sicher, dass „cisis“ über Lese- und Ausführungsberechtigungen verfügt.
 - Die Version des Exporttools muss mit der Mikrocodeversion des Zielarrays übereinstimmen.
- AMS-Leistung:
 - Performance Monitor muss lizenziert sein.
 - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Data Infrastructure Insights AU installiert werden.
- Netzwerkanforderungen
 - Die Exporttools basieren auf Java und verwenden RMI, um mit dem Array zu kommunizieren. Diese Tools sind möglicherweise nicht Firewall-freundlich, da sie bei jedem Aufruf die Quell- und Ziel-TCP-Ports dynamisch aushandeln. Außerdem können sich die Export-Tools verschiedener Modell-Arrays im Netzwerk unterschiedlich verhalten. Wenden Sie sich an HPE, um die Anforderungen Ihres Modells zu erfahren.

Konfiguration

Feld	Beschreibung
Command View Server	IP-Adresse oder vollqualifizierter Domänenname des Command View-Servers
Benutzername	Benutzername für den Command View-Server.
Passwort	Für den Command View-Server verwendetes Kennwort.
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 den JAR-Dateien des Export-Dienstprogramms

Feld	Beschreibung
SNM2Devices – WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Storage Navigator CLI-Pfad: SNM2 CLI-Pfad * Gültige Kontoauthentifizierung: Wählen Sie diese Option, um eine gültige Kontoauthentifizierung auszuwählen * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für die Leistung	Andere Leistungsoptionen außer Kraft setzen
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domänenname des Tuning-Managers
Tuning Manager-Port	Für Tuning Manager verwendeter Port
Tuning Manager-Benutzername	Benutzername für Tuning Manager
Tuning Manager-Passwort	Passwort für Tuning Manager

Hinweis: In HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

Erweiterte Konfiguration

Feld	Beschreibung
Command View-Server-Port	Für den Command View Server verwendeter Port
HTTPs aktiviert	Auswählen, um HTTPs zu aktivieren
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräte ausschließen oder einschließen	Durch Kommas getrennte Liste von Geräte-IDs oder Array-Namen, die ein- oder ausgeschlossen werden sollen
Abfrage-Host-Manager	Auswählen, um den Host-Manager abzufragen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Der Benutzer verfügt nicht über ausreichende Berechtigungen	Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des im Datensammler konfigurierten Benutzerkontos

Problem:	Versuchen Sie Folgendes:
Fehler: Die Speicherliste ist leer. Entweder sind die 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 mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des Benutzerkontos
Fehler: Das HDS-Speicherarray wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HP CommandView AE nicht aktualisiert wird.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des Export-Dienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Export Utility auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort des Export Utility in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass Benutzername und Kennwort in der Konfiguration des Datensammlers korrekt sind. * Bestätigen Sie, dass die Version des Export Utility mit der Mikrocodeversion des Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie die Batchdatei runWin.bat ausführen.
Fehler: Anmeldung beim Exporttool für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt sind. * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler. * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind.
Fehler: Die Exporttools haben „Zeitbereich für Überwachung konnte nicht abgerufen werden“ protokolliert.	* Bestätigen Sie, dass die Leistungsüberwachung auf dem Array aktiviert ist. * Versuchen Sie, die Exporttools außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Export-Dienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird von Storage Navigator Modular CLI nicht unterstützt	* Konfigurieren Sie nur unterstützte Speicher-Arrays. * Verwenden Sie „Geräteliste filtern“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet * Konfigurationsfehler: Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Export-Dienstprogramms. * Prüfen Sie, ob das betreffende Speicherarray im Command View-Server konfiguriert ist. * Legen Sie das Leistungsabfrageintervall auf ein Vielfaches von 60 Sekunden fest.

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen des Auperform-Befehls * 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 der Speicherort von Storage Navigator Modular CLI in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass die Version von Storage Navigator Modular CLI mit der Mikrocodeversion des im Datensammler konfigurierten Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet	Überprüfen Sie, ob das betreffende Speicherarray im Command View-Server konfiguriert ist
Fehler: * Kein Array ist bei der Storage Navigator Modular 2 CLI registriert * Array ist nicht bei der Storage Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei der StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. * Führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus. * Bestätigen Sie, dass die Befehlsausgabe Details zum Array mit IP enthält. * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit der Storage Navigator-CLI: – Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. – Führen Sie den Befehl „set=STONAVM_HOME=“ aus. – Führen Sie den Befehl „auunitaddauto -ip \${ip}“ aus. Ersetzen Sie \${ip} durch die echte IP

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

HP E Alletra 6000 Datenkolektor

Der HP Enterprise Alletra 6000 (früher Nimble) Datensammler unterstützt Inventar- und Leistungsdaten für Alletra 6000-Speicherarrays.

Terminologie

Data Infrastructure Insights erhält von diesem Collector die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Anordnung	Storage

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumen	Volumen
Pool	Speicherpool
Initiator	Speicherhost-Alias
Regler	Speicherknoten
Fibre-Channel-Schnittstelle	Regler

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Um Inventar- und Konfigurationsdaten vom Speicherarray zu erfassen, müssen Sie über Folgendes verfügen:

- Das Array muss installiert und konfiguriert sein und vom Client über seinen vollqualifizierten Domänennamen (FQDN) oder die Array-Verwaltungs-IP-Adresse erreichbar sein.
- Auf dem Array muss NimbleOS 2.3.x oder höher ausgeführt werden.
- Sie müssen über einen gültigen Benutzernamen und ein gültiges Kennwort für das Array verfügen und mindestens über die Rolle „Operator“ verfügen. Die Rolle „Guest“ verfügt nicht über ausreichend Zugriff, um die Initiatorkonfigurationen zu verstehen.
- Port 5392 muss auf dem Array geöffnet sein.

Um Leistungsdaten vom Speicherarray zu erfassen, müssen Sie über Folgendes verfügen:

- 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 hat, ist für Volumes, und alle statistischen Data Infrastructure Insights -Berichte werden aus den Statistiken zu Volumes abgeleitet

Konfiguration

Feld	Beschreibung
Array-Management-IP-Adresse	Vollqualifizierter Domänenname (FQDN) oder IP-Adresse für die Array-Verwaltung.
Benutzername	Benutzername für das Array
Passwort	Passwort für das Array

Erweiterte Konfiguration

Feld	Beschreibung
Hafen	Von der Nimble REST API verwendeter Port. Der Standardwert ist 5392.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Hinweis: Das Standardintervall für die Leistungsabfrage beträgt 300 Sekunden und kann nicht geändert werden. Dies ist das einzige von HPE Alletra 6000 unterstützte Intervall.

Hitachi-Datensysteme

Datensammler der Hitachi Vantara Command Suite

Der Datensammler der Hitachi Vantara Command Suite unterstützt den HiCommand Device Manager-Server. Data Infrastructure Insights kommuniziert mit dem HiCommand Device Manager-Server über die standardmäßige HiCommand-API.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Datensammler der Hitachi Vantara Command Suite. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
PDEV	Scheibe
Zeitschriftenpool	Datenträgergruppe
Speicher-Array	Storage
Port-Controller	Speicherknoten
Array-Gruppe, HDS-Pool	Speicherpool
Logische Einheit, LDEV	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Storage

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten von HDS-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Name – kommt direkt aus dem „Name“-Attribut des HDS HiCommand Device Managers über den GetStorageArray XML-API-Aufruf
- Modell – kommt direkt vom „arrayType“-Attribut des HDS HiCommand Device Manager über den GetStorageArray XML-API-Aufruf
- Anbieter – HDS
- Familie – kommt direkt vom Attribut „arrayFamily“ des HDS HiCommand Device Manager über den GetStorageArray XML-API-Aufruf
- IP – dies ist die Verwaltungs-IP-Adresse des Arrays, keine vollständige Liste aller IP-Adressen auf dem Array
- Rohkapazität – ein Basiswert 2, der die Summe der Gesamtkapazität aller Festplatten in diesem System darstellt, unabhängig von der Festplattenrolle.

Speicherpool

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der HDS-Speicherpool-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Typ: Der Wert hier ist einer der folgenden:
 - RESERVIERT – wenn dieser Pool für andere Zwecke als Datenvolumes vorgesehen ist, z. B. Journaling, Snapshots
 - Thin Provisioning – wenn es sich um einen HDP-Pool handelt
 - Raid-Gruppe – diese werden Sie aus mehreren Gründen wahrscheinlich nicht sehen:

Data Infrastructure Insights vertritt die strikte Haltung, eine doppelte Zählkapazität um jeden Preis zu vermeiden. Auf HDS muss man normalerweise RAID-Gruppen aus Festplatten erstellen, Pool-Volumes auf diesen RAID-Gruppen erstellen und Pools (oft HDP, können aber auch Spezialzwecken dienen) aus diesen Pool-Volumes erstellen. Wenn Data Infrastructure Insights sowohl die zugrunde liegenden RAID-Gruppen als auch die Pools unverändert melden würde, würde die Summe ihrer Rohkapazität die Summe der Festplatten bei weitem übersteigen.

Stattdessen verkleinert der HDS Command Suite-Datensammler von Data Infrastructure Insights die Größe von RAID-Gruppen willkürlich um die 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 in das Data Infrastructure Insights Data Warehouse (DWH) fließen. Der Zweck dieser Entscheidungen besteht darin, eine überladene Benutzeroberfläche für Dinge zu vermeiden, die für die meisten Benutzer unwichtig sind. Wenn Ihr HDS-Array über RAID-Gruppen mit 50 MB freiem Speicherplatz verfügt, können Sie diesen freien Speicherplatz wahrscheinlich nicht sinnvoll nutzen.

- Knoten – N/A, da HDS-Pools nicht an einen bestimmten Knoten gebunden sind
- Redundanz – die RAID-Ebene des Pools. Möglicherweise mehrere Werte für einen HDP-Pool, der aus mehreren RAID-Typen besteht
- Kapazität % – der Prozentsatz, der vom Pool für die Datennutzung verwendet wird, mit den verwendeten GB und der gesamten logischen GB-Größe des Pools
- Überbelegte Kapazität – ein abgeleiteter Wert, der besagt, dass „die logische Kapazität dieses Pools um diesen Prozentsatz überbelegt ist, da die Summe der logischen Volumes die logische Kapazität des Pools um diesen Prozentsatz übersteigt“.
- Snapshot – zeigt die für die Snapshot-Nutzung in diesem Pool reservierte Kapazität an

Speicherknoten

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der HDS-Speicherknoten-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

- Name – Der Name des Front-End-Directors (FED) oder Kanaladapters auf monolithischen Arrays oder der Name des Controllers auf einem modularen Array. Ein bestimmtes HDS-Array verfügt über 2 oder mehr Speicherknoten
- Volumes – Die Volume-Tabelle zeigt alle Volumes an, die einem Port zugeordnet sind, der diesem Speicherknoten gehört.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse des HiCommand Device Manager-Servers
- Nur-Lese-Benutzername und Passwort für die HiCommand Device Manager-Software und Peer-Berechtigungen
- Portanforderungen: 2001 (http) oder 2443 (https)
- Melden Sie sich mit Benutzername und Passwort bei der HiCommand Device Manager-Software an
- Überprüfen Sie den Zugriff auf HiCommand Device Manager
`http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager`

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

- HDS USP-, USP V- und VSP-Leistung
 - Performance Monitor muss lizenziert sein.
 - Der Überwachungsschalter muss aktiviert sein.
 - Das Exporttool (Export.exe) muss in die Data Infrastructure Insights AU kopiert werden.
 - Die Version des Exporttools muss mit der Mikrocodeversion des Zielarrays übereinstimmen.
- AMS-Leistung:
 - NetApp empfiehlt dringend, auf AMS-Arrays ein dediziertes Servicekonto für Data Infrastructure Insights zu erstellen, um Leistungsdaten abzurufen. Storage Navigator erlaubt einem Benutzerkonto nur eine gleichzeitige Anmeldung beim Array. Wenn Data Infrastructure Insights dasselbe Benutzerkonto wie Verwaltungsskripte oder HiCommand verwendet, kann dies dazu führen, dass Data Infrastructure Insights, Verwaltungsskripte oder HiCommand aufgrund der Beschränkung auf ein gleichzeitiges Benutzerkonto nicht mit dem Array kommunizieren können.
 - 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	Für den HiCommand Device Manager-Server verwendetes Passwort.
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 den JAR-Dateien des Export-Dienstprogramms

Feld	Beschreibung
SNM2Devices – WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array-IP: IP-Adresse des Speichers * Storage Navigator CLI-Pfad: SNM2 CLI-Pfad * Gültige Kontoauthentifizierung: Wählen Sie diese Option, um eine gültige Kontoauthentifizierung auszuwählen * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für die Leistung	Andere Leistungsoptionen außer Kraft setzen
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domänenname des Tuning-Managers
Tuning Manager-Port überschreiben	Wenn leer, verwenden Sie den Standardport im Feld „Tuning Manager für Leistung auswählen“, andernfalls geben Sie den zu verwendenden Port ein.
Tuning Manager-Benutzername	Benutzername für Tuning Manager
Tuning Manager-Passwort	Passwort für Tuning Manager

Hinweis: In 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	Für den HiCommand Device Manager verwendeter Port
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräteliste filtern	Durch Kommas getrennte Liste der Geräteseriennummern, die ein- oder ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.
Export-Timeout in Sekunden	Zeitüberschreitung beim Export-Dienstprogramm. Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Der Benutzer verfügt nicht über ausreichende Berechtigungen	Verwenden Sie ein anderes Benutzerkonto mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des im Datensammler konfigurierten Benutzerkontos
Fehler: Die Speicherliste ist leer. Entweder sind die 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 mit mehr Berechtigungen oder erhöhen Sie die Berechtigungen des Benutzerkontos
Fehler: Das HDS-Speicherarray wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HDS HiCommand nicht aktualisiert wird.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des Export-Dienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Export Utility auf der Data Infrastructure Insights Acquisition Unit installiert ist. * Bestätigen Sie, dass der Speicherort des Export Utility in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass Benutzername und Kennwort in der Konfiguration des Datensammlers korrekt sind. * Bestätigen Sie, dass die Version des Export Utility mit der Mikrocodeversion des Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie die Batchdatei runWin.bat ausführen.
Fehler: Anmeldung beim Exporttool für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt sind. * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler. * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind.
Fehler: Die Exporttools haben „Zeitbereich für Überwachung konnte nicht abgerufen werden“ protokolliert.	* Bestätigen Sie, dass die Leistungsüberwachung auf dem Array aktiviert ist. * Versuchen Sie, die Exporttools außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Export-Dienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird von Storage Navigator Modular CLI nicht unterstützt	* Konfigurieren Sie nur unterstützte Speicher-Arrays. * Verwenden Sie „Geräteliste filtern“, um nicht unterstützte Speicher-Arrays auszuschließen.

Problem:	Versuchen Sie Folgendes:
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet * Konfigurationsfehler: Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Export-Dienstprogramms. * Prüfen Sie, ob das betreffende Speicherarray im HiCommand-Server konfiguriert ist. * Legen Sie das Leistungsabfrageintervall auf ein Vielfaches von 60 Sekunden fest.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen des Auperform-Befehls * 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 der Speicherort von Storage Navigator Modular CLI in der Datensammlerkonfiguration korrekt ist. * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie, dass die Version von Storage Navigator Modular CLI mit der Mikrocodeversion des im Datensammler konfigurierten Speicherarrays kompatibel ist. * Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus eine CMD-Eingabeaufforderung und führen Sie folgende Schritte aus: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis. - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicherarray herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicherarray nicht vom Inventar gemeldet	Überprüfen Sie, ob das betreffende Speicherarray im HiCommand-Server konfiguriert ist
Fehler: * Kein Array ist bei der Storage Navigator Modular 2 CLI registriert * Array ist nicht bei der Storage Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei der StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. * Führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus. * Bestätigen Sie, dass die Befehlsausgabe Details zum Array mit IP enthält. * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit der Storage Navigator-CLI: – Öffnen Sie die Eingabeaufforderung und wechseln Sie zum konfigurierten Verzeichnis. – 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 in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des Hitachi Vantara NAS-Datenkollektors

Der Hitachi Vantara NAS-Datensammler ist ein Inventar- und Konfigurationsdatensammler, der die Erkennung von HDS NAS-Clustern unterstützt. Data Infrastructure Insights unterstützt die Erkennung von NFS- und CIFS-Freigaben, Dateisystemen (internen Volumes) und Spans (Speicherpools).

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom HNAS-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Stufe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Spanne	Speicherpool
Systemlaufwerk	Backend-Lun
Dateisystem	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort – Berechtigungsstufe: Supervisor
- Hinweis: Dieser Datensammler ist SSH-basiert, daher muss die AU, die ihn hostet, in der Lage sein, SSH-Sitzungen zu TCP 22 auf dem HNAS selbst oder der Systems Management Unit (SMU), mit der der Cluster verbunden ist, zu initiieren.

Konfiguration

Feld	Beschreibung
HNAS-Host	IP-Adresse oder vollqualifizierter Domänenname des HNAS-Verwaltungshosts
Benutzername	Benutzername für HNAS CLI
Passwort	Für HNAS CLI verwendetes Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 30 Minuten.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Fehler beim Verbinden“ mit den Fehlermeldungen „Fehler beim Einrichten des Shell-Kanals:“ oder „Fehler beim Öffnen des Shell-Kanals“	Wird wahrscheinlich durch Probleme mit der Netzwerkverbindung oder eine falsche SSH-Konfiguration verursacht. Bestätigen Sie die Verbindung mit einem alternativen SSH-Client
„Timeout“ oder „Fehler beim Abrufen der Daten“ mit der Fehlermeldung „Befehl: XXX hat eine Zeitüberschreitung.“	* Versuchen Sie den Befehl mit einem anderen SSH-Client. * Erhöhen Sie das Timeout.
„Fehler beim Verbinden“ oder „Ungültige Anmeldeinformationen“ mit der Fehlermeldung „Konnte nicht mit dem Gerät kommunizieren:“	* IP-Adresse prüfen * Benutzernamen und Passwort prüfen * Verbindung mit alternativem SSH-Client bestätigen

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Hitachi Ops Center-Datensammler

Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Inventar- und Leistungsdaten mehrerer Speichergeräte zuzugreifen. Zur Inventar- und Kapazitätsermittlung muss Ihre Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Für die Leistungserfassung müssen Sie zusätzlich „Analyzer“ bereitgestellt haben.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speichersysteme	Storage
Volumen	Volumen
Paritätsgruppen	Speicherpool (RAID), Datenträgergruppen
Scheibe	Scheibe
Speicherpool	Speicherpool (Thin, SNAP)
Externe Paritätsgruppen	Speicherpool (Backend), Datenträgergruppen
Hafen	Speicherknoten → Controllerknoten → Port
Hostgruppen	Volumenzuordnung und -maskierung
Volumenpaare	Speichersynchronisierung

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

Um Bestandsdaten erfassen zu können, benötigen Sie Folgendes:

- IP-Adresse oder Hostname des Ops Center-Servers, auf dem die Komponente „Common Services“ gehostet wird
- Root-/Sysadmin-Benutzerkonto und -Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center-Komponenten gehostet werden. HDS hat die REST-API-Unterstützung für die Verwendung durch LDAP/SSO-Benutzer erst ab Ops Center 10.8 implementiert.

Leistungsanforderungen

Um Leistungsdaten erfassen zu können, müssen folgende Voraussetzungen erfüllt sein:

Das HDS Ops Center „Analyzer“-Modul muss installiert sein. Speicher-Arrays müssen das Ops Center „Analyzer“-Modul versorgen.

Konfiguration

Feld	Beschreibung
IP-Adresse des Hitachi Ops Center	IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, auf dem die Komponente „Common Services“ gehostet wird
Benutzername	Benutzername für den Ops Center-Server.
Passwort	Für den Ops Center-Server verwendetes Kennwort.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Port 443) ist die Standardeinstellung
TCP-Port überschreiben	Geben Sie den zu verwendenden Port an, wenn dieser nicht der Standardport ist.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten stehende Array-Liste beim Sammeln von Daten ein- oder ausgeschlossen werden soll.
Geräteliste filtern	Durch Kommas getrennte Liste der Geräteseriennummern, die ein- oder ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert ist 300.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Infinidat InfiniBox Datensammler

Der Infinidat InfiniBox (HTTP)-Datensammler wird zum Sammeln von

Bestandsinformationen vom Infinidat InfiniBox-Speichersystem verwendet.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Infinidat InfiniBox-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Node	Regler
Dateisystem	Internes Volumen
Dateisystem	Dateifreigabe
Dateisystemexporte	Aktie

Anforderungen

Im Folgenden sind die Anforderungen für die Konfiguration dieses Datensammlers aufgeführt.

- IP-Adresse oder FQDN des InfiniBox-Verwaltungsknotens
- Administrator-Benutzer-ID und -Passwort
- Port 443 über REST-API

Konfiguration

Feld	Beschreibung
InfiniBox-Host	IP-Adresse oder vollqualifizierter Domänenname des InfiniBox-Verwaltungsknotens
Benutzername	Benutzername für den InfiniBox-Verwaltungsknoten
Passwort	Passwort für den InfiniBox-Verwaltungsknoten

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem InfiniBox-Server verwendet wird. Der Standardwert ist 443.
Inventarabfrageintervall	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Huawei OceanStor Datensammler

Data Infrastructure Insights verwendet den Huawei OceanStor (REST/HTTPS)-Datensammler, um Inventar und Leistung für Huawei OceanStor- und OceanStor Dorado-Speicher zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Dateisystem	Internes Volumen
Regler	Speicherknoten
FC-Port (zugeordnet)	Volumenkarte
Host-FC-Initiator (zugeordnet)	Volumenmaske
NFS/CIFS-Freigabe	Aktie
iSCSI-Link-Ziel	iSCSI-Zielknoten
iSCSI-Link-Initiator	iSCSI-Initiatorknoten
Scheibe	Scheibe
LUN	Volumen

Anforderungen

Zum Konfigurieren dieses Datensammlers sind die folgenden Voraussetzungen erforderlich:

- IP-Adresse des Geräts
- Anmeldeinformationen für den Zugriff auf den OceanStor-Gerätemanager
- Port 8088 muss verfügbar sein

Konfiguration

Feld	Beschreibung
OceanStor-Host-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des OceanStor Device Managers
Benutzername	Name, der für die Anmeldung beim OceanStor Device Manager verwendet wird
Passwort	Passwort zur Anmeldung beim OceanStor Device Manager

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem OceanStor Device Manager verwendet wird. Der Standardwert ist 8088.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.).	Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

IBM

IBM Cleversafe-Datenkollektor

Data Infrastructure Insights verwendet diesen Datenkollektor, um Bestands- und Leistungsdaten für IBM Cleversafe-Speichersysteme zu ermitteln.



Für IBM Cleversafe gilt ein anderer Tarif als für verwaltete Einheiten (Raw TB). Für jeweils 40 TB unformatierte IBM Cleversafe-Kapazität wird 1 ["Verwaltete Einheit \(MU\)"](#) .

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM Cleversafe-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Manager-IP oder Hostname	IP-Adresse oder Hostname des Verwaltungsknotens
Benutzername	Benutzername für das Benutzerkonto mit Superuser- oder Systemadministratorrolle
Passwort	Kennwort für das Benutzerkonto mit der Rolle „Superuser“ oder „Systemadministrator“

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen.
HTTP-Verbindungs-Timeout (Sek.)	HTTP-Timeout in Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

IBM CS-Datenkollektor

Data Infrastructure Insights verwendet diesen Datensammler, um Bestands- und Leistungsdaten für IBM CS-Speichersysteme zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM CS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezugeordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Port 9440

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem IBM CS-Array verwendet wird. Der Standardwert ist 9440.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Datenkollektor der IBM System Storage DS8000-Serie

Der IBM DS (CLI)-Datenkollektor unterstützt die Erfassung von Inventar- und Leistungsdaten für DS6xxx- und DS8xxx-Geräte.

DS3xxx-, DS4xxx- und DS5xxx-Geräte werden unterstützt von ["NetApp E-Series Datenkollektor"](#) . Informationen zu unterstützten Modellen und Firmware-Versionen finden Sie in der Supportmatrix von Data Infrastructure Insights .

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM DS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplattenmodul	Scheibe
Speicherimage	Storage
Extent-Pool	Speicherknoten
Festes Blockvolumen	Volumen
Host-FC-Initiator (zugeordnet)	Volumenmaske

Hinweis: Dies sind nur allgemeine Terminologiezuordnungen und stellen möglicherweise nicht jeden Fall für

diesen Datensammler dar.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie Folgendes:

- IP-Adresse jedes DS-Arrays
- Nur-Lese-Benutzername und Passwort auf jedem DS-Array
- Auf der Data Infrastructure Insights AU installierte Drittanbietersoftware: IBM *dscli*
- Zugriffsvalidierung: Führen Sie *dscli*-Befehle mit dem Benutzernamen und dem Kennwort aus
- Portanforderungen: 80, 443 und 1750

Konfiguration

Feld	Beschreibung
DS-Speicher	IP-Adresse oder vollqualifizierter Domänenname des DS-Geräts
Benutzername	Benutzername für die DS CLI
Passwort	Passwort für die DS CLI
<i>dscli</i> ausführbarer Pfad	Vollständiger Pfad zur ausführbaren Datei <i>dscli</i>

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen Bestandsabfragen (min). Der Standardwert ist 40.
Speicheranzeigenname	Name des IBM DS-Speicherarrays
Aus dem Inventar ausgeschlossene Geräte	Durch Kommas getrennte Liste der Geräteseriennummern, die von der Inventarerfassung ausgeschlossen werden sollen
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.
Leistungsfiltertyp	Einschließen: Nur von Geräten auf der Liste erfasste Daten. Ausschließen: Von diesen Geräten werden keine Daten erfasst
Leistungsfilter-Geräteliste	Durch Kommas getrennte Liste von Geräte-IDs, die in die Leistungserfassung einbezogen oder davon ausgeschlossen werden sollen

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler mit: CMUC00192E, CMUC00191E oder CMUC00190E	* Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über die Webverwaltungskonsole <a href="https://<ip>:8452/DS8000/Console">https://<ip>:8452/DS8000/Console mit dem Array zu kommunizieren. Ersetzen Sie <ip> durch die für den Datensammler konfigurierte IP.
Fehler: * Programm kann nicht ausgeführt werden * Fehler beim Ausführen des Befehls	* Öffnen Sie von der Data Infrastructure Insights Acquisition Unit aus ein CMD. * Öffnen Sie die Datei CLI.CFG im Stammverzeichnis/der Bibliothek der CLI und überprüfen Sie die Eigenschaft JAVA_INSTALL. Bearbeiten Sie den Wert, damit er Ihrer Umgebung entspricht. * Zeigen Sie die auf diesem Computer installierte Java-Version an, indem Sie „java -version“ eingeben. * Pingen Sie die IP-Adresse des IBM-Speichergeräts an, das im ausgegebenen CLI-Befehl angegeben ist. * Wenn alles oben genannte gut funktioniert hat, führen Sie manuell einen CLI-Befehl aus

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des IBM SAN Volume Controller-Datenkollektors

Der IBM SAN Volume Controller (SVC)-Datenkollektor sammelt Inventar- und Leistungsdaten 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. Informationen zu unterstützten Modellen und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom IBM SVC-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Mdisk-Gruppe	Speicherpool
Vdisk	Volumen
MDisk	Backend-LUNs und -Pfade

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezugeordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Inventaranforderungen

- IP-Adresse jedes SVC-Clusters
- Port 22 verfügbar
- Benutzername und Kennwort nur zum Lesen

Leistungsanforderungen

- SVC-Konsole, die für jeden SVC-Cluster obligatorisch und für das SVC Discovery Foundation-Paket erforderlich ist.
- Für die Anmeldeinformationen ist nur zum Kopieren von Leistungsdateien von Clusterknoten auf den Konfigurationsknoten eine Administratorzugriffsebene erforderlich.
- Aktivieren Sie die Datenerfassung, indem Sie per SSH eine Verbindung zum SVC-Cluster herstellen und Folgendes ausführen: `svctask startstats -interval 1`

Hinweis: Alternativ können Sie die Datenerfassung über die SVC-Verwaltungsbenutzeroberfläche aktivieren.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adressen	IP-Adressen oder vollqualifizierte Domännennamen des SVC-Speichers
Inventar-Benutzername	Benutzername für die SVC-CLI
Inventarkennwort	Passwort für die SVC-CLI

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.
So bereinigen Sie gedumpte Statistikdateien	Aktivieren Sie dieses Kontrollkästchen, um die gespeicherten Statistikdateien zu bereinigen.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurationsknoten ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: „Der Befehl kann nicht initiiert werden, da er nicht auf dem Konfigurationsknoten ausgeführt wurde.“	Der Befehl muss auf dem Konfigurationsknoten ausgeführt werden.

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des IBM XIV/A9000-Datenkollektors

Der IBM XIV- und A9000-Datenkollektor (CLI) verwendet die XIV-Befehlszeilenschnittstelle zum Erfassen von Inventardaten, während die Leistungserfassung durch SMI-S-Aufrufe an das XIV/A9000-Array erfolgt, auf dem ein SMI-S-Anbieter auf Port 7778 ausgeführt wird.

Terminologie

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Speichersystem	Storage
Speicherpool	Speicherpool
Volumen	Volumen

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen folgende Voraussetzungen erfüllt sein:

- Portanforderung: TCP-Port 7778
- Benutzername und Kennwort nur zum Lesen
- Die XIV CLI muss auf der AU installiert sein

Leistungsanforderungen

Voraussetzungen für die Leistungserfassung sind:

- SMI-S Agent 1.4 oder höher
- SMI-S-kompatibler CIMService, der auf dem Array ausgeführt wird. Auf den meisten XIV-Arrays ist standardmäßig ein CIMServer installiert.
- Für den CIMServer muss eine Benutzeranmeldung bereitgestellt werden. Die Anmeldung muss über vollständigen Lesezugriff auf die Array-Konfiguration und -Eigenschaften verfügen.
- SMI-S-Namespace. Der Standardwert ist root/ibm. Dies ist im CIMServer konfigurierbar.
- Portanforderungen: 5988 für HTTP, 5989 für HTTPS.
- Unter folgendem Link erfahren Sie, wie Sie ein Konto für die SMI-S-Leistungserfassung erstellen:
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 Domänenname des XIV-Speichers
Benutzername	Benutzername für den XIV-Speicher
Passwort	Passwort für den XIV-Speicher
Vollständiger Pfad zum XIV CLI-Verzeichnis	Vollständiger Pfad zum Ordner, der die XIV CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 40 Minuten.
SMI-S-Protokoll	Für die Verbindung mit dem SMI-S-Anbieter verwendetes Protokoll. Zeigt auch den Standardport an.
SMI-S-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Benutzername	Benutzername für den SMI-S Provider-Host
Passwort	Kennwort für den SMI-S-Provider-Host
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Lenovo Datensammler

Data Infrastructure Insights verwendet den Lenovo-Datensammler, um Bestands- und Leistungsdaten für Lenovo HX-Speichersysteme zu ermitteln.

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Externe Prism-IP-Adresse
- Administrator-Benutzername und -Passwort
- TCP-Port-Anforderung: 9440

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem Array verwendet wird. Der Standardwert ist 9440.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Microsoft

Konfigurieren des Azure NetApp Files Datensammlers

Data Infrastructure Insights verwendet den Azure NetApp Files Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Anforderungen

Zur Konfiguration dieses Datensammlers benötigen Sie folgende Informationen.

- Portanforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Azure-Dienstprinzipal-Client-ID (Benutzerkonto)
- Azure-Dienstprinzipal-Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen für die Data Infrastructure Insights Erkennung ein Azure-Konto einrichten.

Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Anwendung in Azure registrieren, verfügen Sie über die erforderlichen Anmeldeinformationen, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Unter folgendem Link wird beschrieben, wie Sie das Konto für die Erkennung 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-Dienstprinzipal-Client-ID	Anmelde-ID für Azure
Azure-Mandanten-ID	Azure-Mandanten-ID
Azure-Dienstprinzipalauthentifizierungsschlüssel	Login-Authentifizierungsschlüssel
Mir ist bekannt, dass Microsoft mir API-Anfragen in Rechnung stellt.	Aktivieren Sie dies, um zu bestätigen, dass Sie verstanden haben, dass Microsoft Ihnen für API-Anfragen, die durch Insight-Polling gestellt werden, eine Rechnung stellt.

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60

Fehlerbehebung

- Die von Ihrem ANF-Datensammler verwendeten Anmeldeinformationen müssen Zugriff auf alle Azure-Abonnements haben, die ANF-Volumes enthalten.
- Wenn die Leistungserfassung aufgrund des Leserzugriffs fehlschlägt, versuchen Sie, dem Mitwirkenden Zugriff auf Ressourcengruppenebene zu gewähren.

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

Microsoft Hyper-V-Datensammler

Der Microsoft Hyper-V-Datensammler erfasst Inventar- und Leistungsdaten aus der virtualisierten Server-Computerumgebung. Dieser Datensammler kann einen eigenständigen Hyper-V-Host oder einen ganzen Cluster erkennen – erstellen Sie einen Sammler pro eigenständigem Host oder Cluster.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen von Microsoft Hyper-V (WMI). Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Virtuelle Festplatte
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Cluster Shared Volumes (CSV), Partitionsvolume	Datenspeicher

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Internet-SCSI-Gerät, Multi-Path-SCSI-LUN	LUN
Fiber Channel-Anschluss	Hafen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Für Hyper-V muss Port 5985 für die Datenerfassung und den Remotezugriff/die Remoteverwaltung geöffnet sein.
- IP-Adresse oder FQDN des Clusters oder eigenständigen Hypervisors. Die Verwendung des Floating-Cluster-Hostnamens oder der IP ist wahrscheinlich der zuverlässigste Ansatz, anstatt den Collector auf nur einen bestimmten Knoten in einem Cluster zu richten.
- Benutzerkonto auf Administratorebene, das auf allen Hypervisoren im Cluster funktioniert.
- WinRM muss aktiviert sein und auf allen Hypervisoren lauschen
- Portanforderungen: Port 135 über WMI und dynamische TCP-Ports zugewiesen 1024-65535 für Windows 2003 und älter und 49152-65535 für Windows 2008.
- Die DNS-Auflösung muss erfolgreich sein, auch wenn der Datensammler nur auf eine IP-Adresse verweist.
- Bei jedem Hyper-V-Hypervisor muss die „Ressourcenmessung“ für jede VM auf jedem Host aktiviert sein. Dadurch stehen jedem Hypervisor auf jedem Gast mehr Daten für Data Infrastructure Insights zur Verfügung. Wenn dies nicht festgelegt ist, werden für jeden Gast weniger Leistungsmetriken erfasst. Weitere Informationen zur Ressourcenmessung finden Sie in der Microsoft-Dokumentation:

["Übersicht über die Hyper-V-Ressourcenmessung"](#)

["Aktivieren Sie VMResourceMetering"](#)



Der Hyper-V-Datensammler erfordert eine Windows-Erfassungseinheit.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adresse oder Floating-Cluster-FQDN	Die IP-Adresse oder der vollqualifizierte Domänenname für den Cluster oder einen eigenständigen, nicht geclusterten Hypervisor
Benutzername	Administrator-Benutzername für den Hypervisor
Passwort	Passwort für den Hypervisor
DNS-Domänensuffix	Das Hostnamensuffix, das mit dem einfachen Hostnamen kombiniert wird, um den FQDN eines Hypervisors darzustellen

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp

NetApp Cloud Volumes ONTAP Datenkollektor

Dieser Datensammler unterstützt die Bestandserfassung von Cloud Volumes ONTAP -Konfigurationen.

Konfiguration

Feld	Beschreibung
NetApp -Verwaltungs-IP-Adresse	IP-Adresse für Cloud Volumes ONTAP
Benutzername	Benutzername für Cloud Volumes ONTAP
Passwort	Passwort für den oben genannten Benutzer

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS empfohlen. Zeigt auch den Standardport an.
Kommunikationsanschluss überschreiben	Zu verwendender Port, wenn nicht Standard.
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Inventar gleichzeitige Thread-Anzahl	Anzahl gleichzeitiger Threads.
TLS für HTTPS erzwingen	TLS über HTTPS erzwingen
Netzgruppen automatisch suchen	Netzgruppen automatisch suchen
Netgroup-Erweiterung	Shell oder Datei auswählen
HTTP-Lesezeitlimit (Sekunden)	Der Standardwert ist 30 Sekunden
Erzwingen Sie Antworten als UTF-8	Erzwingen Sie Antworten als UTF-8
Leistungsabfrageintervall (min)	Der Standardwert ist 900 Sekunden.
Leistung: Gleichzeitige Threadanzahl	Anzahl gleichzeitiger Threads.
Erweiterte Zählerdatenerfassung	Aktivieren Sie diese Option, damit Data Infrastructure Insights die erweiterten Metriken aus der folgenden Liste erfasst.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp ONTAP AFX-Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Inventar-, EMS-Protokoll- und Leistungsdaten von Speichersystemen mit ONTAP 9.16.0 und höher.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass zum Erstellen eines neuen REST-Benutzers/einer neuen REST-Rolle Administratorberechtigungen erforderlich sind.
 - Funktional stellt Data Infrastructure Insights in erster Linie Leseanforderungen, für die Registrierung von Data Infrastructure Insights beim ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich. Siehe den *Hinweis zu Berechtigungen* direkt unten.
- ONTAP Version 9.16.0 oder höher.
- Portanforderungen: 443

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP Zählern basieren, sollten Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte Zählerdatenerfassung aktivieren“ aktiviert lassen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators 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 *Befehle auf Diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des virtuellen Servers 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. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl

```
security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt aussehen. Ihre tatsächliche Ausgabe kann abweichen:

```
security login rest-role show -vserver <vserver name> -role restRole
```

Vserver	Role Name	API	Access 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>

User/Group	Authentication	Acct	Second
restUser	http	password	restRole
			no
			none

Migration

Um von einem früheren ONTAP Datensammler (ontapi) zum neueren ONTAP REST-Sammler zu migrieren, gehen Sie wie folgt vor:

1. Fügen Sie den REST-Collector hinzu. Es wird empfohlen, die Informationen für einen anderen Benutzer einzugeben als den, der für den vorherigen Collector konfiguriert wurde. Verwenden Sie beispielsweise den im Abschnitt „Berechtigungen“ oben angegebenen Benutzer.
2. Halten Sie den vorherigen Collector an, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector mindestens 30 Minuten lang Daten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ erscheinen.
4. Nach der Ruhephase sollten sich Ihre Daten stabilisieren, da der REST-Collector weiterhin Daten erfasst.

Mit demselben Verfahren können Sie bei Bedarf zum vorherigen Collector zurückkehren.

Konfiguration

Feld	Beschreibung
ONTAP -Verwaltungs-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des NetApp Clusters. Muss eine Cluster-Verwaltungs-IP/ein FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zählerdatenerfassung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
EMS-Ereigniserfassung aktivieren	Wählen Sie diese Option aus, um ONTAP EMS-Protokollereignisdaten einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Storage

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Node	Speicherknoten
Volumen/ FlexVol/ FlexGroup	Internes Volumen
Qtree/FlexTree	Qtree (Typ: Explict/Standard)
S3-Bucket	Qtree (Typ: Bucket)
StoragePod/StorageAvailabilityZone	Speicherpool
Aktie	Aktie
Quote	Quote
SVM (Storage Virtual Machine)	Virtuelle Speichermaschine

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbieternamen, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – Die Array-UUID
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Mikrocode-Version – Firmware.
- Rohkapazität – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?

- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP REST-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Prozessoren – CPU-Anzahl.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können. Die unten stehenden Listen unterstützter und nicht unterstützter Modelle sind nicht vollständig, sollen aber als Orientierung dienen. Im Allgemeinen gilt: Wenn ein

Modell zur selben Familie gehört wie eines auf der Liste, sollte auch die Unterstützung dieselbe 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/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Beim Versuch, einen ONTAP REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest-API unter 10.193.70.14 ist nicht verfügbar: 10.193.70.14 konnte /api/cluster nicht abrufen: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem älteren ONTAP Array (z. B. ONTAP 9.6), das über keine REST-API-Funktionen verfügt. ONTAP 9.14.1 ist die minimale ONTAP Version, die vom ONTAP REST Collector unterstützt wird. Bei Versionen vor REST ONTAP sind Antworten vom Typ „400 Bad Request“ zu erwarten. Bei ONTAP Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, wird möglicherweise die folgende ähnliche Meldung angezeigt: Konfiguration: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist verfügbar: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7, hat aber nicht mindestens die Version 9.14.1.
Ich sehe leere oder „0“-Metriken, wo der ONTAP ontapi-Collector Daten anzeigt.	ONTAP REST meldet keine Metriken, die nur intern auf dem ONTAP -System verwendet werden. Beispielsweise werden von ONTAP REST keine Systemaggregate erfasst, sondern nur SVMs vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Metriken, die möglicherweise Null- oder leere Daten melden: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Speicher: Die meisten Metriken sind eine Zusammenfassung der Metriken des internen Volumes und werden von den oben genannten Faktoren beeinflusst. Speicher-Virtual Machines: REST meldet keine SVMs mehr vom Typ „Daten“ (z. B. „Cluster“, „MGM“, „Knoten“). Möglicherweise stellen Sie auch eine Änderung im Erscheinungsbild von Diagrammen fest, die Daten enthalten. Grund hierfür ist die Änderung des Standardabfragezeitraums für die Leistung von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Aufzeichnen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp ONTAP ASA r2 (All-SAN Array) Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Inventar-, EMS-Protokoll- und Leistungsdaten von Speichersystemen mit ONTAP 9.16.0 und höher.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass zum Erstellen eines neuen REST-Benutzers/einer neuen REST-Rolle Administratorberechtigungen erforderlich sind.
 - Funktional stellt Data Infrastructure Insights in erster Linie Leseanforderungen, für die Registrierung von Data Infrastructure Insights beim ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich. Siehe den *Hinweis zu Berechtigungen* direkt unten.
- ONTAP Version 9.16.0 oder höher.
- Portanforderungen: 443



ASA R2 bezeichnet die Modelle der neuesten Generation der ONTAP ASA Speicherplattform. Dazu gehören die Array-Modelle ASA A1K, A90, A70, A50, A30 und A20.

Für alle ASA -Systeme der vorherigen Generation verwenden Sie bitte die **"ONTAP REST"** Kollektor.

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP Zählern basieren, sollten Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte Zählerdatenerfassung aktivieren“ aktiviert lassen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators 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 *Befehle auf Diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des virtuellen Servers 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. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben.

```

security login create -username ci_user -application http
-authentication-method password -role ci_readonly

```

Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl

```

security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly

```

Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt aussehen. Ihre tatsächliche Ausgabe kann abweichen:

```

security login rest-role show -vserver <vserver name> -role restRole

```

Vserver	Role Name	API	Access 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>

User/Group	Authentication	Acct	Second
Name	Application Method	Role Name	Locked Method
restUser	http password	restRole	no none

Migration

Um von einem früheren ONTAP Datensammler (ontapi) zum neueren ONTAP REST-Sammler zu migrieren, gehen Sie wie folgt vor:

1. Fügen Sie den REST-Collector hinzu. Es wird empfohlen, die Informationen für einen anderen Benutzer einzugeben als den, der für den vorherigen Collector konfiguriert wurde. Verwenden Sie beispielsweise den im Abschnitt „Berechtigungen“ oben angegebenen Benutzer.
2. Halten Sie den vorherigen Collector an, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector mindestens 30 Minuten lang Daten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ erscheinen.
4. Nach der Ruhephase sollten sich Ihre Daten stabilisieren, da der REST-Collector weiterhin Daten erfasst.

Mit demselben Verfahren können Sie bei Bedarf zum vorherigen Collector zurückkehren.

Konfiguration

Feld	Beschreibung
ONTAP -Verwaltungs-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des NetApp Clusters. Muss eine Cluster-Verwaltungs-IP/ein FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zählerdatenerfassung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
EMS-Ereigniserfassung aktivieren	Wählen Sie diese Option aus, um ONTAP EMS-Protokollereignisdaten einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen
Virtuelle Speichermaschine/VServer	Virtuelle Speichermaschine

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – Die Array-UUID
- IP – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- Mikrocode-Version – Firmware.
- Rohkapazität – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- Durchsatz – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?
- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.

- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknotten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP REST-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Prozessoren – CPU-Anzahl.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können. Die unten stehenden Listen unterstützter und nicht unterstützter Modelle sind nicht vollständig, sollen aber als Orientierung dienen. Im Allgemeinen gilt: Wenn ein Modell zur selben Familie gehört wie eines auf der Liste, sollte auch die Unterstützung dieselbe 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/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Beim Versuch, einen ONTAP REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest-API unter 10.193.70.14 ist nicht verfügbar: 10.193.70.14 konnte /api/cluster nicht abrufen: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem älteren ONTAP Array (z. B. ONTAP 9.6), das über keine REST-API-Funktionen verfügt. ONTAP 9.14.1 ist die minimale ONTAP Version, die vom ONTAP REST Collector unterstützt wird. Bei Versionen vor REST ONTAP sind Antworten vom Typ „400 Bad Request“ zu erwarten. Bei ONTAP Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, wird möglicherweise die folgende ähnliche Meldung angezeigt: Konfiguration: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist verfügbar: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7, hat aber nicht mindestens die Version 9.14.1.
Ich sehe leere oder „0“-Metriken, wo der ONTAP ontapi-Collector Daten anzeigt.	ONTAP REST meldet keine Metriken, die nur intern auf dem ONTAP -System verwendet werden. Beispielsweise werden von ONTAP REST keine Systemaggregate erfasst, sondern nur SVMs vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Metriken, die möglicherweise Null- oder leere Daten melden: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Speicher: Die meisten Metriken sind eine Zusammenfassung der Metriken des internen Volumes und werden von den oben genannten Faktoren beeinflusst. Speicher-Virtual Machines: REST meldet keine SVMs mehr vom Typ „Daten“ (z. B. „Cluster“, „MGM“, „Knoten“). Möglicherweise stellen Sie auch eine Änderung im Erscheinungsbild von Diagrammen fest, die Daten enthalten. Grund hierfür ist die Änderung des Standardabfragezeitraums für die Leistung von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Aufzeichnen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Datenkollektor der NetApp ONTAP Data Management Software

Dieser Datensammler erfasst Inventar- und Leistungsdaten von Speichersystemen, auf denen ONTAP ausgeführt wird, mithilfe von schreibgeschützten API-Aufrufen von einem

ONTAP Konto. Dieser Datensammler erstellt außerdem einen Datensatz im Cluster-Anwendungsregister, um den Support zu beschleunigen.

Terminologie

Data Infrastructure Insights erfasst Bestands- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- **Modell** – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, 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 Speichersystemen mit Clusterarchitektur wie ONTAP Data Management ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- **IP** – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- **Mikrocode-Version** – Firmware.
- **Rohkapazität** – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- **Latenz** – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- **Durchsatz** – aggregiert aus internen Volumes. **Verwaltung** – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash-Pool – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?
- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- Überbelegte Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster-Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.

- IOPS – Direkt abgeleitet von ONTAP ZAPI-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP ZAPI-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Wird direkt aus ONTAP ZAPI-Aufrufen des Knotenobjekts abgeleitet.
- Prozessoren – CPU-Anzahl.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützte API-Aufrufe konfiguriert ist.
- Zu den Kontodetails gehören Benutzername und Passwort.
- Portanforderungen: 80 oder 443
- Kontoberechtigungen:
 - Nur-Lese-Rollenamen für die Ontapi-Anwendung auf dem Standard-Vserver
 - Möglicherweise benötigen Sie zusätzliche optionale Schreibberechtigungen. Siehe den Hinweis zu Berechtigungen weiter unten.
- ONTAP -Lizenzanforderungen:
 - FCP-Lizenz und zugeordnete/maskierte Volumes für die Fibre-Channel-Erkennung erforderlich

Berechtigungsanforderungen für die Erfassung von ONTAP Switch-Metriken

Data Infrastructure Insights bietet die Möglichkeit, ONTAP Cluster-Switch-Daten als Option im Collector zu sammeln [Erweiterte Konfiguration](#) Einstellungen. Zusätzlich zur Aktivierung auf dem Data Infrastructure Insights Kollektor müssen Sie auch **das ONTAP -System** selbst konfigurieren, um Folgendes bereitzustellen: ["Switch-Informationen"](#) und stellen Sie sicher, dass die richtige [Berechtigungen](#) gesetzt, um die Switch-Daten an Data Infrastructure Insights senden zu können.

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domänenname des NetApp -Clusters
Benutzername	Benutzername für NetApp Cluster
Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Anschlussart	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Der Standardwert ist HTTPS
Kommunikationsanschluss überschreiben	Geben Sie einen anderen Port an, wenn Sie nicht den Standardport verwenden möchten
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.

Feld	Beschreibung
Für TLS für HTTPS	Lassen Sie TLS nur als Protokoll zu, wenn Sie HTTPS verwenden
Netzgruppen automatisch suchen	Aktivieren Sie die automatische Netzgruppensuche für Exporttrichtlinienregeln
Netgroup-Erweiterung	Expansionsstrategie der Netgroup. Wählen Sie <i>Datei</i> oder <i>Shell</i> . Der Standardwert ist <i>shell</i> .
HTTP-Lesezeitlimit (Sekunden)	Der Standardwert ist 30
Erzwingen Sie Antworten als UTF-8	Zwingt den Datensammlercode, Antworten von der CLI als in UTF-8 vorliegend zu interpretieren
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 900 Sekunden.
Erweiterte Zählerdatenerfassung	Aktivieren Sie die ONTAP Integration. Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Wählen Sie die gewünschten Zähler aus der Liste aus.
Cluster-Switch-Metriken	Erlauben Sie Data Infrastructure Insights , Cluster-Switch-Daten zu erfassen. Beachten Sie, dass Sie zusätzlich zur Aktivierung auf der Data Infrastructure Insights Seite auch das ONTAP -System so konfigurieren müssen, dass es " Switch-Informationen " und stellen Sie sicher, dass die richtige Berechtigungen gesetzt, um die Switch-Daten an Data Infrastructure Insights senden zu können. Siehe „Hinweis zu Berechtigungen“ weiter unten.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können.



Diese Listen sind nicht vollständig und können sich ändern. Wenn ein Modell zur selben Familie gehört wie ein Modell auf der Liste, sollte die Unterstützung grundsätzlich dieselbe sein, dies kann jedoch nicht garantiert werden. Wenn Sie nicht sicher sind, ob Ihr Modell Leistungsmetriken unterstützt, wenden Sie sich an den ONTAP Support.

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/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 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 die Option „Erweiterte

Zählerdatenerfassung“ aktivieren.

Sie sollten außerdem sicherstellen, dass die Schreibberechtigung für die ONTAP -API aktiviert ist. Dies erfordert normalerweise ein Konto auf Clusterebene mit den erforderlichen Berechtigungen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators 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 *Befehle auf 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. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben.

```
security login create -username ci_user -application ontapi  
-authentication-method password -role ci_readonly
```

Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl

```
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_rest -api  
/api/network/ethernet -access readonly  
security login create -user-or-group-name ci_user -application http  
-authmethod password -role ci_readonly_rest
```

Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt aussehen. Ihre tatsächliche Ausgabe kann abweichen:

```

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 Zugriffskontrolle nicht richtig eingestellt ist, können Data Infrastructure Insights REST-Aufrufe fehlschlagen, was zu Datenlücken für das Gerät führt. Wenn Sie es beispielsweise auf dem Data Infrastructure Insights -Collector aktiviert, die Berechtigungen auf dem ONTAP jedoch nicht konfiguriert haben, schlägt die Erfassung fehl. Wenn die Rolle zuvor auf ONTAP definiert wurde und Sie die Rest-API-Funktionen hinzufügen, stellen Sie außerdem sicher, dass *http* zur Rolle hinzugefügt wird.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.
Clusterversion ist < 8.1	Die minimal unterstützte Clusterversion ist 8.1. Aktualisieren Sie auf die minimal unterstützte Version.
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
Fehler: „7-Modus-Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diesen Datensammler verwenden, um 7-Modus-Filer zu ermitteln. Ändern Sie die IP, sodass sie stattdessen auf den CDOT-Cluster verweist.
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.

Problem:	Versuchen Sie Folgendes:
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen 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: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.

Performance

Problem:	Versuchen Sie Folgendes:
Fehler „Leistung konnte nicht von ZAPI erfasst werden“	Dies liegt normalerweise daran, dass die Leistungsstatistik nicht ausgeführt wird. Versuchen Sie auf jedem Knoten den folgenden Befehl: <code>> system node systemshell -node * -command "spmctl -h cmd -stop; spmctl -h cmd -exec"</code>

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp ONTAP REST-Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Inventar-, EMS-Protokoll- und Leistungsdaten von Speichersystemen mit ONTAP 9.14.1 und höher. Verwenden Sie für ONTAP -Systeme früherer Versionen den ZAPI-basierten Collectortyp „NetApp ONTAP Data Management Software“.



Der ONTAP REST-Collector kann als Ersatz für den vorherigen ONTAPI-basierten Collector verwendet werden. Daher kann es zu Unterschieden bei den erfassten oder gemeldeten Messwerten kommen. Weitere Informationen zu den Unterschieden zwischen ONTAPI und REST finden Sie im ["ONTAP 9.14.1 ONTAPI-zu-REST-Zuordnung"](#) Dokumentation.

Anforderungen

Für die Konfiguration und Verwendung dieses Datensammlers gelten die folgenden Voraussetzungen:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass zum Erstellen eines neuen REST-Benutzers/einer neuen REST-Rolle Administratorberechtigungen erforderlich sind.
 - Funktional stellt Data Infrastructure Insights in erster Linie Leseanforderungen, für die Registrierung von Data Infrastructure Insights beim ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich. Siehe den [Hinweis zu Berechtigungen](#) direkt unten.

- ONTAP Version 9.14.1 oder höher.
- Portanforderungen: 443
- Beachten Sie, dass Fpolicy-Metriken im ONTAP REST-Collector nicht unterstützt werden (Workload Security-Datenkollektoren verwenden FPolicy-Server und FPolicy-Metriken ermöglichen Ihnen die Überwachung der Workload Security-Datenerfassungsaktivität). Um Fpolicy-Metriken zu unterstützen, verwenden Sie die ["ONTAP Datenmanagement"](#) Kollektor.

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP -Dashboards von Data Infrastructure Insights auf erweiterten ONTAP Zählern basieren, sollten Sie im Abschnitt „Erweiterte Konfiguration“ des Datensammlers die Option „Erweiterte Zählerdatenerfassung aktivieren“ aktiviert lassen.

Um ein lokales Konto für Data Infrastructure Insights auf Clusterebene zu erstellen, melden Sie sich bei ONTAP mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators 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 *Befehle auf Diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des virtuellen Servers 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}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Nachdem Sie den Befehl „Erstellen“ ausgeführt haben, werden Sie aufgefordert, ein Kennwort für diesen Benutzer einzugeben. Beachten Sie, dass wir im folgenden Befehl die auf *ci_readonly* eingestellte Rolle anzeigen. Wenn Sie in Schritt 3 oben eine Rolle mit einem anderen Namen erstellen, verwenden Sie stattdessen diesen benutzerdefinierten Rollennamen.

```
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Wenn ein AD/LDAP-Konto verwendet wird, sollte der Befehl
```

```
security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

Die resultierende Rolle und Benutzeranmeldung werden etwa wie folgt aussehen. Ihre tatsächliche Ausgabe kann abweichen:

```
security login rest-role show -vserver <vserver name> -role restRole
```

Vserver	Role Name	API	Access 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>

User/Group	Authentication	Authentication	Acct	Second
Name	Application	Method	Role Name	Locked Method
restUser	http	password	restRole	no none

Sie können bei Bedarf den SPI-Zugriff überprüfen:

```
**Vserver:> vserver services web access show -name spi
```

Vserver	Type	Service Name	Role
<vserver name >	admin	spi	admin
<vserver name >	admin	spi	csrestrole

2 entries were displayed.**

Migration

Um von einem früheren ONTAP Datensammler (ontapi) zum neueren ONTAP REST-Sammler zu migrieren, gehen Sie wie folgt vor:

1. Fügen Sie den REST-Collector hinzu. Es wird empfohlen, die Informationen für einen anderen Benutzer einzugeben als den, der für den vorherigen Collector konfiguriert wurde. Verwenden Sie beispielsweise den im Abschnitt „Berechtigungen“ oben angegebenen Benutzer.

2. Halten Sie den vorherigen Collector an, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector mindestens 30 Minuten lang Daten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ erscheinen.
4. Nach der Ruhephase sollten sich Ihre Daten stabilisieren, da der REST-Collector weiterhin Daten erfasst.

Mit demselben Verfahren können Sie bei Bedarf zum vorherigen Collector zurückkehren.

Konfiguration

Feld	Beschreibung
ONTAP -Verwaltungs-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des NetApp Clusters. Muss eine Cluster-Verwaltungs-IP/ein FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Passwort	Passwort für NetApp -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zählerdatenerfassung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
EMS-Ereigniserfassung aktivieren	Wählen Sie diese Option aus, um ONTAP EMS-Protokollereignisdaten einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (Sek.)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Leistungsdaten vom ONTAP Datensammler. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Cluster	Storage
Node	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Volumen	Internes Volumen
Virtuelle Speichermaschine/VServer	Virtuelle Speichermaschine

ONTAP Datenmanagement-Terminologie

Die folgenden Bedingungen gelten für Objekte oder Verweise, die Sie möglicherweise auf den Zielseiten der ONTAP Data Management-Speicherressourcen finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- **Modell** – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Knotenmodellnamen innerhalb dieses Clusters. Wenn alle Knoten in den Clustern vom gleichen Modelltyp sind, wird nur ein Modellname angezeigt.
- **Anbieter** – derselbe Anbieternamen, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- **Seriennummer** – Die Array-UUID
- **IP** – im Allgemeinen handelt es sich dabei um die in der Datenquelle konfigurierten IPs oder Hostnamen.
- **Mikrocode-Version** – Firmware.
- **Rohkapazität** – Summe aller physischen Festplatten im System zur Basis 2, unabhängig von ihrer Rolle.
- **Latenz** – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumes abgeleitet wird.
- **Durchsatz** – aggregiert aus internen Volumes. Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung erstellt.

Speicherpool

- **Speicher** – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- **Typ** – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ verwendet.
- **Knoten** – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- **Verwendet Flash-Pool** – Ja/Nein-Wert – verfügt dieser SATA/SAS-basierte Pool über SSDs, die zur Caching-Beschleunigung verwendet werden?
- **Redundanz** – RAID-Level oder Schutzschema. RAID_DP ist doppelte Parität, RAID_TP ist dreifache Parität.
- **Kapazität** – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz.
- **Überbelegte Kapazität** – Wenn Sie durch den Einsatz von Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- **Snapshot** – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil

ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist. Bei ONTAP in MetroCluster -Konfigurationen ist dies wahrscheinlich, bei anderen ONTAP Konfigurationen ist dies weniger der Fall.

- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus können Replikationsimplementierungen vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als internes Volume oder Volume-Workload angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Speicherknotten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch.
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt.
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array fehlerfrei genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell – Modellname des Knotens.
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens.
- Speicher – Basis-2-Speicher, falls verfügbar.
- Auslastung – Bei ONTAP ist dies ein Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Leistungsabfrage wird eine Zahl zwischen 0 und 100 % gemeldet, die entweder der höheren WAFL Festplattenkonflikt- oder der durchschnittlichen CPU-Auslastung entspricht. Wenn Sie anhaltende Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Knoten nicht groß genug oder es sind nicht genügend rotierende Festplatten vorhanden, um die Schreibarbeitslast aufzunehmen.
- IOPS – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Latenz – Wird direkt aus ONTAP REST-Aufrufen des Knotenobjekts abgeleitet.
- Durchsatz – Direkt abgeleitet von ONTAP REST-Aufrufen des Knotenobjekts.
- Prozessoren – CPU-Anzahl.

ONTAP Leistungsmetriken

Mehrere ONTAP -Modelle bieten Leistungsmetriken für Data Infrastructure Insights , die zur Überwachung oder für Warnmeldungen verwendet werden können. Die unten stehenden Listen unterstützter und nicht unterstützter Modelle sind nicht vollständig, sollen aber als Orientierung dienen. Im Allgemeinen gilt: Wenn ein Modell zur selben Familie gehört wie eines auf der Liste, sollte auch die Unterstützung dieselbe 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/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Beim Versuch, einen ONTAP REST-Datensammler zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest-API unter 10.193.70.14 ist nicht verfügbar: 10.193.70.14 konnte /api/cluster nicht abrufen: 400 Ungültige Anforderung	Dies liegt wahrscheinlich an einem älteren ONTAP Array (z. B. ONTAP 9.6), das über keine REST-API-Funktionen verfügt. ONTAP 9.14.1 ist die minimale ONTAP Version, die vom ONTAP REST Collector unterstützt wird. Bei Versionen vor REST ONTAP sind Antworten vom Typ „400 Bad Request“ zu erwarten. Bei ONTAP Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, wird möglicherweise die folgende ähnliche Meldung angezeigt: Konfiguration: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest-API unter 10.193.98.84 ist verfügbar: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7, hat aber nicht mindestens die Version 9.14.1.
Ich sehe leere oder „0“-Metriken, wo der ONTAP ontapi-Collector Daten anzeigt.	ONTAP REST meldet keine Metriken, die nur intern auf dem ONTAP -System verwendet werden. Beispielsweise werden von ONTAP REST keine Systemaggregate erfasst, sondern nur SVMs vom Typ „Daten“. Weitere Beispiele für ONTAP REST-Metriken, die möglicherweise Null- oder leere Daten melden: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Speicher: Die meisten Metriken sind eine Zusammenfassung der Metriken des internen Volumes und werden von den oben genannten Faktoren beeinflusst. Speicher-Virtual Machines: REST meldet keine SVMs mehr vom Typ „Daten“ (z. B. „Cluster“, „MGM“, „Knoten“). Möglicherweise stellen Sie auch eine Änderung im Erscheinungsbild von Diagrammen fest, die Daten enthalten. Grund hierfür ist die Änderung des Standardabfragezeitraums für die Leistung von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Aufzeichnen.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp Data ONTAP im 7-Mode-Datenkollektor

Für Speichersysteme mit Data ONTAP -Software im 7-Mode verwenden Sie den 7-Mode-Datenkollektor, der die CLI zum Abrufen von Kapazitäts- und Leistungsdaten nutzt.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp 7-Mode-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers

die folgende Terminologie:



Dieser Datensammler ist "veraltet" .

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Raid-Gruppe	Datenträgergruppe
Filer	Storage
Filer	Speicherknoten
Aggregat	Speicherpool
LUN	Volumen
Volumen	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers benötigen Sie Folgendes:

- IP-Adressen des FAS Speichercontrollers und -Partners.
- Port 443
- Ein benutzerdefinierter Benutzername und ein Passwort auf Administratorebene für Controller und Partner-Controller mit den folgenden Rollenfunktionen für 7-Mode:
 - „api-*“: Verwenden Sie dies, um OnCommand Insight die Ausführung aller NetApp Speicher-API-Befehle zu ermöglichen.
 - „login-http-admin“: Verwenden Sie dies, um OnCommand Insight die Verbindung zum NetApp -Speicher über HTTP zu ermöglichen.
 - „security-api-vfiler“: Verwenden Sie dies, um OnCommand Insight die Ausführung von NetApp -Speicher-API-Befehlen zum Abrufen von vFiler-Einheiteninformationen zu ermöglichen.
 - „cli-options“: Verwenden Sie dies, um Speichersystemoptionen zu lesen.
 - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online-/Offline-Status und Freigabestatus) der angegebenen LUN oder LUN-Klasse an.
 - „cli-df“: Verwenden Sie dies, um den freien Speicherplatz anzuzeigen.
 - „cli-ifconfig“: Verwenden Sie dies, um Schnittstellen und IP-Adressen anzuzeigen.

Konfiguration

Feld	Beschreibung
Adresse des Speichersystems	IP-Adresse oder vollqualifizierter Domänenname für das NetApp -Speichersystem
Benutzername	Benutzername für das NetApp -Speichersystem
Passwort	Passwort für das NetApp -Speichersystem

Feld	Beschreibung
Adresse des HA-Partners im Cluster	IP-Adresse oder vollqualifizierter Domänenname für den HA-Partner
Benutzername des HA-Partners im Cluster	Benutzername für den HA-Partner
Kennwort des HA-Partner-Filers im Cluster	Passwort für den HA-Partner

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 20 Minuten.
Verbindungstyp	HTTPS oder HTTP, zeigt auch den Standardport an
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Speichersystemanbindung

Alternativ zur Verwendung des standardmäßigen Administratorbenutzers für diesen Datensammler können Sie einen Benutzer mit Administratorrechten direkt auf den NetApp -Speichersystemen konfigurieren, sodass dieser Datensammler Daten von NetApp -Speichersystemen abrufen kann.

Für die Verbindung mit NetApp -Speichersystemen muss der Benutzer, der beim Erwerb des Haupt-Pfilers (auf dem sich das Speichersystem befindet) angegeben wird, die folgenden Bedingungen erfüllen:

- Der Benutzer muss sich auf vfiler0 (Root-Filer/Pfiler) befinden.

Speichersysteme werden beim Erwerb des Haupt-Pfilers erworben.

- Die folgenden Befehle definieren die Funktionen der Benutzerrolle:
 - „api-*“: Verwenden Sie dies, um Data Infrastructure Insights die Ausführung aller NetApp -Speicher-API-Befehle zu ermöglichen.

Dieser Befehl ist zur Verwendung der ZAPI erforderlich.

- „login-http-admin“: Verwenden Sie dies, um Data Infrastructure Insights die Verbindung zum NetApp -Speicher über HTTP zu ermöglichen. Dieser Befehl ist zur Verwendung der ZAPI erforderlich.
- „security-api-vfiler“: Verwenden Sie dies, um Data Infrastructure Insights die Ausführung von NetApp -Speicher-API-Befehlen zum Abrufen von vFiler-Einheiteninformationen zu ermöglichen.
- „cli-options“: Für den Befehl „Optionen“ und wird für Partner-IP und aktivierte Lizenzen verwendet.
- „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online-/Offline-Status und Freigabestatus) der angegebenen LUN oder LUN-Klasse an.
- „cli-df“: Für die Befehle „df -s“, „df -r“, „df -A -r“ und wird zum Anzeigen des freien Speicherplatzes verwendet.
- „cli-ifconfig“: Für den Befehl „ifconfig -a“ und zum Abrufen der Filer-IP-Adresse.

- „cli-rdfile“: Für den Befehl „rdfile /etc/netgroup“ und zum Abrufen von Netzgruppen verwendet.
- „cli-date“: Für den Befehl „date“ und wird verwendet, um das vollständige Datum zum Abrufen von Snapshot-Kopien zu erhalten.
- „cli-snap“: Für den Befehl „Snap List“ und zum Abrufen von Snapshot-Kopien.

Wenn keine CLI-Date- oder CLI-Snap-Berechtigungen bereitgestellt werden, kann die Erfassung abgeschlossen werden, es werden jedoch keine Snapshot-Kopien gemeldet.

Um eine 7-Mode-Datenquelle erfolgreich zu erwerben und keine Warnungen auf dem Speichersystem zu generieren, sollten Sie eine der folgenden Befehlszeichenfolgen verwenden, um Ihre Benutzerrollen zu definieren. Die zweite hier aufgeführte Zeichenfolge ist eine optimierte Version der ersten:

- Login-http-admin, API-*, Sicherheits-API-vfile, CLI-rdfile, CLI-Optionen, CLI-df, CLI-lun, CLI-ifconfig, CLI-date, CLI-snap, _
- login-http-admin,api-* ,security-api-vfile,cli-

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Erhalten Sie die HTTP-Antwort 401 oder den ZAPI-Fehlercode 13003 und ZAPI gibt „Unzureichende Berechtigungen“ oder „Nicht für diesen Befehl autorisiert“ zurück.	Überprüfen Sie Benutzernamen und Passwort sowie Benutzerrechte/Berechtigungen.
Fehler „Befehl konnte nicht ausgeführt werden“	Überprüfen Sie, ob der Benutzer über die folgenden Berechtigungen auf dem Gerät verfügt: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Überprüfen Sie außerdem, ob die ONTAP Version von Data Infrastructure Insights unterstützt wird, und stellen Sie sicher, dass die verwendeten Anmeldeinformationen mit den Anmeldeinformationen des Geräts übereinstimmen.
Clusterversion ist < 8.1	Die minimal unterstützte Clusterversion ist 8.1. Aktualisieren Sie auf die minimal unterstützte Version.
ZAPI gibt „Clusterrolle ist nicht cluster_mgmt LIF“ zurück.	AU muss mit der Cluster-Management-IP kommunizieren. Überprüfen Sie die IP und wechseln Sie gegebenenfalls zu einer anderen IP
Fehler: „7-Modus-Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diesen Datensammler verwenden, um 7-Modus-Filer zu ermitteln. Ändern Sie die IP, sodass sie stattdessen auf den CDOT-Filer verweist.

Problem:	Versuchen Sie Folgendes:
ZAPI-Befehl schlägt nach erneutem Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
AU konnte keine Verbindung zu ZAPI herstellen	Überprüfen Sie die IP-/Port-Konnektivität und bestätigen Sie die ZAPI-Konfiguration.
AU konnte keine Verbindung zu ZAPI über HTTP herstellen	Überprüfen 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: Die ZAPI-Antwort hat den Fehlercode 13001, „Datenbank ist nicht geöffnet“. Der ZAPI-Fehlercode ist 60 und die Antwort enthält „API wurde nicht rechtzeitig beendet“. Die ZAPI-Antwort enthält „initialize_session() hat eine NULL-Umgebung zurückgegeben“. Der ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht fehlerfrei“.	Überprüfen Sie Netzwerk, Portnummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl über die Befehlszeile der AU-Maschine auszuführen.
Socket-Timeout-Fehler mit ZAPI	Überprüfen Sie die Filer-Konnektivität und/oder erhöhen Sie das Timeout.
Fehler „C-Modus-Cluster werden von der 7-Modus-Datenquelle nicht unterstützt“	Überprüfen Sie die IP und ändern Sie die IP in einen 7-Modus-Cluster.
Fehler „Verbindung zum vFiler fehlgeschlagen“	Überprüfen Sie, ob die Berechtigungen des abrufenden Benutzers mindestens Folgendes umfassen: api-* security-api-vfiler login-http-admin. Bestätigen Sie, dass auf dem Filer mindestens ONTAPI Version 1.7 ausgeführt wird.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp E-Series Legacy Santricity API-Datenkollektor

Der NetApp E-Series Legacy Santricity API-Datensammler sammelt Inventar- und Leistungsdaten. Der Collector unterstützt Firmware 7.x+ mit denselben Konfigurationen und meldet dieselben Daten.

Terminologie

Cloud Insight erhält die folgenden Bestandsinformationen vom NetApp E-Series-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumengruppe	Datenträgergruppe
Speicher-Array	Storage
Regler	Speicherknoten
Volumengruppe	Speicherpool
Volumen	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

E-Series-Terminologie (Landingpage)

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der NetApp E-Series-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbieternamen, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer – Die Seriennummer des Arrays. Bei Speichersystemen mit Clusterarchitektur wie NetApp Clustered Data Ontap ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- IP – im Allgemeinen die IP(s) oder Hostnamen, wie sie in der Datenquelle konfiguriert sind
- Mikrocode-Version – Firmware
- Rohkapazität – Basis-2-Summierung aller physischen Festplatten im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen Volumes abgeleitet wird.
- Durchsatz – der gesamte Host-Durchsatz des Arrays. Idealerweise direkt aus dem Array bezogen, falls nicht verfügbar, summiert Data Infrastructure Insights den Durchsatz der Volumes, um diesen Wert abzuleiten
- Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights -Datenquelle als Teil der Bestandsberichterstattung erstellt

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten werden „Thin Provisioning“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.

- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz – RAID-Level oder Schutzschema. E-Serie meldet „RAID 7“ für DDP-Pools
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz. Diese Werte beinhalten beide die „Erhaltungskapazität“ der E-Serie, was dazu führt, dass sowohl die Zahlen als auch der Prozentsatz höher sind als das, was die Benutzeroberfläche der E-Serie möglicherweise anzeigt
- Überbelegte Kapazität – Wenn Sie über Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamte Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus kann die Replikationsimplementierung vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als Volume-Arbeitslast angezeigt wird.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform keine Festplatten-IOPS verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPS für alle Volumes in diesem Speicherpool ermittelt.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform kein Festplattendurchsatz verfügbar ist, wird dieser Wert aus der Summe der Datenträger aller Datenträger in diesem Speicherpool ermittelt.

Speicherknotten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt
- Status – Integrität des Knotens. Nur verfügbar, wenn das Array gesund genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell – Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens
- Speicher – Basis-2-Speicher, falls verfügbar
- Auslastung – Im Allgemeinen eine CPU-Auslastungszahl oder im Fall von NetApp Ontap ein Controller-Stressindex. Die Nutzung ist derzeit für die NetApp E-Serie nicht verfügbar
- IOPS – eine Zahl, die die hostgesteuerten IOPS auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch Summieren aller IOPS für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Reaktionszeit auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch eine IOP-gewichtete Berechnung aus Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Durchsatz – eine Zahl, die den hostgesteuerten Durchsatz auf diesem Controller darstellt. Idealerweise wird der Datendurchsatz direkt aus dem Array bezogen. Falls er nicht verfügbar ist, wird er durch Summieren des gesamten Durchsatzes für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.

gehören.

- Prozessoren – CPU-Anzahl

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Portanforderung 2463

Konfiguration

Feld	Beschreibung
Durch Kommas getrennte Liste der Array SANtricity Controller-IPs	IP-Adressen und/oder vollqualifizierte Domännennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 30 Minuten
Leistungsabfrageintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

NetApp E-Series REST-Datenkollektor

Der REST-Datensammler der NetApp E-Serie sammelt Inventar-, Protokoll- und Leistungsdaten. Der Collector unterstützt Firmware 7.x+ mit denselben Konfigurationen und meldet dieselben Daten. Der REST-Collector überwacht den Verschlüsselungsstatus von Speicherpools, Festplatten und Volumes, die CPU-Auslastung des Speicherknotens sowie Protokollfunktionen, die im älteren SANtricity E-Series-Collector nicht bereitgestellt werden.

Terminologie

Data Infrastructure Insights erfasst mithilfe von REST die folgenden Bestandsinformationen von der NetApp E-Serie. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Scheibe
Volumengruppe	Datenträgergruppe
Speicher-Array	Storage
Regler	Speicherknoten

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Volumengruppe	Speicherpool
Volumen	Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezugeordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Dieser Collector unterstützt nur E-Series-Modell-Arrays mit **nativen REST-API-Funktionen**. Die E-Series-Organisation liefert eine außerhalb des Arrays installierbare REST-API-Distribution für ältere E-Series-Arrays: Dieser Collector unterstützt dieses Szenario nicht. Benutzer mit älteren Arrays sollten weiterhin Data Infrastructure Insights verwenden. "[E-Serie SANtricity API](#)" Kollektor.
- Das Feld „IP-Adressen des E-Series-Controllers“ unterstützt eine durch Kommas getrennte Zeichenfolge mit zwei IP-/Hostnamen. Der Collector versucht automatisch, den zweiten IP-/Hostnamen zu verwenden, wenn auf den ersten nicht zugegriffen werden kann.
- HTTPS-Port: Standard ist 8443.

Konfiguration

Feld	Beschreibung
IP-Adressen der E-Serie-Controller	Komma-getrennte IP-Adressen und/oder vollqualifizierte Domännennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 30 Minuten
Leistungsabfrageintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

E-Series-Terminologie (Landingpage)

Die folgenden Bedingungen gelten für Objekte oder Referenzen, die Sie möglicherweise auf den Zielseiten der NetApp E-Series-Assets finden. Viele dieser Begriffe gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbieternamen, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer – Die Seriennummer des Arrays. Bei Speichersystemen mit Clusterarchitektur wie NetApp Clustered Data Ontap ist diese Seriennummer möglicherweise weniger nützlich als die Seriennummern der einzelnen „Storage Nodes“.
- IP – im Allgemeinen die IP(s) oder Hostnamen, wie sie in der Datenquelle konfiguriert sind
- Mikrocode-Version – Firmware

- Rohkapazität – Basis-2-Summierung aller physischen Festplatten im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Arbeitslasten, die der Host sowohl beim Lesen als auch beim Schreiben erfährt. Im Idealfall bezieht Data Infrastructure Insights diesen Wert direkt, dies ist jedoch häufig nicht der Fall. Anstelle des Arrays, das dies anbietet, führt Data Infrastructure Insights im Allgemeinen eine IOP-gewichtete Berechnung durch, die aus den Statistiken der einzelnen Volumes abgeleitet wird.
- Durchsatz – der gesamte Host-Durchsatz des Arrays. Idealerweise direkt aus dem Array bezogen, falls nicht verfügbar, summiert Data Infrastructure Insights den Durchsatz der Volumes, um diesen Wert abzuleiten
- Verwaltung – dies kann einen Hyperlink zur Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert von der Data Infrastructure Insights -Datenquelle als Teil der Bestandsberichterstattung erstellt

Speicherpool

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibender Wert aus einer Liste mit aufgezählten Möglichkeiten. Am häufigsten werden „Thin Provisioning“ oder „RAID-Gruppe“ verwendet.
- Knoten – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Zielseite angezeigt.
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz – RAID-Level oder Schutzschema. E-Serie meldet „RAID 7“ für DDP-Pools
- Kapazität – die Werte hier sind die logisch genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der davon genutzte Prozentsatz. Diese Werte beinhalten beide die „Erhaltungskapazität“ der E-Serie, was dazu führt, dass sowohl die Zahlen als auch der Prozentsatz höher sind als das, was die Benutzeroberfläche der E-Serie möglicherweise anzeigt
- Überbelegte Kapazität – Wenn Sie über Effizienztechnologien eine Gesamtsumme an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, ist der Prozentwert hier größer als 0 %.
- Snapshot – verwendete und gesamt Snapshot-Kapazitäten, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität Segmentbereichen ausschließlich für Snapshots zuweist
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung aller Festplatten anzeigt, die Kapazität zu diesem Speicherpool beitragen. Die Festplattenauslastung weist nicht unbedingt eine starke Korrelation mit der Array-Leistung auf. Die Auslastung kann aufgrund von Festplattenneuaufbauten, Deduplizierungsaktivitäten usw. hoch sein, wenn keine vom Host gesteuerten Workloads vorliegen. Darüber hinaus kann die Replikationsimplementierung vieler Arrays die Festplattenauslastung erhöhen, ohne dass dies als Volume-Arbeitslast angezeigt wird.
- IOPS – die Summe der IOPs aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform keine Festplatten-IOPs verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPs für alle Volumes in diesem Speicherpool ermittelt.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn auf einer bestimmten Plattform kein Festplattendurchsatz verfügbar ist, wird dieser Wert aus der Summe der Datenträger aller Datenträger in diesem Speicherpool ermittelt.

Speicherknoten

- Speicher – zu welchem Speicherarray dieser Knoten gehört. Obligatorisch
- HA-Partner – auf Plattformen, auf denen ein Knoten auf einen und nur einen anderen Knoten umgeschaltet wird, wird er im Allgemeinen hier angezeigt

- Status – Integrität des Knotens. Nur verfügbar, wenn das Array gesund genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell – Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer – Die Seriennummer des Knotens
- Speicher – Basis-2-Speicher, falls verfügbar
- Auslastung – Im Allgemeinen eine CPU-Auslastungszahl oder im Fall von NetApp Ontap ein Controller-Stressindex. Die Nutzung ist derzeit für die NetApp E-Serie nicht verfügbar
- IOPS – eine Zahl, die die hostgesteuerten IOPs auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch Summieren aller IOPs für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Reaktionszeit auf diesem Controller darstellt. Idealerweise wird die Quelle direkt aus dem Array bezogen. Wenn sie nicht verfügbar ist, wird sie durch eine IOP-gewichtete Berechnung aus Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Durchsatz – eine Zahl, die den hostgesteuerten Durchsatz auf diesem Controller darstellt. Idealerweise wird der Datendurchsatz direkt aus dem Array bezogen. Falls er nicht verfügbar ist, wird er durch Summieren des gesamten Durchsatzes für Volumes berechnet, die ausschließlich zu diesem Knoten gehören.
- Prozessoren – CPU-Anzahl

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des NetApp HCI Management-Server-Datenkollektors

Der Datensammler des NetApp HCI Management-Servers sammelt NetApp HCI Hostinformationen und erfordert schreibgeschützte Berechtigungen für alle Objekte innerhalb des Management-Servers.

Dieser Datensammler ruft Daten nur vom * NetApp HCI Management-Server* ab. Um Daten aus dem Speichersystem zu sammeln, müssen Sie außerdem die ["NetApp SolidFire"](#) Datensammler.

Terminologie

Data Infrastructure Insights erhält von diesem Datensammler die folgenden Bestandsinformationen. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Scheibe
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Datenspeicher	Datenspeicher

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
LUN	Volumen
Fibre-Channel-Anschluss	Hafen

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse des NetApp HCI Management-Servers
- Nur-Lese-Benutzername und -Passwort für den NetApp HCI Management-Server
- Nur Leseberechtigungen für alle Objekte im NetApp HCI Management-Server.
- SDK-Zugriff auf den NetApp HCI Management-Server – normalerweise bereits eingerichtet.
- Portanforderungen: http-80 https-443
- Zugriff validieren:
 - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim NetApp HCI Management-Server an
 - Überprüfen Sie, ob das SDK aktiviert ist: Telnet <vc_ip> 443

Einrichtung und Anschluss

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
NetApp HCI Storage Cluster MVIP	Virtuelle Verwaltungs-IP-Adresse
SolidFire -Verwaltungsknoten (mNode)	IP-Adresse des Verwaltungsknotens
Benutzername	Benutzername für den Zugriff auf den NetApp HCI Management-Server
Passwort	Kennwort für den Zugriff auf den NetApp HCI -Verwaltungsserver
VCenter-Benutzername	Benutzername für VCenter
VCenter-Passwort	Kennwort für VCenter

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm „Erweiterte Konfiguration“ das Kontrollkästchen **VM-Leistung**, um Leistungsdaten zu erfassen. Die Inventarerfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 20
Filtern Sie VMs nach	Wählen Sie CLUSTER, DATACENTER oder ESX HOST
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Angaben, ob VMs ein- oder ausgeschlossen werden sollen
Geräteliste filtern	Liste der zu filternden VMs (durch Komma getrennt oder durch Semikolon getrennt, wenn im Wert ein Komma verwendet wird) zum Filtern nur nach ESX_HOST, CLUSTER und DATACENTER
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
Fehler: Die Einschlussliste zum Filtern von VMs darf nicht leer sein	Wenn „Liste einschließen“ ausgewählt ist, listen Sie bitte gültige DataCenter-, Cluster- oder Hostnamen auf, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter unter IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den Infrastructure Client mit Virtual Center zu kommunizieren. * Versuchen Sie, über den Managed Object Browser (z. B. MOB) mit Virtual Center zu kommunizieren.
Fehler: VirtualCenter bei IP verfügt über ein nicht konformes Zertifikat, das JVM benötigt	Mögliche Lösungen: * Empfohlen: Generieren Sie das Zertifikat für Virtual Center neu, indem Sie einen stärkeren (z. B. 1024-Bit) RSA-Schlüssel verwenden. * Nicht empfohlen: Ändern Sie die JVM-Konfiguration <code>java.security</code> , um die Einschränkung <code>jdk.certpath.disabledAlgorithms</code> zu nutzen und einen 512-Bit-RSA-Schlüssel zuzulassen. Siehe Versionshinweise zu JDK 7 Update 40 unter " http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html "

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

NetApp SolidFire All-Flash Array-Datenkollektor

Der NetApp SolidFire All-Flash Array-Datenkollektor unterstützt die Bestandsaufnahme und Leistungserfassung von iSCSI- und Fibre Channel SolidFire Konfigurationen.

Der SolidFire Datensammler verwendet die SolidFire REST-API. Die Erfassungseinheit, auf der sich der Datensammler befindet, muss in der Lage sein, HTTPS-Verbindungen zum TCP-Port 443 der SolidFire -Clusterverwaltungs-IP-Adresse herzustellen. Der Datensammler benötigt Anmeldeinformationen, die REST-API-Abfragen im SolidFire Cluster durchführen können.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp SolidFire All-Flash Array-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Fahren	Scheibe
Cluster	Storage
Node	Speicherknoten
Volumen	Volumen
Fibre-Channel-Anschluss	Hafen
Volume-Zugriffsgruppe, LUN-Zuweisung	Volumenkarte
iSCSI-Sitzung	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuzuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Für die Konfiguration dieses Datensammlers gelten die folgenden Voraussetzungen:

- Virtuelle Verwaltungs-IP-Adresse
- Benutzername und Anmeldeinformationen sind schreibgeschützt
- Port 443

Konfiguration

Feld	Beschreibung
Virtuelle Verwaltungs-IP-Adresse (MVIP)	Virtuelle IP-Adresse des SolidFire -Clusters verwalten
Benutzername	Name, der für die Anmeldung beim SolidFire -Cluster verwendet wird
Passwort	Kennwort zum Anmelden beim SolidFire -Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Verbindungstyp auswählen
Kommunikationsanschluss	Für die NetApp API verwendeter Port

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 20 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Wenn SolidFire einen Fehler meldet, wird dieser in Data Infrastructure Insights wie folgt angezeigt:

Beim Versuch, Daten abzurufen, wurde eine Fehlermeldung von einem SolidFire -Gerät empfangen. Der Aufruf war <Methode> (<ParameterString>). Die Fehlermeldung des Geräts lautete (siehe Gerätehandbuch): <message>

Wo:

- Die <Methode> ist eine HTTP-Methode, beispielsweise GET oder PUT.
- Der <parameterString> ist eine durch Kommas getrennte Liste von Parametern, die im REST-Aufruf enthalten waren.
- Die <message> ist die vom Gerät zurückgegebene Fehlermeldung.

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#).

NetApp StorageGRID Datenkollektor

Der NetApp StorageGRID Datenkollektor unterstützt die Bestands- und Leistungserfassung von StorageGRID Konfigurationen.



Um eine konsistente Messung der DII-Berechtigungen über alle StorageGRID -Systeme hinweg unabhängig von der zugrunde liegenden Hardwaretopologie und -konfiguration zu gewährleisten, verwendet Data Infrastructure Insights die gesamte verfügbare Kapazität (storagegrid_storage_utilization_total_space_bytes) anstelle der RAW-Kapazität basierend auf dem physischen Festplattenlayout.

Für Kunden, die das kapazitätsbasierte Lizenzmodell verwenden, wird StorageGRID als „Objekt“-Speicher gemessen.

Für Kunden, die das alte (MU) Lizenzmodell verwenden, wird StorageGRID als Sekundärspeicher mit einem Satz von 40 TiB zu 1 MU gemessen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom NetApp StorageGRID Collector. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für diesen Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
StorageGRID	Storage
Node	Node

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Mieter	Speicherpool
Eimer	Internes Volumen

Anforderungen

Für die Konfiguration dieser Datenquelle gelten die folgenden Voraussetzungen:

- StorageGRID Host-IP-Adresse
- Ein Benutzername und ein Kennwort für einen Benutzer, dem die Rollen „Metrikabfrage“ und „Mandantenzugriff“ zugewiesen wurden
- Port 443

Konfiguration

Feld	Beschreibung
StorageGRID Host-IP-Adresse	Verwaltung Virtuelle IP-Adresse des StorageGRID -Geräts
Benutzername	Name, der für die Anmeldung beim StorageGRID -Gerät verwendet wird
Passwort	Kennwort zum Anmelden bei der StorageGRID -Appliance

Erweiterte Konfiguration

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 60 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 900 Sekunden

Einmaliges Anmelden (SSO)

Der **"StorageGRID"** Firmware-Versionen haben entsprechende API-Versionen; 3.0 API und neuere Versionen unterstützen die Single Sign-On-Anmeldung (SSO).

Firmware-Version	API-Version	Unterstützt Single Sign-On (SSO)
11,1	2	Nein
11,2	3,0	Ja
11,5	3,3	Ja

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im **"Support"** Seite oder in der **"Datensammler-Supportmatrix"** .

Nutanix NX-Datensammler

Data Infrastructure Insights verwendet den Nutanix-Datensammler, um Bestands- und Leistungsdaten für Nutanix NX-Speichersysteme zu ermitteln.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Nutanix-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Speicherpool	Speicherpool
Nutanix-Container	Internes Volumen
Nutanix-Container	Dateifreigabe
NFS-Freigabe	Aktie

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- Die IP-Adresse der externen Datendienste für den Cluster
- Nur-Lese-Benutzername und -Passwort, es sei denn, es werden Volume-Gruppen verwendet. In diesem Fall sind der Administrator-Benutzername und das Administrator-Passwort erforderlich.
- Portanforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
Externe Prism-IP-Adresse	Die IP-Adresse der externen Datendienste für den Cluster
Benutzername	Benutzername für das Admin-Konto
Passwort	Passwort für das Admin-Konto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem Nutanix-Array verwendet wird. Der Standardwert ist 9440.
Inventarabfrageintervall (min)	Intervall zwischen den Bestandsabfragen. Der Standardwert beträgt 60 Minuten.
Leistungsabfrageintervall (Sek.)	Intervall zwischen Leistungsabfragen. Der Standardwert beträgt 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Oracle ZFS Storage Appliance-Datenkollektor

Data Infrastructure Insights verwendet den Oracle ZFS Storage Appliance-Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen mit dem Oracle ZFS-Datenkollektor. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Festplatte (SSD)	Scheibe
Cluster	Storage
Regler	Speicherknoten
LUN	Volumen
LUN-Karte	Volumenkarte
Initiator, Ziel	Volumenmaske
Aktie	Internes Volumen

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

- Hostnamen für den ZFS-Controller-1 und den ZFS-Controller-2
- Administrator-Benutzername und -Passwort
- Portanforderung: 215 HTTP/HTTPS

Erforderliche Leistungsmetriken

Oracle ZFS-Geräte bieten Speicheradministratoren große Flexibilität bei der Erfassung von Leistungsstatistiken. Data Infrastructure Insights erwartet, dass Sie *jeden* Controller in einem Hochverfügbarkeitspaar so konfigurieren, dass die folgenden Metriken erfasst werden:

- smb2.ops[teilen]
- nfs3.ops[teilen]
- nfs4.ops[teilen]
- nfs4-1.ops[teilen]

Wenn der Controller einige oder alle dieser Daten nicht erfasst, führt dies wahrscheinlich dazu, dass Data

Infrastructure Insights die Arbeitslast auf den „internen Volumes“ nicht erfasst oder zu niedrig angibt.

Konfiguration

Feld	Beschreibung
ZFS-Controller-1-Hostname	Hostname für Speichercontroller 1
ZFS-Controller-2-Hostname	Hostname für Speichercontroller 2
Benutzername	Benutzername für das Benutzerkonto des Speichersystemadministrators
Passwort	Kennwort für das Administrator-Benutzerkonto

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP, zeigt auch den Standardport an
Verbindungsport überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Inventarabfrageintervall	Der Standardwert beträgt 60 Sekunden
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldedaten“	ZFS-Benutzerkonto und Passwort validieren
„Anforderung fehlgeschlagen mit Status 404 https://...:215/api/access/v1“	Ihr ZFS-Array ist möglicherweise zu alt, um REST-API-Unterstützung zu bieten. AK 2013.1.3.0 war die erste REST-API-fähige ZFS-Betriebssystemversion und nicht alle ZFS-Geräte können darauf aktualisiert werden.
„Konfigurationsfehler“ mit Fehlermeldung „REST-Dienst ist deaktiviert“	Überprüfen Sie, ob der REST-Dienst auf diesem Gerät aktiviert ist.

Problem:	Versuchen Sie Folgendes:
„Konfigurationsfehler“ mit Fehlermeldung „Benutzer nicht autorisiert für Befehl“	<p>Dieser Fehler ist wahrscheinlich darauf zurückzuführen, dass bestimmte Rollen (z. B. „advanced_analytics“) für den konfigurierten Benutzer nicht enthalten sind.</p> <p>Durch Anwenden des Analytics-Bereichs für den Benutzer mit schreibgeschützter Rolle kann der Fehler möglicherweise behoben werden. Gehen Sie folgendermaßen vor:</p> <ol style="list-style-type: none"> 1. Bewegen Sie im ZFs-System im Bildschirm „Konfiguration → Benutzer“ die Maus über die Rolle und doppelklicken Sie, um die Bearbeitung zu ermöglichen 2. Wählen Sie „Analytics“ aus dem Dropdown-Menü „Bereich“ aus. Es erscheint eine Liste der möglichen Eigenschaften. 3. Klicken Sie auf das oberste Kontrollkästchen, 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 in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Pure Storage FlashArray-Datensammler

Data Infrastructure Insights verwendet den Pure Storage FlashArray-Datensammler, um Bestands- und Leistungsdaten zu erfassen.

Terminologie

Für jeden von Data Infrastructure Insights erfassten Asset-Typ wird die am häufigsten verwendete Terminologie für das Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Laufwerk (SSD)	Scheibe
Anordnung	Storage
Regler	Speicherknoten
Volumen	Volumen
LUN-Karte	Volumenkarte
Initiator, Ziel	Volumenmaske

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des Speichersystems
- Benutzername und Passwort für das Administratorkonto des Pure-Speichersystems.
- Portanforderung: HTTP/HTTPS 80/443

Konfiguration

Feld	Beschreibung
FlashArray-Host-IP-Adresse	IP-Adresse des Speichersystems
Benutzername	Benutzername mit Administratorrechten
Kennwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Anschlussart	Wählen Sie HTTP oder HTTPS. Zeigt auch den Standardport an.
TCP-Port überschreiben	Wenn das Feld „Verbindungstyp“ leer ist, verwenden Sie den Standardport. Andernfalls geben Sie den zu verwendenden Verbindungsport ein.
Inventarabfrageintervall (min)	Der Standardwert beträgt 60 Minuten
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Inventar

Problem:	Versuchen Sie Folgendes:
„Ungültige Anmeldeinformationen“ mit den Fehlermeldungen „Richtlinie lässt dies nicht zu“ oder „Sie sind nicht autorisiert“	Validieren Sie das Pure-Benutzerkonto und das Passwort über die Pure-HTTP-Schnittstelle

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Red Hat Virtualization-Datenkollektor

Data Infrastructure Insights verwendet den Red Hat Virtualization-Datensammler, um Inventardaten von virtualisierten Linux- und Microsoft Windows-Workloads zu sammeln.

Terminologie

Für jeden von Data Infrastructure Insights erfassten Asset-Typ wird die am häufigsten verwendete Terminologie für das Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Scheibe	Virtuelle Festplatte
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Speicherdomäne	Datenspeicher
Logische Einheit	LUN

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologieuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

- IP-Adresse des RHEV-Servers über Port 443 per REST-API
- Nur-Lese-Benutzername und -Passwort
- RHEV Version 3.0+

Konfiguration

Feld	Beschreibung
RHEV-Server-IP-Adresse	IP-Adresse des Speichersystems
Benutzername	Benutzername mit Administratorrechten
Kennwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Kommunikationsport	Für die HTTPS-Kommunikation mit RHEV verwendeter Port
Inventarabfrageintervall (min)	Der Standardwert beträgt 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie im ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Rubrik CDM-Datensammler

Data Infrastructure Insights verwendet den Rubrik-Datensammler, um Bestands- und Leistungsdaten von Rubrik-Speichergeräten zu erfassen.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom Rubrik-Datensammler. Für jeden von Data Infrastructure Insights erworbenen Asset-Typ wird die am häufigsten verwendete Terminologie für dieses Asset angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Cluster	Speicher, Speicherpool
Node	Speicherknoten
Scheibe	Scheibe

Hinweis: Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diese Datenquelle darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 zum Rubrik-Cluster. Ein Kollektor pro Cluster.
- IP-Adresse des Rubrik-Clusters.
- Benutzername und Passwort für den Cluster.
- IP-Adresse oder Hostname des Rubrik-Clusters.
- Für die Basisauthentifizierung ein Benutzername und ein Kennwort für den Cluster. Wenn Sie die Authentifizierung auf Basis eines Dienstkontos bevorzugen, benötigen Sie ein Dienstkonto, ein Geheimnis und eine Organisations-ID
- Portanforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
IP	IP-Adresse des Rubrik-Clusters
Benutzername / Dienstkonto	Benutzername für den Cluster
Passwort / Geheimnis	Kennwort für den Cluster
Organisations-ID für das Service-Konto	Dies muss die vollständige Zeichenfolge sein, z. B. „Organization:::nnnnnn-nnnn....“

Erweiterte Konfiguration

Inventarabfrageintervall (min)	Der Standardwert ist 60
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich habe eine Nachricht erhalten, dass mehr als ein Speicher erstellt wurde.	Überprüfen Sie, ob der Cluster richtig konfiguriert ist und der Collector auf einen einzelnen Cluster verweist.
Umfrage schlägt mit 400 [Ungültige Anfrage] fehl. ... Ungültige ManagedId....	Sie haben das Feld „Organisations-ID“ mit einem Wert ausgefüllt, aber der Rubrik-Cluster glaubt NICHT, dass es sich um eine gültige Organisations-ID handelt, obwohl die Fehlermeldung von Rubrik darauf als „ManagedId“ verweist.

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Konfigurieren des VMware vSphere-Datenkollektors

Der Datensammler für VMware vSphere sammelt Leistungs- und Konfigurationsinformationen von VM-Gästen und ESXi-Hosts und erfordert schreibgeschützte Berechtigungen für alle Objekte innerhalb von vSphere. Ab August 2024 bringt der vSphere-Collector zusätzlich Protokollnachrichten aus vSphere-Umgebungen und einige VMware-spezifische Metriken ein. Bitte beachten Sie, dass Data Infrastructure Insights nur VMware-Protokollinformationen aus Umgebungen mit vSphere 8.0.1 oder höher abrufen kann. Ebenso werden die anbieterspezifischen Metriken nur für vSphere 7+-Umgebungen unterstützt. Daher möchten Sie möglicherweise das Kontrollkästchen „Protokolle“ und/oder „Anbieterspezifische Metriken“ bei einem bestimmten Collector deaktivieren, wenn dieser auf eine ältere vSphere-Instanz verweist.

Terminologie

Data Infrastructure Insights erhält die folgenden Bestandsinformationen vom VMware vSphere-Datenkollektor. Für jeden erworbenen Vermögenswerttyp wird die am häufigsten verwendete Terminologie für den Vermögenswert angezeigt. Beachten Sie beim Anzeigen oder bei der Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter/Modellbegriff	Begriff „Data Infrastructure Insights“
Virtuelle Festplatte	Scheibe
Gastgeber	Gastgeber
Virtuelle Maschine	Virtuelle Maschine
Datenspeicher	Datenspeicher
LUN	Volumen
Fibre-Channel-Anschluss	Hafen

Hierbei handelt es sich lediglich um allgemeine Terminologiezuordnungen, die möglicherweise nicht jeden Fall für diesen Datensammler darstellen.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Angaben erforderlich:

- IP-Adresse des Virtual Center-Servers
- Benutzername und Kennwort im Virtual Center sind schreibgeschützt
- Wir benötigen nur Leseberechtigungen für alle Objekte im Virtual Center.
- SDK-Zugriff auf den Virtual Center-Server – normalerweise bereits eingerichtet.
- Portanforderungen: 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 Anschluss

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Erfassungseinheit	Name der Erfassungseinheit

Konfiguration

Feld	Beschreibung
IP-Adresse des virtuellen Zentrums	IP-Adresse des Virtual Centers
Benutzername	Benutzername für den Zugriff auf das Virtual Center
Passwort	Passwort für den Zugriff auf das Virtual Center

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm „Erweiterte Konfiguration“ das Kontrollkästchen **VM-Leistung**, um Leistungsdaten zu erfassen. Die Inventarerfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Inventarabfrageintervall (min)	Der Standardwert ist 20
Filtern von VMs	Wählen Sie CLUSTER, DATACENTER oder ESX HOST
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Erstellen Sie eine Filterliste (CLUSTER, DATACENTER und/oder ESX_HOST).
Anzahl der Wiederholungsversuche	Der Standardwert ist 3
Kommunikationsanschluss	Der Standardwert ist 443

Geräteliste filtern...	Diese Liste muss aus exakten Zeichenfolgenübereinstimmungen bestehen. Wenn Sie nach ESX_HOST filtern möchten, müssen Sie eine durch Kommas getrennte Liste der exakten „Namen“ Ihrer ESX-Hosts erstellen, wie sie sowohl in Data Infrastructure Insights als auch in vSphere gemeldet werden. Bei diesen „Namen“ kann es sich entweder um IP-Adressen, einfache Hostnamen oder vollqualifizierte Domännennamen (FQDNs) handeln. Dies wird dadurch bestimmt, wie diese Hosts benannt wurden, als sie ursprünglich zu vSphere hinzugefügt wurden. Verwenden Sie beim Filtern nach CLUSTER die Clusternamen im Data Infrastructure Insights-Stil, wie sie von CI auf Hypervisoren gemeldet werden – Data Infrastructure Insights stellt dem vSphere-Clusternamen den Namen des vSphere-Rechenzentrums und einen Schrägstrich voran – „DC1/clusterA“ ist der Clustername, den Data Infrastructure Insights auf einem Hypervisor in ClusterA innerhalb des Rechenzentrums DC1 melden würde.
Leistungsabfrageintervall (Sek.)	Der Standardwert ist 300

Zuordnen von VMware-Tags zu Data Infrastructure Insights -Anmerkungen

Mit dem VMware-Datensammler können Sie Data Infrastructure Insights -Anmerkungen mit auf VMware konfigurierten Tags füllen. Der DII-Annotationsname muss mit dem VMware-*Kategorie*namen identisch sein. Das Tag wird dann als Annotationswert einer DII-Annotation mit demselben Namen wie die Kategorie angewendet. Data Infrastructure Insights füllt immer gleichnamige Textanmerkungen aus und unternimmt den bestmöglichen Versuch, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) auszufüllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht ausfüllen kann, kann es erforderlich sein, die Anmerkung zu entfernen und als Texttyp neu zu erstellen.

Beachten Sie, dass bei VMware-Tags die Groß- und Kleinschreibung beachtet werden kann, bei Data Infrastructure Insights -Tags hingegen nicht. Wenn Sie also in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“ und in VMware Tags mit den Namen „OWNER“, „Owner“ und „owner“ erstellen, werden alle diese Variationen von „owner“ der Annotation „OWNER“ von Cloud Insight zugeordnet.

Beachten Sie Folgendes:

- Data Infrastructure Insights veröffentlicht derzeit nur automatisch Supportinformationen für NetApp -Geräte.
- Da diese Supportinformationen in Form von Anmerkungen vorliegen, können Sie sie abfragen oder in Dashboards verwenden.
- Wenn ein Benutzer den Annotationswert überschreibt oder leert, wird der Wert automatisch erneut ausgefüllt, wenn Data Infrastructure Insights die Annotationen aktualisiert, was einmal täglich geschieht.

Fehlerbehebung

Wenn bei diesem Datensammler Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Fehler: Die Einschlussliste zum Filtern von VMs darf nicht leer sein	Wenn „Liste einschließen“ ausgewählt ist, listen Sie bitte gültige DataCenter-, Cluster- oder Hostnamen auf, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter unter IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die IP-Adresse. * Versuchen Sie, über den VMware Infrastructure Client mit Virtual Center zu kommunizieren. * Versuchen Sie, über den Managed Object Browser (z. B. MOB) mit Virtual Center zu kommunizieren.
Fehler: VirtualCenter bei IP verfügt über ein nicht konformes Zertifikat, das JVM benötigt	Mögliche Lösungen: * Empfohlen: Generieren Sie das Zertifikat für Virtual Center neu, indem Sie einen stärkeren (z. B. 1024-Bit) RSA-Schlüssel verwenden. * Nicht empfohlen: Ändern Sie die JVM-Konfiguration <code>java.security</code> , um die Einschränkung <code>jdk.certpath.disabledAlgorithms</code> zu nutzen und einen 512-Bit-RSA-Schlüssel zuzulassen. Sehen "Versionshinweise zu JDK 7 Update 40" .
Ich sehe die Meldung: „VMware Logs-Paket wird auf VMware unter Version 8.0.1 nicht unterstützt.“	Die Protokollerfassung wird auf VMware-Versionen vor 8.0.1 nicht unterstützt. Aktualisieren Sie Ihre VI Center-Infrastruktur auf Version 8.0.1 oder höher, wenn Sie die Funktion „Protokollsammlungen“ in Data Infrastructure Insights verwenden möchten. Weitere Informationen finden Sie hier "KB-Artikel" .

Weitere Informationen finden Sie in der ["Support"](#) Seite oder in der ["Datensammler-Supportmatrix"](#) .

Datensammlerreferenz – Dienste

Knotendatenerfassung

Data Infrastructure Insights sammelt Metriken von 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 beliebigen Integrationsdatensammlers (Kubernetes, Docker, Apache usw.) auch die Knotendatenerfassung konfiguriert wird.
2. Befolgen Sie die Anweisungen zum Konfigurieren des Agenten. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden als Knotenmetriken erfasst:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Knotendateisystem	Knoten-UUID- Gerätepfadtyp	Knoten-IP Knotenname Knoten- Betriebssystemmodus	Freie Inodes Freie Inodes Gesamtanzahl der verwendeten Inodes Gesamtanzahl der verwendeten Inodes Gesamtanzahl der verwendeten Inodes
Knotendatenträger	Knoten-UUID-Datenträger	Knoten-IP Knotenname Knoten-Betriebssystem	IO-Zeit Laufende IOPS Gesamtanzahl gelesener Bytes (pro Sek.) Lesezeit Gesamtanzahl gelesener Bytes (pro Sek.) Gewichtete IO-Zeit Gesamtanzahl geschriebener Bytes (pro Sek.) Schreibzeit Gesamtanzahl geschriebener Bytes (pro Sek.) Aktuelle Warteschlangenlänge der Festplatte Schreibzeit Lesezeit IO-Zeit
Knoten-CPU	Knoten-UUID-CPU	Knoten-IP Knotenname Knoten-Betriebssystem	System-CPU-Auslastung Benutzer-CPU-Auslastung Leerlauf-CPU-Auslastung Prozessor-CPU- Auslastung Interrupt-CPU- Auslastung DPC-CPU- Auslastung

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Node	Knoten-UUID	Knoten-IP Knotenname Knoten-Betriebssystem	Kernel-Bootzeit Kernel-Kontextwechsel (pro Sek.) Verfügbare Kernel-Entropie Kernel-Interrupts (pro Sek.) Abgespaltene Kernel-Prozesse (pro Sek.) Aktiver Speicher Verfügbarer Gesamtspeicher Verfügbarer Speicher Gepufferter Speicher Zwischengespeicherter Speicher Commit-Limit Als Speicher festgeschriebener Speicher Dirty Memory Freier Speicher hoch Freier Speicher hoch Gesamtspeicher Größe großer Seiten Speicher Große Seiten Freier Speicher Große Seiten Gesamtspeicher niedrig Freier Speicher niedrig Gesamtspeicher Zugeordneter Speicher Seitentabellen Speicher Gemeinsam genutzter Speicher Slab-Speicher Swap Zwischengespeicherter Speicher Swap Freier Speicher Swap Gesamtspeicher Gesamt verwendeter Speicher Gesamt verwendeter Speicher Speicher Vmalloc-Chunk-Speicher Vmalloc Gesamtspeicher Vmalloc Verwendeter Speicher Verdrahteter Speicher Writeback Gesamter Speicher Writeback Temporärer Speicher Cache-Fehler Speicherbedarf Null-Fehler Speicherseitenfehler Speicherseiten Speicher Nicht ausgelagerter Speicher Ausgelagerter Speicher Cache-Kernspeicher Standby-Cache Normaler Speicher Standby-Cache

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Knotennetzwerk	Netzwerkschnittstellenknoten-UUID	Knotenname Knoten-IP Knoten-Betriebssystem	Empfangene Bytes Gesendete Bytes Ausgehende Pakete Verworfen Pakete Ausgehende Fehler Empfangene Pakete Verworfen Pakete Empfangene Fehler Empfangene Pakete Gesendete Pakete

Aufstellen

Informationen zur Einrichtung und Fehlerbehebung finden Sie auf der "[Konfigurieren eines Agenten](#)" Seite.

ActiveMQ-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



ActiveMQ Configuration

Gathers ActiveMQ metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-activemq.conf file.

```
[[inputs.activemq]]
  ## Required ActiveMQ Endpoint, port
  ## USER-ACTION: Provide address of ActiveMQ, HTTP port for ActiveMQ
  server = "<INSERT_ACTIVEMQ_ADDRESS>"
  port = <INSERT_ACTIVEMQ_PORT>
```

- 2 Replace <INSERT_ACTIVEMQ_ADDRESS> with the applicable ActiveMQ server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ACTIVEMQ_PORT> with the applicable ActiveMQ server HTTP port.
- 4 Replace <INSERT_ACTIVEMQ_USERNAME> and <INSERT_ACTIVEMQ_PASSWORD> with the applicable ActiveMQ credentials.
- 5 Modify 'webadmin' if needed (if ActiveMQ server changes web admin root path).
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im "[ActiveMQ-Dokumentation](#)"

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
ActiveMQ-Warteschlange	Namespace- Warteschlangen-Port- Server	Knotenname Knoten-IP Knoten-UUID	Anzahl der Verbraucher Anzahl der Dequeues Anzahl der Enqueues Warteschlangengröße
ActiveMQ-Abonnent	Client-ID Verbindungs-ID Port Server-Namespace	Ist aktiv Zielknotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem- Selektor Abonnement	Anzahl der aus der Warteschlange entfernten Aufgaben Anzahl der versendeten Aufgaben Warteschlangengröße Anzahl der in die Warteschlange entfernten Aufgaben Größe der ausstehenden Warteschlange
ActiveMQ-Thema	Thema Port Server Namespace	Knotenname Knoten-IP Knoten-UUID Knoten- Betriebssystem	Anzahl der Verbraucher Anzahl der Dequeues Anzahl der Enqueues Anzahl der Größe

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Apache-Datensammler

Dieser Datensammler ermöglicht das Sammeln von Daten von Apache-Servern auf Ihrem Mandanten.

Voraussetzungen

- Sie müssen Ihren Apache HTTP-Server eingerichtet und ordnungsgemäß ausgeführt haben
- Sie müssen über Sudo- oder Administratorberechtigungen auf Ihrem Agent-Host/Ihrer VM verfügen
- Normalerweise ist das Apache-Modul `mod_status` 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 Ihres 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.

3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Apache Configuration
Gathers Apache metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps [Need Help?](#)

- 1 Ensure that the Apache HTTP Server system you're going to gather metrics on has the 'mod_status' module enabled and exposed. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-apache.conf file.

```
[[inputs.apache]]
  ## An array of URLs to gather from, must be directed at the machine
  ## readable version of the mod_status page including the auto query string.
  ## USER-ACTION: Provide address of apache server, port for apache server, confirm path for
  ## server-status.
  ## Please specify actual machine IP address, and replace the url with a localhost address if -
```
- 3 Replace <INSERT_APACHE_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_APACHE_PORT> with the applicable Apache server port.
- 5 Modify the '/server-status' path in accordance to the Apache server configuration.
- 6 Restart the Telegraf service.

systemctl restart telegraf

Aufstellen

Das Plugin von Telegraf für den HTTP-Server von Apache erfordert die Aktivierung des Moduls „mod_status“. Wenn dies aktiviert ist, stellt der HTTP-Server von Apache einen HTML-Endpunkt bereit, der in Ihrem Browser angezeigt oder zum Extrahieren des Status der gesamten HTTP-Serverkonfiguration von Apache verwendet werden kann.

Kompatibilität:

Die Konfiguration wurde für Apaches HTTP-Server Version 2.4.38 entwickelt.

Aktivieren von mod_status:

Das Aktivieren und Freigeben der „mod_status“-Module umfasst zwei Schritte:

- Aktivierungsmodul
- Statistiken aus dem Modul anzeigen

Aktivierungsmodul:

Das Laden der Module wird durch die Konfigurationsdatei unter „/usr/local/apache/conf/httpd.conf“ gesteuert. Bearbeiten Sie die Konfigurationsdatei und entfernen Sie die Kommentarzeichen aus den folgenden Zeilen:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Statistiken aus dem Modul anzeigen:

Die Offenlegung von „mod_status“ wird durch die Konfigurationsdatei unter „/usr/local/apache2/conf/extra/httpd-info.conf“ gesteuert. Stellen Sie sicher, dass die Konfigurationsdatei Folgendes enthält (zumindest andere Anweisungen werden dort vorhanden sein):

```
# 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
```

Ausführliche Anweisungen zum Modul „mod_status“ finden Sie im ["Apache-Dokumentation"](#)

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Apache	Namespace-Server	Knoten-IP Knotenname Port Übergeordneter Server Konfigurationsgenerierung Übergeordneter Server MPM-Generierung Server- Betriebszeit wird gestoppt	Beschäftigte Worker Bytes pro Anfrage Bytes pro Sekunde CPU-Kinder System-CPU-Kinder Benutzer-CPU-Last CPU- System-CPU-Benutzer Asynchrone Verbindungen Schließende asynchrone Verbindungen Asynchrone Keep-Alive-Verbindungen Schreibende Verbindungen Gesamtdauer pro Anfrage Inaktive Worker Durchschnittliche Auslastung (letzte 1 Min.) Durchschnittliche Auslastung (letzte 15 Min.) Durchschnittliche Auslastung (letzte 5 Min.) Prozesse Anfragen pro Sekunde Gesamtzugriffe Gesamtdauer Gesamt- KByte Anzeigetafel Anzeigetafel wird geschlossen Anzeigetafel DNS-Lookups Anzeigetafel wird beendet Anzeigetafel Anzeigetafel Leerlaufbereinigung Anzeigetafel Keep-Alive Anzeigetafel wird protokolliert Anzeigetafel geöffnet Anzeigetafel liest Anzeigetafel sendet Anzeigetafel startet Anzeigetafel wartet

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Konsul-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Consul zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Consul.

Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert, "[Installieren eines Agenten](#)" auf Ihrem Mieter.

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 Consul-Konfigurationsbildschirm, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

Aufstellen

Informationen finden Sie im "[Konsuldokumentation](#)".

Objekte und Zähler für Consul

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Consul	Namespace-Check-ID-Dienstknoten	Knoten-IP Knoten-Betriebssystem Knoten-UUID Knotenname Dienstname Name prüfen Dienst-ID Status	Warnung vor kritischem Überholen

Fehlerbehebung

Weitere Informationen finden Sie in der "[Support](#)" Seite.

Couchbase-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Couchbase zu sammeln.


Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Couchbase.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen

variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

 **Couchbase**

Couchbase Configuration
Gathers Couchbase metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps [Need Help?](#)

- Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-couchbase.conf file.

```
## Read metrics from one or many couchbase clusters
[[inputs.couchbase]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://10.10.10.10:8090
  ## https://username:password@10.10.10.10:8090
```
- Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with couchbase server account credentials.
- Replace <INSERT_COUCHBASE_ADDRESS> with the applicable Couchbase address. Please specify a real machine address, and refrain from using a loopback address.
- Replace <INSERT_COUCHBASE_PORT> with the applicable Couchbase port.
- Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im "[Couchbase-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Couchbase-Knoten	Namespace-Cluster Couchbase-Knoten- Hostname	Knotenname Knoten-IP	Speicher Freier Speicher Gesamt
Couchbase-Eimer	Namespace-Bucket- Cluster	Knotenname Knoten-IP	Verwendete Daten Datenabrufe Verwendete Festplatte Anzahl der Elemente Verwendeter Speicher Vorgänge pro Sekunde Verwendetes Kontingent

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

CouchDB-Datensammler

Data Infrastructure Insights verwendet 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



CouchDB Configuration

Gathers CouchDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-couchdb.conf file.

```
## Read CouchDB Stats from one or more servers
[[inputs.couchdb]]
  ## Works with CouchDB stats endpoints out of the box
  ## Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
```

- 2 Replace <INSERT_COUCHDB_ADDRESS> with the applicable CouchDB address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_COUCHDB_PORT> with the applicable CouchDB port.
- 4 Modify the URL if CouchDB monitoring is exposed at different path
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie im "[CouchDB-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
CouchDB	Namespace-Server	Knotenname Knoten-IP	Authentifizierungscache-Treffer Authentifizierungscache-Fehler Datenbank-Lesevorgänge Datenbank-Schreibvorgänge Datenbanken öffnen Betriebssystemdateien öffnen Max. Anforderungszeit Min. Anforderungszeit HTTP-Anforderungsmethoden HTTP-Anforderungsmethoden kopieren HTTP-Anforderungsmethoden löschen HTTP-Anforderungsmethoden abrufen HTTP-Anforderungsmethoden headen HTTP-Anforderungsmethoden posten HTTP-Anforderungsmethoden setzen Statuscodes 200 Statuscodes 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 in der ["Support"](#) Seite.

Docker-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Docker zu sammeln.

Installation


1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Docker.

Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert, ["Installieren eines"](#)

Agenten" auf Ihrem Mieter.


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 Docker-Konfigurationsbildschirm, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Docker Configuration
Gathers Docker metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

 RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps [Need Help?](#)

1

Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-docker.conf file.

```
[[inputs.docker]]
  ## Docker Endpoint
  ## To use TCP, set endpoint = "tcp://[ip]:[port]". By default, Docker uses port 2375 for
  unencrypted and 2376 for encrypted
  ## To use environment variables (ie, docker-machine), set endpoint = "ENV"
```

2

Replace <INSERT_DOCKER_ENDPOINT> with the applicable Docker endpoint.

3

Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).

4

Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Das Telegraf-Eingabe-Plugin für Docker sammelt Metriken über einen angegebenen UNIX-Socket oder einen TCP-Endpunkt.

Kompatibilität

Die Konfiguration wurde für Docker Version 1.12.6 entwickelt.

Einrichten

Zugriff auf Docker über einen UNIX-Socket

Wenn der Telegraf-Agent auf Baremetal ausgeführt wird, 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 frei, indem Sie den Socket als Volume in den Pod einbinden und dieses Volume dann in `/var/run/docker.sock` mounten. Fügen Sie der PodSpec beispielsweise 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 für die Kubernetes-Plattform bereitgestellte Data Infrastructure Insights -Installationsprogramm diese Zuordnung automatisch vornimmt.

Zugriff auf Docker über einen TCP-Endpunkt

Standardmäßig verwendet Docker Port 2375 für unverschlüsselten Zugriff und Port 2376 für verschlüsselten Zugriff.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Engine	Namespace Docker Engine	Knotenname Knoten-IP Knoten-UUID Knoten- Betriebssystem Kubernetes-Cluster Docker-Version Einheit	Speichercontainer Container Angehaltene Container Laufende Container Gestoppte CPUs Go-Routinen Bilder Listener Verwendete Ereignisse Datei- Deskriptoren Daten Verfügbare Daten Gesamt verwendete Daten Metadaten Verfügbare Metadaten Gesamt verwendete Metadaten Pool-Blockgröße

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container	Namespace Containername Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container-Neustart-Zähler Kubernetes-Container-Beendigungsnachrichtenfad Kubernetes-Container-Beendigungsnachrichtentrichtlinie Kubernetes-Pod-Beendigungsfrist Container-Image Container-Status Container-Version Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Container-Name Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Namespace Kubernetes-Pod-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Docker-Version Kubernetes-E/A-Konfiguration gesehen Kubernetes-E/A-Konfigurationsquelle OpenShift-E/A-SCC Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Kompose-Service Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Lizenzschema Erstellungsdatum Schema-Lizenz Schemaname Schema-URL Schema-VCS-URL Schemaanbieter Schemaversion Schema-Schemaversionsbetreuer Kunde Pod Kubernetes-StatefulSet Pod-Name Mandant Webkonsolen-Architektur Autoritative-Quell-URL Erstellungsdatum RH-Build-Host RH-Komponente Verteilungsbereich Installation Release-	Aktiver anonymer Speicher Aktiver Dateispeicher Cache-Speicher Hierarchische Grenze Inaktiver anonymer Speicher Inaktive Dateispeichergrenze Zugeordneter Dateispeicher Maximale Speicherauslastung Speicherseitenfehler Schwerwiegender Seitenfehler Eingelagerter Speicher Ausgelagerter Speicher Größe des residenten Satzes Riesiger residenter Satz Größe des residenten Satzes Gesamter aktiver anonymer Speicher Gesamter aktiver Dateispeicher Gesamter Cache-Speicher Gesamter inaktiver anonymer Speicher Gesamter inaktiver Dateispeicher Gesamter zugeordneter Dateispeicher Gesamter Seitenfehler Speicher Gesamter schwerwiegender Seitenfehler Gesamter ausgelagerter Speicher Gesamter ausgelagerter Speicher Gesamte Größe des residenten Satzes Gesamter residenter Satz Größe des residenten Satzes Gesamter nicht auslagerbarer Speicher Nicht auslagerbarer Speichernutzung Speichernutzung in Prozent Exit-Code OOM beendet PID gestartet bei Failing Streak

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-Block-IO	Namespace Containername Gerät Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Anzahl der Neustarts von Kubernetes-Containern Pfad der Kubernetes-Container-Beendigungsnachrichten Richtlinie für Kubernetes-Container-Beendigungsnachrichten Karenzzeit für Kubernetes-Pod-Beendigung Container-Image Container-Status Container-Version Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Container-Name Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Namespaces Kubernetes-Pod-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Docker-Version Gesehene Kubernetes-Konfiguration Kubernetes-Konfigurationsquelle OpenShift SCC Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Schema Schemaversion Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Kompose-Dienst Schema-Erstellungsdatum Schema-Lizenz Schemaname Schemaanbieter Kunden-Pod Kubernetes-StatefulSet Pod-Name Mandant-Webkonsole Erstellungsdatum Lizenzanbieter Architektur Autoritative Quell-URL RH-Build-Host RH-Komponente Verteilungsbereich Installationsbetreuer Release-Ausführungszusammenfa	IO-Service-Bytes rekursiv Asynchron IO-Service-Bytes rekursiv Lesen IO-Service-Bytes rekursiv Sync IO-Service-Bytes rekursiv gesamt IO-Service-Bytes rekursiv Schreiben IO bedient rekursiv Asynchron IO bedient rekursiv Lesen IO bedient rekursiv Sync IO bedient rekursiv gesamt IO bedient rekursiv Schreiben

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-Netzwerk	Namespace Containername Netzwerk Docker Engine	Container-Image Container-Status Container-Version Knotenname Knoten-IP Knoten-UUID Knoten-Betriebssystem K8s-Cluster Docker-Version Container-ID	RX Verloren RX Bytes RX Fehler RX Pakete TX Verloren TX Bytes TX Fehler TX Pakete

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Docker-Container-CPU	Namespace Containername CPU Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container-Neustart-Zähler Kubernetes-Container-Beendigungsnachrichtenpfad Kubernetes-Container-Beendigungsnachrichtentyp Kubernetes-Pod-Beendigungsfrist Kubernetes-Konfiguration Kubernetes-Konfigurationsquelle OpenShift SCC-Container-Image Containerstatus Containerversion Knotenname Kubernetes-Container-Protokollpfad Kubernetes-Containername Kubernetes-Docker-Typ Kubernetes-Pod-Name Kubernetes-Pod-Name Kubernetes-Container-UID Kubernetes-Sandbox-ID Knoten-IP Knoten-UUID Knoten-Betriebssystem Kubernetes-Cluster Docker-Version Kubernetes-Beschreibung Kubernetes-Anzeigename OpenShift-Tags Schemaversion Pod-Vorlagen-Hash Controller-Revisions-Hash Pod-Vorlagengenerierung Kompose-Dienst Schema-Erstellungsdatum Schema-Lizenz Schemaname Schemaanbieter Kunden-Pod Kubernetes-StatefulSet Pod-Name Mandant-Webkonsole Erstellungsdatum Lizenzanbieter Architektur Autoritative Quell-URL RH-Build-Host RH-Komponente Verteilungsbereich Installationsbetreuer Release-	Drosselungsperioden Drosselung Drosselungsperioden Drosselungszeit Drosselungszeit Nutzung im Kernelmodus Nutzung im Benutzermodus Nutzung in Prozent Nutzung Systemnutzung gesamt

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
Ich sehe meine Docker-Metriken nicht in Data Infrastructure Insights, nachdem ich die Anweisungen auf der Konfigurationsseite befolgt habe.	Überprüfen Sie die Protokolle des Telegraf-Agenten, um zu sehen, ob der folgende Fehler gemeldet wird: E! Fehler im Plugin [inputs.docker]: Beim Versuch, eine Verbindung zum Docker-Daemon-Socket herzustellen, wurde die Berechtigung verweigert. Wenn dies der Fall ist, ergreifen Sie die erforderlichen Maßnahmen, um dem Telegraf-Agenten Zugriff auf den Docker-Unix-Socket zu gewähren, wie oben angegeben.

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Elasticsearch-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Elasticsearch zu sammeln.

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Elasticsearch.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Elasticsearch Configuration

Gathers Elasticsearch metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-elasticsearch.conf file.

```
[[inputs.elasticsearch]]
  ## USER-ACTION: Provide comma-separated list of Elasticsearch servers.
  ## Note that for scenarios in which metrics from multiple Elasticsearch clusters are being
  ## sent to Cloud Insights, the Elasticsearch cluster names must be unique.
  ## Please specify actual machine IP address, and refrain from using a loopback address
```

- 2 Replace <INSERT_ELASTICSEARCH_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ELASTICSEARCH_PORT> with the applicable Elasticsearch port.
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie im "[Elasticsearch-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Elasticsearch-Cluster	Namespace-Cluster	Knoten-IP Knotenname Clusterstatus
Elasticsearch-Knoten	Namespace-Cluster ES-Knoten-ID ES-Knoten-IP ES-Knoten	Zonen-ID

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Flink-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Flink zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Flink.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Flink Configuration

Gathers Flink metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## *****  
## JobManager  
## *****  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL  
  ## for each Job Manager to monitor address
```

- 3 Replace <INSERT_FLINK_JOBMANAGER_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_FLINK_TASKMANAGER_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT_JOLOKIA_PORT> with the applicable jolokia port.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Modify 'Cluster' if needed for Flink cluster designation.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Eine vollständige Flink-Bereitstellung umfasst die folgenden Komponenten:

JobManager: Das Flink-Primärsystem. Koordiniert eine Reihe von TaskManagern. In einer Hochverfügbarkeitskonfiguration verfügt das System über mehr als einen JobManager. **TaskManager:** Hier werden Flink-Operatoren ausgeführt. Das Flink-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Flink-Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Flink Version 1.7.0 entwickelt.

Einrichten

Jolokia Agent Jar

Für alle Einzelkomponenten muss eine Version der Jolokia-Agent-JAR-Datei heruntergeladen werden. Die getestete Version war ["Jolokia-Agent 1.6.0"](#).

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/flink/lib/“ abgelegt ist.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia-API verfügbar gemacht 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 für Jolokia einen anderen Port (8778) wählen. Wenn Sie eine interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die „Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP vom Telegraf-Plugin aus zugänglich sein muss.

Task-Manager

Um TaskManager so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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 für Jolokia einen anderen Port (8778) wählen. Wenn Sie eine interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die „Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP vom Telegraf-Plugin aus zugänglich sein muss.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink Task-Manager	Cluster-Namespace-Server	Knotenname Task-Manager-ID Knoten-IP	Verfügbare Netzwerkspeichersegmente Netzwerkspeichersegmente gesamt Garbage Collection PS MarkSweep-Anzahl Garbage Collection PS MarkSweep-Zeit Garbage Collection PS Scavenge-Anzahl Garbage Collection PS Scavenge-Zeit Heap-Speicher zugesichert Heap-Speicher initialisieren Heap-Speicher max. Verwendeter Heap-Speicher Thread-Anzahl Daemon-Threads Spitzen-Thread-Anzahl Thread-Anzahl insgesamt gestartet
Flink Job	Job-ID des Cluster-Namespace-Servers	Knotenname Jobname Knoten-IP Letzter Prüfpunkt Externer Pfad Neustartzeit	Ausfallzeit Vollständige Neustarts Ausrichtung des letzten Prüfpunkts Gepuffert Dauer des letzten Prüfpunkts Größe des letzten Prüfpunkts Anzahl abgeschlossener Prüfpunkte Anzahl fehlgeschlagener Prüfpunkte Anzahl laufender Prüfpunkte Anzahl Prüfpunkte Betriebszeit

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink Job Manager	Cluster-Namespace-Server	Knotenname Knoten-IP	Garbage Collection PS MarkSweep-Anzahl Garbage Collection PS MarkSweep-Zeit Garbage Collection PS Scavenge-Anzahl Garbage Collection PS Scavenge-Zeit Heap-Speicher zugesichert Heap-Speicher initialisieren Heap-Speicher max. verwendeter Heap-Speicher Anzahl registrierter Task-Manager Anzahl laufender Jobs Verfügbare Task-Slots Gesamt-Thread-Anzahl Daemon-Thread-Anzahl Spitzen-Thread-Anzahl Threads insgesamt gestartet

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink-Aufgabe	Cluster-Namespace Job-ID Aufgaben-ID	Serverknotenname Jobname Sub-Task-Index Task-Versuchs-ID Task-Versuchsnummer Taskname Task-Manager-ID Knoten-IP Aktuelles Eingabewasserzeichen	Puffer im Pool, Nutzung, Puffer in Warteschlangenlänge, Puffer aus, Pool, Nutzung, Puffer aus, Warteschlangenlänge, Anzahl, Puffer lokal, Anzahl, Puffer lokal pro Sekunde, Anzahl, Puffer lokal pro Sekunde, Rate, Anzahl, Puffer extern, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Rate, Anzahl, Puffer extern, Anzahl, Puffer extern pro Sekunde, Anzahl, Puffer extern pro Sekunde, Rate, Anzahl, Bytes lokal, Anzahl, Bytes lokal pro Sekunde, Anzahl, Bytes lokal pro Sekunde, Rate, Anzahl, Bytes lokal pro Sekunde, Rate, Anzahl, Bytes extern, Anzahl, Bytes extern pro Sekunde, Anzahl, Bytes extern pro Sekunde, Rate, Anzahl, Bytes extern pro Sekunde, Anzahl, Bytes extern pro Sekunde, Rate, Anzahl, Datensätze extern, Anzahl, Datensätze extern pro Sekunde, Rate, Anzahl, Datensätze extern, Anzahl, Datensätze extern pro Sekunde, Rate, Anzahl, Datensätze extern pro Sekunde

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Flink-Task-Operator	Cluster-Namespace Job-ID Operator-ID Aufgaben-ID	Serverknotenname Jobname Operatorname Sub-Task-Index Task-Versuchs-ID Task-Versuchsnummer Taskname Task-Manager-ID Knoten-IP	Aktuelles Eingabe-Wasserzeichen Aktuelles Ausgabe-Wasserzeichen Anzahl Datensätze (ein) Anzahl Datensätze (ein) pro Sekunde Anzahl Datensätze (ein) pro Sekunde Rate Anzahl Datensätze (aus) Anzahl Datensätze (aus) pro Sekunde Anzahl Datensätze (aus) pro Sekunde Rate Anzahl verspätet gelöschte Datensätze Zugewiesene Partitionen Verbrauchte Byte-Rate Commit-Latenz (Durchschnitt) Commit-Latenz (Maximal) Commit-Rate Fehlgeschlagene Commits Erfolgreiche Commits Verbindungsabschlussrate Anzahl Verbindungen Anzahl Verbindungserstellungsraten Anzahl Abrufatenz (Durchschnitt) Max. Abrufatenz Abrufatenz Abrufatenz (Durchschnitt) Abrufgröße (Maximal) Abrufgröße (Maximal) Abrufdrosselzeit (Durchschnitt) Max. Abrufdrosselzeit Heartbeat-Rate Eingehende Byte-Rate IO-Verhältnis IO-Zeit (Durchschnitt) (ns) IO-Warteverhältnis IO-Wartezeit (Durchschnitt) Join-Rate durchschnittliche Join-Zeit vor dem letzten Heartbeat Netzwerk-IO-Rate Ausgehende Byte-Rate Verbrauchte Datensätze Rate der Datensätze Verzögerung (Maximal) Datensätze pro Anfrage durchschnittliche Anfragerate Anfragegröße durchschnittliche Anfragegröße (Maximal) Antwortrate Auswahlrate

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Hadoop-Datensammler


Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Hadoop zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Hadoop.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Hadoop Configuration
Gathers Hadoop metrics.

What Operating System or Platform Are You Using?Need Help?

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-hadoop.conf file.

```
#####  
# NAMENODE #  
#####  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia  
  ## Please specify a real machine address, and refrain from using a loopback address
```

- 3 Replace <INSERT_HADOOP_NAMENODE_ADDRESS> with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NameNode's assigned Jolokia port.
- 4 Replace <INSERT_HADOOP_SECONDARYNAMENODE_ADDRESS> with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Secondary NameNode's assigned Jolokia port.
- 5 Replace <INSERT_HADOOP_DATANODE_ADDRESS> with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the DataNode's assigned Jolokia port.
- 6 Replace <INSERT_HADOOP_RESOURCEMANAGER_ADDRESS> with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the ResourceManager's assigned Jolokia port.
- 7 Replace <INSERT_HADOOP_NODEMANAGER_ADDRESS> with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NodeManager's assigned Jolokia port.
- 8 Replace <INSERT_HADOOP_JOBHISTORYSERVER_ADDRESS> with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Job History Server's assigned Jolokia port.
- 9 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 10 Modify 'Cluster' if needed for Hadoop cluster designation.
- 11 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Eine vollständige Hadoop-Bereitstellung umfasst die folgenden Komponenten:

- NameNode: Das primäre System des Hadoop Distributed File System (HDFS). Koordiniert eine Reihe von DataNodes.

- Sekundärer NameNode: ein Warm-Failover für den Haupt-NameNode. In Hadoop erfolgt die Beförderung zum NameNode nicht automatisch. Der sekundäre NameNode sammelt Informationen vom NameNode, um bei Bedarf für die Beförderung bereit zu sein.
- DataNode: Tatsächlicher Eigentümer der Daten.
- ResourceManager: Das primäre Rechensystem (Yarn). Koordiniert eine Reihe von NodeManagern.
- NodeManager: Die Ressource für die Berechnung. Tatsächlicher Speicherort für die Ausführung von Anwendungen.
- JobHistoryServer: Verantwortlich für die Bearbeitung aller Anfragen zum Jobverlauf.

Das Hadoop-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Hadoop-Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Hadoop Version 2.9.2 entwickelt.

Einrichten

Jolokia Agent Jar

Für alle Einzelkomponenten muss eine Version der Jolokia-Agent-JAR-Datei heruntergeladen werden. Die getestete Version war "[Jolokia-Agent 1.6.0](#)".

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/hadoop/lib/“ abgelegt ist.

NameNode

Um NameNode für die Bereitstellung der Jolokia-API zu konfigurieren, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh 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 für die Bereitstellung der Jolokia-API zu konfigurieren, 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.
```

Datenknoten

Um die DataNodes so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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.
```

Ressourcenmanager

Um den ResourceManager für die Bereitstellung der Jolokia-API zu konfigurieren, 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.

Knotenmanager

Um die NodeManager so zu konfigurieren, dass sie die Jolokia-API verfügbar machen, 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.

JobHistoryServer

Um den JobHistoryServer für die Bereitstellung der Jolokia-API zu konfigurieren, 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

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Sekundärer NameNode von Hadoop	Cluster-Namespace-Server	Knotenname Knoten-IP Kompilierungsinformationen Version
Hadoop NodeManager	Cluster-Namespace-Server	Knotenname Knoten-IP
Hadoop-Ressourcenmanager	Cluster-Namespace-Server	Knotenname Knoten-IP
Hadoop-Datenknoten	Cluster-Namespace-Server	Knotenname Knoten-IP Cluster-ID Version
Hadoop-Namensknoten	Cluster-Namespace-Server	Knotenname Knoten-IP Transaktions-ID Zuletzt geschrieben Zeit seit dem letzten Laden Bearbeitungen HA-Status Dateisystemstatus Blockpool-ID Cluster-ID Kompilierungsinformationen Eindeutige Versionsanzahl Version
Hadoop JobHistoryServer	Cluster-Namespace-Server	Knotenname Knoten-IP

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

HAProxy-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



HAProxy Configuration

Gathers HAProxy metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the HAProxy system you're going to gather metrics on has 'stats enable' option. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-haproxy.conf file.

```
# Read metrics of HAProxy, via socket or HTTP stats page
[[inputs.haproxy]]
  ## An array of address to gather stats about. Specify an ip on hostname
  ## with optional port. ie localhost, 10.10.3.33:1936, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## default for the socket: /etc/haproxy/haproxy.sock
  urls = [ "http://10.10.3.33:1936/stats" ]
```

- 3 Replace <INSERT_HAPROXY_ADDRESS> with the applicable HAProxy server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_HAPROXY_PORT> with the applicable HAProxy server port.
- 5 Modify the 'haproxy?stats' path in accordance to the HAProxy server configuration.
- 6 Modify 'username' and 'password' in accordance to the HAProxy server configuration (if credentials are required).
- 7 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Das Plugin von Telegraf für HAProxy basiert auf der Aktivierung von HAProxy Stats. Dies ist eine in HAProxy integrierte Konfiguration, die jedoch nicht standardmäßig aktiviert ist. Wenn aktiviert, stellt HAProxy einen

HTML-Endpunkt bereit, der in Ihrem Browser angezeigt oder zum Extrahieren des Status aller HAProxy-Konfigurationen abgerufen werden kann.

Kompatibilität:

Die Konfiguration wurde für HAProxy Version 1.9.4 entwickelt.

Einrichten:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre Haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt „Standardeinstellungen“ die folgenden Zeilen hinzu. Verwenden Sie dabei Ihren eigenen Benutzer/Ihr eigenes Passwort und/oder Ihre Haproxy-URL:

```
stats enable
stats auth myuser:mypassword
stats uri /haproxy?stats
```

Nachfolgend sehen Sie eine vereinfachte Beispielkonfigurationsdatei 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

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy Frontend	Namespace-Adressproxy	Knoten-IP Knotenname Proxy-ID Modus Prozess-ID Sitzungsratenbegrenzung Server-ID Sitzungsbegrenzungsstatus	Bytes Eingehend Bytes Ausgehend Cache-Treffer Cache-Suchen Komprimierung Bytes Umgangene Komprimierung Bytes Eingehend Komprimierung Bytes Ausgehend Komprimierung Antworten Verbindungsrate Verbindungsrate Max. Verbindungen Gesamt Durch Verbindungsregel abgelehnte Anfragen Durch Sicherheitsbedenken abgelehnte Anfragen Antworten Durch Sicherheitsbedenken abgelehnte Anfragen Durch Sitzungsregel abgelehnte Anfragen Fehler bei Anfragen Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere Anfragen Abgefangene Anfragen Sitzungsrate Sitzungsrate Max. Anfragen Rate Anfragen Rate Max. Anfragen Gesamtanzahl Sitzungen Sitzungen Max. Sitzungen Gesamtanzahl Anfragen Neuschreibungen

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy Server	Namespace-Adress-Proxy-Server	Knoten-IP Knotenname Zeit bis zum Abschluss der Prüfung Fallkonfiguration prüfen Gesundheitswert prüfen Anstiegskonfiguration prüfen Status prüfen Proxy-ID Zeit der letzten Änderung Zeit der letzten Sitzung Modus Prozess-ID Server-ID Status Gewicht	Aktive Server Backup-Server Bytes rein Bytes raus Check-Downs Check-Fehlschläge Client-Abbrüche Verbindungen Durchschnittliche Verbindungsdauer Ausfallzeit Gesamt abgelehnte Antworten Verbindungsfehler Antwortfehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere ausgewählte Server Gesamtwarteschlange Aktuelle Warteschlange Max. Durchschnittliche Warteschlangendauer Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Verbindungswiederverwendung Antwortzeit Durchschnittliche Sitzungen Sitzungen Max. Server-Übertragungsabbrüche Sitzungen Gesamtsitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisungen Anfragen Wiederholungsversuche Anfragen Neuschreibungen

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
HAProxy-Backend	Namespace-Adressproxy	Knoten-IP Knotenname Proxy-ID Letzte Änderung Zeit der letzten Sitzung Modus Prozess-ID Server-ID Sitzungslimit Status Gewicht	Aktive Server Backup- Server Bytes In Bytes Out Cache-Treffer Cache- Lookups Check-Downs Client-Abbrüche Komprimierung Bytes Umgangene Komprimierung Bytes In Komprimierung Bytes Out Komprimierung Antworten Verbindungen Durchschnittliche Verbindungsausfallzeit Anfragen insgesamt aufgrund von Sicherheitsbedenken abgelehnt Antworten aufgrund von Sicherheitsbedenken abgelehnt Verbindungsfehler Antwortfehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten Andere ausgewählte Server Gesamtwarteschlange Aktuelle Warteschlange Max. Durchschnittliche Warteschlangenzeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamte Verbindungswiederverwen- dung Antwortzeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragungsabbrü- che Sitzungen Gesamtsitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisungen Anfragen Wiederholungsversuche Anfragen Neuschreibungen

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

JVM-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von JVM zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie JVM.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Java Configuration

Gathers JVM metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your JVMs. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-jvm.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  # USER-ACTION: Provide address(es) of JVM, port for jolokia, add one URL for each JVM in
  # your cluster
  # Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  # 192.168.1.1 or 127.0.0.1)
```

- 3 Replace <INSERT_JVM_ADDRESS> with the applicable JVM address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable JVM jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie in "[JVM-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
JVM	Namespace JVM	Betriebssystemarchitektur Betriebssystemname Betriebssystemversion Laufzeitspezifikation Laufzeitspezifikationsanbieter Laufzeitspezifikationsversion Betriebszeit Laufzeit- VM-Name Laufzeit-VM- Anbieter Laufzeit-VM- Version Knotenname Knoten-IP	Geladene Klasse, geladene Klasse, gesamt, entladene Klasse, Speicher-Heap, festgeschriebener Speicher, Heap-Init- Speicher, verwendeter Heap, max. Speicher, verwendeter Heap, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, nicht festgeschriebener Speicher, max. nicht festgeschriebener Speicher, verwendeter Speicher, ausstehende Finalisierung, verfügbare OS-Prozessoren, Größe des virtuellen OS- Speichers, Größe des freien OS-physischen Speichers, Größe des freien OS-Swap- Speichers, maximale OS- Dateideskriptoranzahl, Anzahl der geöffneten OS-Dateideskriptoren, CPU-Auslastung des OS- Prozessors, CPU-Zeit des OS-Prozessors, CPU- Auslastung des OS- Systems, durchschnittliche OS- Systemauslastung, gesamt physische OS- Speichergröße, Größe des OS-Swap-Speichers insgesamt, Anzahl der Thread-Daemons, Anzahl der Thread-Spitzen, Anzahl der Threads, Anzahl der gestarteten Threads, Anzahl der Garbage Collector- Kopien, Zeit der Garbage Collector-Kopien, Anzahl der Garbage Collector-

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Kafka-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Kafka Configuration

Gathers Kafka metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-kafka.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of kafka broker(s), port for jolokia, add one URL for
  ## each broker in your cluster
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  ## 127.0.0.1)
```

- 3 Replace <INSERT_KAFKA_BROKER_ADDRESS> with the applicable Kafka broker address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable Kafka broker jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Modify 'Cluster' if needed for Kafka cluster designation.
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Das Kafka-Plugin basiert auf dem Jolokia-Plugin von Telegraf. Um beispielsweise Informationen von allen Kafka-Brokern zu sammeln, muss JMX auf allen Komponenten konfiguriert und über Jolokia verfügbar gemacht werden.

Kompatibilität

Die Konfiguration wurde für Kafka Version 0.11.0.2 entwickelt.

Einrichten

Bei allen folgenden Anweisungen wird davon ausgegangen, dass Ihr Installationsort für Kafka „/opt/kafka“ ist. Sie können die folgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version, die die Jolokia-Agent-JAR-Datei haben muss "[heruntergeladen](#)". Die getestete Version war Jolokia Agent 1.6.0.

Die folgenden Anweisungen gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-agent.jar) am Speicherort „/opt/kafka/libs/“ abgelegt ist.

Kafka-Broker

Um Kafka Brokers so zu konfigurieren, dass die Jolokia-API verfügbar gemacht wird, können Sie Folgendes in <KAFKA_HOME>/bin/kafka-server-start.sh direkt vor dem Aufruf von „kafka-run-class.sh“ 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 im obigen Beispiel „hostname -I“ verwendet wird, um die Umgebungsvariable „RMI_HOSTNAME“ einzurichten. Bei Maschinen mit mehreren IP-Adressen muss dies angepasst werden, um die IP-Adresse zu erfassen, die für RMI-Verbindungen von Bedeutung ist.

Sie können für JMX (9999 oben) und Jolokia (8778) einen anderen Port wählen. Wenn Sie eine interne IP haben, auf die Sie Jolokia sperren möchten, können Sie die „Catch-All“-IP 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP vom Telegraf-Plugin aus zugänglich sein muss. Sie können die Option „-Dcom.sun.management.jmxremote.authenticate=false“ verwenden, wenn Sie keine Authentifizierung wünschen. Die Nutzung erfolgt auf eigene Gefahr.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:
Kafka Broker	Cluster-Namespace-Broker	Knotenname Knoten-IP

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Kibana-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Kibana Configuration

Gathers Kibana metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-kibana.conf file.

```
[[inputs.kibana]]
  ## specify a list of one or more Kibana servers
  ## USER-ACTION: Provide address of kibana server(s), port(s) for kibana server
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  localhost or 127.0.0.1).
```

- 2 Replace <INSERT_KIBANA_ADDRESS> with the applicable Kibana server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_KIBANA_PORT> with the applicable Kibana server port.
- 4 Replace 'username' and 'password' with the applicable Kibana server authentication credentials as needed, and uncomment the lines.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie im "[Kibana-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Kibana	Namespace-Adresse	Knoten-IP Knotenname Version Status	Gleichzeitige Verbindungen Heap Max Verwendeter Heap Anfragen pro Sekunde Antwortzeit Durchschnittliche Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Installation und Konfiguration des Kubernetes Monitoring Operators

Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Vor der Installation des Kubernetes Monitoring Operator

Siehe die ["Voraussetzungen"](#) Dokumentation, bevor Sie den Kubernetes Monitoring Operator installieren oder aktualisieren.

Installieren des Kubernetes Monitoring Operators

Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

KEY2024 (...vw6NdM) ▼

[+ API Access Token](#)

[Production Best Practices](#) ?

Installation Instructions

[Need Help?](#)

Please review the [pre-requisites](#) for installing the NetApp Kubernetes Monitoring Operator.
To update an existing operator installation please follow [these steps](#).

1 Define Kubernetes cluster name and namespace

Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.

Cluster

clustername

Namespace

netapp-monitoring

2 Download the operator YAML files

Execute the following download command in a *bash* prompt.

[Copy Download Command Snippet](#)

[+ Reveal Download Command Snippet](#)

This snippet includes a unique access key that is valid for 24 hours.

3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in `operator-deployment.yaml` and the docker repository settings in `operator-config.yaml`. For more information review [the documentation](#).

Copy Image Pull Snippet

⊞ Reveal Image Pull Snippet

Copy Repository Password

⊞ Reveal Repository Password

This password is valid for 24 hours.

4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- `operator-setup.yaml` - Create the operator's dependencies.
- `operator-secrets.yaml` - Create secrets holding your API key.
- `operator-deployment.yaml`, `operator-cr.yaml` - Deploy the NetApp Kubernetes Monitoring Operator.
- `operator-config.yaml` - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

⊞ Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store `operator-secrets.yaml`**.

6

Next

Schritte zum Installieren des Kubernetes Monitoring Operator-Agenten auf Kubernetes:

1. Geben Sie einen eindeutigen Clusternamen und Namespace ein. Wenn Sie [Upgrade](#) von einem vorherigen Kubernetes-Operator, verwenden Sie denselben Clusternamen und Namespace.
2. Sobald diese eingegeben sind, können Sie den Download-Befehlsausschnitt in die Zwischenablage kopieren.
3. Fügen Sie den Snippet in ein `Bash`-Fenster ein und führen Sie ihn aus. Die Operator-Installationsdateien werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie den optionalen Image Pull-Ausschnitt, fügen Sie ihn in eine `Bash`-Shell ein und führen Sie ihn aus. Sobald die Bilder abgerufen wurden, kopieren Sie sie in Ihr privates Repository. Achten Sie darauf, dieselben Tags und dieselbe Ordnerstruktur beizubehalten. Aktualisieren Sie die Pfade in `operator-deployment.yaml` sowie die Docker-Repository-Einstellungen in `operator-config.yaml`.
5. Überprüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen wie Proxy- oder private Repository-Einstellungen. Weitere Informationen finden Sie unter "[Konfigurationsoptionen](#)".
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie das `kubectl` Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation erfolgt automatisch. Wenn der Vorgang abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche *Weiter*. Denken Sie daran, auch die Datei *operator-secrets.yaml* zu löschen oder sicher zu speichern.

Wenn Sie ein benutzerdefiniertes Repository haben, lesen Sie über [Verwenden eines benutzerdefinierten/privaten Docker-Repositorys](#).

Kubernetes-Überwachungskomponenten

Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Überwachungskomponenten:

- Clustermetriken
- Netzwerkleistung und Karte (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben genannten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie entscheiden, dass Sie eine Komponente für einen bestimmten Collector nicht benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Drei-Punkte-Menü des Collectors auf der rechten Bildschirmseite *Bereitstellung ändern* auswählen.

NetApp / Observability / Collectors

Data Collectors 21 Acquisition Units 4 Kubernetes Collectors

Kubernetes Collectors (13)

[View Upgrade/Delete Documentation](#)

[+ Kubernetes Collector](#)

Filter...

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	Outdated	1.1540.0	1.347.0	1.162.0	
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	
oom-test	Outdated	1.1555.0	N/A	1.101.0	Modify Deployment

Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.

Modify Deployment

Cluster Information

Kubernetes Cluster
ci-demo-01

Network Performance and Map
Enabled - Online

Event Logs
Enabled - Online

Change Analysis
Enabled - Online

Deployment Options

[Need Help?](#)

☒ Network Performance and Map

☒ Event Logs

☒ Change Analysis

Cancel

Complete Modification

Upgrade auf den neuesten Kubernetes Monitoring Operator

DII-Druckknopf-Upgrades

Sie können den Kubernetes Monitoring Operator über die DII Kubernetes Collectors-Seite aktualisieren. Klicken Sie auf das Menü neben dem Cluster, den Sie aktualisieren möchten, und wählen Sie *Upgrade*. Der Betreiber überprüft die Bildsignaturen, erstellt einen Snapshot Ihrer aktuellen Installation und führt das Upgrade durch. Innerhalb weniger Minuten sollte der Status des Operators von „Upgrade läuft“ bis „Neueste“ fortschreiten. Wenn ein Fehler auftritt, können Sie für weitere Einzelheiten den Fehlerstatus auswählen und die Tabelle zur Fehlerbehebung bei Push-Button-Upgrades weiter unten zu Rate ziehen.

Push-Button-Upgrades mit privaten Repositories

Wenn Ihr Operator für die Verwendung eines privaten Repositorys konfiguriert ist, stellen Sie bitte sicher, dass alle zum Ausführen des Operators erforderlichen Bilder und deren Signaturen in Ihrem Repository verfügbar sind. Wenn während des Upgrade-Vorgangs ein Fehler aufgrund fehlender Bilder auftritt, fügen Sie diese einfach zu Ihrem Repository hinzu und versuchen Sie das Upgrade erneut. Um die Bildsignaturen in Ihr Repository hochzuladen, verwenden Sie bitte das Cosign-Tool wie folgt und stellen Sie sicher, dass Sie Signaturen für alle unter 3 angegebenen Bilder hochladen. Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Image Pull Snippet

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Rollback auf eine zuvor ausgeführte Version

Wenn Sie das Upgrade mithilfe der Funktion „Upgrade per Knopfdruck“ durchgeführt haben und innerhalb von sieben Tagen nach dem Upgrade Probleme mit der aktuellen Version des Operators auftreten, können Sie mithilfe des während des Upgrade-Vorgangs erstellten Snapshots ein Downgrade auf die zuvor ausgeführte

Version durchführen. Klicken Sie auf das Menü neben dem Cluster, für den Sie ein Rollback durchführen möchten, und wählen Sie *Rollback* aus.

Manuelle Upgrades

Stellen Sie fest, ob eine Agentenkonfiguration mit dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardnamespace *netapp-monitoring* ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-configuration
```

Wenn eine Agentenkonfiguration vorhanden ist:

- [Installieren](#) der neueste Operator über den vorhandenen Operator.
 - Stellen Sie sicher, dass Sie [Abrufen der neuesten Container-Images](#) wenn Sie ein benutzerdefiniertes Repository verwenden.

Wenn die Agentenkonfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Clusternamen (wenn Ihr Namespace nicht der Standardnamespace „netapp-monitoring“ ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

* Erstellen Sie eine Sicherungskopie des vorhandenen Operators (wenn Ihr Namespace nicht der Standard-Netapp-Monitoring-Namespace ist, ersetzen Sie ihn durch den entsprechenden Namespace):

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>>der bestehende Betreiber.

* <<installing-the-kubernetes-monitoring-operator,Installieren>>der neueste Operator.

- Verwenden Sie denselben Clusternamen.
- Nachdem Sie die neuesten Operator-YAML-Dateien heruntergeladen haben, portieren Sie vor der Bereitstellung alle in agent_backup.yaml gefundenen Anpassungen in die heruntergeladene operator-config.yaml.
- Stellen Sie sicher, dass Sie [Abrufen der neuesten Container-Images](#) wenn Sie ein benutzerdefiniertes Repository verwenden.

Stoppen und Starten des Kubernetes-Überwachungsoperators

So stoppen 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

So entfernen Sie den Kubernetes Monitoring Operator

Beachten Sie, dass der Standardnamespace 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 Monitoring-Operators 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>
```

Hinweis: Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt, befolgen Sie die folgenden Anweisungen, um ältere Versionen des Überwachungsoperators zu deinstallieren.

Führen Sie die folgenden Befehle der Reihe nach aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle die Meldung „Objekt nicht gefunden“ zurückgeben. Diese Nachrichten können bedenkenlos 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 zu Kube-State-Metrics finden Sie unter ["diese Seite"](#) .

Konfigurieren/Anpassen des Operators

Diese Abschnitte enthalten Informationen zum Anpassen Ihrer Operatorkonfiguration, zum Arbeiten mit Proxy, zum Verwenden eines benutzerdefinierten oder privaten Docker-Repositorys oder zum Arbeiten mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource vor der Bereitstellung des Operators bearbeiten, indem Sie die Datei *operator-config.yaml* bearbeiten. Diese Datei enthält auskommentierte Beispiele für Einstellungen. Siehe die Liste der ["Verfügbare Einstellungen"](#) für die neueste Version des Operators.

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 Ihre 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 (Nicht gefunden)“ angezeigt wird, muss Ihr Operator aktualisiert werden, bevor Sie die Agentenkonfiguration verwenden können.

Konfigurieren der Proxy-Unterstützung

Es gibt zwei Stellen, an denen Sie einen Proxy auf Ihrem Mandanten verwenden können, um den Kubernetes Monitoring Operator zu installieren. Dabei kann es sich um dasselbe oder um separate Proxy-Systeme handeln:

- Proxy, der während der Ausführung des Installationscode-Snippets (mit „curl“) benötigt wird, um das System, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights -Umgebung zu verbinden
- Proxy, der vom Ziel-Kubernetes-Cluster zur Kommunikation mit Ihrer Data Infrastructure Insights -Umgebung benötigt wird

Wenn Sie für einen oder beide einen Proxy 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/der Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Legen Sie für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, vor der Installation des Operators die Umgebungsvariablen `http_proxy`/`https_proxy` fest. Für einige Proxy-Umgebungen müssen Sie möglicherweise auch die Umgebungsvariable `no_proxy` festlegen.

Um die Variable(n) festzulegen, führen Sie **vor** der Installation des Kubernetes Monitoring Operator die folgenden Schritte auf Ihrem System aus:

1. Legen Sie die Umgebungsvariable(n) `https_proxy` und/oder `http_proxy` für den aktuellen Benutzer fest:
 - a. Wenn der einzurichtende Proxy keine Authentifizierung (Benutzername/Passwort) hat, führen Sie den folgenden Befehl aus:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der einzurichtende Proxy über eine Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie diesen Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Damit der für Ihren Kubernetes-Cluster verwendete Proxy mit Ihrer Data Infrastructure Insights -Umgebung kommunizieren kann, installieren Sie nach dem Lesen aller dieser Anweisungen den Kubernetes Monitoring Operator.

Konfigurieren Sie den Proxy-Abschnitt der 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 ruft der Kubernetes Monitoring Operator Container-Images aus dem Data Infrastructure Insights Repository ab. Wenn Sie einen Kubernetes-Cluster als Ziel für die Überwachung verwenden und dieser Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder Container-Register abrufen, müssen Sie den Zugriff auf die vom Kubernetes Monitoring Operator benötigten Container konfigurieren.

Führen Sie das „Image Pull Snippet“ aus der Installationskachel des NetApp Monitoring Operator aus. Mit diesem Befehl melden Sie sich beim Data Infrastructure Insights -Repository an, rufen alle Bildabhängigkeiten für den Operator ab und melden sich vom Data Infrastructure Insights -Repository ab. Geben Sie bei der entsprechenden Aufforderung das bereitgestellte temporäre Repository-Passwort ein. Dieser Befehl lädt alle vom Bediener verwendeten Bilder herunter, auch für optionale Funktionen. Unten sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Kernoperator-Funktionalität und Kubernetes-Überwachung

- NetApp-Überwachung
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- Distroless-Root-Benutzer

Ereignisprotokoll

- ci-fluent-bit
- ci-kubernetes-event-exporter

Netzwerkleistung und Karte

- ci-net-observer

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in Ihr privates/lokales/Unternehmens-Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Bildern in Ihrem Repository mit denen im Data Infrastructure Insights -Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Überwachungsoperators in `operator-deployment.yaml` und ändern Sie alle Bildreferenzen, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/ci-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 den neuen Speicherort des Docker-Repositorys widerzuspiegeln. 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 verwenden, 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 implementiert möglicherweise eine zusätzliche Sicherheitsebene, die den Zugriff auf einige Kubernetes-Komponenten blockieren kann.

Toleranzen und Makel

Die DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* und *netapp-ci-net-observer-l4-ds* müssen auf jedem Knoten in Ihrem Cluster einen Pod planen, um Daten auf allen Knoten korrekt zu erfassen. Der Operator wurde so konfiguriert, dass er einige bekannte **Verunreinigungen** toleriert. Wenn Sie benutzerdefinierte Taints auf Ihren Knoten konfiguriert haben und dadurch verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie eine **Toleranz** für diese Taints erstellen. ["in der AgentConfiguration"](#) . Wenn Sie benutzerdefinierte Taints auf alle Knoten in Ihrem Cluster angewendet haben, müssen Sie der Operatorbereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Mehr über Kubernetes erfahren ["Makel und Duldungen"](#) .

Zurück zum ["Seite „NetApp Kubernetes Monitoring Operator Installation“"](#)

Eine Anmerkung zu Geheimnissen

Um dem Kubernetes Monitoring Operator die Berechtigung zum Anzeigen von Geheimnissen im gesamten Cluster zu entziehen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *operator-setup.yaml*:

```
ClusterRole/netapp-ci<namespace>-agent-secret
ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

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 Datei *AgentConfiguration* oder *operator-config.yaml*, um den Abschnitt zur Änderungsverwaltung zu kommentieren und *kindsToIgnoreFromWatch*: *"secrets"* in den Abschnitt zur Änderungsverwaltung aufzunehmen. Beachten Sie 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 der Bildsignaturen des Kubernetes-Überwachungsoperators

Das Image für den Operator und alle zugehörigen Images, die er bereitstellt, sind von NetApp signiert. Sie können die Images vor der Installation manuell mit dem Cosign-Tool überprüfen oder einen Kubernetes-Zulassungscontroller konfigurieren. Weitere Einzelheiten finden Sie in der ["Kubernetes-Dokumentation"](#).

Der öffentliche Schlüssel, der zum Überprüfen der Bildsignaturen verwendet wird, ist in der Installationskachel des Überwachungsoperators unter *Optional: Laden Sie die Operatorbilder in Ihr privates Repository hoch > Öffentlicher Schlüssel der Bildsignatur* verfügbar.

Um eine Bildsignatur manuell zu überprüfen, führen Sie die folgenden Schritte aus:

1. Kopieren und führen Sie das Image Pull Snippet aus
2. Kopieren Sie das Repository-Passwort und geben Sie es ein, wenn Sie dazu aufgefordert werden.
3. Speichern Sie den öffentlichen Schlüssel der Bildsignatur (dii-image-signing.pub im Beispiel).
4. Überprüfen Sie die Bilder mit Cosign. Siehe das folgende Beispiel für die Verwendung von Cosign

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"}, "image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Fehlerbehebung

Wenn beim Einrichten des Kubernetes Monitoring Operators Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
Ich sehe keinen Hyperlink/keine Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End-Speichergerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Speicherservers konfiguriert.	Befolgen Sie die Schritte zum Deinstallieren des vorhandenen Telegraf-Agenten und installieren Sie anschließend den neuesten Telegraf-Agenten neu. Sie müssen Telegraf Version 2.0 oder höher verwenden und Ihr Kubernetes-Clusterspeicher muss aktiv von Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie Folgendes:
<p>Ich sehe in den Protokollen Meldungen, die den folgenden ähneln: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.MutatingWebhookConfiguration konnte nicht aufgelistet werden: 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: *v1.Lease konnte nicht aufgelistet werden: Der Server konnte die angeforderte Ressource nicht finden (get leases.coordination.k8s.io) usw.</p>	<p>Diese Meldungen 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: <i>kubectl version</i> So erhalten Sie die kube-state-metrics-Version: <i>kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'</i> Um diese Meldungen zu verhindern, können Benutzer ihre kube-state-metrics-Bereitstellung ändern, um die folgenden Leases zu deaktivieren: <i>mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources</i> Genauer gesagt können sie das folgende CLI-Argument verwenden: <i>resources=certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges,namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas,secrets,services,statefulsets,storageclasses</i> Die Standardressourcenliste ist: „Zertifikatsignaturanforderungen, Konfigurationszuordnungen, Cronjobs, Daemonsets, Bereitstellungen, Endpunkte, horizontale Pod-Autoskalierer, Ingresses, Jobs, Leases, Grenzwertbereiche, mutierende Webhookkonfigurationen, Namespaces, Netzwerkrichtlinien, Knoten, persistente Volumeansprüche, persistente Volumes, Pod-Unterbrechungsbudgets, Pods, Replikatsets, Replikationscontroller, Ressourcenkontingente, Geheimnisse, Dienste, Statefulsets, Speicherklassen, validierende Webhookkonfigurationen, Volumeanhänge“</p>

Problem:	Versuchen Sie Folgendes:
<p>Ich sehe Fehlermeldungen von Telegraf, die den folgenden ähneln, aber Telegraf wird gestartet und ausgeführt: 11. Okt. 14:23:41 ip-172-31-39-47 systemd[1]: Der Plugin-gesteuerte Server-Agent zum Melden von Metriken in InfluxDB wurde gestartet. 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Cache-Verzeichnis konnte nicht erstellt werden. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.cache: Zugriff verweigert. Ignoriert\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="Öffnen fehlgeschlagen. Ignoriert. Öffnen Sie /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: keine solche Datei oder kein solches Verzeichnis\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11. Okt. 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z !! Telegraf 1.19.3 wird gestartet</p>	<p>Dies ist ein bekanntes Problem. Siehe "Dieser GitHub-Artikel" für weitere Details. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.</p>
<p>Auf Kubernetes melden meine Telegraf-Pods den folgenden Fehler: „Fehler beim Verarbeiten der Mountstats-Informationen: Mountstats-Datei konnte nicht geöffnet werden: /hostfs/proc/1/mountstats, Fehler: Öffnen von /hostfs/proc/1/mountstats: Berechtigung verweigert“</p>	<p>Wenn SELinux aktiviert ist und erzwungen wird, verhindert es wahrscheinlich, dass die Telegraf-Pods auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen können. Um diese Einschränkung zu umgehen, bearbeiten Sie die Agentenkonfiguration und aktivieren Sie die Einstellung „runPrivileged“. Weitere Einzelheiten finden Sie in den OpenShift-Anweisungen.</p>
<p>Auf Kubernetes meldet mein Telegraf ReplicaSet-Pod den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Schlüsselpaar /etc/kubernetes/pki/etcd/server.crt konnte nicht geladen werden:/etc/kubernetes/pki/etcd/server.key: öffne /etc/kubernetes/pki/etcd/server.crt: keine solche Datei oder kein solches Verzeichnis</p>	<p>Der Telegraf ReplicaSet-Pod soll auf einem Knoten ausgeführt werden, der als Master oder für etcd bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master-/etcd-Knoten Verunreinigungen aufweisen. Wenn dies der Fall ist, fügen Sie die erforderlichen Toleranzen zum Telegraf ReplicaSet, telegraf-rs, hinzu. Bearbeiten Sie beispielsweise das ReplicaSet ... <code>kubectl edit rs telegraf-rs</code> ... und fügen Sie der Spezifikation die entsprechenden Toleranzen hinzu. Starten Sie dann den ReplicaSet-Pod neu.</p>

Problem:	Versuchen Sie Folgendes:
<p>Ich habe eine PSP/PSA-Umgebung. Betrifft dies meinen Überwachungsbetreiber?</p>	<p>Wenn Ihr Kubernetes-Cluster mit Pod Security Policy (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie auf den neuesten Kubernetes Monitoring Operator aktualisieren. Befolgen Sie diese Schritte, um auf den aktuellen Operator mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren der vorherige Überwachungsoperator: <code>kubectl delete agent agent-monitoring-netapp -n netapp-monitoring</code> <code>kubectl delete ns netapp-monitoring</code> <code>kubectl delete crd agents.monitoring.netapp.com</code> <code>kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader</code> <code>kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding</code> 2. Installieren die neueste Version des Überwachungsoperators.</p>
<p>Beim Versuch, den Operator bereitzustellen, sind mir Probleme begegnet, und ich verwende PSP/PSA.</p>	<p>1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: <code>kubectl -n <name-space> edit agent</code> 2. Markieren Sie „security-policy-enabled“ als „false“. Dadurch werden die Pod-Sicherheitsrichtlinien und die Pod-Sicherheitszulassung deaktiviert und dem Operator die Bereitstellung ermöglicht. Bestätigen Sie mit den folgenden Befehlen: <code>kubectl get psp</code> (sollte anzeigen, dass die Pod-Sicherheitsrichtlinie entfernt wurde) <code>kubectl get all -n <namespace></code></p>
<p><code>grep -i psp</code> (sollte anzeigen, dass nichts gefunden wurde)</p>	<p>„ImagePullBackoff“-Fehler aufgetreten</p>
<p>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 es ordnungsgemäß erkannt wird. Mehr lesen Informationen zur Konfiguration für benutzerdefinierte/private Repos.</p>	<p>Ich habe ein Problem mit der Bereitstellung meines Überwachungsoperators und die aktuelle Dokumentation hilft mir nicht bei der Lösung.</p>

Problem:	Versuchen Sie Folgendes:
<p>Erfassen oder notieren Sie die Ausgabe der folgenden Befehle und wenden Sie sich an das technische Supportteam.</p> <pre> kubect1 -n netapp-monitoring get all kubect1 -n netapp-monitoring describe all kubect1 -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true kubect1 -n netapp-monitoring logs <telegraf-pod> --all -containers=true </pre>	<p>Net-Observer-Pods (Workload Map) im Operator-Namespace befinden sich in CrashLoopBackOff</p>
<p>Diese Pods entsprechen dem Workload Map-Datensammler für die Netzwerkbeobachtung. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die Mindestkernelversion zu bestätigen. Beispiel: ---- {"ci-tenant-id":"Ihre Mandanten-ID","collector-cluster":"Ihr K8S-Clustername","environment":"prod","level":"error","msg":"Validierung fehlgeschlagen. Grund: Kernelversion 3.10.0 ist niedriger als die Mindestkernelversion 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Net-Observer-Pods erfordern mindestens die Linux-Kernelversion 4.18.0. Überprüfen Sie die Kernelversion mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 ist</p>	<p>Pods werden im Operator-Namespace ausgeführt (Standard: Netapp-Monitoring), aber in der Benutzeroberfläche werden keine Daten für die Workload-Map oder Kubernetes-Metriken in Abfragen angezeigt.</p>
<p>Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Computer mithilfe des Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.</p>	<p>Einige der Net-Observer-Pods im Operator-Namespace befinden sich im Status „Ausstehend“</p>
<p>Net-Observer ist ein DaemonSet 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 die CPU oder den Speicher vorliegt. Stellen Sie sicher, dass im Knoten genügend Speicher und CPU verfügbar sind.</p>	<p>Unmittelbar nach der Installation des Kubernetes Monitoring Operator wird mir in meinen Protokollen Folgendes angezeigt: [inputs.prometheus] Fehler im Plug-In: Fehler beim Senden der 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: no such host</p>

Problem:	Versuchen Sie Folgendes:
Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert wird und der <i>telegraf-rs</i> -Pod vor dem <i>ksm</i> -Pod aktiv ist. Diese Nachrichten sollten aufhören, sobald alle Pods ausgeführt werden.	Ich sehe keine erfassten Metriken für die in meinem Cluster vorhandenen Kubernetes-CronJobs.
Überprüfen Sie Ihre Kubernetes-Version (d. h. <code>kubectl version</code>). Wenn es sich um v1.20.x oder niedriger handelt, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator bereitgestellte Version von kube-state-metrics unterstützt nur v1.CronJob. Bei Kubernetes 1.20.x und darunter befindet sich die CronJob-Ressource unter v1beta.CronJob. Aus diesem Grund kann kube-state-metrics die CronJob-Ressource nicht finden.	Nach der Installation des Operators treten die Telegraf-DS-Pods in CrashLoopBackOff ein und die Pod-Protokolle zeigen „su: Authentifizierungsfehler“ an.
Bearbeiten Sie den Telegraf-Abschnitt in <i>AgentConfiguration</i> und setzen Sie <i>dockerMetricCollectionEnabled</i> auf „false“. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers. "Konfigurationsoptionen" Spezifikation: ... Telegraf: ... - Name: Docker-Ausführungsmodus: - DaemonSet-Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCKET_PLACEHOLDER-Wert: unix:///run/docker.sock	In meinen Telegraf-Protokollen werden immer wieder Fehlermeldungen angezeigt, die den folgenden ähneln: E! [Agent] Fehler beim Schreiben in outputs.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": Kontextfrist überschritten (Client.Timeout beim Warten auf Header überschritten)
Bearbeiten Sie den Telegraf-Abschnitt in <i>AgentConfiguration</i> und erhöhen Sie <i>outputTimeout</i> auf 10 s. Weitere Einzelheiten finden Sie in der Betriebsanleitung des Betreibers. "Konfigurationsoptionen" .	Mir fehlen <i>involvedobject</i> -Daten für einige Ereignisprotokolle.
Stellen Sie sicher, dass Sie die Schritte in der "Berechtigungen" Abschnitt oben.	Warum werden zwei Überwachungsoperator-Pods ausgeführt, einer mit dem Namen netapp-ci-monitoring-operator-<pod> und der andere mit dem Namen monitoring-operator-<pod>?
Ab dem 12. Oktober 2023 hat Data Infrastructure Insights den Operator überarbeitet, um unseren Benutzern einen besseren Service zu bieten. Damit diese Änderungen vollständig übernommen werden können, müssen Sie Entfernen Sie den alten Operator Und installieren Sie die neue .	Meine Kubernetes-Ereignisse wurden unerwartet nicht mehr an Data Infrastructure Insights gemeldet.
Rufen Sie den Namen des Event-Exporter-Pods ab: <div><pre>`kubectl -n netapp-monitoring get pods`</pre></div>	grep event-exporter

Problem:	Versuchen Sie Folgendes:
awk '{print \$1}'	<p>sed 's/event-exporter./event-exporter/'</p> <p>Es sollte entweder „netapp-ci-event-exporter“ oder „event-exporter“ sein. Bearbeiten Sie als Nächstes den Überwachungsagenten <code>kubectl -n netapp-monitoring edit agent</code> und legen Sie den Wert für <code>LOG_FILE</code> so fest, dass er den entsprechenden Event-Exporter-Pod-Namen widerspiegelt, der im vorherigen Schritt gefunden wurde. Genauer gesagt sollte <code>LOG_FILE</code> entweder auf <code>"/var/log/containers/netapp-ci-event-exporter.log"</code> oder <code>"/var/log/containers/event-exporter*.log"</code> gesetzt werden.</p> <p>....</p> <p>fluent-bit:</p> <p>...</p> <ul style="list-style-type: none"> - name: event-exporter-ci <p>substitutions:</p> <ul style="list-style-type: none"> - key: LOG_FILE <p>values:</p> <ul style="list-style-type: none"> - /var/log/containers/netapp-ci-event-exporter*.log <p>...</p> <p>....</p> <p>Alternativ kann man auch deinstallieren Und Neuinstallation der Agent.</p>
Ich sehe, dass vom Kubernetes Monitoring Operator bereitgestellte Pods aufgrund unzureichender Ressourcen abstürzen.	Siehe den Kubernetes Monitoring Operator "Konfigurationsoptionen" um die CPU- und/oder Speichergrenzen nach Bedarf zu erhöhen.
Ein fehlendes Image oder eine ungültige Konfiguration führte dazu, dass die netapp-ci-kube-state-metrics-Pods nicht gestartet werden konnten oder nicht bereit waren. Jetzt steckt das StatefulSet fest und Konfigurationsänderungen werden nicht auf die Netapp-CI-Kube-State-Metrics-Pods angewendet.	Das StatefulSet ist in einem "gebrochen" Zustand. Nachdem Sie alle Konfigurationsprobleme behoben haben, führen Sie einen Bounce der Netapp-CI-Kube-State-Metrics-Pods durch.
netapp-ci-kube-state-metrics-Pods können nach der Ausführung eines Kubernetes Operator-Upgrades nicht gestartet werden und lösen ErrImagePull aus (das Abrufen des Images schlägt fehl).	Versuchen Sie, die Pods manuell zurückzusetzen.
Bei der Protokollanalyse werden für meinen Kubernetes-Cluster Meldungen vom Typ „Ereignis verworfen, da es älter ist als maxEventAgeSeconds“ beobachtet.	Ändern Sie die Operator-Agentenkonfiguration und erhöhen Sie <code>event-exporter-maxEventAgeSeconds</code> (z. B. auf 60 s), <code>event-exporter-kubeQPS</code> (z. B. auf 100) und <code>event-exporter-kubeBurst</code> (z. B. auf 500). Weitere Einzelheiten zu diesen Konfigurationsoptionen finden Sie im "Konfigurationsoptionen" Seite.

Problem:	Versuchen Sie Folgendes:
<p>Telegraf warnt vor unzureichendem sperrbaren Speicher oder stürzt ab.</p>	<p>Versuchen Sie, das Limit des sperrbaren Speichers für Telegraf im zugrunde liegenden Betriebssystem/Knoten zu erhöhen. Wenn eine Erhöhung des Limits keine Option ist, ändern Sie die NKMO-Agentenkonfiguration und setzen Sie <i>unprotected</i> auf <i>true</i>. Dadurch wird Telegraf angewiesen, keinen Versuch zu unternehmen, gesperrte Speicherseiten zu reservieren. Dies kann zwar ein Sicherheitsrisiko darstellen, da entschlüsselte Geheimnisse möglicherweise auf die Festplatte ausgelagert werden, ermöglicht jedoch die Ausführung in Umgebungen, in denen die Reservierung gesperrten Speichers nicht möglich ist. Weitere Informationen zu den <i>ungeschützten</i> Konfigurationsoptionen finden Sie im "Konfigurationsoptionen" Seite.</p>
<p>Ich sehe Warnmeldungen von Telegraf, die etwa wie folgt aussehen: <i>W! [inputs.diskio] Der Datenträgername für „vdc“ konnte nicht ermittelt werden: Fehler beim Lesen von /dev/vdc: keine solche Datei oder kein solches Verzeichnis</i></p>	<p>Für den Kubernetes Monitoring Operator sind diese Warnmeldungen harmlos und können ignoriert werden. Alternativ können Sie den Abschnitt „Telegraf“ in der AgentConfiguration bearbeiten und <i>runDsPrivileged</i> auf „true“ setzen. Weitere Einzelheiten finden Sie im "Konfigurationsoptionen des Betreibers".</p>

Problem:	Versuchen Sie Folgendes:
<p>Mein Fluent-Bit-Pod schlägt mit den folgenden Fehlern fehl: [2024/10/16 14:16:23] [Fehler] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Zu viele offene Dateien [2024/10/16 14:16:23] [Fehler] Initialisierung der Eingabe tail.0 fehlgeschlagen [2024/10/16 14:16:23] [Fehler] [Engine] Initialisierung der Eingabe fehlgeschlagen</p>	<p>Versuchen Sie, Ihre <i>fsnotify</i>-Einstellungen in Ihrem Cluster zu ändern:</p> <div data-bbox="821 258 1484 957" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> sudo sysctl fs.inotify.max_user_instances (take note of setting) sudo sysctl fs.inotify.max_user_instances=<something larger than current setting> sudo sysctl fs.inotify.max_user_watches (take note of setting) sudo sysctl fs.inotify.max_user_watches=<something larger than current setting> </pre> </div> <p>Starten Sie Fluent-bit neu.</p> <p>Hinweis: Um diese Einstellungen auch nach einem Neustart des Knotens dauerhaft zu halten, müssen Sie die folgenden Zeilen in <i>/etc/sysctl.conf</i> einfügen.</p> <div data-bbox="821 1190 1484 1449" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting> </pre> </div>

Problem:	Versuchen Sie Folgendes:
Die Telegraf DS-Pods melden Fehler im Zusammenhang mit dem Kubernetes-Eingabe-Plugin, das keine HTTP-Anfragen stellen kann, da das TLS-Zertifikat nicht validiert werden kann. Zum Beispiel: E! [inputs.kubernetes] Fehler im Plugin: Fehler beim Senden einer HTTP-Anfrage an"<a href="https://<kubelet_IP>;10250/stats/summary": " class="bare">https://<kubelet_IP>;10250/stats/summary": Erhalten"<a href="https://<kubelet_IP>;10250/stats/summary": " class="bare">https://<kubelet_IP>;10250/stats/summary": tls: Zertifikat konnte nicht überprüft werden: x509: Zertifikat für <kubelet_IP> kann nicht validiert werden, da es keine IP-SANs enthält	Dies tritt auf, wenn das Kubelet selbstsignierte Zertifikate verwendet und/oder das angegebene Zertifikat die <kubelet_IP> nicht in der Liste „Subject Alternative Name“ des Zertifikats enthält. Um dieses Problem zu lösen, kann der Benutzer die " Agentenkonfiguration ", und setzen Sie <code>telegraf:insecureK8sSkipVerify</code> auf <code>true</code> . Dadurch wird das Telegraf-Eingabe-Plugin so konfiguriert, dass die Überprüfung übersprungen wird. Alternativ kann der Benutzer das Kubelet konfigurieren für " serverTLSBootstrap ", wodurch eine Zertifikatsanforderung von der API „certificates.k8s.io“ ausgelöst wird.

Weitere Informationen finden Sie in der "[Support](#)" Seite oder in der "[Datensammler-Supportmatrix](#)".

Memcached-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Memcached Configuration

Gathers Memcached metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-memcached.conf file.

```
[[inputs.memcached]]
  ## USER-ACTION: Provide comma-separated list of Memcached IP(s) and port(s).
  ## Please specify actual machine IP address, and refrain from using a loopback address
  (i.e. localhost or 127.0.0.1).
  ## When configuring with multiple Memcached servers, enter them in the format ["server1"
```

- 2 Replace <INSERT_MEMCACHED_ADDRESS> with the applicable Memcached server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_MEMCACHED_PORT> with the applicable Memcached server port.
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im "[Memcached-Wiki](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Memcached	Namespace-Server	Knoten-IP Knotenname	Verbindungen annehmen Bearbeitete Authentifizierungsanfrage n Fehlgeschlagene Authentifizierungen Verwendete Bytes Gelesene Bytes (pro Sek.) Geschriebene Bytes (pro Sek.) CAS Badval CAS-Treffer CAS-Fehlschläge Flush-Anforderungen (pro Sek.) Get-Anforderungen (pro Sek.) Set-Anforderungen (pro Sek.) Touch-Anforderungen (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Offene Verbindungen Aktuell gespeicherte Elemente Decr-Anforderungen Treffer (pro Sek.) Decr-Anforderungen Fehlschläge (pro Sek.) Löschenanforderungen Treffer (pro Sek.) Löschenanforderungen Fehlschläge (pro Sek.) Ausgewiesene Elemente Gültige Ausweisungen Abgelaufene Elemente Get-Treffer (pro Sek.) Get-Fehlschläge (pro Sek.) Verwendete Hash-Bytes Hash wird erweitert Hash-Leistungsstufe Incr-Anforderungen Treffer (pro Sek.) Incr-Anforderungen Fehlschläge (pro Sek.) Server Max. Bytes Listen Deaktiviert Anzahl zurückgeforderte Worker-Threads Anzahl insgesamt geöffnete Verbindungen

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

MongoDB-Datensammler

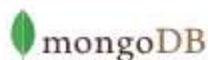
Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von MongoDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MongoDB.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



MongoDB Configuration

Gathers MongoDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

 RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Open mongod.conf. Locate the line beginning with "bindIp", and append the address of the node on which the Telegraf agent resides. After saving the change, restart the MongoDB server.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-mongodb.conf file.

```
[[inputs.mongodb]]
  ## An array of URLs of the form:
  ## "mongodb://" [user ":" pass "@"] host [ ":" port]
  ## For example:
  ## mongodb://user:auth_key@10.10.3.30:27017,
  ## mongodb://10.10.3.30:27017
```

- 3 Replace <INSERT_MONGODB_ADDRESS> with the applicable MongoDB server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_MONGODB_PORT> with the applicable MongoDB port.
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie im ["MongoDB-Dokumentation"](#).

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MongoDB	Namespace-Hostname		

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MongoDB-Datenbank	Namespace Hostname Datenbankname		

Fehlerbehebung

Informationen finden Sie im ["Support"](#) Seite.

MySQL-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



MySQL Configuration

Gathers MySQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-mysql.conf file.

```
[[inputs.mysql]]
  ## USER-ACTION: Provide comma-separated list of mysql credentials, IP(s), and port(s)
  ## e.g. servers = ["user:passwd@tcp(127.0.0.1:3306)?tls=false"]
  ## Please specify actual machine IP address, and refrain from using a loopback address
  (i.e. localhost or 127.0.0.1).
```

- 2 Review and verify the contents of the configuration file.
- 3 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable MySQL credentials.
- 4 Replace <INSERT_PROTOCOL> with the applicable MySQL connection protocol. The typical protocol is tcp.
- 5 Replace <INSERT_MYSQL_ADDRESS> with the applicable MySQL server address. Please specify a real machine address, and refrain from using a loopback address.
- 6 Replace <INSERT_MYSQL_PORT> with the applicable MySQL server port. The typical port is 3306.
- 7 Modify the 'tls' parameter in accordance to the MySQL server configuration.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im ["MySQL-Dokumentation"](#).

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
MySQL	Namespace MySQL-Server	Knoten-IP Knotenname	Abgebrochene Clients (pro Sek.) Abgebrochene Verbindungen (pro Sek.) RX-Bytes (pro Sek.) TX-Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Ereignis ändern Befehle Funktion ändern Befehle Instanz ändern Befehle Prozedur ändern Befehle Server ändern Befehle Tabelle ändern Befehle Tablespace ändern Befehle Benutzer ändern Befehle Analysieren Befehle Zu Keycache zuweisen Befehle Beginnen Befehle Binlog Befehle Prozedur aufrufen Befehle DB ändern Befehle Master ändern Befehle Repl ändern Filterbefehle Prüfen Befehle Prüfsummenbefehle Commit Befehle DB erstellen Befehle Ereignis erstellen Befehle Funktion erstellen Befehle Index erstellen Befehle Prozedur erstellen Befehle Server erstellen Befehle Tabelle erstellen Befehle Trigger erstellen Befehle UDF erstellen Befehle Benutzer erstellen Befehle Ansicht erstellen Befehle Dealloc SQL-Verbindungsfehler Akzeptieren Erstellte temporäre Datenträgertabellen Verzögerte Fehler Befehle leeren Handler Commit InnoDB-Pufferpool Bytes Daten Schlüsselblöcke nicht geleert Schlüsselseanforderungen Schlüsselschreibanforderungen Schlüsselschreibvorgänge Max. Ausführungszeit überschritten Max. verwendete Verbindungen Geöffnete Dateien

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Netstat-Datensammler

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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.

Netstat Configuration

Gathers netstat metrics of the host where telegraf agent is installed.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)
+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-netstat.conf file.

```
# Read TCP metrics such as established, time wait and sockets counts.
[[inputs.netstat]]
# no configuration
[inputs.netstat.tags]
  CloudInsights = "true"
```
- Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Netstat	Knoten-UUID	Knoten-IP Knotenname	

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Nginx-Datensammler


Data Infrastructure Insights verwendet diesen Datensammler, um Metriken 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das "[Agenteninstallation](#)" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Nginx Configuration
Gathers Nginx metrics.

What Operating System or Platform Are You Using?[Need Help?](#)

 Ubuntu & Debian

▼

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

▼

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.
- 2 Nginx metrics are available through a status page when the HTTP stub status module is enabled. Refer to the below link for verifying/enabling `http_stub_status_module`.

```
http://nginx.org/en/docs/http/nginx_http_stub_status_module.html
```

- 3 After verifying the module is enabled, modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {  
    listen    <PORT NUMBER>;  
    Please specify actual machine IP address, and refrain from using a loopback address (i.e.  
    localhost or 127.0.0.1)  
    server_name <IP ADDRESS>;  
    location /nginx_status {  
        stub_status on;  
    }  
}
```

- 4 Reload the configuration:

```
nginx -s reload
```

- 5 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-nginx.conf` file.

```
[[inputs.nginx]]  
  ## USER-ACTION: Provide Nginx status url  
  ## Please specify actual machine IP address where nginx_status is enabled, and refrain from  
  using a loopback address (i.e. localhost or 127.0.0.1).  
  ## When configuring with multiple Nginx servers, enter them in the format ["url1", "url2",  
  "url3"]
```

- 6 Replace `<INSERT_NGINX_ADDRESS>` with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.
- 7 Replace `<INSERT_NGINX_PORT>` with the applicable Nginx port.
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Die Nginx-Metriksammlung erfordert, dass Nginx "[http_stub_status_module](#)" aktiviert werden.

Weitere Informationen finden Sie in der "[Nginx-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Nginx	Namespace-Server	Knoten-IP Knotenname Port	Akzeptiert Aktive bearbeitete Leseanfragen Wartende Schreibanfragen

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

PostgreSQL-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



PostgreSQL Configuration

Gathers PostgreSQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-postgresql.conf file.

```
[[inputs.postgresql]]
# USER-ACTION: Provide credentials for access, address of PostgreSQL server, port for
PostgreSQL server, one DB for access
address = "postgres://<INSERT_USERNAME>:<INSERT_PASSWORD>@<INSERT_POSTGRESQL_ADDRESS>:
<INSERT_POSTGRESQL_PORT>/<INSERT_DB>"
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable PostgreSQL credentials.
- 3 Replace <INSERT_POSTGRESQL_ADDRESS> with the applicable PostgreSQL address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_POSTGRESQL_PORT> with the applicable PostgreSQL port.
- 5 Replace <INSERT_DB> with the applicable PostgreSQL database.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
systemctl restart telegraf
```

Aufstellen

Informationen finden Sie im ["PostgreSQL-Dokumentation"](#) .

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
PostgreSQL-Server	Namespace-Datenbankserver	Knotenname Knoten-IP	Puffer Zugewiesene Puffer Backend-Puffer Backend-Dateisynchronisierungspuffer Checkpoint-Puffer Saubere Checkpoints Synchronisierungszeit Checkpoints Schreibzeit Checkpoints Anfragen Checkpoints Zeitlich begrenzt Max Geschrieben Sauber
PostgreSQL-Datenbank	Namespace-Datenbankserver	Datenbank-OID Knotenname Knoten-IP	Blöcke Lesezeit Blöcke Schreibzeit Blöcke Treffer Blöcke Lesevorgänge Konflikte Deadlocks Client Anzahl Temp. Dateien Bytes Temp. Dateien Anzahl Zeilen Gelöschte Zeilen Abgerufene Zeilen Eingefügte Zeilen Zurückgegebene Zeilen Aktualisierte Transaktionen Festgeschriebene Transaktionen Zurückgesetzte Transaktionen

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Puppet Agent-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken 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 der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Puppet Agent Configuration
Gathers Puppet agent metrics.

What Operating System or Platform Are You Using?[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps[Need Help?](#)

1

Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-puppetagent.conf file.

```
## Reads last_run_summary.yaml file and converts to measurements
[[inputs.puppetagent]]
  ## Location of puppet last run summary file
  ## USER-ACTION: Modify the location if last_run_summary.yaml is on different path
  location = "/var/lib/puppet/state/last_run_summary.yaml"
```

2

Modify 'location' if last_run_summary.yaml is on different path

3

Modify 'Namespace' if needed for puppet agent disambiguation (to avoid name clashes).

4

Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im "[Puppet-Dokumentation](#)"

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
---------	------------	-----------	--------------

Puppenagent	Namespace-Knoten-UUID	Knotenname Standort Knoten-IP-Version Konfigurationszeichenfolge-Version Puppet	Änderungen Gesamtereignisse Fehlerereignisse Erfolgsereignisse Gesamtressourcen Geänderte Ressourcen Fehlgeschlagene Ressourcen Neustart fehlgeschlagene Ressourcen Nicht synchronisierte Ressourcen Neu gestartete Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Konfigurationsabrufzeit Cron-Zeit Ausführungszeit Dateizeit Filebucket-Zeit Lastrun-Zeit Paketzeit Zeitplanzeit Servicezeit Sshauthorizedkey-Zeit Gesamtzeit Benutzer
-------------	-----------------------	---	---

Fehlerbehebung

Weitere Informationen finden Sie in der ["Support"](#) Seite.

Redis-Datensammler

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Redis zu sammeln. Redis ist ein Open-Source-Datenstrukturspeicher im Arbeitsspeicher, der als Datenbank, Cache und Nachrichtenbroker verwendet wird und die folgenden Datenstrukturen unterstützt: Zeichenfolgen, Hashes, Listen, Sets und mehr.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Redis.

Wählen Sie das Betriebssystem oder die Plattform aus, auf der der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten für die Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das ["Agenteninstallation"](#) Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel zur Verwendung mit diesem Datensammler aus. Sie können einen neuen Agentenzugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agentenzugriffsschlüssel** klicken. Best Practice: Verwenden Sie nur dann einen anderen Agent-Zugriffsschlüssel, wenn Sie Datensammler beispielsweise nach Betriebssystem/Plattform gruppieren möchten.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen variieren je nach Art des Betriebssystems oder der Plattform, die Sie zum Sammeln von Daten verwenden.



Redis Configuration

Gathers Redis metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Configure Redis to accept connections from the address of the node on which the Telegraf agent resides. Open the Redis configuration file.

```
vi /etc/redis.conf
```

- 2 Locate the line that begins with 'bind 127.0.0.1', and append the address of the node on which the Telegraf agent resides

```
bind 127.0.0.1 <NODE_IP_ADDRESS>
```

- 3 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-redis.conf file.

```
# Read metrics from one or many redis servers
[[inputs.redis]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## tcp://username:password@127.0.0.1:6379
```

- 4 Replace <INSERT_REDIS_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.

- 5 Replace <INSERT_REDIS_PORT> with the applicable Redis port.

- 6 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Aufstellen

Informationen finden Sie im "[Redis-Dokumentation](#)".

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Merkmale:	Datenpunkte:
Redis	Namespace-Server		

Fehlerbehebung

Weitere Informationen finden Sie in der"Support" Seite.

Objektsymbolreferenz

In Data Infrastructure Insights verwendete Objektsymbole.

Infrastruktursymbole:

Storage

BSA

Backend Storage Array

BV

Backend Volume

D

Disk

IV

Internal Volume

M

Masking

P

Path

Q

Q-Tree

Qu

Quota

Sh

Share

S

Storage

SN

Storage Node

SP

Storage Pool

T

Tape

V

Volume

VSA

Virtual Storage Array

VV

Virtual Volume

Networking

F

Fabric

INP

ISCSI Network Portal

IS

ISCSI Session

NAS

NAS

NPV

NPV Switch

NPV

NPV Chassis

P

Port

S

Switch

Z

Zone

ZM

Zone Members

Compute

DS

Datastore

H

Host

VM

Virtual Machine

VMDK

VMDK

Application

A

Application

Misc.

?

Unknown

?

Generic

!

Violation

!

Failure

Kubernetes-Symbole:



Cluster



Namespace



Workload



Node



Pod

Überwachung der Netzwerkleistung von Kubernetes und Kartensymbole:



Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.